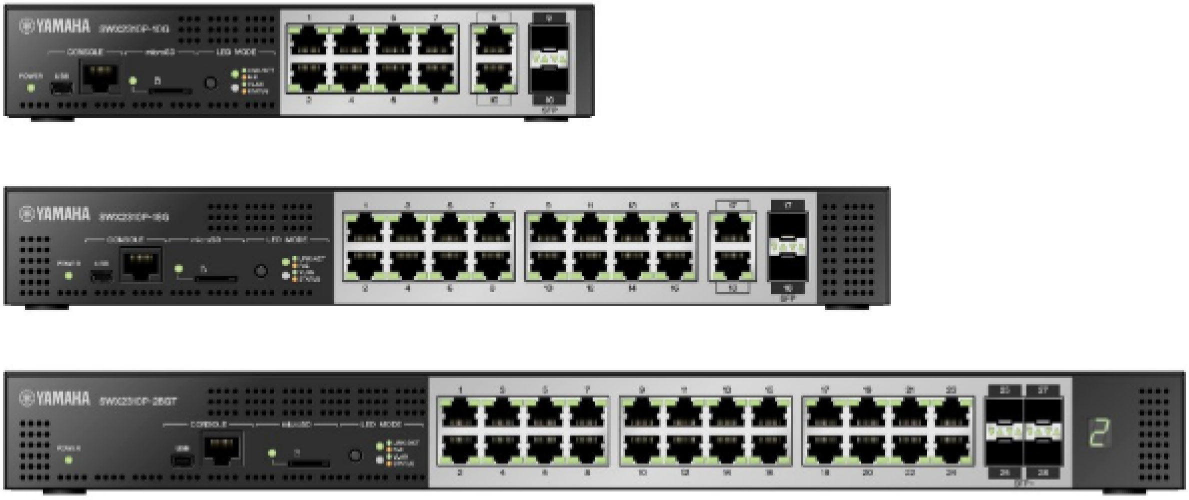
YAMAHA

SWX2310P series

Technical Data



EN

Contents

Important Notice . . . 1
  Login Security . . . 1
    Function Overview . . . 1
    Applicable Models and Revisions . . . 1
    Precautions When Updating Firmware . . . 2
    Related Documentation . . . 3
Maintenance and Operation Functions . . . 4
  User Account Management . . . 4
    Function Overview . . . 4
    Definition of Terms Used . . . 4
    Function Details . . . 4
      User account function settings . . . 4
      User authentication . . . 5
      What to do if you forget your login password . . . 8
    Related Commands . . . 8
    Examples of Command Execution . . . 9
      Adding a user . . . 9
    Points of Caution . . . 9
    Related Documentation . . . 10
  LED Control . . . 11
    Function Overview . . . 11
    Definition of Terms Used . . . 11
    Function Details . . . 11
      POWER LED . . . 11
      SD LED . . . 12
      Port LED . . . 12
      Stack ID display LED . . . 19
    Related Commands . . . 19
    Examples of Command Execution . . . 19
      Checking LAN/SFP port status . . . 20
      Checking LAN/SFP port loop detection status . . . 20
      Set default LED mode . . . 21
  Use of External Memory . . . 22
    Function Overview . . . 22
    Definition of Terms Used . . . 22
    Function Details . . . 22
      External memory that can be used . . . 22
      Folder structure . . . 22
      Mounting and unmounting the SD card . . . 23
      SD card boot (firmware, config) . . . 23
      Applying SD card booting automatically (firmware, config) . . . 24
      Firmware Update . . . 26
      Saving and copying a config file . . . 26
      Saving a log file . . . 26
      Saving technical support information . . . 26
      Saving statistical information . . . 27

Backing up and restoring system information . . . 27
List of related commands . . . 27
Examples of Command Execution . . . 28
Unmount SD card . . . 28
Mount SD card . . . 28
Back up log file . . . 28
Saving technical support information . . . 28
Points of Caution . . . 29
Related Documentation . . . 29
Boot Information Management . . . 30
Function Overview . . . 30
Related Commands . . . 30
Examples of Command Execution . . . 30
Show boot information . . . 30
Clear boot information . . . 31
Points of Caution . . . 31
Related Documentation . . . 31
Show Chassis Information . . . 32
Function Overview . . . 32
Function Details . . . 32
Use commands to show chassis information . . . 32
Obtain technical support information remotely . . . 35
Save technical support information on external memory . . . 36
Related Commands . . . 36
Examples of Command Execution . . . 36
Show inventory information . . . 36
Show operating information . . . 37
Show technical support information . . . 37
Points of Caution . . . 38
Related Documentation . . . 38
System Self-Diagnostics . . . 39
Function Overview . . . 39
Definition of Terms Used . . . 39
Function Details . . . 39
Diagnostics . . . 39
Diagnostic results displayed . . . 40
Deleting on-demand diagnostics results . . . 40
Test Details . . . 40
Loading Test . . . 40
RTC Test . . . 41
Packet Processor Test . . . 41
PHY Test . . . 41
Thermal Test . . . 41
Fan Test . . . 41
Thermal Sensor Test . . . 41
PoE Test . . . 41
SFP Test . . . 41
Related Commands . . . 41

Examples of Command Execution . . . 42
Display system self-diagnostic results . . . 42
Performing on-demand diagnostics . . . 43
Discard on-demand diagnostics results . . . 43
Points of Caution . . . 43
Related Documentation . . . 43
Cable Diagnostics . . . 44
Function Overview . . . 44
Definition of Terms Used . . . 44
Function Details . . . 44
How to diagnose cables . . . 44
Related Commands . . . 44
Examples of Command Execution . . . 45
Perform the cable diagnostics . . . 45
Checking previous diagnostic results . . . 45
Points of Caution . . . 45
Related Documentation . . . 45
Config Management . . . 46
Function Overview . . . 46
Definition of Terms Used . . . 46
Function Details . . . 46
Running config . . . 46
Startup config . . . 46
Default config . . . 47
Deciding the config file at startup . . . 47
Controlling the config file via TFTP . . . 47
Related Commands . . . 48
Examples of Command Execution . . . 49
Select startup config . . . 49
Save running config . . . 49
Copy startup config . . . 49
Erase startup config . . . 50
Points of Caution . . . 50
Related Documentation . . . 50
Remote Access Control . . . 51
Function Overview . . . 51
Definition of Terms Used . . . 51
Function Details . . . 51
Related Commands . . . 52
Examples of Command Execution . . . 53
TELNET server access control . . . 53
SSH server access control . . . 54
HTTP server access restrictions . . . 54
TFTP server access restrictions . . . 55
SNMP server access restrictions . . . 55
Points of Caution . . . 55
Related Documentation . . . 56
Time Management . . . 57

Function Overview . . . 57
Definition of Terms Used. . . . 57
Function Details . . . 57
Manually setting the date and time . . . 57
Automatically setting the date and time . . . 57
Time zone setting. . . . 58
Daylight saving time setting . . . 58
Related Commands . . . 58
Examples of Command Execution . . . 59
Set clock manually . . . 59
Automatically setting the time . . . 59
Daylight saving time setting . . . 59
Points of Caution . . . 60
Related Documentation . . . 60
SNMP. . . . 61
Function Overview . . . 61
Definition of Terms Used. . . . 61
Function Details . . . 61
SNMPv1 . . . 61
SNMPv2c. . . . 62
SNMPv3. . . . 62
Restricting SNMP server access . . . 63
Private MIBs . . . 63
Related Commands . . . 63
Examples of Command Execution . . . 64
SNMPv1 setting example . . . 64
SNMPv2c setting example . . . 64
SNMPv3 setting example . . . 65
Points of Caution . . . 65
Related Documentation . . . 66
RMON . . . 67
Function Overview . . . 67
Definition of Terms Used. . . . 67
Function Details . . . 67
Common between groups . . . 68
Ethernet statistics group . . . 68
History group . . . 69
Alarm group . . . 70
Event group . . . 72
Setting by SetRequest from an SNMP manager. . . . 72
Related Commands . . . 73
Examples of Command Execution . . . 74
Setting an Ethernet statistics group. . . . 74
Setting a history group. . . . 74
Setting an alarm event group . . . 75
Points of Caution . . . 76
Related Documentation . . . 76
sFlow . . . 77

Function Overview . . . 77
Definition of Terms Used. . . . 78
Function Details . . . 78
Related Commands . . . 79
Examples of Command Execution . . . 80
Points of Caution . . . 80
Related Documentation . . . 81
SYSLOG . . . 82
Function Overview . . . 82
Definition of Terms Used. . . . 82
Function Details . . . 82
List of related commands . . . 83
Examples of Command Settings . . . 83
Points of Caution . . . 84
Related Documentation . . . 84
Firmware Update . . . 85
Function Overview . . . 85
Definition of Terms Used. . . . 85
Function Details . . . 85
Update by transmitting the firmware update . . . 85
Using an HTTP client to update the firmware . . . 86
Update using an SD card . . . 88
Reboot after writing . . . 88
Related Commands . . . 89
Examples of Command Execution . . . 89
Using an HTTP client to update the firmware . . . 89
Using an HTTP client to update the firmware (in a proxy server environment) . . . 90
Update using an SD card . . . 91
Points of Caution . . . 92
Related Documentation . . . 92
L2MS (Layer2 Management Service). . . . 93
Function Overview . . . 93
Definition of Terms Used. . . . 93
Function Details . . . 94
Compatible models . . . 94
Usage . . . 94
L2MS protocol . . . 95
Monitoring agents . . . 95
Agent ownership. . . . 95
Agent operations . . . 96
Information notifications from agents. . . . 98
Monitoring connected terminals . . . 100
Related Commands . . . 101
Examples of Command Execution . . . 102
Monitoring settings for agents . . . 102
Enable terminal management function . . . 102
Enable sending/receiving L2MS control frames . . . 103
Enable event monitoring function . . . 103

Enabling/disabling the zero-config function . . . 103
Points of Caution . . . 104
Device configuration . . . 104
Terminal monitoring . . . 104
Use in conjunction with other functionality . . . 105
SYSLOG Message List . . . 106
Related Documentation . . . 116
Mail Notification . . . 117
Function Overview . . . 117
Definition of Terms Used . . . 117
Function Details . . . 117
Action . . . 117
Mail server settings . . . 117
Specify the mail template . . . 118
Functions that support mail notification . . . 119
Mail body example . . . 122
Related Commands . . . 127
Points of Caution . . . 127
Related Documentation . . . 128
LLDP . . . 129
Function Overview . . . 129
Definition of Terms Used . . . 129
Function Details . . . 129
Operating specifications . . . 129
TLV list . . . 131
Supported MIBs . . . 134
Related Commands . . . 134
Examples of Command Execution . . . 135
Set LLDP frame transmission/reception . . . 135
Show LLDP interface status . . . 136
Show LLDP connected device information . . . 136
Points of Caution . . . 137
Related Documentation . . . 137
LLDP Automatic Setting (Access Point Link) . . . 138
Function Overview . . . 138
Definition of Terms Used . . . 138
LLDP . . . 138
Function Details . . . 138
Basic specifications . . . 138
RADIUS server automatic settings . . . 139
Yamaha wireless access point dead/alive monitoring . . . 141
Log saving before Yamaha wireless access points stop . . . 142
Related Commands . . . 143
Setting Examples . . . 143
Points of Caution . . . 143
Related Documentation . . . 143
Terminal Monitoring . . . 145
Function Overview . . . 145

Definition of Terms Used 146
Function Details 146
Monitoring by ping (ICMP Echo request/reply) 146
Monitoring according to frame reception volume 146
Monitoring with LLDP 147
Related Commands 147
Settings via the Web GUI 147
Terminal monitoring top page 147
Adding or modifying a monitored terminal 148
Checking the state of a monitored terminal 150
Points of Caution 150
Related Documentation 150
Performance Observations 151
Function Overview 151
Definition of Terms Used 152
Function Details 152
Resource and traffic usage observation 152
Observation data backup 152
Observation data export 153
Related Commands 154
Settings via the Web GUI 154
Viewing the resource usage amount 155
Viewing the traffic usage amount 155
Viewing power consumption data 157
Backing up, clearing, or exporting observation data 157
Points of Caution 160
Related Documentation 160
Schedule Function 161
Function Overview 161
Definition of Terms Used 161
Function Details 161
Time Trigger 161
Event Trigger 163
Action 163
Related Commands 164
Setting Examples 164
Supplying PoE power to wireless LAN access points only during specified hours 164
Obtaining internal information when microSD memory is inserted 164
Unavailable Commands 165
SYSLOG 166
Points of Caution 166
Related Documentation 167
Dante Optimization Setting Function 168
Function Overview 168
Definition of Terms Used 168
Function Details 168
Automatic optimization settings using LLDP 171
Manual optimization settings via the Web GUI 172

Related Commands 172

Examples of Command Execution. 173

Automatic optimization settings using LLDP 173

Points of Caution 173

Related Documentation. 174

ProAV Settings 175

Function Overview 175

Definition of Terms Used 175

Details on ProAV Profiles 175

Dante profiles 175

NDI profiles 179

Settings for using multiple profiles 181

Kitting and Troubleshooting 184

[Kitting] Initial setup without having to think about IP addresses 184

[Kitting] Applying the same settings to multiple Yamaha switches at once 187

[Troubleshooting] Checking the network status. 190

[Troubleshooting] Checking the Dante device status 192

Points of Caution 193

Related Documentation. 193

Trademarks and Trade Names. 193

Linking Security to the ADECIA System. 194

Function Overview 194

Definition of Terms Used 194

Function Details 195

Automatic recognition of ADECIA components 195

Remote network switch control 195

Status notification from network switches 196

Related Commands 197

Security Linking Default Settings 197

Points of Caution 197

Related Documentation. 197

Stack Function 198

Function Overview 198

Definition of Terms Used 198

Function Details 199

Stack configuration 199

Connection between member switches 200

Main switch selection and MAC address assignment. 200

Operations on virtual switches 201

Network switch status when stacking. 201

Detection and measures for abnormal conditions. 202

Related Commands 204

Stack Initial Settings 204

Preparation of necessary equipment. 204

Member switch settings 204

Connecting member switches 207

Exchanging Member Switches 208

Exchange procedure using an SD card 208

Exchange procedure without using an SD card . . . 209
Firmware Update . . . 210
Firmware parallel update. . . . 211
Firmware sequential update . . . 211
Points of Caution . . . 212
Related Documentation. . . . 214
Default Settings List . . . 215
Interface Control Functions . . . 219
Basic Interface Functions . . . 219
Function Overview . . . 219
Definition of Terms Used . . . 219
Function Details . . . 219
Interface types . . . 219
Interface control . . . 219
LAN/SFP port defaults . . . 221
Port mirroring . . . 221
Frame counter . . . 221
SFP module optical receive level monitoring . . . 223
Tx queue usage monitoring . . . 224
ifIndex Assignment . . . 224
Related Commands . . . 224
Examples of Command Execution. . . . 225
Basic LAN port settings. . . . 225
Set port mirroring . . . 226
Show LAN/SFP port information . . . 226
Points of Caution . . . 227
Related Documentation. . . . 227
Link aggregation . . . 228
Function Overview . . . 228
Definition of Terms Used . . . 228
Function Details . . . 229
Static/LACP link aggregation: common specifications. . . . 229
Static link aggregation. . . . 229
LACP link aggregation . . . 230
Related Commands . . . 231
Examples of Command Execution. . . . 232
Set the static logical interface . . . 232
Setting the LACP logical interface . . . 235
Points of Caution . . . 239
Related Documentation. . . . 239
Port Authentication Function . . . 240
Function Overview . . . 240
Definition of Terms Used . . . 240
Function Details . . . 241
IEEE 802.1X authentication. . . . 242
MAC authentication . . . 243
Web authentication . . . 244
Using multiple authentication functions . . . 248

Host mode 250
Dynamic VLAN 250
VLAN for unauthenticated or failed-authentication ports 251
EAP pass-through function 251
Attribute values sent to the RADIUS server 252
Related Commands 252
Examples of Command Execution 253
Set IEEE 802.1X authentication 253
Set MAC authentication. 255
Set Web authentication 256
Points of Caution 258
Related Documentation 258
Port Security Function 259
Function Overview 259
Definition of Terms Used 259
Function Details 259
Limiting the terminals that can access 259
Related Commands 260
Examples of Command Execution 260
Limiting the terminals that can access 260
Points of Caution 261
Related Documentation 261
PoE Control 262
Function Overview 262
Definition of Terms Used 262
Function Details 262
PoE power supply function enable/disable control 262
Power supply class and maximum number of ports that can be powered simultaneously 262
Guard band 263
PoE power priority 263
PoE power supply actions 263
Power supply setting by LLDP 264
Related Commands 264
Examples of Command Execution 264
PoE Port Power Supply Settings 264
Points of Caution 265
Related Documentation 265
Layer 2 Functions 266
Forwarding Database (FDB) 266
Function Overview 266
Definition of Terms Used 266
Function Details 266
FDB entry 266
Automatic MAC address acquisition 268
MAC address manual setting 268
Related Commands 269
Examples of Command Execution 269
Referring to the FDB 269

Delete dynamic entries . . . 269
Changing the dynamic entry ageing time . . . 270
Register static entries . . . 270
Delete static entries . . . 270
Points of Caution . . . 270
Related Documentation . . . 270
VLAN . . . 271
Function Overview . . . 271
Definition of Terms Used . . . 271
Function Details . . . 271
Defining a VLAN ID . . . 271
VLAN settings for the LAN/SFP ports . . . 271
VLAN access control . . . 272
Default VLAN . . . 273
Native VLAN . . . 273
Private VLAN . . . 273
Voice VLAN . . . 273
Related Commands . . . 274
List of related commands . . . 274
Examples of Command Execution . . . 275
Port-based VLAN settings . . . 275
Tagged VLAN settings . . . 276
Private VLAN settings . . . 278
Voice VLAN settings . . . 280
Points of Caution . . . 281
Related Documentation . . . 281
Multiple VLAN . . . 282
Function Overview . . . 282
Definition of Terms Used . . . 282
Function Details . . . 282
Operating specifications . . . 282
Examples of traffic between multiple VLAN groups . . . 283
Communication example when inter-VLAN routing is possible . . . 283
Related Commands . . . 284
Examples of Command Execution . . . 284
Multiple VLAN settings example 1 . . . 284
Multiple VLAN settings example 2 . . . 286
Points of Caution . . . 289
Related Documentation . . . 289
Spanning Tree . . . 290
Function Overview . . . 290
Definition of Terms Used . . . 290
Function Details . . . 290
Related Commands . . . 291
Examples of Command Execution . . . 292
MSTP setting example . . . 292
Points of Caution . . . 300
Related Documentation . . . 300

Unique Loop Detection 301
Function Overview 301
Definition of Terms Used 301
Function Details 301
Loop detection operating specifications. 301
Loop detection examples 303
Related Commands 304
Examples of Command Execution 304
Points of Caution 306
Related Documentation. 306
DHCP Snooping 307
Function Overview 307
Definition of Terms Used 307
Function Details 307
Enabling DHCP snooping 307
Binding database 308
DHCP snooping by port type. 308
Option 82. 309
DHCP packet rate limits 311
DHCP snooping statistical information. 311
SYSLOG output. 311
Related Commands 311
Examples of Command Execution. 312
Designating trusted interfaces 312
Enabling DHCP snooping 312
Points of Caution 312
Layer 3 Functions 313
IPv4/IPv6 Common Settings 313
Function Overview 313
Definition of Terms Used 313
Function Details 313
DNS client settings. 313
Equal cost multipath settings. 314
Related Commands 314
Examples of Command Execution. 315
DNS client settings. 315
Equal-cost multi-paths. 316
Points of Caution 316
Related Documentation. 316
Basic IPv4 Settings 317
Function Overview 317
Definition of Terms Used 317
Function Details 317
IPv4 address settings 317
Auto IP function 317
Route information settings 318
ARP table settings 319
MTU settings 319

Related Commands . . . 320
Examples of Command Execution . . . 320
IPv4 network environment settings (DHCP) . . . 320
Points of Caution . . . 321
Related Documentation . . . 321
Basic IPv6 Settings . . . 323
Function Overview . . . 323
Definition of Terms Used . . . 323
Function Details . . . 323
IPv6 address settings . . . 323
Route information settings . . . 324
Neighbor cache table settings . . . 325
MTU settings . . . 326
DHCPv6-PD client settings . . . 326
Related Commands . . . 326
Examples of Command Execution . . . 327
Setting up an IPv6 network environment (fixed settings) . . . 327
Setting up an IPv6 network environment (automatic settings using RA) . . . 328
IPv6 network environment setting (DHCPv6) . . . 329
IPv6 network environment settings (DHCPv6-PD) . . . 329
Points of Caution . . . 331
Related Documentation . . . 331
Static Routing . . . 332
Function Overview . . . 332
Definition of Terms Used . . . 332
Function Details . . . 332
VLAN interface route information . . . 332
Static route information . . . 332
Display of routing table . . . 333
Route information priority (management distance) . . . 334
Enabling the routing function . . . 334
Related Commands . . . 334
Points of Caution . . . 334
Related Documentation . . . 334
IP Multicast Functions . . . 335
IGMP Snooping . . . 335
Function Overview . . . 335
Definition of Terms Used . . . 336
Function Details . . . 337
Related Commands . . . 339
Examples of Command Execution . . . 339
IGMP snooping settings (with multicast router) . . . 339
IGMP snooping settings (without multicast router) . . . 341
IGMP snooping settings (If distributing data in both directions) . . . 343
IGMP snooping settings (for separating multiple multicast environments with VLANs) . . . 347
Points of Caution . . . 349
Related Documentation . . . 349
MLD Snooping . . . 350

- Function Overview . . . 350
- Definition of Terms Used . . . 350
- Function Details . . . 351
- Related Commands . . . 352
- Examples of Command Execution . . . 353
  - MLD snooping settings (with multicast router) . . . 353
  - MLD snooping settings (without multicast router) . . . 354
- Points of Caution . . . 357
- Related Documentation . . . 357

Traffic Control Functions . . . 358

- ACL . . . 358
  - Function Overview . . . 358
  - Definition of Terms Used . . . 358
  - Function Details . . . 358
    - Generate access list . . . 359
    - Applying to the interface . . . 359
    - Settings for the LAN/SFP port and logical interface . . . 359
    - VLAN interface settings . . . 360
  - Related Commands . . . 360
  - Examples of Command Execution . . . 361
    - IPv4 access list settings . . . 361
    - IPv6 access list settings . . . 367
    - MAC access list settings . . . 370
  - Points of Caution . . . 373
  - Related Documentation . . . 374
- QoS . . . 375
  - Function Overview . . . 375
  - Definition of Terms Used . . . 375
  - Function Details . . . 376
    - Enabling or disabling QoS control . . . 376
    - QoS processing flow . . . 376
    - Transmission queue assignments . . . 377
    - Transmission queue assignments (frames sent from the network switch unit) . . . 379
    - Traffic classification . . . 379
    - Pre-marking . . . 380
    - Metering/policing/remarking . . . 381
    - Storing in the transmission queue . . . 385
    - Scheduling . . . 385
    - Shaping . . . 386
    - Optimizing web conference application settings . . . 387
    - Separate table 1: Standard PHB (RFC recommended value) . . . 388
  - Related Commands . . . 389
  - Examples of Command Execution . . . 390
    - Priority control (SP) using DSCP values . . . 390
    - Priority control (SP+WRR) using an access list . . . 392
    - Priority control using port priority trust mode . . . 396
    - Bandwidth control using access list (twin rate / individual policer) . . . 397
    - Bandwidth control using access list (single rate / aggregate policer) . . . 399

Points of Caution 400
Related Documentation. 401
Trademarks and Trade Names. 401
Flow Control 402
Function Overview 402
Definition of Terms Used 402
Function Details 402
IEEE 802.3x flow control 402
Back pressure. 403
Related Commands 404
Examples of Command Execution. 404
Points of Caution 404
Related Documentation. 404
Storm Control 405
Function Overview 405
Definition of Terms Used 405
Function Details 405
Related Commands 406
Examples of Command Execution. 406
Points of Caution 406
Related Documentation. 406
Application layer function 407
RADIUS server 407
Function Overview 407
Definition of Terms Used 408
Function Details 409
Root certificate authority. 409
RADIUS client settings. 410
User registration. 410
Restricting the authentication method 411
Enabling the RADIUS server function. 411
Reflecting settings in operation 412
Issue client certificate 412
Revoking a client certificate 413
Sending a certificate by mail. 413
Checking settings and certificates. 414
Mail notification of expiration of client certificate 415
Importing and exporting user information 416
Backing up and restoring all RADIUS server related information 416
Restoring RADIUS server information backed up by a Yamaha wireless access point (WLX series) . 417
SYSLOG output information 417
Related Commands 418
Setting Examples 419
Using RADIUS server functions and port authentication function simultaneously 419
Using RADIUS server functions for authentication of users logging in to a Yamaha router 420
Using RADIUS server functions for MAC authentication of Yamaha wireless access points (WLX series) 421
Using RADIUS server functions to connect to a Yamaha wireless access point (WLX series) using a

certificate 423
Points of Caution 425
Related Documentation. . . . 427
Other Information 428
SNMP MIB Reference 428

Important Notice

Login Security

Function Overview

BASIC

This product includes the following user account management improvements as countermeasures for ensuring cyber security.
To eliminate the risk of malicious cyber-attacks and ensure the product is used safely, be sure to read this document carefully and specify an appropriate user password before use.
For more information, refer to User Account Management.

- **Mandatory administrator registration**
    - At least one administrator account must be registered for this product.
      Therefore, a default administrative user (username: admin and password: admin) has been specified for logging in to the product the first time.
    - When first logging into the switch, specify **admin** as the username and password.
    - After logging in using the default administrative user account, the user is prompted to change the password setting.
- **Stricter limits on guest user operations**
    - If the privileged password (administrative password) has not been changed from the default setting, the following operations that use the privileged password (administrative password) will be restricted.
        - Users without administrator rights cannot transition to the privileged EXEC mode.
        - Factory settings cannot be restored using CLI/ GUI operations.
        - Cannot accept connections as a TFTP server.
    - To perform the above operations, change the privileged password (administrative password).
- **Countermeasure for Brute-Force Attacks**
    - As a countermeasure against brute-force attacks, login restrictions are applied after a login fails.
    - If an incorrect password is entered three successive times when logging into the switch via the console, web GUI, or other means, login is disabled for **one minute** thereafter, even if the correct password is entered.
    - If the password is entered incorrectly, wait at least one minute before trying to login again.

Applicable Models and Revisions

User account management has been improved in the following models and revisions.

Models	Revisions
SWX3220-16MT SWX3220-16TMs	Rev.4.02.10 or later
SWX3200-52GT SWX3200-28GT	Rev.4.00.25 or later
SWX3100-18GT SWX3100-10G	Rev.4.01.29 or later

Models	Revisions
SWX2322P-16MT	Rev.2.06.10 or later
SWX2320-16MT	Rev.2.05.10 or later
SWX2310-52GT SWX2310-28GT SWX2310-18GT SWX2310-10G	Rev.2.04.11 or later
SWR2310-28GT SWR2310-18GT SWR2310-10G	Rev.2.04.12 or later
SWX2310P-28GT SWX2310P-18G SWX2310P-10G	Rev.2.02.24 or later
SWR2311P-10G	Rev.2.02.25 or later
SWP2-10SMF SWP2-10MMF	Rev.2.03.16 or later

Precautions When Updating Firmware

If the firmware is updated with stronger user account management functionality, be sure to register an administrator account according to the following procedure before using the switch.

1. Register the administrator account with the previous firmware running, which has not been updated with stronger user account management functionality.
    - If an administrator account already exists, then no account registration is necessary.
    - However, if a password was not specified for the administrator account, be sure to specify a password.
    - It is not a problem if the user name for the administrator account is the default “admin”.

    ```
    Yamaha>enable
    Yamaha#configure terminal
    Yamaha(config)#username (username) privilege on password (password)
    ```

2. Create a guest user
   If necessary, create a guest user.
    - If using the username command, create it with the privilege option disabled (off).

    ```
    Yamaha(config)#username (username) privilege off password (password)
    ```

3. Change the privileged password (administrative password)
    - To change the privileged password (administrative password) using a command, use the enable password command.

    ```
    Yamaha(config)#enable password (special privileged access password)
    ```

4. Update the firmware to the version with a countermeasure taken
    - Update the firmware to the version with a countermeasure taken in accordance with Firmware Update.

Related Documentation

- User account management
- Remote Access Control
- Firmware Update

Maintenance and Operation Functions

User Account Management

Function Overview

This product provides the functions shown below for managing user accounts.

- Functions for setting user information
- Functions for user authentication by user name and password

Definition of Terms Used

Default Administrative User

Users with administrator rights specified in default factory settings.
Username: admin and password: admin

Administrative User

Users with administrator rights.
Administrative users are users with the privilege option switched on using the username command.

Guest User

Users without administrator rights and that require entering the privileged password (administrative password) in order to access the privileged EXEC mode.
Guest users are users with the privilege option switched off using the username command.

Privileged Password (Administrative Password)

The password used to assign administrator rights and specified using the enable password command.

Unnamed User

Users with a blank username setting.
Rev. 2.02.23 or earlier firmware versions permitted using unnamed user accounts under factory default settings, but unnamed user accounts were eliminated for newer firmware versions with stronger user account management functionality.

Function Details

User account function settings

User information settings

Use the **username** command to specify the following user information.

- User name
- Password
- Assignment of administrator rights

With factory default settings, the administrative username and password are both “admin”.

Setting the privileged password (administrative password)

The privileged password (administrative password) is set using the **enable password** command.
Privileged passwords (administrative passwords) are used for the following applications.

- To initialize devices
- To transition users without administrator rights to the privileged EXEC mode by using the console
- To use a TFTP client to send a config file or firmware to the switch

The factory default privileged password (default administrative password) setting is **admin**, but the operations described above cannot be performed if the privileged password (default administrative password) is set to the default setting.
To perform any of those operations, change the privileged password (administrative password) in advance.

Administrator rights

User login operations can be restricted depending on whether or not the user has administrator rights.

- Users with administrator rights can change device settings or update firmware.
- Users without administrator rights can only view device information without changing any settings.

Specifically, the following differences apply depending on whether or not the user has administrator rights.

	Console		Web GUI	
	Administrative user (with rights)	Guest user (without rights)	Administrative user (with rights)	Guest user (without rights)
Show device information	Yes	Yes	Yes	Yes
View settings	Yes	No	Yes	Limited (*1)
Change settings	Yes	No	Yes	No
Restart or initialize devices	Yes	No	Yes	No
Update firmware	Yes	No	Yes	No

*1: Cannot view passwords or other security-related settings.

Once the **enable** command is executed and the privileged password (administrative password) is entered, the privileged EXEC mode can be accessed to perform operations equivalent to an administrative user, even if logged in as a guest user.
For information about the rights required to execute each command, refer to the command reference.

Encrypt password

Specified passwords can be encrypted using the **password-encryption** command.

To encrypt a password, specify the **password-encryption enable** setting.
Once a password has been encrypted, it cannot be restored to an unencrypted character string state, even by specifying the **password-encryption disable** setting.
Encryption applies to the passwords specified by the following commands.

- **enable password** command
- **username** command

User authentication

When logging in to the console

When the following login prompt appears after connecting to the console, log in by entering the specified username and password.

```
Username:
Password:
```

For factory default settings, log in by entering “admin” as the default administrative username (and “admin” as the password).
After using “admin” to log in, the password must be changed to specify a new password.

```
Username: admin
Password: ①

SWX2310P-28GT Rev.2.02.06 (Tue Mar 13 08:41:39 2018)
  Copyright (c) 2015-2016 Yamaha Corporation. All Rights Reserved.

Please change the default password for admin.
New Password: ②
New Password(Confirm): ③
Saving ...
Succeeded to write configuration
```

① Enter “admin”

② Enter the new password.

③ Enter the same password again.

If an incorrect password is entered three successive times, login by that same user is restricted for one minute.

```
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.
```

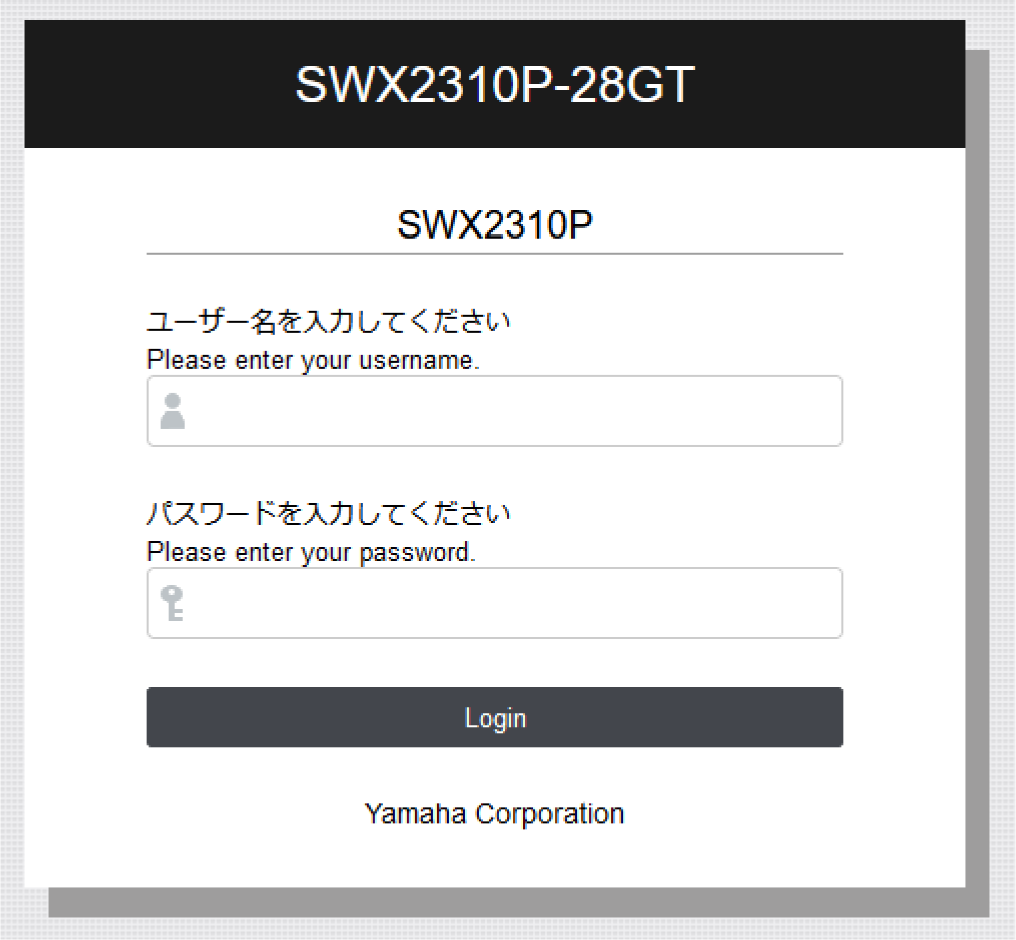
If a login restriction occurs, the following message is output in the INFO level SYSLOG.

Connection method	Output message
Serial console	Login access from serial console as {username} was restricted
TELNET	Login access from TELNET as {username} was restricted: {IP address}
SSH	Login access from SSH as {user name} was restricted: {IP address}
Web GUI	Login access from HTTP as {username} was restricted: {IP address}

Note that if a user with a login restriction enters an incorrect password again, the remaining time until the restriction is cancelled is reset to one minute again.

When logging in to the web GUI

When the following login form appears after accessing the web GUI, log in by entering the specified username and password.



SWX2310P-28GT

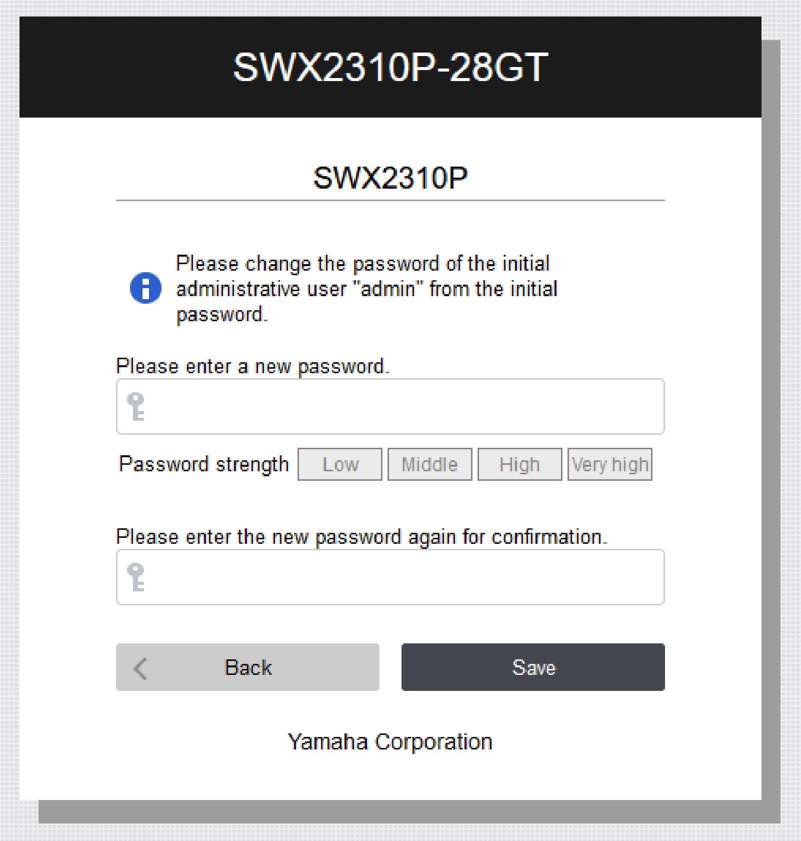
SWX2310P

ユーザー名を入力してください
Please enter your username.

パスワードを入力してください
Please enter your password.

Yamaha Corporation

For factory default settings, log in by entering “admin” as the default administrative username (and “admin” as the password).
If prompted to change the password after using “admin” to log in, specify a new password.



SWX2310P-28GT

SWX2310P

Please change the password of the initial administrative user "admin" from the initial password.

Please enter a new password.

Please enter the new password again for confirmation.

Yamaha Corporation

What to do if you forget your login password

If the product is rebooted connected to the **serial console** and **"I" (uppercase letter I)** is entered during the booting process, the product can be rebooted with factory default settings.
Note that the function is disabled if SD card booting is used.

```
BootROM - X.XX
Booting from SPI flash

SWX2310P-28GT BootROM Ver.1.00      #### Enter “I” as soon as the boot ROM version is
displayed. ####

Initialize or not ?(y/n) y

Loading config0 because can't read config in SD card.
Starting .............................................
Loading configuration ... Done!

SWX2310P-28GT Rev.2.02.06 (Tue Mar 13 08:41:39 2018)
  Copyright (c) 2015-2016 Yamaha Corporation. All Rights Reserved.
```

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Setting the privileged password (administrative password)	enable password

Operations	Operating commands
Encrypt password	password-encryption
Set user	username
Show user information	show users

Examples of Command Execution

Adding a user

The following example assigns **administrator rights** to the user “**yamaha**” and specifies the password “**yamaha_pass**”.

```
Yamaha#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Yamaha(config)#username yamaha privilege on password yamaha_pass
Yamaha(config)#exit
Yamaha#exit

Username: yamaha
Password:

SWX2310P-28GT Rev.2.02.06 (Tue Mar 13 08:41:39 2018)
  Copyright (c) 2015-2016 Yamaha Corporation. All Rights Reserved.

Yamaha>enable
Yamaha#
```

Points of Caution

- If no administrative user (user with administrator rights) exists in startup-config when the product is booted, then a default administrative user (with username “admin” and password “admin”) will be added automatically.
  For example, that would occur in the following case.
    - Product is booted with factory default settings configured
    - Firmware is updated to a newer version than Rev. 2.02.23 after the product was operated using Rev. 2.02.23 or older firmware and only unnamed users.
- If a user with no password is specified in startup-config when the product is booted, then a password with the same character string as the username will be added automatically.
  For example, that would occur in the following case.
    - Firmware is updated to a newer version than Rev. 2.02.23 after Rev. 2.02.23 or older firmware was used to specify users with no password.

      Settings configured with Rev. 2.02.23 or earlier firmware version

      ```
      username yamaha1
      username yamaha2 privilege on
      ```

      Settings after updating firmware to a newer version than Rev. 2.02.23

```
username yamaha1 password yamaha1
username yamaha2 privilege on password yamaha2
```

- If the password (admin) for the default administrative user admin is left unchanged, then the following restrictions are applied.
    - Network switches cannot be accessed by TELNET, SSH, HTTP, or HTTPS from a network segment other than the maintenance VLAN.
    - Login by users other than the default administrative user is not permitted.

      ```
      Username: yamaha
      Password:
      % Please login as user "admin".
      ```

    - The following commands cannot be executed. Similar setting changes cannot be performed via the web GUI either.
        - ip address / no ip address
          Note: Only “ip address dhcp” can be executed.
        - auto-ip / no auto-ip
        - ipv6 / no ipv6
        - ipv6 address / no ipv6 address
        - management interface / no management interface

Related Documentation

- Remote Access Control

LED Control

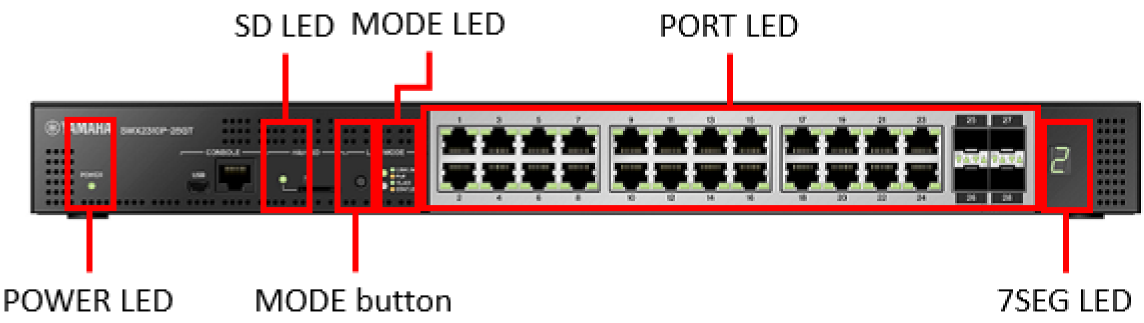
Function Overview

This product includes the following LEDs and button on the main unit.

- LED and button types

LED type	Description
POWER LED	Indicates the power supply status.
microSD LED	Indicates the microSD card connection and usage status.
Port LED	Indicate the LAN/SFP cable connection and usage status.
MODE button	Switches the LED mode.
Stack ID display LED (7SEG LED)	Displays the stack number. Only installed in the SWX2310P-28GT.

The layout of the LEDs and button is shown below.

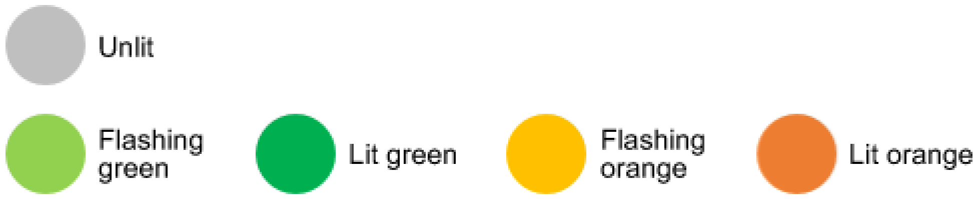


Definition of Terms Used

Legend of port LED illumination

Port LED illumination mentioned in subsequent explanations are illustrated below.

- Legend of port LED illumination



Function Details

POWER LED

The POWER LED lamp indicates the product power supply status.
The power supply status indicated by each POWER LED illumination mode is described below.

- Power supply status indicated by each POWER LED illumination mode

POWER LED illumination mode	Status
Unlit	Power is off.
Flashing green	Power is on and system is starting up.
Steady green	Power is on and system is operating normally.
Steady orange	Power is on and an error has occurred in the system.

When the following errors are detected, the POWER indicator illuminates steady orange.
Check the error that was detected and take the appropriate actions.

- Fan stopped

  The fan that exhausts heat generated by the product has stopped.
  Immediately stop using the product and be sure to contact the dealer for inspection or service.

- Temperature error inside the product

  The temperature inside the product is abnormal.
  Review the ambient conditions where installed and install the product correctly so that internal temperature is appropriate.

You can use the **show environment** command to check temperature and fan errors.

SD LED

The SD LED lamp indicates the microSD card connection and usage status.
The connection status indicated by each SD LED illumination mode is described below.

- Connection status indicated by each SD LED illumination mode

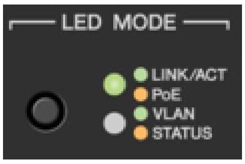
SD LED illumination mode	Status
Unlit	Not available, because a microSD card is not inserted or unmounted.
Flashing green	The microSD card is being accessed.
Steady green	A microSD card is inserted and available for use.

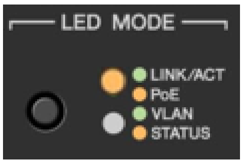
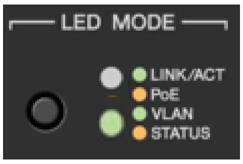
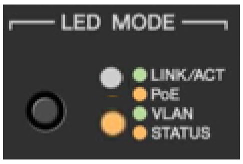
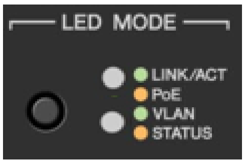
Do not remove the microSD card while flashing green, because the microSD card is being accessed.

Port LED

Indicator modes and switching between them

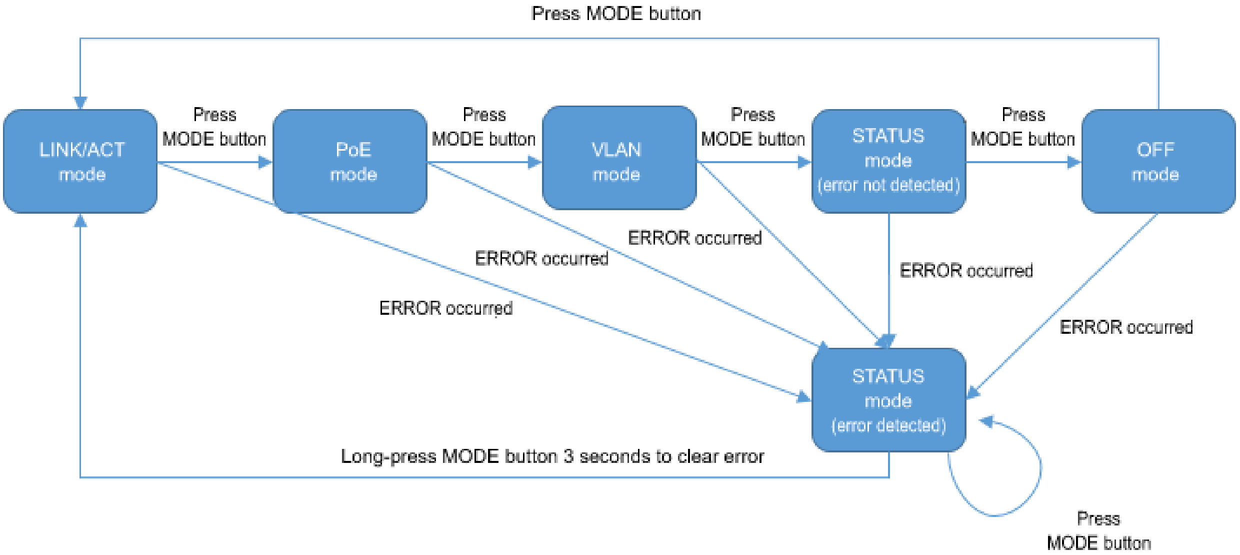
This product offers the following five display modes.

Mode name	MODE LED illumination status	Function Overview
LINK/ACT mode		The left LED of LAN/SFP ports indicates the link status and the right LED indicates the connection speed.

Mode name	MODE LED illumination status	Function Overview
PoE mode		Indicates the power supply status of the PoE power supply port.
VLAN mode		Indicates the VLAN IDs set for the LAN/SFP ports.
STATUS mode		Displays the error status of the LAN/SFP ports.
OFF mode		Switches off LAN/SFP port LEDs to minimize power consumption.

The display mode can be switched using the MODE button.
The flowchart below shows how to switch the indicator mode.

- Switching the indicator mode (when the default LED mode is the LINK/ACT mode)



The **display mode after system startup** and the **display mode after error is resolved** depend on the default LED mode setting.

If an error is detected by the following functions, the port LEDs automatically switch to the STATUS mode.

- Loop detection
- SFP optical reception level monitoring
- PoE supply

Even if you press the MODE button when an error is detected, the product will remain in the STATUS mode. (No further action will be accepted until all errors have been resolved.)
When you press and hold the MODE button for three seconds in this status, all error conditions are reset and the LEDs switch to the indications according to the default LED mode settings.
(For details, refer to **LED indications in STATUS mode**.)

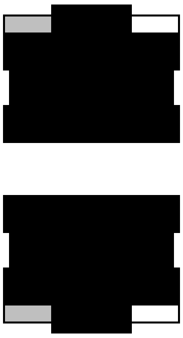
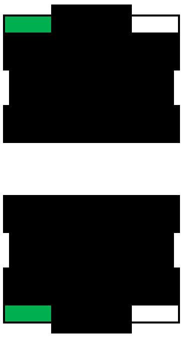
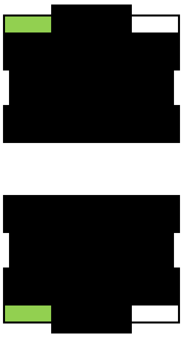
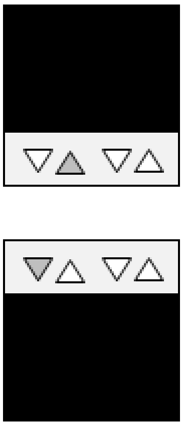
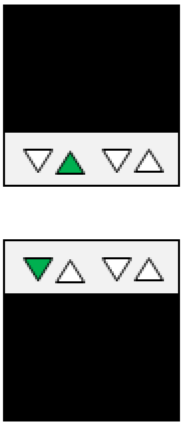
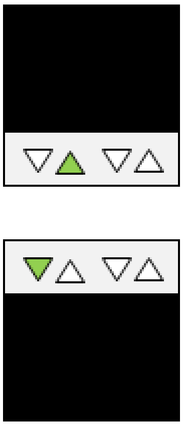
LED indications in LINK/ACT mode

In the LINK/ACT mode, port LEDs are illuminated as shown below.

- LAN/SFP port link status
- LAN/SFP port connection speed

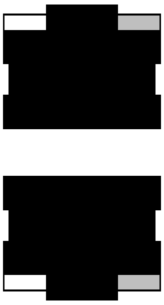
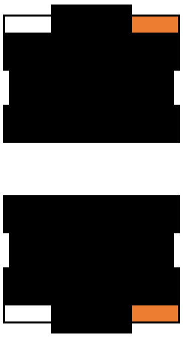
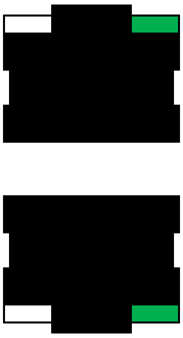
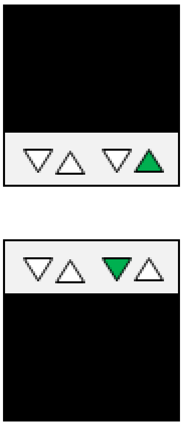
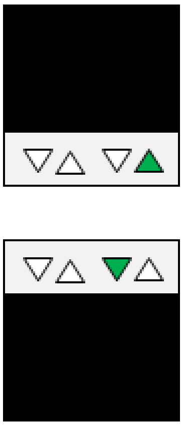
The link status LED indications are shown below.

- LAN/SFP port link status LED indications

	While link is down	While link is up	While forwarding data
LAN port	 (Off)	 (Steady green)	 (Flashing green)
SFP port	 (Off)	 (Steady green)	 (Flashing green)

The connection speed LED indications are shown below.

- Connection speed LED indications for LAN/SFP ports

	10M Link	100M Link	1000M Link	10000M Link
LAN port	 (Off)	 (Steady orange)	 (Steady green)	(None)
SFP port	(None)	(None)	 (Steady green)	 (Steady green)

LED indications in PoE mode

In the PoE mode, the power supply status is indicated on the port LED of the port capable of PoE supply (hereinafter referred to as PoE port).

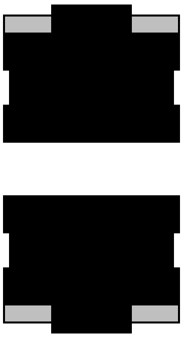
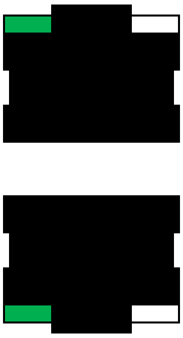
In the stack configuration, the display mode cannot be changed to the PoE mode.
The power supply ports for each model are as follows.

- Power supply port by model

Model name	Power supply port
SWX2310P-10G	Ports #1 to #8
SWX2310P-18G	Ports #1 to #16
SWX2310P-28GT	Ports #1 to #24

The LED indications in the PoE mode are shown below.

- Power supply port LED indications

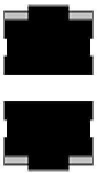
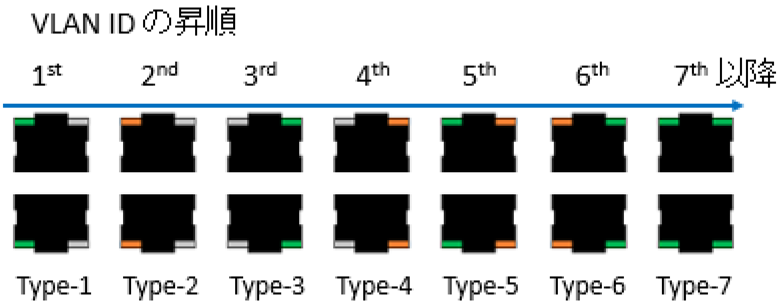
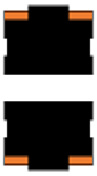
	No power supply	Power is being supplied
LAN port	 (Off)	 (Steady green)

LED indications in VLAN mode

In the VLAN mode, the port LEDs indicate the VLAN association status.

In the stack configuration, the display mode cannot be changed to the VLAN mode.
The port LED illumination statuses are shown below.

- Port LED illumination statuses in VLAN mode

LAN/SFP port VLAN association status	Port LED illumination status
The port is not associated with any VLAN	 (Off)
The port is associated with one VLAN	 VLAN ID の昇順 1st 2nd 3rd 4th 5th 6th 7th 以降 Type-1 Type-2 Type-3 Type-4 Type-5 Type-6 Type-7 The six lowest VLAN IDs are indicated in specific illumination patterns. All VLAN IDs from the 7th lowest one are indicated in an identical illumination pattern.
The port is associated with multiple VLANs	 (The port LEDs on the left and right are lit in steady orange)

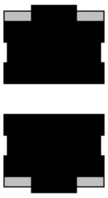
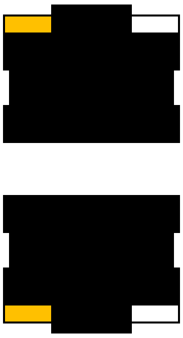
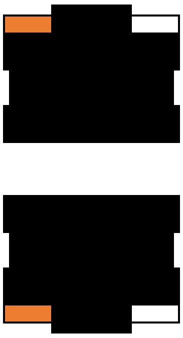
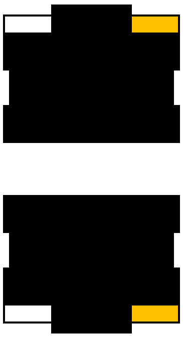
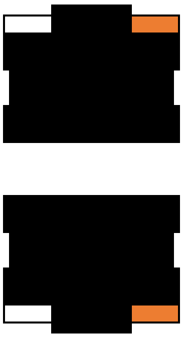
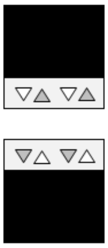
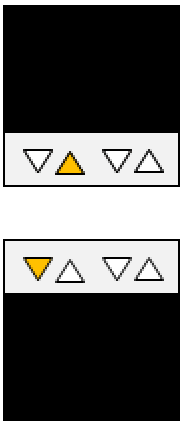
- The default VLAN (VLAN #1) is excluded from the subject of indication. It is not counted as an associated VLAN.

- The VLAN association status does not depend on the link status of each LAN/SFP port. Ports in the link-down status are also included in the subject of indication.
- VLAN IDs in the subject of indication are only those with associated LAN/SFP ports.
  Those for which only the VLAN IDs are defined (without associated LAN/SFP ports) are excluded from the subject of indication.

LED indications in STATUS mode

In STATUS mode, the port LEDs indicate the status of errors generated by the following product functions.

- Loop detection
- SFP optical reception level monitoring
- PoE supply
- Port LED indications in error status

	Normal state	Loop detection or SFP optical Rx level abnormality	PD error	PoE system limit	PoE port limit
LAN port	 (Off)	 (Left LED flashing orange)	 (Left LED steady orange)	 (Right LED flashing orange)	 (Right LED steady orange)
SFP port	 (Off)	 (Left LED flashing orange)	(None)	(None)	(None)

When the product detects an error, it overrides the current mode and switches to STATUS mode.
The following conditions trigger an error in respective functions.

- Loop detection
  - Loop was detected, so port was blocked
  - Loop was detected, so port was shut down

- SFP optical reception level monitoring
    - SFP optical reception level fell below the normal range
    - SFP optical reception level exceeded the normal range
- PoE supply
    - Power supply stopped because the port limit (maximum power supply per port) exceeded
    - Power supply to low priority ports stopped because the system limit (maximum power supply of the entire system) exceeded
    - A PD error was detected

The cause of the error can be checked using the **show error port-led** command.

During active errors in the STATUS mode, LEDs will automatically switch to the **default LED mode** in the following states.

- All of the following errors were resolved.
    - Blocked status due to loop detection is resolved.
    - Shutdown status due to loop detection is resolved.
        - The monitoring time elapsed after the shutdown due to loop detection.
        - The unit linked up after the **no shutdown** command was executed during shutdown due to loop detection.
    - SFP optical reception level recovered.
    - The PoE port error was resolved.
- Press and hold the MODE button (for three seconds) to forcibly reset (clear) the error status.

LED indication for OFF mode

If the default LED mode is the OFF mode, the port LEDs remain off regardless of the link status.
Even if the default LED mode is OFF, if an error occurs then the mode automatically switches to the STATUS mode and displays the error status.

Changing the LED mode after system startup

This product enables the LED mode after system startup (the default LED mode) to be changed.
The initial default LED mode is set to **LINK/ACT** mode, but it can be changed using the **led-mode default** command.
However, the LED mode cannot be changed in the stack configuration.

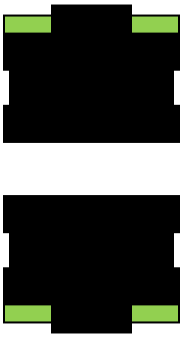
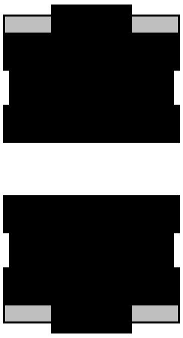
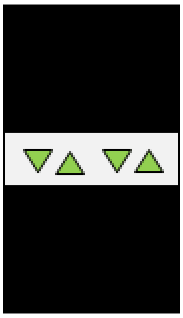
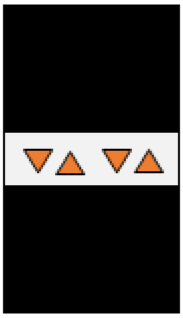
You can check the default LED mode and the currently displayed LED mode using the **show led-mode** command.

If an active error is resolved in the **STATUS** mode, the mode is switched back to the default LED mode.

Other port LED indications

Regardless of the LED mode status, all port LEDs will illuminate as indicated below during startup initialization and firmware updates.

- Other port LED indications

	Updating firmware	Initializing
LAN port	 (Flashing green)	 (Off)
SFP port	 (Flashing green)	 (Steady orange)

Stack ID display LED

The stack ID display LED (7SEG LED) installed on the SWX2310P-28GT displays the stack ID in the stack configuration after the startup countdown is displayed.
If a stack is not configured, the number ‘1’ is displayed.
If an error occurs while a stack is configured, the letter ’E’ is displayed to indicate the error.

If the default LED mode is the OFF mode, the stack ID display LED is also switched off.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Show LAN/SFP port status	show interface
Show loop detection setting status	show loop-detect
Show VLAN information	show vlan brief
Set default LED mode	led-mode default
Show LED mode	show led-mode
Show port error status	show error port-led

Examples of Command Execution

Checking LAN/SFP port status

Use the **show interface** command to check the LAN/SFP port status.

```
Yamaha#show interface
show interface
Interface port1.1
  Link is UP
  Hardware is Ethernet
  HW addr: ac44.f23d.0b2c
  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          : 317111
           bytes            : 31387581
           multicast packets: 317074
    output packets          : 162694
           bytes            : 220469213
           multicast packets: 162310
           broadcast packets: 149
           drop packets     : 0
   :
(Shows information for all LAN ports)
```

Checking LAN/SFP port loop detection status

Check the LAN/SFP port loop detection status.

```
Yamaha#show loop-detect
loop-detect: Enable

loop-detect: Enable

port      loop-detect    port-blocking           status
-------------------------------------------------------
port1.1        enable           enable           Normal
port1.2        enable           enable           Normal
port1.3        enable           enable           Normal
port1.4        enable           enable           Normal
port1.5        enable           enable           Normal
port1.6        enable           enable           Normal
port1.7        enable           enable           Normal
port1.8        enable           enable           Normal
port1.9        enable           enable           Normal
port1.10       enable           enable           Normal
-------------------------------------------------------
(*): Indicates that the feature is enabled.
```

Set default LED mode

Set the default LED mode to the OFF mode.

```
Yamaha#configure terminal
Yamaha(config)#led-mode default off ①
Yamaha(config)#exit
Yamaha#show led-mode ②
default mode : off
current mode : off
```

① Set default LED mode

② Show LED mode

Use of External Memory

Function Overview

This product provides the following functions using external memory.

- SD card boot (firmware, config)
    - The system can be started using a firmware file and config file from an SD card.
- Applying SD card booting automatically (firmware, config)
    - The firmware and config file used for SD card booting can be applied the next time the product is booted, even if the SD card is unavailable.
- Firmware Update
    - This unit's firmware can be updated by loading a firmware file from an SD card.
- Saving and copying a config file
    - The running-config that is currently running on the system can be saved to an SD card, and config files can be copied from the SD card to the unit's flash ROM or from the unit's flash ROM to the SD card.
- Saving a log file
    - By executing the **save logging** command you can back up the log file to an SD card.
- Saving technical support information
    - Technical support information (the result of executing the **show tech-support** command) can be saved to an SD card.
- Saving statistical information
    - Observations of resource information and traffic information are backed up regularly.
    - This statistical information can be saved as a CSV format file.
- Backing up and restoring system information
    - System information (including configurations) can be backed up to an SD card.
    - Backed up system information can be restored into the unit's flash ROM.

Definition of Terms Used

None

Function Details

External memory that can be used

Requirements for external memory that can be used are as follows.

- Card type: microSD card / microSDHC card
- File format: FAT16/FAT32

Folder structure

The SD card must contain the following folder structure.

```
Device name   +-- firmware          Firmware file storage folder
              |
              |
              +-- startup-config    Startup config storage folder
              |
              |
              +-- log               SYSLOG storage folder
              |
              |
              +-- techsupport       Technical support information storage folder
              |
              |
              +-- data              System-wide folder
              |
              |
              +-- backup-system     System backup folder
```

Mounting and unmounting the SD card

If the SD card is inserted when starting up or after startup, it is automatically mounted and becomes available.

To prevent loss of files, execute the **unmount sd** command or execute the unmount operation from the Web GUI before removing the SD card.
If the SD card is unmounted, it cannot be used.
If you want to once again use the SD card after executing the **unmount sd** command, you must execute the following.

- Remove and reinsert the SD card
- Execute the **mount sd** command
- Execute mount from the Web GUI

SD card boot (firmware, config)

The system can be started using a firmware file and config file from an SD card.
In order to use SD card boot, the following conditions must be satisfied.

- SD card using a firmware file
  - The SD card is connected when the system starts up.
  - The following files exist in the SD card.
    - /swx2310p/firmware/swx2310p.bin
  - **boot prioritize sd enable** is set.
- **boot prioritize sd enable** is set in the factory default setting.
- SD card boot using a config file
  - The SD card is connected when the system starts up.
  - The following files exist in the SD card.
    - /swx2310p/startup-config/config.txt
  - **startup-config select sd** is set.
- **startup-config select sd** is set in the factory default setting.

The file used for SD card booting can also be automatically saved to internal flash ROM memory using the automatic SD card booting function (see Automatic SD card booting).

You can use the **show environment** command to check whether SD card boot was successful.

- In the case of SD card boot using a firmware file, “Startup Firmware” will indicate “exec(SD).”
- In the case of SD card boot using a config file, “Startup Configuration” will indicate “config(SD).”

In the case of SD card boot using a config file, executing the **write** and **copy running-config startup-config** commands will update the config file on the SD card.
If SD card boot using a config file fails, startup config #0 is loaded.
Also, the following message is shown in the console and in SYSLOG.

```
Loading config0 because can't read config in SD card.
```

Applying SD card booting automatically (firmware, config)

The firmware and config used for SD card booting can be automatically saved to internal flash ROM memory. This function can be used to easily install previously prepared firmware and config files in newly purchased devices (with factory settings).

Preparations before using automatic saving

In order to use this function, the following conditions must be satisfied.

- SD card booting is enabled by either of the following methods. (For details, see SD card booting.)
  - The **boot prioritize sd enable** command is specified and firmware is installed with an appropriate path for SD cards.
  - **startup-config select sd** is specified and the config file is installed with an appropriate path.
- The automatic SD card booting function is enabled.
  - The automatic SD card booting function can be enabled using the **boot auto-apply enable** command.
    (This function is enabled in the factory default settings)
  - The **show environment** command “boot auto-apply” display results can be used to confirm whether the function is enabled or disabled.
- Prepare a file for automatically applying the automatic SD card booting function.
  - If firmware is applied automatically
    - Prepare an **auto-apply.txt** file (empty text file) in the firmware folder in the SD card.

      ```
      /swx2310p/firmware/auto-apply.txt
      ```
  - If a config file is applied automatically
    - Prepare an **auto-apply.txt** file (empty text file) in the startup-config folder in the SD card.

      ```
      /swx2310p/startup-config/auto-apply.txt
      ```

Procedure for automatic SD card booting

Use the following procedure to automatically apply SD card booting.

1. Implement preparations. (See Preparations before using automatic saving)
2. Insert the SD card and boot the network switch.
3. When SD card booting is finished, automatically save the specified file in internal flash memory. (Booting by automatic SD card booting takes longer than normal.)

4. Save the results from automatic SD card booting. (See Automatic SD card booting results.)
5. Automatically unmount the SD card.
6. Automatically switch off the microSD LED.

Automatic SD card booting results

Automatic SD card booting results are saved in the SD card.

File name and directory path	Log
/swx2310p/startup-config/auto-apply-result.txt	Serial: Date and time: Result
/swx2310p/firmware/auto-apply-result.txt	Serial: Date and time: Result

Location for saving config file

To change the config location to a user-specified config ID, rename the **auto-apply.txt** file created, as indicated below.
If no config location is specified, the default config ID of 0 is applied.

File name and directory path	Config ID
/swx2310p/startup-config/auto-apply.txt	0
/swx2310p/startup-config/auto-apply0.txt	0
/swx2310p/startup-config/auto-apply1.txt	1
/swx2310p/startup-config/auto-apply2.txt	2
/swx2310p/startup-config/auto-apply3.txt	3
/swx2310p/startup-config/auto-apply4.txt	4

Points of Caution

Note the following precautions when using this function.

- When the automatic SD card booting is successful, the function is automatically disabled.
  To avoid it being disabled automatically, the character string “keep” must be included at the top of the **auto-apply.txt** file created, as shown below.

  ```
  keep
  ```

- This function is disabled if the stack function is enabled.
- If the SD card does not contain an **auto-apply.txt** file, the function is disabled.
- If the device was not booted from the SD card, the automatic SD card booting function will fail even if an **auto-apply.txt** file exists.
  Refer to SD card booting to confirm that the file in the SD card and the SD card booting function are enabled.
- If automatic SD card booting fails, only the SD card will be unmounted without automatically disabling the function.
- To prevent malfunction, be sure to delete the **auto-apply.txt** file if the automatic SD card booting function is not used.

Firmware Update

This unit’s firmware can be updated by loading a firmware file from an SD card.

In order to use this function, the following conditions apply.

- The following files exist in the SD card.
  - /swx2310p/firmware/swx2310p.bin

If the above file exists on the inserted SD card, executing the **firmware-update sd execute** command updates the firmware in flash ROM using the firmware in the SD card.

When the **firmware-update sd execute** command is executed, the user will be asked whether to maintain the mounted state of the SD card when the firmware file has finished loading. Remove the SD card as necessary after it is unmounted.
Note that if the SD card is left inserted during the automatic reboot in conjunction with firmware update, the system will start up with the firmware file on the SD card.

The firmware in member switches of a stack configuration can also be updated by executing the **firmware-update sd execute** command from the main switch.

Saving and copying a config file

The running-config that is currently running on the system can be saved to an SD card. (The **copy running-config startup-config** command and the **write** command)

You can copy the config file from the SD card to internal flash ROM, or from internal flash ROM to the SD card. (The **copy startup-config** command)

The contents of startup-config in the SD card can be erased or viewed. (The **erase startup-config** command and the **show startup-config** command)

The following folder in the SD card is affected.

- /swx2310p/startup-config

Saving a log file

By executing the **save logging** command you can back up the log file to an SD card.

The **logging backup sd** command enables SYSLOG backup to the SD card.
If SYSLOG backup to the SD card is enabled, executing the **save logging** command will save the following log file with its save date to the SD card.

- /swx2310p/log/YYYYMMDD_log.txt
  *YYYYMMDD=year month day

The log files in the SD card cannot be viewed or erased.

Saving technical support information

Technical support information (the result of executing the **show tech-support** command) can be saved to an SD card.
Executing the **copy tech-support sd** command will save the following technical support information file with its save date to the SD card.

- /swx2310p/techsupport/YYYYMMDDHHMMSS_techsupport.txt *YYYYMMDD=year month day, HHMMSS=hours minutes seconds

The technical support information files in the SD card cannot be viewed or erased.

If the **copy tech-support sd** command is executed from the main switch in a stack configuration, a file containing technical support information for member switches is saved.

Saving statistical information

Observations of resource information and traffic information are backed up regularly.
To enable backup of statistical information to the SD card, you must make settings via the Web GUI in [Administration]–[Maintenance]–[Summary data management].

This statistical information for the observed data can be saved via the Web GUI as a CSV format file.

Backing up and restoring system information

This unit's system information can be backed up to an SD card, and the backed up system information can be restored to a desired network switch.
With an SD card connected to this unit, executing the **backup system** command will create a system information backup in the following folder.

- /swx2310p/backup-system

If the file swx2310p.bin exists in the /swx2310p/firmware/ folder when backup is executed, it is backed up as a firmware file.

To restore the backed up system information, connect the SD card containing the system information backup to the desired network switch, and execute the **restore system** command.
If the firmware file was backed up, a firmware update is also performed using that file.
When restore is completed, the system will restart.

The system information backup contains the following.

- Settings associated with the unit
  - startup-config #0 - #4 and associated information
  - Setting values for the startup-config select command
  - Setting values for the boot prioritize sd command
- Firmware file
- Only if the specified folder of the SD card contained a firmware file when the backup was executed.

For this reason, when replacing a unit due to malfunction or another reason, the replacement unit can be returned to the same condition as the original unit simply by restoring the backed up system information.
Do not edit or delete the backed up system information.

List of related commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Mount SD card	mount sd
Unmount SD card	unmount sd
Set SD card backup of log	logging backup sd

Operations	Operating commands
Back up log	save logging
Saving technical support information	copy tech-support sd
Save running config	copy running-config startup-config
Save running config	write
Copy startup config	copy startup-config
Erase startup config	erase startup-config
Show startup config	show startup-config
Back up system information	backup system
Restore system information	restore system

Examples of Command Execution

Unmount SD card

Unmount the SD card.

```
Yamaha>unmount sd
```

Mount SD card

Mount the SD card.

```
Yamaha>mount sd
```

Back up log file

By executing the **save logging** command you can back up the log file to the SD card as well.

```
Yamaha(config)#logging backup sd enable ①
Yamaha(config)#exit
Yamaha#save logging ②
```

① Enable SD card backup of logs

② Back up logs

Saving technical support information

Save technical support information.

```
Yamaha#copy tech-support sd
```

Points of Caution

None

Related Documentation

- Config Management
- SYSLOG
- Firmware Update
- Performance Observations

Boot Information Management

Function Overview

As system boot information, this product manages the information shown in the table below.

Management item	Description
System startup time	Time that the system booted up
Running firmware information	Firmware version currently running, and date generated
Firmware information for previous startup	Version and generated date of the firmware for the previous startup
Reason for boot	Reason why the system booted up. The following are recorded: * Startup due to power-on * Restart due to the reload command * Restart due to the cold start command * Restart due to the startup-config select command * Restart due to the boot prioritize sd command * Restart due to the restore system command * Restart due to the stack enable command * Restart due to firmware updates * Restart due to memory exhaustion * Restart due to kernel panic * Restart due to abnormal termination of process

This product stores the current boot information and information on the previous four boots, for a total of five boot records.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Show boot information	show boot
Clear boot information	clear boot list

Examples of Command Execution

Show boot information

- This shows the current boot information.

```
Yamaha>show boot 0
 Running EXEC: SWX2310P Rev.2.02.02 (Tue Dec  5 11:37:39 2017)
Previous EXEC: SWX2310P Rev.2.02.02 (Tue Dec  5 11:37:39 2017)
Restart by reload command
```

- This shows a list of the boot history.

```
Yamaha>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
--- ---------- -------- --------------------------------------------------
```

Clear boot information

- This clears the boot information.

```
Yamaha#clear boot list
```

Points of Caution

None.

Related Documentation

None.

Show Chassis Information

Function Overview

This product provides the following functionality that can be used to obtain product information, operating information, and so on.

- Use commands to show chassis information
- Obtain technical support information remotely
- Save technical support information on external memory

Technical support information includes a wide variety of data analysis information, including not only product information and operating information for this product, but also configuration information and process operating status information.
The functions can be used to show all information for a device at the same time.

Function Details

Use commands to show chassis information

This function shows chassis information by entering a command in the console.
The following chassis information can be shown.

Display item	Explanation	Commands
Inventory information	Shows information for this product, such as inventory name, model number, and product ID. If an SFP module has been inserted, the inventory information for the module will also be shown.	show inventory
Operating information	Shows the operating information for this product's programs, such as running software information, CPU usage, memory usage, boot time.	show environment
Process list	Shows the system summary information and a list of running processes.	show process
Memory usage status	Shows the memory usage status for each process.	show memory
Disk usage status	Shows the usage status of the disks used in the system.	show disk-usage
Technical support information	Shows all available operating information as data analysis information necessary for technical support. If the stack function is enabled, technical support information is shown for member switches in addition to information for the main switch.	show tech-support

Show inventory information

Product information for the main unit and SFP module can be shown using the **show inventory** command.
Product information includes the following information.

- Name (NAME)
- Description (DESCR)
- Vendor Name (Vendor)
- Product ID (PID)

- Version ID (VID)
- Serial number (SN)

Show operating information

System operating status can be shown using the **show environment** command. The system operating status includes the following information.

- Boot version
- Firmware revision
- Serial number
- MAC address
- CPU usage ratio
- Memory usage ratio
- Fan operating status
- Fan RPM
- Firmware file
- Startup config file
- Setting the automatic SD card booting function
- Serial baud rate
- Startup time
- Current time
- Elapsed time from boot
- Unit temperature status
- Unit temperature

Show technical support information

Technical support information can be shown using the **show tech-support** command. Technical support information includes results from executing the following commands.

When the stack function is enabled, technical support information for all devices in the stack configuration is shown.
However, the commands executed on the main switch and member switches are different. For details, refer to the command list.

- List of commands to be executed

Commands	Stacking disabled	Stacking enabled	
		Main switch	Member switch
show running-config	Yes	Yes	Yes
show startup-config	Yes	Yes	Yes
show stack	Yes (*1)	Yes (*1)	Yes (*1)
show environment	Yes	Yes	Yes
show system-diagnostics	Yes	Yes	Yes
show clock detail	Yes	Yes	-

show disk-usage	Yes	Yes	Yes
show inventory	Yes	Yes	Yes
show boot all	Yes	Yes	Yes
show boot prioritize sd	Yes	Yes	Yes
show logging	Yes	Yes	Yes
show process	Yes	Yes	Yes
show memory	Yes	Yes	Yes
show users	Yes	Yes	Yes
show interface	Yes	Yes	-
show frame-counter	Yes	Yes	-
show vlan brief	Yes	Yes	-
show spanning-tree mst detail	Yes	Yes	-
show etherchannel status detail	Yes	Yes	-
show loop-detect	Yes	Yes	-
show mac-address-table	Yes	Yes	-
show l2ms detail	Yes	Yes	-
show qos queue-counters	Yes	Yes	-
show ddm status	Yes	Yes	Yes
show errdisable	Yes	Yes	-
show auth status	Yes	Yes	-
show auth supplicant	Yes	Yes	-
show power-inline	Yes	Yes	-
show error port-led	Yes	Yes	-
show ip interface brief	Yes	Yes	-
show ip forwarding	Yes	Yes	-
show ipv6 interface brief	Yes	Yes	-
show ipv6 forwarding	Yes	Yes	-
show ip route	Yes	Yes	-
show ip route database	Yes	Yes	-
show ipv6 route	Yes	Yes	-
show ipv6 route database	Yes	Yes	-
show arp	Yes	Yes	-
show ipv6 neighbors	Yes	Yes	-
show ip igmp snooping groups	Yes	Yes	-

show ip igmp snooping interface	Yes	Yes	-
show ipv6 mld snooping groups	Yes	Yes	-
show ipv6 mld snooping interface	Yes	Yes	-
show ip dhcp snooping binding	Yes	Yes	-
show ip dhcp snooping statistics	Yes	Yes	-
show radius-server local certificate status	Yes	Yes	-
show radius-server local nas	Yes	Yes	-
show radius-server local user	Yes	Yes	-
show radius-server local certificate list	Yes	Yes	-
show radius-server local certificate revoke	Yes	Yes	-
show sflow	Yes	Yes	-
show sflow sampling	Yes	Yes	-

*1 This command is only included in stack-compatible models.

Obtain technical support information remotely

Technical support information (output results from show tech-support) can be obtained from the product by remote access via the Web GUI or TFTP.

Web GUI

In order to operate this product’s HTTP server, use the steps shown below to set up a network environment that allows remote access.

1. Decide on the VLAN that will be used for maintenance.
2. Set the IPv4 address on the maintenance VLAN. Set it using the ip address command.
3. Permit access from the maintenance VLAN to the HTTP server. To specify a different VLAN than for management interface command settings, use the http-server interface command.

Execute the following operations by accessing the Web GUI.

- Show technical support information on the Web GUI
    - In the “TECHINFO” menu, press the “Show in browser” button. The execution result of the “show tech-support” command is shown.
    - To close, press the web browser’s close button.
- Obtain technical support information from the Web GUI
    - In the “TECHINFO” menu, press the “Obtain as text file” button to start the download automatically.
    - The file is saved with a file name in the following format.
        - techinfo_YYYYMMDDhhmmss.txt (where “YYYYMMDDhhmmss” is the date/time the command was executed)

TFTP

In order to operate this product’s TFTP server, use the steps shown below to set up a network environment that allows remote access.

1. Decide on the VLAN that will be used for maintenance.
2. Set the IPv4 address on the maintenance VLAN. Set it using the ip address command.
3. Permit access from the maintenance VLAN to the TFTP server. To specify a different VLAN than for management interface command settings, use the tftp-server interface command.

If using a TFTP client, specify **techinfo** in the remote path for obtaining technical support information.

Save technical support information on external memory

You can use the **copy tech-support sd** command to save this product's *technical support information (the output result of "show tech-support") *on an SD card.
Before executing this command, you must insert an SD card.
The information is saved in the SD card with the following file name.

- /swx2310p/techsupport/YYYYMMDDHHMMSS_techsupport.txt (where "YYYYMMDDHHMMSS" is the date/time the command was executed)

Related Commands

Related commands are indicated below.
For command details, refer to the command reference.

Operations	Operating commands
Show inventory information	show inventory
Show operating information	show environment
Process list	show process
Memory usage status	show memory
Disk usage status	show disk-usage
Show technical support information	show tech-support
Save technical support information	copy tech-support sd

Examples of Command Execution

Show inventory information

The following shows product information for the main unit and SFP module.

```
Yamaha>show inventory
NAME: L2 POE switch
DESCR: SWX2310P-10G
Vendor: Yamaha
PID: SWX2310P-10G
VID: 0000
SN: S00000000

NAME: SFP1
DESCR: 1000BASE-LX
Vendor: YAMAHA
PID: YSFP-G-LX
VID: 0000
```

```
SN: 00000000000

NAME: SFP2
DESCR: 1000BASE-SX
Vendor: YAMAHA
PID: YSFP-G-SX
VID: 0000
SN: 00000000000
```

Show operating information

The following shows the system operating status.

```
Yamaha>show environment
SWX2310P-10G BootROM Ver.1.00
SWX2310P Rev.2.02.02 (Tue Dec  5 11:37:39 2017)
main=SWX2310P-10G ver=00 serial=S00000000 MAC-Address=00a0.de00.0000
CPU:   7%(5sec)   8%(1min)   8%(5min)    Memory:  18% used
Fan status: Normal
Fan speed: FAN1=4444RPM FAN2=4444RPM FAN3=4444RPM
Startup firmware: exec0
Startup Configuration file: config0
Auto-apply: Enable
Serial Baudrate: 9600
Boot time: 2018/01/01 11:13:44 +09:00
Current time: 2018/01/02 16:19:43 +09:00
Elapsed time from boot: 1days 05:06:04
Temperature status: Normal
Temperature: 28 degree C

Yamaha>
```

Show technical support information

The following shows technical support information.

```
Yamaha#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
#
```

Points of Caution

None

Related Documentation

None

System Self-Diagnostics

Function Overview

This product includes system self-diagnostic function.

The system self-diagnostic function detects the following types of errors.

- Startup process errors
- Hardware component errors
  - Interface (Ethernet port)
  - RTC
  - SFP
  - Fan
  - PoE controller
  - Thermal sensor
- Temperature anomaly

Definition of Terms Used

RTC（Real-Time Clock）

Device used to manage time

PoE Controller

Device used for PoE (power over Ethernet) control.

PSE（Power Sourcing Equipment）

A device that supplies power. On this page it is considered synonymous with PoE controller.

Packet Processor

Device used to process packets.

Function Details

Diagnostics

Three types of system self-diagnostic functionality, either boot-up diagnostics, on-demand diagnostics, or health monitoring diagnostics, are available depending on when diagnostics are performed.
The features of each type are indicated below.

- Boot-up diagnostics
  - Automatically executes whenever the system starts up.
  - Detects startup process errors and hardware component errors (RTC, etc.).
- On-demand diagnostics
  - Can be executed at user-specified times set using the **system-diagnostics on-demand execute** command.
  - Detects hardware component (interface) errors.
  - All ports are shut down during diagnostics and the system is restarted when finished.

- Health monitoring diagnostics
    - Running continuously in the background during system operation
    - Detects hardware component errors (fan errors, etc.) and temperature abnormalities.
    - Health monitoring diagnostics results are displayed via the GUI and LED indicators (only some test results are indicated via the LED indicators).

Each diagnosis runs multiple tests. The tests performed for each diagnosis are indicated below.
For a detailed list of tests performed, refer to Test Details.

Test Type	Boot-up diagnostics	On-demand diagnostics	Health monitoring diagnostics
Loading Test	Yes		
RTC Test	Yes		
Packet Processor Test	Yes		
PHY Test		Yes	
Thermal Test			Yes
Fan Test			Yes
Thermal Sensor Test			Yes
PoE Test			Yes
SFP Test			Yes

Diagnostic results displayed

Diagnostic results can be checked using the **show system-diagnostics** command.
Though the system is automatically restarted after on-demand diagnostics, diagnostic results can be confirmed after restarting.

Deleting on-demand diagnostics results

On-demand diagnostics results can be deleted using the **clear system-diagnostics on-demand** command.

Test Details

Details about each test item are indicated below.

Loading Test

This verifies the loading status of software modules.
A “Pass” result is output if all modules are successfully loaded, whereas a “Fail” result is output if even one module fails to load.

The **show system-diagnostics** command does not indicate information about modules that failed to load.

To identify which module failed to load, use the **show logging** command to search the following log.
Note: XXXX part shows the module name.

```
[   HAMON]:err: An unexpected error has occurred. (XXXX deamon)
```

RTC Test

This verifies access to the RTC register.
A time value is obtained from the RTC two times, resulting in “Pass” if the time value changed or “Fail” if the time values are identical.
A “Fail” result also occurs if the test fails to obtain a time value from the RTC (or load the register).

Packet Processor Test

This verifies accessing the packet processor register.
A “Pass” result occurs if the value written in the packet processor register matches the loaded value, whereas a “Fail” result occurs if the values do not match.
A “Fail” result also occurs if the test fails to access the register.

PHY Test

This verifies access to the PHY register.
A “Pass” result occurs if the value written in the PHY register matches the loaded value, whereas a “Fail” result occurs if the values do not match.
A “Fail” result also occurs if the test fails to access the register.

Thermal Test

This monitors the CPU, PHY, SFP module, thermal sensor (chassis), and PSE temperatures.
If the temperature exceeds a threshold value, a warning is indicated.

Fan Test

This monitors the fan speed.
It indicates a warning if the fan stops rotating or the rotation speed increases.

Thermal Sensor Test

This monitors the thermal sensors.
It indicates a warning if a thermal sensor abnormality has been detected.

PoE Test

This monitors the PoE power supply status.
It indicates a warning if an error occurs in the PoE power supply control.

SFP Test

This monitors the SFP module optical input level.
It generates a warning if the optical input level exceeds a certain range.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Display system self-diagnostic results	show system-diagnostics
Execute on-demand diagnostics	system-diagnostics on-demand execute

Operations	Operating commands
Discard on-demand diagnostics results	clear system-diagnostics on-demand

Examples of Command Execution

Display system self-diagnostic results

1. Check the system self-diagnostics results as follows.

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

- Bootup
  Loading Test: Pass

  RTC Test: Pass

  Packet Processor Test: Pass

- On-demand
Last on-demand diagnostics information:
 Date     : 2021/07/07 09:00:00 +09:00
 BootROM  : Ver.1.01
 Firmware : Rev.2.02.23

  PHY Test:
    Port   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16
    --------------------------------------------------------------------
           P   P   P   P   P   P   P   P   P   P   P   P   P   P   P   P

    Port  17  18
    ------------
           P   P

- Health monitoring
  Thermal Test:
    CPU: Normal, PHY: Normal, SFP: Normal, TS: Normal, PSE: Normal

  Fan Test: Normal

  Thermal Sensor Test: Normal

  PoE Test:
    Port   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16
    --------------------------------------------------------------------
           N   N   N   N   N   N   N   N   N   N   N   N   N   N   N   N

  SFP Test:
    Port  17  18
    ------------
           N   N
```

Performing on-demand diagnostics

1. Perform on-demand diagnostics as follows.

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

Discard on-demand diagnostics results

1. Delete the on-demand diagnostic results as follows.

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

Points of Caution

- All ports are automatically shut down and restarted whenever on-demand diagnostics are performed. Therefore, use particular caution before executing on-demand diagnostics while the system is being operated.
- On-demand diagnostics are only executed if the stack status is standalone or disabled. To perform on-demand diagnostics when a stack is configured, first disconnect the connections between member switches.
- If online diagnostics are performed remotely, such as via Telnet or the web console, simplified results cannot be displayed before restarting because all ports are shut down during diagnostics. Use the **show system-diagnostics** command to check diagnostic results after restarting.

Related Documentation

None

Cable Diagnostics

Function Overview

The cable diagnostic function can be used to easily check whether or not the LAN cable connected to the LAN port has a faulty connection/circuit.
It can be used to troubleshoot network problems or as an easy way to check cables when setting up networks.

Definition of Terms Used

TDR (Time Domain Reflector)

The TDR is used to measure the length of LAN cables or the location of damage based on the reflected signals from a pulse signal sent through the LAN cables.

Function Details

How to diagnose cables

The cable diagnostic function can easily diagnose LAN cables using the time domain reflection (TDR) method.
Cable diagnostics is started by executing the **cable-diagnostics tdr execute interface** command.
If the **show cable-diagnostics tdr** command is executed after the diagnostics process is finished, the following diagnostic results are displayed.

Item	Description
Cable status	The following cable states can be detected. * OK: The cable is electrically connected. * Open: Either no device is connected on the opposite end or the cable is faulty. * Short: A short circuit occurred. Results are displayed for each pair.
Distance to the cable failure point	If the cable status is “Open” or “Short”, then the distance to the fault is displayed. Results are displayed for each pair.

Results from executing cable diagnostics the previous time can be checked using the **show cable-diagnostics tdr** command.
Only the immediately previous diagnostic results are retained and then overwritten the next time the cable diagnostics command is executed again.
The immediately previous results can be deleted using the **clear cable-diagnostics tdr** command.

Related Commands

Related commands are indicated below.
For command details, refer to the command reference.

Operations	Operating commands
Perform the cable diagnostics	cable-diagnostics tdr execute interface
Display cable diagnostics	show cable-diagnostics tdr
Clear cable diagnostic results	clear cable-diagnostics tdr

The following commands included in smart switches can be used in the same way as the commands above.

- test cable-diagnostics tdr interface
- show test cable-diagnostics tdr
- clear test cable-diagnostics tdr

Examples of Command Execution

Perform the cable diagnostics

Diagnose of the LAN cable connected to port 1.1 as follows.

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

Checking previous diagnostic results

Display the previous diagnostic results as follows.

```
Yamaha# show test cable-diagnostics tdr
Last run on Tue May 31 18:12:13 2022
Port      Pair  Status  Fault distance
-------------------------------------------
port1.1   1     OK      -
          2     OK      -
          3     Open    15  m
          4     Open    15  m
```

Points of Caution

- This function performs simplified diagnostics. Note that it cannot be used for precision diagnosis of more specialized equipment.
- Cables 10 m or longer can be diagnosed. Cables shorter than 10 m cannot be diagnosed in some cases.
- Communication is temporarily stopped during cable diagnostics.
- Diagnostics cannot be performed if a **shutdown** command is specified for a corresponding port or the port is shut down either because a loop was detected or for any other reason.
- Diagnostics cannot be performed properly in some cases if the port on the opposite end is linked at a speed less than 1 Gbps.
- Diagnostics cannot be performed properly if PoE power is supplied at a corresponding port.
- If a stack is configured, commands cannot be executed from member switches in the stack.

Related Documentation

- None

Config Management

Function Overview

This product uses the following config information to maintain the value of settings.

Config type	Description	User operations possible
Running config (running-config)	The currently-running setting values. Managed in RAM.	View / Save to startup config
Startup config (startup-config)	Saved setting values. Five config files are maintained in ROM, and one on the SD card. When the system starts up, either the config from ROM that is selected by the **startup-config select** command or the config from the SD card is loaded. One configuration on the SD card is controlled in the "/swx2310p/startup-config" folder.	View / Delete / Copy
Default config (default-config)	The default setting values. Managed in ROM.	No operations possible

Definition of Terms Used

None

Function Details

Running config

running-config is the settings that are currently operating; since it is maintained in RAM, it is destroyed at reboot.
On this product, commands executed in configuration mode are immediately applied to running-config, and the unit operates according to these settings.
The contents of running-config can be viewed by using the **show running-config** command.

Startup config

startup-config is settings that are saved in flash ROM or on the SD card, and the contents are preserved through reboot.
When this product is started, the settings of startup-config are applied as the initial settings of running-config.

This product can maintain five startup configs in flash ROM and one startup config on the SD card.
The startup-config in the unit's flash ROM is managed with an ID of 0 to 4, and the config on the SD card is managed with the keyword "sd".

To specify which of the five types of config in the unit's flash ROM are used, use the **startup-config select** command.

- By default, **sd** is used.
- When executing the **startup-config select** command, the user selects whether to restart. If you don't restart, no change occurs in the command setting.
  If you choose to restart, the unit restarts with the startup-config of the ID specified by the user's command.

When updating from firmware Rev.2.02.09 or earlier to firmware Rev.2.02.10 or later, if **startup-config select 0** is

specified, the setting value will automatically be changed to **startup-config select sd**.
Therefore, if you are using the system with a microSD card containing CONFIG inserted, be aware that the system will boot from the SD card.
This does not apply if you execute the startup-config select command with firmware Rev.2.02.10 or later and then downgrade to firmware Rev.2.02.09 or earlier.

For easier management, you can use the **startup-config description** command to give each config a **Description (explanatory text)**.

If you attempt to start up in a state where startup-config does not exist, such as after executing the **cold start** command, the default-config is automatically applied.

The running-config settings can be saved in startup-config by the **copy running-config startup-config** command or the **write** command.
The contents of startup-config can be erased by the **erase startup-config** command, viewed by the **show startup-config** command, and copied by the **copy startup-config** command.

Default config

default-config contains settings saved in internal flash ROM that are needed for this product to operate minimally as a switch. Like startup-config, the contents are preserved even after a restart.
The factory settings are maintained as default-config.
If startup-config does not exist when the system starts, default-config is copied to startup-config, and applied to running-config.
The contents of default-config cannot be viewed.

Deciding the config file at startup

The following describes the flow for deciding the config file used when this product starts up.

1. The **startup-config select** command setting value is referenced to determine the startup-config that will be used.
   If the **startup-config select** command has specified **sd**, and an SD card on which startup-config is saved is not inserted, then startup-config #0 is selected.
2. If the startup-config that is determined exists, the corresponding data is applied as running-config in RAM.
   If the startup-config determined according to the value of the **startup-config select** command does not exist in ROM, then default-config is applied to RAM.

If startup using the config in the SD card fails, the following message is shown in the console and in SYSLOG.

```
Loading config0 because can't read config in SD card.
```

Controlling the config file via TFTP

If this product’s TFTP server function is enabled, a TFTP client installed on a PC or other remote terminal can be used to perform the following.

1. Acquire the currently running running-config and startup-config
2. Apply a previously prepared settings file as startup-config

In order for the TFTP server to function correctly, an IP address must be specified for the VLAN.
The settings files can be acquired/set from a remote terminal in binary mode. Specify the following as the remote path of the acquisition source/transmission destination of the settings files.
Also, specify the administrative password in the form “/PASSWORD” appended to the end of the remote path.
However, the config file cannot be obtained or specified if the default administrative password is still specified.

The administrative password setting must be changed in advance.
The startup-config settings are applied as running-config after the system is restarted.

Target CONFIG	Target file	Remote path	Get (GET)	Setting (PUT)	Automatic restart
running-config	CONFIG file (.txt)	config	Yes	Yes	-
startup-config # 0	CONFIG file (.txt)	config0	Yes	Yes	-
	All settings (.zip)	config0-all	Yes	Yes	-
startup-config # 1	CONFIG file (.txt)	config1	Yes	Yes	-
	All settings (.zip)	config1-all	Yes	Yes	-
startup-config # 2	CONFIG file (.txt)	config2	Yes	Yes	-
	All settings (.zip)	config2-all	Yes	Yes	-
startup-config # 3	CONFIG file (.txt)	config3	Yes	Yes	-
	All settings (.zip)	config3-all	Yes	Yes	-
startup-config # 4	CONFIG file (.txt)	config4	Yes	Yes	-
	All settings (.zip)	config4-all	Yes	Yes	-
startup-config # SD	CONFIG file (.txt)	configsd	Yes	Yes	-
	All settings (.zip)	configsd-all	Yes	Yes	-

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

Target CONFIG	Target file	Remote path	Get (GET)	Setting (PUT)	Automatic restart
Currently running startup-config	CONFIG file (.txt)	reconfig	-	Yes	Yes

When applying (PUT) a settings file, make sure that the target CONFIG and the target file type are correct.

If an incorrect file is specified, the contents cannot be reflected correctly.
For running-config, you need to add the following to the beginning of the settings file.

```
!
! Switch Configuration
!
```

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Save running config	copy running-config startup-config
Save running config	write
Copy startup config	copy startup-config

Operations	Operating commands
Erase startup config	erase startup-config
Show startup config	show startup-config
Select startup config	startup-config select
Set description for startup config	startup-config description

Examples of Command Execution

Select startup config

Select startup-config #1 and restart the system.

```
Yamaha#startup-config description 1 TEST ①
Yamaha#startup-config select 1 ②
reboot system? (y/n): y ③
```

① Set the description “TEST” to startup-config #1

② Select startup-config #1

③ Restart the system

Save running config

Save running-config.

```
Yamaha#copy running-config startup-config
Suceeded to write configuration
Yamaha#
```

Copy startup config

Copy startup-config #2 to the SD card.

```
Yamaha#copy startup-config 2 sd ①
Suceeded to copy configuration
Yamaha#show startup-config sd ②
!
!  Last Modified: Tue Mar 13 17:34:02 JST 2018
!
dns-client enable
!
interface port1.1
 switchport
 switchport mode access
 no shutdown
!
...
```

① Copy startup-config #2 to the SD card

② Show startup-config on the SD card

Erase startup config

Erase startup-config from the SD card.

```
Yamaha#erase startup-config sd ①
Suceeded to erase configuration
Yamaha#
```

① Erase startup-config in the SD card

Points of Caution

None

Related Documentation

- Use of External Memory

Remote Access Control

Function Overview

This product lets you restrict access to the following applications that implement network services.

- TELNET server
- SSH server
- HTTP server / HTTPS server
- TFTP server
- SNMP server

Definition of Terms Used

None

Function Details

The following four functions are provided to limit access to network services.

- Control whether to leave the service in question running in the background on the system (start/stop control)
- Change reception port number
- Limit access destinations for services currently running
- Limit the source IP addresses that can access services currently running

The following functions that correspond to each network service are shown in the table below.

- Network service access control

Network service	Start/stop control	Change reception port number	Access destination restriction	Access source restriction
TELNET server	Yes	Yes	Yes	Yes
SSH server	Yes	Yes	Yes	Yes
HTTP server HTTPS server	Yes	Yes	Yes	Yes
TFTP server	Yes	Yes	Yes	No
SNMP server	× (Always booted)	× (Always 161)	No	Yes

1. Multiple instances of a network service cannot be started.
   If the start control is applied to the same service that is currently running, the service will restart.
   Consequently, any connected sessions will be **disconnected**.
2. Limiting access destinations for network services is done for the **VLAN interface**.
3. Sources permitted to access network services can be restricted by specifying **access source IP address** and **access permit/deny** settings.
4. The default settings for the network services are shown in the table below.

Network service	Start/stop status	Reception port number	Access destination restriction	Access source restriction
TELNET server	run	23	Only default maintenance VLAN (VLAN #1) permitted	Allow all
SSH server	stop	22	Only default maintenance VLAN (VLAN #1) permitted	Allow all
HTTP server	run	80	Only default maintenance VLAN (VLAN #1) permitted	Allow all
HTTPS server	stop	443		
TFTP server	stop	69	Only default maintenance VLAN (VLAN #1) permitted	Allow all
SNMP server	run	161	Allow all	Allow all

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Network service	Operations	Operating commands
Common	Maintenance VLAN	management interface
TELNET server	Start/stop	telnet-server
	Change reception port number	telnet-server enable (use argument to specify port number)
	Access control	telnet-server interface
	IP address access control	telnet-server access
	Show settings	show telnet-server
SSH server	Start/stop	ssh-server
	Change reception port number	ssh-server enable (use argument to specify port number)
	Access control	ssh-server interface
	IP address access control	ssh-server access
	Check whether client is alive	ssh-server client alive
	Show settings	show ssh-server
	Generate host key	ssh-server host key generate
	Clear host key	clear ssh-server host key
	Show public key	show ssh-server host key

Network service	Operations	Operating commands
HTTP server	Start/stop HTTP server	http-server
	Change HTTP server’s reception port number	http-server enable (use argument to specify port number)
	Start/stop HTTPS server	http-server secure
	Change HTTPS server’s reception port number	http-server secure enable (use argument to specify port number)
	Access control	http-server interface
	IP address access control	http-server access
	Show settings	show http-server
TFTP server	Start/stop	tftp-server
	Access control	tftp-server interface
SNMP server	Access control by IP address and community name	snmp-server access

Examples of Command Execution

TELNET server access control

This example restricts access to the TELNET server.

Change the TELNET server’s reception port to 1024.
Change the maintenance VLAN to **VLAN #1000** and allow access. Access from other than the maintenance VLAN is denied.

Connection to the TELNET server is allowed only by clients from 192.168.100.1.
If you specify telnet-server access, access from IP addresses that do not meet the conditions is denied.

```
Yamaha(config)#telnet-server enable 1024 ①
Yamaha(config)#management interface vlan1000 ②
Yamaha(config)#telnet-server access permit 192.168.100.1 ③
Yamaha(config)#end
Yamaha#show telnet-server ④
Service:Enable
Port:1024
Management interface(vlan):1000
Interface(vlan):None
Access:
    permit 192.168.100.1
```

① Change the reception port to 1024 and reboot the TELNET server

② Allow access from VLAN #1000 as the maintenance VLAN

③ Allow access only from 192.168.100.1

④ Check the settings

SSH server access control

This example restricts access to the SSH server.

Generate the SSH server host key.

Register a user name and password.

Login from an SSH client is possible only for a registered user and password.

Change the SSH server’s reception port to 1024.

Change the maintenance VLAN to **VLAN #1000** and permit access to **VLAN #2**.

Consequently, access is only permitted from **VLAN #1000** and from **VLAN #2** on the maintenance VLAN.
If you specify ssh-server access, access from IP addresses that do not meet the conditions is denied.

```
Yamaha#ssh-server host key generate ①
Yamaha#show ssh-server host key ②
ssh-dss (Omitted)
ssh-rsa (Omitted)
Yamaha#
Yamaha#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Yamaha(config)#username user1 password pw1 ③
Yamaha(config)#ssh-server enable 1024 ④
Yamaha(config)#management interface vlan1000 ⑤
Yamaha(config)#ssh-server interface vlan2 ⑥
Yamaha(config)#end
Yamaha#show ssh-serverr ⑦
Service:Enable
Port:1024
Hostkey:Generated
Client alive :Disable
Management interface(vlan):1000
Interface(vlan):2
Access:None
Yamaha#
```

① Create a host key

② Check contents of the key

③ Register a username and password.

④ Change the reception port to 1024 and reboot the SSH server

⑤ Allow access from #1000 as the maintenance VLAN

⑥ Allow access from VLAN #2

⑦ Check the settings

HTTP server access restrictions

This example restricts access to the HTTP server.

Change the HTTP server reception port to 8000 and permit access from **VLAN #2**.

That permits access only from the default maintenance VLANs **VLAN #1** and **VLAN #2**.

Connection to the HTTP server is allowed only by clients from 192.168.100.1.
If you specify http-server access, access from IP addresses that do not meet the conditions is denied.

```
Yamaha(config)#http-server enable 8000 ①
Yamaha(config)#http-server interface vlan2 ②
Yamaha(config)#http-server access permit 192.168.100.1 ③
Yamaha(config)#end
Yamaha#show http-server ④
HTTP :Enable(8000)
HTTPS:Disable
Management interface(vlan):1
Interface(vlan):2
Access:
    permit 192.168.100.1
```

① Change the reception port to 8000 and reboot the HTTP server

② Allow access from VLAN #2

③ Allow access only from 192.168.100.1

④ Check the settings

TFTP server access restrictions

This example restricts access to the TFTP server.

Change the TFTP server reception port to 2048 and permit access from **VLAN #10**.
Allow access only from the default maintenance VLANs **VLAN #1** and **VLAN #10**.

```
Yamaha(config)#tftp-server enable 2048 ①
Yamaha(config)#tftp-server interface vlan10 ②
```

① Change the reception port to 2048 and reboot the TFTP server

② Allow access from VLAN #10

SNMP server access restrictions

This restricts access to the SNMP server.

Access to “public” communities is restricted to clients from 192.168.100.0/24.
In addition, access to “private” communities is restricted to clients from 192.168.100.1.

```
Yamaha(config)#snmp-server access permit 192.168.100.0/24 community public ①
Yamaha(config)#snmp-server access permit 192.168.100.1 community private ②
```

① The community name “public” allows access only from 192.168.100.0/24

② The community name “private” allows access only from 192.168.100.1

Points of Caution

If the password (admin) for the default administrative user admin is left unchanged, then the following restrictions are applied.

- Network switches cannot be accessed by TELNET, SSH, HTTP, or HTTPS from a network segment other than the maintenance VLAN.

The following restrictions apply if a TFTP server is accessed from a TFTP client.

- Access is denied if the privileged password (administrative password) is still set to the default setting. Privileged passwords (administrative passwords) must be changed in advance.
- If the primary and secondary addresses for a VLAN being accessed are the same segment, then the IPv4 secondary address cannot be accessed.

- If accessing the VLAN with an IPv6 address, then only the IPv6 address specified last can be accessed. Because the internal address is reset if the network switch is started, that means only the bottom IPv6 address listed in the order they were configured can be accessed.
- Only the IP address of the VLAN with the closest routing to the TFTP client can be accessed. For example, a TFTP client located on VLAN 1 cannot access VLAN 2 IP addresses for the network switch.

Related Documentation

- User account management

Time Management

Function Overview

This product provides the functions shown below for managing the date and time.

- Manual (user-configured) date/time information setting function
- Automatic date/time setting information function via network
- Time zone setting function
- Function for setting “daylight saving time” (DST or “daylight time”) settings

Definition of Terms Used

UTC（Coordinated Universal Time）

This is an official time used when recording worldwide times.
UTC is used as a basis to determine standard time in all countries around the world.
For instance, Japan (JST, or Japan standard time) is nine hours ahead of Coordinated Universal Time, and is thus shown as “+0900 (JST)”.

SNTP（Simple Network Time Protocol）

This is a simple protocol to correct clocks by using SNTP packets.
This protocol is defined in RFC4330.

Function Details

Manually setting the date and time

Use the **clock set** command to directly enter clock setting values.

Automatically setting the date and time

Date and time information is collected from a specified time server, and set in this product.
Defined in RFC4330, SNTP (Simple Network Time Protocol) is used as a communication protocol.
Up to two time servers can be specified using an IPv4 address, IPv6 address, or fully qualified domain name (FQDN).
Port number 123 is used for the SNTP client. (This setting cannot be changed by the user.)
The **ntpdate** command can be used to select one of two methods for automatically setting date and time settings.

- One-shot update (a function to update when a command is inputted)
- Interval update (a function to update in a 1–24-hour cycle from command input)

If clock settings are synchronized with two time servers specified, queries are processed in the order they are displayed by the **show ntpdate** command, which is NTP server 1 and then NTP server 2.
Queries to NTP server 2 are only processed if synchronization with NTP server 1 fails.
Given default settings, **one hour** is specified as the interval update cycle.
However, when the default time cannot be set right after booting up the system, the time server will be queried in a one-minute cycle, regardless of the interval cycle time.
Synchronization with the time server operates with one sampling (the frequency of replies from the server) and with a timeout of 1 second.
Synchronization is blocked during command execution, and an error message is outputted if a timeout occurs.

Time zone setting

In order to manage the time for the region considered as the “base of daily life”, the “clock timezone” command is used to manage the time zone of the users, and reflect this into the time.
The time zone can be set in ±1 hour increments for Coordinated Universal Time (UTC), from -12 hours to +13 hours.
The default time zone value for this product is **+9.0**.

Daylight saving time setting

Users can set “daylight saving time” (DST or “daylight time”) settings using the **clock summer-time** command.
The following parameter settings are specified.

- Time zone name
  The time zone name is displayed when daylight saving time is in effect.
- Start and end times of daylight saving time
  You can specify the time in one of two ways:
  - Recurring
    If daylight saving time occurs every year for the same period, then this specifies the week and day of the month it occurs.
  - Specific dates
    This specifies the specific dates daylight saving time is applied.
- Offset
  This specifies how long (minutes) to extend the daylight saving time period.
  The setting range is from 1 to 1440 minutes. The setting value is **60 minutes** unless specified otherwise.

Overlapping daylight saving time periods cannot be specified.
Daylight saving time settings can be checked using the show clock detail command.

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Set clock manually	clock set
Time zone setting	clock timezone
Set daylight saving time settings (recurring)	clock summer-time recurring
Set daylight saving time settings (specific date)	clock summer-time date
Show current time	show clock
Set NTP server	ntpdate server
Synchronize time from NTP server (one-shot update)	ntpdate oneshot
Synchronize time from NTP server (update interval)	ntpdate interval
Show NTP server time synchronization settings	show ntpdate

Examples of Command Execution

Set clock manually

In this example, the time zone is set to **JST** and the current time is set to **2014.01.21 15:50:59**.

```
Yamaha#configure terminal
Yamaha(config)#clock timezone JST ①
Yamaha(config)#exit
Yamaha#clock set 15:50:59 Jan 21 2014 ②
Yamaha#show clock ③
15:50:59 JST Tue Jan 21 2014
```

① Time zone setting

② Time settings

③ Show current time

Automatically setting the time

In this example, the time zone is set to **+9.00** and the local address **192.168.1.1** and **ntp.nict.jp** are specified as the NTP servers.
Also, the NTP server update cycle is changed to **once every 24 hours**.

```
Yamaha#configure terminal
Yamaha(config)#clock timezone +9:00 ①
Yamaha(config)#ntpdate server ipv4 192.168.1.1 ②
Yamaha(config)#ntpdate server name ntp.nict.jp ③
Yamaha(config)#ntpdate interval 24 ④
Yamaha(config)#exit
Yamaha#show clock ⑤
10:03:20 +9:00 Mon Dec 12 2016
Yamaha#show ntpdate ⑥
NTP server 1 : 192.168.100.1
NTP server 2 : ntp.nict.jp
adjust time : Mon Dec 12 10:03:15 2016 + interval 24 hours
sync server : 192.168.100.1
```

① Time zone setting

② Set NTP server

③ Set NTP server

④ Set NTP server update cycle to 24 hours

⑤ Show current time

⑥ Show NTP time synchronization settings

Daylight saving time setting

Recurring

In this example, daylight saving time is set to occur every year starting from 2 AM on the second Sunday of March to 2 AM on the first Sunday of November.

```
Yamaha#configure terminal
```

```
Yamaha(config)#clock summer-time JDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00 ①
Yamaha(config)#exit
Yamaha#show clock detail ②
Fri Jan  1 00:00:20 JST 2021

Summer Time
  Type   : Recurring
  Offset : 60 (min)
  From   : Sun Mar 14 02:00:00 JST 2021 ③
  To     : Sun Nov 7 02:00:00 JDT 2021
```

① Daylight saving time setting

② Check the daylight saving time settings

③ Show the actual dates of the next (or currently in effect) daylight saving time period

Specific dates

In this example, the settings specify starting daylight saving time at 2 AM on March 14, 2021, and ending it on November 7, 2021.

```
Yamaha#configure terminal
Yamaha(config)#clock summer-time JDT date Mar 14 2021 2:00 Nov 7 2021 2:00 ①
Yamaha(config)#exit
Yamaha#show clock detail ②
Fri Jan  1 00:02:54 JST 2021

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

① Daylight saving time setting

② Check the daylight saving time settings

Points of Caution

None

Related Documentation

- RFC 4330: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

SNMP

Function Overview

Setting SNMP (Simple Network Management Protocol) makes it possible to monitor and change network management information for SNMP management software.
In this instance, this product will operate as an SNMP agent.

This product supports communication using SNMPv1, SNMPv2c, and SNMPv3. In terms of management information bases (MIB), it supports RFC1213 (MIB-II) and private MIBs (Yamaha switches).

SNMPv1 and SNMPv2 protocols send notification of the group name (referred to as a “community”) to recipients and only communicate between hosts that belong to that same community. In that case, different community names can be specified for two access modes, either the read-only or read-write mode.
In this way, community names function as a kind of password, but they carry inherent security risks because they must be sent over a network using plain text. The use of SNMPv3 is recommended when more secure communications are required.
SNMPv3 offers communication content authentication and encryption. SNMPv3 does away with the concept of community and instead uses security models called “USM” (User-based Security Model) and “VACM” (View-based Access Control Model). These models provide a higher level of security.

SNMP messages that notify the status of this product are called “traps”. This product transmits standard SNMP traps. In SNMPv1, trap requests that do not ask for an answer with the confirmation of receipt from the recipient are specified as the notification message format. However, with SNMPv2c and SNMPv3, either an “inform” request asking for an answer from the recipient, or a trap request can be selected.

Since this product does not specifically specify a default community name value for read-only and transmission traps used for SNMPv1 and SNMPv2c protocols, be sure to specify an appropriate community name. However, as described above, community names are sent over the network in plain text, so be careful to never use a login password or administrator password as the community name.
By default, no access is possible in each SNMP version. The transmission host for the trap is not set, so traps will not be sent anywhere.

This product can restrict access to the SNMP server. Specifying access restrictions can restrict access from unintended hosts.

Definition of Terms Used

None

Function Details

The main characteristics of each SNMP version and the router setting policies are explained below.
For specific examples of settings, see **“Examples of Command Execution”** below.

SNMPv1

This is authentication between the SNMP manager and agent by using community names.
The controlling device (this product) is divided and managed by zones called “communities”.

- Accessing the MIB objects

  Community names specified using the **snmp-server community** command are used to permit access. Access is possible from a VLAN interface whose IP address has been specified.

- SNMP traps

  The status of switches can be sent to hosts specified using the **snmp-server host** command.
  The **snmp-server enable trap** command is used to specify the kind of trap to send.

The **snmp-server startup-trap-delay** command is used to specify when to send the trap during startup.

SNMPv2c

As with SNMPv1, community names are used for authentication between the SNMP manager and agents.
The **snmp-server community** command is used to specify the community names used to access switches by SNMPv2c.
The “GetBulk” and “Inform” requests are also now supported from this version.
These requests are used to efficiently retrieve multiple MIB objects, and to confirm replies to notification packets sent from this product.

- Accessing the MIB objects
  Community names specified using the **snmp-server community** command are used to permit access.
  Access is possible from a VLAN interface whose IP address has been specified.

- SNMP traps
  The status of switches can be sent to hosts specified using the **snmp-server host** command.
  Also, the settings of this command can be used to select whether the transmitted message format is a trap or inform request.
  Inform requests are used to request confirmation of reply to the recipient.
  The **snmp-server startup-trap-delay** command is used to specify when to send the trap during startup.

SNMPv3

In addition to all of the functions offered in SNMPv2, SNMPv3 offers more robust security functions.
SNMPv3 can authenticate and encrypt SNMP packets sent across the network to protect packets from eavesdropping, spoofing, falsification, replay attacks, and other risks and achieve security levels not possible with SNMPv1 or SNMPv2c functionality, such as community names or SNMP manager IP addresses.

- Security
  SNMPv3 offers the following security functions.

  1. USM (User-based Security Model)
     USM is a model for maintaining security at the message level. It offers authentication and encryption based on shared key cryptography and prevents falsification of message streams.

     - Security level
       The security level can be specified using the parameter settings for the group to which users belong.
       Security levels are classified based on a combination of authentication and encryption, as indicated below.

       - noAuthNoPriv : No authentication or encryption
       - AuthNoPriv : Authentication only
       - AuthPriv : authentication and encryption

     - User authentication
       For authentication, HMAC is used in the procedure to authenticate the integrity (whether data has been falsified or not) and the source.
       A hash is used in the authentication key to confirm whether the message has been falsified, and whether the sender is the user themselves.
       Both HMAC-MD5-96 and HMAC-SHA-96 are supported as hash algorithms.

     - Encryption
       With SNMPv3, SNMP messages are encrypted for the purpose of preventing leakage of managed information.
       Both the DES-CBC and AES128-CFB encryption schemes are supported.

The **snmp-server user** command can be used to specify usernames, corresponding group names, user authentication methods, encryption methods, and passwords.
The necessary authentication and encryption settings can be made according to the security level specified in the group settings.

2. VACM (View-based Access Control Model)
   VACM is a model for controlling access to SNMP messages.

   - Group

     With VACM, the access policies mentioned below are defined per group, not per user.
     Use the **snmp-server user** command with the optional "group" setting to specify user group affiliation. The MIB views set here that are accessible to the specified groups can be configured.

   - MIB view
     With SNMPv3, a collection of accessible MIB objects can be defined for each group. When defined, the collection of MIB objects is called the "MIB view". The "MIB view" is expressed as a collected view sub-tree that shows the object ID tree.
     Use the **snmp-server view** command to specify the MIB view. Whether the MIB view should be included or excluded in each view sub-tree can be selected.

   - Access policy

     With VACM, set the MIB view that will permit reading and writing for each group.

     Use the **snmp-server group** command to set the group name, security level, and MIB view.
     The MIB view is the MIB view specified using the **snmp-server view** command.

- SNMP traps

  The status of switches can be sent to hosts specified using the **snmp-server host** command.

  In order to transmit a trap, the **snmp-server user** command must first be used to configure the user.
  Also, the settings of this command can be used to select whether the transmitted message format is a trap or inform request.

  Inform requests are used to request confirmation of reply to the recipient.
  The **snmp-server startup-trap-delay** command is used to specify when to send the trap during startup.

Restricting SNMP server access

Hosts able to access the product's SNMP server can be specified using the **snmp-server access** command.

Access from unintended hosts can be restricted by only allowing access from the intended SNMP manager.

Default settings accept access from all hosts. Specify access restrictions based on the operating environment.
For more information about access restrictions, refer to Remote Access Control.

Private MIBs

This product supports yamahaSW, which is a proprietary private MIB for switch management.
This private MIB allows the obtaining of information for Yamaha's proprietary functions, and for more detailed information about the switch.
For information about supported private MIBs and how to obtain private MIBs, refer to the "SNMP MIB Reference" chapter in the HTML version of this document.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Set host that receives SNMP notifications	snmp-server host

Operations	Operating commands
Set how long to wait for notification messages to be transmitted when starting up the system.	snmp-server startup-trap-delay
Set notification type to transmit	snmp-server enable trap
Set system contact	snmp-server contact
Set system location	snmp-server location
Set SNMP community	snmp-server community
Set SNMP view	snmp-server view
Set SNMP group	snmp-server group
Set SNMP user	snmp-server user
Specify SNMP server access settings	snmp-server access
Show SNMP community information	show snmp community
Show SNMP view settings	show snmp view
Show SNMP group settings	show snmp group
Show SNMP user settings	show snmp user

Examples of Command Execution

SNMPv1 setting example

This example makes SNMPv1-based network monitoring possible under the following conditions.

1. Set the read-only community name “public”.
2. Set the trap destination as “192.168.100.11”, and set trap community name to “snmptrapname”.
3. Hosts that can access communities named “public” are restricted to only 192.168.100.0/24.

```
Yamaha(config)# snmp-server community public ro                            ... 1
Yamaha(config)# snmp-server host 192.168.100.11 traps version 1 snmptrapname ... 2
Yamaha(config)# snmp-server access permit 192.168.100.0/24 community public  ... 3
```

SNMPv2c setting example

This example makes SNMPv2c-based network monitoring possible under the following conditions.

1. Set the readable/writable community name as “private”.
2. Specify the notification message destination as “192.168.100.12”, the notification type as “inform” request format, and the notification destination community name as “snmpinformsname”.
3. Hosts that can access communities named “private” are restricted to only 192.168.100.12.

```
Yamaha(config)# snmp-server community private rw                              ...1
Yamaha(config)# snmp-server host 192.168.100.12 informs version 2c snmpinformsname ...2
Yamaha(config)# snmp-server access permit 192.168.100.12 community private        ...3
```

SNMPv3 setting example

This example makes SNMPv3-based network monitoring possible under the following conditions.

1. Specify the view that shows the internet node (1.3.6.1) and below as “most”.
2. Specify the view that shows the mib-2 node (1.3.6.1.2.1) and below as “standard”.
3. Create the user group “admins” and assign full access rights to the “most” view for all users in the “admins” group.
4. Create the user group “users” and assign read-only access rights for the “standard” view to users in the “users” group.
5. Create an “admin1” user that belongs to the “admins” group.
   Set the password to “passwd1234”, using the “HMAC-SHA-96” authentication algorithm.
   Set the encryption password to “passwd1234”, using the “AES128-CFB” encryption algorithm.
6. Create an “user1” user that belongs to the “users” group.
   Set the password to “passwd5678”, using the “HMAC-SHA-96” authentication algorithm.
7. Send notifications in trap format (without response confirmation) to 192.168.10.3.
8. Send notifications in inform request format to 192.168.20.3.

```
Yamaha(config)# snmp-server view most 1.3.6.1 include                               ... 1
Yamaha(config)# snmp-server view standard 1.3.6.1.2.1 include                       ... 2
Yamaha(config)# snmp-server group admins priv read most write most                  ... 3
Yamaha(config)# snmp-server group users auth read standard                          ... 4
Yamaha(config)# snmp-server user admin1 admins auth sha passwd1234 priv aes passwd1234 ... 5
Yamaha(config)# snmp-server user user1 users auth sha passwd5678                    ... 6
Yamaha(config)# snmp-server host 192.168.10.13 traps version 3 priv admin1          ... 7
Yamaha(config)# snmp-server host 192.168.20.13 informs version 3 priv admin1        ... 8
```

Points of Caution

- Check the SNMP version that can be used with the SNMP manager beforehand. It is necessary to configure this product in accordance with the SNMP version that will be used.
- This product is not compatible with the following functions related to SNMPv3.
  - Proxy function
  - Access to MIB objects after the SNMPv2 subtree (1.3.6.1.6). Changing SNMPv3-related settings via SNMP is also not supported.
- Character string specifications for the community name, username, password, and group name are as follows.
  - When enclosed in single or double quotation marks, the character string in the single or double quotation marks is used.
    - The case where there is a character string outside the single or double quotation marks is not supported.
    - If a character string is enclosed in single or double quotation marks, the single or double quotation marks on both ends are not included in the character count.
    - The group name is assigned to the character string used with the **snmp-server user** command.
      - It is not assigned to the character string used with the **snmp-server group** command.
  - The use of \ is not supported.
  - The use of only single or double quotation marks is not supported.

- SNMP server access restrictions specified using the **snmp-server access** command only apply to SNMPv1 and SNMPv2c access. They do not apply to SNMPv3 access.

Related Documentation

- Yamaha RTpro SNMP
- Yamaha RTpro Private MIB
- SNMP MIB Reference

RMON

Function Overview

By making settings for the RMON (Remote network MONitering) function, you can monitor and record the traffic volume and error occurrences for each interface.
Since the settings for the RMON function and the data obtained by the RMON function are held as an MIB, they can be retrieved and edited from the SNMP manager.

The RMON function of this product supports the following groups defined in RFC2819.

- Ethernet statistics group
- History group
- Alarm group
- Event group

Definition of Terms Used

RMON MIB

MIB for the RMON function, defined in RFC2819

Ethernet statistics group

MIB group defined as group 1 of the RMON MIB.
This holds a table for monitoring Ethernet statistical information.
The information in the table includes counters for the number of packets, the number of errors, etc.
The etherStatsTable is the applicable MIB for this product.

History group

MIB group defined as group 2 of the RMON MIB.
At a specified interval, it measures the same information as the Ethernet statistics group, and has a table for saving the history of this information.
The MIBs relevant for this product are the historyControlTable and the etherHistoryTable.

Alarm group

MIB group defined as group 3 of the RMON MIB.
At the specified interval, the statistical information of the Ethernet statistics group is compared with the threshold values.
If the sampled values exceed the threshold values, the event defined for the event group is generated.
The alarmTable is the applicable MIB for this product.

Event group

MIB group defined as group 9 of the RMON MIB.
This is the action taken in response when the alarm group conditions are met.
The eventTable is the applicable MIB for this product.

Function Details

The operating specifications for operation of the RMON function are shown below.

Common between groups

The specifications common between groups are given below.

1. In order to enable the RMON function on this product, the system-wide RMON function must be enabled.
    - Use the **rmon** command to make settings.
    - This is enabled by default.
    - You can also set this by using the private MIB ysrmonSetting(1.3.6.1.4.1.1182.3.7.1).

Ethernet statistics group

The operating specifications for the Ethernet statistics group are given below.

1. Make settings by using the **rmon statistics** command on an interface.
2. Starting at the point at which you specified the **rmon statistics** command, statistical information is collected, and the etherStatsTable of the RMON MIB will be available for retrieval.
3. This can be specified for a physical interface.
4. A maximum of eight **rmon statistics** commands can be specified for the same interface.
5. If an **rmon statistics** command is deleted, the collected statistical information is also deleted.
6. If an **rmon statistics** command is overwritten, the previously collected statistical information is deleted, and collection is started once again.
7. If the RMON function is disabled system-wide, collection of statistical information is halted.
   If the RMON function is subsequently enabled system-wide, the previously collected statistical information is deleted, and collection is started once again.
8. The supported OIDs in the Ethernet statistics group are as follows.

```
rmon(1.3.6.1.2.1.16)
 +- statistics(1.3.6.1.2.1.16.1)
     +- etherStatsTable(1.3.6.1.2.1.16.1.1)
             + etherStatsEntry(1.3.6.1.2.1.16.1.1.1) { etherStatsIndex }
                 +- etherStatsIndex(1.3.6.1.2.1.16.1.1.1.1)         (read-only)
                 +- etherStatsDataSource(1.3.6.1.2.1.16.1.1.1.2)    (read-create)
                 |Interface being monitored
                 +- etherStatsDropEvents(1.3.6.1.2.1.16.1.1.1.3)    (read-only)
                 |Number of packets dropped
                 +- etherStatsOctets(1.3.6.1.2.1.16.1.1.1.4)        (read-only)
                 |Number of octets received
                 +- etherStatsPkts(1.3.6.1.2.1.16.1.1.1.5)          (read-only)
                 |Number of packets received
                 +- etherStatsBroadcastPkts(1.3.6.1.2.1.16.1.1.1.6) (read-only)
                 |Number of broadcast packets received
                 +- etherStatsMulticastPkts(1.3.6.1.2.1.16.1.1.1.7) (read-only)
                 |Number of multicast packets received
                 +- etherStatsCRCAlignErrors(1.3.6.1.2.1.16.1.1.1.8)(read-only)
                 |Number of FCS error packets received
                 +- etherStatsUndersizePkts(1.3.6.1.2.1.16.1.1.1.9) (read-only)
                 |Number of undersize packets received (packets smaller than 64 octets)
                 +- etherStatsOversizePkts(1.3.6.1.2.1.16.1.1.1.10) (read-only)
                 |Number of oversize packets received (packets larger than 1518 octets)
                 +- etherStatsFragments(1.3.6.1.2.1.16.1.1.1.11)    (read-only)
                 |Number of fragment packets received
                 |(packets smaller than 64 octets with abnormal FCS)
                 +- etherStatsJabbers(1.3.6.1.2.1.16.1.1.1.12)      (read-only)
```

```
                  |Number of jabber packets received
                  |(packets larger than 1518 octets with abnormal FCS)
                  +- etherStatsCollisions(1.3.6.1.2.1.16.1.1.1.13)   (read-only)
                  |Number of collisions
                  +- etherStatsOwner(1.3.6.1.2.1.16.1.1.1.20)        (read-create)
                  |Name of owner
                  +- etherStatsStatus(1.3.6.1.2.1.16.1.1.1.21)       (read-create)
                        Status of statistical group
```

History group

The operating specifications for the history group are shown below.

1. Make settings by using the **rmon history** command on an interface.
2. Starting at the point at which you specified the **rmon history** command, historical information is collected at the specified interval, and the etherHistoryTable of the RMON MIB will be available for retrieval.
3. This can be specified for a physical interface.
4. A maximum of eight **rmon history** commands can be specified for the same interface.
5. If an **rmon history** command is deleted, the collected historical information is also deleted.
6. If an **rmon history** command is overwritten, the previously collected historical information is deleted, and collection is started once again.
7. If the RMON function is disabled system-wide, collection of historical information is halted.
   If the RMON function is subsequently enabled system-wide, the previously collected historical information is deleted, and collection is started once again.
8. The supported OIDs in the Ethernet history group are as follows.

```
 rmon(1.3.6.1.2.1.16)
  +- history(1.3.6.1.2.1.16.2)
      +- historyControlTable(1.3.6.1.2.1.16.2.1)
      |+ historyControlEntry(1.3.6.1.2.1.16.2.1.1) { historyControlIndex }
      |+- historyControlIndex(1.3.6.1.2.1.16.2.1.1.1)           (read-only)
      |+- historyControlDataSource(1.3.6.1.2.1.16.2.1.1.2)      (read-create)
      ||Interface being monitored
      |+- historyControlBucketsRequested(1.3.6.1.2.1.16.2.1.1.3)(read-create)
      ||Number of history group history saves requested
      |+- historyControlBucketsGranted(1.3.6.1.2.1.16.2.1.1.4)  (read-only)
      ||Number of history group histories saved
      |+- historyControlInterval(1.3.6.1.2.1.16.2.1.1.5)        (read-create)
      ||Interval at which history group histories are saved
      |+- historyControlOwner(1.3.6.1.2.1.16.2.1.1.6)           (read-create)
      ||Name of owner
      |+- historyControlStatus(1.3.6.1.2.1.16.2.1.1.7)          (read-create)
      |History group status
      |
      +- etherHistoryTable(1.3.6.1.2.1.16.2.2)
              + etherHistoryEntry(1.3.6.1.2.1.16.2.2.1) { etherHistoryIndex,
etherHistorySampleIndex }
                  +- etherHistoryIndex(1.3.6.1.2.1.16.2.2.1.1)         (read-only)
                  +- etherHistorySampleIndex(1.3.6.1.2.1.16.2.2.1.2)   (read-only)
                  +- etherHistoryIntervalStart(1.3.6.1.2.1.16.2.2.1.3) (read-only)
                  |Interval at which history group histories are saved
                  +- etherHistoryDropEvents(1.3.6.1.2.1.16.2.2.1.4)    (read-only)
```

```
                 |Number of packets dropped
                 +- etherHistoryOctets(1.3.6.1.2.1.16.2.2.1.5)        (read-only)
                 |Number of octets received
                 +- etherHistoryPkts(1.3.6.1.2.1.16.2.2.1.6)          (read-only)
                 |Number of packets received
                 +- etherHistoryBroadcastPkts(1.3.6.1.2.1.16.2.2.1.7) (read-only)
                 |Number of broadcast packets received
                 +- etherHistoryMulticastPkts(1.3.6.1.2.1.16.2.2.1.8) (read-only)
                 |Number of multicast packets received
                 +- etherHistoryCRCAlignErrors(1.3.6.1.2.1.16.2.2.1.9)(read-only)
                 |Number of FCS error packets received
                 +- etherHistoryUndersizePkts(1.3.6.1.2.1.16.2.2.1.10)(read-only)
                 |Number of undersize packets received (packets smaller than 64 octets)
                 +- etherHistoryOversizePkts(1.3.6.1.2.1.16.2.2.1.11) (read-only)
                 |Number of oversize packets received (packets larger than 1518 octets)
                 +- etherHistoryFragments(1.3.6.1.2.1.16.2.2.1.12)    (read-only)
                 |フNumber of fragment packets received
                 |(packets smaller than 64 octets with abnormal FCS)
                 +- etherHistoryJabbers(1.3.6.1.2.1.16.2.2.1.13)      (read-only)
                 |Number of jabber packets received
                 |(packets larger than 1518 octets with abnormal FCS)
                 +- etherHistoryCollisions(1.3.6.1.2.1.16.2.2.1.14)   (read-only)
                 |Number of collisions
                 +- etherHistoryUtilization(1.3.6.1.2.1.16.2.2.1.15)  (read-only)
                       Estimated value of network usage ratio
```

Alarm group

The operating specifications for the alarm group are shown below.

1. Use the **rmon alarm** command to make settings.
2. From the point that the **rmon alarm** command is specified, sampling occurs at the specified interval.
3. If an **rmon alarm** command is overwritten, the previous sampling data is deleted, and sampling is started once again.
4. If the RMON function is disabled system-wide, sampling is halted.
   If the RMON function is subsequently enabled system-wide, the previous sampling data is deleted, and sampling is started once again.
5. Only etherStatsEntry(.1.3.6.1.2.1.16.1.1.1) MIB objects that have a counter type can be specified as the object of alarm group monitoring.
6. If the Ethernet statistics group used by the **rmon alarm** command is deleted, the **rmon alarm** command is also deleted.
7. If the event group used by the **rmon alarm** command is deleted, the **rmon alarm** command is also deleted.
8. The supported OIDs in the alarm group are as follows.

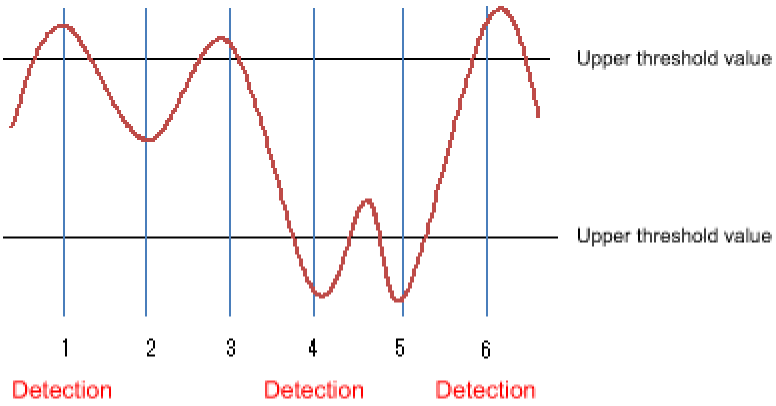
```
rmon(1.3.6.1.2.1.16)
 +- alarm(1.3.6.1.2.1.16.3)
     +- alarmTable(1.3.6.1.2.1.16.3.1)
             + alarmEntry(1.3.6.1.2.1.16.3.1.1) { alarmIndex }
                 +- alarmIndex(1.3.6.1.2.1.16.3.1.1.1)              (read-only)
                 +- alarmInterval(1.3.6.1.2.1.16.3.1.1.2)           (read-create)
                 |Sampling interval
                 +- alarmVariable(1.3.6.1.2.1.16.3.1.1.3)           (read-create)
                 |MIB object to be monitored
```

```
                    +- alarmSampleType(1.3.6.1.2.1.16.3.1.1.4)         (read-create)
                    |Sampling type
                    +- alarmValue(1.3.6.1.2.1.16.3.1.1.5)              (read-only)
                    |Estimated value
                    +- alarmStartupAlarm(1.3.6.1.2.1.16.3.1.1.6)       (read-create)
                    |Threshold value used for first alarm determination
                    +- alarmRisingThreshold(1.3.6.1.2.1.16.3.1.1.7)    (read-create)
                    |Upper threshold value
                    +- alarmFallingThreshold(1.3.6.1.2.1.16.3.1.1.8)   (read-create)
                    |Lower threshold value
                    +- alarmRisingEventIndex(1.3.6.1.2.1.16.3.1.1.9)   (read-create)
                    |Event index when crossing upper limit
                    +- alarmFallingEventIndex(1.3.6.1.2.1.16.3.1.1.10) (read-create)
                    |Event index when crossing lower limit
                    +- alarmOwner(1.3.6.1.2.1.16.3.1.1.11)             (read-create)
                    |Name of owner
                    +- alarmStatus(1.3.6.1.2.1.16.3.1.1.12)            (read-create)
                         Alarm group status
```

Alarm detection is determined by an upper threshold value and a lower threshold value. If the threshold value is crossed, the specified event is executed.

If an alarm is detected, the alarm will not be detected again until the value crosses the opposite threshold.

The following cases are explained as examples.



- At point 1, the upper threshold value is crossed, so an alarm is detected.
  The threshold value that is used for the very first decision can be specified by STARTUP.
  In the example above, we will assume that the STARTUP value is “1” (using only the upper threshold value (risingAlarm)) or “3” (using both the upper threshold value and the lower threshold value (risingOrFallingAlarm)).
- At point 2, an alarm is not detected.
- At point 3, the upper threshold value is crossed, but since the opposite threshold was not previously crossed, an alarm is not detected.
- At point 4, the lower threshold value is crossed, and since the upper threshold was previously crossed, an alarm is detected.
- At point 5, the lower threshold value is exceeded, but since the opposite upper threshold was not previously crossed, an alarm is not detected.
- At point 6, the upper threshold value is crossed, and since the lower threshold was previously crossed, an

alarm is detected.

Event group

The operating specifications for the event group are shown below.

1. Use the **rmon event** command to make settings.
2. The following operations can be specified for the event group.
    - Record to log
    - Send SNMP trap
    - Record to log and send SNMP trap
3. If trap transmission is specified, the following SNMP commands must be set in order to transmit the SNMP trap.
    - **snmp-server host**
    - **snmp-server enable trap rmon**
4. The following operations will be carried out when specifying trap transmission.
    - SNMPv1、SNMPv2c
        - Only the traps for which the community name specified using the **rmon event** command, and for which the community name specified by the **snmp-server host** command are matching will be transmitted.
    - SNMPv3
        - Only the traps for which the community name specified using the **rmon event** command, and for which the user name specified by the **snmp-server host** command are matching will be transmitted.
5. The supported OIDs in the event group are as follows.

```
rmon(1.3.6.1.2.1.16)
 +- event(1.3.6.1.2.1.16.9)
     +- eventTable(1.3.6.1.2.1.16.9.1)
             + eventEntry(1.3.6.1.2.1.16.9.1.1) { eventIndex }
                 +- eventIndex(1.3.6.1.2.1.16.9.1.1.1)       (read-only)
                 +- eventDescription(1.3.6.1.2.1.16.9.1.1.2)  (read-create)
                 |Event description
                 +- eventType(1.3.6.1.2.1.16.9.1.1.3)        (read-create)
                 |Event type
                 +- eventCommunity(1.3.6.1.2.1.16.9.1.1.4)   (read-create)
                 |Community name
                 +- eventLastTimeSent(1.3.6.1.2.1.16.9.1.1.5) (read-only)
                 |Event execution time
                 +- eventOwner(1.3.6.1.2.1.16.9.1.1.6)       (read-create)
                 |Name of owner
                 +- eventStatus(1.3.6.1.2.1.16.9.1.1.7)      (read-create)
                       Event group status
```

Setting by SetRequest from an SNMP manager

The same content as the commands of each group can be specified by using SetRequest from an SNMP manager.
The procedure for making settings from an SNMP manager is as follows.

As an example, we explain how to make new settings for the Ethernet statistics information (etherStatsTable)

group to port1.1 using index number 1.
Similar operations can be used to make settings for a supported MIB on other groups.

1. Make SNMP settings to allow the MIB to be written.
   For details, refer to **SNMP**.
2. For etherStatsStatus.1, specify “2” (createRequest).
   The “.1” of etherStatsStatus.1 is the etherStatsTable index.
3. For etherStatsDataSource.1, specify ifIndex.5001 as the interface to be monitored.
   ifIndex.5001 indicates port1.1.
4. Specifying “owner” is optional, but if you do, specify the text string in etherStatsOwner.1.
5. For etherStatsStatus, specify “1” (valid).

When you perform the above steps, the following commands are specified for port1.1.
We assume that “RMON” was set as the “owner” setting.

```
rmon statistics 1 owner RMON
```

Below we show how to disable the RMON function system-wide from the SNMP manager.

1. Make SNMP settings to allow the MIB to be written.
   For details, refer to **SNMP**.
2. For ysrmonSetting(1.3.6.1.4.1.1182.3.7.1), specify “2” (disabled).

When you perform the above steps, the following commands are specified.

```
rmon disable
```

To specify enable, set ysrmonSetting(1.3.6.1.4.1.1182.3.7.1) to “1” (enabled).

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Enable the RMON function	rmon
Set RMON Ethernet statistics group	rmon statistics
Set RMON history group	rmon history
Set RMON event group	rmon event
Set RMON alarm group	rmon alarm
Show RMON function status	show rmon
Show RMON Ethernet statistics group status	show rmon statistics
Show RMON history group status	show rmon history
Show RMON event group status	show rmon event

Operations	Operating commands
Show RMON alarm group status	show rmon alarm
Clear RMON Ethernet statistics group counters	rmon clear counters

Examples of Command Execution

Setting an Ethernet statistics group

Make Ethernet statistics group settings for port 1.1, and from the SNMP manager, retrieve the MIB of the Ethernet statistical information group.

■ Setting Procedure

1. Enable the Ethernet statistics group setting for port1.1.
   The index of the Ethernet statistics group is “1.”

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

   ① Enable the Ethernet statistics group settings

2. From the SNMP manager, make SNMP settings that the MIB of the Ethernet statistics group can be retrieved.
   In this example, we use “private” access on SNMPv1 or SNMPv2c.

```
Yamaha(config)#snmp-server community private rw ①
```

   ① Set the readable/writable community name as “private”.

3. From the SNMP manger, it will be possible to retrieve the etherStatsTable(.1.3.6.1.2.1.16.1.1) with the community name “private.”

Setting a history group

Make settings for the history group of port1.1 and retrieve the MIB of the history group from the SNMP manager.

■ Setting Procedure

1. Enable the port1.1 history group setting.
   The index of the history group is “1.”

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

   ① Enable the history group settings

2. From the SNMP manager, make SNMP settings that the MIB of the history group can be retrieved.
   In this example, we use “private” access on SNMPv1 or SNMPv2c.

```
Yamaha(config)#snmp-server community private rw ①
```

① Set the readable/writable community name as “private”.

3. From the SNMP manger, it will be possible to retrieve the etherHistoryTable(.1.3.6.1.2.1.16.2.2) with the community name “private.”

Setting an alarm event group

Use the alarm group to monitor the statistical information values of the Ethernet statistics group.
The conditions for monitoring are as follows.

- The MIB to be monitored is port1.1’s etherStatsPkts(.1.3.6.1.2.1.16.1.1.1.5).
- The sampling interval is 180 seconds.
- The sampling type is delta.
- The upper threshold value is 2000.
- The lower threshold value is 1000.

When the above monitoring conditions are matched, the following event group is executed.

- Record to log and send SNMP trap
- Community name is “RMON”

■ Setting Procedure

1. Make the required settings for SNMP trap transmission.

```
Yamaha(config)#snmp-server host 192.168.100.3 traps version 2c RMON ①
Yamaha(config)#snmp-server enable trap rmon ②
```

① Set the trap destination

② Enable transmission of traps for the RMON function

2. Make event group settings.
The index of the event group is “1.”

```
Yamaha(config)#rmon event 1 log-trap RMON ①
```

① Enable the event group settings

3. In order to set the alarm group’s monitoring target MIB object, enable the port1.1 Ethernet statistics group setting.
The index of the Ethernet statistics group is “1.”

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

① Enable the Ethernet statistics group settings

4. Set the alarm group with the listed conditions.
The index of the alarm group is “1.”

```
Yamaha(config)#rmon alarm 1 etherStatsPkts.1 interval 180 delta rising-threshold 3000
```

```
event 1 falling-threshold 2000 event 1 ①
```

① Enable an alarm group

Points of Caution

None

Related Documentation

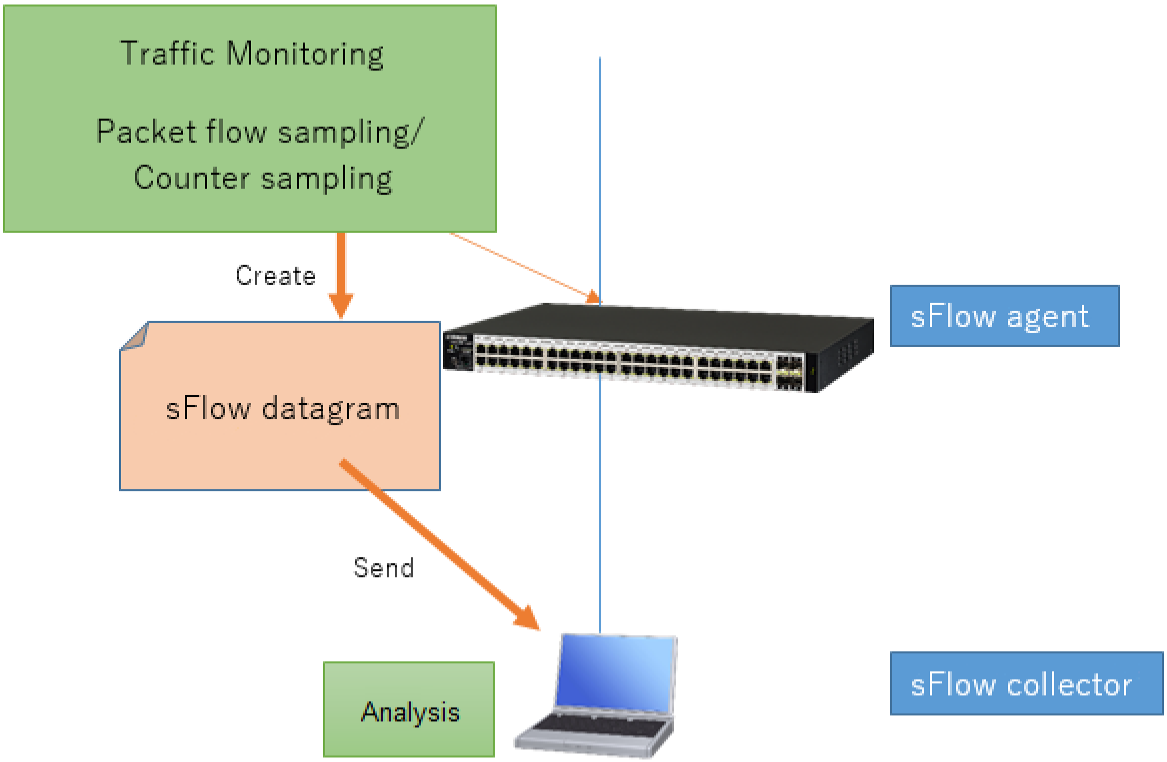
- Maintenance and Operation Functions: SNMP

sFlow

Function Overview

sFlow is technology for monitoring traffic.
Rather than monitoring all packets in traffic flow, sFlow can monitor traffic information statistically based on sampling only a specific percent of packets.

sFlow monitoring is configured with sFlow agents and sFlow collectors.



- sFlow agent
    - Monitors traffic by sampling and creates sFlow information.
    - Sends sFlow datagrams, which store sFlow information, to the sFlow collector.
- sFlow collector
    - Receives sFlow datagrams, which store sFlow information, sent from the sFlow agent.
    - Collects and analyzes the sFlow information from datagrams indicated above.

sFlow agents can perform two types of sFlow sampling.
Either one or both of the following types of information is stored in sFlow datagrams.

- Packet flow sampling
    - This samples a specified percent of packets sent and received at the interface.
- Counter sampling
    - This samples data from the interface counter at regular intervals.

This product functions as an sFlow agent.
The sFlow collector must be supplied separately.

This product is compatible with sFlow Version 5 (https://sflow.org/sflow_version_5.txt).

Definition of Terms Used

sFlow agent

After monitoring traffic by sampling and creating sFlow information, the sFlow agent sends the sFlow information to an sFlow collector.
This product functions as an sFlow agent.

sFlow collector

The sFlow collector collects and analyzes the sFlow information received from sFlow agents.

Packet flow sampling

This sampling method samples a specific percent of the total packets sent and received at the interface.

Counter sampling

This sampling method obtains interface counter values at regular intervals.

sFlow datagram

sFlow datagrams are UDP packets that store the information sFlow agents obtain by sampling.
They are sent from sFlow agents to sFlow collectors.

Function Details

The operating specifications for sFlow functionality are indicated below.

1. Use the **sflow enable** command to enable sFlow functionality.
    - The default setting is **sflow disable** (disabled).
2. Use the **sflow agent** command to specify the following sFlow agent settings.
    - IP address
        - IPv4 address
        - IPv6 address
    - The IP address specified using this command is used in the sFlow header of sFlow datagrams.
    - No setting is specified in default settings.
3. Use the **sflow collector** command to specify the following sFlow collector settings.
    - IP address
        - IPv4 address
        - IPv6 address
    - UDP port number
        - The default value is 6343.
    - sFlow datagrams are sent to the IP address and UDP port number specified using this command.
    - No setting is specified in default settings.
    - Only one sFlow collector can be specified for this product.
    - Sampling is not started unless this command is specified.
4. Packet flow sampling operations are described below.
    - The **sflow sampling-rate** command is used to specify the sampling rate at physical ports and sample packet flow at the corresponding ports.

        - No setting is specified in default settings.
    - The sampling rate is specified as the number of packets from which one packet is sampled.
        - For example, for a sampling rate setting of 1000, one packet is sampled from each 1000 packets that are sent or received at the corresponding port.
    - Sent and received packets are sampled separately.
    - Packets are individually sampled at each port.
    - Use the **sflow max-header-size** command to specify the maximum header size value for Ethernet frames being sampled during packet flow sampling.
        - The default value is 128.
    - Specifying the sampling rate using the **sflow sampling-rate** command results in the following actions.
        - The new sampling rate will be applied after sampling at the previous sampling rate setting is finished.

5. Counter sampling actions are described below.
    - If the **sflow polling-interval** command is used to specify the polling interval for a physical port, counter sampling is performed at that port.
        - No setting is specified in default settings.
    - The polling interval setting specifies the number of seconds between counter sampling.
        - For example, if a polling interval value of 30 is specified, counter information for the corresponding port is sampled once every 30 seconds.
    - Packets are individually sampled at each port.
6. This product sends the following types of sFlow datagrams.
    - Use the **sflow collector max-datagram-size** command to specify the maximum sFlow datagram size.
    - sFlow datagrams from packet flow sampling store the following information for sFlow version 5.
        - Raw Packet Header(enterprise = 0, format = 1)
    - sFlow datagrams from counter sampling store the following information for sFlow version 5.
        - Generic Interface Counters(enterprise = 0, format = 1)
        - Ethernet Interface Counters(enterprise = 0, format = 2)
        - Disabled counters include a maximum counter value. (For 32-bit counters, sFlow datagrams store the “0xFFFFFFFF” value.)

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Enables sFlow functionality	sflow
Sets sFlow agents	sflow agent
Sets sFlow collectors	sflow collector
Sets the maximum sFlow datagram size	sflow collector max-datagram-size
Sets the sampling rate for packet flow sampling	sflow sampling-rate
Sets the maximum Ethernet frame header size for packet flow sampling	sflow max-header-size

Operations	Operating commands
Sets the polling interval for counter sampling	sflow polling-interval
Displays the sFlow status	show sflow
Displays the sFlow sampling information	show sflow sampling

Examples of Command Execution

The following samples packets by sFlow packet flow sampling and counter sampling at port 1.1.

1. Set the IP address for the sFlow agent.

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

2. Set the IP address for the sFlow collector.

```
Yamaha(config)#sflow collector 192.168.100.2
```

3. Set the sampling rate for packet flow sampling at the applicable port.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#sflow sampling-rate 1000
```

4. Set the polling interval for counter sampling at the applicable port.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#sflow polling-interval 30
```

5. Enable sFlow.

```
Yamaha(config)#sflow enable
```

Points of Caution

- sFlow is not compatible with management information bases (MIB).
- In stack configurations, the show sflow sampling command does not synchronize sampling information between the main and member switches in the stack.
- In environments with high communication volumes, the following might occur if a small value is specified for the **sflow sampling-rate** command. In such cases, consider changing the **sflow sampling-rate** command value.
    - Higher CPU usage rate values are displayed using the **show environment** command.
    - The “sFlow Drop Sampling Count” value displayed by the **show sflow** command is included in count values.
        - If that value is counted, packets sampled by packet flow sampling dropped because they cannot be processed due to the high load. (* The sampling is actually dropped in this case, not the packets themselves.)

- Since the values vary depending on the number of sampling-target ports and whether or not other functions are operating, recommended values cannot simply be suggested. However, as a guideline, the **sflow sampling-rate** command values that are unlikely to cause sFlow drops even when all ports are in use are described below.
    - When using a 1G interface … 2000 (1/2000)
    - When using a 10G interface … 10000 (1/10000)

Related Documentation

None

SYSLOG

Function Overview

This product provides the SYSLOG functions shown below as a means to ascertain the operating state.

1. Functions to collect, reference, and delete the log that is accumulated inside this product
2. Functions for output to the console simultaneously with logging
3. Functions for transmitting to a previously-registered notification destination (SYSLOG server) simultaneously with logging

Logging, output to console, and notifications to the SYSLOG server are performed according to the output level specified by the user. Processing occurs only for the permitted messages.
Logging occurs in RAM, and is automatically backed up to flash ROM or can be backed up manually.
When backing up manually, you can also back up to an SD card at the same time.
Notifications to the SYSLOG server are done simultaneously with logging, but only if a SYSLOG server has been registered.

Definition of Terms Used

None

Function Details

The SYSLOG function is described below.

1. Logging occurs in RAM, and can accumulate up to 10,000 items.
   Backup to Flash ROM can be performed by the following means.
   - Automatic backup performed every hour since system boot
   - Manual backup performed by the **save logging** command
   - Backup performed when the **write** command is executed successfully
2. The accumulated logs can be viewed by the **show logging** command.
   It can also be deleted by the **clear logging** command.
   The **show logging** command shows the information in RAM.
   The log information for this product is based on the premise that the information in RAM and flash ROM always matches.
   (When the system starts, the log information in flash ROM is applied to RAM, and the service is started.
   The log information in RAM is not deleted following execution of a backup.)
3. Log transmission occurs only if the notification destination (SYSLOG server) has been registered.
   You can use the **logging host** command to register up to two notification destinations.
   Specify the notification destination either by IP address or FQDN.
   As the port number of the notification destination, the default port number 514 is used. (This setting cannot be freely set by the user.)
   The **logging facility** command can be used to specify the facility value of log notifications. The factory default setting is local0(16).
   The **logging format** command can be used to change the format of log notifications to not include the header portion (timestamp and hostname). The following are log examples.
   - Without the format specified (no logging format)

```
<134>Jan  1 00:00:00 Yamaha [     IMI]:inf: Configuration file is saved in
```

```
"config0"
```

- With the format specified (logging format legacy)

```
<134>[     IMI]:inf: Configuration file is saved in "config0"
```

4. The level of log that is transmitted (SYSLOG priority) can be set using the **logging trap** command.
   This product allows you to enable or disable output for each level of log.
   With the factory settings, the output-level enables only Information and Error.

5. The **logging backup sd** command enables SYSLOG backup to the SD card.
   If SYSLOG backup to the SD card is enabled, executing the **save logging** command will save the dated log file to the SD card.

List of related commands

Related commands are indicated below.
For details, refer to the Command Reference.

Function name	Command name
Set log output level	logging trap
Set log console output	logging stdout
Set log notification destination (SYSLOG server)	logging host
Change the log notification format	logging format
Back up log	save logging
Clear log	clear logging
Show log	show logging
Set SD card backup of log	logging backup sd
Set the logging facility value	logging facility

Examples of Command Settings

1. Enable debug-level log output, and start log output to the SYSLOG server (192.168.1.100) with a facility value of 10.
   Also output informational-level log to the console.

```
Yamaha(config)# logging trap debug ①
Yamaha(config)# logging facility 10 ②
Yamaha(config)# logging host 192.168.1.100 ③
Yamaha(config)# logging stdout info ④
```

① Enable the debug-level log output

② Set the facility value to 10

③ Register a SYSLOG server

④ Output an informational-level log to the console

2. Stop notifications to the SYSLOG server.

```
Yamaha(config)# no logging host
```

3. Save and show the accumulated log information.

```
Yamaha# save logging ①
Yamaha# show logging ②
2018/03/08 20:42:46: [ SESSION]:inf: Login succeeded as (noname) for HTTP: 192.168.1.40
2018/03/09 10:06:42: [     NSM]:inf: Interface port1.11 changed state to down
2018/03/09 10:09:48: [ SESSION]:inf: Logout timer expired as (noname) from HTTP:
192.168.1.40
2018/03/09 16:19:36: [     NSM]:inf: Interface port1.17 changed state to up
 :
```

① Save the log in RAM to ROM

② Show the accumulated logs

4. Clear the accumulated log information.

```
Yamaha# clear logging ①
Yamaha# show logging ②
 ③
```

① Clear all accumulated logs

② Show the logs

③ Nothing is shown because they have been erased

Points of Caution

None

Related Documentation

None

Firmware Update

Function Overview

This product offers the following two firmware update functions, in order to correct problems in the program and to add new functionality.

1. Firmware updates can be transmitted and applied to this product from a remote terminal such as a computer.
2. This product's built-in HTTP client can access an HTTP server, to download and apply the latest firmware.
3. A firmware update placed on the SD card can be applied to this product.

These update functions can be used to upgrade or downgrade the version of firmware used on this product.
During firmware updating, **all port LEDs flash green**, regardless of the LED display mode setting.

When a stack is configured, the updated firmware is written simultaneously to the stack main and member switches.
When successfully finished writing the updated firmware, the **system is automatically rebooted in order to apply the new firmware**.
For instructions on how to specify rebooting the system, refer to **Reboot after writing**.

Definition of Terms Used

None

Function Details

Update by transmitting the firmware update

This function transmits firmware updates to this product from a remote terminal, such as a computer, and applies it as boot firmware.
The update process is executed using a **TFTP client** or the **Web GUI**.

Using a TFTP client to update the firmware

Firmware can be updated by using a **TFTP client** installed on a computer or other remote terminal to transmit the updated firmware to this device.
In order to operate this product's TFTP server, use the steps shown below to set up a network environment that allows remote access.

1. Decide on the VLAN that will be used for maintenance.
2. Set the IPv4 address on the maintenance VLAN. Set it using the **ip address** command.
3. Permit access from the maintenance VLAN to the TFTP server. Use the **tftp-server interface** command or the **management interface** command to specify that setting.
4. Enable the TFTP server. Enable the server using the **tftp-server enable** command.

Follow the rules below when sending the firmware update using the TFTP client.

- Set the transmission mode to "**binary mode**".
- As shown in the table below, specify the remote path to which the firmware update is sent.
- Specify the administrative password in the form "/PASSWORD" at the end of the remote path.
  However, the firmware update cannot be applied if the administrative password is still set to the default setting. The administrative password setting must be changed in advance.

When updating firmware that uses TFTP clients, the following three types of updates are possible.

- Updated firmware

Type	Remote path
Internal firmware	exec

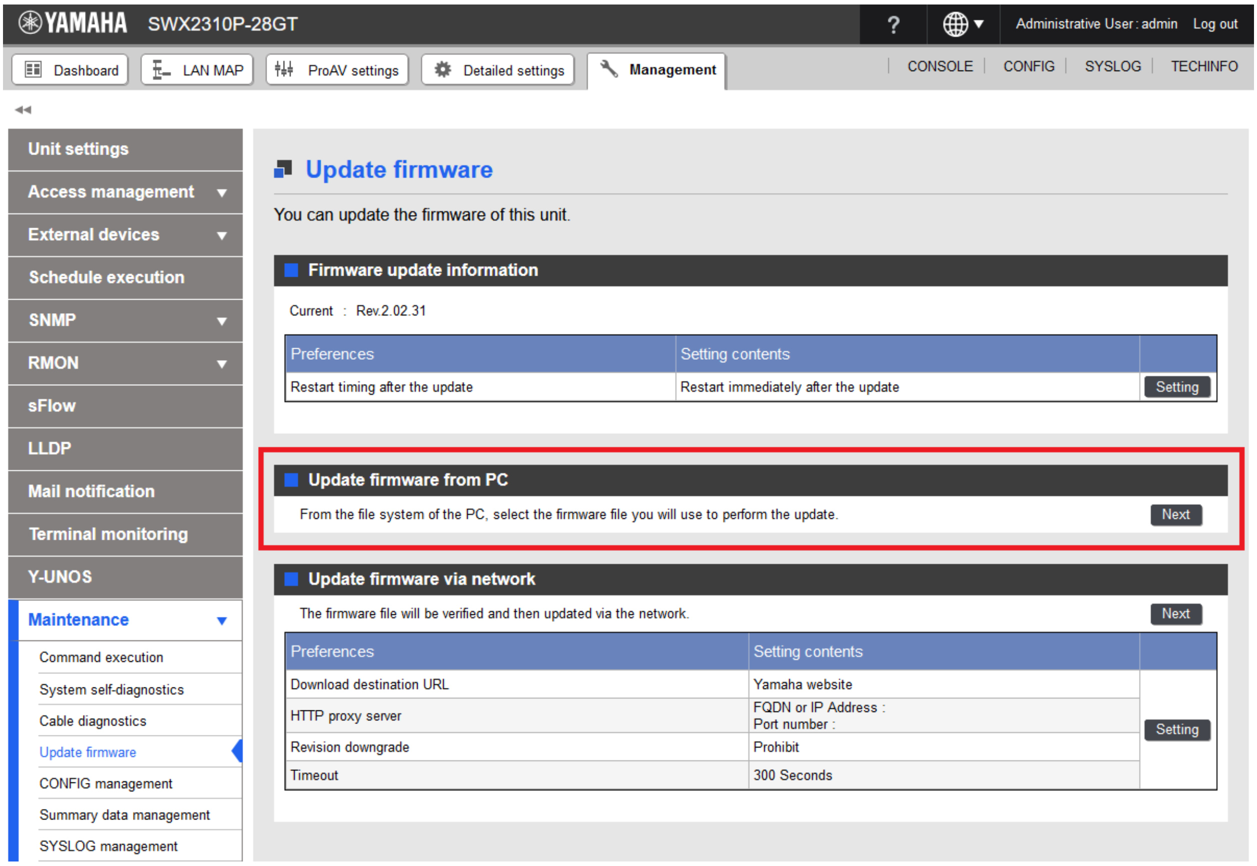
If there is no problem with the firmware update that was sent, the firmware update will be saved.

Updating the firmware by specifying a local file in the Web GUI

Specify the firmware update located on the terminal accessing the Web GUI, and apply it to this product. This function does not do a version comparison with the existing firmware, and will overwrite the specified firmware regardless of version.

To update firmware by specifying a local file, click **[Maintenance] - [Firmware update]** in the Web GUI on the computer. (Refer to the part shown in a red frame on the screenshot below.)
Refer to the help contents within the GUI for the specific operation method.

- Initial screen on the Web GUI for updating firmware using a computer



Update firmware

You can update the firmware of this unit.

Firmware update information

Current : Rev.2.02.31

Preferences	Setting contents	
Restart timing after the update	Restart immediately after the update	Setting

Update firmware from PC

From the file system of the PC, select the firmware file you will use to perform the update. Next

Update firmware via network

The firmware file will be verified and then updated via the network. Next

Preferences	Setting contents	
Download destination URL	Yamaha website	Setting
HTTP proxy server	FQDN or IP Address : Port number :	
Revision downgrade	Prohibit	
Timeout	300 Seconds	

Using an HTTP client to update the firmware

This method of firmware update uses an HTTP client to obtain the firmware update from a specified URL, and then apply it to this product.
This function assumes that the firmware version will be upgraded. Downgrading to a previous version will only be permitted if “revision-down” is allowed.
The firmware cannot be rewritten with the same version of firmware.
This function cannot be used when the stack is enabled.
An HTTP client can be used to update the firmware using the methods below.

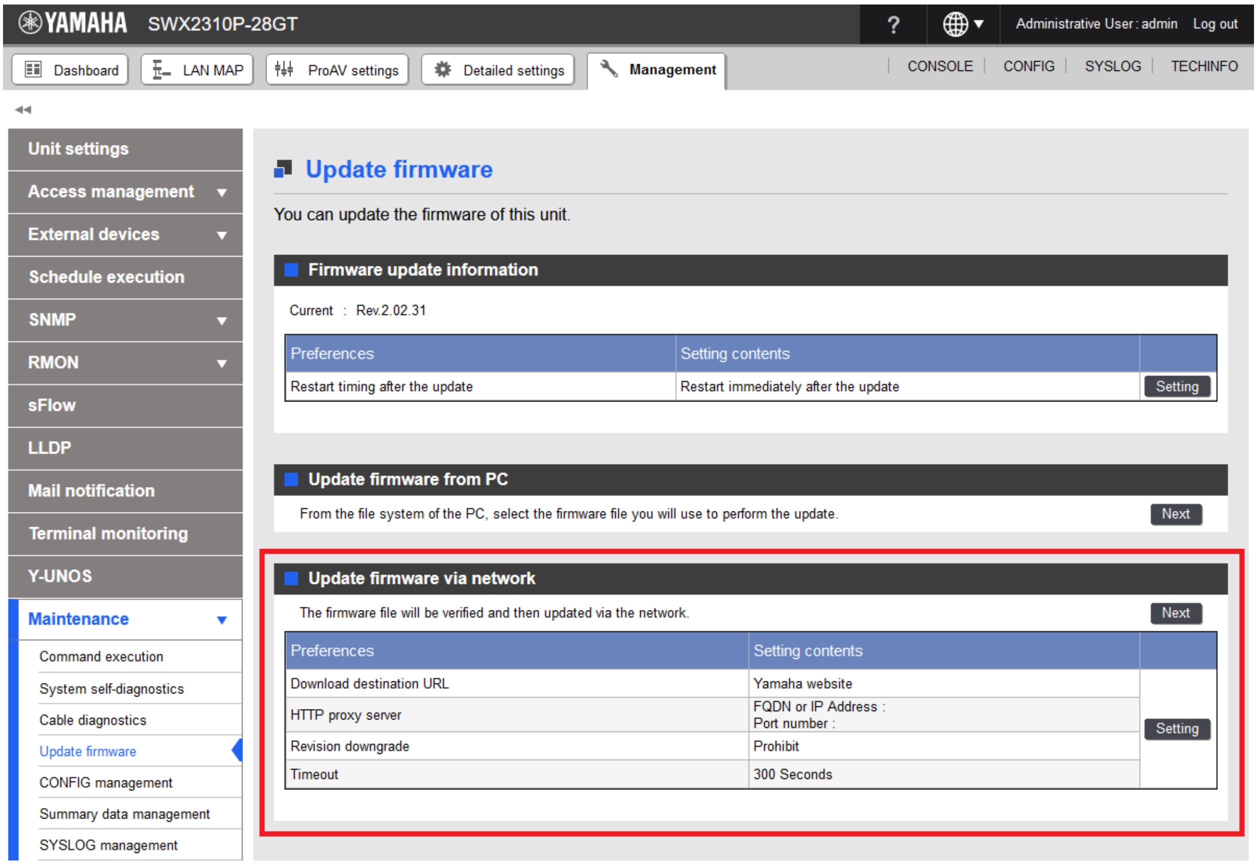
- Use the **firmware-update** command in the CLI (command-line interface).
- Execute **update firmware via network** in the Web GUI.

Updating the firmware with an HTTP client is done by using the settings value shown in the table below.

Setting parameter	Explanation
Download source URL	Sets the source URL from which the firmware is downloaded. A URL of up to 255 characters in length can be set. The input format is “\http://IPv4/IPv6 address of the server” or “\http://hostname/path name”. If an IPv6 address is specified, it must be enclosed in square brackets like “[IPv6 address]”. If the server port number is other than 80, it must be specified within the URL in the form “\http://IP address of the server:port number/path name” or “\http://hostname:port number/path name”. Default value settings are specified in the following location. http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2310p.bin
Proxy Server URL	Specifies the proxy server to use for updating firmware. Specify it either as an IPv4/IPv6 address or FQDN. FQDNs can be up to 255 characters long. No proxy server is specified in default settings. Proxy servers must be specified as an IPv4/IPv6 address or in the form “\http://hostname/path name port number”. If an IPv6 address is specified, it must be enclosed in square brackets like “[IPv6 address]”.
Permit downward revision	Sets whether the current version of firmware can be downgraded to a previous version. The default value is “Don’t allow”. Overwriting the firmware with the same version of firmware is not permitted.
Timeout	Specifies the timer for monitoring the completion of the processes shown below. * Version check of old and new firmware * The download monitoring timer from the specified URL can be specified from **100 seconds to 86,400 seconds**, and the initial setting is set to **300 seconds**.

For instructions on using the **firmware-update** command, refer to “**Examples of Command Execution**” or the “**Command Reference**”.
To **update firmware over the network** using the Web GUI, execute **[Maintenance] - [Firmware update]** on the Web GUI. (Refer to the part shown in a red frame on the screenshot below.)
Refer to the help contents within the GUI for the specific operation method.

- Initial Web GUI Screen for Updating Firmware via the Network



Update firmware

You can update the firmware of this unit.

Firmware update information

Current : Rev.2.02.31

Preferences	Setting contents	
Restart timing after the update	Restart immediately after the update	Setting

Update firmware from PC

From the file system of the PC, select the firmware file you will use to perform the update. Next

Update firmware via network

The firmware file will be verified and then updated via the network. Next

Preferences	Setting contents	
Download destination URL	Yamaha website	Setting
HTTP proxy server	FQDN or IP Address : Port number :	
Revision downgrade	Prohibit	
Timeout	300 Seconds	

Update using an SD card

The firmware stored on the SD card inserted in the unit will be applied as the updated firmware.
This update is performed from the CLI (Command-line interface) using the **firmware-update sd execute** command.
If a stack was configured, commands can only be executed from the main switch in the stack.
After entering the firmware update confirmation, the update will continue even if the SD card is removed. To unmount the SD card when executing the command, enter “N” in the confirmation of continued SD card mounting status, or specify the “sd-unmount” option with the command.
If the system is rebooted with the SD card inserted in the main unit, the system will be booted using the firmware in the SD card, as specified by the **boot prioritize sd** command.

- File path in SD card /swx2310p/firmware/swx2310p.bin

Reboot after writing

When successfully finished writing the firmware update, the system is automatically rebooted.
However, the system is not rebooted if the “no-reboot” option is specified for **firmware-update execute** or **firmware-update sd execute** commands.
If the **firmware-update reload-time** command is specified without specifying the “no-reboot” option, then the system is rebooted according to the reboot time setting.
The revision after the next reboot can be confirmed by executing the **show firmware-update** command.

If a stack is configured, the firmware update method can be selected using the **firmware-update reload-method** command.

- How to simultaneously update member switches in a configuration
- How to update without stopping network services

For an operation overview of the firmware update methods, refer to **Firmware Update in the stack public technical data**.

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Set firmware update site	firmware-update url
Set proxy server	firmware-update http-proxy
Execute firmware update	firmware-update execute
Set firmware download timeout duration	firmware-update timeout
Permit downward revision	firmware-update revision-down
Show firmware update function settings	show firmware-update
Execute firmware update from SD card	firmware-update sd execute
Set firmware update reboot time	firmware-update reload-time
Set the firmware update restart method during stack configuration	firmware-update reload-method

Examples of Command Execution

Using an HTTP client to update the firmware

In this example, the firmware update is stored on the local HTTP server, and this product is set to manage the firmware in order to perform the update.

- Change the download URL to **http://192.168.100.1/swx2310p.bin**.
- The downward revision setting is left **disabled**.
- The timeout value is left at **300 sec**.
- A reboot time is not specified, but the system is **rebooted immediately after updates**.

1. The download URL is changed, and the firmware update settings are confirmed.

```
Yamaha(config)#firmware-update url http://192.168.100.1/swx3210p.bin ①
Yamaha(config)#exit
Yamaha#show firmware-update ②
url:http://192.168.100.1/swx2310p.bin
http-proxy: -
timeout: 300 (seconds)
revision-down: Disable
firmware revision for next boot: -
reload-time: -
reload-method: Normal
```

① Set download source URL

② Show firmware update function settings

2. The firmware update is executed.

```
Yamaha#firmware-update execute ①
Found the new revision firmware
```

```
Current Revision: Rev.2.02.01
New Revision:     Rev.2.02.03
Downloading...
Update to this firmware? (y/n)y ②
Updating...
Finish

③
```

① Execute firmware update

② Enter y

③ The system automatically reboots

3. Pressing “CTRL+C” during the firmware update process will interrupt the update.

```
Yamaha#firmware-update execute
Found the new revision firmware
Current Revision: Rev.2.02.01
New Revision:     Rev.2.02.03
Downloading... ①
^CCanceled the firmware download
```

① Press the Ctrl and C keys

Using an HTTP client to update the firmware (in a proxy server environment)

This updates the firmware by specifying a proxy server.

- The **initial** download URL setting is left unchanged.
- The proxy server is set to **http://192.168.100.1:8080**.
- The downward revision setting is left **disabled**.
- The timeout value is left at **300 sec**.
- A reboot time is not specified, but the system is **rebooted immediately after updates**.

1. Specify the HTTP proxy settings and confirm the firmware update settings.

```
Yamaha(config)#firmware-update http-proxy http://192.168.100.1 8080 ①
Yamaha(config)#exit
Yamaha#show firmware-update ②
url: http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx3220.bin
http-proxy: http://192.168.100.1:8080
timeout: 300 (seconds)
revision-down: Disable
firmware revision for next boot: -
reload-time: -
reload-method: Normal
```

① Set HTTP proxy

② Show firmware update function settings

2. The firmware update is executed.

```
Yamaha#firmware-update execute ①
Found the new revision firmware
Current Revision: Rev.2.02.01
New Revision:     Rev.2.02.03
Downloading...
Update to this firmware? (y/n)y ②
Updating...
Finish

③
```

① Execute firmware update

② Enter y

③ The system automatically reboots

Update using an SD card

In this example, the firmware update is placed on an SD card inserted in the unit, and this product is set to manage the firmware in order to perform the update.
This is an example of a two-stack configuration.

- Change the reboot time to **23:30**.
- Change the reboot method to **reboot the stack main and member switches sequentially**.

1. Change the reboot time and reboot method.

```
Yamaha(config)#firmware-update reload-time 23 30 ①
Yamaha(config)#firmware-update reload-method sequential ②
Yamaha(config)#exit
```

① Set the reboot time

② Set the reboot method

2. Insert the SD card into the main switch in the stack and execute the firmware update.

```
Yamaha#firmware-update sd execute ①
Update the firmware.
Current Revision: Rev.2.02.01
New Revision:     Rev.2.02.03

Update to this firmware? (y/n)y ②
Continue without unmounting the SD card? (y/n)n ③
Unmounted the SD card.  Pull out the SD card.
Updating...
Finish
Yamaha#
(Reboots at specified reboot time)
```

① Execute firmware update

② Enter y

③ Enter n

3. The stack member firmware is updated at the same time as the stack main switch, but the members are rebooted after the firmware in the stack main switch has been rebooted.
   The following log history is displayed on stack member consoles.

```
    (Press ENTER on the stack main. The firmware is received and the update
starts.)
    Receiving exec file...
    Testing received file...
    Writing to Nonvolatile memory...
    Done.

    (Wait for restart of stack main then reboot)
```

4. After checking the version of the update firmware, you can enter “n” to cancel.

```
    Yamaha#firmware-update sd execute ①
    Update the firmware.
    Current Revision: Rev.2.02.01
    New Revision:     Rev.2.02.03

    Update to this firmware? (y/n)n ②
    Yamaha#
```

① Execute firmware update

② Enter n

Points of Caution

If the system is rebooted or the power is turned off during firmware update, the update will be interrupted and the system will start with the firmware before the update operation.

Related Documentation

- Maintenance and Operation Functions: LED Control

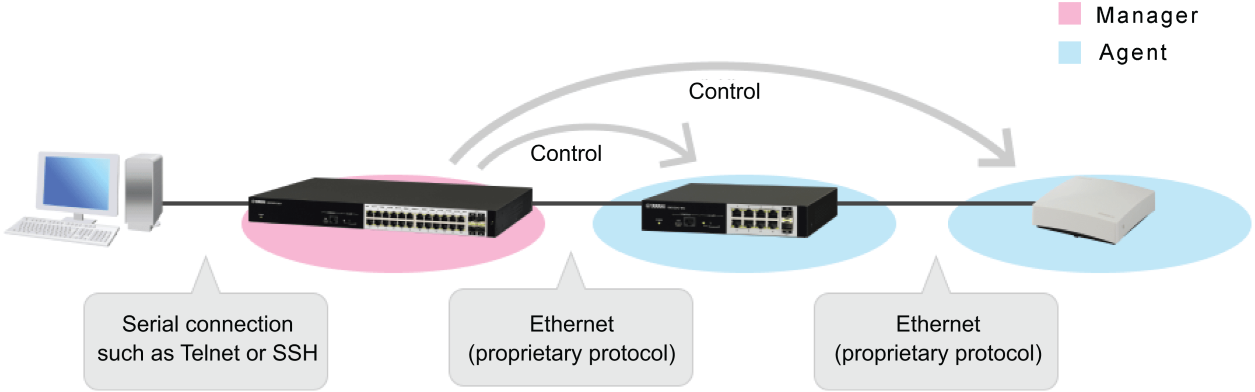
L2MS (Layer2 Management Service)

Function Overview

L2MS (Layer2 Management Service) is functionality for managing Yamaha network devices at the layer 2 level.
L2MS consists of one L2MS manager unit (referred to as “manager” below) that performs centralized management and multiple L2MS agent units (referred to as “agents” below) that are controlled from the manager.
Devices can be used as either a manager or agent.

The following illustrates how to connect the computer, manager, and agents.

- L2MS connection method


Manager
Agent
Control
Control
Serial connection such as Telnet or SSH
Ethernet (proprietary protocol)
Ethernet (proprietary protocol)

Connect the computer to the manager via a serial connection or log in via Telnet or HTTP/HTTPS.
The manager includes commands for managing the agents and a web GUI for specifying the settings or checking the status of agents. These can be used to operate the agents.
The manager is connected to agents via Ethernet cables and uses a proprietary protocol (L2MS) for communication.

This functionality has the following characteristics.

- Initial settings are not required
  Although IP addresses must be specified if using Telnet or SSH, initial settings do not need to be specified for agents, because the functionality uses a proprietary protocol (L2MS) for communication.
  When Ethernet cables are connected, the manager automatically recognizes subordinate agents.
- Multiple supported terminals can be controlled simultaneously
  The manager can recognize and control multiple agents simultaneously.

The proprietary communication protocol used by L2MS is the same protocol as used for communication by the switch control functionality supported by Yamaha routers and SWX series and WLX series.
That means both SWX series and WLX series devices can be managed from the manager.

Definition of Terms Used

Manager

A manager is a device that manages Yamaha network devices functioning as an agent based on L2MS and switch control functionality.
It manages Yamaha network switches and Yamaha wireless access points within the network.

Agent

A Yamaha network switch or Yamaha wireless access point that is managed by a manager based on L2MS and switch control functionality.

Settings can be checked or changed from the manager.

Function Details

Compatible models

Devices can be used as either an L2MS manager or agent.

If operating as a manager, each manager can control a **maximum of 128** agent units.
The following models can be managed as an agent.
As described earlier, any device that supports switch control functionality (agents) can also be controlled.

- SWX2100 series (SWX2100-8G, SWX2100-16G, SWX2100-24G, SWX2100-5PoE, SWX2100-10PoE)
- SWX2110 series (SWX2110-5G, SWX2110-8G, SWX2110-16G)
- SWX2110P series (SWX2110P-8G)
- SWX2200 series (SWX2200-8G, SWX2200-24G, SWX2200-8PoE)
- SWX2210 series (SWX2210-8G, SWX2210-16G, SWX2210-24G)
- SWX2210P series (SWX2210P-10G, SWX2210P-18G, SWX2210P-28G)
- SWX2220 series (SWX2220-10NT, SWX2220-18NT, SWX2220-26NT)
- SWX2221P series (SWX2221P-10NT)
- SWX2220P series (SWX2220P-18NT, SWX2220P-26NT)
- SWX2300 series (SWX2300-8G, SWX2300-16G, SWX2300-24G)
- SWX2310 series (SWX2310-10G, SWX2310-18GT, SWX2310-28GT, SWX2310-52GT)
- SWX2310P series (SWX2310P-10G, SWX2310P-18G, SWX2310P-28GT)
- SWX2320 series (SWX2320-16MT)
- SWX2322P series (SWX2322P-16MT)
- SWX3100 series (SWX3100-10G, SWX3100-18GT)
- SWX3200 series (SWX3200-28GT, SWX3200-52GT)
- SWX3220 series (SWX3220-16MT, SWX3220-16TMs)
- WLX series (WLX202, WLX212, WLX222, WLX302, WLX313, WLX322, WLX323, WLX402, WLX413)

If operated as an agent, the unit is managed by the Yamaha router or Yamaha network switch manager.
For details about compatible Yamaha router models, refer to Switch control functionality of Yamaha routers.

Usage

The L2MS operation and role are set by the **l2ms** command.

- In the case of L2MS managers
  L2MS managers manage the SWX and WLX series switches operating as agents.
  The **terminal-watch enable** command can be used to periodically acquire and monitor information about computers and other terminals present in the network.

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#l2ms enable
Yamaha(config-l2ms)#l2ms role manager
Yamaha(config-l2ms)#terminal-watch enable
```

- In the case of L2MS agents
  The unit is managed by the Yamaha router or Yamaha network switch operating as a manager.

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#l2ms enable
Yamaha(config-l2ms)#l2ms role agent
```

The **show l2ms** command can be used to check a current action and role of the agents.

L2MS protocol

L2MS control is performed using the proprietary protocol L2 frames indicated below.

- Content of L2MS Protocol L2 Frames

Item	Value
Destination MAC	01:a0:de:00:e8:12 to 01:a0:de:00:e8:15
Ethertype	0xe812, 0xe813

If a firewall is specified between the manager and agents, the firewall settings must allow these L2 frames to pass through.

Monitoring agents

Managers monitor subordinate agents by sending query frames at regular intervals.
Agents respond to query frames by sending a response frame to notify the manager that they exist.

The interval between sending query frames is specified using the **agent-watch interval** command.
Increasing the setting value will decrease the sending frequency, but will lengthen the time for the manager to recognize an agent after it is contacted.
Decreasing the setting value will, conversely, increase the sending frequency, but shorten the time for the manager to recognize an agent after it is contacted.

If the manager does not receive a response frame from an agent after sending the specified number of query frames, the manager will decide that the corresponding agent has gone down.
The number of attempts is specified by the **agent-watch down-count** command.
If the Ethernet cable connected to the agent is disconnected, in some cases the manager might decide that the agent has gone down sooner than specified by the command.

Specify appropriate setting values for **agent-watch interval** and **agent-watch down-count** commands based on the given network environment being used.

Agent ownership

No agent may be simultaneously controlled by multiple managers.
Therefore, only specify one manager per network.

If an agent receives a query frame after rebooting, that agent will be managed by the manager that sent the query frame.
That relationship is canceled if any of the following occur.

- A query frame is not received for 30 seconds.
- The manager is rebooted.

- The **l2ms reset** command is executed by the manager.

Agent operations

If a manager sets a setting for an L2MS-compliant agent or checks its operating status, such actions are referred to as "operating the agent".
Agents are operated using the LAN map on the web GUI.
To operate an agent, log into the manager web GUI and select the applicable agent in the LAN map.

For more detailed LAN map operating instructions, refer to the web GUI help page.

Note that agents cannot be operated using commands executed by the manager.

The following describes how to operate each operable agent via the LAN map.

Operations for SWX2100 series units

The following operations can be performed for agents.

- Display the status of the device and ports
- Show and control the power supply status of ports (PoE-equipped models only)
- Show/maintain network switch settings (show function settings, update firmware, restart, etc.)

Operations for SWX2110 and SWX2110P series units

The following operations can be performed for agents.

- Display the status of the device and ports
- Show and control the power supply status of ports (PoE-equipped models only)
- Set/maintain network switch settings (change function settings, update firmware, reboot, etc.)
- Set ports (VLAN tags, etc.)
- Save and restore config settings

Operations for SWX2200 series units

The following operations can be performed for agents.

- Display the status of the device and ports
- Show and control the power supply status of ports (PoE-equipped models only)
- Set/maintain network switch settings (change function settings, update firmware, reboot, etc.)
- Save settings to the manager and synchronize settings with settings saved in the manager

If SWX2200 settings are set from the manager, the settings are saved in both the manager and SWX2200 unit.

The settings are saved as a separate file from the manager config file, but the **startup-config select** command can be used to change the config settings at the same time.

If the SWX2200 unit is managed by the manager, settings in the manager and SWX2200 unit will be kept synchronized.
For details on synchronization of settings, refer to 3.6.7 Synchronizing Settings.

The status of settings in SWX2200 units managed by the manager can be checked using the **show l2ms agent-config** command.

Operations for SWX2210, SWX2210P, SWX2220, SWX2221P, and SWX2220P series units

The following operations can be performed for agents.

- Display the status of the device and ports
- Show and control the power supply status of ports (PoE-equipped models only)
- Change settings and perform maintenance (changing function settings, rebooting, etc.)
- Specify port settings (tagged VLAN, multiple VLANs, etc.)
- Specify link aggregation
- Change the IP address setting
- Save and restore config settings
- Use HTTP proxy functionality to log into the agent GUI.
- Find this switch (SWX2220/SWX2221P/SWX2220P models only)

If the HTTP proxy functionality is enabled, then it is possible to log into agent GUIs from the manager LAN map. That eliminates the need to enter a username and password for logging into an agent.

If SWX2210, SWX2210P, SWX2220, SWX2221P, or SWX2220P series units are managed by a manager configured with factory settings, then DHCP client settings are specified automatically.
For more details, refer to “3.6.8. HTTP Proxy Function and Setting IP Addresses.” * The SWX2210 model supports Rev.1.02.10 and later firmware.
* The SWX2210P model supports Rev.1.03.08 and later firmware.

Operations for SWX2300, SWX2310, SWX2310P, SWX2320, SWX2322P, SWX3100, SWX3200, and SWX3220 series units

The following operations can be performed for agents.

- Display the status of the device and ports
- Show and control the power supply status of ports (PoE-equipped models only)
- Change the IP address setting
- Save and restore the config
- Saving and restoring the config of the SWX2300 are supported by Rev.2.00.14 and later firmware.
- Use HTTP proxy functionality to log into the agent GUI.

If the HTTP proxy functionality is enabled, then it is possible to log into agent GUIs from the manager LAN map. That eliminates the need to enter a username and password for logging into an agent.

If an SWX2300/SWX2310/SWX2310P/SWX2320/SWX2322P/SWX3100/SWX3200/SWX3220 series unit is managed by a manager with factory settings, then DHCP client settings are specified automatically.
For more details, refer to “3.6.8. HTTP Proxy Function and Setting IP Addresses.”

Operations for WLX series units

The following operations can be performed for agents.

- Display the status of devices, LAN ports, and wireless modules
- Change the IP address setting
- Save and restore config settings
- Use HTTP proxy functionality to log into the agent GUI.

If the HTTP proxy functionality is enabled, then it is possible to log into agent GUIs from the manager LAN map. That eliminates the need to enter a username and password for logging into an agent.

If a WLX series unit is managed by a manager configured with factory settings, then DHCP client settings are specified automatically.
For more details, refer to “3.6.8. HTTP Proxy Function and Setting IP Addresses.”

Synchronizing settings

If an SWX2200 unit is managed by a manager, then settings held in the manager and SWX2200 unit are kept synchronized.
Synchronization is unidirectional from the manager to the SWX2200 unit, with the SWX2200 unit always operating based on settings in the manager.

When the manager starts managing an SWX2200 unit, it first checks whether the manager and SWX2200 settings match.
If they do not match, the following processes are performed.

1. All SWX2200 settings are restored to default values.
2. Function setting values held by the manager are sent to the SWX2200 unit.

The manager periodically monitors the settings of subordinate SWX2200 units and synchronizes them if a discrepancy is detected.

Synchronization may take some time (several tens of seconds to several minutes).
During synchronization, other SWX2200 operations are disabled.
Attempting to specify settings will cause an error without applying the settings to the manager or SWX2200 unit.

HTTP Proxy Function and Setting IP Addresses

The following actions can be performed on SWX2300, SWX2310, SWX2310P, SWX2320, SWX2322P, SWX3100, SWX3200, or SWX3220 series or WLX series models.

In the factory default settings or the status immediately after execution of the **cold start** command, a fixed IP address is set. (L2MS functions as an agent.)
At this time, if the agent is managed by the manager, **the DHCP client setting will automatically be configured.**

This is to avoid duplicate IP addresses if multiple agents exist.
Since IP addresses are assigned by the DHCP server within the network, agent web GUIs can be accessed via the HTTP proxy server. However, that requires specifying the **http-server enable** setting in the agent.
If a DHCP server does not exist in the network, then IP addresses cannot be obtained and agent IP addresses must be specified on the manager LAN map.
Once the IP setting is specified and the startup config has been saved, it will not be automatically specified in the DHCP client thereafter.

Information notifications from agents

If an agent managed by a manager detects a change or error in its own status, it sends information to notify the manager.

Information sent from the agent is output in the manager SYSLOG or LAN map.
For details on messages output to the SYSLOG, refer to “7. SYSLOG Message List.”

The following information is included in notifications from agents.

- Information in Notifications from Each Agent to the Manager

Agent	Information sent
SWX2100 series	Port link up/down Loop detection SFP optical RX level error (SWX2100-24G) Power supply function status for each port (PoE-equipped models only) Power supply function error for each device (PoE-equipped models only)
SWX2110 series SWX2110P series	Port link up/down Loop detection Power supply function status for each port (PoE-equipped models only) Power supply function error for each device (PoE-equipped models only)
SWX2200 series SWX2210 series SWX2210P series SWX2220 series SWX2221P series SWX2220P series	Port link up/down Loop detection Fan abnormal stop (SWX2200-24G, SWX2200-8PoE, SWX2210P, SWX2220-18NT/26NT, SWX2221P, SWX2220P) Power supply function status for each port (PoE-equipped models only) Power supply function error for each device (PoE-equipped models only) Temperature error (SWX2220-18NT/26NT, SWX2221P, SWX2220P) Terminal monitoring status (SWX2220, SWX2221P, SWX2220P) L2MS manager duplication (SWX2220, SWX2221P, SWX2220P)
SWX2300 series	Port link up/down Loop detection SFP optical RX level error Sending queue usage rate error

Agent	Information sent
SWX2310 series SWX2310P series SWX2320 series SWX2322P series SWX3100 series SWX3200 series SWX3220 series	Port link up/down Stack port link up/down (stack-compatible models only) Loop detection SFP optical RX level error Sending queue usage rate error Power supply function status for each port (PoE-equipped models only) Power supply function error for each device (PoE-equipped models only) Temperature error (SWX2310-52GT, SWX2310P, SWX3200, SWX2320, SWX2322P, SWX3220) Fan error (SWX2310-52GT, SWX2310P, SWX3200, SWX2320, SWX2322P, SWX3220) Power supply error (SWX3200) Temperature sensor error (SWX2310P) Terminal monitoring status (operating or down) L2MS manager duplication
WLX series	Change in settings of the wireless function

Monitoring connected terminals

Specifying the **terminal-watch enable** command in the manager enables functionality for monitoring connected terminals, so that information about terminals connected to the manager and agents can be managed.
The manager manages the following information about connected terminals.

- If the Manager and Agents are Yamaha Network Switches
  - Terminal MAC address
  - Manager or agent port number to which the terminal is connected
  - Date/time when terminal was detected
- If the Agent is a Yamaha wireless access point
  - Terminal MAC address
  - SSID to which the terminal is connected
  - Frequency (2.4 or 5 GHz) of terminal connection
  - Date/time when terminal was detected

This information can be viewed using the **show l2ms detail** command.

The recommended maximum number of terminals managed by this function is **200 units**, regardless of network configuration.
Note that more than the recommended number of units in the network could cause LAN map actions on the web GUI to be sluggish or unresponsive.

The manager will search for connected terminals or delete managed terminal information based on changes in the network.

The target and timing of manager searches for connected terminals are indicated below.
If new terminal information is found as a result of the search, it is determined that a terminal was detected.

- Timing and Object of Terminal Searches

Timing	Terminal
When the manager port is linked up	Corresponding port on the manager
When a new agent is detected	All ports on the detected agent
When link-up notification is received from a managed agent	Corresponding port on the agent
When the time specified by the **terminal-watch interval** command elapses	The manager and all agents

The following indicates what managed terminal information is deleted and when it is deleted if the manager determines that the terminal has disappeared from a network.

- Terminal for Which Information is Deleted and Deletion Timing

Timing	Terminal
When the manager port is linked down	Terminal connected to the corresponding manager port
When an agent is detected to be down	All terminals connected to that agent
When a port link-down notification is received from a managed agent	Terminal connected to the corresponding agent port
When a previously-detected terminal is not found in connected terminal search	Terminals not found

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

- List of L2MS-related commands

Operations	Operating commands
Switch to L2MS mode	l2ms configuration
Enable L2MS function	l2ms enable
Set role of L2MS function	l2ms role
Set agent monitoring time interval	agent-watch interval
Set number of times for deciding agent is down	agent-watch down-count
Enable terminal management function	terminal-watch enable
Set terminal information acquisition interval	terminal-watch interval
Set terminal information acquisition interval for terminals below wireless AP	wireless-terminal-watch interval
Enable event monitoring function	event-watch enable
Set event information acquisition interval	event-watch interval

Operations	Operating commands
Enable sending/receiving L2MS control frames	l2ms filter enable
Set whether to use agent zero-config function	config-auto-set enable
Reset agent management	l2ms reset
Show L2MS information	show l2ms
Show L2MS agent configuration information	show l2ms agent-config
Enable snapshot function	snapshot enable
Include/remove terminal for snapshot comparison	snapshot trap terminal
Create snapshot	snapshot save
Delete snapshot	snapshot delete
Set LAN map log output	logging event lan-map

Examples of Command Execution

Monitoring settings for agents

Set the agent monitoring time interval.

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#agent-watch interval 8
```

Set the number of monitoring times before deciding an agent is down.

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#agent-watch down-count 7
```

Enable terminal management function

Enable the terminal monitoring function.

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#terminal-watch enable
```

Set the time interval for acquiring terminal information.

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#terminal-watch interval 3600
```

Show the terminal information obtained by the manager.

```
Yamaha>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
```

Enable sending/receiving L2MS control frames

Disable sending or receiving L2MS control frames at port1.5.

```
Yamaha(config)#interface port1.5
Yamaha(config-if)#l2ms filter enable
```

Enable event monitoring function

Disable the event monitoring function.

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#event-watch disable
```

Set the time interval between acquiring event information.

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#event-watch interval 60
```

Enabling/disabling the zero-config function

This specifies whether the manager uses the zero-config function for agents.
This setting must be specified in the manager.

Disable the zero config function.

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#l2ms enable
Yamaha(config-l2ms)#l2ms role manager
Yamaha(config-l2ms)#config-auto-set disable
```

Points of Caution

Device configuration

A maximum of **128 agents** can be managed.

If the agents are used connected in series, a maximum of **8 agents can be connected from the manager**.
Nine or more agents cannot be connected to the manager in series.
If up to 8 agents are connected in series from the manager, then the specified maximum number of managed agents can be controlled.

Connecting nine or more agents in series from the manager could prevent properly recognizing or controlling agents due to delays in L2MS communication or cause the following types of problems.

- The synchronization process might not function correctly.
- If agent settings are modified from the GUI, correct execution might not be possible.

If a non-Yamaha switch exists in the L2MS communication route, such as between the manager and an agent, it might not be possible to control the agent correctly.
If you are configuring a network that includes a non-Yamaha switch, verify its operation beforehand.

Terminal monitoring

The recommended maximum number of managed units in a network is **200 units**.
Including more than the recommended maximum number of managed units could cause the LAN map in the Web GUI to become sluggish or unresponsive.
If necessary, disable the terminal management function (terminal-watch disable command).

Terminal searches use the information registered in the FDB (MAC address table) for the applicable devices. Therefore, depending on when the search is performed, a connected terminal might not be detected or a terminal no longer in the network might be detected.

If a link is detected to be down for a manager or Yamaha network switch port, all information for the terminal connected to that port is deleted even if the terminal is registered in the FDB (MAC address table).

It may take L2MS several seconds to recognize an agent after it is connected to a port.
During that time, the corresponding agent is treated as a terminal.

Yamaha network devices that are not managed as an agent by the manager are treated as terminals.

Terminal searches performed at intervals specified by the **terminal-watch interval** command search for terminals connected to the manager or all agents, which might take twenty to thirty minutes to complete for some network configurations.
However, other processes are not disabled until terminal searches are completed.

If a non-Yamaha L2 switch is connected to an L2MS-compliant device, the terminals connected to the non-Yamaha L2 switch are detected as terminals connected to the L2MS-compliant device.
However, if a terminal and a Yamaha network switch are connected in parallel to a non-Yamaha L2 switch, the terminal connected to the non-Yamaha L2 switch cannot be detected.

Use in conjunction with other functionality

Use in conjunction with a VLAN

If using a VLAN, ports used for L2MS communication must be specified as an access port or as a trunk port assigned by the native VLAN.
L2MS communication is not possible via a trunk port not assigned by the native VLAN.

Use in conjunction with mirroring

If the mirroring function is used, L2MS communications sent and received at the monitor port are also copied. Therefore, L2MS might not function properly if the manager or an agent is connected to a mirror port, so do not connect a manager or an agent to a mirror port.

Use in conjunction with an ACL

L2MS communication is not subject to ACL control.
Although the ACL discards frames that are not specified in the permissions list (tacit rejection), L2MS communications are not subject to ACL control, so frames are forwarded without being discarded.

Use in conjunction with STP or loop detection functionality

L2MS communication is not possible on ports blocked by STP or loop detection functionality.

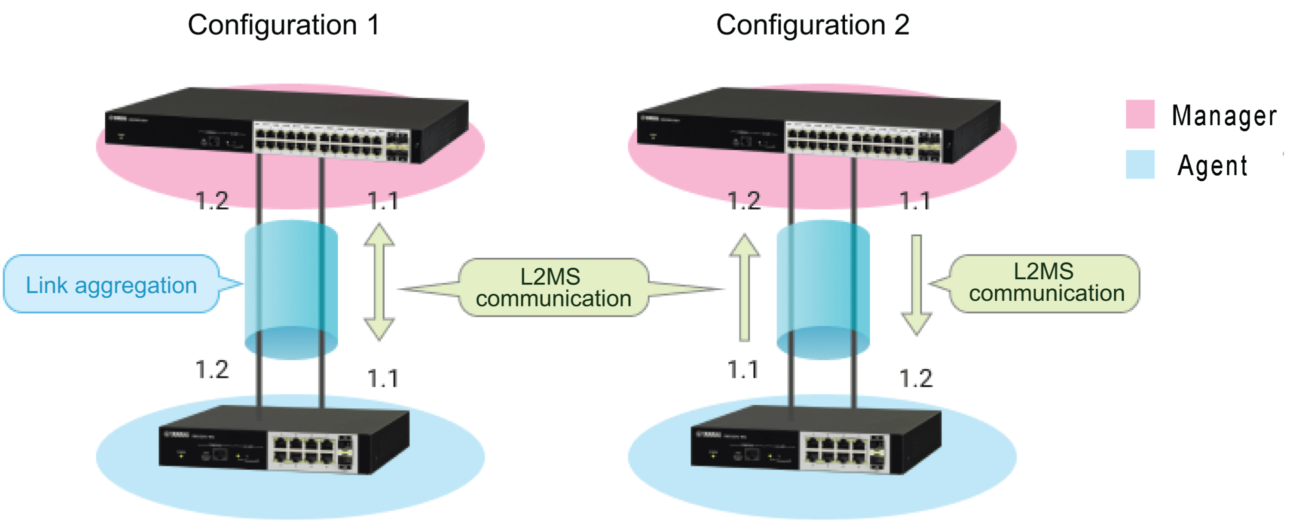
Link switching by STP could prevent the manager from recognizing the topology correctly, which could prevent finding agents or cause routing errors when agents are found.
In such cases, reset agent management after STP has finished switching the link by executing the **l2ms reset** command.

If multiple MST instances are operating, L2MS control frames are sent and received on the logical route (tree) formed by CIST (instance #0).

Use in conjunction with link aggregation

If link aggregation is used, L2MS communication is considered to be occurring on “the lowest-numbered linked-up port associated with the logical interface”.
If link aggregation is used in conjunction with the monitoring function for connected terminals and a terminal is discovered at the end of a logical interface connection, then the terminal is considered to be connected to “the lowest-numbered linked-up port associated with the logical interface” and the corresponding port number is shown.

In Configuration 1, L2MS communication is assumed to be occurring between respective ports 1.1.
In Configuration 2, L2MS communication is assumed to be occurring between manager port 1.1 and agent port 1.1.



Use in conjunction with the stack function

L2MS functions if even one unit is operating.

Even if the stack function is enabled, it is operated as one standalone unit if it cannot negotiate with a member switch.
L2MS will function even in that case.

- The L2MS manager can detect L2MS agents.
- L2MS agents are detected by the L2MS manager.
  However, only devices connected below the standalone switch are detected, while not detecting devices connected to other network switches assumed to be down.

SYSLOG Message List

L2MS outputs the following SYSLOG messages.

Output messages appended with the “[L2MS]” prefix.

SYSLOG messages displayed for units functioning as a manager are also appended with the "**route** (*addr*):"prefix. “_route*” refers to the route and “**addr**” the agent MAC address (indicated in all lowercase, in the form “xxxx.xxxx.xxxx”).

- SYSLOG Messages Displayed When the Unit Starts Up or the Operating Mode is Changed

Category	Output Level	Message	Meaning
Operation mode	informational	Start L2MS(Manager)	The L2MS unit was started as the manager.
		Start L2MS (agent)	The L2MS unit is started as an agent.
		L2MS is disabled	The L2MS did not start because it was disabled in settings.
		L2MS mode change **mode_from** to **mode_to**	The operating mode is changed from **mode_from** to **mode_to**.

- SYSLOG Messages Displayed When Operating as the Manager

Category	Output Level	Message	Meaning
Agent management	informational	Find agent	An agent was detected.
		Detect down	An agent is down.
Sync start	informational	Sync start	Agent synchronization process was started.
		Sync done	Agent synchronization process is finished.
		Sync failed	Agent synchronization process failed.
	debug	Can’t get param of sync	Failed to obtain the agent information needed for synchronization process.
Config Management	informational	Received config (*file*)	The manager received and saved the config file (*file*) from the agent.
		Sent config (*file*)	The manager sent the config file (*file*) to the agent.
		Removed config (*file*)	The config file (*file*) was deleted.
Device management	debug	Update device info	Terminal information for the terminal connected to the agent was updated.
		Fail to update device info	Failed to update terminal information for the terminal connected to the agent.
Terminal Information Database Management	debug	_path* : Format Version: Not found.	The format version is not indicated in the terminal information database file **path**.
		_path* : Format Version: Illegal value.	An invalid value is included in the format version indicated in the terminal information database file **path**.
		_path* : Device Information: Illegal value. (*line*)	An invalid value is indicated in the device information indicated in the terminal information database file **path**. (“_line*” line)
		_path* : Device Information: Duplicate device. (*line*)	A conflicting device is indicated in device information in the terminal information database file **path**. (“_line*” line)
		_path* : Character Code: Not Shift_JIS.	Non-Shift JIS characters are included in the character string code in the terminal information database file **path**.
Manager Duplication	informational	L2MS manager duplication detected. (*addr*, port *X_)	A duplicate L2MS manager was detected. (MAC address, port number where duplication was detected)
		L2MS manager duplication resolved. (*addr*, port *X_)	The L2MS manager duplication was resolved. (MAC address, port number where duplication was detected)

- SYSLOG messages are displayed appended with the prefix “[LANMAP]” for devices operating as the manager if the **logging event lan-map** command was executed.

Category	Output Level	Message	Meaning
Snapshot function	informational	SnapShot: Not found. [Device_Name: " *device_name_", MAC_Address: *addr_]	There is a Yamaha switch that cannot be found.
		SnapShot: Not found. [MAC_Address: *addr_]	There is a terminal that cannot be found.
		SnapShot: Unknown. [Device_Name: " *device_name_" , MAC_Address: *addr_]	There is an unregistered Yamaha switch.
		SnapShot: Unknown. [MAC_Address: *addr_]	There is an unregistered terminal.
		SnapShot: Route difference. [Device_Name: " *device_name_", Route: *route_(UpLink: *uplink_port_), Route(SnapShot): *route_snapshot_(UpLink: *uplink_port_snapshot_), MAC_Address: *addr_]	A Yamaha network switch with a different connection port was found. The correct route is **route_snapshot and the uplink port is *uplink_port_snapshot**.
		SnapShot: Route difference. [Route: *route_, Route(SnapShot): *route_snapshot_, MAC_Address: *addr_]	There is a terminal of a different connection port. The correct route is **route_snapshot**.
		SnapShot: Status recovered. [Device_Name: " *device_name_", MAC_Address: *addr_]	The state of the Yamaha switch matches the snapshot.
		SnapShot: Status recovered. [MAC_Address: *addr_]	The terminal status matched the snapshot file.

- The manager receives the following information notifications from agents.

Category	Output Level	Message	Meaning
Link status	informational	port **N** link up(10-hdx)	Agent port **N** linked up at 10 Mbps half-duplex.
		port **N** link up(10-fdx)	Agent port **N** linked up at 10 Mbps full-duplex.
		port **N** link up(100-hdx)	Agent port **N** linked up at 100 Mbps full-duplex.
		port **N** link up(100-fdx)	Agent port **N** linked up at 100 Mbps full-duplex.
		port **N** link up(1000-fdx)	Agent port **N** linked up at 1 Gbps full-duplex.
		port **N** link up(2500-fdx)	Agent port **N** linked up at 2.5 Gbps full-duplex.
		port **N** link up(5000-fdx)	Agent port **N** linked up at 5 Gbps full-duplex.
		port **N** link up(10000-fdx)	Agent port **N** linked up at 10 Gbps full-duplex.
		port **N** link down	Agent port **N** linked down.
		stack port(port *N_) link up	The agent stack port (port *N_) linked up.
		stack port(port *N_) link down	The agent stack port (port *N_) linked down.

Category	Output Level	Message	Meaning
Loop detection	informational	port **N** loop detect	A loop has occurred at agent port **N**.
		sa **N** loop detect	A loop has occurred at agent static logical interface # **N**.
		po **N** loop detect	A loop has occurred at agent LACP logical interface # **N**.
Wireless Functions	informational	Airlink setting changed	An agent wireless functionality setting was changed.
PoE	informational	port **N** PoE state(supply-class0)	Power supply was started to a class0 device at agent port **N**.
		port **N** PoE state(supply-class1)	Power supply was started to a class1 device at agent port **N**.
		port **N** PoE state(supply-class2)	Power supply was started to a class2 device at agent port **N**.
		port **N** PoE state(supply-class3)	Power supply was started to a class3 device at agent port **N**.
		port **N** PoE state(supply-class4)	Power supply was started to a class4 device at agent port **N**.

Category	Output Level	Message	Meaning
PoE	informational	port **N** PoE state(supply-class5)	Power supply was started to a class5 device at agent port **N**.
		port **N** PoE state(supply-class6)	Power supply was started to a class6 device at agent port **N**.
		port **N** PoE state(supply-class7)	Power supply was started to a class7 device at agent port **N**.
		port **N** PoE state(supply-class8)	Power supply was started to a class8 device at agent port **N**.
		port **N** PoE state(terminate)	Power supply was stopped at agent port **N**.
		port **N** PoE state(overcurrent)	Power supply was stopped at agent port **N** because an overcurrent occurred.
		port **N** PoE state(forced-terminate)	Power supply was stopped at ports where class 3 (15.4 W) power was supplied by supplying class 4 (30 W) power at agent port **N**.
		port **N** PoE state(over-supply)	Power supply was stopped because the peak power supply rate exceeded the maximum supply capacity at agent port **N**.
		port **N** PoE state(over-temperature)	Power supply was stopped because a temperature error occurred at agent port **N**.
		port **N** PoE state(fanlock)	Power supply was stopped because the fan stopped at agent port **N**.
		port **N** PoE state(power-failure)	Power supply was stopped because the power supply failure occurred at agent port **N**.
		port **N** PoE state(class-failure)	Power supply was stopped because a higher than specified power supply class was detected at agent port **N**.
		PoE state(over-guardband)	The agent power supply level entered the guardband range.
		port **N** PoE state(pd-failure)	Power supply was stopped because a power input error was detected at agent port **N**.
		port **N** PoE state(guardband-restrict)	Power supply was stopped because a power supply that exceeded the guardband was detected at agent port **N**.
		PoE state error(over-supply)	The agent power supply exceeded the maximum power supply capacity.
		PoE state error(stop-supply)	The agent power supply stopped.
		PoE state error(power-failure)	An agent power supply error occurred.

Category	Output Level	Message	Meaning
PoE	informational	PoE state error(over-temperature, stop) Stack **N** PoE state error(over-temperature, stop)	Power supply was stopped due to an agent temperature error. Power supply was stopped due to an agent (stack ID: *N_) temperature error.
		PoE state error(over-temperature, normal) Stack **N** PoE state error(over-temperature, normal)	Power supply that stopped due to an agent temperature error was restored. Power supply stopped due to an agent (stack ID: *N_) temperature error was restored.
		PoE state error(fanlock, stop) Stack **N** PoE state error(fanlock, stop)	Power supply was stopped because the agent fan stopped. Power supply was stopped because the agent (stack ID: *N_) fan stopped.
		PoE state error(fanlock, normal) Stack **N** PoE state error(fanlock, normal)	Power supply stopped because an agent fan stopped was restored. Power supply stopped because an agent (stack ID: *N_) fan stopped was restored.
		PoE state error(power-failure, stop) Stack **N** PoE state error(power-failure, stop)	Power supply was stopped due to an agent power supply abnormality. Power supply was stopped due to an agent (stack ID: *N_) power supply abnormality.
SFP Optical RX Level	informational	port **N** SFP RX power(low)	The SFP optical RX level decreased below the lower limit threshold value at agent port **N**.
		port **N** SFP RX power(high)	The SFP optical RX level exceeded the upper limit threshold value at agent port **N**.
		port **N** SFP RX power(normal)	The SFP optical RX level at agent port **N** returned to normal.
Send Queue Usage	informational	port **N** queue **Q** usage rate(busy)	The sending load at agent port **N** is high (QoS transmission queue: *Q_)
		port **N** queue **Q** usage rate(full)	The sending load at agent port **N** reached the upper limit (QoS transmission queue: *Q_)
		port **N** queue **Q** usage rate(recovered)	The sending load at Agent port **N** returned to normal (QoS transmission queue: *Q_)

Category	Output Level	Message	Meaning
Terminal Monitoring	informational	ping: *ip-address_(*description*) state(DOWN)	Ping monitoring indicated *ip-address_(*description*) has gone down.
		ping: *ip-address_(*description*) state(UP)	ping monitoring indicated *ip-address_(*description*) is now operating.
		ping: *ip-address_(*description*) state(IDLE)	*ip-address*(*description*) is not being monitored by ping monitoring.
		Frame Counter: *port_(*description*) state(DOWN)	Monitoring according to frame reception volume indicates *port_(*description*) has gone down.
		Frame Counter: *port_(*description*) state(UP)	Monitoring according to frame reception volume indicates *port_(*description*) is now operating.
		Frame Counter: *port_(*description*) state(IDLE)	*port*(*description*) is not being monitored according to frame reception volume.
		LLDP: *port_(*description*) state(DOWN)	LLDP frame monitoring indicates *port_(*description*) has gone down.
		LLDP: *port_(*description*) state(UP)	LLDP frame monitoring indicates *port_(*description*) is now operating.
		LLDP: *port_(*description*) state(IDLE)	*port*(*description*) is not being monitored by LLDP frame monitoring.
Power supply	informational	Power voltage(high) Stack **N** Power voltage(high)	The agent power supply voltage exceeded the upper threshold value. The agent (stack ID: *N_) power supply voltage exceeded the upper threshold value.
		Power current(high) Stack **N** Power current(high)	An overcurrent occurred in the agent power supply. An overcurrent occurred in the agent (stack ID: *N_) power supply.
Fan	informational	Fan lock	The agent fan stopped.
		FAN control(high) Stack **N** FAN control(high)	The agent fan rpm increased. The agent (stack ID: *N_) fan rpm increased.
		FAN control(low) Stack **N** FAN control(low)	The agent fan rpm decreased. The agent (stack ID: *N_) fan rpm decreased.
		FAN **X** (stop) Stack **N** FAN **X** (stop)	The agent fan (FAN *X_) stopped. The agent (stack ID: *N_) fan (FAN *X_) stopped.
		FAN **X** (normal) Stack **N** FAN **X** (normal)	The agent fan (FAN *X_) was restored. The agent (stack ID: *N_) fan (FAN *X_) was restored.

Category	Output Level	Message	Meaning
Temperature	informational	CPU temperature(high) Stack **N** CPU temperature(high)	The agent CPU temperature exceeded the threshold value. The agent (stack ID: *N_) CPU temperature exceeded the threshold value.
		CPU temperature(normal) Stack **N** CPU temperature(normal)	The agent CPU temperature returned to normal. The agent (stack ID: *N_) CPU temperature returned to normal.
		CPU temperature error(alarm) Stack **N** CPU temperature error(alarm)	An agent CPU temperature error occurred. The agent (stack ID: *N_) CPU temperature error occurred.
		CPU temperature error(normal) Stack **N** CPU temperature error(normal)	The agent CPU temperature error was resolved. The agent (stack ID: *N_) CPU temperature error was resolved.
		PHY temperature(high) Stack **N** PHY temperature(high)	The agent PHY temperature exceeded the threshold value. The agent (stack ID: *N_) PHY temperature exceeded the threshold value.
		PHY temperature(normal) Stack **N** PHY temperature(normal)	The agent PHY temperature returned to normal. The agent (stack ID: *N_) PHY temperature returned to normal.
		PHY temperature error(alarm) Stack **N** PHY temperature error(alarm)	An agent PHY temperature error occurred. The agent (stack ID: *N_) PHY temperature error occurred.
		PHY temperature error(normal) Stack **N** PHY temperature error(normal)	The agent PHY temperature error was resolved. The agent (stack ID: *N_) PHY temperature error was resolved.
		SFP temperature(high) Stack **N** SFP temperature(high)	The agent SFP module temperature exceeded the threshold value. The agent (stack ID: *N_) SFP module temperature exceeded the threshold value.
		SFP temperature(normal) Stack **N** SFP temperature(normal)	The agent SFP module temperature returned to normal. The agent (stack ID: *N_) SFP module temperature returned to normal.
		SFP temperature error(alarm) Stack **N** SFP temperature error(alarm)	An agent SFP module temperature error occurred. The agent (stack ID: *N_) SFP module temperature error occurred.
		SFP temperature error(normal) Stack **N** SFP temperature error(normal)	The agent SFP module temperature error was resolved. The agent (stack ID: *N_) SFP module temperature error was resolved.

Category	Output Level	Message	Meaning
Temperature	informational	Stack **N** Unit temperature(high)	The agent unit temperature exceeded the threshold value. The agent (stack ID: *N_) unit temperature exceeded the threshold value.
		Unit temperature(normal) Stack **N** Unit temperature(normal)	The agent unit temperature returned to normal. The agent (stack ID: *N_) unit temperature returned to normal.
		Unit temperature error(alarm) Stack **N** Unit temperature error(alarm)	A temperature error occurred in an agent unit. The agent (stack ID: *N_) unit temperature error occurred.
		Unit temperature error(normal) Stack **N** Unit temperature error(normal)	The temperature error in the agent unit was resolved. The agent (stack ID: *N_) unit temperature error was resolved.
		PSE temperature(high) Stack **N** PSE temperature(high)	The agent PSE temperature exceeded the threshold value. The agent (stack ID: *N_) PSE temperature exceeded the threshold value.
		PSE temperature(normal) Stack **N** PSE temperature(normal)	The agent PSE temperature returned to normal. The agent (stack ID: *N_) PSE temperature returned to normal.
		PSE temperature error(alarm) Stack **N** PSE temperature error(alarm)	An agent PSE temperature error occurred. The agent (stack ID: *N_) PSE temperature error occurred.
		PSE temperature error(normal) Stack **N** PSE temperature error(normal)	The agent PSE temperature error was resolved. The agent (stack ID: *N_) PSE temperature error was resolved.
		MAC temperature(high) Stack **N** MAC temperature(high)	The agent MAC temperature exceeded the threshold value. The agent (stack ID: *N_) MAC temperature exceeded the threshold value.
		MAC temperature(normal) Stack **N** MAC temperature(normal)	The agent MAC temperature returned to normal. The agent (stack ID: *N_) MAC temperature returned to normal.
		MAC temperature error(alarm) Stack **N** MAC temperature error(alarm)	An agent MAC temperature error occurred. The agent (stack ID: *N_) MAC temperature error occurred.
		MAC temperature error(normal) Stack **N** MAC temperature error(normal)	The agent MAC temperature error was resolved. The agent (stack ID: *N_) MAC temperature error was resolved.

Category	Output Level	Message	Meaning
Temperature	informational	Thermal sensor(alarm) Stack **N** Thermal sensor(alarm)	An agent temperature sensor error occurred. The agent (stack ID: *N_) temperature sensor error occurred.
Config Management	informational	Executing a config … **progress** % (*file*)	Agent config file (*file*) settings are being restored. (**progress**%).
		Finished executing a config (*file*)	Finished restoring the agent config file (*file*).
		line: **errmsg** (*file*)	An **errmsg** error occurred on line **line** while restoring the agent config file (*file*).
Manager Duplication	informational	l2ms-manager-duplication(occur). (*addr*, port *X_)	A duplicate L2MS manager was detected at an agent. (MAC address, port number where duplication was detected)
		l2ms-manager-duplication(stop). (*addr*, port *X_)	The L2MS manager duplication at the agent was resolved. (MAC address, port number where duplication was detected)
Function	informational	unsupported function(*function*)	The agent firmware does not support the corresponding protocol. The _function* part shows one of the following: Setting info Status l2ms info SFP RX power Qos queue rate Qos queue rate2 Terminal monitoring System monitoring Note: Only output the first time after the “Find agent” message. The log output is suppressed after the first time. These are reset once link down is detected.

- SYSLOG Messages Displayed When Operating as an Agent

Category	Output Level	Message	Meaning
Agent management	infromational	Start management by manager(*addr*)	Agent is now managed by the manager.
		Release from manager(*addr*)	Agent is no longer managed by the manager.
Restart	informational	Restart by manager request.	This restarts the network switch as requested by a manager.

Category	Output Level	Message	Meaning
Config Management	infromational	Sent config to manager (*addr*)	Config file was sent to the manager.
		Received config from manager (*addr*)	Config file was received from the manager.
		Restart for update settings.	The unit will restart in order to update the received config file.
Manager Duplication	informational	L2MS manager duplication detected. (*addr*, port *X_)	A duplicate L2MS manager was detected. (MAC address, port number where duplication was detected)
		L2MS manager duplication resolved. (*addr*, port *X_)	The L2MS manager duplication was resolved. (MAC address, port number where duplication was detected)

Related Documentation

- Switch control functions of Yamaha routers

Mail Notification

Function Overview

The mail notification function sends mail notifications of information detected by the L2MS function or terminal monitoring function.
By specifying the following settings, mail notifications can be sent with information detected by various functions.

- Specify settings for the mail server used to send mails.
- Specify the mail template.

Definition of Terms Used

Mail Template

The mail template defines the collection of information needed for sending mail.

- Mail server to use
- Sender mail address
- Recipient mail address
- Subject of mail
- Notification content
- Transmission wait time

Function Details

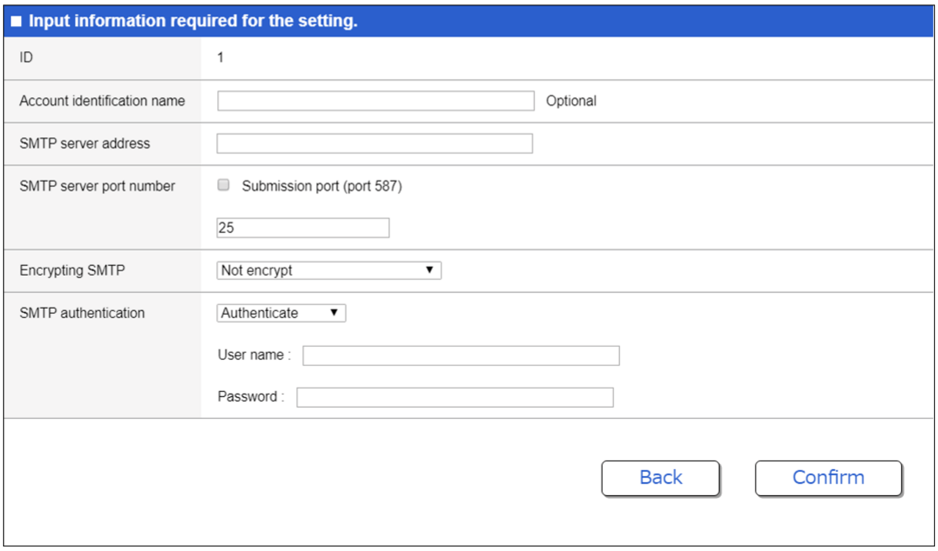
Action

After mail server settings and mail template settings have been configured correctly, the mail notification function will enter the send-standby state whenever a notification event occurs for a function that supports mail notification.
When the mail notification function is in the send-standby state, the function will wait until the specified mail transmission wait time specified in each mail template elapses.
When the mail transmission wait time has elapsed, the mail notification function combines the information for notification events that occurred during the wait time into a single mail and sends it to the recipient.

Mail server settings

Settings can be specified in the **List of Registered Mail Servers** displayed by clicking [Detailed settings] - [mail notification] in the web GUI.
To display the **Mail server settings**, click the **New** button or the **Setting** button for existing settings.
In **Mail server settings**, make the following settings.

- Account identification name
  Name for uniquely identifying the mail server settings. This setting may be omitted.
- SMTP server address
- SMTP server port number
- Encrypting SMTP
  Selects either “SMTP over SSL” or “STARTTLS” as the encryption method.
- SMTP authentication
  To use SMTP authentication, enter the username and password.



■ Input information required for the setting.

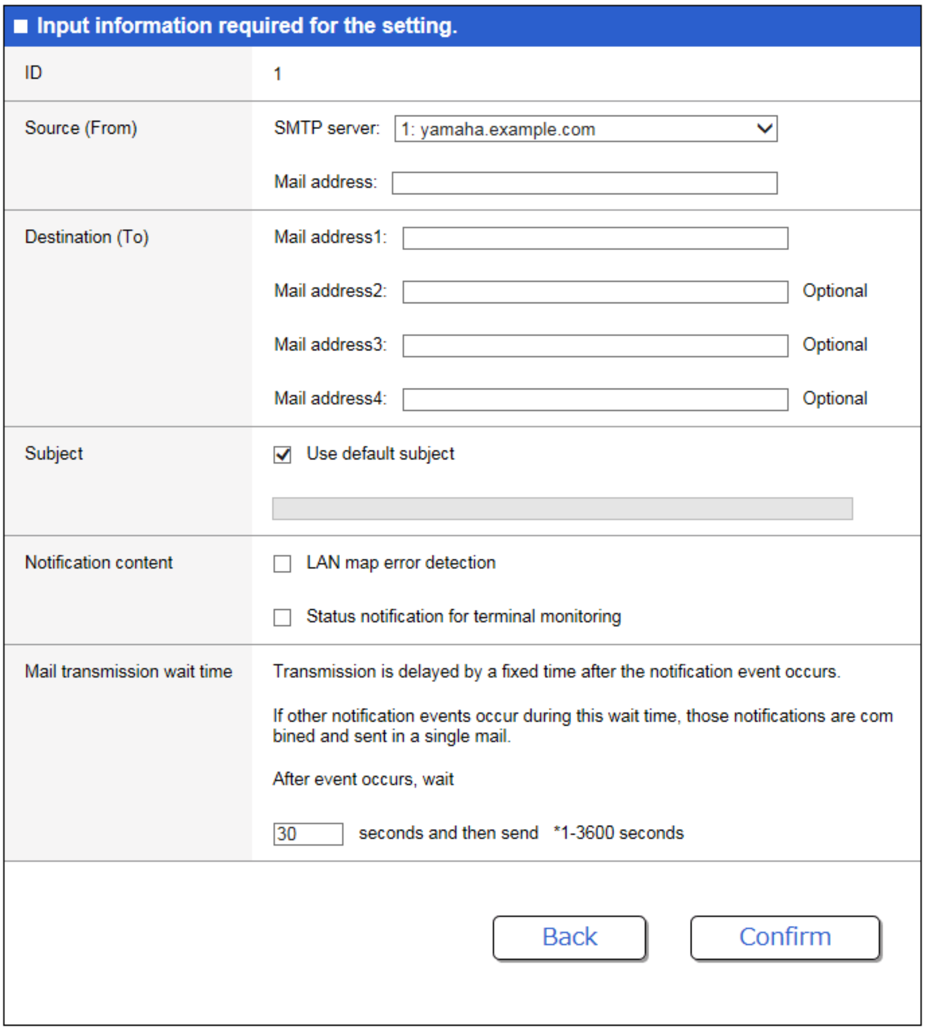
ID	1
Account identification name	Optional
SMTP server address	
SMTP server port number	□ Submission port (port 587) 25
Encrypting SMTP	Not encrypt ▼
SMTP authentication	Authenticate ▼ User name : Password :

Specify the mail template

Mail template settings can be specified by clicking [Detailed settings] - [mail notification] in the web GUI to display the **List of mail notification settings**.

Press the **New** button or the **Setting** button for an existing setting to display **mail notification settings**.
In **mail notification settings**, specify the following settings.

- Source (From)
- Destination (To)
- Subject
  If the **Use default subject** box is checked, then the mail subject will always be in the form **Notification from (device name)**.
- Notification content
  Error types can be specified in detail for **LAN map error detection**, so that only the specified type of notifications are output.
- Mail transmission wait time



■ Input information required for the setting.

ID	1
Source (From)	SMTP server: 1: yamaha.example.com Mail address:
Destination (To)	Mail address1: Mail address2: Optional Mail address3: Optional Mail address4: Optional
Subject	☑ Use default subject
Notification content	□ LAN map error detection □ Status notification for terminal monitoring
Mail transmission wait time	Transmission is delayed by a fixed time after the notification event occurs. If other notification events occur during this wait time, those notifications are com bined and sent in a single mail. After event occurs, wait 30 seconds and then send *1-3600 seconds

Functions that support mail notification

The following functions support mail notification.

- LAN MAP
  The following notification events can be included in mail notifications.

Category	Type	Event	Description
Device abnormality	Fan error	Fan Lock	Fan stopped
		Fan speed	Fan rotation speed increased
		Fan stop	A specific fan stopped
	Power supply abnormality	Power voltage	Power supply voltage exceeded the upper threshold value
		Power supply	Overcurrent occurred in power supply
	Temperature anomaly	CPU temperature CPU temperature error PHY temperature PHY temperature error SFP temperature SFP module temperature error Unit temperature Unit temperature error PSE temperature PSE temperature error MAC temperature MAC temperature error	Yamaha network switch temperature (CPU, PHY, SFP module, main unit, PSE, or MAC temperature) exceeded the upper threshold value
			The Yamaha network switch temperature returned to normal
		Thermal Sensor invalid	A Yamaha network switch temperature sensor error occurred
Loop Detection	Loop was detected	Loop Detect	Loop was detected at a port
			The loop detected at the port was resolved
SFP optical Rx level abnormality	SFP optical input level error	SFP RX Power	SFP optical input level exceeded the threshold value
			SFP optical input level returned to the normal range

Category	Type	Event	Description
Transmission Queue Monitoring	Sending queue usage ratio error	Queue Usage Rate	Sending queue usage ratio increased
			Sending queue usage ratio reached upper limit
			Sending queue usage ratio returned to normal value
PoE supply	Temperature anomaly	Over Temperature	Power supply stopped due to a temperature anomaly
	Maximum power supply capacity was exceeded	Over Supply	The power supply exceeded the maximum supply capacity
	Power supply abnormality	Power Failure	The power supply source malfunctioned
	Power supply stopped due to a power supply class error	Class Failure	Power supply was stopped because a class greater than the power supply class setting was detected at the power supply port
	Power supply stopped due to a class4 power supply	Forced Terminate	Power supply to a port that was being supplied class3 (15.4 W) power was stopped due to a class4 (30 W) power supply at the port
	Power supply stopped due to overcurrent	Over Current	Power supply stopped because an excessive current was supplied to a port
	Power supply stopped because power supply capacity was exceeded	PoE state error(over-supply)	The power supply exceeded the maximum supply capacity
			Maximum power supply capacity exceeded has been resolved
	Power supply stopped due to temperature error	PoE state error(over-temperature)	Power supply stopped due to a temperature anomaly
			Power supply stop due to temperature error was resolved
	Power supply stopped due to stoppage of fan	PoE state error(fanlock)	Power supply stopped because the fan stopped
			Power supply stop due to stopped fan was resolved
	Power supply stopped due to power supply abnormality	PoE state error(power-failure)	Power supply stopped due to a PoE power supply abnormality

Category	Type	Event	Description
Snapshot	Invalid device connected	Illegal Equipment(SnapShot)	Device not registered in snapshot was detected
			Invalid device connection was resolved
	Connection port mismatch	Port Mismatch(SnapShot)	Device with a connection port that differs from snapshot was detected
			Connection port mismatch was resolved
	Device lost	Disappearance Equipment(SnapShot)	A device registered in the snapshot is not connected
			Device loss was resolved
L2MS Manager Duplication	L2MS Manager Duplication	L2MS manager duplication	A duplicate L2MS manager was detected

- Terminal monitoring function
  The following notification events can be included in mail notifications.

Category	Type	Description
Ping monitoring	Up detection	Terminal up was detected
	Down detection	Terminal down was detected
Frame reception volume monitoring	Up detection	Terminal up was detected
	Down detection	Terminal down was detected
LLDP monitoring	Up detection	Terminal up was detected
	Down detection	Terminal down was detected

- Stack function
  The following notification events can be included in mail notifications.

Type	Description
Stack port link down	The stack port connected to the member switch went link-down
Heartbeat error detection	A member switch heartbeat error was detected
Member switch was upgraded	A member switch was upgraded to a main switch

Mail body example

The body of a notification mail includes content such as the following.

For details, refer to the technical reference for each function.
Up to 100 items can be included in one notification mail.

```
Model: SWX2310P-28GT                 * Model name
Revision: Rev.2.02.02                * Firmware version
Name: SWX2310P-28GT_XXXXXXXX         * Host name
Time: 2017/06/13 11:42:56            * Mail transmission time
Template ID: 1                       * Mail template ID
```

```
<<<<<<<<<<<<<<<<<<<<<<<<    Lan Map Information    >>>>>>>>>>>>>>>>>>>>>>>>>

[SFP RX Power]

  Type                                Device_Name
  MAC_Address                         Err_Port
  Route
  State
============================================================================
(Detected: 2017/06/13 10:09:40  Recovered: 2017/06/13 10:10:10)
  SWX2310P-10G                        SWX2310P-10G_S4K000398
  00a0.deae.b89c                      1.9
  port1.7(UpLink:1.5)
  Low
----------------------------------------------------------------------------

[Queue Usage Rate]

  Type                                Device_Name
  MAC_Address                         Err_Port
  Route
  State
============================================================================
(Detected: 2017/06/13 10:15:42  Recovered: 2017/06/13 10:17:24)
  SWX2310P-10G                        SWX2310P-10G_S4K000398
  00a0.deae.b89c                      1.6
  port1.7(UpLink:1.5)
  Full(Queue:2)
----------------------------------------------------------------------------

[Fan Lock]

  Type                                Device_Name
  MAC_Address
  Route
============================================================================
(Detected: 2017/06/13 10:28:43  Recovered: ----/--/-- --:--:--)
  SWX2200-8PoE                        SWX2200-8PoE_S45000345
  00a0.de83.4146
  port1.5(UpLink:2)
----------------------------------------------------------------------------
(Detected: 2017/06/13 10:42:13  Recovered: 2017/06/13 10:42:22)
  SWX2200-24G                         SWX2200-24G_X00000344
  00a0.de2a.dbbb
  port1.1(UpLink:23)
----------------------------------------------------------------------------

<<<<<<<<<<<<<<<<<<    Terminal Monitoring Information    >>>>>>>>>>>>>>>>>>>

[via Ping]

 Date                      Status    IP Address        Description
----------------------------------------------------------------------------
 2017/06/13 Thu 10:42:56   UP        192.168.100.155   IP_Camera_1
 2017/06/13 Thu 10:51:00   DOWN      192.168.100.155   IP_Camera_1
 2017/06/13 Thu 10:54:02   UP        192.168.100.10    Wireless_AP_1
 2017/06/13 Thu 11:29:27   UP        192.168.100.155   IP_Camera_1
 2017/06/13 Thu 11:30:31   DOWN      192.168.100.10    Wireless_AP_1

[via Bandwidth Usage]

 Date                      Status    Interface         Description
----------------------------------------------------------------------------
 2017/06/13 Thu 10:45:43   UP        port1.4           IP_Camera_2
 2017/06/13 Thu 10:45:56   UP        port1.6           Note_PC_1
 2017/06/13 Thu 10:50:00   DOWN      port1.6           Note_PC_1
 2017/06/13 Thu 10:53:27   DOWN      port1.4           IP_Camera_2

[via LLDP]

 Date                      Status    Interface         Description
----------------------------------------------------------------------------
 2017/06/13 Thu 10:53:56   UP        port1.3           Note_PC_2
 2017/06/13 Thu 11:11:54   DOWN      port1.3           Note_PC_2
 2017/06/13 Thu 11:14:24   UP        port1.3           Note_PC_2

<<<<<<<<<<<<<<<<<<<<<<<<<<    Stack Information    >>>>>>>>>>>>>>>>>>>>>>>>>

 Date                      Information
----------------------------------------------------------------------------
 2017/06/13 Thu 10:53:44   The stack port changed state to down. (port1.27)
 2017/06/13 Thu 10:53:46   Promoted to a main. (Old main ID : 1)
 2017/06/13 Thu 10:59:10   Occurred the heartbeat error. (ID : 1)
```

Content of LAN map notifications

- Notification content of each event

  The content of LAN map notification mails differs depending on the event type.
  The content of notifications for each event type is indicated below.

Event	Type Device_Name MAC_Address	Comment	Stack_ID	Err_Port	Fan_number	Route	Route(SnapShot)	State
Fan Lock	Yes	No	No	No	No	Yes	No	No
Fan speed		No	Yes	No	No	Yes	No	No
Fan stop		No	Yes	No	Yes	Yes	No	No
Power voltage Power supply		No	Yes	No	No	Yes	No	No
CPU temperature CPU temperature error PHY temperature PHY temperature error SFP temperature SFP module temperature error Unit temperature Unit temperature error PSE temperature PSE temperature error MAC temperature MAC temperature error Thermal Sensor invalid		No	Yes	No	No	Yes	No	No
Loop Detect		No	No	Yes	No	Yes	No	No
SFP RX Power		No	No	Yes	No	Yes	No	Yes

Event	Type Device_Name MAC_Address	Comment	Stack_ID	Err_Port	Fan_number	Route	Route(SnapShot)	State
Queue Usage Rate	Yes	No	No	Yes	No	Yes	No	Yes
Over Temperature Over Supply Power Failure		No	No	No	No	Yes	No	No
Class Failure Forced Terminate Over Current		No	No	Yes	No	Yes	No	No
PoE state error(over-supply) PoE state error(over-temperature) PoE state error(fanlock) PoE state error(power-failure)		No	Yes	No	No	Yes	No	No
Illegal Equipment(SnapShot)		Yes	No	No	No	Yes	No	No
Port Mismatch(SnapShot)		Yes	No	No	No	Yes	Yes	No
Disappearance Equipment(SnapShot)		Yes	No	No	No	No	Yes	No
L2MS manager duplication		Yes	No	Yes	No	Yes	No	No

- Detailed content of notification
  A detailed description of the various information included in notifications is indicated below.

Notification content	Example:	Description
Detected	Detected: 2021/10/01 8:25:40	Indicates the date/time the error occurred.
Recovered	Recovered: 2021/10/01 10:09:40	Indicates the date/time the error was resolved.
Type	SWX2310P-28GT	Indicates the model name.
Device_Name	SWX2310P-28GT_XXXXXXXXXX	Indicates the device name.
MAC_Address	ac44.f2xx.xxxx	Indicates the MAC address.
Comment	Snapshot: Comment	Indicates comments specified in the LAN map device list.
	L2MS manager duplication: ac44.f2xx.xxxx	Indicates the MAC address of duplicate L2MS managers.
Stack_ID	1	Indicates the stack ID.

Notification content	Example:	Description
Err_Port	1.5	Indicates the port number where the error occurred.
Fan_number	1	Indicates the fan number where the error occurred.
Route	port1.20(UpLink:1.2)	Indicates routing information for applicable devices.
Route(SnapShot)	port1.20(UpLink:1.2)	Indicates routing information on the snapshot for applicable devices.
State	SFP optical Rx level abnormality: Low	Indicates SFP optical input level as either “Low” or “High”.
	Transmission queue monitoring: Full (Queue: 2)	Indicates either “Busy” or “Full” as the transmission queue usage status and the transmission queue number.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
SMTP mail server setting	mail server smtp host
SMTP mail server name setting	mail server smtp name
Mail notification trigger setting	mail notify trigger
Mail sending template setting mode	mail template
Mail sending server ID setting	send server
Mail sender address setting	send from
Mail recipient address setting	send to
Mail subject setting	send subject
Mail wait time setting	send notify wait-time
Mail certificate setting	mail send certificate
Mail certificate notification setting	mail send certificate-notify
Certificate expiration date notification timing setting	mail certificate expire-notify
Show mail information	show mail information

Points of Caution

The following are precautions related to SMTP authentication.

- The SMTP authentication only supports the LOGIN method.
- PLAIN, CRAM-MD5, and other methods are not supported.

Precautions for using firmware not compatible with the mail notification function.

- If the firmware is updated from a version that does not support a command to a version that does support the command, commands specified in the web GUI are directly carried over as command settings.
- To revert to the firmware version that does not support the commands, any changes to settings made using the firmware that does support the commands are not migrated and must be specified again after restoring the older version.
- If no settings were changed, then the current settings can be maintained.

The following are precautions related to LAN map error detection.

- Errors are indicated in notifications as active until the error is resolved, even if the error notification is disabled without resolving the error.
- Specifically, even after a notification is disabled, an mail is sent after the error is resolved and is included in mails about the occurrence of other errors.

Related Documentation

- L2MS Control
- Terminal Monitoring
- Stacking

LLDP

Function Overview

LLDP is a protocol for passing device management information between a device and its neighboring devices. This is a simple protocol in which a device unidirectionally advertises its own information and neighbor devices receive this information. However, since LLDP-compliant devices maintain the information received from neighbor devices as MIB objects, the user can access this information via SNMP and ascertain what type of devices are connected to which interfaces are.
This protocol is also used for negotiation between devices that support PoE (Power Over Ethernet).

Definition of Terms Used

LLDP

Link Layer Discovery Protocol.
This is defined in IEEE 802.1AB.

LLDP-MED

LLDP for Media Endpont Devices.
This is defined in ANSI/TIA-1057.

Function Details

Operating specifications

Basic specifications

This product supports the following operations.

- LLDP frames are transmitted from any LAN/SFP port to convey information about the device itself.
- LLDP frames are received at any LAN/SFP port to obtain information about neighboring devices.
- Information transmitted via LLDP about the device itself, and information obtained via LLDP about neighbor devices, etc., can be referenced via SNMP.

LLDP sends and receives information using Type, Length, and Value (TLV) attributes.
For details on the TLV information sent by this product, refer to **TLV list**.

This product’s LLDP supports the following MIBs of SNMP. For details, refer to **3.3 Supported MIBs**.

- LLDP-MIB
- LLDP-EXT-DOT3-MIB
- LLDP-V2-MIB
- LLDP-EXT-DOT3-V2-MIB
- LLDP-EXT-MED-MIB

The following settings are required in order to use the LLDP function.

- Enable LLDP functionality for the overall system using the **lldp run** command.
- Create LLDP agents at applicable interfaces using the **lldp-agent** command.
- Specify the LLDP frame transmit/receive mode using the **set lldp** command.

The LLDP function is **enabled** in default settings for this product.

LLDP frames are always transmitted without tags, regardless of the VLAN settings of the transmitting switch port.
They are also transmitted without tags from a trunk port without a native VLAN.

When LLDP is used for PoE negotiation, it is necessary to configure the port to which the PoE powered device is connected so that LLDP can be transmitted and received.

Transmitted information settings

Use the following commands to specify the LLDP frames that are transmitted from the device itself. There are also some TLVs (required TLVs) that are transmitted regardless of the settings of the following commands.

- **tlv-select basic-mgmt** command (basic management TLV)
- **tlv-select ieee-8021-org-specific** command (IEEE 802.1 TLV)
- **tlv-select ieee-8023-org-specific** command (IEEE 802.3 TLV)
- **tlv-select med** command (LLDP-MED TLV)

The system name and description that are transmitted in the basic management TLVs are specified by the **lldp system-name** command and the **lldp system-description** command.
The type of management address is **set management-address-tlv** command.

Transmission timer setting

LLDP frame transmission interval is specified by the **set timer msg-tx-interval** command.
The multiplier for calculating the hold time (TTL) for device information is set by the **set msg-tx-hold** command. The TTL for LLDP transmission is the result of the following calculation. The default is **121** seconds.

- **TTL = (value set by the "set timer msg-tx-interval" command) × (value set by the "set msg-tx-hold" command) + 1 (second)**

When a neighbor device is connected to a LAN/SFP port for which LLDP frame transmission is enabled, LLDP frames are transmitted rapidly at a fixed interval according to the high-speed transmission interval setting.
The transmission interval and the number of transmissions for high speed transmission are set by the **set timer msg-fast-tx** command and the **set tx-fast-init**.

If the **set lldp** command is used to change the setting from a state in which LLDP frame transmission is enabled to a state in which the frame transmission is disabled, this product transmits a shut-down frame, notifying the neighbor device that LLDP frame transmission has stopped.
Subsequently, even if LLDP frame transmission is once again enabled, LLDP frame transmission to the neighbor device is stopped for a time.
The stopped duration until the next transmission occurs after transmitting the shutdown frame is set by the **set timer reinit-delay** command.

Maximum connected devices setting

The maximum number of connected devices that can be managed by the corresponding port is set by the **set too-many-neighbors limit** command.
The default value for the maximum number of connected devices is **5 devices**.

Checking LLDP information

LLDP interface settings and received information about neighbor devices can be checked by using the **show lldp interface** command or the **show lldp neighbors** command.

To clear the LLDP frame counter, use the **clear lldp counters** command.

- Access point link
  This function sends and receives proprietary LLDP frames between Yamaha network switches and Yamaha wireless access points to automatically perform specific processes, such as specifying settings based on information in the LLDP notifications or saving log data.
  AP link function setting is specified using the **lldp auto-setting** command.
  For details, refer to **LLDP Automatic Setting (Access Point Link)**.

- Dante optimization setting
  This function automatically specifies settings optimized for the Dante digital audio network.
  The Dante optimization settings function is set using the **lldp auto-setting** command.
  For more information, refer to **Dante Optimization Settings Function**.

- LLDP reception interval monitoring
  This function monitors whether specific connected terminals are live or dead.
  For details, refer to **Terminal Monitoring**.

- Voice VLAN
  With the voice VLAN function, LLDP-MED can be used to specify voice traffic settings for IP telephony.
  For details, refer to **VLAN**.

TLV list

The TLVs supported by this product are listed below.

- Required TLVs
- Basic management TLVs
- IEEE 802.1 TLV
- IEEE 802.3 TLV
- LLDP-MED TLV

For detailed specifications of each TLV, refer to IEEE 802.1AB (LLDP) and ANSI/TIA-1057 (LLDP-MED).
The TLVs that are transmitted by this product are explained below.

Required TLVs

If LLDP frame transmission is enabled, these TLVs are always transmitted.

Three TLVs are transmitted: chassis ID, port ID, and TTL.
The required TLVs are listed below.

Type	Description	Length	Value (only fixed values are listed)
Chassis ID	Chassis ID	6 bytes	MAC address of the device
Port ID	Port ID	7 to 8 bytes	Port name (portX.X)
Time To Live (TTL)	Hold time of device information (sec)	2 bytes	

Basic management TLVs

These TLVs are transmitted if LLDP frame transmission is enabled and the **tlv-select basic-mgmt** command is specified.

System-related management information is transmitted, such as name, system capabilities, and address.
The basic management TLVs are listed below.

Type	Description	Length	Value (only fixed values are listed)
Port Description	Port description string	0 to 255 bytes	
System Name	System name string Default: Hostname	0 to 255 bytes	
System Description	System description string Default: Model name + Firmware revision	0 to 255 bytes	
System Capabilities	Capabilities supported by the system	2 bytes	0x0004（bridge）
	Enabled system capabilities	2 bytes	0x0004（bridge）
Management Address	Management address IP address (4 bytes) or MAC address (6 bytes)	4 or 6 bytes	
	Interface sub-type	1 byte	0x02 (ifIndex)
	Interface number	4 Byte	ifIndex value

IEEE 802.1 TLV

These TLVs are transmitted if LLDP frame transmission is enabled and the **tlv-select ieee-8021-org-specific** command is specified.

These transmit information such as VLAN and link aggregation for the corresponding port.
The IEEE 802.1 TLVs are listed below.

Type	Description	Length	Value (only fixed values are listed)
Port VLAN ID	Port VLAN number	2 bytes	
Port and Protocol VLAN ID	Protocol VLAN support and enable/disable	1 byte	0x00 (no support)
	Protocol VLAN number	2 bytes	0x0000
Protocol Identity	Byte string that identifies the protocol	0 to 255 bytes	
Link Aggregation	Aggregation capability and status	1 byte	
	ifIndex number of aggregation logical interface	4 Byte	
VLAN Name	Name of the VLAN to which the port belongs	0 to 32 bytes	

IEEE 802.3 TLV

These TLVs are transmitted if LLDP frame transmission is enabled and the **tlv-select ieee-8023-org-specific** command is specified.

Auto negotiation support information, PoE information, etc. for the corresponding port are transmitted.
The IEEE 802.3 TLVs are listed below.

Type	Description	Length	Value (only fixed values are listed)
MAC/PHY Configuration/Status	Auto negotiation support, and whether enabled or disabled	1 byte	
	Supported communication method for auto negotiation	2 bytes	
	Operational MAU Type Data signaling rate and duplex mode (IETF RFC 4836)	2 bytes	
Power Via MDI	MDI power support status	1 byte	
	PSE power pair Selection of wiring to be used for power supply	1 byte	0x01 (signal line)
	Power class Class0 to Class4	1 byte	
	Power type PSE Device/PD Device	2 bit	0b00 (PSE Device)
	Power source Primary/Secondary	2 bit	0b01 (Primary)
	Priority	2 bit	
	Power required from PD device (in units of 0.1 watts)	2 bytes	
	Power supply of PSE device (in units of 0.1 watts)	2 bytes	
Link Aggregation	Aggregation capability and status	1 byte	
	ifIndex number of aggregation logical interface	4 Byte	
Maximum Frame Size	Maximum frame size	2 bytes	

LLDP-MED TLV

These TLVs are transmitted if LLDP frame transmission is enabled and the **tlv-select med** command is specified.

These are used to transmit information about network policy and extended PoE of the port.
The LLDP-MED TLVs are listed below.

Type	Description	Length	Value (only fixed values are listed)
LLDP-MED Capabilities	Transmittable LLDP-MED TLVs	2 bytes	0x000B (LLDP-MED Capabilities, Network Policy, Extended Power-via-MDI TLV)
	Device type	1 byte	0x04 (Network Connectivity)

Type	Description	Length	Value (only fixed values are listed)
Network Policy	Application type	1 byte	0x01 (Voice)
	Voice VLAN information	3 Byte	
Extended Power-via-MDI	Power type PSE Device/PD Device	2 bit	0b00 (PSE Device)
	Power source Primary/Secondary	2 bit	0b01 (Primary)
	Power priority	4 bit	
	Power required from PD (in units of 0.1 watts)	2 bytes	

Network policy is only transmitted via the port specified by Voice VLAN.

Supported MIBs

Refer to the following SNMP MIB Reference for information on the MIBs that are supported.

- SNMP MIB Reference

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Enable LLDP function	lldp run
Set system description text string	lldp system-description
Set system name	lldp system-name
Create LLDP agent	lldp-agent
Set LLDP transmission/reception mode	set lldp
Set the type of management address	set management-address-tlv
Set basic management TLV	tlv-select basic-mgmt
Set IEEE-802.1 TLV	tlv-select ieee-8021-org-specific
Set IEEE-802.3 TLV	tlv-select ieee-8023-org-specific
Set LLDP-MED TLV	tlv-select med
Set the LLDP frame transmission interval	set timer msg-tx-interval
Set duration to stop transmission following LLDP transmission stop until transmission is once again possible	set timer reinit-delay
Set the multiplier for calculating the hold time (TTL) for device information	set msg-tx-hold

Operations	Operating commands
Set LLDP frame transmission interval for high-speed transmission term	set timer msg-fast-tx
Set number of LLDP frames transmitted for high-speed transmission term	set tx-fast-init
Set the maximum number of connected devices that can be managed by each port	set too-many-neighbors limit
Show interface status	show lldp interface
Show connected device information for all interfaces	show lldp neighbors
Clear LLDP frame counters	clear lldp counters
Set Dante optimization setting function and AP link function using LLDP	lldp auto-setting

Examples of Command Execution

Set LLDP frame transmission/reception

For port1.1, enable LLDP frame transmission/reception.

Basic management TLVs, IEEE 802.1 TLVs, IEEE 802.3 TLVs, and LLDP-MED TLVs are transmitted.

Set the LLDP frame transmission interval to 60 seconds. Set the LLDP frame TTL to 181 seconds.

Set “SWITCH1” as the name of the transmitting system.
Specify 10 as the maximum number of connected devices managed by the port.

```
Yamaha#configure terminal
Yamaha(confif)#lldp system-name SWITCH1 ①
Yamaha(config)#interface port1.1
Yamaha(config-if)#lldp-agent ②
Yamaha(lldp-agent)#tlv-select basic-mgmt ③
Yamaha(lldp-agent)#tlv-select ieee-8021-org-specific ④
Yamaha(lldp-agent)#tlv-select ieee-8023-org-specific ⑤
Yamaha(lldp-agent)#tlv-select med ⑥
Yamaha(lldp-agent)#set timer msg-tx-interval 60 ⑦
Yamaha(lldp-agent)#set msg-tx-hold 3 ⑧
Yamaha(lldp-agent)#set too-many-neighbors limit 10 ⑨
Yamaha(lldp-agent)#set lldp enable txrx ⑩
Yamaha(lldp-agent)#exit
Yamaha(config-if)#exit
Yamaha(config)#lldp run ⑪
Yamaha(config)#exit
```

① Set system name

② Create LLDP agent, mode transition

③ Set basic management TLV

④ Set IEEE 802.1 TLV

⑤ Set IEEE 802.3 TLV

⑥ Set LLDP-MED TLV

⑦ Set transmission interval

⑧ Set multiplier for TTL calculation: TTL = 60 x 3 + 1 = 181 seconds

⑨ Maximum connected devices setting

⑩ Set LLDP transmission/reception mode

⑪ Enable LLDP function

Show LLDP interface status

Show the port1.1 LLDP interface information.

```
Yamaha#show lldp interface port1.1 ①
Agent Mode                    : Nearest bridge
Enable (tx/rx)                : Y/Y
Message fast transmit time    : 1
Message transmission interval : 30
Reinitialization delay        : 2
MED Enabled                   : Y
Device Type                   : NETWORK_CONNECTIVITY
LLDP Agent traffic statistics
  Total frames transmitted       : 0
```

① Show interface information

Show LLDP connected device information

Show LLDP connected device information.

```
Yamaha#show lldp neighbors ①
Interface Name           : port1.1
System Name              : SWX3100-10G
System Description       : SWX3100 Rev.4.01.02 (Mon Dec  4 12:33:18 2017)
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
```

① Show connected device information

Points of Caution

None

Related Documentation

- SNMP
- Terminal Monitoring
- Dante Optimization Settings
- PoE Control
- VLAN
- LLDP Automatic Setting (Access Point Link)

LLDP Automatic Setting (Access Point Link)

Function Overview

The LLDP automatic setting specifies sending/receiving proprietary LLDP frames between Yamaha network switches and Yamaha wireless access points to automatically perform specific processes, such as specifying settings based on information in LLDP notifications or saving log data.

The following functionality can be achieved by LLDP automatic settings.

- RADIUS server automatic settings
  - This automatically specifies information about RADIUS servers currently operating at the Yamaha wireless access point in the Yamaha network switch. That makes it easy to configure an authentication function in Yamaha wireless access points as a RADIUS server or in Yamaha network switches as a RADIUS client.
- Yamaha wireless access point dead/alive monitoring
  - This uses LLDP to automatically monitor whether Yamaha wireless access points connected to the product are dead or alive.
- Log saving before Yamaha wireless access points stop
  - It can be used to save log data up to immediately prior to shutting off power to Yamaha wireless access points by sending a notification before shutting off PoE power supply from a Yamaha network switch to a Yamaha wireless access point.

To determine Yamaha network switch and wireless access point models that support LLDP automatic setting function, refer to the following.

- Technical reference: LLDP automatic setting examples

Definition of Terms Used

LLDP

Link Layer Discovery Protocol.
This is defined in IEEE 802.1AB.

Function Details

Basic specifications

If LLDP automatic setting function is enabled, proprietary LLDP frames will be sent and received between Yamaha network switches and Yamaha wireless access points.

LLDP automatic settings are specified using the **lldp auto-setting** command.
LLDP automatic setting function is **enabled** in default settings.

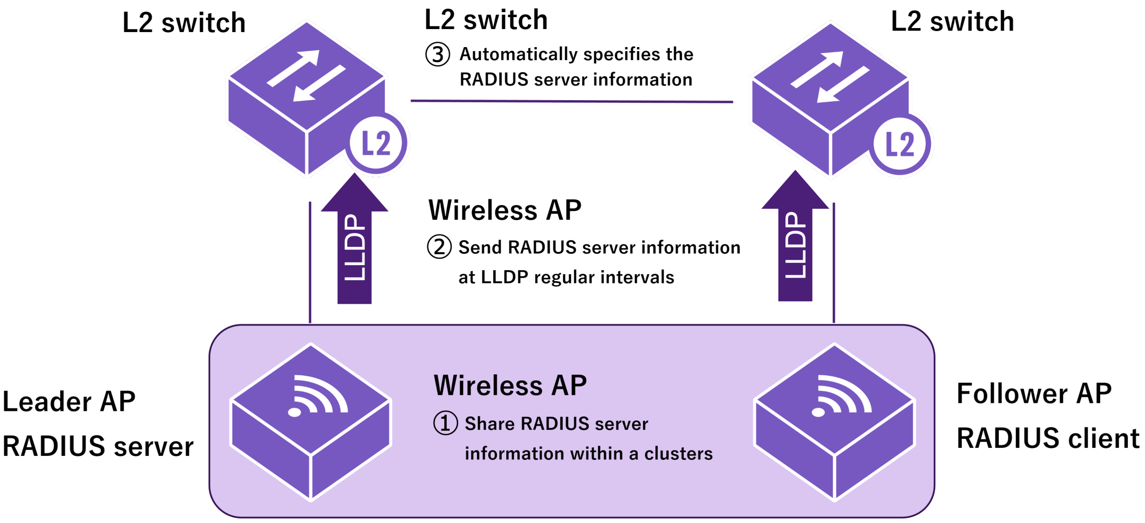
In order to use this function, reception of LLDP frames must be enabled.
For this reason, check in advance that the following settings have been made.

- Enable LLDP functionality for the overall system using the **lldp run** command.
- Create LLDP agents at applicable interfaces using the **lldp-agent** command.
- Specify the LLDP frame transmit/receive mode using the **set lldp** command.

LLDP frame transmission and reception are **enabled** in product default settings.

RADIUS server automatic settings

This function automatically specifies information in the product about RADIUS servers currently operating at Yamaha wireless access points (clusters). That makes it easy to configure an authentication function in Yamaha wireless access points as a RADIUS server or in Yamaha network switches as a RADIUS client.
Authentication settings for each port on the product must be set manually by the user based on the given environment. For details about the settings, refer to Port authentication function in the technical reference.


L2 switch
L2 switch
③ Automatically specifies the RADIUS server information
L2 switch
L2
L2
LLDP
Wireless AP
② Send RADIUS server information at LLDP regular intervals
LLDP
Leader AP
RADIUS server
Wireless AP
① Share RADIUS server information within a clusters
Follower AP
RADIUS client

RADIUS server information sent by Yamaha wireless access points

Yamaha wireless access points send RADIUS server information based on the following criteria.

- LLDP and LLDP automatic settings are enabled
- Cluster functionality is enabled
- Cluster leader APs are functioning as a RADIUS server
- Cluster follower APs are functioning as RADIUS client that connects to a leader AP RADIUS server.

For details about Yamaha wireless access point settings, refer to the Yamaha wireless access point technical reference.

If the criteria for sending information are satisfied, Yamaha wireless access points send notifications with the following RADIUS server information at LLDP regular intervals.

- IP address of the RADIUS server
- UDP port number for RADIUS server authentication
- Shared password for communicating with RADIUS server

RADIUS server entry control

If the product LLDP automatic setting function is enabled and RADIUS server information is received from a Yamaha wireless access point, then a **radius-server host** command with an optional **dynamic** string added to the end is automatically specified in the running-config.
In the remaining explanation below, the **radius-server host** command appended by an optional **dynamic** string is referred to as a “dynamic entry”, whereas the manually specified **radius-server host** command is referred to as a “static entry”.
Dynamic entries appended with the optional **dynamic** string are not saved in the startup-config file, even if the **write** command is executed.
After dynamic entry is set by automatic settings, static entry can be set by manually deleting the **dynamic** option.
However, static entry cannot be changed to dynamic entry by manually adding the **dynamic** option.

- Example of Dynamic Entry of **radius-server host** Command

```
radius-server host 192.168.100.241 auth-port 1234 key EXAMPLE dynamic
```

Dynamic entries specified by LLDP automatic settings are appended with LLDP reception port number and term of validity information.
If identical RADIUS server information is received from multiple ports, the RADIUS server information received from the port with the **smallest port number** is retained.
The **TTL (Time to Live)** value included in the received LLDP frame is specified as the term of validity.
The default TTL value for LLDP frames sent from Yamaha wireless access points is **120** seconds.
If new RADIUS server information is received within TTL seconds, then the term of validity is updated, whereas if new RADIUS server information is not received within TTL seconds, then the dynamic entry is deleted.
However, if an LLDP shutdown frame with TTL = 0 is received, then the dynamic entry is immediately deleted.
You can check the RADIUS server information with the **show radius-server** command. An asterisk (*) will be added to the automatically specified RADIUS server host, and the LLDP reception port number (LLDP Received port) and term of validity (Expires) information will be displayed.

- Example of using the **show radius-server** command to show dynamic entry information

```
SWX#show radius-server
Server Host : 192.168.100.241*
 LLDP Received port : port1.2
 Expires : 00:00:33
 Authentication Port : 1234
 Secret Key : EXAMPLE
 Timeout : 10 sec
 Retransmit Count : 5
 Deadtime : 0 min

* - Assigned by LLDP.
```

A total of up to **8** RADIUS server information entries, including dynamic and static entries, can be specified for the product.
Using static entries is prioritized over using dynamic entries.
Therefore, even if the maximum number of RADIUS server information entries are already specified, new static entries can be specified if there are any dynamic entries among existing entries.
In that case, the dynamic entry with the highest LLDP reception port number is deleted.

Points of Caution

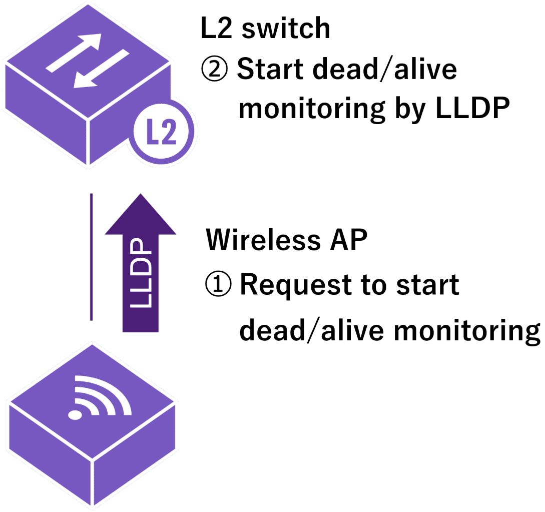
If the above functionality is used, note the following precautions.

- Connection to Yamaha wireless access point unit
  - To enable automatic setting of RADIUS server information, Yamaha network switches must be connected directly to a Yamaha wireless access point that support LLDP automatic setting functionality.
  - For Yamaha network switches not directly connected to a Yamaha wireless access point, specify RADIUS server settings manually.
- Command input mode restrictions when the stack function is enabled
  - If the stack function is enabled, users permitted to transition to the global configuration mode are restricted. For details, refer to Stack Function.

    - Because settings automatically transition to the global configuration mode if RADIUS server settings are received by LLDP from a Yamaha wireless access point and applied, users that are already in the global configuration mode via the console or who are in an individual configuration mode are forced to transition to the privileged EXEC mode.
- Characters permitted in shared passwords for communicating with RADIUS servers
    - Question mark and space characters cannot be used. Do not use those characters when setting shared passwords (RADIUS server, client, or secret) for Yamaha wireless access point units.
- Set response wait time for the entire RADIUS server
    - If multiple RADIUS servers are configured, set the **auth timeout server-timeout** command setting value, which sets the total wait time for all RADIUS servers, to a value equal to or larger than the product of the **radius-server timeout** command setting value times the **radius-server retransmit** command setting value plus one times the number of RADIUS servers. For command details, refer to the command reference.

Yamaha wireless access point dead/alive monitoring

When a Yamaha network switch receives a request from a Yamaha wireless access point to start dead/alive monitoring, it automatically starts monitoring by LLDP whether the Yamaha wireless access point is dead or alive.


L2
L2 switch
② Start dead/alive monitoring by LLDP
LLDP
Wireless AP
① Request to start dead/alive monitoring

Yamaha wireless access points send dead/alive monitoring requests based on the following criteria.

- LLDP and LLDP automatic settings are enabled

If the dead/alive monitoring request is received with the LLDP automatic setting function enabled in the Yamaha network switch, then an LLDP reception interval monitoring setting is registered for the LLDP reception port.
At ports where the setting is registered, the alive/dead status is monitored by LLDP. If no LLDP signals are received/sent for a certain period, the PoE power supply is temporarily (5 seconds) switched off to try and restore the Yamaha wireless access point.
Also, a notification will be issued when a communication interruption is detected in SNMP traps and L2MS traps. For details, refer to the technical reference for terminal monitoring.

Points of Caution

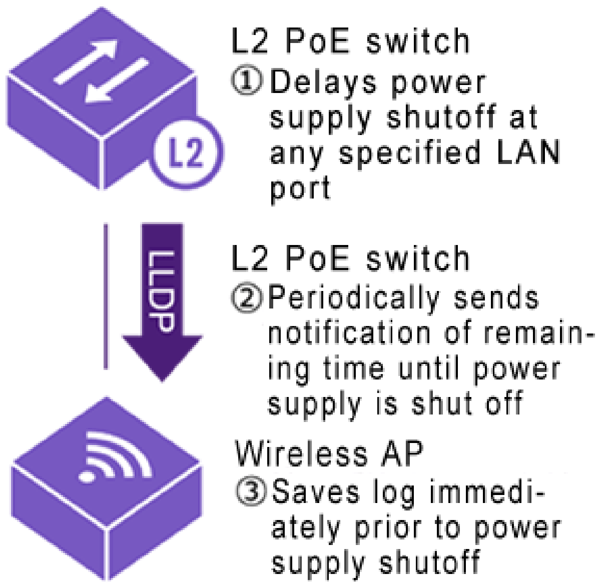
If the above functionality is used, note the following precautions.

- If dead/alive monitoring is no longer necessary, such as after the Yamaha wireless access point connection port was changed, manually delete the settings that became unnecessary after the Yamaha wireless access point connection port was changed.

Log saving before Yamaha wireless access points stop

The scheduling function can be used to operate the product so that PoE power to a wireless access point is shut off only during a specified period.
Because that suddenly shuts off power to the wireless access point, unsaved log data is normally lost, but this model is able to save that Yamaha wireless access point log data by using LLDP to notify the device about the PoE power shutoff timing.

Power supply shutoff timing notices are sent if the **power-inline disable delay** command was used at a given LAN port to specify a PoE power shutoff delay time (delay option).
If the Web GUI is used to select the “Stop power supply after notifying the Yamaha wireless AP” setting for the easy schedule template settings function, the setting for shutting off the power 10 minutes after executing the schedule (**power-inline disable delay 600** command) is registered.


L2
L2 PoE switch
①Delays power supply shutoff at any specified LAN port
LLDP
L2 PoE switch
②Periodically sends notification of remaining time until power supply is shut off
Wireless AP
③Saves log immediately prior to power supply shutoff

If the following criteria are satisfied at a port with power shutoff being delayed, the LLDP transmission interval is overridden and changed to 30 seconds.

- The LLDP transmission interval setting must be greater than 30 seconds.
- LLDP and LLDP automatic settings are enabled

However, if the power supply is already shut off or the **power-inline enable** command was used to cancel the power supply shutoff delay, then the LLDP transmission interval will revert to the original setting value.
If the LLDP transmission interval is overridden and changed to 30 seconds by this function, then an asterisk is appended to the LLDP transmission interval value shown by the **show lldp interface** command.

- Example of LLDP transmission interval shown by the **show lldp interface** command

```
SWX#show lldp interface port1.2
Agent Mode                    : Nearest bridge
Enable (tx/rx)                : Y/Y
Message fast transmit time    : 1
Message transmission interval : 30*
Reinitialization 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

* - Assigned by LLDP.
```

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Enable LLDP automatic settings	lldp auto-setting
Enable LLDP function	lldp run
Create LLDP agent	lldp-agent
Set LLDP transmission/reception mode	set lldp
Set LLDP frame transmission interval	set timer msg-tx-interval
Set RADIUS server host	radius-server host
Set response wait time for a single RADIUS server	radius-server timeout
Set number of times to resend requests to RADIUS server	radius-server retransmit
Show RADIUS server setting status	show radius-server
Set response wait time for the entire RADIUS server	auth timeout server-timeout
Set the PoE power supply function (interface)	power-inline
Show interface status	show lldp interface

Setting Examples

For instructions on how to configure respective Yamaha network switch and wireless access point settings, refer to the following.

- Technical reference: LLDP automatic setting examples

Points of Caution

See the precautions indicated for each function.

Related Documentation

- LLDP
- RADIUS server
- Port Authentication Function
- Terminal Monitoring
- PoE Control
- Schedule Function

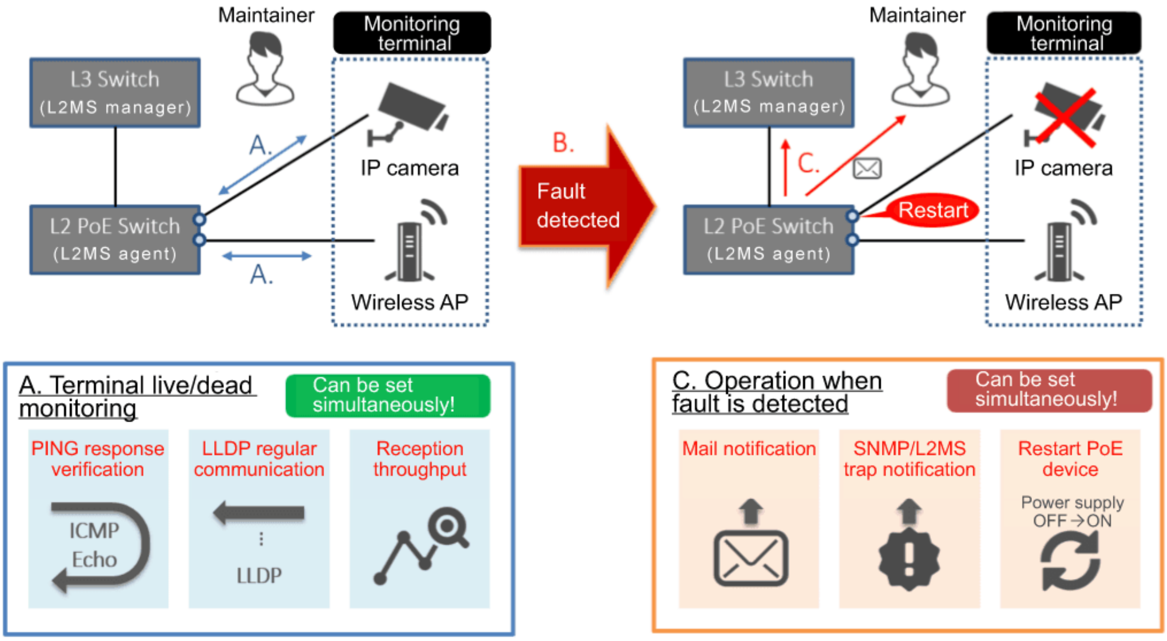
- Stack Function
- Technical reference: LLDP automatic setting examples

Terminal Monitoring

Function Overview

The terminal monitoring function checks the dead-or-alive state of specific terminals connected to the network switch.
The operating specifications for the terminal monitoring function are shown below.

- Terminal monitoring function overview
  Example of an L2MS manager with an L3 switch and an L2MS agent with an intelligent L2 PoE switch



As dead/alive monitoring methods, the following **three types** are provided.

1. **Ping-based communication monitoring**
   Ping (ICMP Echo request/reply) is issued at regular intervals to a terminal that has an IP address, and the terminal is determined to be down if there is no longer a response.
   The user can specify the ping response wait time and the number of failures before the connection is determined to be down.
2. **Frame reception volume monitoring**
   The frame reception volume is monitored at regular intervals for an individual port, and the terminal is determined to be down if the traffic falls below a specified volume.
   The user can specify the monitoring start threshold value and the threshold value at which a down condition is determined.
   Monitoring starts when the traffic exceeds the monitoring start threshold value, and a down condition is determined when the traffic falls below the down decision threshold.
3. **LLDP reception interval monitoring**
   The LLDP received at regular intervals by an individual port is monitored.
   Using the TTL which is a required item in the data portion of an LLDP packet, a down condition is determined if LLDP is not received within the TTL interval.

If monitoring detects a terminal fault (down), the following processing is **automatically** performed.

1. **Alert display in the dashboard screen**
   An indication that a fault (down) occurred for the monitored terminal is displayed in the alert screen of the dashboard.

2. **Alert shown in LAN map screen**

    - If the network switch monitoring the terminal is an L2MS manager
    LAN map notification and history information are used to indicate an error (down) occurred in a monitored terminal.

    - If the network switch monitoring the terminal is an L2MS agent
    The L2MS trap function is used to notify the L2MS manager.
    When the L2MS manager receives a notification, it uses the LAN map screen to indicate an error (down) occurred in a monitored terminal.

By **the user's choice**, the following operations can be applied in parallel.

1. **Fault detection notification by mail**
   Notification that a monitored terminal has experienced a fault is sent to the desired recipient.

2. **Notification to an SNMP manager**
   A trap is sent to the SNMP manager specified by a command.

3. **Restart of a terminal due to temporary stop of PoE supply**
   If a down condition is detected on a port to which PoE power is being supplied, PoE power supply is temporarily turned off in an attempt to recover the monitored terminal.

Definition of Terms Used

None

Function Details

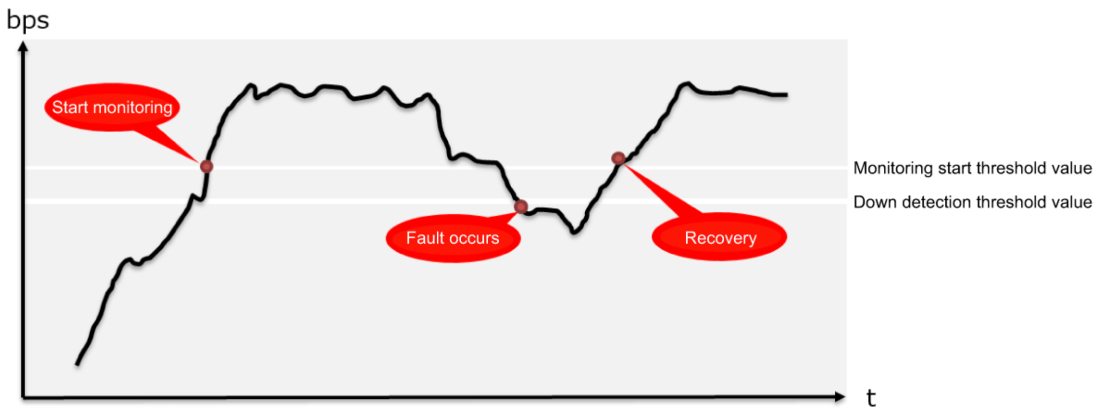
Monitoring by ping (ICMP Echo request/reply)

Specifications for terminal monitoring by ping are given below.

1. The interval of ICMP Echo request transmission from the network switch is fixed at **5 sec**.
2. The ICMP Echo request that is transmitted has the following format.
    - As the ID field of the ICMP header, the **unique ID assigned to each monitored terminal** is specified.
    - As the sequence field of the ICMP header, a number that is sequentially incremented from 0 is specified.
3. The validity of the ICMP Echo reply is checked as follows.
    - Whether the ID field of the ICMP header contains the ID that was specified when sending the request
    - Whether the sequence field of the ICMP header contains the sequence number that was specified when sending the request
4. The wait time for ICMP Echo reply can be changed in the range of **1–60 sec**, and the default is **2 sec**.
5. The number of failures to receive the ICMP Echo reply from the monitored terminal after which a fault is determined can be set in the range of **1–100**, and the default is **twice**.
6. Monitoring with ping can be done for a **maximum of 64 units**.
7. If sending a mail notification or SNMP trap is enabled, they are sent in the following cases.
    - When a terminal is detected to be down (sent every 24 hours while down)
    - When a terminal is detected to be up (sent when monitoring is started or restored)

Monitoring according to frame reception volume

The way in which this device monitors according to frame reception volume is described below.


bps
Start monitoring
Fault occurs
Recovery
Monitoring start threshold value
Down detection threshold value
t

1. At one-second intervals, the number of octets received at the port is referenced, and the number of octets received during one second is calculated.
    - **All ports are the object of observation.**
2. Using the number of octets received during one second and the link speed, **the reception throughput (bps) and reception ratio (%)** are calculated.
3. Monitoring according to frame reception volume starts when **the monitoring start threshold value (bps) specified by the user** is exceeded.
4. After monitoring has started, a fault (down) is detected if the volume falls below **the down detection threshold value (bps) specified by the user**.
5. If sending a mail notification or SNMP trap is enabled, they are sent in the following cases.
    - When a terminal is detected to be down
    - When a terminal is detected to be up (sent when monitoring is started or restored)

Monitoring with LLDP

1. Using the TTL which is a required item in the data portion of an LLDP frame, a down condition is determined if LLDP is not received within the TTL time.
2. Monitoring starts when an LLDP frame is first received.
3. This monitoring can be specified individually by port.
4. If sending a mail notification or SNMP trap is enabled, they are sent in the following cases.
    - When a terminal is detected to be down
    - When a terminal is detected to be up (sent when monitoring is started or restored)
    - When a terminal stopped LLDP functionality

Related Commands

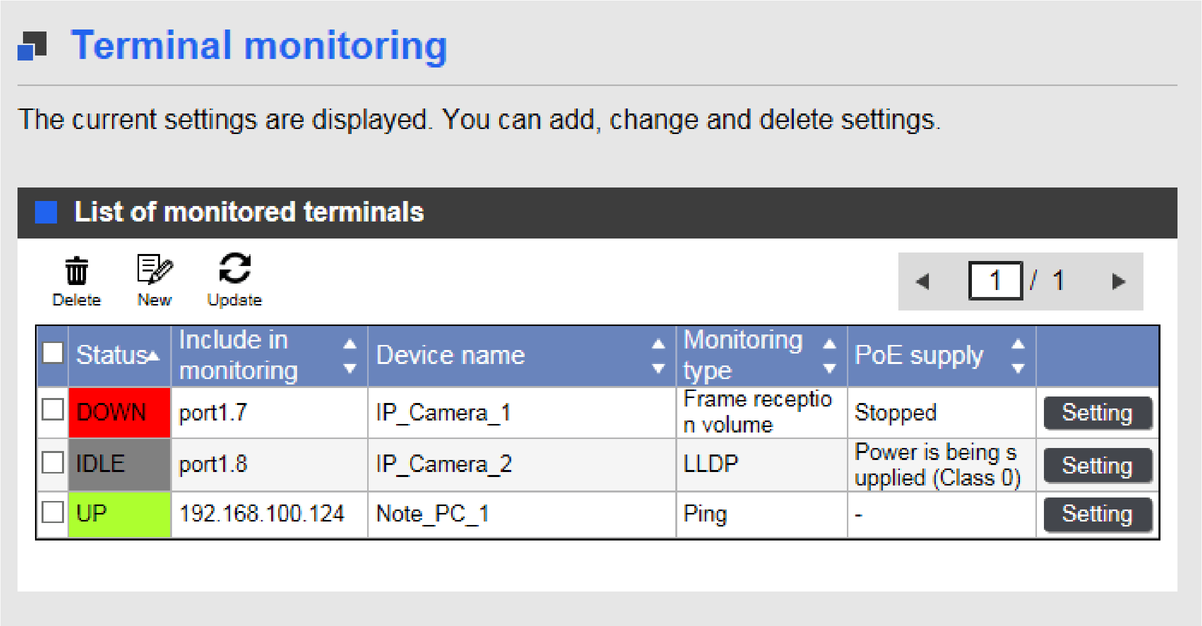
This function does not support settings via commands.

Settings via the Web GUI

Terminal monitoring settings can be done from **[Advanced settings]-[Terminal monitoring]** of the Web GUI. Details on the settings in each screen can be referenced via the Web GUI help.

Terminal monitoring top page

The top page of terminal monitoring is shown below.



Terminal monitoring

The current settings are displayed. You can add, change and delete settings.

List of monitored terminals

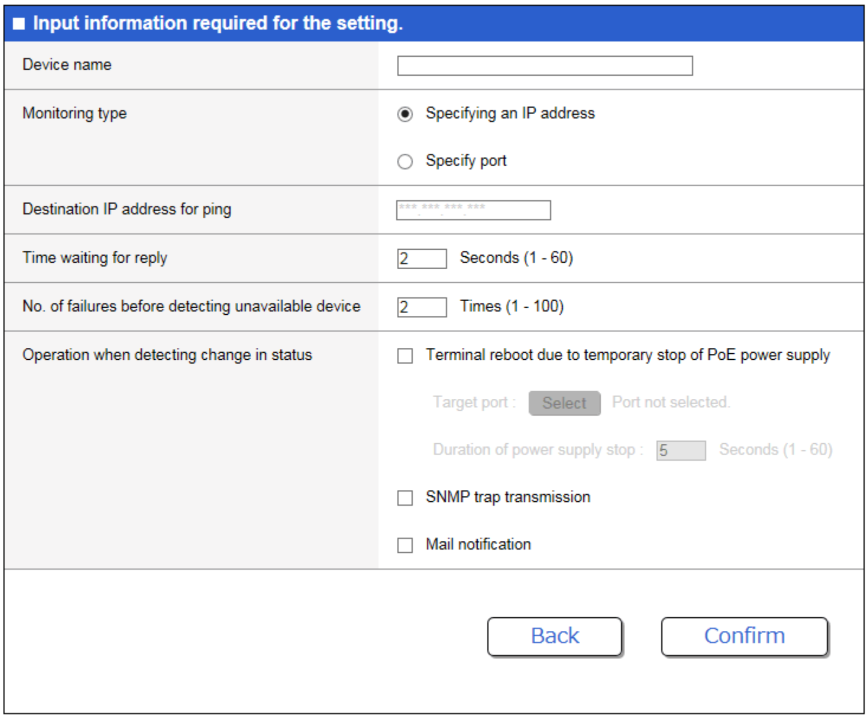
□	Status▲	Include in monitoring	Device name	Monitoring type	PoE supply	
□	DOWN	port1.7	IP_Camera_1	Frame reception volume	Stopped	Setting
□	IDLE	port1.8	IP_Camera_2	LLDP	Power is being supplied (Class 0)	Setting
□	UP	192.168.100.124	Note_PC_1	Ping	-	Setting

- If you want to newly add a terminal for monitoring, press the **New** icon.
- If you want to change a currently-specified monitored terminal, press the [**Setting**] button in the list. If you want to delete a currently-specified monitored terminal, select the **check box** of that terminal, and press the [**Delete**] button.
- If you want to ascertain the current state of the monitored terminal for which you are making settings, press the [**Update**] button to acquire the latest state.

Adding or modifying a monitored terminal

The method for adding a new monitored terminal, or for making changes, is shown below for each method of monitoring.

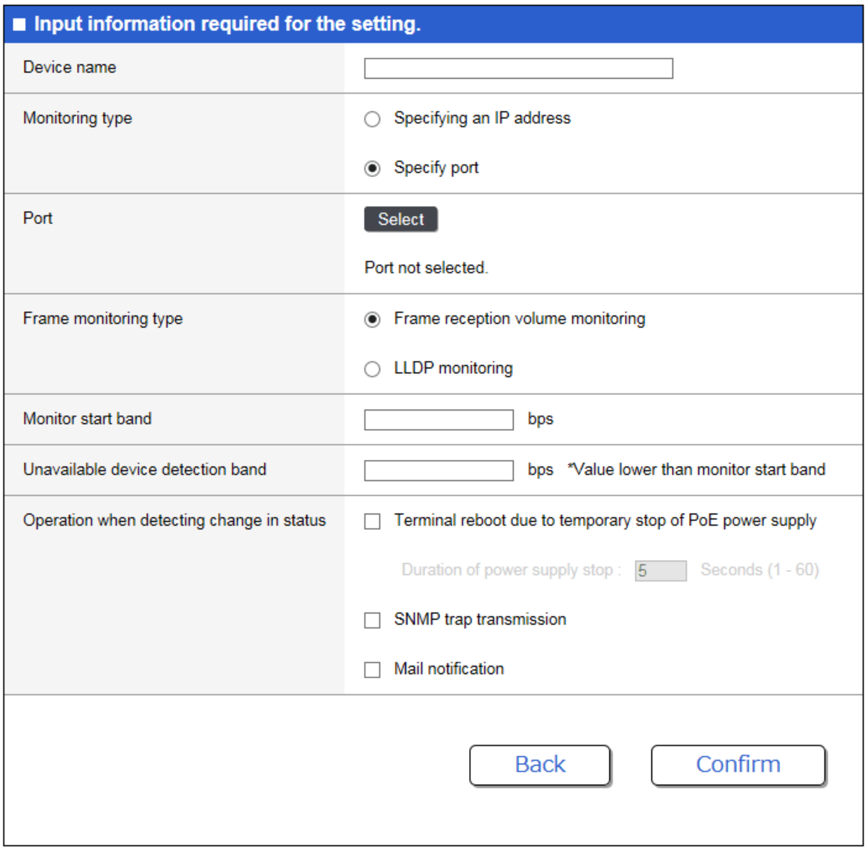
1. Monitoring by ping



Input information required for the setting.

Device name	
Monitoring type	● Specifying an IP address ○ Specify port
Destination IP address for ping	***.***.***.***
Time waiting for reply	2 Seconds (1 - 60)
No. of failures before detecting unavailable device	2 Times (1 - 100)
Operation when detecting change in status	□ Terminal reboot due to temporary stop of PoE power supply Target port : Select Port not selected. Duration of power supply stop : 5 Seconds (1 - 60) □ SNMP trap transmission □ Mail notification

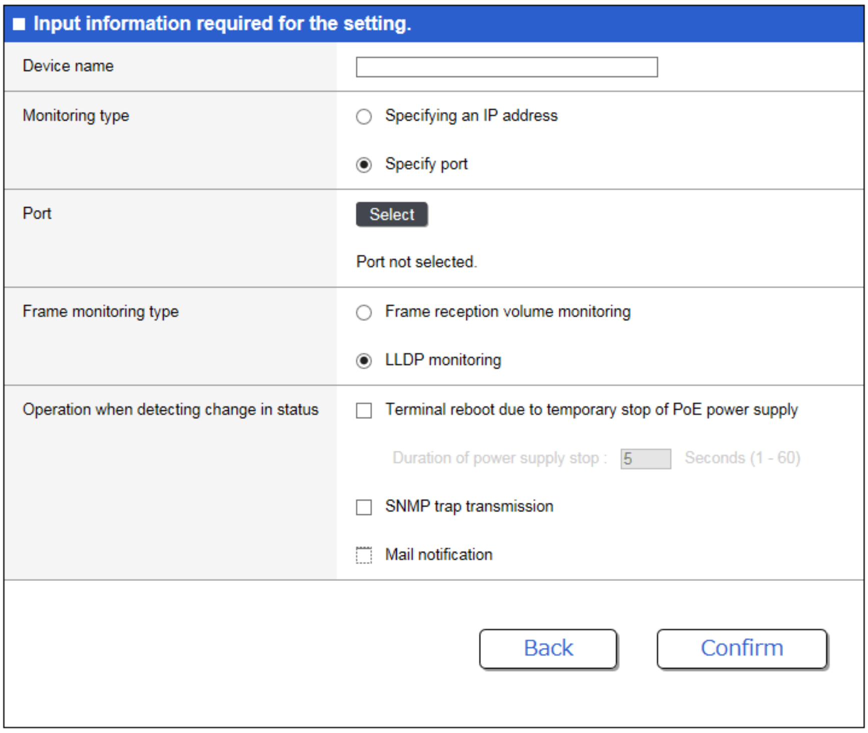
2. Frame reception volume monitoring



■ Input information required for the setting.

Device name	
Monitoring type	○ Specifying an IP address ● Specify port
Port	Select Port not selected.
Frame monitoring type	● Frame reception volume monitoring ○ LLDP monitoring
Monitor start band	bps
Unavailable device detection band	bps *Value lower than monitor start band
Operation when detecting change in status	□ Terminal reboot due to temporary stop of PoE power supply Duration of power supply stop : 5 Seconds (1 - 60) □ SNMP trap transmission □ Mail notification

3. LLDP reception interval monitoring



■ Input information required for the setting.

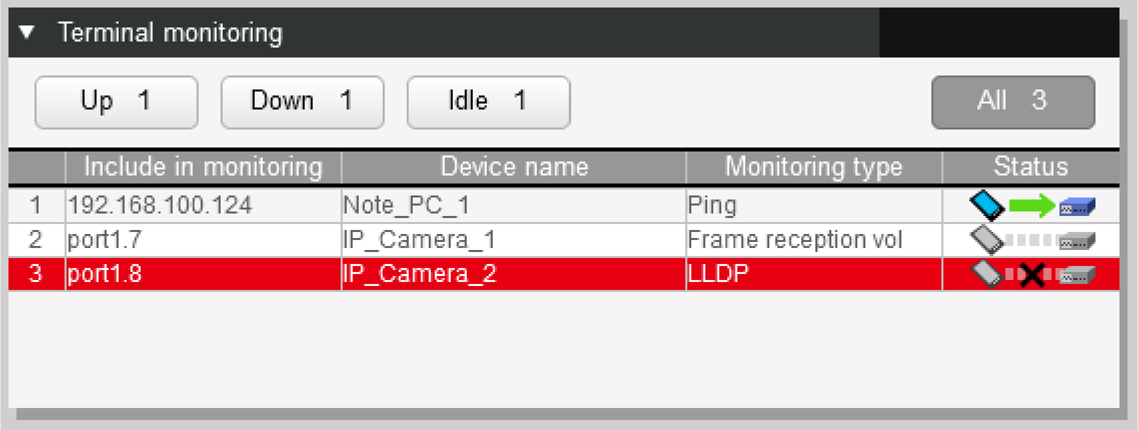
Device name	
Monitoring type	○ Specifying an IP address ● Specify port
Port	Select Port not selected.
Frame monitoring type	○ Frame reception volume monitoring ● LLDP monitoring
Operation when detecting change in status	□ Terminal reboot due to temporary stop of PoE power supply Duration of power supply stop : 5 Seconds (1 - 60) □ SNMP trap transmission □ Mail notification

- **Restart terminal by controlling PoE supply** can be specified only for models that support PoE supply.
- **Use the traffic observation function when deciding the monitoring start threshold value and the down detection threshold value settings for frame reception volume monitoring.**
- If you want mail notification to be sent in the event of a fault, you must separately make **mail notification settings**.
  For details, refer to **Technical reference: [Maintenance and operation functions] - [Mail**

notification] and to **Web GUI help: [Management] - [Mail notification]**.

Checking the state of a monitored terminal

The state of a specified monitored terminal can be checked in the **terminal monitoring gadget of the dashboard**.



	Include in monitoring	Device name	Monitoring type	Status
1	192.168.100.124	Note_PC_1	Ping	→
2	port1.7	IP_Camera_1	Frame reception vol	
3	port1.8	IP_Camera_2	LLDP	✕

- For each monitored terminal, this shows the monitoring target, model name, monitoring type, and status.
- The following three states are shown as the state of the monitored terminal.
  - **Idle** : Monitoring is not yet being performed:
  - **Up** : The monitored terminal is operating correctly:
  - **Down** : The monitored terminal is not operating correctly: ✕
- Point the mouse cursor above a status column to show the status for that monitored terminal.
- If you click the **[Idle]** , **[Up]**, or **[Down]** button in the upper part of the dashboard, only the monitored terminals that are in the corresponding state are shown. (The **[All]** button shows terminals of all states.)
- If not even one monitor terminal is registered, the display indicates “No monitored terminals are registered.”

Points of Caution

None

Related Documentation

- Performance Observations

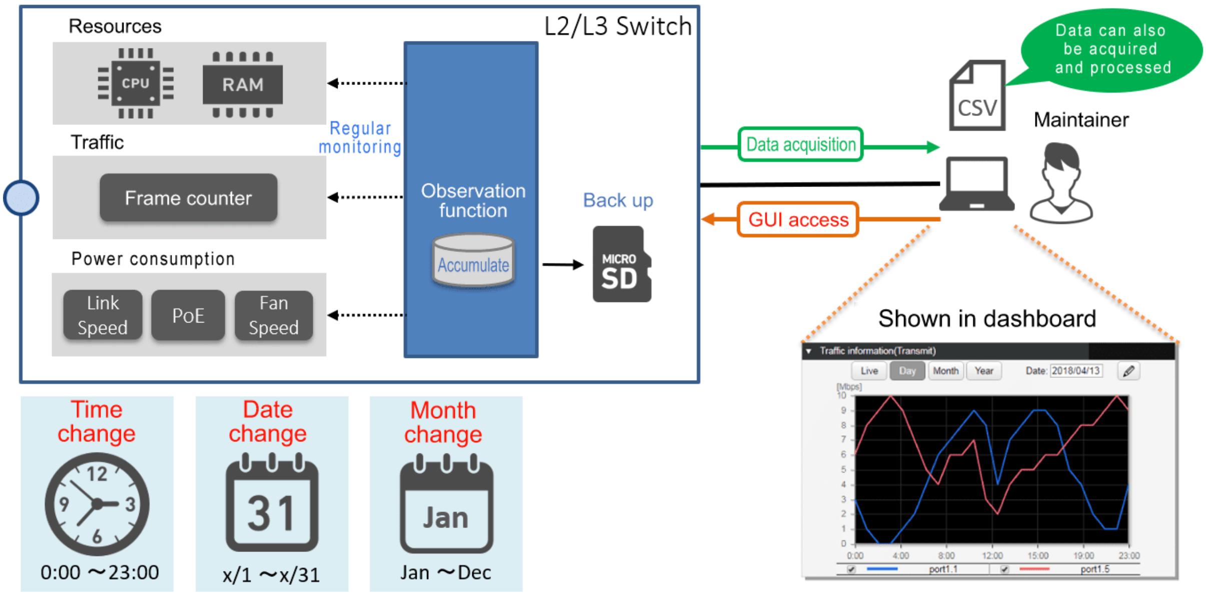
Performance Observations

Function Overview

This product provides a mechanism for constantly observing the system’s performance.
An overview of the function is given below.

Items for standing observation

Resource (CPU, memory) usage amount
Traffic volume, such as bandwidth usage amount based on the port's frame counter
Power consumption estimated based on the link speed, PoE power supply level, and FAN rpm



This product constantly observes the following three types of data.

1. Resource usage amount: CPU and memory usage amount
2. Traffic volume: The volume of communication port bandwidth used (transmission/reception)
3. Power consumption: Estimated based on the link speed, PoE power supply level, and fan RPM

Based on the results of observation, one year’s worth of the following change data is accumulated inside this product.

- **Hourly change**: Change for each hour (e.g. 0:00, 1:00, ...)
- **Daily change**: Change for each day of each month (e.g. 1/1, 1/2, ...)
- **Weekly change**: Change for each day of the week (e.g. SUN, MON, ...)
- **Monthly change**: Change for each month (e.g. Jan, Feb, ...)

The accumulated data **can be backed up to an SD card. ***
By accessing this product via the Web GUI, the maintenance personnel can view the various types of change data including live data in the dashboard, and can also acquire the accumulated result in a PC.
Since the acquired data is in *CSV format, it can also be manipulated using spreadsheet software on a PC.
Maintenance personnel can use this functionality for the following purposes.

- Determine the short-term communication status
- Predict long-term network equipment demand
- Notice wasteful power consumption by determining current power consumption levels

Definition of Terms Used

None

Function Details

Resource and traffic usage observation

Starting immediately after boot, this device automatically **observes the CPU and memory and the transmit/receive throughput of each port every second. ***
The observed data is *normalized using a moving average, and **one year of data is saved in RAM**.

Observation data backup

Backup of observation data can be specified only in the Web GUI.
Backup of observation data **assumes that an SD card is inserted** in this device.
If backup is enabled, the most recent hour of observation data every hour starting at the point it was enabled (e.g., 1:00, 2:00 ...) is saved on the SD card.
The saved data is dedicated binary data of this device.
The save-destination on the SD card and the file name of the backup data file are as follows.

1. Resource information
    1. **Hourly change data**
       /[model name]/data/resource/YYYYMM_smsys_res_monitor_hour.bin
    2. **Daily change data (data for each day)**
       /[model name]/data/resource/YYYYMM_smsys_res_monitor_day.bin
    3. **Weekly change data**
       /[model name]/data/resource/YYYYMM_smsys_res_monitor_week.bin
    4. **Monthly change data**
       /[model name]/data/resource/YYYY_smsys_res_monitor_month.bin
2. Traffic information
    1. **Hourly change data**
       /[model name]/data/trf/YYYYMM_trf_bandwidth_hour.bin
    2. **Daily change data**
       /[model name]/data/trf/YYYYMM_trf_bandwidth_day.bin
    3. **Weekly change data**
       /[model name]/data/trf/YYYYMM_trf_bandwidth_week.bin
    4. **Monthly change data**
       /[model name]/data/trf/YYYY_trf_bandwidth_month.bin
3. Power consumption information
    1. **Hourly change data**
       /[model name]/data/power/YYYYMM_smsys_pwr_monitor_hour.bin
    2. **Daily change data**
       /[model name]/data/power/YYYYMM_smsys_pwr_monitor_day.bin
    3. **Weekly change data**
       /[model name]/data/power/YYYYMM_smsys_pwr_monitor_week.bin
    4. **Monthly change data**
       /[model name]/data/power/YYYY_smsys_pwr_monitor_month.bin

- **[Model name]** is the following.
    - For the SWX2320-16MT: **swx2320**
    - For the SWX2322P-16M: **swx2322p**
    - For the SWX3220-16MT/16TMs: **swx3220**
    - For the SWX3200-28GT/52GT: **swx3200**
    - For the SWX3100-10G/18GT: **swx3100**
    - For the SWX2310P-10G/18G/28GT: **swx2310p**
    - For the SWX2310-10G/18GT/28GT/52GT: **swx2310**
- **YYYY: Year, MM: month** will be set.
- Since this is a proprietary Yamaha format, it cannot be referenced.

Observation data export

Observation data can be exported to a computer only via the web GUI.

Data is exported as *multiple CSV files compressed in zip format. *
The structure of the compressed files are given below.

1. When resource observation data is exported
    - zip file name: **YYYYMMDDhhmmss_resource_csv.zip**
    - Folder structure

      ```
      YYYYMMDDhhmmss_resource_csv
          +- 20170922_resource_hour.csv ①
          +-     :
          +- 20170925_resource_hour.csv ②
          +- 201709_resource_day.csv ③
      ```

      ① CPU, memory, and hourly change data for September 22, 2017

      ② CPU, memory, and hourly change data for September 25, 2017

      ③ CPU, memory, and daily change data for September 2017
2. When transmission traffic observation data is exported
    - zip file name: **YYYYMMDDhhmmss_trf_tx_csv.zip**
    - Folder structure

      ```
      YYYYMMDDhhmmss_trf_tx_csv
          +- 20170922_trf_tx_hour.csv ①
          +-     :
          +- 20170925_trf_tx_hour.csv ②
          +- 201709_trf_tx_day.csv ③
      ```

      ① Transmission traffic and hourly change data for September 22, 2017

      ② Transmission traffic and hourly change data for September 25, 2017

      ③ Transmission traffic and daily change data for September 2017
3. When reception traffic observation data is exported
    - zip file name: **YYYYMMDDhhmmss_trf_rx_csv.zip**

    - Folder structure

```
YYYYMMDDhhmmss_trf_rx_csv
    +- 20170922_trf_rx_hour.csv ①
    +-     :
    +- 20170925_trf_rx_hour.csv ②
    +- 201709_trf_rx_day.csv ③
```

① Reception traffic and hourly change data for September 22, 2017

② Reception traffic and hourly change data for September 25, 2017

③ Reception traffic and daily change data for September 2017

4. If power consumption observation data was exported
    - zip file name: **YYYYMMDDhhmmss_pwr_csv.zip**
    - Folder structure

```
YYYYMMDDhhmmss_pwr_csv
    +- 20170922_pwr_hour.csv ①
    +-     :
    +- 20170925_pwr_hour.csv ②
    +- 201709_pwr_day.csv ③
```

① Power consumption and hourly change data for September 22, 2017

② Power consumption and hourly change data for September 25, 2017

③ Power consumption and daily change data for September 2017

- **YYYYMMDDhhmmss** specifies the date and time when the data was exported (date and time the file was created).

Related Commands

This function does not support settings via commands.

Settings via the Web GUI

Performance observation can be controlled from the following pages of the Web GUI.

- Viewing the resource usage amount
    - This can be viewed in the **[Dashboard]** item **[Resource information (graph)]**.
- Viewing the traffic usage amount
    - This can be viewed in the **[Dashboard]** item **[Traffic information (graph)]**.
- Viewing power consumption data
    - Data can be viewed in the **[Power consumption information (graph)]** field on the **[Dashboard]**.
- Backing up, clearing, or exporting observation data
    - Select **[Management]** and then settings can be specified in the **[Maintenance] - [Summary data management]** field.

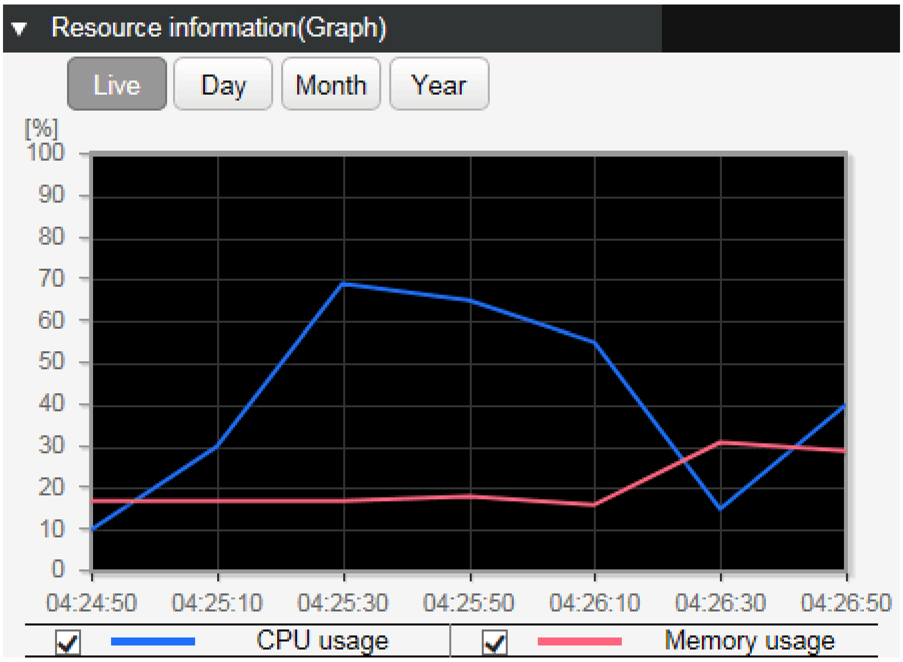
      (Data can also be cleared or exported using the **menu buttons** (•••) in each **[Dashboard]** gadget.)

Details on how to view and make settings in each screen can be referenced via the Web GUI help.

Viewing the resource usage amount

The resource information (graph) screen is shown below.

- Example when **Live** is selected for resource information (graph)



1. The graph rendering can be changed using the following buttons.
   - Current situation: **Live**
     The various current usage ratios are obtained at one-second intervals and shown on the graph.
   - Hourly change: **Day**

     The various usage ratios for the specified day are shown at one-hour intervals on the graph.
     To specify the day, use the day-specifying box in the upper right of the gadget.
   - Daily change: **Month**

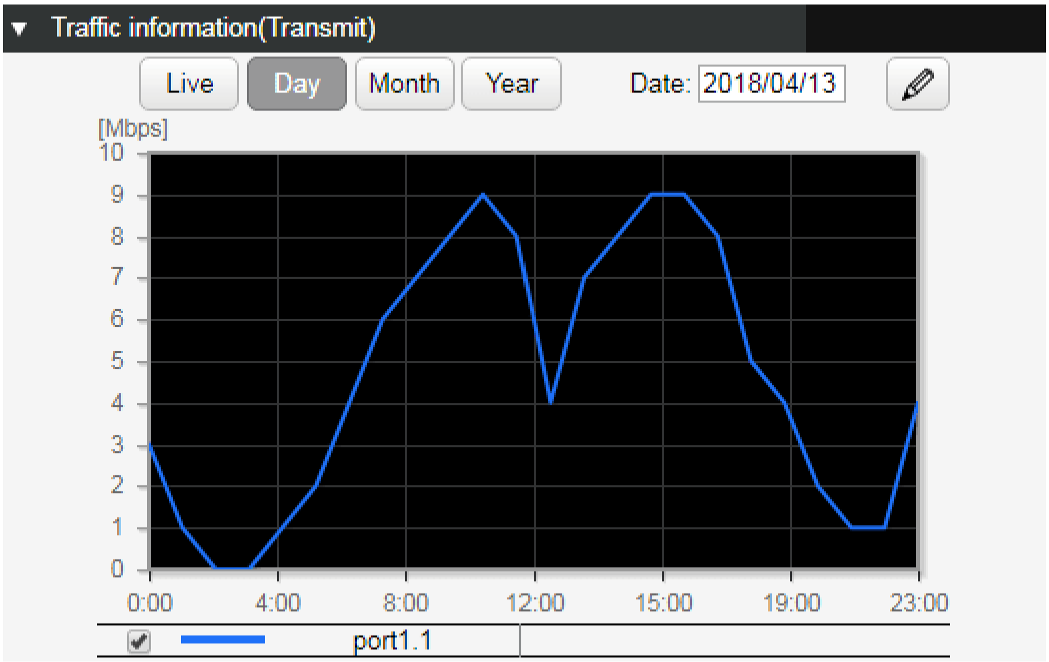
     The various usage ratios for the specified month are shown at one-day intervals.
     To specify the month, use the month-specifying box in the upper right of the gadget.
   - Monthly change: **Year**

     The various usage ratios for the specified year are shown at one-month intervals.
     To specify the year, use the select box in the upper right of the gadget.
   - It is not currently possible to reference changes in the day of the week.
2. If the CPU and memory usage ratios exceed **80%**, then *a warning message is shown on the dashboard. *
   If the ratio falls below 80% after having exceeded 80%, the warning is automatically cleared.

Viewing the traffic usage amount

The traffic usage amount (graph) screen is shown below.

- Example of when traffic usage amount (graph) **Day** is selected / Example of **reception traffic**



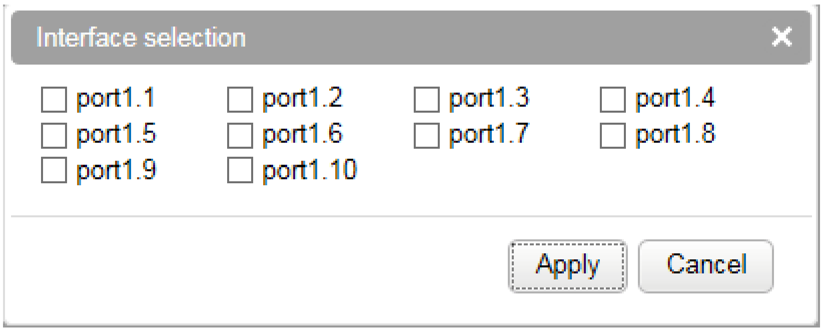
1. The traffic usage amount of each port can be shown separately for **transmission** and **reception**.
2. The graph rendering can be changed using the following buttons.
   - Current situation: **Live**

     The various current usage ratios are obtained at one-second intervals and shown on the graph.
     The most recent **two minutes** of the obtained data is held and rendered on the graph.
   - Hourly change: **Day**

     The various usage ratios for the specified day are shown at one-hour intervals on the graph.
     To specify the day, use the day-specifying box in the upper right of the gadget.
   - Daily change: **Month**

     The various usage ratios for the specified month are shown at one-day intervals.
     To specify the month, use the month-specifying box in the upper right of the gadget.
   - Monthly change: **Year**

     The various usage ratios for the specified year are shown at one-month intervals.
     To specify the year, use the select box in the upper right of the gadget.
   - It is not currently possible to reference changes in the day of the week.
3. To select the interface to be shown, click the **[Interface selection] menu button** (•••) and then select the interface in the following screen.

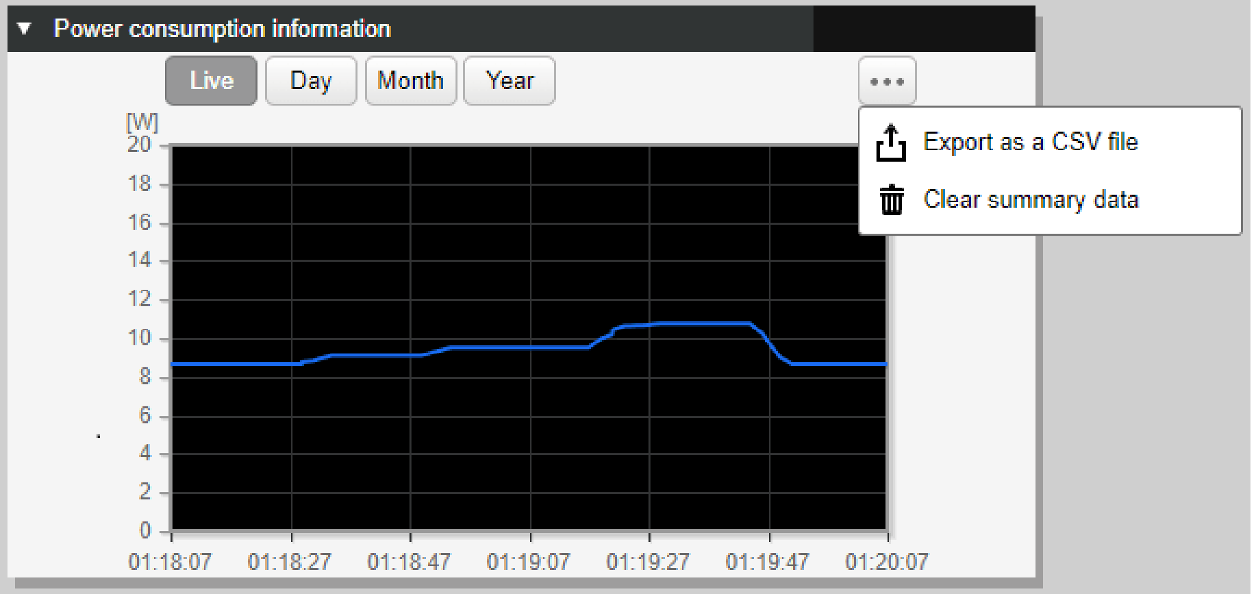


4. If the traffic usage ratio exceeds 60%, a warning message is shown on the dashboard.
   If the ratio falls below 50% after having exceeded 60%, the warning is automatically cleared.

Viewing power consumption data

The power consumption information (graph) screen is shown below.

- Example of power consumption information (graph) when **Live** is selected.



1. The graph rendering can be changed using the following buttons.
   - Current situation: **Live**
     This shows the current power consumption levels measured at one-second intervals.
   - Hourly change: **Day**

     This shows the power consumption levels on the specified date at one-hour intervals.
     To specify the day, use the day-specifying box in the upper right of the gadget.
   - Daily change: **Month**

     This shows the power consumption levels during the specified month at one-day intervals.
     To specify the month, use the month-specifying box in the upper right of the gadget.
   - Monthly change: **Year**

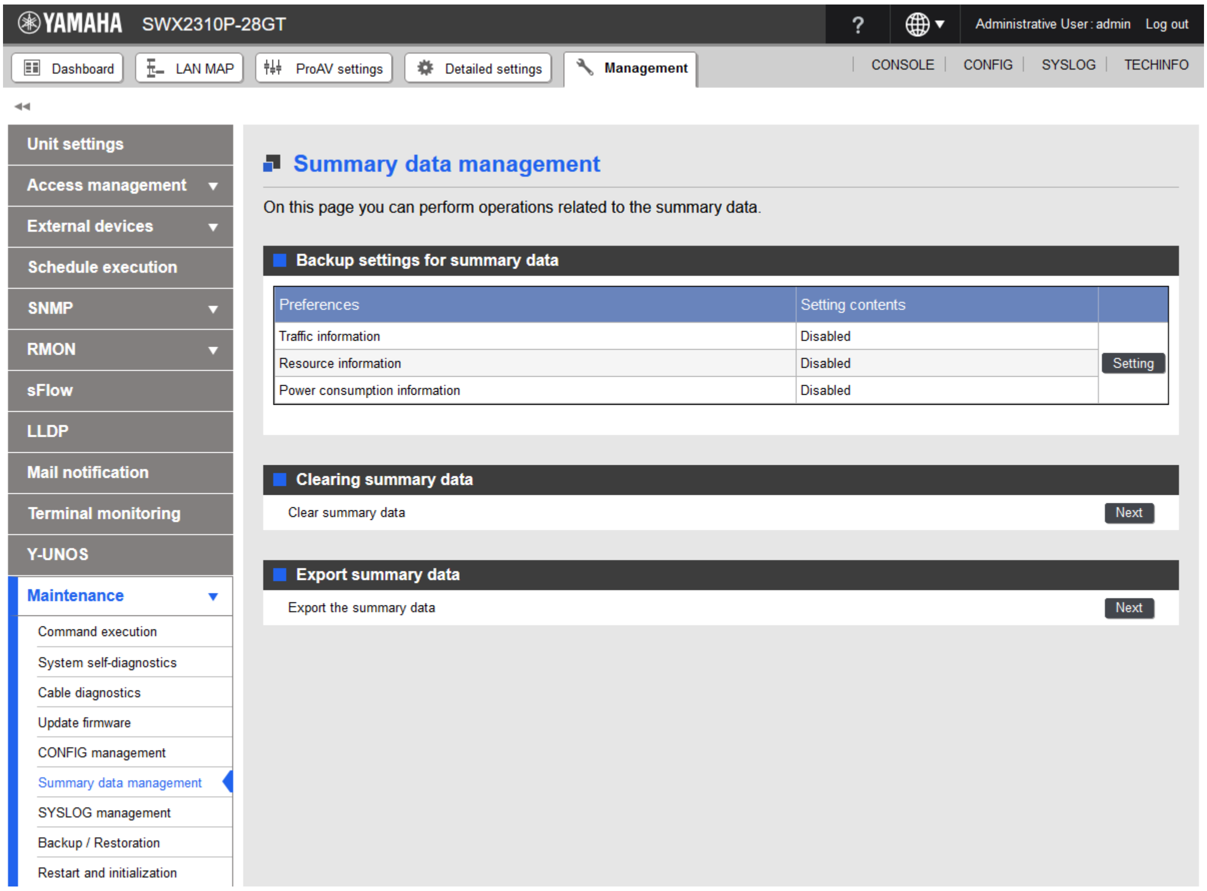
     This shows the power consumption levels during the specified year at one-month intervals.
     To specify the year, use the select box in the upper right of the gadget.
   - It is not currently possible to reference changes in the day of the week.
2. The following recommended methods reduce power consumption.
   - Decrease the link speed of ports with low bandwidth usage.
   - Use the Schedule execution function to shut down unused ports and PoE power supply at midnight and on holidays.

Backing up, clearing, or exporting observation data

Backup, clearing, and exporting of observation data is performed from **[Management] - [Maintenance] - [Summary data management]**.

(Data can also be cleared or exported using the **menu buttons** (•••) in each **[Dashboard]** gadget.)
The [Summary data management] screen is shown below.

- Summary data management screen (top page)



Summary data management

On this page you can perform operations related to the summary data.

Backup settings for summary data

Preferences	Setting contents
Traffic information	Disabled
Resource information	Disabled
Power consumption information	Disabled

Clearing summary data

Clear summary data

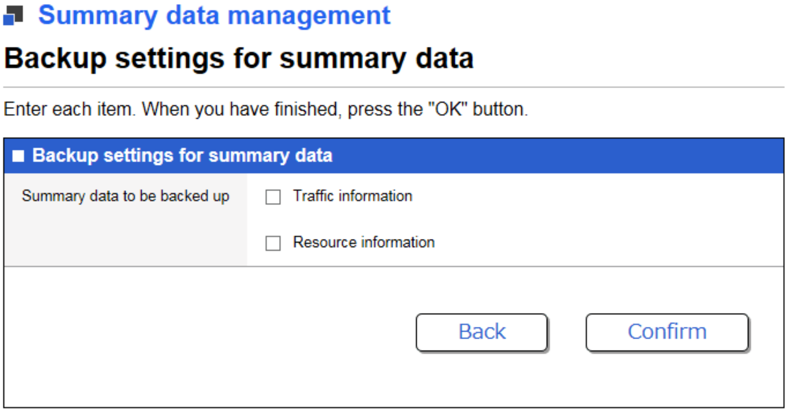
Export summary data

Export the summary data

Observation data backup settings

Make the observation data backup settings from **[Top page] - [Backup settings for summary data]**.
The screen that appears after you press the **[Settings]** button is shown below.

- Observation data backup settings screen



Summary data management

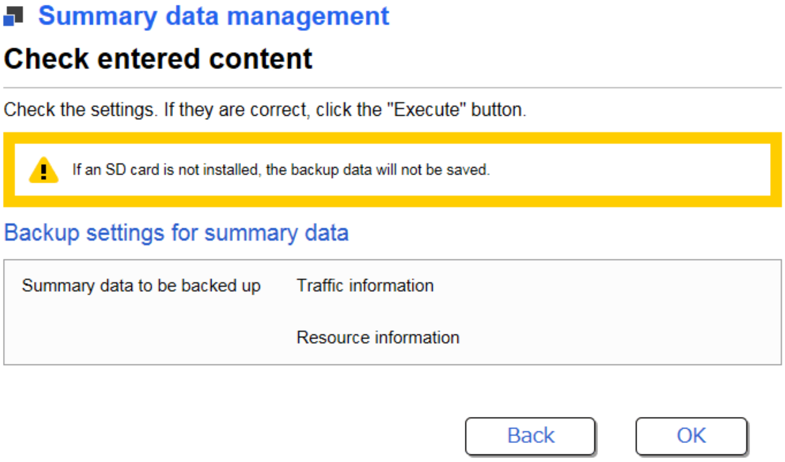
Backup settings for summary data

Enter each item. When you have finished, press the "OK" button.

Backup settings for summary data

Summary data to be backed up: □ Traffic information □ Resource information

- Place a check mark in the check box of the summary data for which you want to enable backup, and then press the **[Confirm]** button.
After you press the button, the following screen appears.



Summary data management

Check entered content

Check the settings. If they are correct, click the "Execute" button.

If an SD card is not installed, the backup data will not be saved.

Backup settings for summary data

Summary data to be backed up	Traffic information Resource information

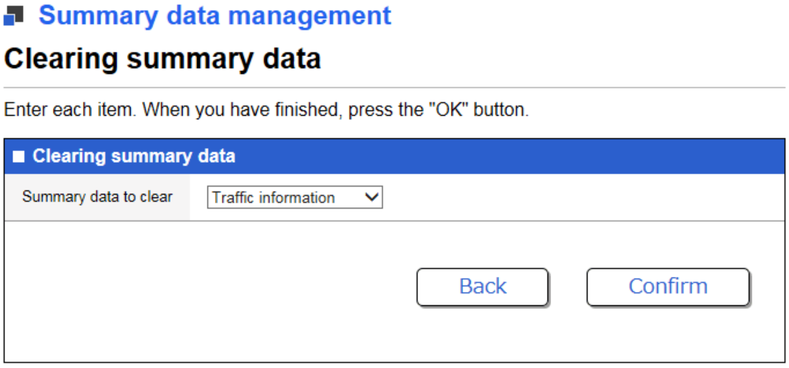
- If you decide to cancel this setting, press the **[Back]** button in each screen.

Clearing observation data

Clear the observation data from **[Top page] - [Clearing summary data]**.

(Data can also be cleared using the **menu buttons** (***) in each **[Dashboard]** gadget.)
The screen that appears after you press the **[Next]** button is shown below.

- Clear observation data screen



Summary data management

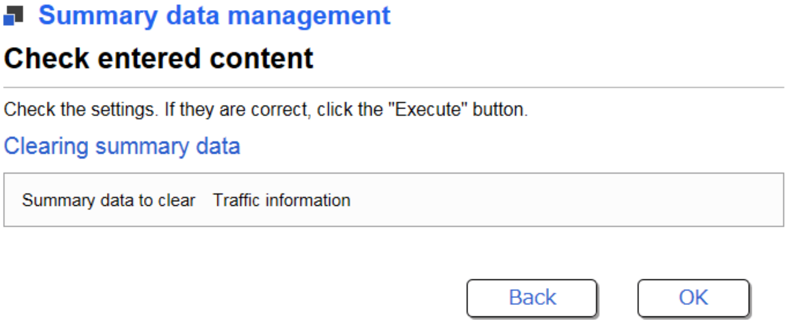
Clearing summary data

Enter each item. When you have finished, press the "OK" button.

Clearing summary data

Summary data to clear	Traffic information

- In the select box, choose the summary data to be cleared and then click the **[Confirm]** button.
After you press the button, the following screen appears.



Summary data management

Check entered content

Check the settings. If they are correct, click the "Execute" button.

Clearing summary data

Summary data to clear	Traffic information

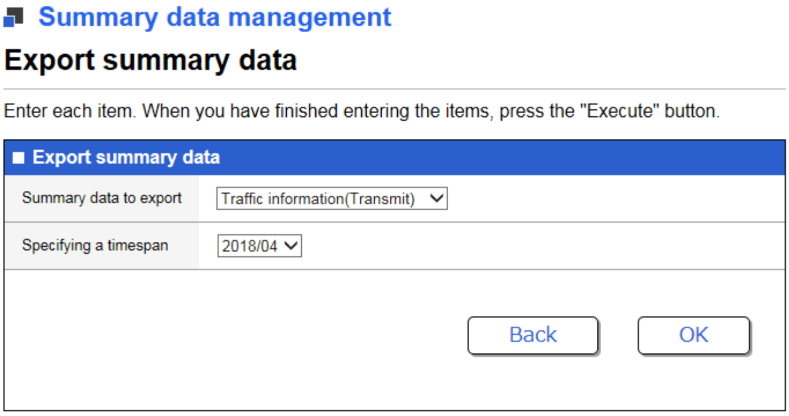
- To cancel the operation, click the [Back] button displayed in each screen.

Exporting observation data

Export the observation data from **[Top page] - [Export summary data]** in the summary data management.

(Data can also be exported using the **menu buttons** (***) in each **[Dashboard]** gadget.)
The screen that appears after you press the [Next] button is shown below.

- Observation data export screen



Summary data management

Export summary data

Enter each item. When you have finished entering the items, press the "Execute" button.

■ Export summary data

Summary data to export	Traffic information(Transmit)
Specifying a timespan	2018/04

- In the select box, choose the observation data to be exported to the computer used to access the web GUI. Then select the time period of observation data to be exported.
  After selecting the period, click the **[OK]** button to download the zip file.
- To cancel the operation, click the **[Back]** button.

Points of Caution

None

Related Documentation

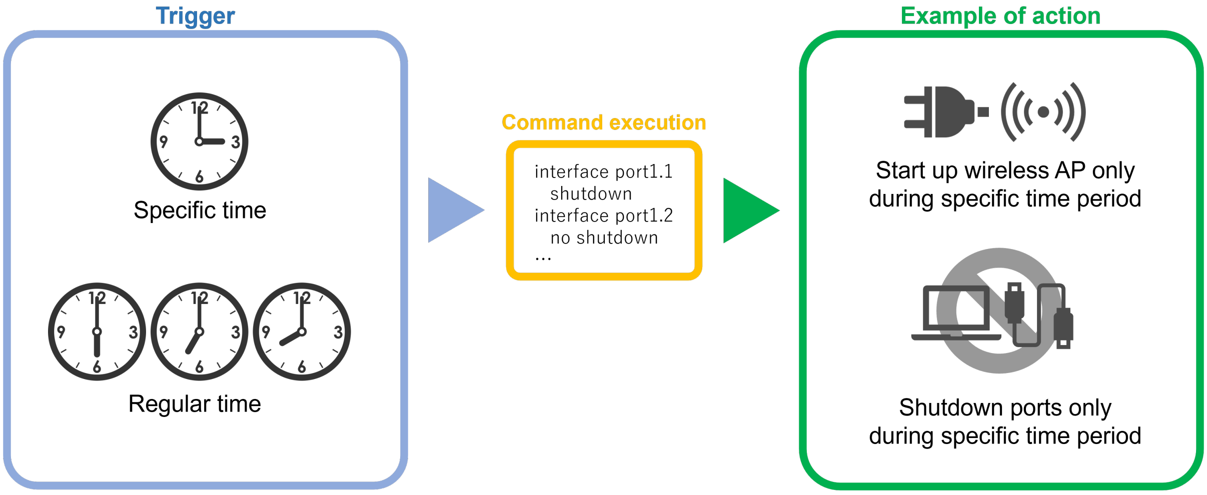
None

Schedule Function

Function Overview

Scheduling functionality is used to execute specific processes when any particular time or event occurs. This functionality enables the following types of actions using a Yamaha network switch.

- Apply QoS to a specific VLAN only during a specific period.
- Supplies PoE power to wireless LAN access points only during the specified period.
- Periodically saves “tech-support” information in microSD memory.


Trigger
Specific time
Regular time
Command execution
Example of action
Start up wireless AP only during specific time period
Shutdown ports only during specific time period

```
interface port1.1
  shutdown
interface port1.2
  no shutdown
...
```

Definition of Terms Used

Trigger

General term for conditions/criteria, such as that the internal clock time matches a specified time or that a specific event occurs.

Time Trigger

Condition that the internal clock time matches a specified time.

Event Trigger

Condition that a specific event occurs.

Action

Action executed when a trigger is activated.

Function Details

Scheduling functionality involves specifying “triggers” and actions, which are the two parameter settings for executing specific process “actions” when a particular specified time or event trigger occurs.

Time Trigger

Time triggers can be specified in terms of year, month, day, hour, minute, and second.

Time triggers are specified using the **schedule** command.
Available setting parameters are indicated below.

Type		Specification method	Setting value example
Date	Month 1-12	One specific month (such as only December)	12
		Multiple specific months (such as only January and February)	1,2
		Range from specific month to December (such as February to December)	2-
		Range from specific month to specific month (such as February to July)	2-7
		Range from January to specific month (such as January to July)	-7
		Every month	*
	Day 1-31	One specific day (such as day 1 only)	1
		Multiple specific days (such as days 1 and 2 only)	1,2
		Range from specific day to last day (such as day 2 to month-end)	2-
		Range from specific day to specific day (such as days 2 to 7)	2-7
		Range from day 1 to specific day (such as days 1 to 7)	-7
		Every day	*
		Specific day-of-week only (such as Monday only)	mon
		Multiple specific days of the week only (such as Saturday and Sundays only)	sat,sun
		Range from specific day-of-week to specific day-of-week (such as Monday to Friday)	mon-fri
		Range from Sunday to specific day-of-the-week (such as Sunday to Friday)	-fri

Type		Specification method	Setting value example
Hours, minutes, seconds	Hours 0-23	Specific hour only (such as 23:00 only)	23
		Multiple specific hours only (such as 01:00 and 22:00 only)	1,22
		Range from specific hour to 23:00 (such as 02:00 to 23:00)	2-
		Range from specific hour to specific hour (such as 02:00 to 21:00)	2-21
		Range from hour 00:00 to specific hour (such as 00:00 to 21:00)	-21
		Each hour	*
	Minutes 0-59	One specific minute only (such as minute 59 only)	59
		Multiple specific minutes only (such as minutes 1 and 50 only)	1,50
		Range from specific minute to minute 59 (such as minutes 2 to 59)	2-
		Range from specific minute to specific minute (such as minutes 2 to 50)	2-50
		Range from minute 0 to specific minute (such as minutes 0 to 50)	-50
		Each minute	*
	Seconds 0-59	One specific second only (such as second 59 only) This setting may be omitted.	59

Event Trigger

Either of the following events can be specified as an event trigger.

Time triggers are specified using the **schedule** command.
Events that can be specified are indicated below.

Type	Description
startup	Action is executed when startup occurs.
sd-attached	Action is executed when a microSD card is inserted.

Action

Processes executed when a time trigger or event trigger is activated are called actions.
To specify actions, use the **schedule template** command to switch to the schedule template mode and then specify the action using the **cli-command** or **script** command.
The following two actions are available.

Action	Command for settings	Description
Executes specified command	cli-command command	Executes the specified commands in ascending order of ID numbers.

Action	Command for settings	Description
Executes Specified Script	script command	Executes the character strings in the **first 100 lines** of the specified file **/(model name)/schedule/script.txt** in external memory (microSD) as a command.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operating mode	Commands	Description
Global configuration mode	schedule	Specifies a schedule template ID that specifies the trigger and defines the action.
	schedule template	Specifies the schedule template ID and switches to the schedule template mode.
Schedule template mode	description	Specifies description of the schedule template.
	action	Enables/disables the schedule template. Use disable to temporarily disable schedule function.
	cli-command	Defines command executed when trigger is activated.

Setting Examples

Supplying PoE power to wireless LAN access points only during specified hours

Supply PoE power to wireless LAN access points connected to port1.1 and port1.2 on weekdays only between 8:00 and 17:00.

```
Yamaha#
Yamaha# configure terminal
Yamaha(config)# schedule 1 time */mon-fri 8:00:00 1
Yamaha(config)# schedule template 1
Yamaha(config-schedule)# cli-command 1 configure terminal
Yamaha(config-schedule)# cli-command 2 interface port1.1-2
Yamaha(config-schedule)# cli-command 3 power-inline enable
Yamaha(config-schedule)# exit
Yamaha(config)#
Yamaha(config)# schedule 2 time */mon-fri 17:00:00 2
Yamaha(config)# schedule template 2
Yamaha(config-schedule)# cli-command 1 configure terminal
Yamaha(config-schedule)# cli-command 2 interface port1.1-2
Yamaha(config-schedule)# cli-command 3 power-inline disable
Yamaha(config-schedule)# end
Yamaha#
```

Obtaining internal information when microSD memory is inserted

Automatically saves tech-support in microSD memory when microSD card is inserted.

```
Yamaha#
Yamaha# configure terminal
Yamaha(config)# schedule 1 event sd-attached 1
Yamaha(config)# schedule template 1
Yamaha(config-schedule)# cli-command 1 copy tech-support sd
Yamaha(config-schedule)# end
Yamaha#
```

Unavailable Commands

The following commands cannot be executed for the schedule function.

- backup system
- baudrate select
- boot prioritize sd / no boot prioritize sd
- certificate user
- Commands that begin 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 that begin with “ntpdate” or “no ntpdate”
- password / no password
- password-encryption / no password-encryption
- ping /ping6
- quit
- reload
- remote-login
- restart
- restore system
- schedule / no schedule
- schedule template / no schedule template
- Commands that begin with “show”
- ssh
- ssh-server host key generate
- Commands that begin with “stack” or “no stack”
- startup-config select / no startup-config select
- telnet

- traceroute / traceroute6

SYSLOG

The schedule function outputs the following SYSLOG messages.

Level	Output	Description
Info	[SCHEDULE]:inf:ID:X command is done	The schedule template ID:X command was executed when the trigger was activated.
	[SCHEDULE]:inf:ID:X script is done	The schedule template ID:X script was executed when the trigger was activated.
Error	[SCHEDULE]:err:ID:X cmd[ID][COMMAND] is prohibited to execute	Execution of the prohibited command COMMAND in schedule template ID:X was suppressed.
	[SCHEDULE]:err:ID:X cmd[ID][COMMAND] is failed to execute	Command failed in schedule template ID:X due to invalid command format or inappropriate parameter setting.
	[SCHEDULE]:err:ID:X microSD is not mounted	Script execution failed at schedule template ID:X because microSD was not inserted.
	[SCHEDULE]:err:ID:X failed to get the schedule forlder path	Script execution failed at schedule template ID:X because the expected directory containing the script was not found.
	[SCHEDULE]:err:ID:X script is not found	Script execution failed at schedule template ID:X because the script file was not found.
	[SCHEDULE]:err:ID:X failed to add action to queue	Action failed at schedule template ID:X because action was discarded due to the many actions waiting for execution in the queue.

Points of Caution

- When actions are executed, the cli-command executes actions in ascending ID number order.
- When actions are executed, even if a command specified by the cli-command results in an execution error, the remaining commands are executed.
- If both a cli-command and script command are specified in the same schedule template, then the script command is executed and the cli-command is not executed.
- If multiple triggers are activated simultaneously, then actions are executed in ascending order of schedule template ID number.
- The following precautions apply for devices that include a stack.
  - A “startup” event trigger was not activated in stack member switches.
  - A “sd-attached” event trigger was not activated in stack member switches.
- The trigger is not activated if a stack is enabled and is in the standalone state.
- If the trigger activation time elapses due to the time setting being set manually by the clock set command or being changed by NTP, then any existing triggers scheduled to be activated within 59 seconds of when the current time setting was changed will be activated.
- If the trigger activation time was changed backward manually by the clock set command or by NTP, then the time triggers are checked again starting from the time to which it was set back.
- This function can be used to periodically save the configuration, but periodic rewriting will consume ROM capacity more quickly. ROM failures due to frequent rewriting are not warranted for free repairs, even if they occur during the warranty period.

Related Documentation

- None

Dante Optimization Setting Function

Function Overview

The Dante setting optimization function makes it easy to build the optimal environment for Dante digital audio networks.
The function allows users to easily configure all Dante settings at the same time without having to think about individual Dante settings (such as QoS, IGMP snooping, disable flow control, and disable EEE settings).

Definition of Terms Used

Dante

Dante is a digital audio network specification developed by the Audinate Corporation.

ADECIA

ADECIA is Yamaha's teleconferencing system. It connects processors, microphones, and speakers used for teleconferencing via a LAN (Dante).

ADECIA Components

Devices (teleconferencing processors, microphones, and speaker system) included in ADECIA systems.

LLDP

Protocol for passing device information to neighboring devices.

Function Details

Dante settings can be optimized by the following two methods.

- Automatic optimization settings using LLDP
  - Automatically applies optimized settings by receiving LLDP frames independently from ADECIA components.
- Manual optimization settings via the Web GUI
  - Applies optimized settings from the ProAV settings page indicated in the web GUI of this product.

The settings that can be collectively specified at the same time using the Dante setting optimization function are listed below. For automatic setting optimization using LLDP, the applicable settings will differ depending on the ADECIA component firmware version.

Object of setting	Function	Commands	Applicability		
			LLDP (ADECIA V2.5 or earlier)	LLDP (ADECIA V2.8 or later)	Web GUI
Entire system	Disable flow control	flowcontrol disable	Yes	Yes	Yes
	Enable QoS	qos enable	Yes	Yes	Yes
	Optimize transmission queue by DSCP value	qos dscp-queue 8 2	Yes	Yes	Yes
		qos dscp-queue 26 3	-	Yes	Yes
		qos dscp-queue 34 4	-	Yes	Yes
		qos dscp-queue 46 5	Yes	Yes	Yes

Object of setting	Function	Commands	Applicability		
			LLDP (ADECIA V2.5 or earlier)	LLDP (ADECIA V2.8 or later)	Web GUI
Entire system	Optimize transmission queue by DSCP value	qos dscp-queue 48 5	-	Yes	Yes
		qos dscp-queue 56 7	Yes	Yes	Yes
		qos dscp-queue [not indicated above] 0	Yes	Yes	Yes
		no qos wrr-weight [0 to 7]	-	Yes	Yes
	Always forward linked local multicasts	l2-unknown-mcast forward link-local	-	Yes	Yes
	Enable LLDP	lldp run	-	-	Yes
VLAN interface	Disable shutdown	no shutdown	-	-	Yes
	Flood unknown multicasts	l2-unknown-mcast flood	-	Yes	Yes
	Enable IGMP snooping	ip igmp snooping enable	Yes	Yes	Yes
	Set IGMP snooping version	ip igmp snooping version 3	Yes	Yes	Yes
	Enable IGMP snooping fast-leave function	ip igmp snooping fast-leave auto-assignment	-	Yes	Yes
	Enable IGMP query transmission function	ip igmp snooping querier	Yes	Yes	Yes
	Set IGMP query transmission interval	ip igmp snooping query-interval 30	Yes	Yes	Yes
	Disable IGMP report-suppression function	ip igmp snooping report-suppression disable	-	Yes	Yes
	Enable IGMP report forwarding function	ip igmp snooping report-forward enable	-	Yes	Yes

Object of setting	Function	Commands	Applicability		
			LLDP (ADECIA V2.5 or earlier)	LLDP (ADECIA V2.8 or later)	Web GUI
VLAN interface	Disable IGMP packet TTL value checking function	ip igmp snooping check ttl disable	Yes	Yes	Yes
	Disable IGMP packet RA checking function	ip igmp snooping check ra disable	-	Yes	Yes
	Disable IGMP packet ToS checking function	ip igmp snooping check tos disable	-	Yes	Yes
	Enable data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression enable	-	Yes	Yes
	Set always forwarding PTP packets	l2-mcast flood 224.0.1.129	-	Yes	Yes
		l2-mcast flood 224.0.1.130	-	Yes	Yes
		l2-mcast flood 224.0.1.131	-	Yes	Yes
		l2-mcast flood 224.0.1.132	-	Yes	Yes
		l2-mcast flood 239.254.3.3	-	Yes	Yes

Object of setting	Function	Commands	Applicability		
			LLDP (ADECIA V2.5 or earlier)	LLDP (ADECIA V2.8 or later)	Web GUI
LAN/SFP port	Set QoS trust mode to DSCP	qos trust dscp	Yes	Yes	Yes
	Disable flow control	flowcontrol disable	Yes	Yes	Yes
	Disable EEE	eee disable	Yes	Yes	Yes
	Set MRU	mru 1522	-	Yes	Yes
	Set L2MS filter	l2ms filter disable	-	-	Yes
	Set BPDU filter	spanning-tree bpdu-filter disable	-	-	Yes
	Create LLDP agent	lldp-agent	-	-	Yes
	Enable LLDP transmission and reception	set lldp enable txrx	-	Yes	Yes
	Set basic management TLV	tlv-select basic-mgmt	-	Yes	Yes

Automatic optimization settings using LLDP

Settings optimized for Dante can be applied automatically by receiving LLDP frames created independently by ADECIA components.

Automatic optimization settings via LLDP are set by the **lldp auto-setting** command.
By default, this product is set to **enable** automatic optimization settings via LLDP.

ADECIA components transmit Yamaha-proprietary LLDP frames that contain the following contents.

- EEE (Energy-Efficient Ethernet) disable setting
- Flow control disable setting
- Diffserve base QoS setting
- IGMP snooping settings

If this function is enabled and a corresponding LLDP frame is received, then the settings are automatically applied to the running-config settings for the overall system, for the VLAN interface that received the frame, and for the LAN/SFP port where the LLDP frame was received.
However, the function is disabled if even one of the automatically specified settings differs from factory settings.

If you save using the **copy running-config startup-config** command or the **write** command, the settings are also applied to the startup-config that is used for the next and subsequent startups.

Even if the port to which the device is connected experiences a link-down state after automatic optimization settings, the automatically added settings are maintained.

This function can be used only for a physical interface (LAN/SFP port). It cannot be used with a link aggregated logical interface.

In addition, LAN/SFP port modes can only be used at access ports. They cannot be used at trunk ports.
This function cannot be used if the stack function is enabled on models that support it.

In order to use this function, reception of LLDP frames must be enabled.
For this reason, check in advance that the following settings have been made.

- Enable LLDP functionality for the overall system using the **lldp run** command.
- Create LLDP agents at applicable interfaces using the **lldp-agent** command.
- Specify the LLDP frame transmit/receive mode using the **set lldp** command.

LLDP frame transmission and reception are **enabled** in product default settings.

Manual optimization settings via the Web GUI

For information on how to apply the Dante optimization settings using the web GUI, refer to the ProAV setting function.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Set Dante automatic optimization settings function using LLDP	lldp auto-setting
Enable LLDP function	lldp run
Create LLDP agent	lldp-agent
Set LLDP transmission/reception mode	set lldp
Set basic management TLV	tlv-select basic-mgmt
Set flow control (system)	flowcontrol
Set flow control (interface)	flowcontrol
Enable QoS	qos
Set DSCP - transmission queue ID conversion table	qos dscp-queue
Set egress queue scheduling	qos wrr-weight
Set QoS trust mode	qos trust
Shutdown	shutdown
Set forwarding multicast frames	l2-mcast flood
Set forwarding unknown multicasts	l2-unknown-mcast
Enable/disable IGMP snooping	ip igmp snooping
Set IGMP snooping version	ip igmp snooping version
Set IGMP snooping fast-leave	ip igmp snooping fast-leave
Set IGMP query transmission function	ip igmp snooping querier

Operations	Operating commands
Set IGMP query transmission interval	ip igmp snooping query-interval
Set IGMP packet TTL value checking function	ip igmp snooping check ttl
Set IGMP packet RA checking function	ip igmp snooping check ra
Set IGMP packet ToS checking function	ip igmp snooping check tos
Set IGMP report suppression function	ip igmp snooping report-suppression
Enable IGMP report forwarding function	ip igmp snooping report-forward
Enable transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression
Set L2MS filter	l2ms filter
Set BPDU filter	spanning-tree bpdu-filter
Set EEE	eee
Set MRU	mru

Examples of Command Execution

Automatic optimization settings using LLDP

Enable automatic optimization settings using LLDP.
Enable LLDP transmission and reception on port1.1.

```
Yamaha#configure terminal
Yamaha(config)#interface port1.1
Yamaha(config-if)#lldp-agent ①
Yamaha(lldp-agent)#set lldp enable txrx ②
Yamaha(lldp-agent)#exit
Yamaha(config-if)#exit
Yamaha(config)#lldp run ③
Yamaha(config)#lldp auto-setting enable ④
```

① Create LLDP agent, mode transition

② Set LLDP transmission/reception mode

③ Enable LLDP function

④ Enable automatic optimization settings using LLDP

Points of Caution

- Using LLDP to specify settings automatically
    - This function can be used only for a physical interface (LAN/SFP port). It cannot be used with a link aggregated logical interface.
    - LAN/SFP port modes can only be used at access ports. They cannot be used at trunk ports.
    - This function cannot be used if the stack function is enabled on models that support it.
    - This functionality is disabled if even one of the automatically specified settings differs from factory settings.

Related Documentation

- ProAV Setting Function
- LLDP
- QoS
- Flow Control
- IGMP Snooping
- Basic Interface Functions
- Spanning Tree
- L2MS
- ADECIA Product Information

ProAV Settings

Function Overview

From the web GUI “ProAV Settings” page, you can perform simple GUI operations to collectively configure optimal settings for AVoIP networks on which to transmit audio and video traffic such as Dante and NDI.
The following ProAV profiles can be set on this product.

- Dante
- NDI

This technical reference explains the details on the commands that are set when a ProAV profile is applied, as well as kitting (initial setup) and troubleshooting.
For details on how to use the web GUI “ProAV Settings” page, refer to ###.

Definition of Terms Used

- Dante

  Dante is a professional audio networking solution developed by Audinate, Inc.
  A single LAN cable can be used to carry out bidirectional communication of all the information required for a digital audio system, such as multi-channel audio transmission, clock synchronization signals, and control signals.

- NDI

  NDI is a new protocol developed by Newtek, Inc. to support live video production workflows over IP.
  In a typical Gigabit Ethernet environment, this protocol enables real-time mutual transmission of information such as video, audio, and metadata.

- Yamaha LAN Monitor
  Yamaha LAN Monitor is a computer application that allows you to monitor and control Yamaha network switch information and connected devices on your computer.

Details on ProAV Profiles

Dante profiles

The following commands are collectively applied by Dante profiles.

- List of commands applied by Dante profiles

Object of setting	Function	Commands
Entire system	Disable flow control	flowcontrol disable
	Enable QoS	qos enable
	Optimize transmission queue by DSCP value	qos dscp-queue 8 2
		qos dscp-queue 26 3
		qos dscp-queue 34 4
		qos dscp-queue 46 5
		qos dscp-queue 48 5
		qos dscp-queue 56 7
		qos dscp-queue [not indicated above] 0
		no qos wrr-weight [0 to 7]
	Always forward linked local multicasts	l2-unknown-mcast forward link-local
	Enable LLDP	lldp run
	Enable PTP	ptp enable

Object of setting	Function	Commands
VLAN interface	Set profile type	proav profile-type dante-primary/dante-secondary
	Cancel shutdown	no shutdown
	Flood unknown multicasts	l2-unknown-mcast flood
	Always forward PTP packets	l2-mcast flood 224.0.1.129
		l2-mcast flood 224.0.1.130
		l2-mcast flood 224.0.1.131
		l2-mcast flood 224.0.1.132
		l2-mcast flood 239.254.3.3
	Enable IGMP snooping	ip igmp snooping enable
	Set IGMP snooping version	ip igmp snooping version 3
	Enable IGMP snooping fast-leave function	ip igmp snooping fast-leave auto-assignment
	Enable IGMP query transmission function	ip igmp snooping querier
	Set IGMP query transmission interval	ip igmp snooping query-interval 30
	Disable IGMP report-suppression function	ip igmp snooping report-suppression disable
	Enable IGMP report forwarding function	ip igmp snooping report-forward enable
	Disable IGMP packet TTL value checking function	ip igmp snooping check ttl disable
	Disable IGMP packet RA checking function	ip igmp snooping check ra disable
	Disable IGMP packet ToS checking function	ip igmp snooping check tos disable
	Enable data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression enable
LAN/SFP port	Disable flow control	flowcontrol disable
	Set MRU	mru 1522
	Set QoS trust mode to DSCP	qos trust dscp
	Set L2MS filter	l2ms filter disable / enable (*1)
	Set BPDU filter	spanning-tree bpdu-filter disable / enable (*2)
	Disable EEE	eee disable
	Enable LLDP transmission and reception	lldp-agent set lldp enable txrx tlv-select basic-mgmt
	Enable PTP	ptp enable

Details on the settings are as follows:

- **Disable flow control**
  - **Disabling flow control** ensures that transmission and reception of Dante traffic continue even when the bandwidth is congested.
- **Enable QoS**
  - By **enabling QoS**, the priority is given to Dante traffic forwarding.
  - By **optimizing transmission queues by DSCP value**, DSCP values related to Dante traffic are assigned to high-priority transmission queues.
  - By **setting the QoS trust mode to DSCP**, the priority control is performed by referring to the DSCP values.
- **Enable IGMP snooping**
  - By **enabling IGMP snooping**, multicast traffic is forwarded only to ports where multicast receivers exist, and unnecessary traffic is not forwarded.
  - **Set the IGMP snooping version to IGMPv3**.
    In a network configuration using multiple switches, if the switches have different versions, a warning message will be displayed on the "Multicast page" of the ProAV GUI.
    When using a Dante network, set the version to IGMPv3.
  - By **enabling the IGMP snooping fast leave function**, multicast traffic forwarding stops immediately when a multicast receiver stops receiving it.
    When a multicast receiver switches between audio and video, the multicast traffic before the switching can be prevented from causing noise.
  - By **enabling the auto-assignment option of the fast leave function**, fast leave is not performed on ports connecting switches in a network configuration using multiple switches.
    This prevents immediate stop of multicast traffic forwarding when receivers who want to receive the multicast traffic still exist on the opposing switch.
  - **Enable the IGMP query transmission function (querier function)**.
    When IGMP snooping is used, a querier must exist on the same network.
    If there are multiple queriers on the same network, the querier with the smallest IP address becomes the representative querier, and the other queriers automatically stop transmitting queries.
  - By **setting the IGMP query transmission interval to 30 seconds**, the IGMP snooping learning state can converge more quickly.
  - By **disabling the IGMP report suppression function**, IGMP reports are forwarded directly without being proxied in a network configuration using multiple switches.
  - By **enabling the IGMP report suppression function**, IGMP reports are forwarded directly without being proxied in a network configuration using multiple switches.
  - By **disabling the IGMP packet TTL value/RA/ToS checking function**, even if an invalid IGMP packet is received, the information is appropriately corrected and the IGMP packet is forwarded.
  - By **enabling the data transfer suppression function for multicast router ports**, you can conserve the bandwidth between switches in a network configuration using multiple switches.
    Normally, all multicast traffic is forwarded to the multicast router port regardless of existence of a multicast receiver. Therefore, in a bidirectional transmission environment, unnecessary multicast traffic consumes the bandwidth between switches.
    By using this function, multicast traffic is forwarded only if a multicast receiver exists on the opposing switch, thereby conserving the bandwidth between switches.
- **Always forward control-use multicast packets**
  - By **always forwarding linked local multicasts**, control packets such as mDNS used by Dante are always forwarded when IGMP snooping is enabled.
  - By **always forwarding PTP packets**, control packets for time synchronization used by Dante are

always forwarded when IGMP snooping is enabled.

    - By **flooding unknown multicasts**, multicast traffic without a receiver is forwarded when IGMP snooping is enabled.

- **Disable jumbo frames**
    - By **setting the MRU to 1522 bytes**, jumbo frame forwarding is disabled.
- **Disable EEE**
    - **Disabling the power saving function** prevents the function from affecting data transfer performance.
- **Enable LLDP**
    - **Enabling LLDP transmission and reception** enables the **IGMP snooping fast leave function** and the **IGMP report forwarding function**.
      This is because these two IGMP functions operate by using LLDP to determine whether the opposing device is a switch.
- **Set L2MS filter** (*1)
    - Only if the Dante network is configured as **a redundant Dante primary/secondary** configuration, the **L2MS filter is enabled** on the Dante secondary port.
      L2MS refers to a Yamaha-original control packet used to monitor and control Yamaha switches with integrated management applications such as Yamaha LAN Monitor.
      In the redundant configuration, the switches are connected with two cables, a primary cable and a secondary cable. Therefore, enabling the L2MS filter prevents control packets from looping and causing congestion.
      In addition, in network configurations other than the redundant configuration, the **L2MS filter is disabled**.
- **Set BPDU filter** (*2)
    - Only if the Dante network is configured as **a redundant Dante primary/secondary** configuration, the **BPDU filter is enabled** on the Dante secondary port.
      In a redundant configuration, the network switches are connected with two cables, a primary cable and a secondary cable. Therefore, enabling the BPDU filter prevents port blocking.
      In addition, in network configurations other than the redundant configuration, the **BPDU filter is disabled**.
- **Set profile type**
    - This setting is used as an identifier to identify the profile type in the ProAV GUI.

NDI profiles

The following commands are collectively applied by NDI profiles.

- List of commands applied by NDI profiles

Object of setting	Function	Commands
Entire system	Enable flow control	flowcontrol enable
	Disable QoS	qos disable
	Always forward linked local multicasts	l2-unknown-mcast forward link-local
	Enable LLDP	lldp run
	Disable PTP	ptp disable

Object of setting	Function	Commands
VLAN interface	Set profile type	proav profile-type ndi
	Cancel shutdown	no shutdown
	Flood unknown multicasts	l2-unknown-mcast flood
	Enable IGMP snooping	ip igmp snooping enable
	Set IGMP snooping version	ip igmp snooping version 2
	Enable IGMP snooping fast-leave function	ip igmp snooping fast-leave auto-assignment
	Enable IGMP query transmission function	ip igmp snooping querier
	Set IGMP query transmission interval	ip igmp snooping query-interval 125
	Disable IGMP report-suppression function	ip igmp snooping report-suppression disable
	Enable IGMP report forwarding function	ip igmp snooping report-forward enable
	Disable IGMP packet TTL value checking function	ip igmp snooping check ttl disable
	Disable IGMP packet RA checking function	ip igmp snooping check ra disable
	Disable IGMP packet ToS checking function	ip igmp snooping check tos disable
	Enable data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression enable
LAN/SFP port	Enable flow control	flowcontrol both
	Set MRU	mru 1522
	Disable L2MS filter	l2ms filter disable
	Disable EEE	eee disable
	Enable LLDP transmission and reception	lldp-agent set lldp enable txrx tlv-select basic-mgmt
	Enable PTP	ptp disable

Details on the settings are as follows:

- **Enable flow control**
  - By **enabling flow control**, when the bandwidth becomes congested, traffic transmission is temporarily stopped until the congestion clears, preventing packet loss.
- **Disable QoS**
  - By **disabling QoS**, packets will be forwarded without priority control.
- **Enable IGMP snooping**
  - By **enabling IGMP snooping**, multicast traffic is forwarded only to ports where multicast receivers exist, and unnecessary traffic is not forwarded.
  - **Set the IGMP snooping version to IGMPv2**.
    In a network configuration using multiple switches, if the switches have different versions, a

warning message will be displayed on the “Multicast page” of the ProAV GUI.
When using an NDI network, set the version to IGMPv2.

  - By **enabling the IGMP snooping fast leave function**, multicast traffic forwarding stops immediately when a multicast receiver stops receiving it.
    When a multicast receiver switches between audio and video, the multicast traffic before the switching can be prevented from causing noise.
  - By **enabling the auto-assignment option of the fast leave function**, fast leave is not performed on ports connecting switches in a network configuration using multiple switches.
    This prevents immediate stop of multicast traffic forwarding when receivers who want to receive the multicast traffic still exist on the opposing switch.
  - **Enable the IGMP query transmission function (querier function)**.
    When IGMP snooping is used, a querier must exist on the same network.
    If there are multiple queriers on the same network, the querier with the smallest IP address becomes the representative querier, and the other queriers automatically stop transmitting queries.
  - **Set the IGMP query interval value to the default of 125 seconds**.
  - By **disabling the IGMP report suppression function**, IGMP reports are forwarded directly without being proxied in a network configuration using multiple switches.
  - By **enabling the IGMP report suppression function**, IGMP reports are forwarded directly without being proxied in a network configuration using multiple switches.
  - By **disabling the IGMP packet TTL value/RA/ToS checking function**, even if an invalid IGMP packet is received, the information is appropriately corrected and the IGMP packet is forwarded.
  - By **enabling the data transfer suppression function for multicast router ports**, you can conserve the bandwidth between switches in a network configuration using multiple switches.
    Normally, all multicast traffic is forwarded to the multicast router port regardless of existence of a multicast receiver. Therefore, in a bidirectional transmission environment, unnecessary multicast traffic consumes the bandwidth between switches.
    By using this function, multicast traffic is forwarded only if a multicast receiver exists on the opposing switch, thereby conserving the bandwidth between switches.

- **Disable jumbo frames**
  - By **setting the MRU to 1522 bytes**, jumbo frame forwarding is disabled.
- **Disable EEE**
  - **Disabling the power saving function** prevents the function from affecting data transfer performance.
- **Enable LLDP**
  - **Enabling LLDP transmission and reception** enables the **IGMP snooping fast leave function** and the **IGMP report forwarding function**.
    This is because these two IGMP functions operate by using LLDP to determine whether the opposing device is a switch.
- **Set profile type**
  - This setting is used as an identifier to identify the profile type in the ProAV GUI.

Settings for using multiple profiles

On the “Custom” page of the ProAV profile, you can set any profile for each port.
Depending on the profile combination, conflicts in settings may occur, resulting in differences in settings compared to the case where a single profile is used.

When multiple profiles are used

- List of commands that are applied when multiple profiles are used

Object of setting	Function	Dante profiles	NDI profiles
Entire system	Disable flow control	flowcontrol disable	
	Enable QoS	qos enable	
	Optimize transmission queue by DSCP value	qos dscp-queue 8 2	
		qos dscp-queue 26 3	
		qos dscp-queue 34 4	
		qos dscp-queue 46 5	
		qos dscp-queue 48 5	
		qos dscp-queue 56 7	
		qos dscp-queue [not indicated above] 0	
		no qos wrr-weight [0 to 7]	
	Always forward linked local multicasts	l2-unknown-mcast forward link-local	
	Enable LLDP	lldp run	
	Enable PTP	ptp enable	

Object of setting	Function	Dante profiles	NDI profiles
VLAN interface	Set profile type	proav profile-type dante-primary/dante-secondary +	proav profile-type ndi
	Cancel shutdown	no shutdown +	no shutdown
	Flood unknown multicasts	l2-unknown-mcast flood +	l2-unknown-mcast flood
	Enable IGMP snooping	ip igmp snooping enable +	ip igmp snooping enable
	Set IGMP snooping version	ip igmp snooping version 3 +	ip igmp snooping version 2
	Enable IGMP snooping fast-leave function	ip igmp snooping fast-leave auto-assignment +	ip igmp snooping fast-leave auto-assignment
	Enable IGMP query transmission function	ip igmp snooping querier +	ip igmp snooping querier
	Set IGMP query transmission interval	ip igmp snooping query-interval 30 +	ip igmp snooping query-interval 125
	Disable IGMP report-suppression function	ip igmp snooping report-suppression disable +	ip igmp snooping report-suppression disable
	Enable IGMP report forwarding function	ip igmp snooping report-forward enable +	ip igmp snooping report-forward enable
	Disable IGMP packet TTL value checking function	ip igmp snooping check ttl disable +	ip igmp snooping check ttl disable
	Disable IGMP packet RA checking function	ip igmp snooping check ra disable +	ip igmp snooping check ra disable
	Disable IGMP packet ToS checking function	ip igmp snooping check tos disable +	ip igmp snooping check tos disable
	Enable data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression enable	ip igmp snooping mrouter-port data-suppression enable
	Always forward PTP packets	l2-mcast flood 224.0.1.129	-
		l2-mcast flood 224.0.1.130	
		l2-mcast flood 224.0.1.131	
		l2-mcast flood 224.0.1.132	
		l2-mcast flood 239.254.3.3	

Object of setting	Function	Dante profiles	NDI profiles
LAN/SFP port	Set flow control	flowcontrol disable	flowcontrol both
	Set MRU	mru 1522 +	mru 1522
	Set QoS trust mode	qos trust dscp +	qos trust port-priority qos port-priority-queue 2
	Set L2MS filter	l2ms filter disable +	l2ms filter disable
	Disable EEE	eee disable +	eee disable
	Enable LLDP transmission and reception	lldp-agent set lldp enable txrx tlv-select basic-mgmt +	lldp-agent set lldp enable txrx tlv-select basic-mgmt

Differences between using multiple profiles and using a single profile are as follows:

- **Flow control**
  - To enable QoS, **flow control** is disabled for the entire system.
- **QoS**
  - **QoS is enabled** for the entire system.
  - **The transmission queues are optimized based on the DSCP values** across the entire system.
  - For ports with a Dante profile applied, by **setting the QoS trust mode to DSCP**, the priority control is performed by referring to the DSCP values.
  - For ports with an NDI profile applied, by **setting the QoS trust mode to port priority and fixing the transmission queue to 2 (default)**, the packet forwarding priority control is not performed.

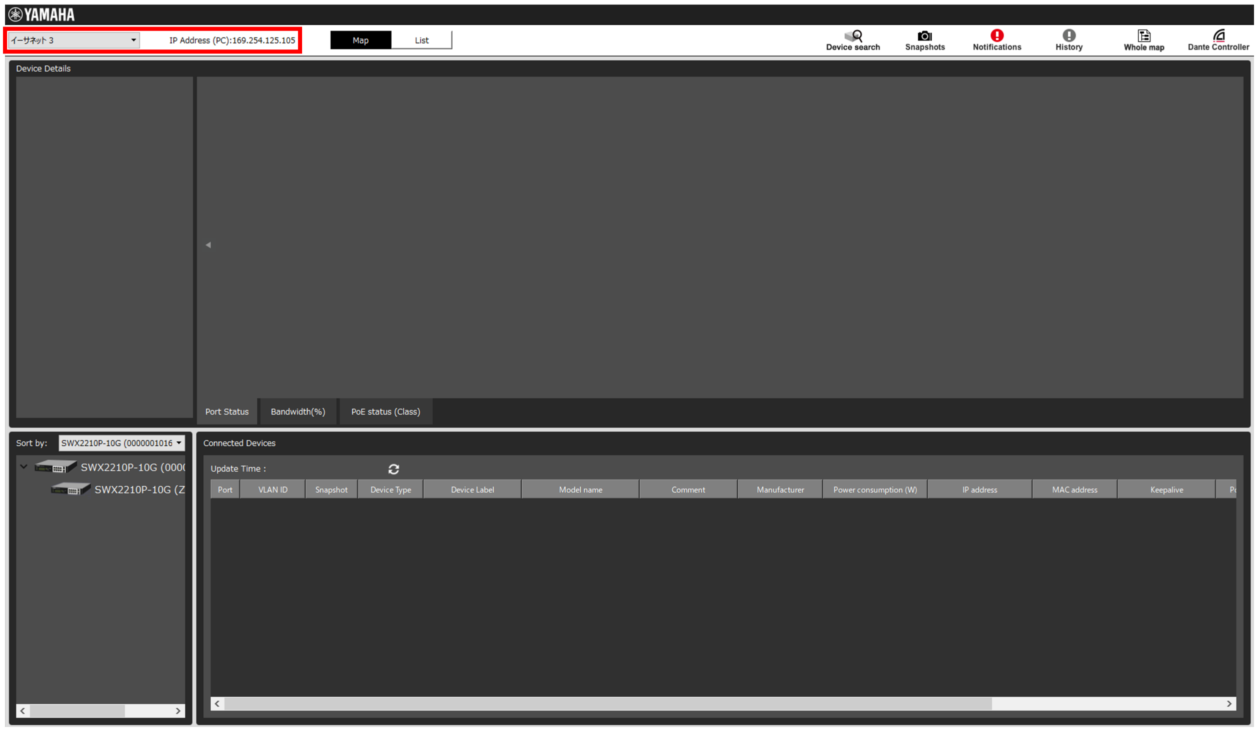
Kitting and Troubleshooting

By utilizing the “Yamaha LAN Monitor”, an integrated management tool for Yamaha network devices, you can easily perform kitting (initial setup) and troubleshooting.
Yamaha LAN Monitor can be downloaded for free. For details on how to install and use Yamaha LAN Monitor, refer to the user guide.

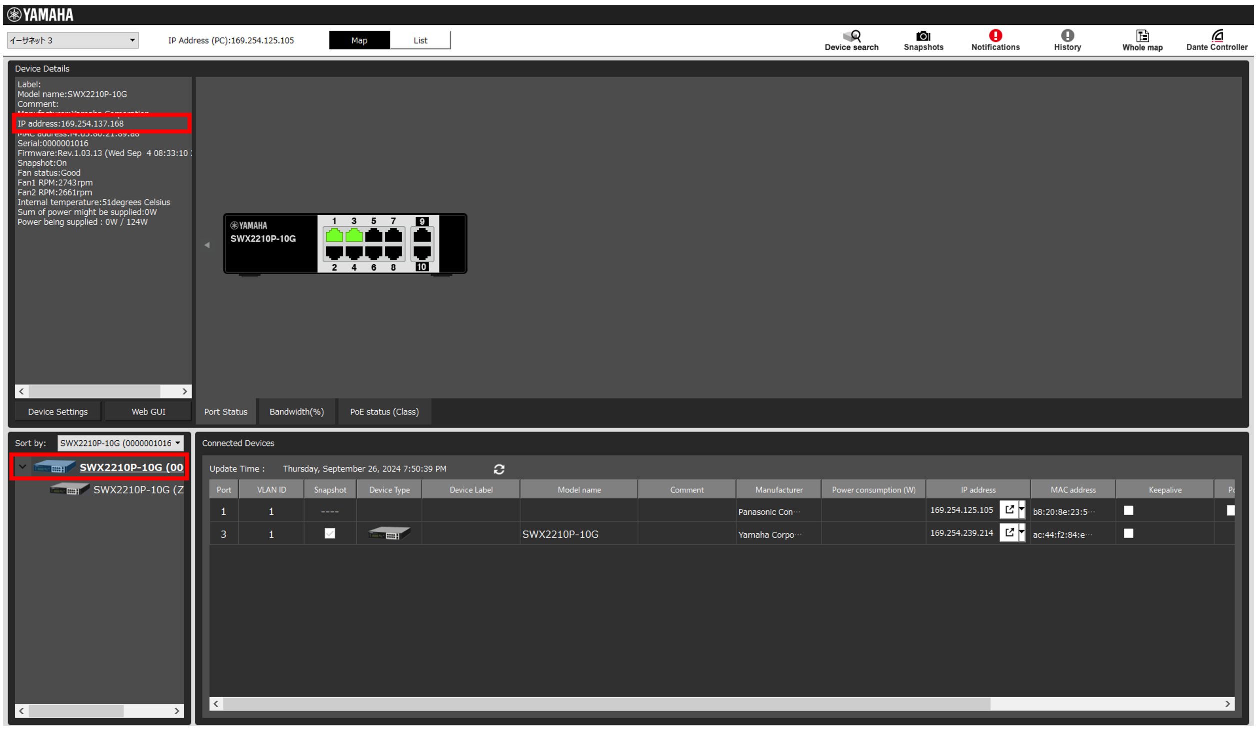
[Kitting] Initial setup without having to think about IP addresses

Normally, when using two or more switches in a network, you must appropriately set the IP address of each switch to avoid IP address duplication.
However, if you have a closed AVoIP network that does not need to be connected to an external network, you can use the **Auto IP function** of the switches to automatically assign link local addresses.
By combining a Yamaha switch in the factory default settings with Yamaha LAN Monitor, you can easily apply the ProAV profile without having to think about setting IP addresses.

1. As a preliminary step, install Yamaha LAN Monitor on your computer and set the IP address of the network adapter used by the computer to “Acquire automatically”.
   This procedure allows the computer to operate with a link local address.
   (*If a DHCP server exists, the IP address can be acquired via DHCP. However, since a closed AVoIP network is assumed this time, the explanation of DHCP is omitted.)
2. Connect multiple switches in the factory default settings, connect the computer to a port on any switch, and start Yamaha LAN Monitor. When you start it, the following screen will appear.
   Make sure that the correct network adapter of the computer is selected in the upper left corner of the screen and that the IP address of the computer is a link local address starting with “169.254.”



3. You can check the IP address by clicking the switch icon on Yamaha LAN Monitor.
The default IP address of the Yamaha switch is “192.168.100.240/24”. *When the switch is placed under the management of Yamaha LAN Monitor in its factory default settings (state without any changes to its settings), the address will automatically switch to a link local address. *
If the IP address of the switch starts with “169.254.”, the switch is operating with a link local address. If the address remains as “192.168.100.240”, wait a while until it switches to a link local address, and then refresh the display.
*Note that, if the Yamaha switch settings have already been changed from the default settings, the switch will not automatically switch to a link local address. *If the address does not switch to the link local address after a while, reset the switch to its default settings.
With this product, you can physically initialize the settings by turning on the power while holding down the LED MODE button on the front of the chassis, and then releasing the button when all port LEDs turn orange.



Label:
Model name:SWX2210P-10G
Comment:
Manufacturer:Yamaha Corporation
IP address:169.254.137.168
MAC address:[illegible]
Serial:0000001016
Firmware:Rev.1.03.13 (Wed Sep 4 08:33:10
Snapshot:On
Fan status:Good
Fan1 RPM:2743rpm
Fan2 RPM:2661rpm
Internal temperature:51degrees Celsius
Sum of power might be supplied:0W
Power being supplied : 0W / 124W

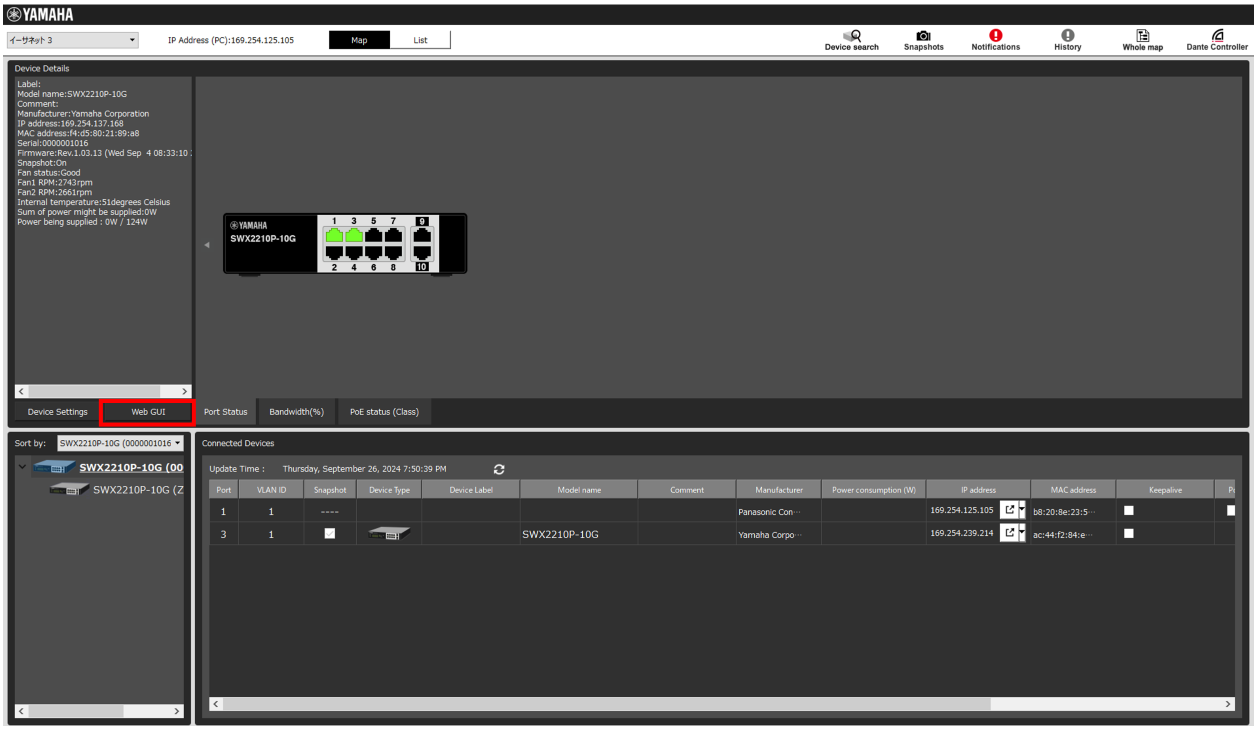
Update Time : Thursday, September 26, 2024 7:50:39 PM

Port	VLAN ID	Snapshot	Device Type	Device Label	Model name	Comment	Manufacturer	Power consumption (W)	IP address	MAC address	Keepalive	P
1	1	----					Panasonic Con···		169.254.125.105	b8:20:8e:23:5···	□	□
3	1	☑			SWX2210P-10G		Yamaha Corpo···		169.254.239.214	ac:44:f2:84:e···	□	

4. Once you have confirmed that the IP address of the switch has changed to a link local address, click the

“Web GUI” button.

The computer browser automatically opens and displays the web GUI of the switch.

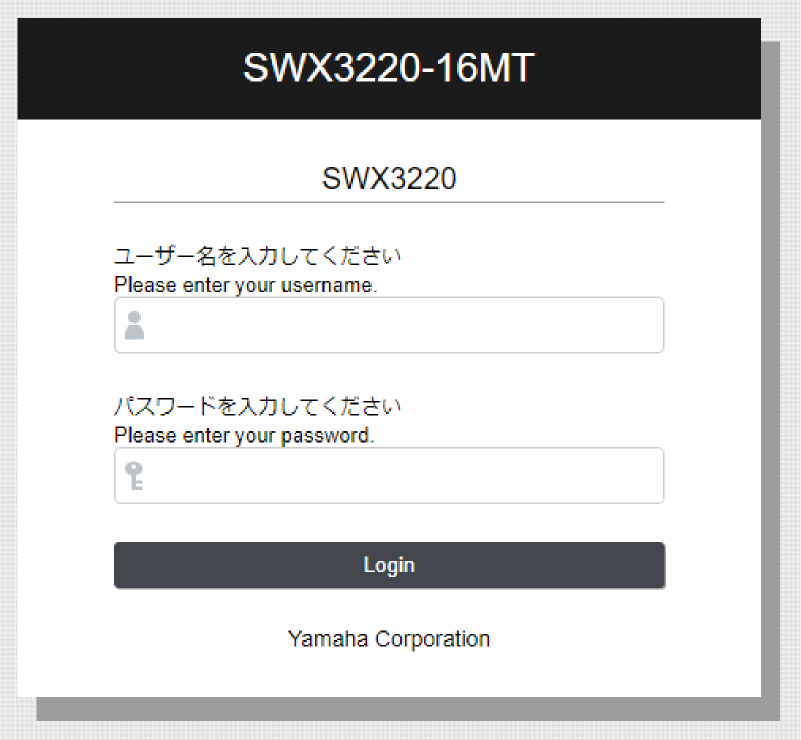


Label:
Model name:SWX2210P-10G
Comment:
Manufacturer:Yamaha Corporation
IP address:169.254.137.168
MAC address:f4:d5:80:21:89:a8
Serial:0000001016
Firmware:Rev.1.03.13 (Wed Sep 4 08:33:10
Snapshot:On
Fan status:Good
Fan1 RPM:2743rpm
Fan2 RPM:2661rpm
Internal temperature:51degrees Celsius
Sum of power might be supplied:0W
Power being supplied : 0W / 124W

Update Time : Thursday, September 26, 2024 7:50:39 PM

Port	VLAN ID	Snapshot	Device Type	Device Label	Model name	Comment	Manufacturer	Power consumption (W)	IP address	MAC address	Keepalive	P
1	1	----					Panasonic Con···		169.254.125.105	b8:20:8e:23:5···	□	□
3	1	☑			SWX2210P-10G		Yamaha Corpo···		169.254.239.214	ac:44:f2:84:e···	□	

5. On the web GUI login screen, enter the username “admin” and password “admin”.
After selecting the language, you will be asked to change your password. Set a password of your choice.



SWX3220-16MT

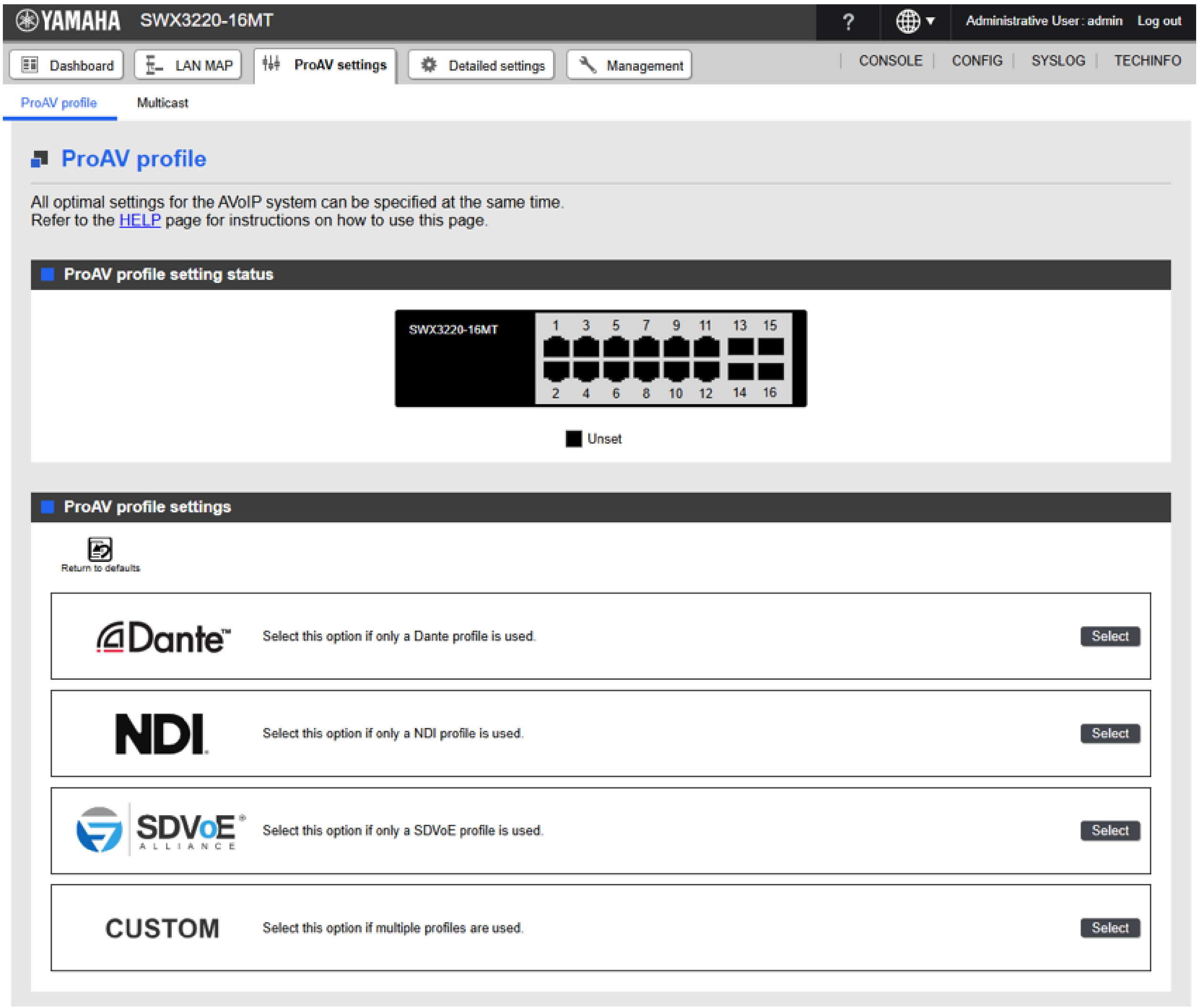
SWX3220

ユーザー名を入力してください
Please enter your username.

パスワードを入力してください
Please enter your password.

Yamaha Corporation

6. Once you have logged in to the web GUI, click the “ProAV Settings” button in the global menu at the top of the screen.
The “ProAV Profile” page will appear as shown below.



ProAV profile

All optimal settings for the AVoIP system can be specified at the same time.
Refer to the HELP page for instructions on how to use this page.

ProAV profile setting status

■ Unset

ProAV profile settings

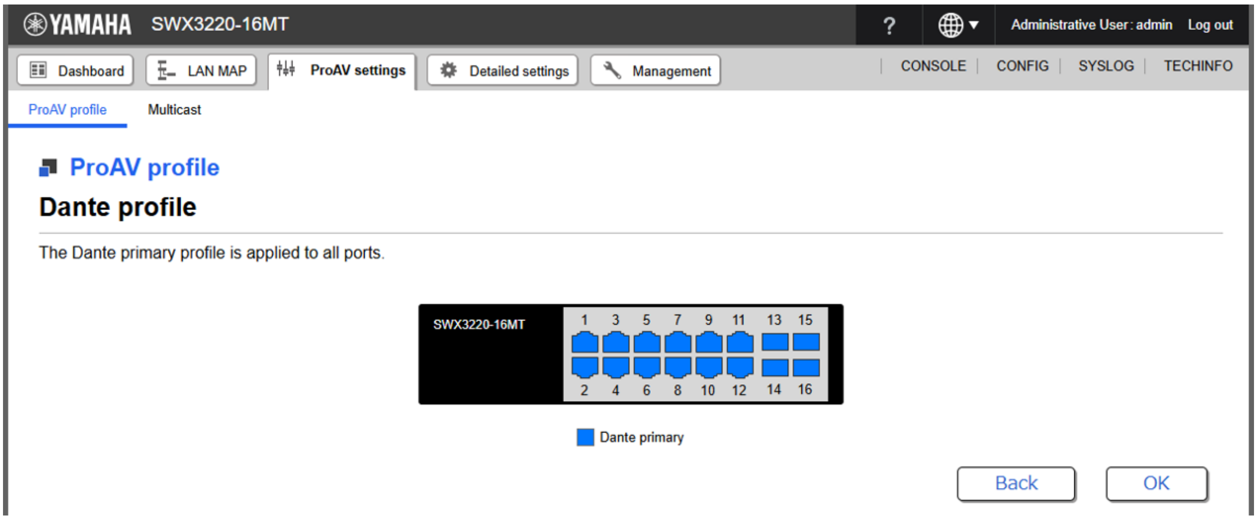
Select this option if only a Dante profile is used.

Select this option if only a NDI profile is used.

Select this option if only a SDVoE profile is used.

Select this option if multiple profiles are used.

7. Finally, apply the ProAV profile on the settings page. The ProAV profile setup is now completed.



ProAV profile

Dante profile

The Dante primary profile is applied to all ports.

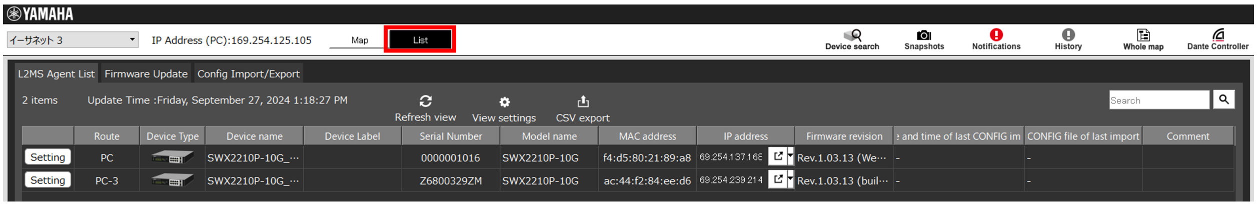
🟦 Dante primary

[Kitting] Applying the same settings to multiple Yamaha switches at once

Yamaha LAN Monitor can distribute configuration files (CONFIG files) to multiple Yamaha switches at once.
If you are using link local addresses as the IP addresses and want to apply the same settings to all switches, you can efficiently configure the settings for multiple switches.
Note that, if the switch is operated with a fixed IP address, you will need to reconfigure the IP address setting to prevent IP address duplication.

1. Follow the steps in 4.1 to apply the ProAV profile to one switch.

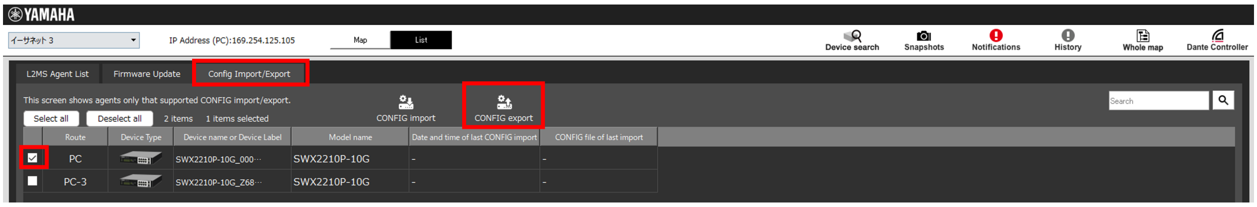
2. Click on the “List” tab at the top of the screen. A list of detected Yamaha switches will be displayed.



2 items Update Time :Friday, September 27, 2024 1:18:27 PM

	Route	Device Type	Device name	Device Label	Serial Number	Model name	MAC address	IP address	Firmware revision	≥ and time of last CONFIG im	CONFIG file of last import	Comment
Setting	PC		SWX2210P-10G_···		0000001016	SWX2210P-10G	f4:d5:80:21:89:a8	69.254.137.16€	Rev.1.03.13 (We···	-	-	
Setting	PC-3		SWX2210P-10G_···		Z6800329ZM	SWX2210P-10G	ac:44:f2:84:ee:d6	69.254.239.214	Rev.1.03.13 (buil···	-	-	

3. Click the “Config Import/Export” tab at the top of the screen.
Additionally, check the switch to which the ProAV profile has already been applied, and click the “Config export” button.

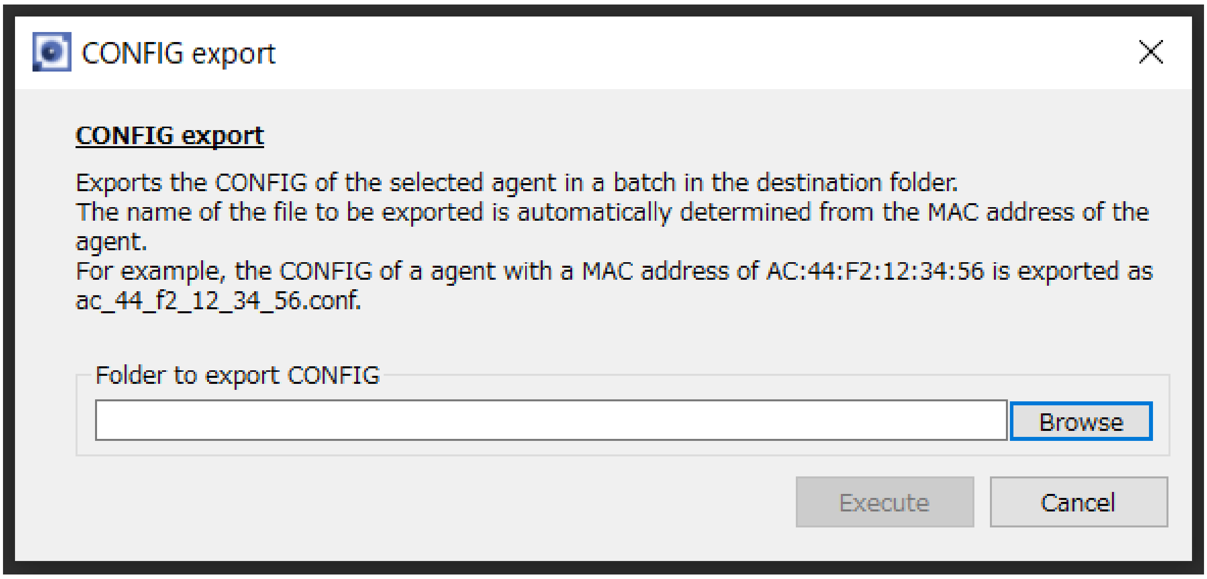


This screen shows agents only that supported CONFIG import/export.

2 items 1 items selected

	Route	Device Type	Device name or Device Label	Model name	Date and time of last CONFIG import	CONFIG file of last import
☑	PC		SWX2210P-10G_000···	SWX2210P-10G	-	-
□	PC-3		SWX2210P-10G_Z68···	SWX2210P-10G	-	-

4. The “Config export” dialog will appear. Select the directory in which you want to save the CONFIG file and click the “Execute” button.

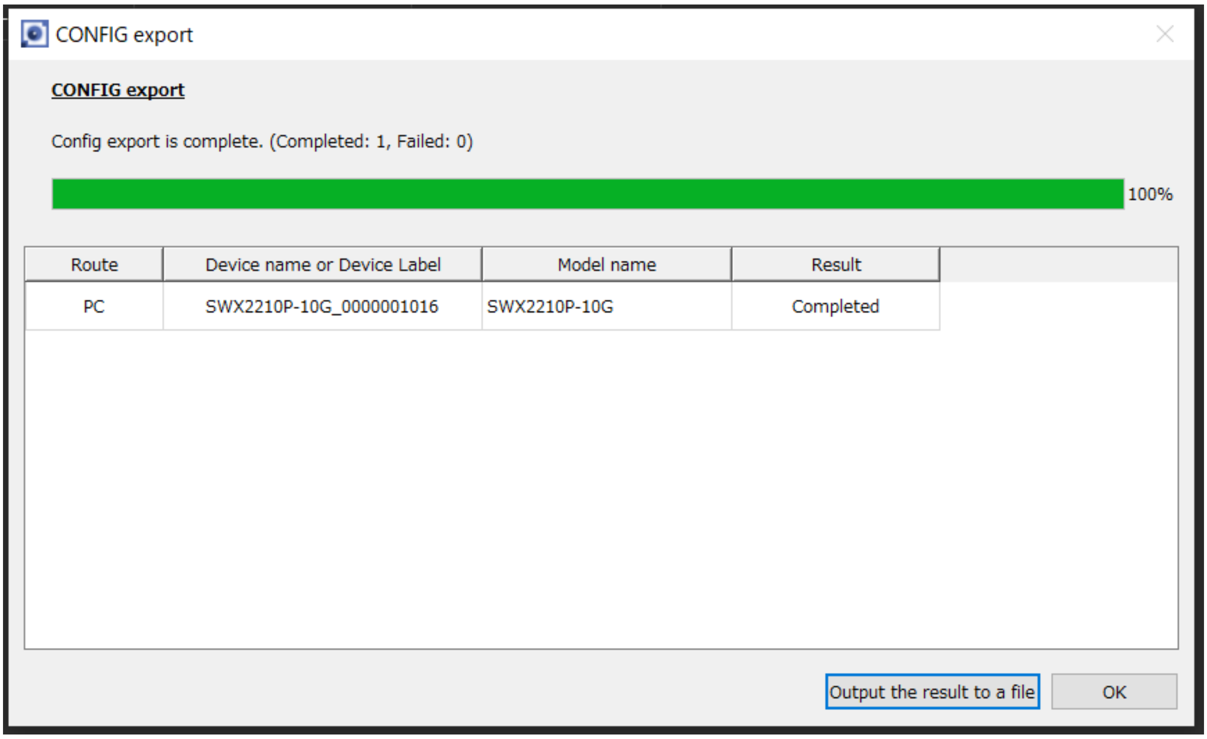


CONFIG export

Exports the CONFIG of the selected agent in a batch in the destination folder.
The name of the file to be exported is automatically determined from the MAC address of the agent.
For example, the CONFIG of a agent with a MAC address of AC:44:F2:12:34:56 is exported as ac_44_f2_12_34_56.conf.

Folder to export CONFIG

5. The dialog will display the progress and result of the export. Click the “OK” button when the export is completed.

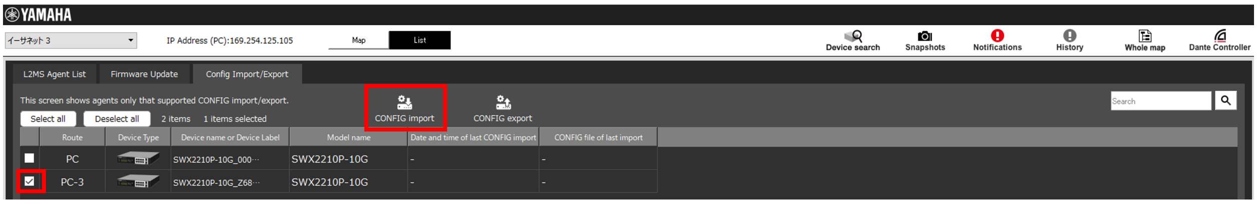


CONFIG export

Config export is complete. (Completed: 1, Failed: 0)

Route	Device name or Device Label	Model name	Result
PC	SWX2210P-10G_0000001016	SWX2210P-10G	Completed

6. Additionally, check the switch to which you want to apply the ProAV profile, and click the “Config import” button.
   If you want to apply the profile to multiple switches, check multiple check boxes.



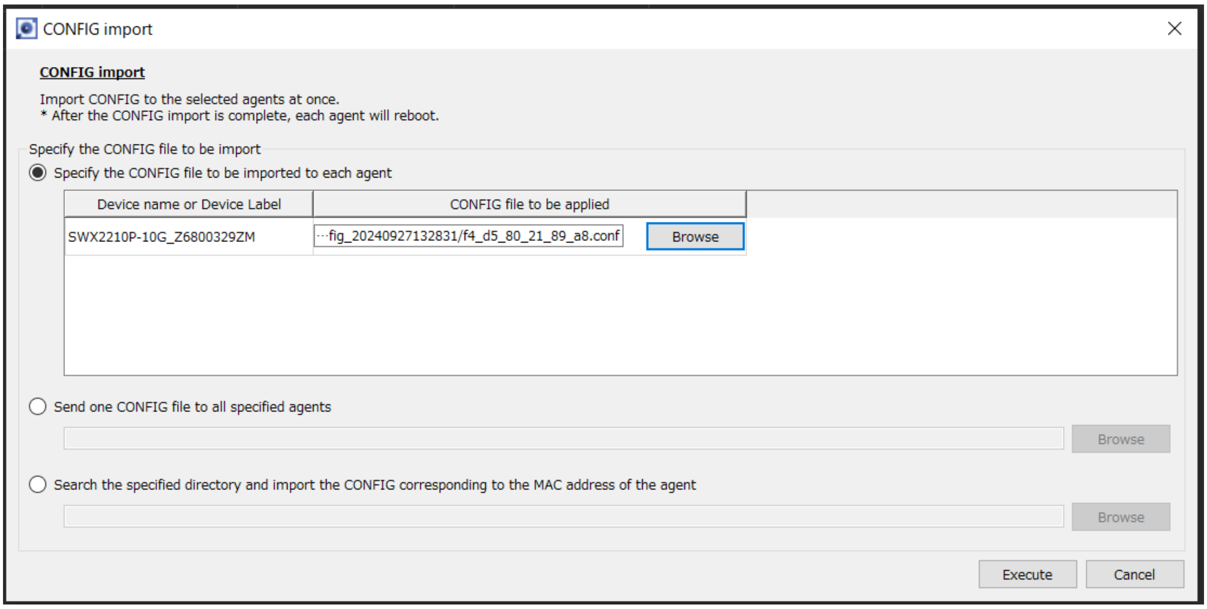
IP Address (PC):169.254.125.105

This screen shows agents only that supported CONFIG import/export.

2 items 1 items selected

	Route	Device Type	Device name or Device Label	Model name	Date and time of last CONFIG import	CONFIG file of last import
□	PC		SWX2210P-10G_000···	SWX2210P-10G	-	-
☑	PC-3		SWX2210P-10G_Z68···	SWX2210P-10G	-	-

7. The “Config import” dialog will appear. Select the CONFIG file saved in the previous step as an import file, and click the “Execute” button.
   You can specify a CONFIG file for each selected switch, or you can specify the same CONFIG file for all selected switches.
   In an environment where different models of switches are used, specify the appropriate CONFIG file for each model.



CONFIG import

Import CONFIG to the selected agents at once.
* After the CONFIG import is complete, each agent will reboot.

Specify the CONFIG file to be import

● Specify the CONFIG file to be imported to each agent

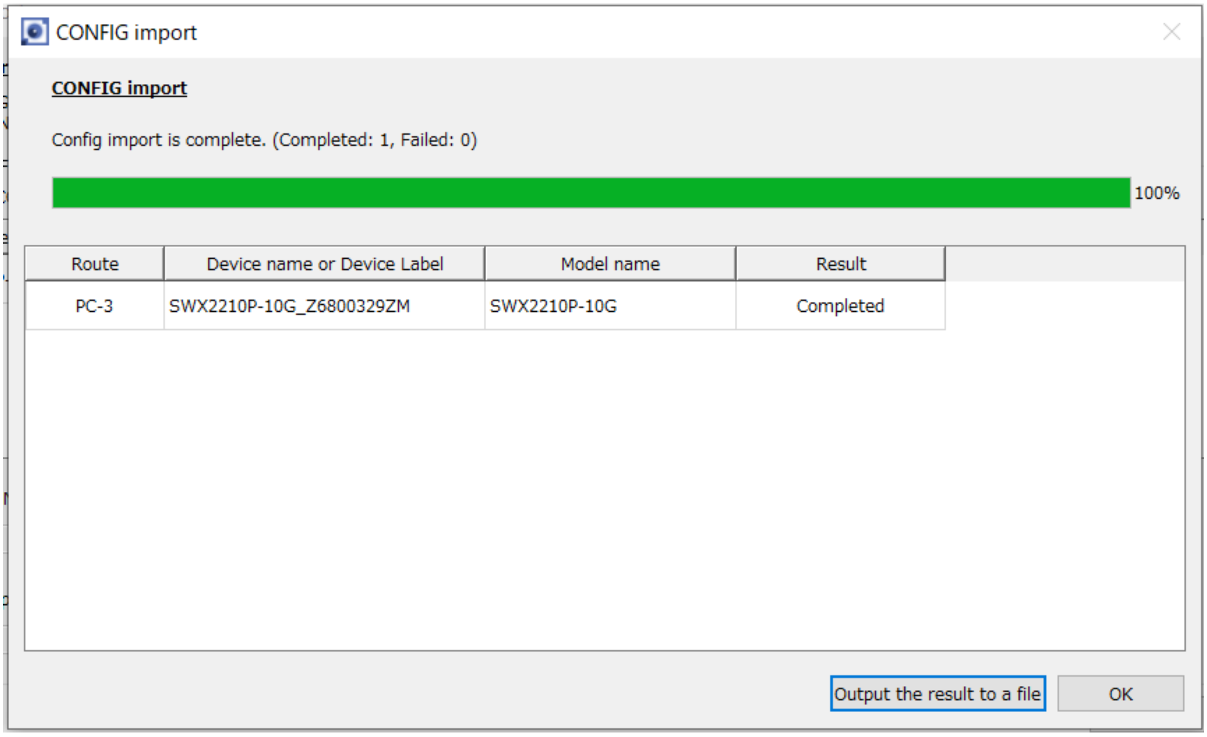
Device name or Device Label	CONFIG file to be applied
SWX2210P-10G_Z6800329ZM	···fig_20240927132831/f4_d5_80_21_89_a8.conf

○ Send one CONFIG file to all specified agents

○ Search the specified directory and import the CONFIG corresponding to the MAC address of the agent

8. The dialog will display the progress and result of the import. Click the “OK” button when the import is completed.

The switch that receives CONFIG will automatically reboot and the new settings will be applied after the bootup.



CONFIG import

Config import is complete. (Completed: 1, Failed: 0)

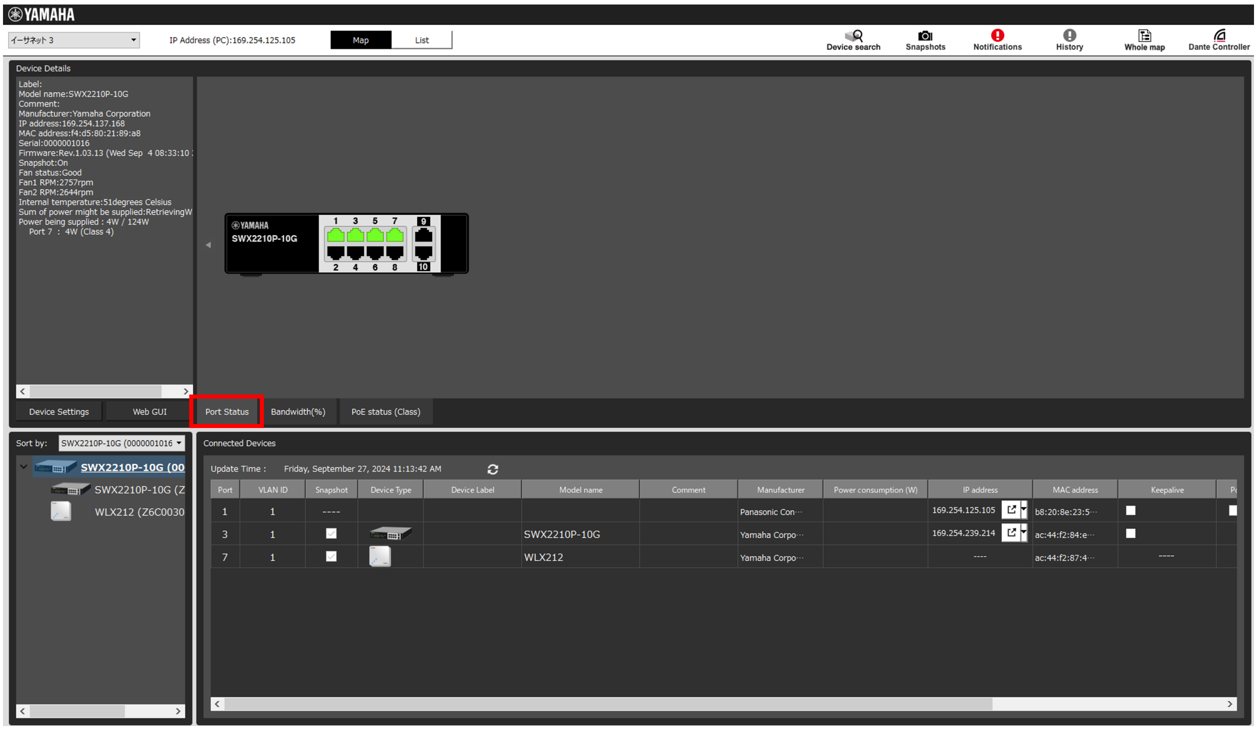
Route	Device name or Device Label	Model name	Result
PC-3	SWX2210P-10G_Z6800329ZM	SWX2210P-10G	Completed

You can also update the firmware on multiple Yamaha switches at once by following the similar procedure using the “Firmware Update” button.
In this way, Yamaha LAN Monitor can be used as a kitting tool for multi-device environments, so please make use of it.

[Troubleshooting] Checking the network status

By using Yamaha LAN Monitor, you can visualize the connection configuration of the entire network, and also check traffic bandwidth usage and PoE power supply status.

1. Click the switch icon.
   “Port Status” is selected by default, which displays real-time link status on the front panel at the top of the screen.
   The tree view at the bottom left of the screen allows you to check the current network connection configuration, and the connected device view at the bottom right of the screen allows you to see which devices are connected to which ports.



IP Address (PC):169.254.125.105

Label:
Model name:SWX2210P-10G
Comment:
Manufacturer:Yamaha Corporation
IP address:169.254.137.168
MAC address:f4:d5:80:21:89:a8
Serial:0000001016
Firmware:Rev.1.03.13 (Wed Sep 4 08:33:10
Snapshot:On
Fan status:Good
Fan1 RPM:2757rpm
Fan2 RPM:2644rpm
Internal temperature:51degrees Celsius
Sum of power might be supplied:RetrievingW
Power being supplied : 4W / 124W
Port 7 : 4W (Class 4)

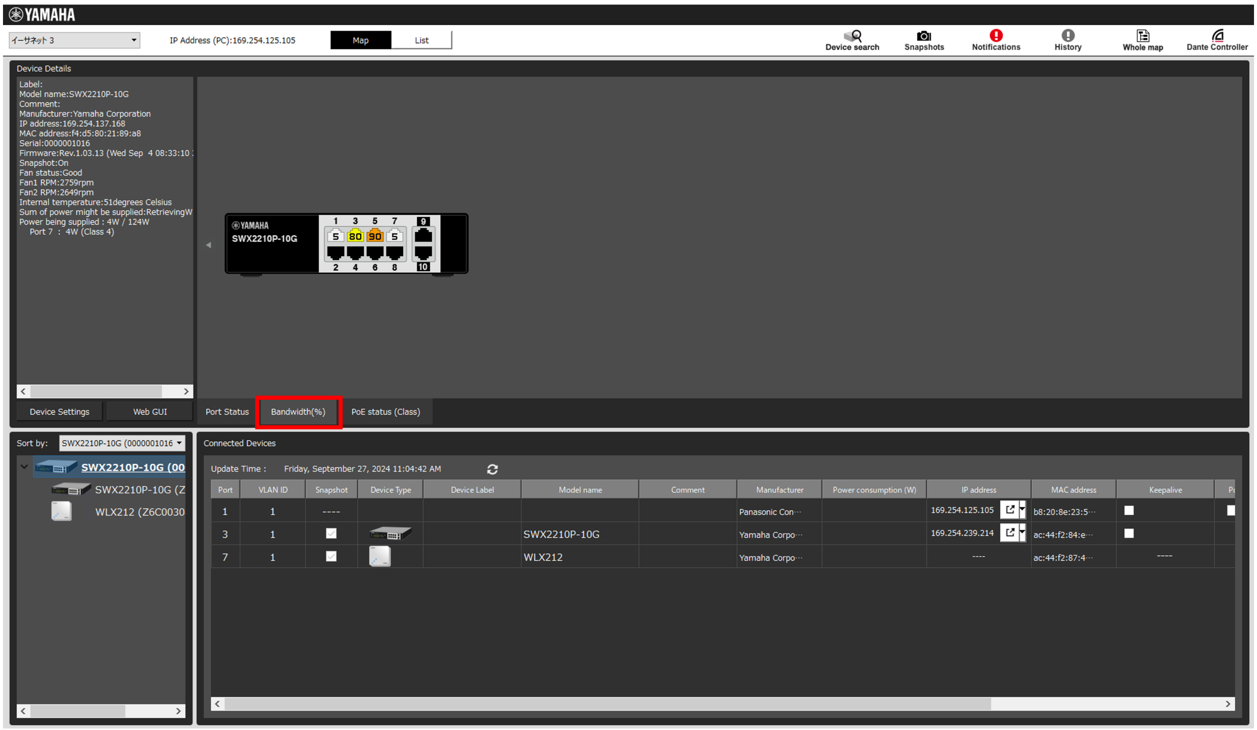
Sort by: SWX2210P-10G (0000001016

SWX2210P-10G (00
SWX2210P-10G (Z
WLX212 (Z6C0030

Update Time : Friday, September 27, 2024 11:13:42 AM

Port	VLAN ID	Snapshot	Device Type	Device Label	Model name	Comment	Manufacturer	Power consumption (W)	IP address	MAC address	Keepalive	P
1	1	----					Panasonic Con···		169.254.125.105	b8:20:8e:23:5···	□	□
3	1	☑			SWX2210P-10G		Yamaha Corpo···		169.254.239.214	ac:44:f2:84:e···	□	
7	1	☑			WLX212		Yamaha Corpo···		----	ac:44:f2:87:4···	----	

2. To check the traffic bandwidth usage, click the “Bandwidth Usage (%)” button.
The bandwidth utilization of each port is displayed as the percentage against the link speed.
When the bandwidth utilization is close to its upper limit, the port icon appears yellow, orange, or red.



IP Address (PC):169.254.125.105

Label:
Model name:SWX2210P-10G
Comment:
Manufacturer:Yamaha Corporation
IP address:169.254.137.168
MAC address:f4:d5:80:21:89:a8
Serial:0000001016
Firmware:Rev.1.03.13 (Wed Sep 4 08:33:10
Snapshot:On
Fan status:Good
Fan1 RPM:2759rpm
Fan2 RPM:2649rpm
Internal temperature:51degrees Celsius
Sum of power might be supplied:RetrievingW
Power being supplied : 4W / 124W
Port 7 : 4W (Class 4)

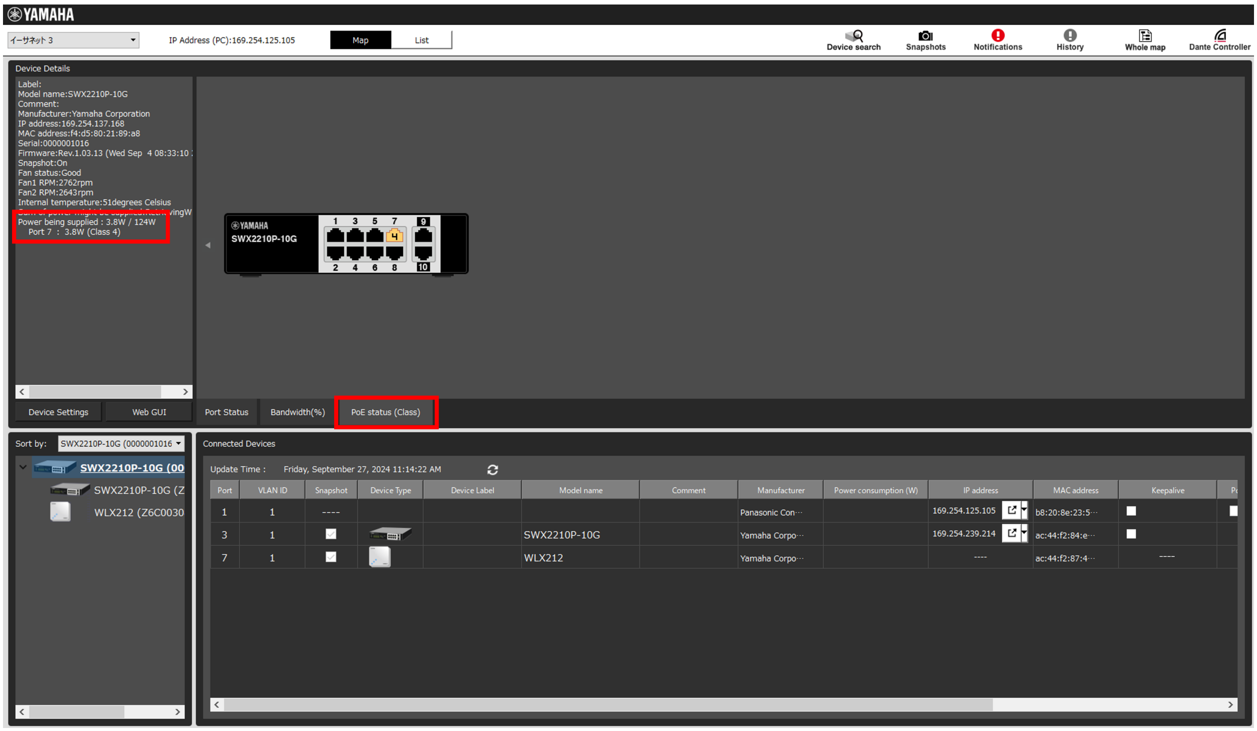
Sort by: SWX2210P-10G (0000001016

SWX2210P-10G (00
SWX2210P-10G (Z
WLX212 (Z6C0030

Update Time : Friday, September 27, 2024 11:04:42 AM

Port	VLAN ID	Snapshot	Device Type	Device Label	Model name	Comment	Manufacturer	Power consumption (W)	IP address	MAC address	Keepalive	P
1	1	----					Panasonic Con···		169.254.125.105	b8:20:8e:23:5···	□	□
3	1	☑			SWX2210P-10G		Yamaha Corpo···		169.254.239.214	ac:44:f2:84:e···	□	
7	1	☑			WLX212		Yamaha Corpo···		----	ac:44:f2:87:4···	----	

3. To check the PoE power supply status, click “PoE Power Supply Status (Class)”.
The power supply class is displayed for ports that are supplying power, and the device details view in the upper left corner of the screen shows the total power supply and the power supply of each port.



Device Details

Label:
Model name:SWX2210P-10G
Comment:
Manufacturer:Yamaha Corporation
IP address:169.254.137.168
MAC address:f4:d5:80:21:89:a8
Serial:0000001016
Firmware:Rev.1.03.13 (Wed Sep 4 08:33:10
Snapshot:On
Fan status:Good
Fan1 RPM:2762rpm
Fan2 RPM:2643rpm
Internal temperature:51degrees Celsius
Sum of power might be supplied:RetrievingW
Power being supplied : 3.8W / 124W
Port 7 : 3.8W (Class 4)

Connected Devices

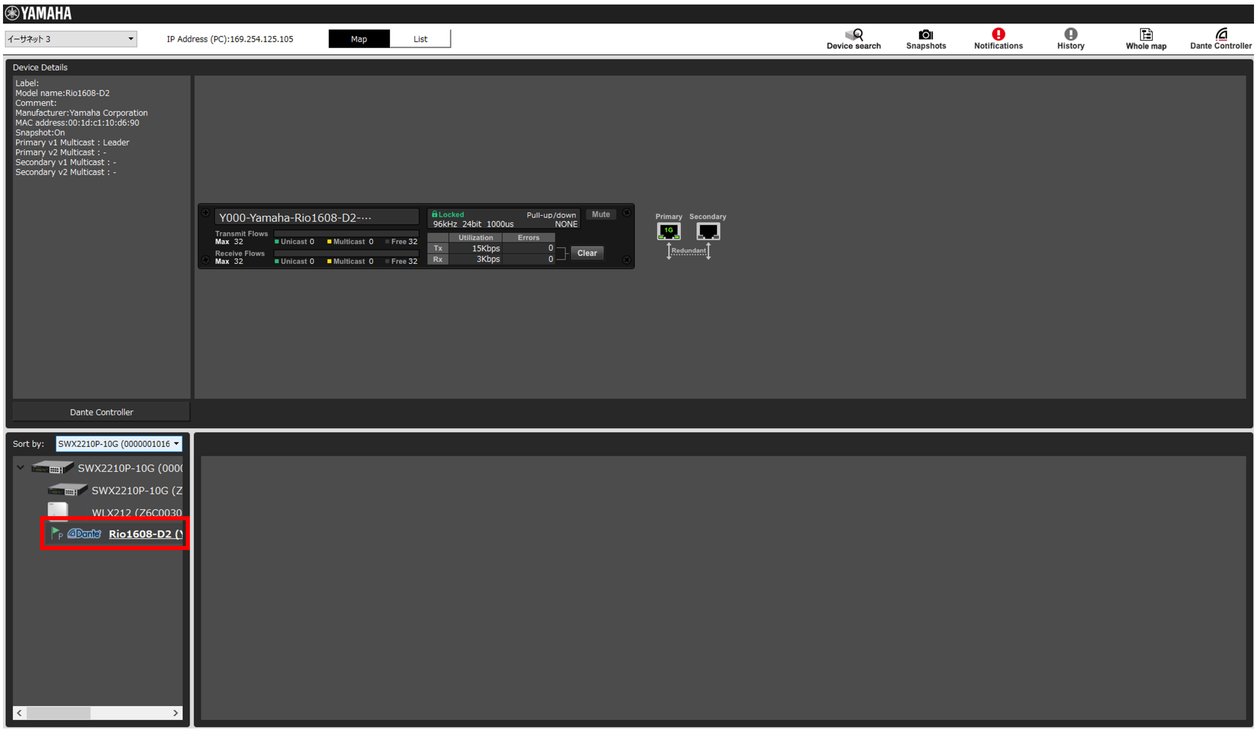
Update Time : Friday, September 27, 2024 11:14:22 AM

Port	VLAN ID	Snapshot	Device Type	Device Label	Model name	Comment	Manufacturer	Power consumption (W)	IP address	MAC address	Keepalive	Po
1	1	----					Panasonic Con···		169.254.125.105	b8:20:8e:23:5···	□	□
3	1	☑			SWX2210P-10G		Yamaha Corpo···		169.254.239.214	ac:44:f2:84:e···	□	
7	1	☑			WLX212		Yamaha Corpo···		----	ac:44:f2:87:4···	----	

[Troubleshooting] Checking the Dante device status

Yamaha LAN Monitor allows you to check the status of Dante devices and open Dante Controller with one click if it is installed on your computer.
Note that, in order to view Dante devices, Dante Control and Monitoring and Dante Discovery must be installed when Yamaha LAN Monitor is installed.

1. With a Dante device connected to the Yamaha switch, click on the Dante device icon.
   You can monitor the status of the primary and secondary ports, the number of transmission and reception flows, etc.
   You can also check information such as whether the operating mode of the Dante device is “redundant mode” or “daisy chain mode”.



Device Details

Label:
Model name:Rio1608-D2
Comment:
Manufacturer:Yamaha Corporation
MAC address:00:1d:c1:10:d6:90
Snapshot:On
Primary v1 Multicast : Leader
Primary v2 Multicast : -
Secondary v1 Multicast : -
Secondary v2 Multicast : -

Y000-Yamaha-Rio1608-D2-···

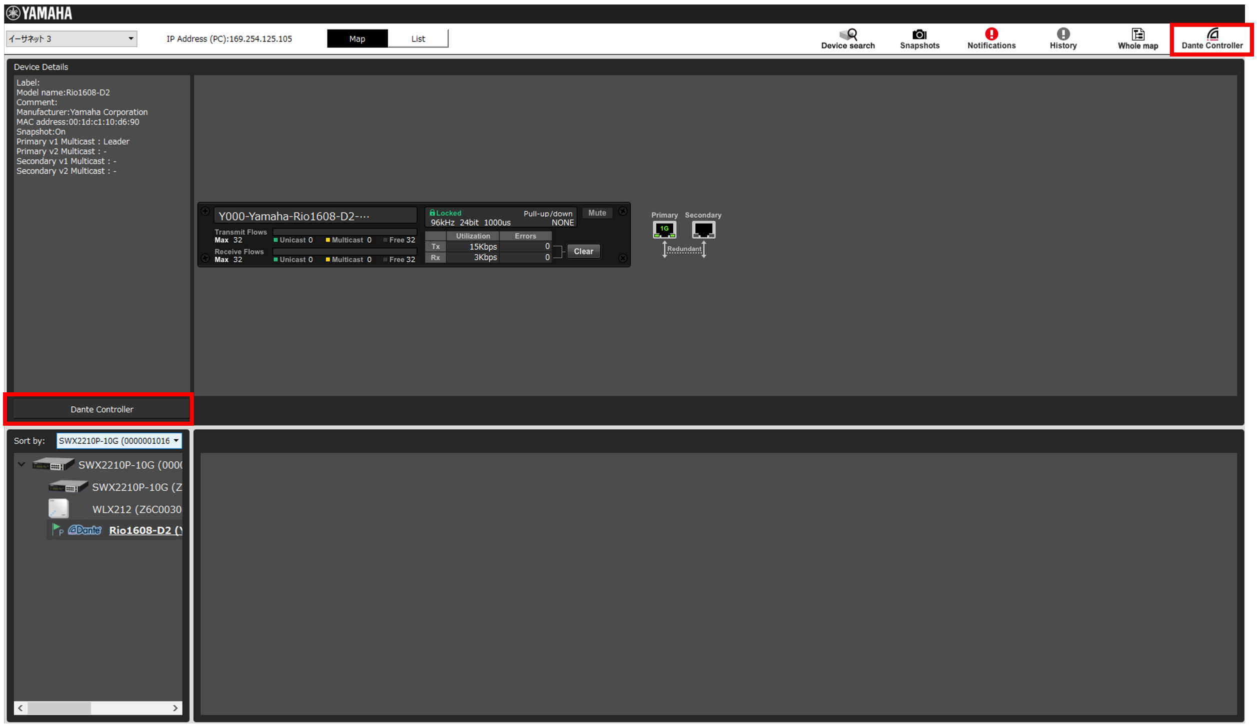
96kHz 24bit 1000us NONE

Transmit Flows
Max 32 Unicast 0 Multicast 0 Free 32
Receive Flows
Max 32 Unicast 0 Multicast 0 Free 32

	Utilization	Errors
Tx	15Kbps	0
Rx	3Kbps	0

2. Dante Controller can be started by clicking the “Dante Controller” button in the top right or center of the screen. (Dante Controller must be installed beforehand.)

You can seamlessly switch between Yamaha LAN Monitor and Dante Controller on a single computer, making troubleshooting more efficient.



Label:
Model name:Rio1608-D2
Comment:
Manufacturer:Yamaha Corporation
MAC address:00:1d:c1:10:d6:90
Snapshot:On
Primary v1 Multicast : Leader
Primary v2 Multicast : -
Secondary v1 Multicast : -
Secondary v2 Multicast : -

Points of Caution

- The settings configured collectively in ProAV settings are intended for use when this product is used as a switch dedicated to the AVoIP network.
  When building a complex network, such as mixing an existing in-house network with an AVoIP network, use the GUI advanced settings pages and commands to appropriately configure the settings.
- When applying the ProAV profile, ports that belong to a logical interface must be detached from the logical interface.
  If necessary, first detach the ports from the logical interface, assign the profile, and then re-attach them to the logical interface.
- The ProAV profile assumes an AVoIP network consisting only of Yamaha network switches.
  Note that, when the IGMP snooping function is used in a multi-vendor environment, determination of the opposing device via LLDP may not work.
- If the stack function is enabled on a model that supports the stack function, the ProAV settings cannot be used.

Related Documentation

- None.

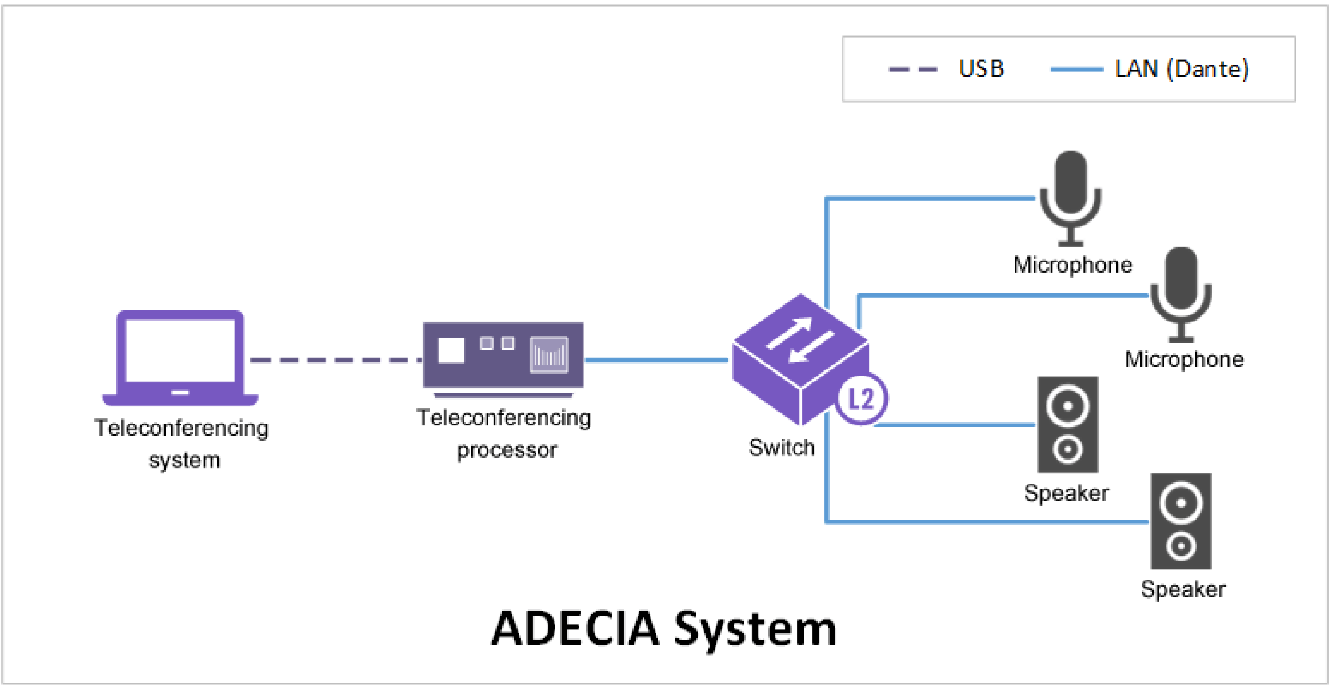
Trademarks and Trade Names

- Dante™ is a registered trademark of Audinate Pty Ltd.
- NDI® is a registered trademark of Vizrt NDI AB.

Linking Security to the ADECIA System

Function Overview

As conferencing systems are increasingly assigned IP values, it has become essential to have security functions for preventing unauthorized access to the network.
Yamaha's ADECIA one-stop sound solution for teleconferencing uses technology (device authentication) with a solid track record in the IT industry to ensure the system is robust in terms of security risks.



This product functions in combination with the ADECIA system to ensure even users unfamiliar with IT technologies can easily utilize the security functionality.
More specifically, product security functions can be enabled via the graphic user interface (GUI) for the teleconferencing processor, which is a component of the ADECIA system. (For more details about teleconferencing processor specifications, refer to ADECIA Product Information.)
If the product security function is enabled, devices not registered as authenticated cannot access the network.

The product achieves linked security using the following three functions.

1. Automatic recognition of ADECIA components
   The teleconferencing processor GUI automatically displays information about applicable network switches being controlled.
2. Remote network switch control
   From the teleconferencing processor, enable device authentication of the network switch.
3. Status notification from network switches
   A notification is sent to the teleconferencing processor if unauthorized access is detected by a network switch.

Definition of Terms Used

ADECIA

The ADECIA is a sound system equipped with microphones and speaker systems optimized for rooms/classrooms where teleconferencing or lectures will be conducted.
The ADECIA system includes the following components.

- Teleconferencing processor that handles routing within the system, audio processing, and connection to the computer where teleconferencing application software is installed
- Network switches for connecting to respective components
- Dante-compatible microphone
- Dante-compatible speaker system

Dante

Dante is a digital audio network specification developed by the Audinate Corporation.

Yamaha Unified Network Operation Service (Y-UNOS)

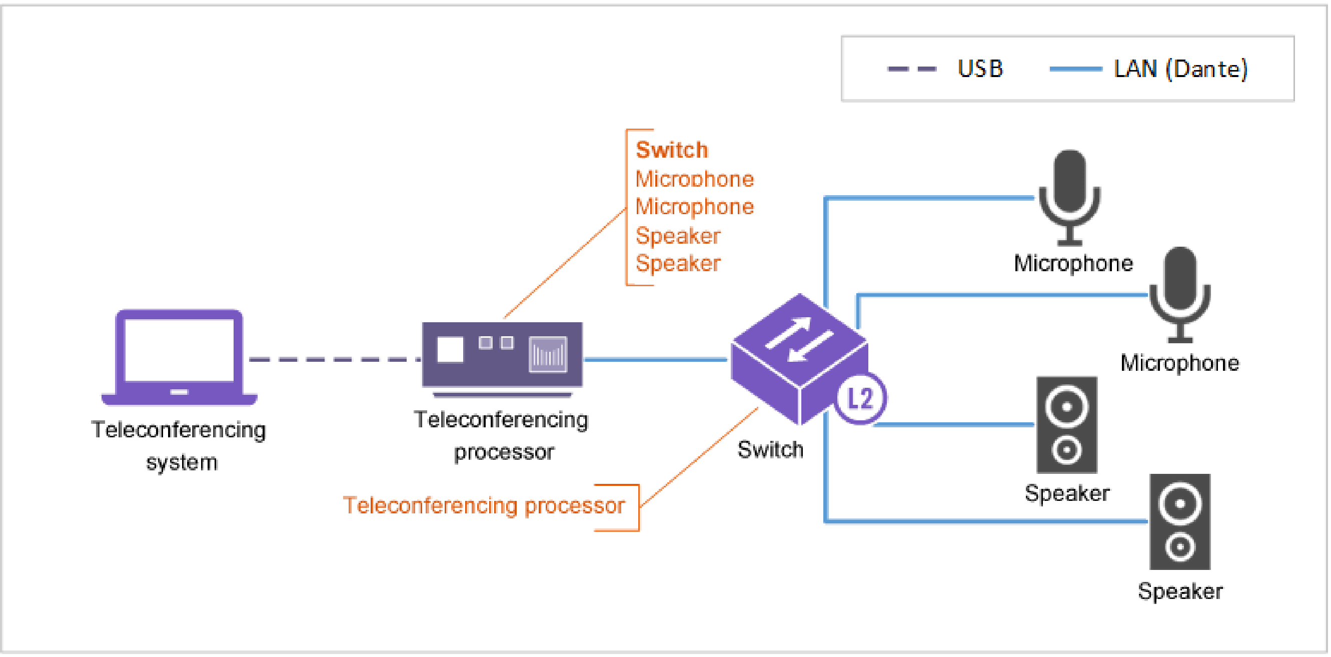
Y-UNOS is a service for linking devices via the network.
Also, network switches are linked to ADECIA security functionality by compliance with Y-UNOS. This product and teleconferencing processors in ADECIA components support the Y-UNOS service.

Function Details

Automatic recognition of ADECIA components

This product automatically recognizes Y-UNOS-compatible devices within the same network (maintenance VLAN) as the product.
Security links to the ADECIA system utilize this functionality for the following.

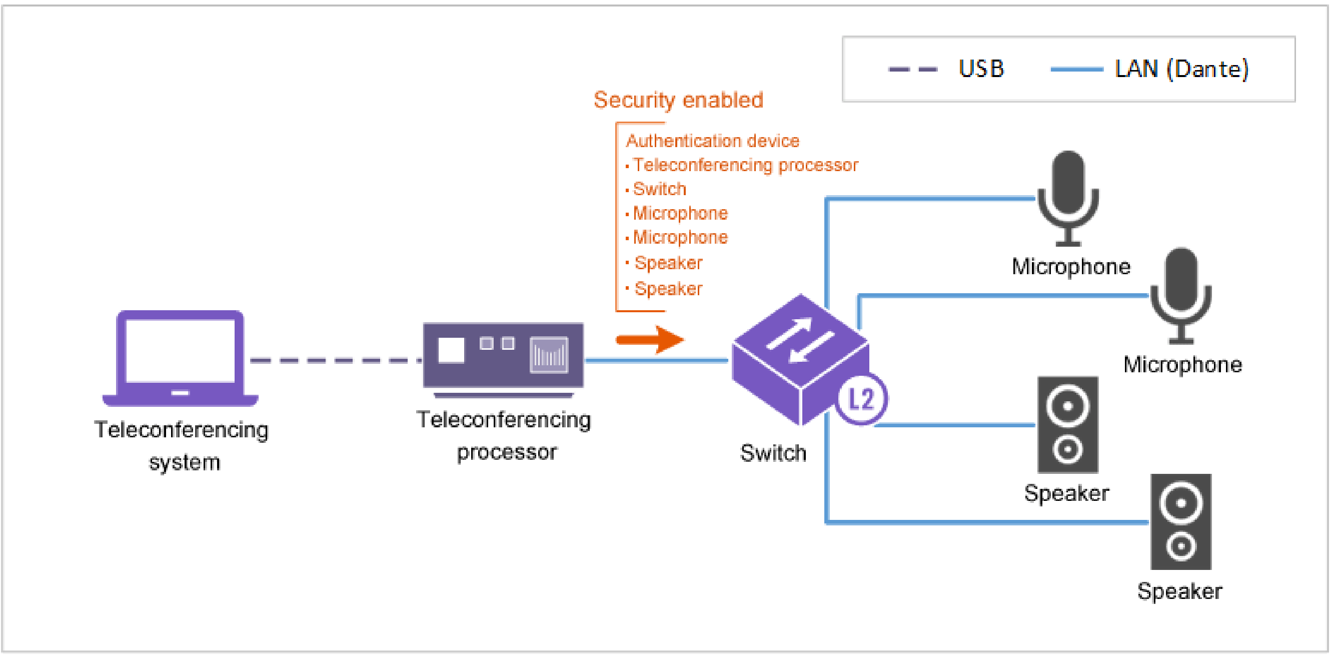
- The GUI for the teleconferencing processor displays a list of network switches where security is specified.
- The GUI for the teleconferencing processor displays a list of devices subject to device authentication (devices with permission for connecting to the network).
- The network switch determines which teleconferencing processor is notified of unauthorized access.



Remote network switch control

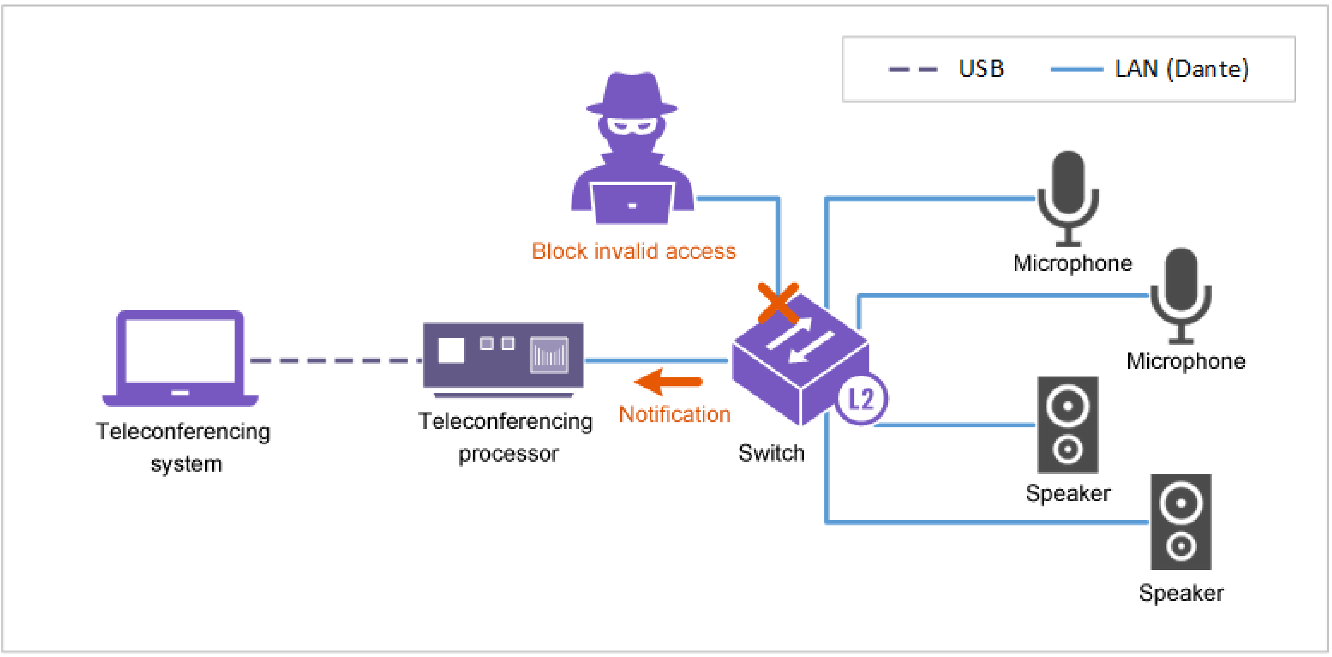
This product can use Y-UNOS functionality to apply settings from other devices connected to the same network (maintenance VLAN).
To link security, the following settings are applied to individual network switches by commands from the teleconferencing processor. Note that those settings are configured automatically by the security linking function for all devices at the same time, so users do not need to think about each setting.

- Generate root certificate authority
- Specify authenticated users (devices)
- Set local RADIUS server function
- Set host mode (all interfaces)
- Set MAC authentication function (all interfaces)
- Set RADIUS server host
- Set MAC authentication function for the entire system



Status notification from network switches

This product can use Y-UNOS functionality to notify other devices connected to the same network (maintenance VLAN) about its own status.
To link security, this product can notify all teleconferencing processors if invalid access to the product occurred (an unregistered device was connected).



Related Commands

Related commands are indicated below.
For command details, refer to the command reference.

Operations	Operating commands
Enable/disable the security linking function (Y-UNOS)	y-unos
Show Y-UNOS status	show y-unos

Security Linking Default Settings

If security is linked to the ADECIA system, use the most recent firmware to apply security linking settings.
For information about how to update the firmware and apply settings, refer to Linking security to ADECIA in the product technical information site for Yamaha network switch products.

Points of Caution

1. Be sure to configure default settings for security linking before the above functionality is first used.
2. Do not change settings during use, such as by using product commands or the GUI.
    - The functionality might not function properly if the settings are changed.
3. Be sure to remove the microSD card after default settings for security linking are executed.
    - If the microSD card left inserted, the firmware update and configuration will be applied the next time the product is started.
4. This function cannot be used if the stack function is enabled.
    - Disable the stack function before using this function.
    - Beware that the functionality for automatic SD card booting (firmware and system configuration) will not function if the stack function is enabled.

Related Documentation

- Use of External Memory
- Firmware Update
- Stack Function
- Yamaha network switch product technical information site—Linking security to ADECIA
- Yamaha network switch product technical information site—Firmware information
- ADECIA Product Information

Stack Function

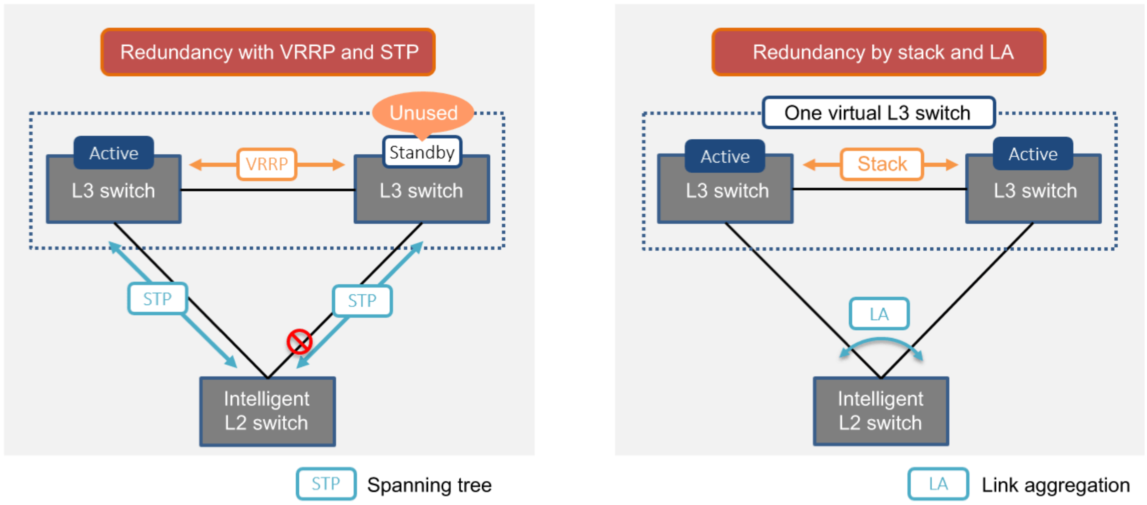
Function Overview

The stack function connects multiple network switches and **operates them as a single virtual network switch**.
The features of the stack are shown below.

1. Realizing the redundancy with high usage efficiency
   There are two methods for configuring networks without a single point of failure (SPOF). Either **configure networks with VRRPs and STPs** or **using stacks and link aggregation**.
   By using the stack, unlike VRRP, there is no standby network switch, so you can increase the usage efficiency of the network switch while ensuring redundancy.

2. Easy port expansion
   You can easily increase the number of available ports by adding network switches.

   - Stack overview



You can increase the usage efficiency of the switch while ensuring redundancy!
Easy port expansion!

The stack function is **disabled** in default factory settings.

Definition of Terms Used

Member switch

A network switch that makes up the stack.
Each switch is identified by a stack ID.

Stack ID

An ID that identifies the member switches that make up the stack.
The stack ID can be set from 1 to the maximum number of stacks that can be configured (currently 2).

Main switch

The main switch is selected from among member switches for managing other member switches.
Given default settings, the switch with stack ID 1 operates as the main switch.

Virtual switch

A single logical switch consisting of multiple member switches using the stack function.

Stack port
SFP+ slot used to connect the network switches that make up the stack.

Stack link
A connection between member switches that make up a stack.

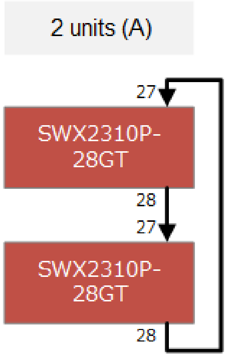
Function Details

Stack configuration

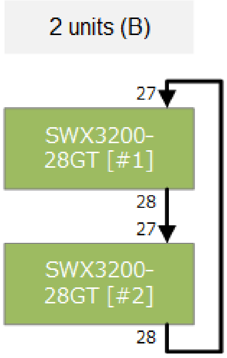
The configurations that can be stacked for each model are shown below.

Only configurations with two units of the same model are supported.
However, considering that stacks should reduce the impact of failures, **make sure stacks are always configured with two stack links.**

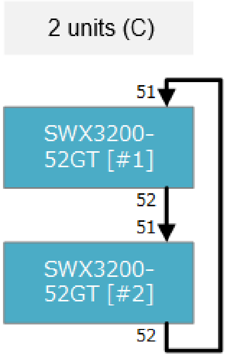
- SWX2310P-28GT stack configuration



- SWX3200-28GT stack configuration



- SWX3200-52GT stack configuration



Connection between member switches

When the stack function is enabled, the following SFP+ slots are switched to stack ports for connecting between members.

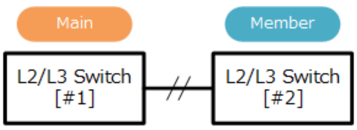
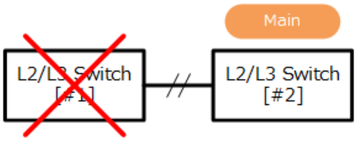
- SWX2310P-28GT : Ports 27 and 28
- SWX3200-28GT : Ports 27 and 28
- SWX3200-52GT : Ports 51 and 52

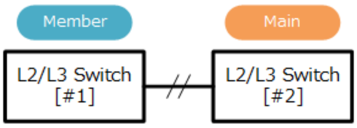
Unlike normal communication ports, stack ports are used only for communication between member switches. Connection between member switches is only possible with a **direct connection cable (YDAC-10G-1M/3M) or an SFP+ module (YSFP-10G-SR/LR)** provided by Yamaha.
When connecting with another company's product, the stack link will be forced down.
Stack ports are connected to the **lower and higher number ports** on member switches.

Main switch selection and MAC address assignment

The rules for main switch selection and MAC address assignment are indicated below.
Note that the MAC address used in the stack configuration is applied according to the following rules in order to eliminate the impact on communication.

1. In the default stack configuration, the MAC address of the main switch (switch with ID 1) is used as the MAC address of the virtual switch.
2. If a member switch other than the main switch is disconnected (due to an error) during stack configuration, then the virtual switch will continue to use the specified MAC address.
3. If the main switch is disconnected (due to an error) during stack configuration, the virtual switch will continue to use the specified MAC address.
   In other words, the MAC address of the network switch that is not included in the stack configuration is used.
4. Even if a network switch other than the failed switch (a network switch with a different MAC address) is installed as a member switch, the virtual switch will continue to use the specified MAC address.
   If you want to reconfigure the stack with the current configuration status, restart the virtual switch at the same time to perform reconstruction.
   (The stack with ID 1 becomes the main switch and the virtual switch uses the MAC address of the main switch.)
   - Main switch selection and MAC address assignment

No	Stack configuration		Main switch selection rule
1	Initial composition		The stack with ID 1 specified is selected as the main switch. In that case, the MAC address of stack ID 1 is used as the virtual switch MAC address.
2	Fault occurrence		If an error occurs in the main switch, the member switch with the smallest stack ID number is selected as the main switch. In that case, the virtual switch retains the MAC address of stack ID 1.

No	Stack configuration		Main switch selection rule
3	Abnormal state recovery		If a network switch with a failure is reinstalled in the stack, the switch currently selected as the main switch will continue to function as the main switch. In that case, the virtual switch MAC address remains the MAC address of stack ID 1 where the failure occurred.

Operations on virtual switches

Operations on virtual switches in a stack configuration are basically controlled from the main switch.
The specifications related to operation are shown below.

1. Logging in to a virtual switch **always logs into the main switch. ***
   If necessary, the *remote-login command can be used to log into another member switch.
   - Prompt when logging into the main switch

   ```
   Yamaha>
   ```

   - Prompt when logging into a member switch

   ```
   Yamaha-2> ①
   ```

   ① The stack ID number is indicated after the host name.
2. The configuration (running-config, startup-config) for the virtual switch is always synchronized between member switches.
   When finished configuring settings, be sure to save the running-config settings using the **write** command.
   Note, however, that the **write** command can only be executed from the main switch.
3. When operating a virtual switch, the information stored in the L2/L3 network switch (e.g. FDB learning information, ARP cache, etc.) is automatically synchronized.
   There is no need for the user to be aware of this.
4. To view the virtual switch log, log in and then execute the **show logging** command.
   In that state, the log shown is for the main switch. To view the log for a member switch, use the **remote-login** command to log into the applicable member switch and view the corresponding log.

Network switch status when stacking

The member switch manages the status in the stack configuration as follows.
That status can be viewed using the **show stack** command.

1. **Setting**
   - A state in which one or more stack port links are up, and the settings necessary for stacking between member switches are performed.
     Specifically, the configuration is automatically ascertained between member switches.
2. **Active**
   - A state in which automatic recognition of the configuration between member switches is completed, various settings are synchronized, and virtualization is performed by multiple member switches.

Virtualization is performed by two or more switches.

3. **Inactive**
    - A state in which a failure has occurred and the virtual switch has been removed.
      All communication ports, including stack ports, are forcibly shut down and communication is disabled. (Closed state)
4. **Standalone**
    - The stack function is enabled, but since negotiation cannot be performed with the member switch, it is operating on one unit.
      Transition to this state occurs when there is no opposing switch temporarily, such as during initial installation.
      In this state, the stack ID must be enabled, so it is operated **with the specified ID setting**.
5. **Standalone(separated)**
    - Same status as Standalone status indicated above.
      However, it remembers that a stack was once configured and retains main switch selection information that can be used when reconfiguring the stack.
6. **Disable**
    - The stack function is disabled.
      In this state, **the stack is operated with the ID number forcibly set to 1** (even if the stack ID was set to a value other than **1**).

Detection and measures for abnormal conditions

When a member switch in the stack configuration detects an error, it tries to resolve it autonomously within the virtual switch so that the network service is not affected.
This switch monitors the following abnormal conditions.

- **Abnormality detection on the local node**
    1. Does not meet stack configuration conditions (stack ID error, firmware version error)
    2. Stack link error (down detection)
    3. Fan stopped
    4. Thermal sensor abnormality (only for the SWX2310P-28GT)
    5. Voltage value error
    6. Current value error
- **Connection node error detection**
    1. Heartbeat frame reception timeout

Heartbeat is a function to check whether member switches are operating normally.
If the heartbeat frame is not received for a certain period (currently 4 seconds), it is determined that an error has occurred in the member switch.

The operation when an error is detected is shown below.

Detected node	Detected content		Operation after detection	State after detection	Remarks
Main switch	Setting error	Abnormal stack ID or firmware version	As a virtual switch, it is determined that processing cannot be continued, and the network port and stack link are forcibly taken down and disconnected from the stack configuration.	Inactive	
	Stack link down	One of the two links down	The status of the main switch is maintained, but two-way communication is achieved via one link.	Active	
		Both links down	The status of the main switch is maintained.	Standalone (separated)	Possible double-main status
	HW error	Fan stopped, thermal abnormality, voltage/current value error	In this state, it is determined that the network switch cannot continue to be treated as the main switch, so the network ports and stack links are forcibly disabled to disconnect the switch from the stack configuration.	Inactive	
	Heartbeat error	Notifications from member switches stopped	Continues to be operated as the main switch.	Standalone (separated) or Active	If there is only one remaining configuration, Standalone (separated)
Non-main member switch	Setting error	Abnormal stack ID or firmware version	As a virtual switch, it is determined that processing cannot be continued, and the network port and stack link are forcibly taken down and disconnected from the stack configuration.	Inactive	
	Stack link down	One of the two links down	The member switch status is maintained, but two-way communication is achieved with one switch.	Active	
		Both links down	Upgraded to a main switch to continue service.	Standalone (separated)	Possible double-main status
	HW error	Fan stopped, thermal abnormality, voltage/current value error	In this state, it is determined that the network switch cannot continue to be treated as a member switch, so the network ports and stack links are forcibly disabled to disconnect the switch from the stack configuration.	Inactive	
	Heartbeat error	Notifications from the main switch stopped	Upgraded to a main switch to continue service.	Standalone (separated) or Active	If there is only one remaining configuration, Standalone (separated)

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Setting stack functions	stack
Changing the stack ID number	stack renumber
Setting the IP address range used for stack ports	stack subnet
Show stack information	show stack

Stack Initial Settings

The initial setting flow for stack configuration is shown below.

1. Preparation of necessary equipment
2. Member switch settings
3. Connecting member switches

Preparation of necessary equipment

Prepare the equipment necessary to configure the stack.

- Member switch
  Prepare the member switches for stack configuration.
  For the stackable configurations, refer to **3.1 Stack configuration**.
- Stack port connection cable
  Determine and prepare the interfaces to connect the member switches.
  Use **direct connection cables** to configure stacks within a rack and **SFP+ modules** to configure them across longer distances, such as between floors or buildings.
  For more details, refer to **3.2 Connection between member switches**.
- External memory (SD card)
  It is recommended to use external memory to save backup data such as configs and logs during stack operation.
  By using external memory, you can use it to recover the config if a failure occurs.

Member switch settings

Set the member switches that constitute the stack.
Consider the following before you begin configuration.

1. **Determining stack IDs to be assigned to member switches**
   Stack IDs to be assigned to member switches must be **statically determined**.
   During initial settings, **stack ID: 1 will be the main switch.**
2. **Determining the save destination for the startup config**
   Determine the save destination for the startup config during stack configuration.
   Select 0 to 4 in the flash ROM as the save destination and indicate in the description that it is for saving stack information.

After reviewing, **configure member switches individually** according to the following procedure.

1. **Starting the member switches**
   Start the member switches individually and access them from the serial console.

2. **Checking and updating the firmware version**
   Use the **show environment** command to check the current firmware version.

```
Yamaha> show environment
SWX3200-52GT BootROM Ver.1.00
SWX3200-52GT Rev.4.00.05 (Fri Mar  9 09:34:05 2018) ①
main=SWX3200-52GT ver=00 serial=S00000000 MAC-Address=00a0.de00.0000
...
```

① Check the firmware version

Use the **RTpro** site to check the most recent version released.
If the public firmware version of the relevant switch is newer than the firmware that is running, update it.

- It is recommended that **the firmware version in member switches be updated to the latest version with fixes for known issues**.
- Given default settings, **firmware updating using an SD card** is enabled.
  Refer to **Firmware update** for how to update using an SD card.

3. **Setting the save destination for the startup config**
   Use the **startup-config select** command to select the configuration used for stack operations.
   At this time, it is recommended to set the description to use for the config during stack operation.

```
Yamaha> enable
Yamaha# startup-config description 2 Stack ①
Yamaha# startup-config select 2 ②
reboot system? (y/n): y ③
```

① Set the description “Stack” to startup-config #2

② Select startup-config #2

③ Restart the system

4. **Setting the stack ID**
   Check the network switch status with **show stack** to confirm that the stack function is disabled.
   Also check the stack ID. The default stack ID setting is **1**.

```
Yamaha> enable
Yamaha#
Yamaha# show stack
Stack: Disable

Configured ID        : 1
Subnet on stack port : Auto-ip
Virtual MAC-Address  : 00a0.de00.0000

ID  Model          Status      Role      Serial       MAC-Address
------------------------------------------------------------------------

Interface    Status
------------------------------------------------------------------------
```

```
Yamaha#
```

If necessary, change the stack ID number using the **stack renumber** command.

```
Yamaha(config)# stack 1 renumber 2 ①
Yamaha(config)# do show stack
Stack: Disable

Configured ID        : 2
Subnet on stack port : Auto-ip
Virtual MAC-Address  : 00a0.de00.0000

ID  Model          Status      Role     Serial       MAC-Address
------------------------------------------------------------------------

Interface    Status
------------------------------------------------------------------------

Yamaha#
```

① Change the stack ID number from #1 to #2

5. **Enabling the stack function**

Enable the stack function using the **stack enable** command.

After entering the command, reboot the device.
Default-config is applied after rebooting is finished.

```
Yamaha(config)#stack enable ①
reset configuration and reboot system? (y/n): y ②
```

① Enable the stack function

② Restart the system

After rebooting, check the network switch status with **show stack** to confirm that the stack function is enabled.
Also check the save destination of the startup config.

```
Yamaha> enable
Yamaha#
Yamaha# show stack
Stack: Enable ①

Configured ID        : 1
Running ID           : 1
Status               : Standalone
Subnet on stack port : Auto-ip
Virtual MAC-Address  : 00a0.de00.0000

ID  Model          Status      Role     Serial       MAC-Address
------------------------------------------------------------------------
1   SWX3200-52GT   Standalone  Main     S000000000   00a0.de00.0000
... (Because it is operating with one unit, it is Standalone Main)
```

```
Interface    Status
------------------------------------------------------------------------
port1.51     down
port1.52     down

Yamaha>show environment
SWX3200-52GT BootROM Ver.1.00
SWX3200-52GT Rev.4.00.05 (Fri Mar  9 09:34:05 2018)
main=SWX3200-52GT ver=00 serial=S00000000 MAC-Address=00a0.de00.0000
CPU:   2%(5sec)   2%(1min)   1%(5min)    Memory:  10% used
Fan status: Normal
Fan speed: FAN1=4000RPM FAN2=3870RPM
Startup firmware: exec0
Startup Configuration file: config2 ②
Serial Baudrate: 9600
Boot time: 2018/01/01 11:06:36 +09:00
Current time: 2018/01/02 16:12:23 +09:00
Elapsed time from boot: 1days 05:05:49
Temperature status: Normal
Temperature: 37 degree C
Voltage: 11.99V    Current: 0.741A
```

① The stack function is enabled

② Confirm that the specified startup config is correctly applied.

Connecting member switches

Connect stack-enabled network switches using **direct connection cables** or **SFP+ modules**.

For connection instructions refer to Connection between member switches.
The member switches **can be connected with either the power turned on or off**.

After connecting the member switches, check the system status using the **show stack** command.

```
Yamaha# 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
------------------------------------------------------------------------
1   SWX3200-52GT   Active      Main     S000000000   00a0.de00.0000
... (Switch with stack ID 1 is main)
2   SWX3200-52GT   Active      Member   S000000000   00a0.de00.0000
... (Switch with stack ID 2 is member)

Interface    Status
------------------------------------------------------------------------
port1.51     up
port1.52     up
port2.51     up
```

```
port2.52     up
```

Use the **backup system** command to back up the initial setting status of the member switch to the SD card.
By saving the following firmware files in the indicated folder on the SD card, both settings and firmware can be backed up during backup execution.

- SWX2310P-28GT: [Folder]/swx2310p/firmware, [Firmware file]swx2310p.bin
- SWX3200-28GT and SWX3200-52GT: [Folder]/swx3200/firmware, [Firmware file]swx3200.bin

```
Yamaha> enable
Yamaha# backup system ①
Succeeded to backup system files and firmware file.
Yamaha# remote-login 2 ②

Entering character mode
Escape character is '^]'.

SWX3200-52GT Rev.4.00.XX
  Copyright (c) 2018 Yamaha Corporation. All Rights Reserved.

Yamaha-2> enable
Yamaha-2# backup system ③
Succeeded to backup system files and firmware file.
```

① Copy all main switch settings to the SD card

② Remotely log in to a member switch (Stack ID: 2)

③ Copy all the settings for member switch (stack ID: 2) to the SD card

This completes the initial stack settings.

Install the virtual switch in the network to be used and perform the settings required for operation.
After completing the settings required for operation, backup should be performed in case of an abnormality, just as with the initial settings.

Exchanging Member Switches

The following describes how to replace a member switch after a fault occurs in a configuration with two SWX3200-52GT switches.
The following shows each case of using and not using an SD card.

Exchange procedure using an SD card

Member switches are exchanged by backup/restore using an SD card.

- Exchange procedure

  1. **In normal operation**
     After completing the setting to the member switches, back up the system information to the SD card in consideration of failure.

     To back up system information, execute the **backup system** command.
     Before backing up the system information, also backup the firmware by saving the swx3200.bin file (firmware file) in the /swx3200/firmware folder in the SD card.

  2. **Fault occurrence**
     Assume that an error occurs in the member switch with stack ID 2.

3. **Fault recovery**
   Prepare the member switches to be exchanged and connect the SD card that contains the backup of the failed switches.
   Apply the firmware and system information by executing the **restore system** command.
   After they are applied, **turn off the power, connect to the network switch currently functioning as the main switch, and turn on the power** to restore the stack configuration.

Exchange procedure without using an SD card

Exchange the member switches without using an SD card.

1. **At the start of operation**
   After installation of the member switches is completed, store the same revision firmware as the firmware written in the member switches on a PC, etc.
   Record the serial number, config ID being used, and stack ID of each member switch.

```
Yamaha> show environment
SWX3200-52GT BootROM Ver.1.00
SWX3200 Rev.4.00.05 (Fri Mar  9 09:34:05 2018)
main=SWX3200-52GT ver=00 serial=S00000000 MAC-Address=00a0.de00.0000 ①
CPU:   2%(5sec)   2%(1min)   1%(5min)    Memory:  10% used
Fan status: Normal
Fan speed: FAN1=4000RPM FAN2=3870RPM FAN3=3870RPM FAN4=4000RPM
Startup firmware: exec0
Startup Configuration file: config1 ②
Serial Baudrate: 9600
Boot time: 2018/01/01 11:06:36 +09:00
Current time: 2018/01/02 16:12:23 +09:00
Elapsed time from boot: 1days 05:05:49
Temperature status: Normal
Temperature: 37 degree C
Voltage: 11.99V    Current: 0.741A
Yamaha>
Yamaha> show stack
Stack: Enable

Configured ID        : 1 ③
Running ID           : 1
Status               : Active
Subnet on stack port : Auto-ip
Virtual MAC-Address  : 00a0.de00.0000

ID  Model          Status      Role     Serial       MAC-Address
------------------------------------------------------------------------
1   SWX3200-52GT   Active      Main     S000000000   00a0.de00.0000
2   SWX3200-52GT   Active      Member   S000000000   00a0.de00.0000

Interface    Status
------------------------------------------------------------------------
port1.51     up
port1.52     up
port2.51     up
port2.52     up
```

① Serial number

② Config ID

③ Stack ID

2. **Fault occurrence**
   Assume that an error occurs in the member switch with stack ID 2.

3. **Fault recovery**
   Prepare the member switches to be exchanged and write the saved firmware.
   Start the member switches and change the config ID used at startup.

   - If the config ID used at the start of operation was 0, there is no need to change the config ID.

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

     After rebooting, enable the stack function.
     For the stack ID to be set, refer to the member switch serial number and stack ID recorded at the start of operation.

     ```
     Yamaha> enable
     Yamaha# configure terminal
     Yamaha(config)# stack 1 renumber 2 ①
     Yamaha(config)# stack enable ②
     reset configuration and reboot system? (y/n): y
     ```

     ① Set stack ID 2

     ② Enable the stack function

     After enabling the stack function, **turn off the power, connect to the network switch functioning as the main switch, and turn on the power** to restore the stack configuration.

Firmware Update

The following two methods are provided for updating the firmware during stack configuration.

1. **Method to update member switches during configuration simultaneously (parallel update)**
2. **Method to update without stopping network services (sequential update)**

Parallel update is an effective method if you have enough time to allow a service outage.
However, *during stack configuration, it is recommended that updates be performed sequentially without a service outage. *
Note that firmware updates during stack configuration are supported only for the following.

- Update based on using a TFTP client or web GUI to send the firmware update
- Update using an SD card

If the firmware is updated while the SD card is inserted, SD card boot may be performed when restarting.
The SD card boot can be disabled with the **boot prioritize sd** command.

```
Yamaha> enable
Yamaha# boot prioritize sd disable ①
reboot system? (y/n): y
```

① Disable SD card boot

For more information, refer to **Firmware Update**.

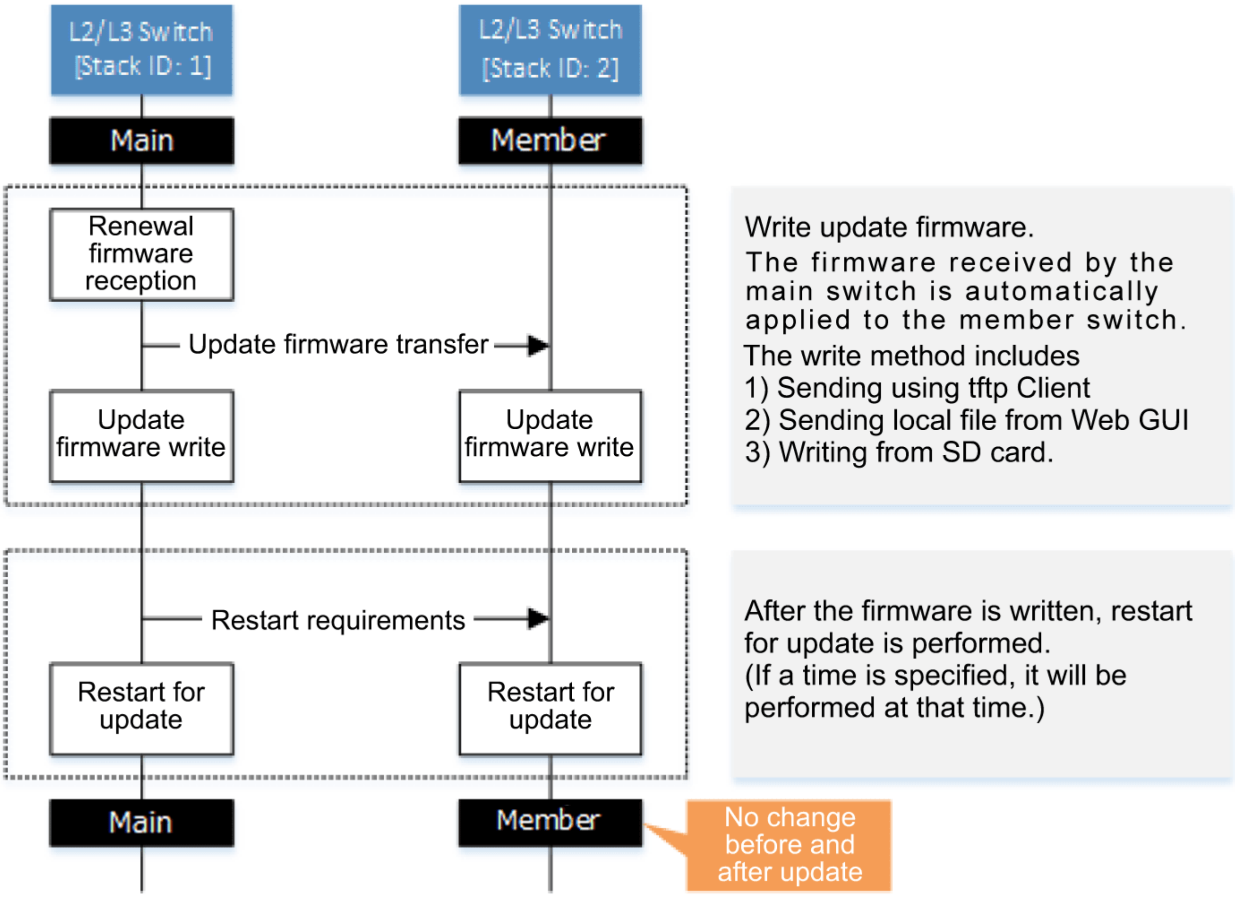
Firmware parallel update

Firmware parallel update updates the firmware of the member switches in the stack configuration at the same time.
The service will be stopped because the entire virtual switch is restarted for the update.
Note the following points when performing parallel update.

- Confirm that the firmware update method is set to **normal** (**firmware-update reload-method** command).
- Confirm that the firmware update application time is set to the **specified time** (**firmware-update reload-time** command).

An overview of parallel update is shown below.

- Parallel update process flow



Write update firmware.
The firmware received by the main switch is automatically applied to the member switch.
The write method includes
1) Sending using tftp Client
2) Sending local file from Web GUI
3) Writing from SD card.

After the firmware is written, restart for update is performed.
(If a time is specified, it will be performed at that time.)

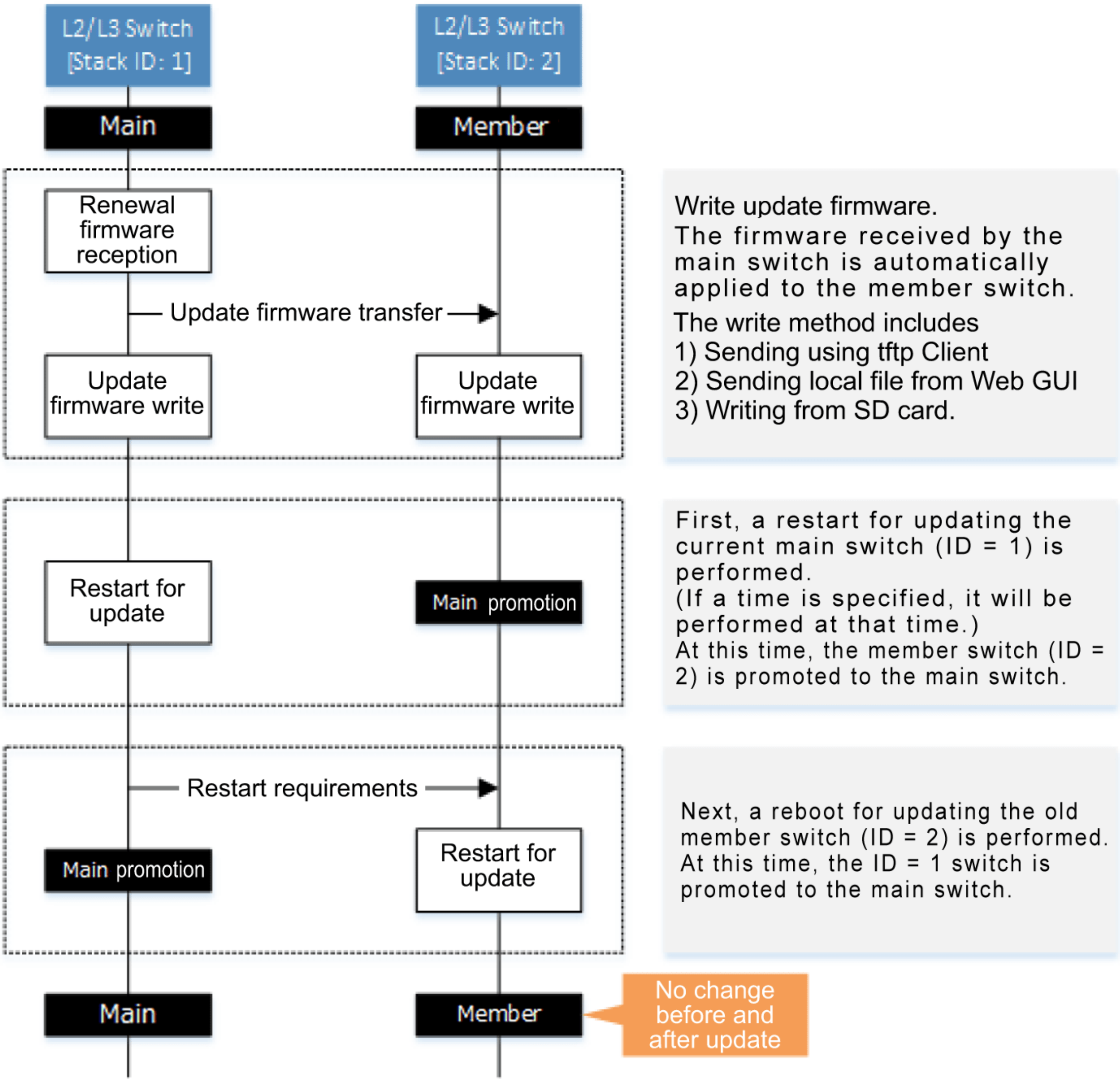
Firmware sequential update

Firmware serial update updates the firmware of the member switches in the stack configuration sequentially.
This update does not involve any service outage because the entire virtual switch does not need to be rebooted for the update. (* Refer to section 6 in **Points of Caution**.)
When performing a sequential update, note the following points.

- Confirm that the firmware update method is set to **sequential** (**firmware-update reload-method** command).
- Confirm that the firmware update application time is set to the **specified time** (**firmware-update reload-time** command).

An overview of sequential update is shown below.

- Sequential update process flow


L2/L3 Switch [Stack ID: 1]
L2/L3 Switch [Stack ID: 2]
Main
Member
Renewal firmware reception
Update firmware transfer
Update firmware write
Update firmware write
Write update firmware.
The firmware received by the main switch is automatically applied to the member switch.
The write method includes
1) Sending using tftp Client
2) Sending local file from Web GUI
3) Writing from SD card.
Restart for update
Main promotion
First, a restart for updating the current main switch (ID = 1) is performed.
(If a time is specified, it will be performed at that time.)
At this time, the member switch (ID = 2) is promoted to the main switch.
Restart requirements
Main promotion
Restart for update
Next, a reboot for updating the old member switch (ID = 2) is performed.
At this time, the ID = 1 switch is promoted to the main switch.
Main
Member
No change before and after update

Points of Caution

1. When the stack function is enabled, the following functions cannot be used.
   - RMON
   - IPv6
   - VRRP
   - MLD snooping
2. When the stack function is enabled, it can be used as a function, but some restrictions occur.
   - Mirroring function
     - Mirroring between member switches is not possible.
   - Flow control
     - Pause frame cannot be transmitted.
   - Back pressure function

        - When communicating via the stack port, jam signals are not transmitted.
    - Port LED
        - Only for the SWX2310P-28GT, the LED does not blink in Link/Act mode.
    - SFP optical reception level monitoring
        - The optical reception level of the stack port is not monitored.
    - Link aggregation
        - The maximum number of logical interfaces is reduced by one.
    - MODE button
        - When a stack is configured with the SWX2310P-28GT switches, control using the MODE button is **disabled**.
          As with the SWX3200-28GT/52GT switches, **this network switch automatically transitions to STATUS mode** when a loop occurs.
    - Command line input
        - The users who can transition to global configuration mode are limited.
          When the console side is in global configuration mode and the telnet side transitions to global configuration mode, the console side automatically transitions to privileged EXEC mode.
          Console, telnet, ssh, remote login, and GUI settings are exclusively controlled.
        - It is not possible to log in from the main switch and other member switch consoles at the same time.
    - DHCP client
        - If the stack function is enabled and the Auto IP function is used on the stack port, the DHCP client cannot be used.
    - startup-config select command
        - Do not use the **startup-config select** command while the stack is configured. It may become impossible to configure correctly.
          To switch the config using the startup-config select command, disconnect the direct attach cable and cancel the stack configuration before executing.

3. When the stack function is enabled, make sure that the stack configuration is configured before setting functions with commands or the GUI.
   If the stack is not configured correctly, the settings may not be reflected correctly.
   The **write** command and **copy running-config startup-config** command can be executed only on the main switch (in an active state).
   They cannot be executed on a member switch or an incorrectly configured stack.
4. When the stack function is enabled, the stack control packets use transmission queues #7 and #6, so do not assign other packets to transmission queues #7 and #6.
   When QoS is enabled, transmission queues #7 and #6 are assigned by default in the CoS-transmission queue ID conversion table, so change the assignment.
5. When the stack function is enabled, the initial setting for the transmission queue specification for frames transmitted from the network switch unit is transmission queue #6.
   Do not change the transmission queue specification setting for frames transmitted from the network switch unit from the initial setting.
6. If there is a difference between the settings (startup-config) in the main switch and in a member switch during stack configuration, the member switch settings are changed and the switch is rebooted.
7. If there is a difference between the stack port IP address range settings for the main switch and a member switch during stack configuration, communication between stacks cannot be performed properly.

Related Documentation

- Firmware Update

Default Settings List

SWX2310P series default settings are indicated below.

- System-wide default settings

Category	Setting Parameter	Setting value
Console	Console timeout	600 sec
	Number of VTYs	8
	Number of lines displayed	24
Password	Default administrative user	User name: admin Password: admin
	Administrative password	admin
	Encrypt password	Not encrypted
Time Management	Time zone	JST (UTC＋9.0)
	NTP server	None
	NTP update cycle	Once per hour
SNMP	Action	Disabled
RMON	Action	Enabled
sFlow	Action	Disabled
SYSLOG	debug level log output	OFF
	information level log output	ON
	error level log output	ON
	SYSLOG server	None
Firmware Update	Download URL	firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2310p.bin
	Permit downward revision	Prohibit
	Timeout	300 sec
LLDP	Action	Enabled
	Automatic setting function	Enabled
L2MS	Action	Enabled
	Role	Agent
Stacking	Action	Disabled
	Stack ID	1
	IP address range used for stack port	Auto IP

Category	Setting Parameter	Setting value
Access control	Telnet server status	Start
	Telnet server access	Allow only VLAN #1
	SSH server status	Do not start
	TFTP server status	Do not start
	HTTP server status	Start
	HTTP server access	Allow only VLAN #1
	Secure HTTP server status	Do not start
Maintenance VLAN	VLAN interface	VLAN #1
Interface control	Link aggregation	None
	Port authentication	Disabled
	Port security	Disabled
	PoE supply	Enabled
Layer 2 functions	Automatic MAC address acquisition	Enabled
	Automatic MAC address acquisition aging time	300 sec
	Spanning tree	Enabled
	Unique Loop Detection	Disabled
	Multiple VLAN	None
Layer 3 functions	Static routing	None
	Routing between VLANs	Disabled
	Policy-based routing	-
	OSPF	-
	RIP	-
	VRRP	-
IP multicast	IGMP snooping	Disabled
	MLD snooping	Disabled
	IGMP	-
	PIM	-
DNS client	Action	Enabled

Category	Setting Parameter	Setting value
Traffic control	QoS	Disabled
	QoS (DSCP - Transmission queue ID conversion table)	None
	Flow control (IEEE 802.3x)	Disabled
	ACL	None
AP layer functionality	DHCP server	-
	DHCPv6 server	-
	DHCP relay	-
	DNS relay	-
	RADIUS server	Disabled
WebGUI	Language setting	Japanese

- Default settings for each LAN/SFP port

Category	Setting Parameter	Setting value
Basic settings	Speed/communication 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
	Unique Loop Detection	Enabled
Traffic control	QoS trust mode	CoS
	Flow control (IEEE 802.3x)	Disabled
	Storm Control	Disabled
LLDP agent	Transmit/receive mode	Transmit and receive
PoE supply	Power supply actions	Enabled
	PoE power priority	Low

- Settings for default VLAN (vlan1)

Category	Setting Parameter	Setting value
Layer 3 functions	IPv4 address	192.168.100.240/24

Category	Setting Parameter		Setting value
IP multicast	Multicast frame forwarding		239.192.128.250 (for Y-UNOS)
	IGMP Snooping	Action	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	Action	Disabled
		Querier	Disabled
		Fast-Leave	Disabled

Interface Control Functions

Basic Interface Functions

Function Overview

Here we explain the basic interface functions of this product.

Definition of Terms Used

Combo port

There are two types of ports to choose from: LAN port and SFP port.
The LAN port and SFP port cannot be used at the same time. If both ports are connected, the SFP port has priority.
If there is a valid setting for only the LAN port, it will not be applied to the SFP port.

Function Details

Interface types

This product can handle the five interface types shown in the table below.

Interface types	Interface ID	Explanation
LAN port	port	This is a physical port of this product. There are three types: a fixed LAN port and a removable SFP/SFP+ port. This interface is expressed as **port** followed by "stack ID" + "." + "port number printed on the chassis." Specifying LAN port #1: **port1.1**
Combo port		
SFP+ port		
VLAN interface	vlan	This is a User-defined VLAN. This interface is expressed as **vlan** followed by "VLAN ID". Specifying VLAN1: **vlan1**
Static logical interface	sa	This is the User-defined link aggregation. Multiple LAN/SFP ports can be grouped together and used as one interface. This interface is expressed as "**sa**" or "**po**," followed by "logical link ID." Specifying the LACP logical interface for logical link ID #1: po1
LACP logical interface	po	

Interface control

The interface on this product can be controlled as shown in the table below.

- Interface control items

Control items	Commands	Explanation
Set description	**description**	Sets the description text for the applicable interface.
Enable/disable	**shutdown**	Enables/disables the interface.
Communication speed/communication mode	**speed-duplex**	Sets the communication speed and communication mode for the interface. (Select from the following values.) - Auto negotiation - 10Gbps / Full duplex - 1Gbps / Full duplex - 100Mbps / Full duplex - 100Mbps / Half duplex - 10Mbps / Full duplex - 10Mbps / Half duplex
MRU	**mru**	Sets the maximum frame size that can be received by the interface, within a range of **64–10,240 bytes**.
Cross/straight automatic detection (Auto MDI/MDI-X function)	**mdix**	Automatically detects the port type (MDI or MDI-X) of the connected port and the cable type (cross or straight). This function gives the ability to interconnect without dependency.
Speed downshift	-	This function automatically reduces the speed and attempts to link when a LAN cable that cannot be used with 1000BASE-T is connected. This function is always enabled for LAN ports. (Cannot be disabled.)
EEE	**eee**	Sets whether to use the energy saving technology for Ethernet (EEE: Energy Efficient Ethernet). This is standard for IEEE 802.3az.

Command control of the interface is performed as shown on the table below.

- Interface control functionality chart

Interface name	Set description	Enable/disable	Communication speed/communication mode	MRU	Cross/straight automatic detection	EEE
LAN port	Yes	Yes	Yes (*1)	Yes	Yes	Yes
Combo port	Yes	Yes	Yes (*2)	Yes	Yes (*3)	Yes (*3)
SFP+ port	Yes	Yes	Yes (*4)	Yes	No	No
VLAN interface	Yes	No	No	No	No	No
Static logical interface	Yes	Yes	No	No	No	No
LACP logical interface	Yes	Yes	No	No	No	No

1 : The communication speed/communication mode setting for the LAN port cannot be selected as *10Gbps / Full duplex.
2: The communication speed/mode setting for the combo port is either *auto negotiation or **1Gbps / Full duplex**.
3: The settings for the combo port are applied only to LAN ports.
***4: The communication speed/communication mode setting for the SFP+ port can be either *auto negotiation** or **10Gbps / Full duplex**.
If **10Gbps / Full duplex** is set and an SFP module is connected, the module will operate at **1Gbps / Full duplex**.

LAN/SFP port defaults

The product LAN/SFP ports are in the following state given default settings.

- All LAN/SFP ports function as access ports (ports that handle untagged frames), and belong to the default VLAN (VLAN #1).
- The following functions are enabled for the default VLAN (VLAN #1) to which all LAN/SFP ports belong.
  - MSTP：Multiple Spanning Tree Protocol
  - IGMP Snooping
  - IPv4 address (192.168.100.240/24)
  - Access from a Telnet client
  - Access from a web client

Port mirroring

This product provides a port mirroring function, which copies the data traffic from a selected LAN/SFP port to another specified port.
The communication status can be analyzed by collecting the copied packets.
The product enables specifying up to one sniffer port.
The monitoring direction (send/receive, send only, or receive only) can be selected for monitored ports.
The **mirror** command can be used to set the port mirroring.
The port mirroring setting is disabled in default settings.

Frame counter

This product counts the number of frames transmitted/received for each LAN/SFP port. (This is called a “frame counter”.)
To reference the frame counter, use the **show frame counter** command.
The table below shows the display items for the frame counter and their maximum values.

- Received frame counter display items

Display item	Explanation	Maximum value
Octets	Number of octets received	18,446,744,073,709,551,615
Packets (*1)	Number of received packets	34,359,738,360
Broadcast packets (*2)	Number of broadcast packets received	4,294,967,295
Multicast packets (*2)	Number of multicast packets received	4,294,967,295

Display item	Explanation	Maximum value
Unicast packets (*2)	Number of unicast packets received	4,294,967,295
Undersize packets (*2)	Number of undersize packets received (packets smaller than 64 octets)	4,294,967,295
Oversize packets (*2)	Number of oversize packets received (packets larger than 1523 octets (*3))	4,294,967,295
Fragments (*2)	Number of fragment packets received (packets smaller than 64 octets with abnormal CRC)	4,294,967,295
Jabbers (*2)	Number of jabber packets received (packets larger than 1523 octets with abnormal CRC (*3))	4,294,967,295
FCS errors (*2)	Number of FCS error packets received	4,294,967,295
RX errors	Number of reception errors	4,294,967,295
Drop packets (*4)	Number of packets dropped from the reception buffer	4,294,967,295

(*1) : The packet value is the total of the (*2) packets.

(**3): This will change, depending on the *MRU** that is set for the LAN/SFP port.
(*4): This is shown only if tail drop is disabled.

- Transmitted frame counter display items

Display item	Explanation	Maximum value
Octets	Number of octets transmitted	18,446,744,073,709,551,615
Packets (*1)	Number of packets transmitted	12,884,901,885
Broadcast packets (*2)	Number of broadcast packets transmitted	4,294,967,295
Multicast packets (*2)	Number of multicast packets transmitted	4,294,967,295
Unicast packets (*2)	Number of unicast packets received	4,294,967,295
TX errors	Number of transmission errors	4,294,967,295
Collisions	Number of collision occurrences	4,294,967,295
Drop Packets(*3)	Number of tail-dropped transmission packets	536,870,911

(*1) : The packet value is the total of the (*2) packets.
(*3): This is shown only if tail drop is enabled.

- Transmitted/received frame counter display items

Display item	Explanation	Maximum value
64 octet packets	Number of packets with 64 octet length transmitted/received	4,294,967,295
65–127 octet packets	Number of packets with 65–127 octet length transmitted/received	4,294,967,295

Display item	Explanation	Maximum value
128–255 octet packets	Number of packets with 128–255 octet length transmitted/received	4,294,967,295
256–511 octet packets	Number of packets with 256–511 octet length transmitted/received	4,294,967,295
512–1,023 octet packets	Number of packets with 512–1,023 octet length transmitted/received	4,294,967,295
1,024 to MAX octet packets	Number of packets with 1,024–maximum octet length (*1) transmitted/received	4,294,967,295

(*1): This will change, depending on the **MRU** that is set for the LAN/SFP port.

The frame counter can also be cleared by using the **clear counters** command.

When you execute the **show interface** command which shows the status of the LAN/SFP ports, information on the number of transmitted and received frames is shown, but this information is shown based on the frame counter information.
The number of frames transmitted/received that is displayed using the **show interface** command and how the frame counter is handled are shown below.

- Number of frames transmitted/received that is displayed by the **show interface** command, and how the frame counter is handled

Display item		Information on the frame counter referred to
input	packets	**Received frame counter** packets
	bytes	**Received frame counter** octets
	multicast packets	**Received frame counter** multicast packets
	drop packets(*1)	**Received frame counter** drop packets
output	packets	**Transmitted frame counter** packets
	bytes	**Transmitted frame counter** octets
	multicast packets	**Transmitted frame counter** multicast packets
	broadcast packets	**Transmitted frame counter** broadcast packets
	drop packets(*1)	**Transmitted frame counter** drop packets

(*1): If tail drop is enabled this shows only the transmission information; if it is disabled this shows only the reception information.

SFP module optical receive level monitoring

This product provides the function for monitoring the optical receive level of an SFP/SFP+ module connected to the SFP/SFP+ port.
If a fault occurs in an SFP/SFP+ module's optical receive level, this product's port lamp indications change to a dedicated state, and a SYSLOG message is output.
The optical RX power error state can be forcibly cleared by pressing and holding the MODE switch for three seconds.
When the optical receive level returns to the normal range, this product's port lamp indications will recover, and a SYSLOG message is output.

The SYSLOG message is not output when the corresponding port is linked down or the optical RX power error state is forcibly cleared.
The SFP/SFP+ module's optical receive level monitoring settings can be made using the **sfp-monitor** command.
By default, SFP module optical receive level monitoring is enabled.

Tx queue usage monitoring

If the transmit queue's usage ratio becomes high (above 60%, above 100%), a SYSLOG message is output.
A SYSLOG message is also output when the transmit queue's usage ratio returns to the normal range (below 50%).
The tx queue usage monitoring setting (for the entire system or individual LAN/SFP ports) can be set using the **tx-queue-monitor** command.
All tx queue usage monitoring settings are enabled in default settings.

ifIndex Assignment

ifIndex is an ID number linked to the interface and used by SNMP, DHCP, etc.
It is assigned as indicated in the table below.

Range of ifIndex	Interface assignment	Assignment rule	Example
301 - 4394	VLAN interface	ifIndex = 300 + VLAN ID	301: vlan1 4394: vlan4094
4501 - 4596	Static logical interface	ifIndex = 4500 + static logical interface number	4501: sa1 4596: sa96
4601 - 4727	LACP logical interface	ifIndex = 4600 + LACP logical interface number	4601: po1 4727: po127
5001 - 6050	LAN/SFP port	ifIndex = 4000 + 1000 × stack ID + port number	5001: port1.1 6001: port2.1 6050: port2.50

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

- Basic interface functions: list of related commands

Operations	Operating commands
Set description	description
Shutdown	shutdown
Set communication speed and communication mode	speed-duplex
Set MRU	mru
Set cross/straight automatic detection	mdix auto
Set EEE	eee
Show EEE capabilities	show eee capabilities
Show EEE status information	show eee status

Operations	Operating commands
Set port mirroring	mirror
Show port-mirroring status	show mirror
Show interface status	show interface
Show simplified interface status	show interface brief
Show frame counter	show frame-counter
Clear frame counters	clear counters
Show SFP/SFP+ status	show ddm status
Set SFP module optical receive level monitoring	sfp-monitor rx-power
Set tx queue usage monitoring setting (system)	tx-queue-monitor usage-rate
Set tx queue usage monitoring setting (LAN/SFP ports)	tx-queue-monitor usage-rate
Show the tx queue usage monitoring setting	show tx-queue-monitor
Resets interface	interface reset

Examples of Command Execution

Basic LAN port settings

Some examples of basic LAN port settings are shown below.
For details on how to make the settings, refer to the Command Reference.

- Set the description text for LAN port #1 (port1.1).

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#description Connected to rtx1200-router
```

- Disable LAN port #1 (port1.1).

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#shutdown
```

- Enable LAN port #1 (port1.1).

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#no shutdown
```

- Set the communication speed and communication mode for LAN port #1 (port1.1) to **100Mbps/Full**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#speed-duplex 100-full
```

Set port mirroring

In this example, we will set LAN port #1 to monitor the frames transmitted by LAN port #4 and the frames transmitted by LAN port #5.
The roles of the ports are shown below.

- Sniffer port: LAN port #1 (port1.1)
- Monitored port: LAN port #4 (port1.4), LAN port #5 (port1.5)
  1. Specifies the monitored port for LAN port #1 (port 1.1), which is a sniffer port.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#mirror interface port1.4 direction both ①
Yamaha(config-if)#mirror interface port1.5 direction transmit ②
```

① Monitor transmitted and received frames

② Monitor transmitted frames

  2. Checks the port mirroring setting.

```
Yamaha#show mirror
Sniffer Port   Monitored Port  Direction
=============  ==============  ==========
port1.1        port1.4         both
port1.1        port1.5         transmit
```

Show LAN/SFP port information

- Confirm the status of LAN port #1 (port1.1).

```
Yamaha#show interface port 1.1
Interface port1.1
  Link is UP
  Hardware is Ethernet
  HW addr: 00a0.deae.b89f
  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          : 0
           bytes            : 0
           multicast packets: 0
    output packets          : 0
           bytes            : 0
           multicast packets: 0
           broadcast packets: 0
```

```
            drop packets     : 0
```

Points of Caution

None

Related Documentation

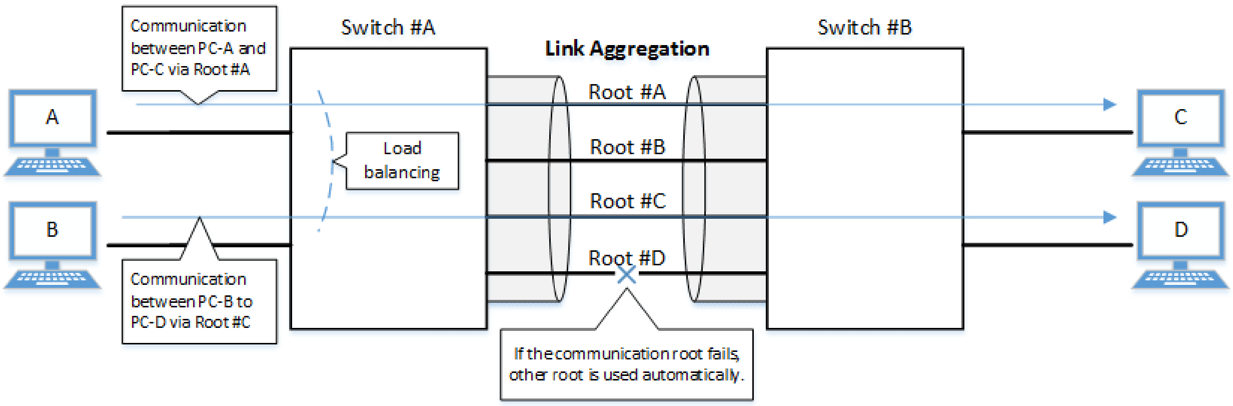
None

Link aggregation

Function Overview

Link aggregation is a function used to combine multiple LAN/SFP ports that connect network devices, and handle them as a single logical interface.
Link aggregation is a technology that is useful when multiple communications occur. Communications can be distributed by using a load balance function within the combined lines.
If one LAN/SFP port fails within the lines that were combined using link aggregation, and communications cannot be made, the other ports will continue communicating.

- Link aggregation function overview


Communication between PC-A and PC-C via Root #A
Switch #A
Link Aggregation
Switch #B
A
B
C
D
Root #A
Root #B
Root #C
Root #D
Load balancing
Communication between PC-B to PC-D via Root #C
If the communication root fails, other root is used automatically.

The link aggregation functions in this network switch are shown below.

- Link aggregation functions

Functions provided	Contents
Static link aggregation	Link aggregation for manually setting the LAN/SFP ports to combine. This begins to operate as a logical interface when the LAN/SFP ports link up.
LACP link aggregation	Link aggregation that uses **LACP** to combine the LAN/SFP ports. This begins to operate as a logical interface when the negotiation via LACP between the connected devices is successful.

Definition of Terms Used

LACP

Abbreviation for “Link Aggregation Control Protocol”. This is a technology standardized in IEEE802.1AX-2008, and is also called EtherChannel.

- IEEE802.1AX-2008 Link Aggregation Task Force

Load balance

This is a function to distribute forwarded frames between the LAN/SFP ports that are associated with the logical interface.
As a distribution rule, the L2/L3/L4 information within frames is used.

Function Details

Static/LACP link aggregation: common specifications

The common specifications for the static/LACP link aggregation functions of this network switch are shown below.

1. The link aggregation on this network switch can be defined for **127 interfaces,** including both static and LACP (126 interfaces for stacks).
   A single logical interface can be associated with **up to eight LAN/SFP ports**.
2. The settings shown below must be the same for each of the LAN/SFP ports contained within.
   - Port mode (access/trunk [including native VLAN settings])
   - Associated VLAN
   - QoS trust mode (including port priority and default CoS settings)
   - Loop detection (enables/disables loop detection and enables/disables port blocking)
3. Executes the following process when a LAN/SFP port is associated with a logical interface.
   - LAN/SFP ports that are linked up will be **linked down**.
     The logical interface's default value will be set to **shutdown**, in order to safely integrate the logical interface into the system.
   - MSTP settings will be discarded and will revert to their defaults.
     When dissociating a LAN/SFP port from the logical link, the MSTP settings for the relevant port will revert to their defaults as well.
4. The following operations can be performed for the logical interface.
   - Add description text (**description** command)
   - Enable/disable the interface (**shutdown** command)
5. Another LAN/SFP port cannot be associated with a logical interface in operation.
   To associate a LAN/SFP port, make sure to **shut down** the logical interface before associating.
6. LAN/SFP ports that are associated with a logical interface that is in operation cannot be removed.
   When dissociating a LAN/SFP port, make sure to **shut down** the logical interface before dissociating.
   LAN/SFP ports that have been dissociated from a logical interface will be in **shutdown** mode. Enable the ports as necessary (using "**no shutdown**").
7. Load balance settings can be made on the logical interface. The rules that can be set for this are shown below.
   The default value when defining a logical interface is the **destination/source MAC address**.
   - Destination MAC address
   - Source MAC address
   - Destination/source MAC address
   - Destination IP address
   - Source IP address
   - Destination/source IP address
   - Destination port number
   - Source port number
   - Destination/source port numbers

Static link aggregation

The operating specifications for static link aggregation are shown below.

1. An interface number from **1–96** can be assigned to the static logical interface.
2. Use the **static-channel-group** command to associate a LAN/SFP port with a static logical link interface.
    - When associating a LAN/SFP port with an interface number for which there is no static logical interface, a new logical interface will be generated.
    - When the associated port no longer exists as a result of removing a LAN/SFP port from a static logical interface, the relevant logical interface will be deleted.
3. Use the **show static-channel-group** command to show the static logical interface's status.

LACP link aggregation

The operating specifications for LACP link aggregation are shown below.
Refer to **"3.1 Static/LACP link aggregation: common specifications"** for the common specifications of static link aggregation.

1. An interface number from **1–127** can be assigned to the LACP logical interface.
2. Use the **channel-group** command to associate a LAN/SFP port with an LACP logical link interface.
    - When associating an LAN/SFP, specify the following **operating modes**. (It is recommended to specify "active mode".)
        - **Active mode**
          The LACP frame will be voluntarily transmitted, and negotiation with the opposing device's port will begin.
        - **Passive mode**
          The LACP frame will not be voluntarily transmitted, but will instead be transmitted when a frame is received from the opposing device.
    - When associating a LAN/SFP port with an interface number for which there is no LACP logical interface, a new logical interface will be generated.
    - When the associated port no longer exists as a result of removing a LAN/SFP port from an LACP logical interface, the relevant logical interface will be deleted.
3. The parameters that influence the operations of the LACP logical interface are shown below.
    - **LACP timeout**
      LACP timeout indicates the down time that was determined, when an LACP frame has not been received from the opposing device.
      Specify either "**Long" (90 sec.) or "Short" (3 sec.)** using the **lacp timeout** command.
      The LACP timeout value is stored in the LACP frame and transmitted to the opposing device.
      The opposing device that received the frame will transmit the LACP frames it has stored at **intervals equaling 1/3** of the LACP timeout value.
      The default value when the logical interface is generated is "**Long (90 sec.)**".
    - **LACP system priority**
      The LACP system priority is used when deciding **which device will control the logical interface**, when communicating with the opposing device. The **LACP system priority** and **MAC address** values (in combination referred to as the **system ID**) are exchanged with the interfacing device and the device with the highest LACP system priority level is assigned control. If both devices have the same LACP system priority level, the device with the lower MAC address is assigned control.
      The device assigned control determines which LAN or SFP ports associated with the logical interface are enabled (activated).
      LACP system priority values within the range **1 to 65535** can be specified using the **lacp system-priority** command, where the lower the setting value, the higher the priority level. The default value when the logical interface is generated is set to **32768 (0x8000)**.
    - **LACP port priority**
      LACP port priority is used to **control active/standby for the LAN/SFP ports that are associated with**

the logical interface. If more than the maximum number of LAN/SFP ports (8 ports) is associated with a logical interface, then the port status is controlled based on the **LACP port priority**.
If ports have the same **LACP port priority**, then the port with the lower **port number** is given priority.
If a stack is configured, port numbers for network switches with a lower **stack ID** are prioritized regardless of the port number. For example, port 1.10 is prioritized over port 2.1.
LACP port priority values within the range **1 to 65535** can be specified using the **lacp port-priority** command, where the lower the setting value, the higher the priority level. The default LACP port priority setting is **32768 (0x8000)**.

4. LAN/SFP ports in half-duplex communication mode do not support LACP link aggregation.
   - Half-duplex LAN/SFP ports that are associated with an LACP logical interface are never activated.
5. The following describes actions that occur if LAN/SFP ports with different communication speeds are located on the same logical interface.
   To configure link aggregation with a mixture of different communication speeds, enable multi-speed link aggregation.
   - Actions if multi-speed link aggregation is enabled (**lacp multi-speed enable**)
     - Activate all associated ports (up to a maximum 8 ports), regardless of communication speed.
     - Load balancing treats all associated ports as equivalent.
       - That increases the risk of a communication overflow occurring at a slow associated port.
       - If there are more than the maximum 8 LAN/SFP ports, higher priority values are assigned to faster associated ports.
     - If the other device cannot accept a different communication speed, then both interacting devices mutually exchange lists of associated ports and activate associated port that can be used by both devices.
       Consequently, the process is limited by the device that cannot accept different communication speeds.
   - Actions if multi-speed link aggregation is disabled (**lacp multi-speed disable**)
     - Only associated ports with a communication speed the same as the port first linked up are activated.
       - Other ports with a different communication speed remain in standby mode.
       - If auto negotiation is enabled, only associated ports with a communication speed that is the same as the negotiation result of the first negotiation will be activated.
     - If links go down for all the ports first linked up, then the link will go down for the LACP logical interface as well.
6. The **show etherchannel** command can be used to check the LACP logical interface status.
   - The **show etherchannel status detail** command can be used to check the activation status of associated ports.
7. LACP link aggregation is used even if a stack is configured. However, the following restriction applies.
   - A total of **126** logical interfaces can be defined for both static and LACP.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

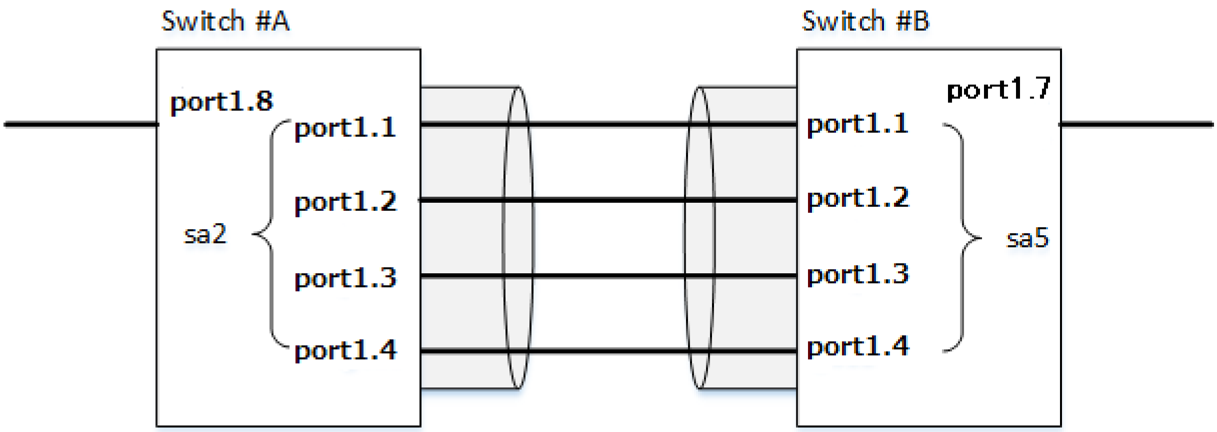
Operations	Operating commands
Set the static logical interface	static-channel-group

Operations	Operating commands
Show the static logical interface status	show static-channel-group
Set the LACP logical interface	channel-group
Set LACP system priority	lacp system-priority
Show LACP system priority	show lacp sys-id
Set LACP multi-speed link aggregation	lacp multi-speed
Set LACP timeout	lacp timeout
Clear LACP packet counter	clear lacp
Show LACP packet counter	show lacp counters
Show the status of the LACP logical interface	show etherchannel
Set load balance function rules	port-channel load-balance

Examples of Command Execution

Set the static logical interface

In this example, we will set link aggregation to use four LAN ports, in order to communicate between network switches.



- Static link aggregation is set to static.
  The logical interface numbers are as follows: Switch A: #2, switch B: #5.
- The LAN ports associated with the logical interface are all access ports, and are associated with the VLAN #1000.

1. Define [switch A] VLAN #1000, and associate it with LAN ports (#1, #2, #3, #4, #8).
   Together with this, associate LAN ports (#1, #2, #3, #4) with logical interface #2.

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 1000 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface port1.8 ②
Yamaha(config-if)#switchport access vlan 1000 ③
Yamaha(config-if)#interface port1.1 ④
Yamaha(config-if)#switchport access vlan 1000 ⑤
Yamaha(config-if)#static-channel-group 2 ⑥
Yamaha(config-if)#interface port1.2
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2
Yamaha(config-if)#interface port1.3
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2
Yamaha(config-if)#interface port1.4
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2
```

① Define VLAN #1000

② Set LAN port #8

③ Set the port as access port and associate it with VLAN #1000

④ Set LAN port #1

⑤ Set the port as access port and associate it with VLAN #1000

⑥ Associate it with logical interface #2

2. Confirm the setting status of [switch A] logical interface #2.

```
Yamaha#show static-channel-group
% Static Aggregator: sa2
% Member:
   port1.1
   port1.2
   port1.3
   port1.4
```

3. Define [switch B] VLAN #1000, and associate it with LAN ports (#1, #2, #3, #4, #7).
Together with this, associate LAN ports (#1, #2, #3, #4) with logical interface #5.

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 1000
Yamaha(config-vlan)#exit
Yamaha(config)#interface port1.7
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#interface port1.1
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.2
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.3
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.4
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
```

4. Confirm the setting status of [switch B] logical interface #5.

```
Yamaha#show static-channel-group
```

```
% Static Aggregator: sa5
% Member:
   port1.1
   port1.2
   port1.3
   port1.4
```

5. Enable [switch A] logical interface.

```
Yamaha(config)#interface sa2 ①
Yamaha(config-if)#no shutdown ②
```

① Set logical interface #2

② Enable the logical interface

6. Enable [switch B] logical interface.

```
Yamaha(config)#interface sa5 ①
Yamaha(config-if)#no shutdown ②
```

① Set logical interface #5

② Enable the logical interface

7. Confirm the setting status of [switch A] logical interface.

```
Yamaha#show interface sa2
Interface sa2
  Link is UP ①
  Hardware is AGGREGATE
  ifIndex 4502, MRU 1522
  Vlan info :
    Switchport mode        : access
    Ingress filter         : enable
    Acceptable frame types : all
    Default Vlan           : 1000
    Configured Vlans       : 1000
  Interface counter:
    input  packets          : 1020
           bytes            : 102432
           multicast packets: 1020
    output packets          : 15
           bytes            : 1845
           multicast packets: 15
           broadcast packets: 0
```

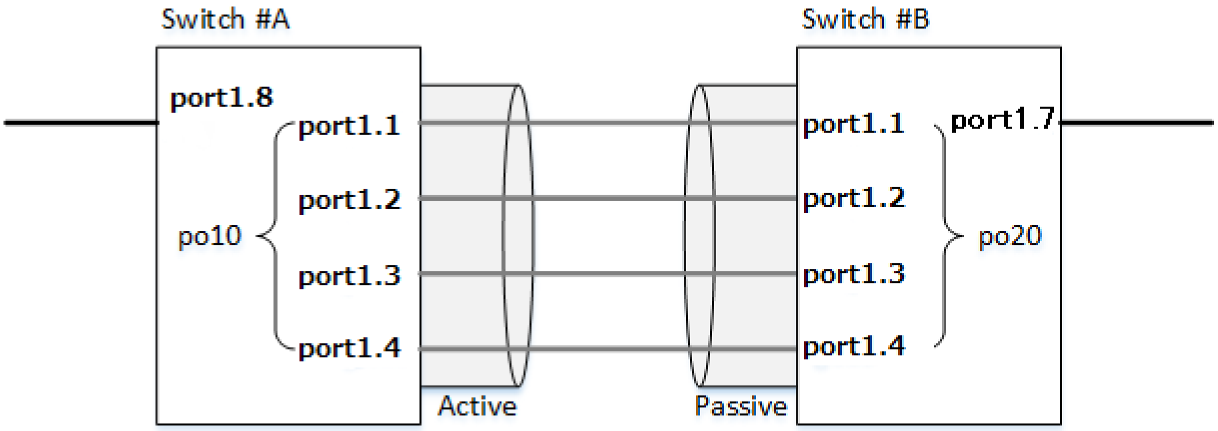
① Enabled

8. Confirm the setting status of [switch B] logical interface.

```
Yamaha#show interface sa5
Interface sa5
  Link is UP
  Hardware is AGGREGATE
  ifIndex 4505, MRU 1522
  Vlan info :
    Switchport mode        : access
    Ingress filter         : enable
    Acceptable frame types : all
    Default Vlan           : 1000
    Configured Vlans       : 1000
  Interface counter:
    input  packets          : 24
           bytes            : 2952
           multicast packets: 24
    output packets          : 2109
           bytes            : 211698
           multicast packets: 2109
           broadcast packets: 0
```

Setting the LACP logical interface

In this example, we will set link aggregation to use four LAN ports, in order to communicate between network switches.



- Use **LACP** for link aggregation.
  The logical interface numbers are as follows: Switch A: #10, switch B: #20.
  Set the switch A logical interface to **active status**, and the switch B logical interface to **passive status**.
- The LAN ports associated with the logical interface are all access ports, and are associated with the VLAN #1000.
- For load balance, set the destination/source IP address.

  1. Define [switch A] VLAN #1000, and associate it with LAN ports (#1, #2, #3, #4, #8).
     Together with this, associate LAN ports (#1, #2, #3, #4) in **active status** with the **logical interface #10**.
     The logical interface at this point in time will be in **shutdown** mode.

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 1000 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface port1.8
Yamaha(config-if)#switchport access vlan 1000 ②
Yamaha(config-if)#interface port1.1
Yamaha(config-if)#switchport access vlan 1000 ③
Yamaha(config-if)#channel-group 10 mode active ④
Yamaha(config-if)#interface port1.2
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 10 mode active
Yamaha(config-if)#interface port1.3
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 10 mode active
Yamaha(config-if)#interface port1.4
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 10 mode active
```

① Define VLAN #1000

② Set the port as access port and associate it with VLAN #1000

③ Set the port as access port and associate it with VLAN #1000

④ Associate the port with logical interface #10 in active state

2. Confirm the setting status of [switch A] logical interface #10.

```
Yamaha#show etherchannel
% Lacp Aggregator: po10
% Member:
   port1.1
   port1.2
   port1.3
   port1.4
Yamaha#show lacp sys-id ①
% System 8000,00-a0-de-ae-b9-1f
Yamaha#show interface po10
Interface po10
  Link is DOWN ②
  Hardware is AGGREGATE
  ifIndex 4610, MRU 1522
  Vlan info :
    Switchport mode        : access
    Ingress filter         : enable
    Acceptable frame types : all
    Default Vlan           : 1000
    Configured Vlans       : 1000
  Interface counter:
    input  packets          : 0
           bytes            : 0
           multicast packets: 0
    output packets          : 0
           bytes            : 0
           multicast packets: 0
           broadcast packets: 0
```

① Check that the LACP system ID is set to the default value (0x8000).

② Link is in down

3. Define [switch B] VLAN #1000, and associate it with LAN ports (#1, #2, #3, #4, #7).
Together with this, associate LAN ports (#1, #2, #3, #4) in **passive status** with the **logical interface #20**.

The logical interface at this point in time will be in **shutdown** mode.

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 1000 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface port1.7
Yamaha(config-if)#switchport access vlan 1000 ②
Yamaha(config-if)#interface port1.1
Yamaha(config-if)#switchport access vlan 1000 ③
Yamaha(config-if)#channel-group 20 mode passive ④
Yamaha(config-if)#interface port1.2
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 20 mode passive
Yamaha(config-if)#interface port1.3
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 20 mode passive
Yamaha(config-if)#interface port1.4
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 20 mode passive
```

① Define VLAN #1000

② Set the port as access port and associate it with VLAN #1000

③ Set the port as access port and associate it with VLAN #1000

④ Associate the port with logical interface #20 in passive state

4. Confirm the setting status of [switch B] logical interface #20.

```
Yamaha#show etherchannel
% Lacp Aggregator: po20
% Member:
   port1.1
   port1.2
   port1.3
   port1.4
Yamaha#show lacp sys-id ①
% System 8000,00-a0-de-ae-b8-7e
Yamaha#show interface po20
Interface po20
  Link is DOWN ②
  Hardware is AGGREGATE
  ifIndex 4620, MRU 1522
  Vlan info :
    Switchport mode        : access
    Ingress filter         : enable
    Acceptable frame types : all
    Default Vlan           : 1000
    Configured Vlans       : 1000
  Interface counter:
    input  packets          : 0
           bytes            : 0
           multicast packets: 0
    output packets          : 0
           bytes            : 0
           multicast packets: 0
```

```
              broadcast packets: 0
```

① Check that the LACP system ID is set to the default value (0x8000).

② Link down state

5. Set the load balance of [switch A] to the destination/source IP address, and enable the interface.

```
Yamaha(config)#port-channel load-balance src-dst-ip ①
Yamaha(config)#interface po10 ②
Yamaha(config-if)#no shutdown ③
```

① Set the load balance

② Set logical interface #10

③ Enable the logical interface

6. Set theload balance of [switch B] to the destination/source IP address, and enable the interface.

```
Yamaha(config)#port-channel load-balance src-dst-ip ①
Yamaha(config)#interface po20 ②
Yamaha(config-if)#no shutdown ③
```

① Set the load balance

② Set logical interface #20

③ Enable the logical interface

7. Confirm the setting status of [switch A] logical interface.
Link up and confirm whether frames are being sent and received.

```
Yamaha#show interface po10
Interface po10
  Link is UP
  Hardware is AGGREGATE
  ifIndex 4610, MRU 1522
  Vlan info :
    Switchport mode        : access
    Ingress filter         : enable
    Acceptable frame types : all
    Default Vlan           : 1000
    Configured Vlans       : 1000
  Interface counter:
    input  packets          : 560
           bytes            : 58239
           multicast packets: 560
    output packets          : 98
           bytes            : 12474
           multicast packets: 98
           broadcast packets: 0
Yamaha#
Yamaha#show lacp-counter
% Traffic statistics
Port       LACPDUs         Marker          Pckt err
        Sent     Recv     Sent     Recv     Sent     Recv
```

```
% Aggregator po10 , ID 4610
port1.1      50      47      0       0       0       0
port1.2      49      46      0       0       0       0
port1.3      49      46      0       0       0       0
port1.4      49      46      0       0       0       0
```

8. Confirm the setting status of [switch B] logical interface.
   Link up and confirm whether frames are being sent and received.

```
Yamaha#show interface po20
Interface po20
  Link is UP
  Hardware is AGGREGATE
  ifIndex 4620, MRU 1522
  Vlan info :
    Switchport mode        : access
    Ingress filter         : enable
    Acceptable frame types : all
    Default Vlan           : 1000
    Configured Vlans       : 1000
  Interface counter:
    input  packets          : 78
           bytes            : 9914
           multicast packets: 78
    output packets          : 438
           bytes            : 45604
           multicast packets: 438
           broadcast packets: 0
Yamaha#
Yamaha#show lacp-counter
% Traffic statistics
Port       LACPDUs         Marker         Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
% Aggregator po20 , ID 4620
port1.1      55      57      0       0       0       0
port1.2      54      56      0       0       0       0
port1.3      54      56      0       0       0       0
port1.4      54      56      0       0       0       0
```

Points of Caution

- A host port that is associated with a private VLAN cannot be aggregated as a link aggregation logical interface.
- If access list settings exist for the received frame of a LAN/SFP port, the ports cannot be aggregated as a link aggregation logical interface.

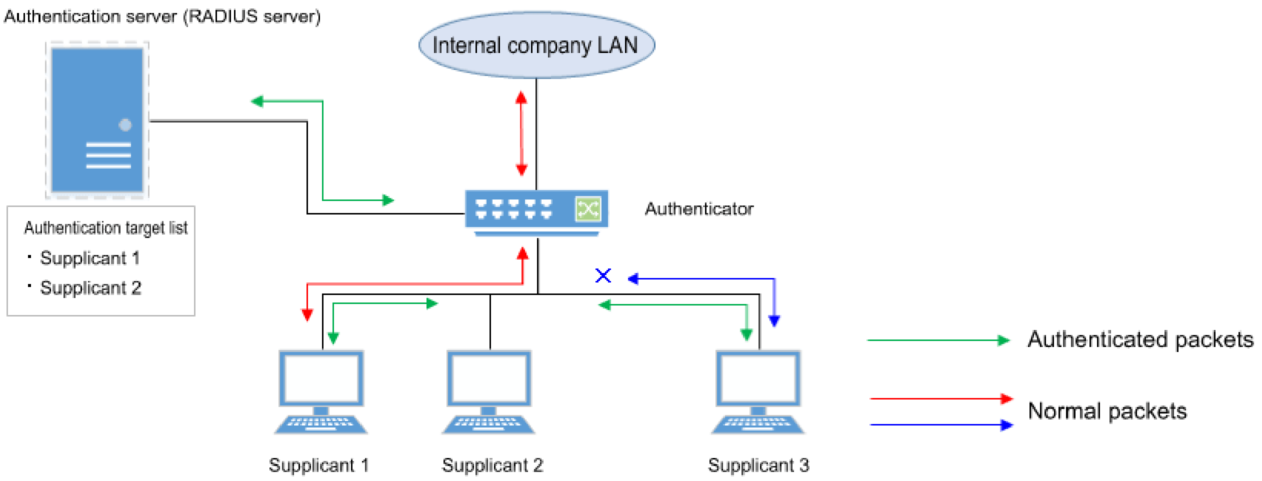
Related Documentation

- LAN/SFP Port Control: Basic Interface Settings

Port Authentication Function

Function Overview

Port authentication is a function that authenticates devices or users.
This authenticates a device connected to the LAN/SFP port, and permits LAN access only for devices that succeeded in authenticating.
Devices that are not yet authenticated or that failed to authenticate can be denied access to the LAN, or permitted to access only a specific VLAN.



Definition of Terms Used

IEEE 802.1X

The authentication standard used when connecting to the LAN.

Authenticator

A device or software that authenticates a supplicant connected to a LAN/SFP port.
It mediates between the supplicant and the authentication server, controlling access to the LAN according to the success or failure of authentication.

Supplicant

A device or software that connects to an authenticator and receives authentication.

Authentication server

A device or software that authenticates a supplicant that is connected via the authenticator.
This manages authentication information such as user names, passwords, MAC addresses, and associated VLANs.

EAP (Extended authentication protocol)

This is an authentication protocol that extends PPP, allowing various authentication methods to be used.
This is defined in RFC3748.

EAP over LAN (EAPOL)

This is a protocol for conveying EAP packets between the supplicant and the authenticator.

EAP over Radius

This is a protocol for conveying EAP packets between the authenticator and the authentication server (RADIUS server).

EAP-MD5 (Message digest algorithm 5)

Client authentication using user name and password.
This uses an MD5 hash value to authenticate.

EAP-TLS (Transport Layer Security)

This uses the digital certificates of the server and the client to authenticate.
With the transport layer encrypted, the digital certificates are exchanged and authenticated.
This is defined in RFC2716 and RFC5216.

EAP-TTLS (Tunneled TLS)

This is an extended version of EAP-TLS.
This uses the digital certificate of the server to establish a TLS communication route, and within this encrypted communication route uses a password to authenticate the client.
This is defined in RFC5281.

EAP-PEAP (Protected EAP)

The principle of operation is equivalent to EAP-TTLS (the only difference is the protocol inside the encrypted tunnel).
This uses the digital certificate of the server to establish a TLS communication route, and within this encrypted communication route uses a password to authenticate the client.

Function Details

The operating specifications for port authentication are shown below.
As port authentication functions, this product supports IEEE 802.1X authentication, MAC authentication, and Web authentication.
The following table shows the distinctive features of each authentication method.

	MAC authentication	IEEE 802.1X authentication	Web authentication
Authenticated element	MAC address	User name and password (EAP-MD5, EAP-TTLS, EAP-PEAP)	User name and password
Authenticated object (supplicant)	Device	Device or user	Device or user
Functions needed by supplicant	None	IEEE 802.1X authentication function	Web browser
Operation when authenticating	None	User name and password entry (EAP-MD5, EAP-TTLS, EAP-PEAP)	User name and password entry

This product assumes a RADIUS server as the authentication server.

Note that the port authentication function of this product has the following limitations.

- The number of supplicants that can be authenticated is one for each port in single host mode or multi host mode; for multi supplicant mode, the maximum is **512** for the entire system.

- It cannot be used on a private VLAN port.
- It cannot be used on a voice VLAN port.
- If port authentication is enabled, a spanning tree topology change will occur according to the authentication result.
  If you want to avoid this, specify “spanning-tree edgeport” for the authentication port to which the supplicant will be connected.
- Web authentication can be used only in the multi supplicant mode.
- Web authentication cannot be used together with a guest VLAN.
- When using the stack function, a file saved on the main switch is referenced as the Web Authentication screen customization file.
- When using the stack function, if a member switch is added, the authentication information of the supplicant connected to the logical interface is cleared.
- When using the stack function, if the main switch is demoted to a member switch status, authentication information is cleared from connected supplicants.
- Trunk ports can only be used in the multi supplicant mode.
- Trunk ports cannot use dynamic or guest VLANs.
- If you also use the L2MS function on a trunk port, you must set the native VLAN to be provided.
- If the following supplicant VLAN is changed by a dynamic VLAN, then the authentication function may not work properly.
    - DHCP server
    - L2MS compatible device

IEEE 802.1X authentication

IEEE 802.1X authentication uses EAP to authenticate in units of devices or users.
The supplicant receiving authentication must support IEEE 802.1X authentication.

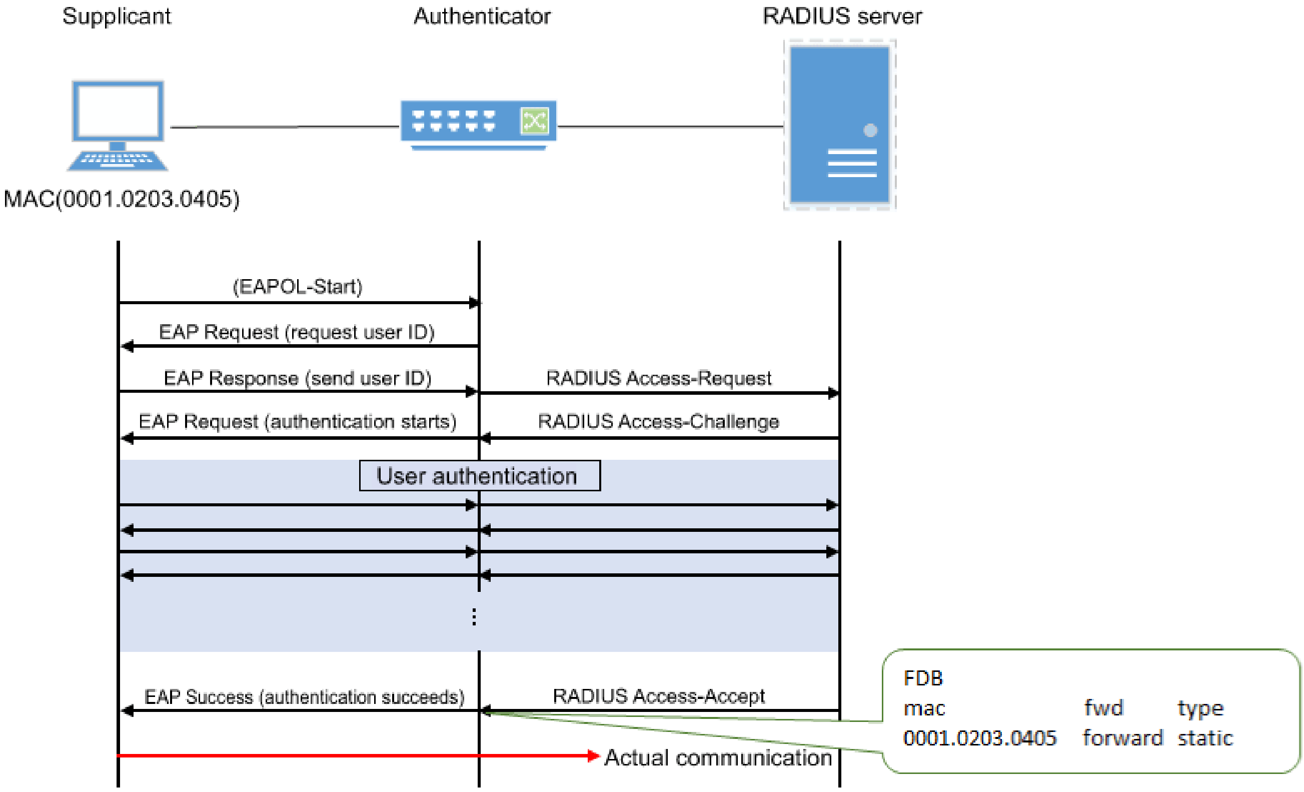
This product operates as an authenticator that communicates with the supplicant via EAP over LAN and communicates with the RADIUS server via EAP over RADIUS.
The authentication process itself occurs directly between the supplicant and the RADIUS server.

As authentication methods, this product supports EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP.
The features of each authentication method are shown in the following table.

	Client authentication method	Server authentication method	Ease of implementation	Degree of safety
EAP-MD5	User name and password entry	No authentication	Easy	Low
EAP-TLS	Client certificate	Server certificate	Complex	High
EAP-TTLS	User name and password entry	Server certificate	Medium	Medium
EAP-PEAP	User name and password entry	Server certificate	Medium	Medium

Make settings for the supplicant and the RADIUS server as appropriate for the authentication method you use.

The basic procedure for IEEE 802.1X authentication is shown in the following diagram.



The supplicant is connected to the LAN, and transmits a communication start message (EAPOL-Start) message to start authentication.

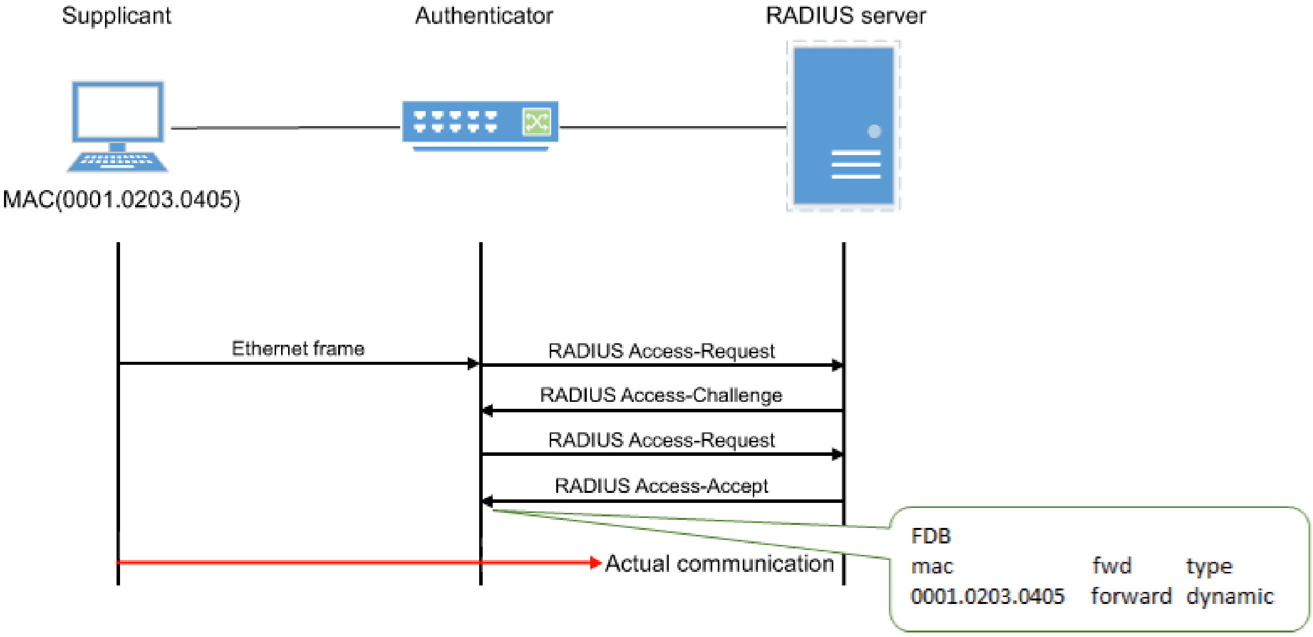
When authentication succeeds, authentication success (Success) notification is sent to the supplicant, and the supplicant's MAC address is registered in the FDB, permitting the supplicant to access the network.

If authentication fails, an authentication failure (Failure) notification is sent to the supplicant, and network access is denied for the supplicant.
(Even without authentication, it is possible to permit access to a specific VLAN if a guest VLAN has been specified.)

MAC authentication

MAC authentication uses the MAC address of a device to authenticate an individual device.
Since the supplicant does not need any special function to be authenticated, authentication is possible even for devices that do not support IEEE 802.1X.

The basic procedure for MAC authentication is shown in the following diagram.



When this product receives any Ethernet frame from the supplicant, it queries the RADIUS server with the supplicant's MAC address as the user name and password.
EAP-MD5 is used as the authentication mode between this product and the RADIUS server.

When authentication succeeds, the supplicant's MAC address is registered in the FDB, permitting the supplicant to access the network.
However, it can be registered as a static entry by specifying MAC authenticated static registration (using the **auth-mac static** command).

If authentication fails, the supplicant is denied network access.
(Even without authentication, it is possible to permit access to a specific VLAN if a guest VLAN has been specified.)

The supplicant's MAC address must be registered as the user name and password in the RADIUS server, in one of the following formats.

- XX-XX-XX-XX-XX-XX (hyphen delimited)
- XX:XX:XX:XX:XX:XX (colon delimited)
- XXXXXXXXXXXX (not delimited)

This product lets you use the **auth-mac auth-user** command to change the format of the MAC address query that is made to the RADIUS server.
Specify the appropriate command according to the format of the MAC addresses that are registered in the RADIUS server.

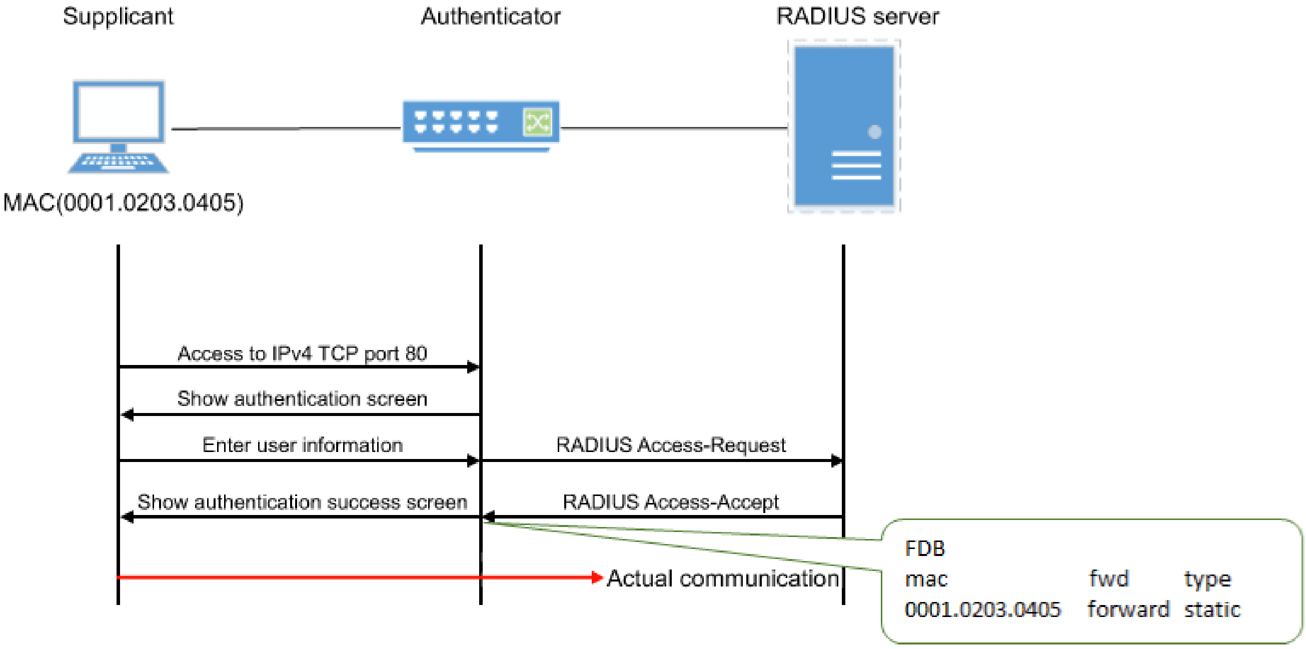
Web authentication

Web authentication is a function that authenticates a user when a user name and password are entered from the supplicant's web browser.

HTTP is supported as the communication method between the web browser and the network switch.
Because web authentication performs authentication by communicating via HTTP, it is necessary for IP communication between this product and the supplicant to be possible even before authentication.
Either the DHCP server must assign an IP address to the supplicant, or the supplicant must specify an IP address statically.

Web authentication operates only in the multi supplicant mode.
Also, this cannot be used together with a guest VLAN.

The basic procedure for web authentication is shown in the following diagram.



This product queries the RADIUS server using the user name and password that were entered in the supplicant's web browser.
EAP-MD5 is used as the authentication mode between this product and the RADIUS server.

When authentication succeeds, the supplicant's MAC address is registered in the FDB, permitting the supplicant to access the network.

If authentication fails, the supplicant is denied network access.

Operations on the supplicant

When the supplicant's web browser accesses IPv4 TCP port 80, the following authentication screen appears.

+
image::web-auth-default.png[image,width=700, role=th]

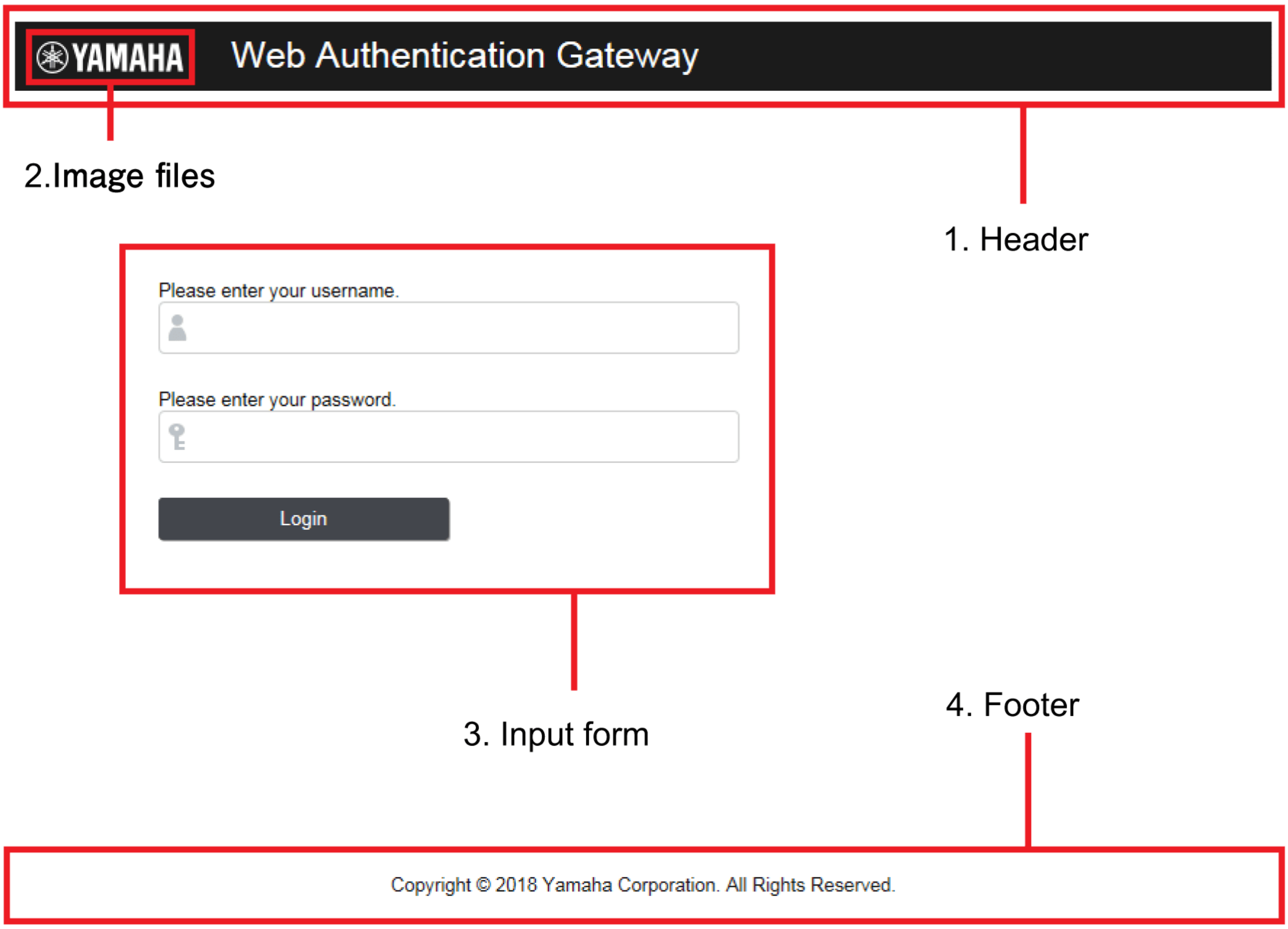
To be authenticated, enter a user name and password, and click the [Login] button.

The supplicant's MAC address is registered in the FDB, permitting the supplicant to access the network.
If authentication fails three times in succession, authentication is temporarily restricted.

Customizing the authentication screen

The displayed content on the Web authentication screen (the edited HTML, CSS and image files) can be copied to this product, and the following parts can be customized.

Note that we cannot provide support for how to code in HTML/CSS or what formatting to use, or for any troubles that may occur due to modifications to the code.



YAMAHA Web Authentication Gateway

Please enter your username.

Please enter your password.

Login

Copyright © 2018 Yamaha Corporation. All Rights Reserved.

1. Header
   The header section includes the “header.html” and “style.css” files. Edit these files and copy them to this product in order to customize them.
2. Image file
   Copy the image provided to this product in order to modify it.
3. Input form
   The display style used for the input form is defined in the “style.css” file. Although the text cannot be changed, you can edit the “style.css” file and copy it to this product in order to change the input form’s design.
4. Footer
   The footer section includes the “footer.html” and “style.css” files. Edit these files and copy them to this product in order to customize them.

The following explains how to modify the Web authentication screen.

Preparing the authentication screen customization files

The following files are used to customize the Web authentication screen.

- header.html
- footer.html
- logo.png

- style.css

Use the Web browser to access the “header.html”, “footer.html” and “style.css” files from the network switch.
For example if the IP address of the network switch is 192.168.100.240, you can use the following URL to access the file from a PC connected to a port on which Web authentication is enabled, and then use the browser’s “Save as” command to save the file on the PC.

- http://192.168.100.240/web-auth/header.html
- http://192.168.100.240/web-auth/footer.html
- http://192.168.100.240/web-auth/style.css

Save files with an “.html” or “.css” extension and with UTF-8 character encoding specified.

For the image file logo.png, prepare a desired image file on the PC, and save it with the file name logo.png.
The maximum file size is 1 MB.

Editing the authentication screen customization files

Edit the above-mentioned HTML and CSS files as appropriate on your PC.
You are free to edit each file in accordance with HTML and CSS specifications, but please note the following points.

- The only image file that can be referenced from the “header.html” and “footer.html” files is “logo.png”.
- The extension of the HTML/CSS file must be “.html” or “.css” and the character encoding must be consistent with UTF-8.

Placing the authentication screen customization files

When you have prepared the files, place them in /model name/startup-config/web-auth/ on the SD card.
After placing the files, use the **copy auth-web custom-file** command or the **copy startup-config** command to copy the authentication screen customization files to the network switch.

If the following files exist in the folder hierarchy in which the currently-running CONFIG is saved, they are used to generate the Web authentication screen.

You can determine the currently-running CONFIG number by using the **show environment** command.
Even if the network switch started up using the CONFIG on the SD card, you can customize the Web authentication screen by placing these files in /model name/startup-config/web-auth/ on the SD card.

- header.html
  This is used as the header section referenced from the authentication screen. If this file does not exist, the original “header.html” is used.
- footer.html
  This is used as the footer section referenced from the authentication screen. If this file does not exist, the original “footer.html” is used.
- logo.png
  This is used as the logo in the upper left of the authentication screen. If this file does not exist, the original Yamaha logo is shown.
- style.css
  This is used as the “style.css” referenced from the authentication screen. If this file does not exist, the original style.css is used.

When you have finished placing the edited files, check the display by using your browser to access the Web authentication screen.
If you need to make additional changes, edit the files on your PC, and transfer them again.

Canceling customization

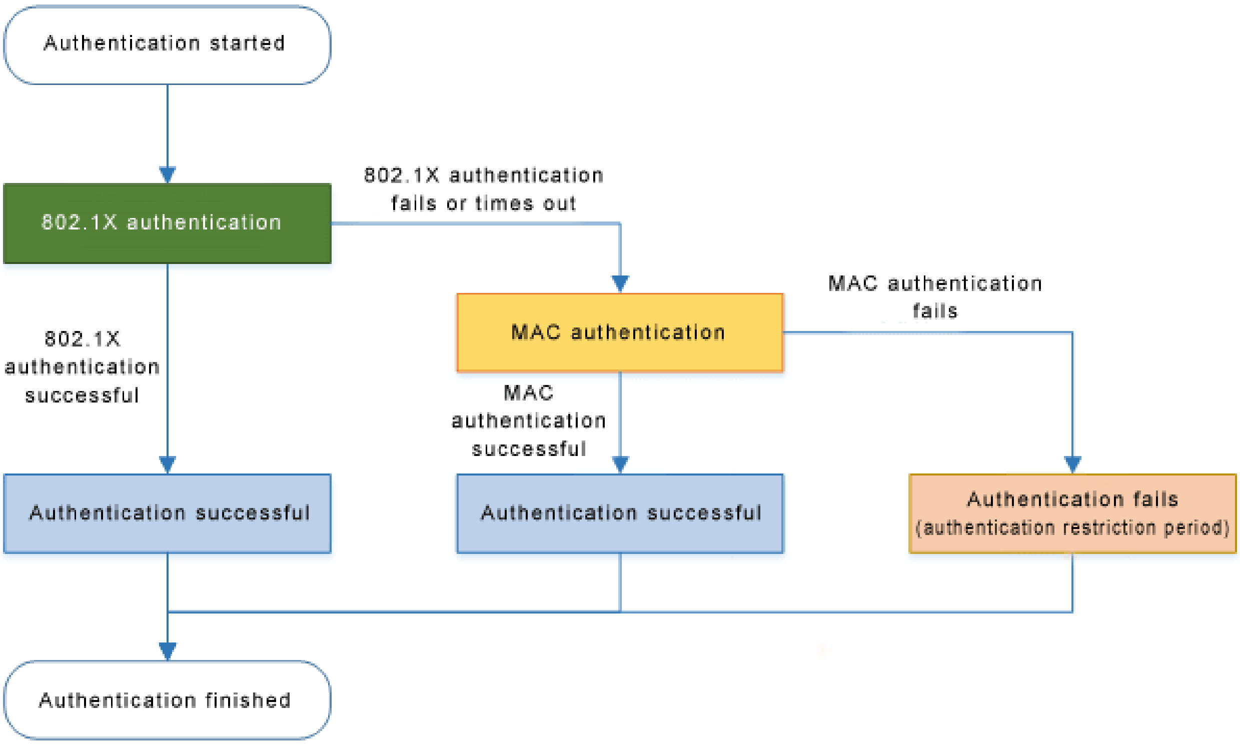
If you decide to cancel customization of the authentication screen, delete the customization files from the folder in which the currently-running CONFIG is saved. You will revert to the original authentication screen.
To delete the files, you can use the **erase auth-web custom-file** command or the **erase startup-config** command.
However, since the **erase startup-config** command also deletes files such as config.txt, you should first copy files such as config.txt to an SD card etc. as a backup.

Using multiple authentication functions

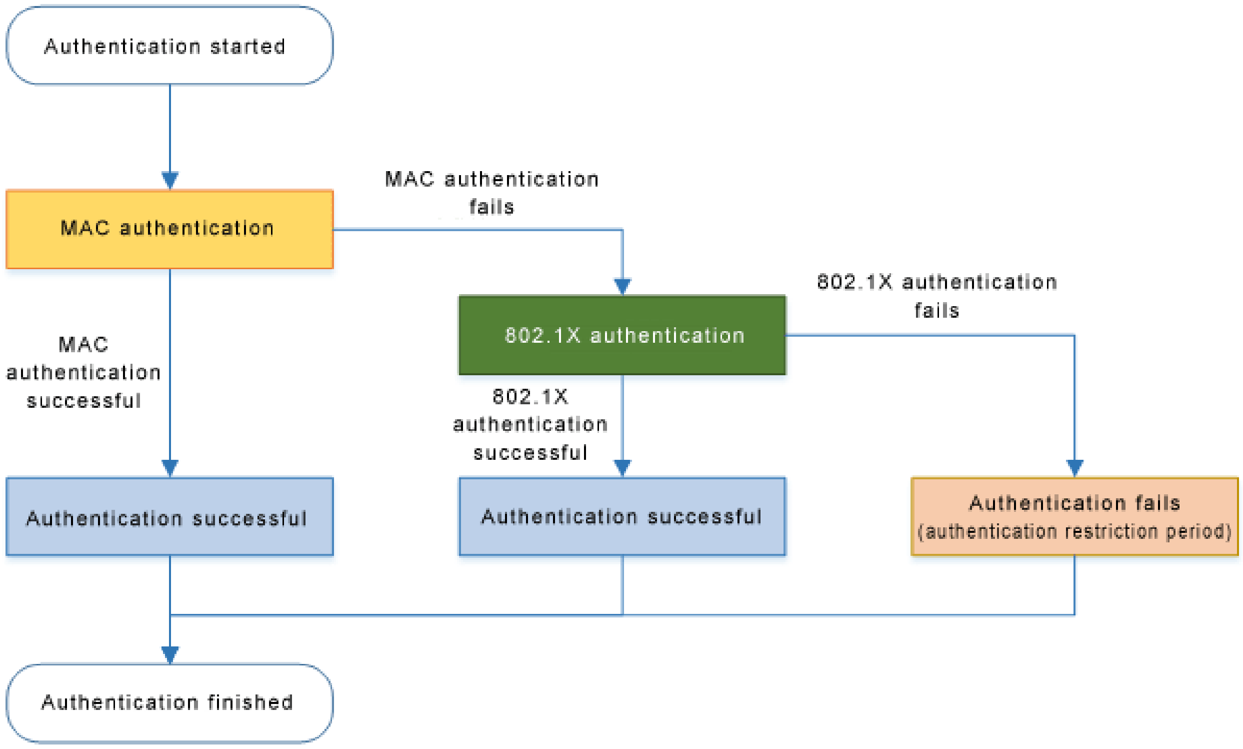
This product allows using a combination of IEEE 802.1X authentication, MAC authentication, and/or Web authentication at the same port.
When network switches are used in combination, each switch is successively authenticated in the authentication order specified using the auth order command. With default settings, IEEE 802.1X authentication is prioritized.
For web authentication, network switches are authenticated by entering an ID and password in the Web Authentication screen, where the authentication method is changed to web authentication.

If multiple authentication methods are used simultaneously, basic operations are as follows.

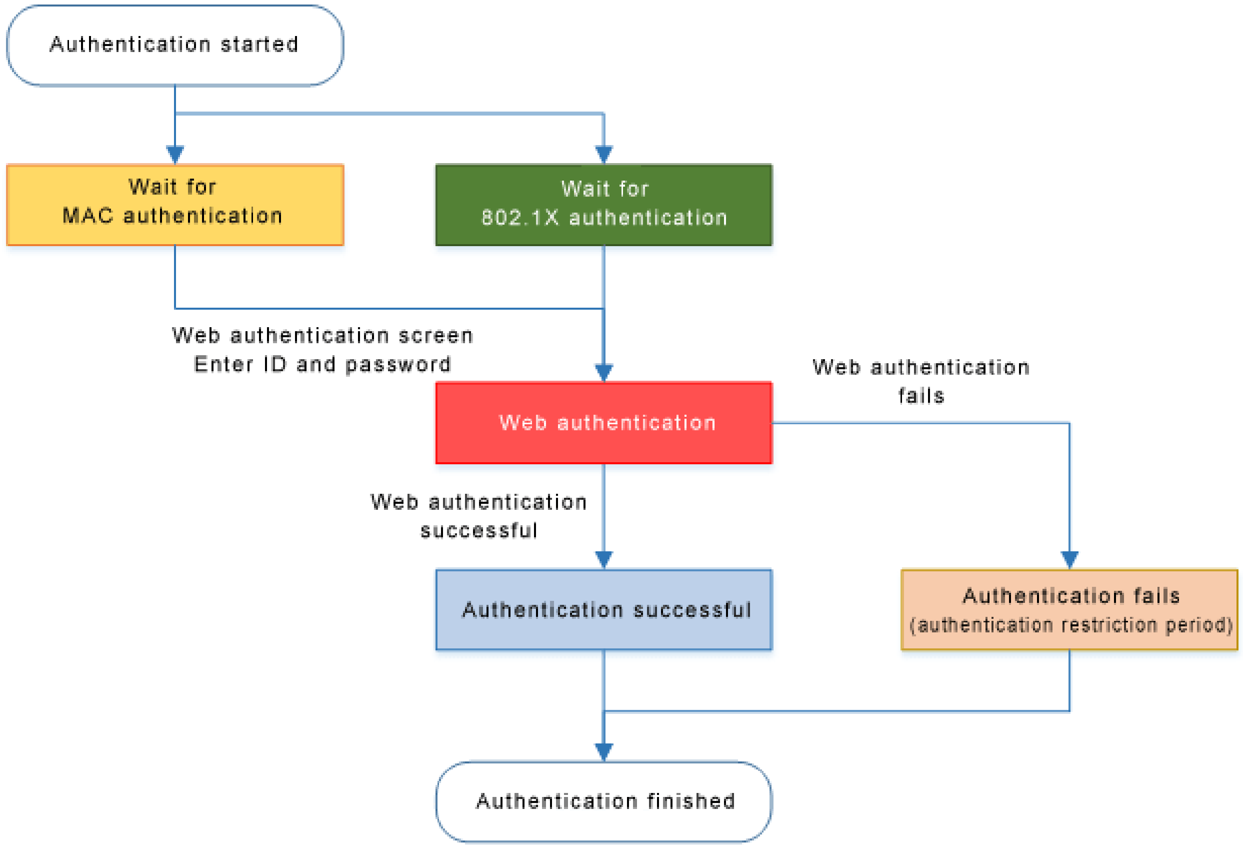
- If both IEEE 802.1X authentication and MAC authentication are used, with IEEE 802.1X authentication prioritized


Authentication started
802.1X authentication
802.1X authentication fails or times out
802.1X authentication successful
MAC authentication
MAC authentication fails
MAC authentication successful
Authentication successful
Authentication successful
Authentication fails (authentication restriction period)
Authentication finished

- If both IEEE 802.1X authentication and MAC authentication are used, with MAC authentication prioritized


Authentication started
MAC authentication
MAC authentication fails
802.1X authentication
802.1X authentication fails
MAC authentication successful
802.1X authentication successful
Authentication successful
Authentication successful
Authentication fails (authentication restriction period)
Authentication finished

- If both web authentication and IEEE 802.1X/MAC authentication are used


Authentication started
Wait for MAC authentication
Wait for 802.1X authentication
Web authentication screen Enter ID and password
Web authentication
Web authentication fails
Web authentication successful
Authentication successful
Authentication fails (authentication restriction period)
Authentication finished

note

- If authentication succeeds with any one of the methods, authentication has succeeded.
- If the reauthentication setting is enabled, then reauthentication is performed using the method with which authentication succeeded.
- If multiple authentication methods are used, forwarding control settings received via an unauthenticated port will be discarded.

- If both IEEE 802.1X authentication and MAC authentication are being used and an EAPOL start signal is received from an unauthenticated supplicant, authentication will switch to IEEE 802.1X authentication even if MAC authentication is already in progress.
- If both IEEE 802.1X authentication and MAC authentication are being used, even if the first authentication method fails, authentication will switch to the next authentication method without entering the restriction period.
- If both IEEE 802.1X authentication and MAC authentication are being used and any Ethernet frame is received from a supplicant, the product transmits an EAP request.
- If Web authentication is also being used, unauthenticated supplicants are registered in FDB as static/discard.

Host mode

This product lets you select the host mode for the port authentication function.
Host mode indicates how an applicable supplicant's communication will be permitted on the authentication port.

This product lets you choose from the following host modes.

- Single host mode

  This mode permits communication for only one supplicant for each LAN/SFP port.
  Communication is permitted only for the first supplicant that successfully authenticates.

- Multi host mode

  This mode permits communication for multiple supplicants for each LAN/SFP port.
  When a supplicant successfully authenticates and communication is permitted, another supplicant that is connected to the same LAN/SFP port and that successfully authenticates is also permitted to communicate on the same VLAN.

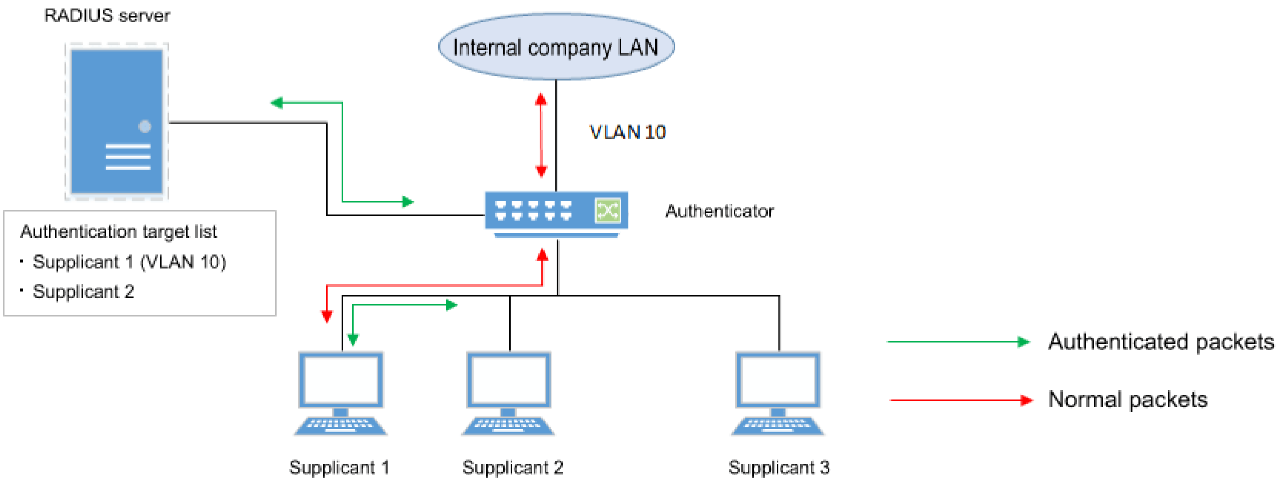
- Multi supplicant mode

  This mode permits communication for multiple supplicants for each LAN/SFP port.

  Each supplicant is distinguished by its MAC address, permitting communication in units of supplicants.
  When using dynamic VLAN functions, you can specify the VLAN for each supplicant.

Dynamic VLAN

This product supports dynamic VLANs using IEEE 802.1X, MAC, or Web authentication.
Dynamic VLAN is a function that changes the authentication port's associated VLAN according to the VLAN attribute values in authentication information in notifications received from the RADIUS server.



As shown in the illustration above, if a port's associated VLAN is 1, and the received authentication data has a

VLAN attribute of 10, then following successful authentication, the authentication port's associated VLAN is 10, and communication on VLAN 10 is permitted.

For the RADIUS server, make settings so that the authentication information sent from the server includes the following attribute values.

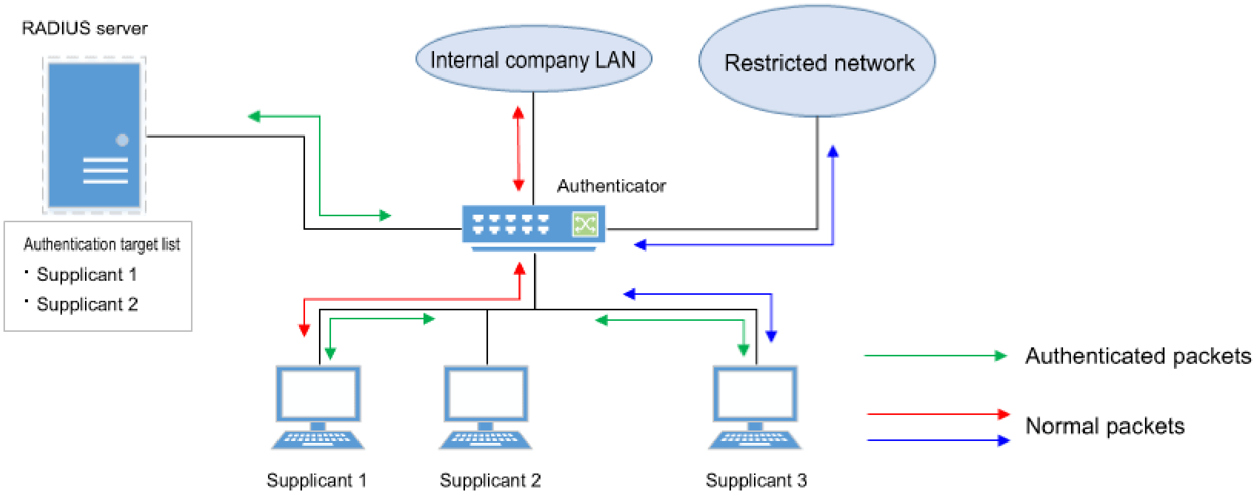
- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = IEEE-802 (6)
- Tunnel-Private-Group-ID = VLAN ID

If a dynamic VLAN is used, the following actions will occur in respective host modes.

- Single host mode
  The authentication port's associated VLAN is changed according to the VLAN attribute value of the supplicant that successfully authenticates.
- Multi host mode
  The authentication port's associated VLAN is changed according to the VLAN attribute value of the supplicant that successfully authenticates.
  Other supplicants that are connected to the same port are also permitted to communicate on the same VLAN.
- Multi supplicant mode
  The authentication port's associated VLAN is changed according to the VLAN attribute value of the supplicant that successfully authenticates.
  You can specify the VLAN for each supplicant.

VLAN for unauthenticated or failed-authentication ports

This product's IEEE 802.1X authentication and MAC authentication allow you to specify a guest VLAN so that unauthenticated ports or ports that failed authentication will be assigned to a specific VLAN.
In the multi supplicant mode, you can specify this for each supplicant.



This is useful when you want to partially provide functions on a limited network even to a supplicant that has not succeeded in authenticating, as shown in the illustration above.

EAP pass-through function

You can switch between enable and disable for EAP pass-through and configure whether EAPOL frames are to be forwarded.
The authentication function will be prioritized for interfaces on which the 802.1X authentication function is

enabled, and EAP pass-through will not be applied.

Attribute values sent to the RADIUS server

The NAS-Identifier attribute value can be notified to the RADIUS server.
The character string set with the **auth radius attribute nas-identifier** command is sent to the RADIUS server as the NAS-Identifier attribute value.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

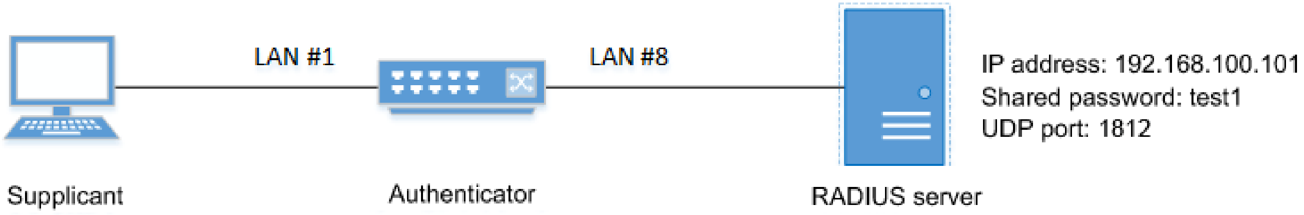
Operations	Operating commands
Set IEEE 802.1X authentication function for the entire system	aaa authentication dot1x
Set MAC authentication function for the entire system	aaa authentication auth-mac
Set Web authentication function for the entire system	aaa authentication auth-web
Set IEEE 802.1X authentication function operating mode	dot1x port-control
Set unauthenticated port forwarding control for IEEE 802.1X authentication	dot1x control-direction
Set number of retransmitted EAPOL packets	dot1x max-auth-req
Set MAC authentication function	auth-mac enable
Set MAC address format setting for MAC authentication	auth-mac auth-user
MAC authenticated static registration setting	auth-mac static
Set Web authentication function	auth-web enable
Set redirect-destination URL following successful Web authentication	auth-web redirect-url
Copy Web authentication screen customization files	copy auth-web custom-file
Delete Web authentication screen customization files	erase auth-web custom-file
Set host mode	auth host-mode
Authentication order setting	auth order
Set reauthentication	auth reauthentication
Set dynamic VLAN	auth dynamic-vlan-creation
Set guest VLAN	auth guest-vlan
Set restriction period following failed authentication	auth timeout quiet-period
Set re-authentication interval	auth timeout reauth-period
Set response wait time for the entire RADIUS server	auth timeout server-timeout
Set response wait time for the supplicant	auth timeout supp-timeout
Set RADIUS server host	radius-server host
Set response wait time for a single RADIUS server	radius-server timeout
Set number of times to resend requests to RADIUS server	radius-server retransmit

Operations	Operating commands
Set shared password for RADIUS server	radius-server key
Set availability time restriction for RADIUS server	radius-server deadtime
Setting the NAS-Identifier attribute to notify the RADIUS server	auth radius attribute nas-identifier
Show port authentication status	show auth status
Show RADIUS server setting status	show radius-server
Show supplicant status	show auth supplicant
Show statistical information	show auth statistics
Clear statistical information	clear auth statistics
Clear authentication status	clear auth state
Set time at which authentication state is cleared (system)	auth clear-state time
Set time at which authentication state is cleared (interface)	auth clear-state time
Set EAP pass through	pass-through eap

Examples of Command Execution

Set IEEE 802.1X authentication

Make settings so that IEEE 802.1X authentication can be used.



- We will use LAN port #1 as the authentication port to which the supplicant is connected.
- We will set the **host mode** to the **multi supplicant mode**.
- We will use VLAN #10 as the **guest LAN**.
- We will use 192.168.100.101 as the IP address of the RADIUS server that is connected.

■ Setting Procedure

1. Define VLAN #10 as the guest VLAN.

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
```

① Define VLAN #10

2. Enable the IEEE 802.1X authentication function for the entire system.

```
Yamaha(config)#aaa authentication dot1x
```

3. Set IEEE 802.1X authentication for LAN port #1.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#dot1x port-control auto ①
Yamaha(config-if)#auth host-mode multi-supplicant ②
Yamaha(config-if)#auth guest-vlan 10 ③
Yamaha(config-if)#exit
```

① Set the IEEE 802.1X authentication operating mode to auto

② Set the host mode to the multi supplicant mode

③ Define VLAN #10 as the guest VLAN

4. Set RADIUS server settings.

```
Yamaha(config)#radius-server host 192.168.100.101 key test1 ①
```

① Set the host to 192.168.100.101 and the shared password to “test1”

5. Check RADIUS server settings.

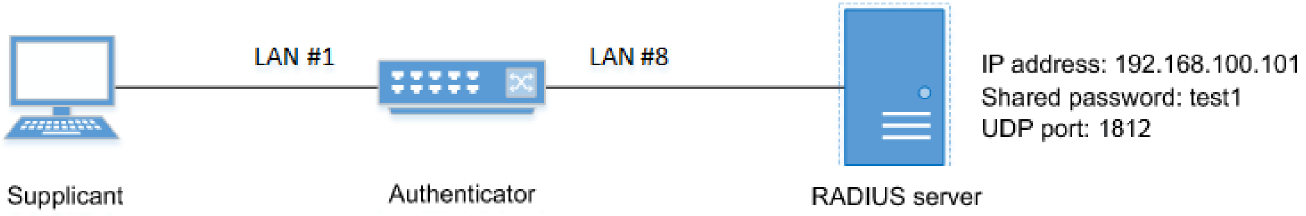
```
Yamaha#show radius-server
Server Host : 192.168.100.101
  Authentication Port : 1812
  Secret Key          : test1
  Timeout             : 5 sec
  Retransmit Count    : 3
  Deadtime            : 0 min
```

6. Check port authentication settings.

```
Yamaha#show auth status
[System information]
  802.1X Port-Based Authentication : Enabled
  MAC-Based Authentication         : Disabled
  WEB-Based Authentication         : Disabled

  Clear-state time : Not configured

  Redirect URL :
    Not configured

  RADIUS server address :
    192.168.100.101 (port:1812)

[Interface information]
  Interface port1.1 (up)
    802.1X Authentication   : Force Authorized (configured:auto)
    MAC Authentication      : Disabled (configured:disable)
    WEB Authentication      : Enabled (configured:disable)
    Host mode                : Multi-supplicant
    Dynamic VLAN creation    : Disabled
    Guest VLAN               : Enabled (VLAN ID:10)
    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
```

Set MAC authentication

Make settings so that MAC authentication can be used.



- We will use LAN port #1 as the authentication port to which the supplicant is connected.
- We will set the **host mode** to the **multi supplicant mode**.
- We will use 192.168.100.101 as the IP address of the RADIUS server that is connected.

■ Setting Procedure

1. Enable the MAC authentication function for the entire system.

```
Yamaha(config)#aaa authentication auth-mac
```

2. Set MAC authentication for LAN port #1.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#auth-mac enable ①
Yamaha(config-if)#auth host-mode multi-supplicant ②
Yamaha(config-if)#exit
```

① Enable MAC authentication

② Set the host mode to the multi supplicant mode

3. Set RADIUS server settings.

```
Yamaha(config)#radius-server host 192.168.100.101 key test1 ①
```

① Set the host to 192.168.100.101 and the shared password to “test1”

4. Check RADIUS server settings.

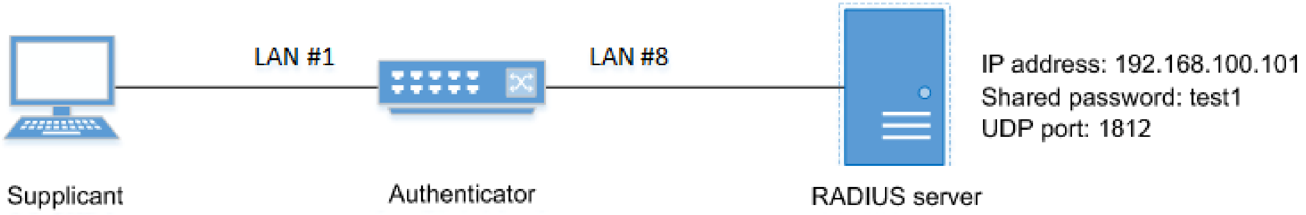
```
Yamaha#show radius-server
Server Host : 192.168.100.101
  Authentication Port : 1812
  Secret Key          : test1
  Timeout             : 5 sec
  Retransmit Count    : 3
  Deadtime            : 0 min
```

5. Check port authentication settings.

```
Yamaha#show auth status
[System information]
  802.1X Port-Based Authentication : Disabled
  MAC-Based Authentication         : Enabled
  WEB-Based Authentication         : Disabled

  Clear-state time : Not configured

  Redirect URL :
    Not configured

  RADIUS server address :
    192.168.100.101 (port:1812)

[Interface information]
  Interface port1.1 (up)
    802.1X Authentication   : Force Authorized (configured:-)
    MAC Authentication      : Enabled (configured:enable)
    WEB Authentication      : Disabled (configured:disable)
    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
    Authentication status   : Unauthorized
```

Set Web authentication

Make settings so that Web authentication can be used.



- We will use LAN port #1 as the authentication port to which the supplicant is connected.
- We will assume that the IP address of the supplicant is set to 192.168.100.10.
- We will use 192.168.100.101 as the IP address of the RADIUS server that is connected.

■ Setting Procedure

1. Assign an IP address to the authenticator for IP communication.

```
Yamaha(config)#interface valn1
Yamaha(config-if)#ip address 192.168.100.240/24
Yamaha(config-if)#exit
```

2. Enable the Web authentication function for the entire system.

```
Yamaha(config)#aaa authentication auth-web
```

3. Set Web authentication for LAN port #1.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#auth host-mode multi-supplicant ①
Yamaha(config-if)#auth-web enable ②
Yamaha(config-if)#exit
```

① Set the host mode to the multi supplicant mode

② Enable Web authentication

4. Set RADIUS server settings.

```
Yamaha(config)#radius-server host 192.168.100.101 key test1 ①
```

① Set the host to 192.168.100.101 and the shared password to “test1”

5. Check RADIUS server settings.

```
Yamaha#show radius-server
Server Host : 192.168.100.101
  Authentication Port : 1812
  Secret Key          : test1
  Timeout             : 5 sec
  Retransmit Count    : 3
  Deadtime            : 0 min
```

6. Check port authentication settings.

```
Yamaha#show auth status
[System information]
  802.1X Port-Based Authentication : Disabled
  MAC-Based Authentication         : Disabled
  WEB-Based Authentication         : Enabled
  Clear-state time : Not configured

  Redirect URL :
    Not configured

  RADIUS server address :
    192.168.100.101 (port:1812)

[Interface information]
  Interface port1.1 (up)
    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
```

Points of Caution

Using dynamic VLAN in the multi supplicant mode will consume internal resources.
These resources are also used by the ACL and QoS functions. There may not be enough resources according to the settings.
Use caution, since communications may not be possible if there are not enough resources, even though authentication might succeed.

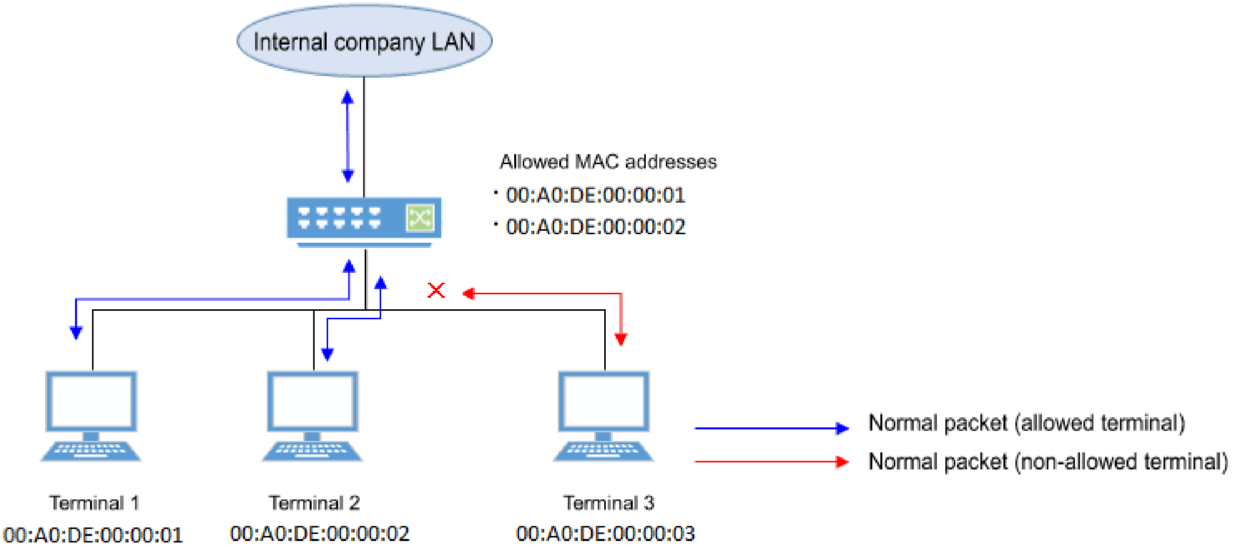
Related Documentation

- Built-in RADIUS Server
- Example Using the WLX402 Internal Radius server

Port Security Function

Function Overview

Port security is a function that limits communication to only permitted terminals, preventing access from illegal terminals.



Definition of Terms Used

None

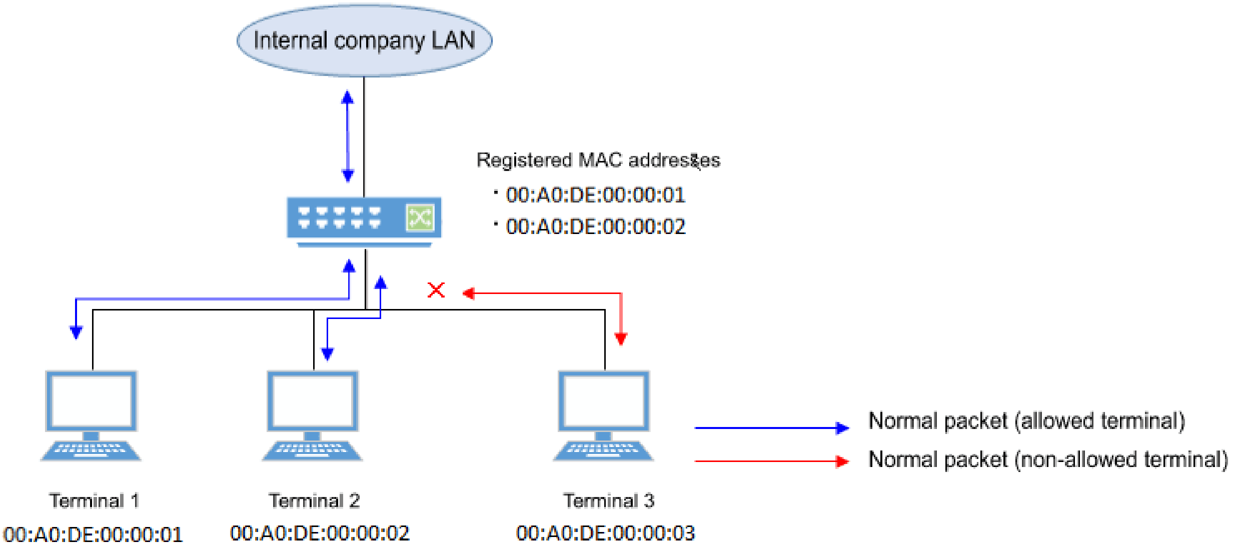
Function Details

For ports on which the port security function is enabled, you can pre-register the MAC address of a terminal for which you want to permit communication, thereby allowing communication only for permitted terminals. Conversely, if there is access from a terminal that is not registered (an illegal terminal), this is considered illegal access, and the packets are discarded.
Depending on the settings, the corresponding port can also be shut down.

The port security function cannot be used simultaneously with the port authentication function.

Limiting the terminals that can access

Simply by enabling the port security function, and using the **port-security mac-address** command to register the MAC addresses of the terminals for which you want to permit communication, you can limit the terminals that are permitted access.



Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Set port security function	port-security enable
Register permitted MAC addresses	port-security mac-address
Set operation for when security violation occurs	port-security violation
Show port security status	show port-security status

Examples of Command Execution

Limiting the terminals that can access

Manually specify the MAC address so that only the permitted terminal can communicate.

1. Enable port security on LAN port #1.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#port-security enable
```

2. Register the MAC address that you want to permit.

```
Yamaha(config)#port-security mac-address 00A0.DE00.0001 forward port1.1 vlan 1
Yamaha(config)#port-security mac-address 00A0.DE00.0002 forward port1.1 vlan 1
```

3. Check the port security status.

```
Yamaha#show port-security status
 Port      Security  Action     Status    Last violation
---------------------------------------------------------------------------------------------
```

```
--------- --------- ---------- --------- --------------------
port1.1   Enabled   Discard    Normal    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
```

Points of Caution

- Use the **no shutdown** command to recover the port that has shut down due to illegal access.
  The status that can be checked with the **show port-security status** command will not return to normal until the port links up. (The status will remain in shutdown state.)
- If the wrong port is specified with the **port-security mac-address** command, traffic and violation frames will not be correctly detected.

Related Documentation

None

PoE Control

Function Overview

PoE (Power over Ethernet) is a technology that supplies power using an Ethernet cable (category 5e or higher).

This product complies with **IEEE 802.3at**, which allows the product to supply power to Class 4 powered devices. In IEEE 802.3at, terms called

- Power supply side (device that supplies power) PSE: Power Sourcing Equipment
- Power receiving side (device that receives power): PD: Powered Device

are defined.
This product uses **Alternative A**, which uses the signal lines (1, 2, 3, 6) of cables as the power supply method.

Definition of Terms Used

None

Function Details

PoE power supply function enable/disable control

Ports that support PoE power supply of this product (hereinafter referred to as PoE ports) are as follows.

- SWX2310P-10G: ports 1 to 8
- SWX2310P-18G: ports 1 to 16
- SWX2310P-28GT: ports 1 to 24

This product allows you to enable/disable the power supply function for each port.

The power supply function of all the PoE ports of this product is enabled as the factory default.
If the connected device is a normal Ethernet device, the power will not be supplied and the device will operate as a **normal Ethernet port**.
This product continues to provide power to PDs even if the ports are shut down.

Power supply class and maximum number of ports that can be powered simultaneously

This product is a power supply device that complies with the PoE standards. It can supply **up to 30 W of power per port**.

It automatically detects the connected PD, identifies its power class, and starts the power supply.
The following table lists the power classes defined in IEEE 802.3at and the guideline for the maximum number of ports that can be simultaneously powered (the number of ports that can be simultaneously connected when each PD consumes power up to its limit).

Class	Power of device that receives power (MAX)	Power of device that supplies power	Maximum number of ports that can be powered simultaneously (Upper limit of PoE power supply)		
			SWX2310P-10G(124W)	SWX2310P-18G(247W)	SWX2310P-28GT(370W)
0	13.0 W	15.4 W	8	16	24
1	3.84 W	4.0 W	8	16	24
2	6.49 W	7.0 W	8	16	24
3	13.0 W	15.4 W	8	16	24

4	25.5 W	30.0 W	4 (*)	8 (*)	12 (*)

- (*): Depending on the power consumption of the device that receives power, the simultaneous power supply beyond the number of ports listed can be performed.

Guard band

A guardband is a margin set for the maximum power supply to prevent unexpected power outages.
If the available power supply amount reaches or falls below the guardband, power supply to a newly connected PD will be suppressed.
For example, if the guardband is set to 10 W on the SWX2310P-10MT (upper limit of available power supply amount: 124 W), a newly-connected PD is not powered when the total PoE supply power of all ports is 114 W or more (when the available power supply amount is 10 W or less).
Setting this guard band value appropriately can prevent a newly connected PD from stopping the power supply to other PDs.
This product allows you to set the guardband value within the range of **0 to 30 W**, and the value is set to **7 W** as the factory default.

PoE power priority

This product allows you to specify the power supply priority order for each PoE port.
The priority is **critical**, **high**, and **low** in descending order, and it is set to low for all ports as the factory default.
Among ports with the same priority setting, the smaller the port number, the higher the priority. The priority goes down in the port number order (1 → 2 → 3…).

PoE power supply actions

This product performs the following processes depending on the power consumption.

- When the total PoE supply power of all ports is about to exceed the upper limit of the available PoE power supply
  Power supply from PoE ports is stopped in the order from the lower priority to ensure that the total PoE supply power remains within the upper limit of the available PoE power supply.
  At this time, the MODE LED status automatically transitions to the STATUS mode, and the SPEED LED of the port to which power supply has been stopped flashes orange.
  In addition, “portX.X over system power limit” is output to SYSLOG.
- If the available power supply amount reaches or falls below the guardband
  Power will continue to be supplied to PDs that are already being powered. However, power will not be supplied to a newly-connected PD regardless of its PoE power priority.
  At this time, the MODE LED status automatically transitions to the STATUS mode, and the SPEED LED of the port to which power has not been supplied flashes orange.
  In addition, “portX.X restricted by guard band” is output to SYSLOG.
- When the PoE supply power of a specific PoE port has exceeded the upper limit of the available PoE power supply per port
  Power supply to the corresponding PoE port will be stopped. Power supply to other PoE ports will continue.
  At this time, the MODE LED status automatically transitions to the STATUS mode, and the SPEED LED of the port to which power supply has been stopped illuminates steady orange.
  In addition, “portX.X over load” is output to SYSLOG.
- If the PoE supply power is other than the above (within normal range)
  Power supply to PDs will continue.
  At this time, if the MODE LED status has transitioned to the STATUS mode due to the above factors, the MODE LED will return to the MODE before the automatic transition.

In addition, the following processing will be performed if the PoE port status or the available power supply amount has changed.

- When power supply is started
  "portX.X power on" is output to SYSLOG.
  When the MODE LED is in the PoE mode, the LINK LED of the port that has started supplying power illuminates steady green.
- When power supply is stopped
  "portX.X power off" is output to SYSLOG.
  When the MODE LED is in the PoE mode, the LINK LED of the port that has stopped supplying power switches off.
- If the available power supply amount reaches or falls below the guardband
  "Supplying power reached to guard band threshold" is output to SYSLOG.
- If the available power supply amount recovers from the state on or below the guardband
  "Supplying power fell below guard band threshold" is output to SYSLOG.

Power supply setting by LLDP

When the product receives an LLDP frame containing the Power via MDI TLV from a PD, it automatically changes the power supply action of the PoE port according to the received frame setting value.
This function only works on PoE ports that can receive LLDP frames.
The Power via MDI TLVs and the corresponding actions to be changed are as shown below.

Power via MDI TLV (IEEE802.3)	Action to be changed
Power priority	PoE power priority
PD requested power value	Upper limit of available power supply amount per port

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Set the PoE power supply function for the entire system	power-inline
Set the PoE power supply function on an interface basis	power-inline
Set the description text for PoE ports	power-inline description
Set the PoE port priority	power-inline priority
Set a guard band	power-inline guardband
Show PoE power supply information	show power-inline

Examples of Command Execution

PoE Port Power Supply Settings

Specify the settings for the power supply function of port1.8.

```
Yamaha(config)#power-inline enable ①
Yamaha(config)#interface port1.8
Yamaha(config-if)#power-inline description "AP1" ②
Yamaha(config-if)#power-inline priorty critical ③
Yamaha(config-if)#power-inline enable ④
Yamaha(config-if)#exit
Yamaha(config)#exit
```

① Enable the PoE supply function for the entire system. * Not required if the default settings are used

② Set “AP1” as the PoE port description

③ Set the priority of the PoE port to the highest (critical)

④ Enable the PoE supply function for the interface. * Not required if the default settings are used

Points of Caution

None

Related Documentation

- LED Control
- LLDP
- SYSLOG

Layer 2 Functions

Forwarding Database (FDB)

Function Overview

The Forwarding Database (subsequently referred to as the FDB) manages the combination of destination MAC addresses, transmission ports, and VLANs.
This product uses the FDB to determine the forwarding destination port for the received frames.

1. Enable/disable acquisition function
2. Hold Time adjustment for FDB entries acquired
3. Timeout clear for FDB entries acquired
4. Manual registration of FDB entries (static entries)

Definition of Terms Used

FDB

Abbreviation of “Forwarding Data Base.”
This database manages the combination of destination MAC address, transmission port, and VLAN.

FDB entry

This is data registered in the FDB, and consists of multiple elements.

Function Details

FDB entry

On this product, the contents listed in the table below are registered as a single entry in the FDB.
Up to 16,384 addresses can be registered, including addresses registered via automatic acquisition and manual registration.

Element managed	Description	
MAC address	Device MAC addresses can be either unicast or multicast.	
VLAN-ID (FID)	The VLAN ID to which the device belongs. This is a value from 1–4094.	
Forwarding destination interface ID	The interface on which the device exists. LAN/SFP ports are static/LACP logical interfaces.	
Action	The processing method for frames addressed to the device. There are two processing methods, “discard” and “forward”.	
Entry registration type	dynamic	Entries registered through automatic acquisition
	static	Entries registered manually via commands
	multicast	Entries acquired by IGMP/MLD Snooping

MAC address

This is one of the FDB key items; the VLAN-ID and MAC address are combined to become the record key. Operation differs depending on whether the MAC address is unicast or multicast.

- Unicast
  Since the forwarding destination interface ID must be uniquely determined for a given record key, duplication is not allowed.
  (Multiple combinations of the same VLAN-ID and MAC address do not exist.)
- Multicast
  Multiple forwarding destination interface IDs may exist for a given key record.
  In this case, frames are sent to multiple forwarding destination interface IDs.

The MAC addresses of all received frames can be acquired, and the source MAC address is acquired and registered in the FDB.
However, if the transmission source MAC address is multicast, this is considered an invalid frame and is discarded without being registered.
Each VLAN interface created internally consumes one FDB entry.

Automatically acquired MAC address information is maintained until the ageing timeout.

If multiple multicast MAC addresses are specified, all are considered as one in this case.

```
VLAN  port    mac             fwd      type    timeout
   1  port1.1 0100.0000.1000  forward  static       0
   1  port1.2 0100.0000.1000  forward  static       0
   1  port1.3 0100.0000.1000  forward  static       0
   1  port1.4 0100.0000.1000  forward  static       0
   1  port1.5 0100.0000.1000  forward  static       0
   1  port1.6 0100.0000.1000  forward  static       0
```

VLAN-ID

MAC address acquisition is done per VLAN, and the MAC address and VLAN are managed in the FDB as a pair.
For different VLANs, identical MAC addresses are also acquired.

Forwarding destination interface ID

The following IDs are registered.

- LAN/SFP port (port)
- Static/LACP logical interface (sa,po)

Action

This defines the action for a received frame that matches a key record.
If the MAC address is unicast, the actions are as follows.

- forward ... Forward to the forwarding destination interface ID.
- discard ... Discard without forwarding.

If the MAC address is multicast, the actions are as follows.

- forward ... Forward to the forwarding destination interface ID.

- discard ... Cannot be specified.
  (The discard setting cannot be made if the MAC address is multicast.)

Registration type

- dynamic … Registered and deleted automatically. The registration result does not remain in the config settings file.
- static … Registered and deleted manually, and therefore remains in the config settings file.
- multicast … Automatically registered and deleted by the IGMP/MLD snooping function. The registration result does not remain in the config settings file.

Automatic MAC address acquisition

Automatic MAC address acquisition refers to the active creation and registration of FDB entries based on the information for the source MAC address of the received frame and the information for the reception port.
Entries registered through automatic acquisition are called “dynamic entries”.
A timer (ageing time) is used to monitor individual entries.
Entries for MAC addresses that have not received frames within a certain amount of time will be automatically deleted from FDB entries by an aging timer.
This prevents invalid device entries from being left over in the FDB due to power shutoff, being moved and so on.
If a frame is received within the specified amount of time, the monitoring timer will be reset.

The control specifications for automatic acquisition are shown below.

1. Automatic MAC address acquisition can be enabled or disabled using the **mac-address-table learning** command.
   The setting is enabled by default.
2. If automatic acquisition is changed from enabled to disabled, **all dynamic entries that have been learned will be deleted**.
   The acquisition function “disable” setting is useful when you want to flood all ports with all received frames.
3. Aging timer settings for dynamic entries are specified using **mac-address-table ageing-time** command.
   This value is set to 300 seconds by default.
4. The actual time when entries are deleted by the aging time occurs within double the seconds specified as the timer setting value.
5. Clear the dynamic entries that have been acquired by using the **clear mac-address-table dynamic** command.
   The entire contents of the FDB can be cleared at once; or a VLAN number can be specified and all MAC addresses acquired by that VLAN can be cleared from the FDB.
   Specifying the port number will clear all MAC addresses from the FDB that were acquired from that port.
6. Use the **show mac-address-table** command to check the automatic acquisition status.

MAC address manual setting

In addition to automatic acquisition using received frames, MAC addresses can be set on this product by using user commands.
Entries that have been registered by using commands are called “static entries”.

The specifications for manual settings are shown below.

1. Use the **mac-address-table static** command to register static entries.
2. When registering static entries, dynamic acquisition will not be performed on the corresponding MAC addresses.

Entries that have already been acquired will be deleted from the FDB, and will be registered as static entries.

3. Use the **no mac-address-table static** command to delete static entries.
4. Either “forward” or “discard” can be specified for the destination MAC address of a received frame.
    - When forwarding is specified, either the LAN/SFP port forwarding destination or the static/LACP logical interface can be specified.
    - When discarding is specified, frames received by the MAC address will not be forwarded to any port, and will be discarded.
5. If registering a multicast MAC address, you cannot specify “discard.”
   Also, the following MAC addresses cannot be registered.
    - 0000.0000.0000
    - 0100.5e00.0000～0100.5eff.ffff
    - 0180.c200.0000–0180.c200.000f
    - 0180.c200.0020–0180.c200.002f
    - 3333.0000.0000～3333.ffff.ffff
    - ffff.ffff.ffff

Related Commands

Operations	Operating commands
Enable/disable the MAC address learning function	mac-address-table learning
Set dynamic entry ageing time	mac-address-table ageing-time
Delete dynamic entries	clear mac-address-table dynamic
Register static entries	mac-address-table static
Delete static entries	no mac-address-table static
View the MAC address table	show mac-address-table

Examples of Command Execution

Referring to the FDB

```
Yamaha#show mac-address-table
VLAN  port     mac             fwd      type     timeout
   1  port1.2  00a0.de11.2233  forward  static         0
   1  port1.1  1803.731e.8c2b  forward  dynamic      300
   1  port1.1  782b.cbcb.218d  forward  dynamic      300
```

Delete dynamic entries

Deleting an FDB entry registered in the FDB (MAC address 00:a0:de:11:22:33)

```
Yamaha#clear mac-address-table dynamic address 00a0.de11.2233
```

Changing the dynamic entry ageing time

This example shows how to change the dynamic entry ageing time to 400 seconds.

```
Yamaha(config)#mac-address-table ageing-time 400
```

Register static entries

This example shows how frames addressed to a device associated with VLAN #10 (MAC address 00:a0:de:11:22:33) can be forwarded to LAN port 2 (port1.2).

```
Yamaha(config)#mac-address-table static 00a0.de11.2233 forward port1.2 vlan 10
```

This example shows how to discard the frames sent to a device associated with VLAN #10 (MAC address 00:a0:de:11:22:33).
Specifying the interface name ("port1.2" in the example) will have no effect on operations. Since this cannot be omitted, specify the LAN/SFP port.

```
Yamaha(config)#mac-address-table static 00a0.de11.2233 discard port1.2 vlan 10
```

Delete static entries

This example shows how to delete the forwarding settings sent to a device associated with VLAN #10 (MAC address 00:a0:de:11:22:33).

```
Yamaha(config)#no mac-address-table static 00a0.de11.2233 forward port1.2 vlan 10
```

Points of Caution

If the **l2-unknown-mcast** command is configured to discard unknown multicast frames, using the **mac-address-table static** command to passively forward a multicast MAC address will have no effect when registered.

Related Documentation

None

VLAN

Function Overview

VLAN (Virtual LAN) is technology that allows a LAN to be constructed virtually, without regard to the physical structure of connections.

This product lets you use VLANs to divide the LAN into multiple **broadcast domains**.

The VLANs that are supported by this product are shown below.

VLAN types	Summary
Port-based VLAN	Groups that can communicate are configured for each LAN/SFP port.
Tagged VLAN	Groups that can communicate are identified, based on the fixed-length tag information appended to the Ethernet frame. Multiple and different VLANs can be made to communicate by means of one LAN/SFP port.
Private VLAN	Groups that can communicate within the same VLAN can be divided up. It consists of the following three types of VLANs: - Primary VLAN - Isolated VLAN - Community VLAN
Multiple VLAN	Each LAN/SFP port can be divided into multiple groups that can communicate. Refer to this information for multiple VLANs.
Voice VLAN	This allows audio and data to be handled separately on an access port.

Definition of Terms Used

Broadcast domain

This is a range in which broadcast frames can be delivered in a network, such as an Ethernet.

Devices that are connected by relaying a data link layer (MAC layer), such as switching hubs, can belong to the same broadcast domain.

A broadcast domain generally refers to the network in an Ethernet.

Function Details

Defining a VLAN ID

On product, a maximum of 255 VLANs can be defined, with VLAN IDs ranging from 2–4094. (ID #1 is used as the default VLAN ID.)

VLAN IDs are defined using the **vlan** command, after the **vlan database** command is used to enter VLAN mode.

For details, refer to the Command Reference.

VLAN settings for the LAN/SFP ports

The following settings must be configured after defining the VLANs to use, in order to make use of VLAN on this product.

- Set LAN/SFP port mode settings
- Set associated VLAN for LAN/SFP ports

1. The LAN/SFP ports on this product are set to one of the following modes.

    - Access port
      This is a port that handles untagged frames. It can be associated with one VLAN.
    - Trunk port

      This is a port that handles both tagged and untagged frames.

      It can be associated with multiple VLANs, and is mainly used to connect switches to one another. This product only supports IEEE 802.1Q. (Cisco ISL is not supported.)
2. Use the **switchport mode** command to set the LAN/SFP port mode.
   When setting the trunk port, use the input filter ("ingress-filter") to control whether frames not belonging to the specified VLAN ID will be handled.
    - Input filter enabled: Only frames set to the specified VLAN ID will be handled.
    - Input filter disabled: Frames with any VLAN ID will be handled.
3. Use the **show interface switchport** command to check the LAN/SFP port setting mode.
4. Use the **switchport access vlan** command to set which VLANs belong to the access port.
5. Use the **switchport trunk allowed vlan** command to set which VLANs belong to the trunk port.
   As the trunk port can be associated with multiple VLANs, use the "all", "none", "except", "add" and "remove" settings as shown below.
    - add

      Adds the specified VLAN ID.
      VLAN IDs that can be added are limited by the IDs that are defined by the VLAN mode.
    - remove
      Deletes the specified VLAN ID.
    - all

      Adds all VLAN IDs specified by the VLAN mode.
      The VLAN IDs added by the VLAN mode can also be added after this command is executed.
    - none
      The trunk port will not be associated with any VLAN.
    - except

      Adds all other VLAN IDs except for the ones specified.
      The VLAN IDs added by the VLAN mode can also be added after this command is executed.
6. A VLAN that uses untagged frames (native VLAN) can be specified for the trunk port.
7. Tagged audio frames can be transferred by specifying a voice VLAN for an access port.
8. Use the **show vlan** command to check which VLANs belong to a LAN/SFP port.

VLAN access control

This product provides an VLAN access map function, to control access to the VLAN.
The VLAN access map can be associated with a standard/extended IP access control list and a MAC address control list as VLAN ID filtering parameters.
The VLAN access map is operated using the commands shown below.

- Create VLAN access map: **vlan access-map** command
- Set VLAN access map parameters: **match access-list** command
- Assign VLAN access map: **vlan filter** command
- Show VLAN access map: **show vlan access-map** command

Default VLAN

The default VLAN is VLAN #1 (vlan1), which exists in this switch by default.

As the default VLAN is a special VLAN, it always exists and cannot be deleted.
The following operations can be used to automatically delete the relevant port from the default VLAN.

- Setting the VLAN for an access port
- Setting any VLAN other than the default as the native VLAN for the trunk port
- Setting the native VLAN for the trunk port to “none”

Native VLAN

A native VLAN is a VLAN that associates untagged frames received by the LAN/SFP port that was set as a trunk port.

Defining an LAN/SFP port as a trunk port will set the default VLAN (VLAN #1) as the native VLAN.

Use the **switchport trunk native vlan** command when specifying a certain VLAN as the native VLAN.
If you do not want to handle untagged frames on the LAN/SFP port, you can set the native VLAN to none.
(Specify “none” with the “**switchport trunk native vlan**” command.)

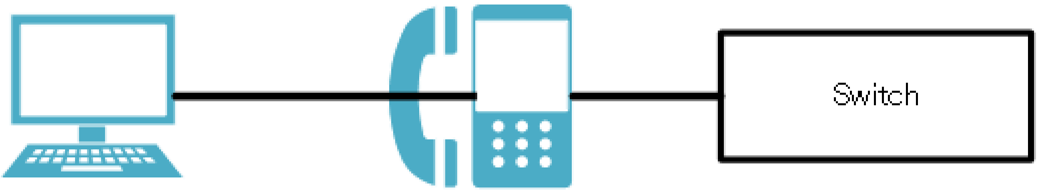
Private VLAN

This product can configure a private VLAN for further dividing up groups that can communicate within the same subnet.
The operating specifications are shown below.

1. A private VLAN contains the following three VLAN types.
   - Primary VLAN
     This is the parent VLAN of the secondary VLAN.
     Only one primary VLAN can be set per private VLAN.
   - Isolated VLAN
     This is a kind of secondary VLAN, which only sends traffic to a primary VLAN.
     Only one primary VLAN can be set per private VLAN.
   - Community VLAN
     This is a kind of secondary VLAN, which only sends traffic to VLANs in the same community and to a primary VLAN.
     Multiple community VLANs can be set for each private VLAN.
2. A primary VLAN may contain multiple promiscuous ports.
   Access ports, trunk ports, or static/LACP logical interfaces are the ports that can be used as promiscuous ports.
3. Only access ports can be used as host ports for a secondary VLAN (isolated VLAN, community VLAN).
4. A secondary VLAN (isolated VLAN, community VLAN) can be associated with one primary VLAN.
   Use the **switchport private-vlan mapping** command to create the association.
   - An isolated VLAN can be associated with multiple promiscuous ports contained within a private VLAN.
   - A community VLAN can be associated with multiple promiscuous ports contained within a private VLAN.

Voice VLAN

Voice VLAN is a function that can prevent audio from being adversely affected even when IP phone voice traffic is mixed with PC data traffic.



Some IP phones have two ports: a port for connection to the network switch and a port for connection to the PC. By connecting the network switch to the IP phone, and the IP phone to the PC, it is possible to use one port of the network switch to handle the IP phone audio traffic and the PC's data traffic.
Using the voice VLAN function in this type of configuration allows the audio data and the PC data to be separated so that noise is less likely to occur on the IP phone, or to handle the audio data with a higher priority.

Voice VLAN settings are made by the **switchport voice vlan** command.
Set one of the following to be handled as voice traffic.

- Frames with the 802.1p tag
- Priority tag frames (802.1p tags with a VLAN ID of 0 and only the CoS value specified)
- Untagged frames

When tagged frames are handled as voice traffic, untagged frames are handled as data traffic.

By using LLDP, this product can automatically apply settings to a connected IP telephone.
The conditions for making automatic settings are as follows.

- LLDP-MED TLV transmission is enabled on the port for which voice VLAN is enabled.
- The connected IP phone supports settings via LLDP-MED.

If the above conditions are satisfied, and when an IP phone is connected to the corresponding port, voice VLAN information (tagged/untagged, VLAN ID, the CoS value to be used, DSCP value) are notified according to the Network Policy TLV of LLDP-MED when an IP phone is connected to the corresponding port.
The IP phone will transmit voice data according to the information that was provided to it from this unit.

The CoS value specified for the IP phone is set by the **switchport voice cos** command, and the DSCP value is set by the **switchport voice dscp** command.
In order to give priority to handling voice traffic, QoS settings (enable QoS, set trust mode) according to the IP phone settings are also required.

The limitations of voice VLAN are as follows.

- It can be used only on a physical interface port that is assigned as an access port.
  It cannot be used on a link aggregation logical interface or on a VLAN logical interface.
- The voice VLAN function and the port authentication function cannot be used together.

Related Commands

List of related commands

- Related commands are indicated below.

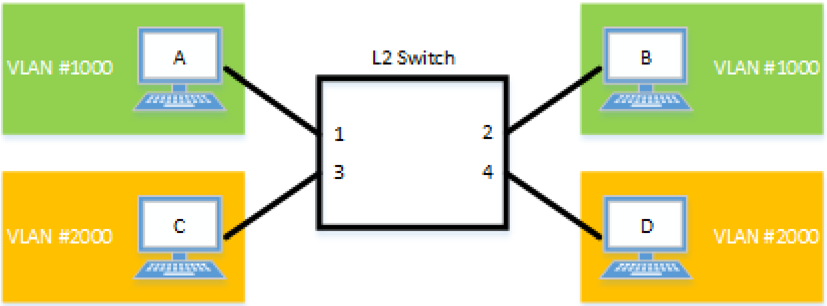
Operations	Operating commands
Enter VLAN mode	vlan database
Define VLAN interface, or change a predefined VLAN	vlan
Define a private VLAN	private-vlan

Operations	Operating commands
Set the secondary VLAN for a private VLAN	private-vlan association
Create VLAN access map	vlan access-map
Set VLAN access map parameters	match
Assign VLAN access map to VLAN	vlan filter
Set access port (untagged port)	switchport mode access
Set associated VLAN of an access port (untagged port)	switchport access vlan
Set trunk port (tagged port)	switchport mode trunk
Set associated VLAN for trunk port (tagged port)	switchport trunk allowed vlan
Set native VLAN for trunk port (tagged port)	switchport trunk native vlan
Set ports for private VLAN (promiscuous port, host port)	switchport mode private-vlan
Configure VLAN for private VLAN port and host port	switchport private-vlan host-association
Configure VLAN for private VLAN port and promiscuous port	switchport private-vlan mapping
Configure voice VLAN	switchport voice vlan
Set CoS value for voice VLAN	switchport voice cos
Set DSCP value for voice VLAN	switchport voice dscp
Show VLAN information	show vlan
Show private VLAN information	show vlan private-vlan
Show VLAN access map	show vlan access-map
Show VLAN access map filter	show vlan filter

Examples of Command Execution

Port-based VLAN settings

In this example, a port-based VLAN is configured for this product in order to allow communication between hosts A–B and hosts C–D.



The LAN port settings for this product are as follows.

- LAN ports #1 and #2: Set as access port, and associated with VLAN #1000
- LAN ports #3 and #4: Set as access port, and associated with VLAN #2000

■ **Setting Procedure**

1. Switch to VLAN mode using the **vlan database** command, and define two VLANs using the **vlan** command.

```
Yamaha(config)# vlan database ①
Yamaha(config-vlan)# vlan 1000 ②
Yamaha(config-vlan)# vlan 2000 ③
Yamaha(config-if)# exit
```

① Switch to VLAN mode

② Create VLAN #1000

③ Create VLAN #2000

2. Set LAN ports #1–2 as access ports, and associate them with VLAN #1000.

```
Yamaha(config)# interface port1.1-2 ①
Yamaha(config-if)# switchport mode access ②
Yamaha(config-if)# switchport access vlan 1000 ③
Yamaha(config-if)# exit
```

① Switch to interface mode

② Set the ports as access port

③ Define a VLAN ID

3. Set LAN ports #3–4 as access ports, and associate them with VLAN #2000.

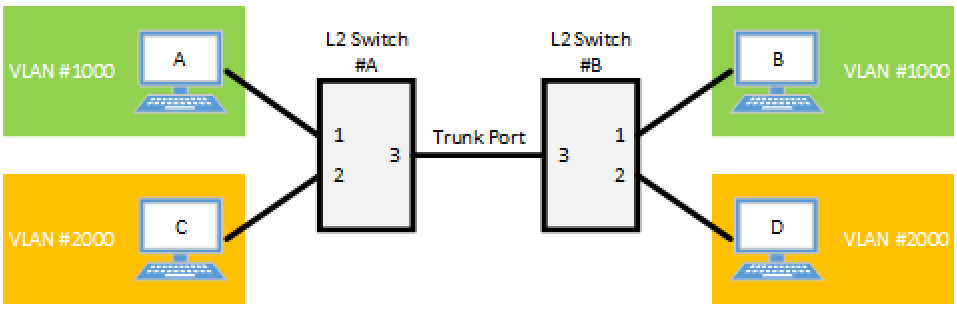
```
Yamaha(config)# interface port1.3-4
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 2000
Yamaha(config-if)# exit
```

4. Confirm the VLAN settings.

```
Yamaha#show vlan brief
(u)-Untagged, (t)-Tagged
VLAN ID  Name             State   Member ports
======= ================ ======= ===============================
1       default          ACTIVE  port1.5(u) port1.6(u)
                                 port1.7(u) port1.8(u)
1000    VLAN1000         ACTIVE  port1.1(u) port1.2(u)
2000    VLAN2000         ACTIVE  port1.3(u) port1.4(u)
```

Tagged VLAN settings

In this example, a tagged VLAN is configured between #A and #B of this product, in order to communicate between hosts A–B and hosts C–D.



The LAN port settings for #A and #B of this product are as follows.

- LAN port #1: Set as access port, and associated with VLAN #1000
- LAN port #2: Set as access port, and associated with VLAN #2000
- LAN port #3: Set as trunk port, and associated with LAN #1000 and VLAN #2000

1. [Switch #A/#B] Define VLAN.

```
Yamaha(config)#vlan database ①
Yamaha(config-vlan)#vlan 1000 ②
Yamaha(config-vlan)#vlan 2000 ③
```

① Switch to vlan mode

② Define VLAN #1000

③ Define VLAN #2000

2. [Switch #A/#B] Set LAN port #1 as the access port, and associate it with VLAN #1000.

```
Yamaha(config)#interface port1.1 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport access vlan 1000 ③
Yamaha(config-if)#exit
```

① Switch to interface mode

② Set the ports as access port

③ Associate it with VLAN #1000

3. [Switch #A/#B] Set LAN port #2 as the access port, and associate it with VLAN #2000.

```
Yamaha(config)#interface port1.2 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport access vlan 2000 ③
Yamaha(config-if)#exit
```

① Switch to interface mode

② Set the ports as access port

③ Associate it with VLAN #2000

4. [Switch #A/#B] Set LAN port #3 as a trunk port, and associate it with VLAN #1000/#2000.

```
Yamaha(config)#interface port1.3 ①
Yamaha(config-if)#switchport mode trunk ②
Yamaha(config-if)#switchport trunk allowed vlan add 1000 ③
Yamaha(config-if)#switchport trunk allowed vlan add 2000 ④
Yamaha(config-if)#exit
```

① Switch to interface mode

② Set the port as trunk port

③ Add VLAN #1000

④ Add VLAN #2000

5. Confirm the VLAN settings.

```
Yamaha#show vlan brief
(u)-Untagged, (t)-Tagged

VLAN ID  Name                             State   Member ports
======= ================================ ======= =====================
1       default                          ACTIVE  port1.3(u)
1000    VLAN1000                         ACTIVE  port1.1(u) port1.3(t)
2000    VLAN2000                         ACTIVE  port1.2(u) port1.3(t)
```

Private VLAN settings

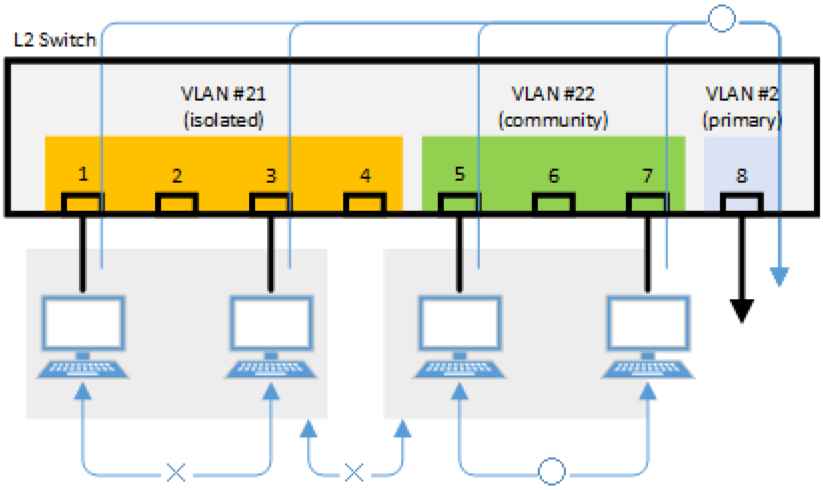
This example makes private VLAN settings for this product, to achieve the following.

Hosts connected to ports 1–7 will connect to the Internet and other external lines, through the line to which port 8 is connected

Communications between hosts connected to ports 1–4 are blocked (isolated VLAN: VLAN #21)

Communications between hosts connected to ports 5–7 are permitted (community VLAN: VLAN #22)

Communications between hosts connected to ports 1–4 and ports 5–7 are blocked



1. Define the VLAN ID to be used for the private VLAN.

```
Yamaha(config)# vlan database ①
Yamaha(config-vlan)# vlan 2 ②
Yamaha(config-vlan)# vlan 21
Yamaha(config-vlan)# vlan 22
Yamaha(config-vlan)# private-vlan 2 primary ③
Yamaha(config-vlan)# private-vlan 21 isolated ④
Yamaha(config-vlan)# private-vlan 22 community ⑤
Yamaha(config-vlan)# private-vlan 2 association add 21 ⑥
Yamaha(config-vlan)# private-vlan 2 association add 22
Yamaha(config-vlan)# exit
```

① Switch to VLAN mode

② Create VLAN

③ Configure primary VLAN

④ Configure isolated VLAN

⑤ Configure community VLAN

⑥ Associate the ports with primary VLAN

2. Configure the isolated VLAN (VLAN #21) for LAN ports 1–4.

```
Yamaha(config)#interface port1.1-4 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport access vlan 21 ③
Yamaha(config-if)#switchport mode private-vlan host ④
Yamaha(config-if)#switchport private-vlan host-association 2 add 21
Yamaha(config-if)#exit
```

① Switch to interface mode

② Set the ports as access port

③ Associate the ports with VLAN #21

④ Set the ports as private VLAN host port

3. Configure the community VLAN (VLAN #22) for LAN ports 5–7.

```
Yamaha(config)#interface port1.5-7 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport access vlan 22 ③
Yamaha(config-if)#switchport mode private-vlan host ④
Yamaha(config-if)#switchport private-vlan host-association 2 add 22
Yamaha(config-if)#exit
```

① Switch to interface mode

② Set the ports as access port

③ Associate the ports with VLAN #22

④ Set the ports as private VLAN host port

4. Configure the primary VLAN (VLAN #2) for LAN port 8. (Promiscuous port)

```
Yamaha(config)#interface port1.8 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport access vlan 2 ③
Yamaha(config-if)#switchport mode private-vlan promiscuous ④
Yamaha(config-if)#switchport private-vlan mapping 2 add 21
Yamaha(config-if)#switchport private-vlan mapping 2 add 22
Yamaha(config-if)#exit
```

① Switch to interface mode

② Set the ports as access port

③ Associate the ports with VLAN #2

④ Set the ports as private VLAN promiscuous port

5. Confirm the VLAN settings.

```
Yamaha#show vlan brief
(u)-Untagged, (t)-Tagged

VLAN ID  Name                            State   Member ports
======= ================================ ======= ======================
1       default                          ACTIVE
2       VLAN0002                         ACTIVE  port1.8(u)
21      VLAN0021                         ACTIVE  port1.1(u) port1.2(u)
                                                 port1.3(u) port1.4(u)
22      VLAN0022                         ACTIVE  port1.5(u) port1.6(u)
                                                 port1.7(u)

Yamaha#show vlan private-vlan
 PRIMARY        SECONDARY          TYPE          INTERFACES
 -------        ---------       ----------      ----------
       2              21          isolated       port1.1 port1.2
                                                 port1.3 port1.4
       2              22         community       port1.5 port1.6
                                                 port1.7
```

Voice VLAN settings

Make voice VLAN settings for this product, and implement the following.

Connect an IP phone to port 1. Connect a PC to the other LAN port of the IP phone.
Using LLDP-MED, make the following settings from this product for the IP phone.

- As voice traffic for the IP phone, transmit and receive 802.1q tagged frames of VLAN #2.
- Untagged frames are transmitted and received as PC data traffic.
- Use a CoS value of 6 when transmitting and receiving voice traffic.

1. Define the VLAN ID used by the voice VLAN.

```
Yamaha(config)# vlan database ①
Yamaha(config-vlan)# vlan 2 ②
Yamaha(config-vlan)# exit
```

① Switch to VLAN mode

② Create VLAN

2. Set voice VLAN for LAN port #1.

```
Yamaha(config)#interface port1.1 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport voice vlan 2 ③
Yamaha(config-if)#switchport voice cos 6 ④
Yamaha(config-if)#exit
```

① Switch to interface mode

② Set the ports as access port

③ Configure voice traffic as tagged frames for VLAN #2

④ Set the CoS value for voice traffic to 6

3. Set QoS for LAN port #1.

```
Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust cos ③
Yamaha(config-if)#exit
```

① Enable QoS

② Switch to interface mode

③ Set trust mode to CoS

4. Set LLDP-MED transmission and reception for LAN port #1.

```
Yamaha(config)#interface port1.1 ①
Yamaha(config-if)#lldp-agent ②
Yamaha(lldp-agent)#tlv-select med ③
Yamaha(lldp-agent)#set lldp enable txrx ④
Yamaha(lldp-agent)#exit
Yamaha(config-if)#exit
Yamaha(config)#lldp run ⑤
Yamaha(config)#exit
```

① Switch to interface mode

② Create LLDP agent, mode transition

③ Set LLDP-MED TLV

④ Set LLDP transmission/reception mode

⑤ Enable LLDP function

Points of Caution

A host port that is associated with a private VLAN cannot be aggregated as a link aggregation logical interface; this limitation is specific to host ports.

Related Documentation

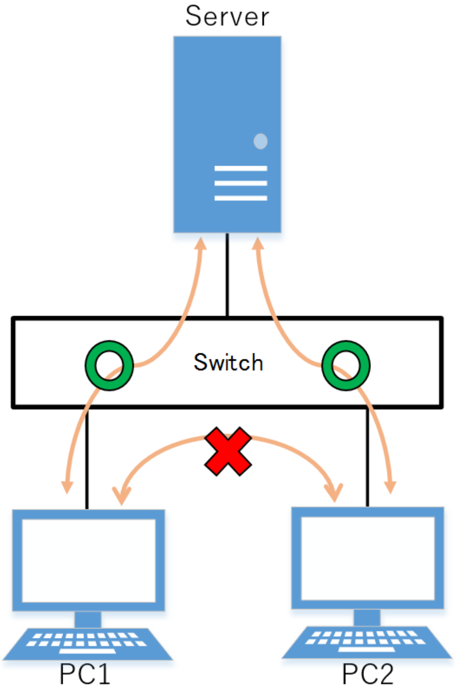
- Multiple VLAN

Multiple VLAN

Function Overview

On a multiple VLAN, by associating a port with a multiple VLAN group, you can block traffic from ports that do not belong to the same multiple VLAN group.
You can also join a single port to multiple VLAN groups.
By using this function, it is easy to handle requests to block only traffic between terminals, such as the example below.

- Example of using multiple VLANs



Definition of Terms Used

None

Function Details

Operating specifications

Use the **switchport multiple-vlan group** command to configure a multiple VLAN group.
Multiple VLANs can be configured as LAN/SFP ports and link aggregation logical interfaces.
If you wish to configure a multiple VLAN group for a trunk port, this will be applied to all relevant VLANs that belong to the port in question.
The multiple VLAN group settings will also be applied to a multicast frame.

This can be used together with the following functions. Control of traffic enable/disable for these functions is set according to the multiple VLAN group settings.

- Port-based VLAN/tagged VLAN/voice VLAN
- Port authentication

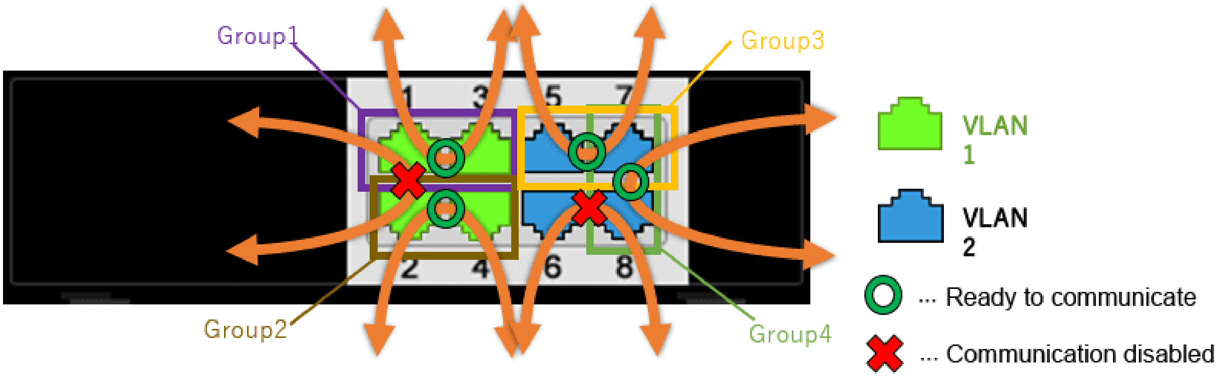
A multiple VLAN can contain up to **256** groups.

Use the **show vlan multiple-vlan group** command to confirm the setting status for the interface of each multiple

VLAN group.

Examples of traffic between multiple VLAN groups

- Example of traffic for a multiple VLAN group



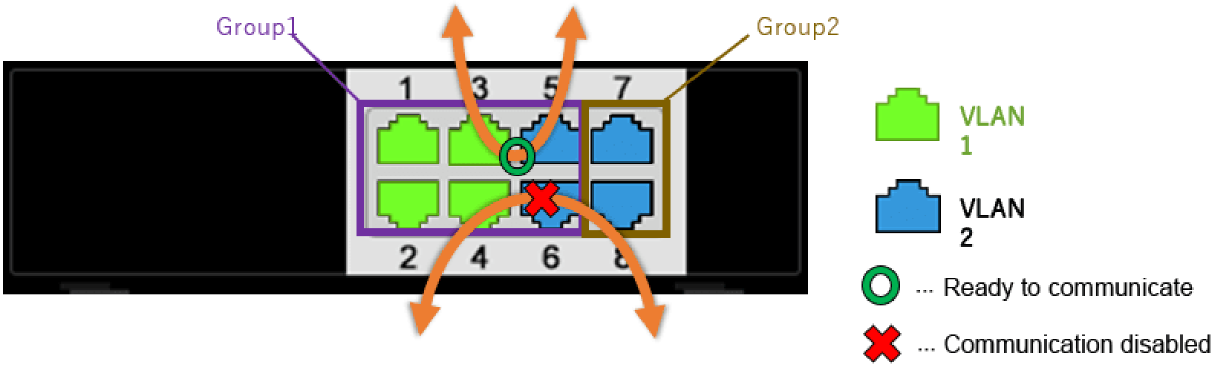
When using multiple VLAN group settings (Group #1 through #4) as shown in the diagram above, enabling/disabling traffic between specific ports A/B and the reasons for such as shown in the table below.

Port number A (group)	Port number B (group)	Traffic enable/disable	Reason
port1.1 (Group 1)	port1.2 (Group 2)	Disabled	The multiple VLAN group is different
port1.1 (Group 1)	port1.3 (Group 1)	Enabled	Associated with multiple VLAN group #1
port1.2 (Group 2)	port1.4 (Group 2)	Enabled	Associated with multiple VLAN group #2
port1.5 (Group 3)	port1.7 (Group 3,4)	Enabled	Associated with multiple VLAN group #3
port1.6 (no group)	port1.8 (Group 4)	Disabled	The multiple VLAN group is different
port1.7 (Group 3,4)	port1.8 (Group 4)	Enabled	Associated with multiple VLAN group #4

Also, traffic can be established between ports that are not associated with a multiple VLAN group, so long as it is within the same VLAN.

Communication example when inter-VLAN routing is possible

- Example of inter-VLAN routing communication



Inter-VLAN routing is possible with L3 switches with routing enabled. In inter-VLAN routing, packets that are routed by hardware can be controlled by multiple VLAN groups.
When using multiple VLAN group settings (Group #1 through #2) as shown in the diagram above, enabling/disabling traffic between specific ports A/B and the reasons for such as shown in the table below.

Port number A (group)	Port number B (group)	Traffic enable/disable	Reason
port1.3 (Group 1)	port1.5 (Group 1)	Enabled	Associated with multiple VLAN group #1
port1.4 (Group 1)	port1.8 (Group 2)	Disabled	The multiple VLAN group is different

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

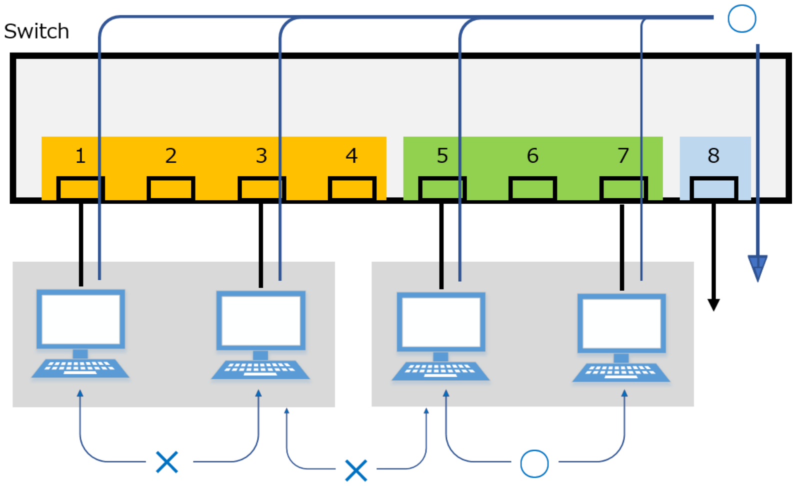
Operations	Operating commands
Multiple VLAN group settings	switchport multiple-vlan group
Settings for the name of multiple VLAN group	multiple-vlan group name
Set YMPI frame transmission function when multiple VLANs are specified	multiple-vlan transfer ympi
Show multiple VLANs	show vlan multiple-vlan

Examples of Command Execution

Multiple VLAN settings example 1

This configures multiple VLAN settings to achieve the following.

Hosts connected to ports 1–7 will connect to the Internet and other external lines, through the line to which port 8 is connected
Communications between hosts connected to ports 1–4 are blocked
Communications between hosts connected to ports 5–7 are permitted
Communications between hosts connected to ports 1–4 and ports 5–7 are blocked



The multiple VLAN group settings are as follows.

- port1.1: Associated with multiple VLAN group #1
- port1.2: Associated with multiple VLAN group #2
- port1.3: Associated with multiple VLAN group #3
- port1.4: Associated with multiple VLAN group #4
- port1.5: Associated with multiple VLAN group #5
- port1.6: Associated with multiple VLAN group #5
- port1.7: Associated with multiple VLAN group #5
- port1.8: Associated with multiple VLAN groups #1, #2, #3, #4, and #5

1. This sets the name of multiple VLAN group #1 to “Network1”.

   ```
   Yamaha(config)# multiple-vlan group 1 name Network1 ①
   ```

   ① Settings for the name of multiple VLAN group #1

2. This sets the name of multiple VLAN group #5 to “Network5”.

   ```
   Yamaha(config)# multiple-vlan group 5 name Network5 ①
   ```

   ① Settings for the name of multiple VLAN group #5

3. Associates port1.1 through port1.4 with multiple VLAN groups #1 through #4 respectively.

   ```
   Yamaha(config)# interface port1.1 ①
   Yamaha(config-if)# switchport multiple-vlan group 1 ②
   Yamaha(config-if)# exit
   Yamaha(config)# interface port1.2 ③
   Yamaha(config-if)# switchport multiple-vlan group 2 ④
   Yamaha(config-if)# exit
   Yamaha(config)# interface port1.3 ⑤
   Yamaha(config-if)# switchport multiple-vlan group 3 ⑥
   Yamaha(config-if)# exit
   Yamaha(config)# interface port1.4 ⑦
   Yamaha(config-if)# switchport multiple-vlan group 4 ⑧
   Yamaha(config-if)# exit
   ```

   ① Switch to interface mode

   ② Configure multiple VLAN group

   ③ Switch to interface mode

   ④ Configure multiple VLAN group

   ⑤ Switch to interface mode

   ⑥ Configure multiple VLAN group

   ⑦ Switch to interface mode

   ⑧ Configure multiple VLAN group

4. This associates port1.5 through port1.7 with multiple VLAN group #5.

   ```
   Yamaha(config)# interface port1.5-7 ①
   Yamaha(config-if)# switchport multiple-vlan group 5 ②
   ```

```
Yamaha(config-if)# exit
```

① Switch to interface mode

② Specify multiple VLAN group

5. This associates port1.8 with multiple VLAN groups #1, #2, #3, #4, #5.

```
Yamaha(config)# interface port1.8 ①
Yamaha(config-if)# switchport multiple-vlan group 1-5 ②
Yamaha(config-if)# exit
```

① Switch to interface mode

② Specify multiple VLAN group

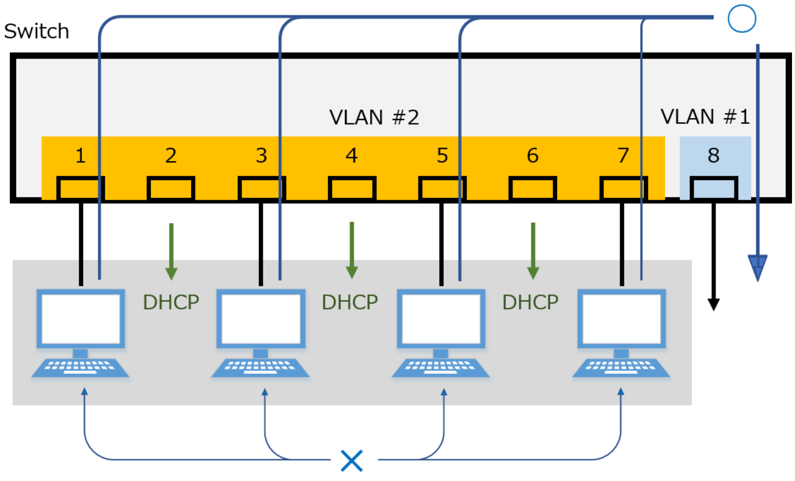
6. This checks the multiple VLAN group settings.

```
Yamaha>show vlan multiple-vlan
GROUP ID  Name                            Member ports
======== ================================ ======================
1        Network1                         port1.1 port1.8
2        GROUP0002                        port1.2 port1.8
3        GROUP0003                        port1.3 port1.8
4        GROUP0004                        port1.4 port1.8
5        Network5                         port1.5 port1.6
                                          port1.7 port1.8
```

Multiple VLAN settings example 2

This configures multiple VLAN settings to achieve the following.

Hosts connected to ports 1 to 7 will connect to the Internet and other external lines, through the line to which port 8 is connected
Hosts connected to ports 1 to 7 are associated with VLAN #2 and assigned an IP address using the DHCP server functions
The IP address for VLAN #2 is 192.168.110.240/24 and the range of assigned addresses is from 192.168.110.2 to 192.168.110.191/24
Communication is blocked between hosts connected to ports 1 to 7



The multiple VLAN group settings are as follows.

- port1.1: Associated with multiple VLAN group #1
- port1.2: Associated with multiple VLAN group #2
- port1.3: Associated with multiple VLAN group #3
- port1.4: Associated with multiple VLAN group #4
- port1.5: Associated with multiple VLAN group #5
- port1.6: Associated with multiple VLAN group #6
- port1.7: Associated with multiple VLAN group #7
- port1.8: Associated with multiple VLAN groups #1, #2, #3, #4, #5, #6, and #7
- Assign ports port1.1 to port1.7 to VLAN #2.

```
Yamaha(config)# interface port1.1-7
Yamaha(config-if)# switchport access vlan 2
Yamaha(config-if)#
```

```
Yamaha(config)# interface vlan2
Yamaha(config-if)# ip address 192.168.110.240/24
```

- Create the DHCP pool “pool_vlan2”.

```
Yamaha(config)# dhcp pool pool_vlan2
Yamaha(config-dhcp)①
```

① Switch to the DHCP mode

- Specify the VLAN #2 network portion 192.168.110.0/24 in the DHCP pool.

```
Yamaha(config-dhcp)# network 192.168.110.0/24
```

- Specify the address assignment range from 192.168.110.2 to 192.168.110.191 in the DHCP pool.

```
Yamaha(config-dhcp)# range 192.168.110.2 192.168.110.191
```

- Specify the default gateway to be notified in DHCP option settings and specify the DNS server in the DHCP pool.

```
Yamaha(config-dhcp)# default-router 192.168.110.240 ①
Yamaha(config-dhcp)# dns-server 192.168.110.1 ②
Yamaha(config-dhcp)# exit ③
```

① The default gateway address is 192.168.110.240 (its own address)

② The DNS server address is 192.168.110.1

③ Exit the DHCP mode

- Activate the DHCP server functions for vlan2.

```
Yamaha(config)# interface vlan2 ①
Yamaha(config-if)# dhcp-server enable ②
Yamaha(config-if)# exit ③
```

① Switch to interface mode

② Enable the DHCP server functions for the interface

③ Exit the interface mode

- Activate the DHCP server functions for the entire system.

```
Yamaha(config)# dhcp-server enable ①
```

① Enable the DHCP server functions for the entire system

- Associate port1.1 through port1.7 with multiple VLAN groups #1 through #7 respectively.

```
Yamaha(config)# interface port1.1 ①
Yamaha(config-if)# switchport multiple-vlan group 1 ②
Yamaha(config-if)# exit
Yamaha(config)# interface port1.2 ③
Yamaha(config-if)# switchport multiple-vlan group 2 ④
Yamaha(config-if)# exit
Yamaha(config)# interface port1.3 ⑤
Yamaha(config-if)# switchport multiple-vlan group 3 ⑥
Yamaha(config-if)# exit
Yamaha(config)# interface port1.4 ⑦
Yamaha(config-if)# switchport multiple-vlan group 4 ⑧
Yamaha(config-if)# exit
Yamaha(config)# interface port1.5 ⑨
Yamaha(config-if)# switchport multiple-vlan group 5 ⑩
Yamaha(config-if)# exit
Yamaha(config)# interface port1.6 ⑪
Yamaha(config-if)# switchport multiple-vlan group 6 ⑫
Yamaha(config-if)# exit
Yamaha(config)# interface port1.7 ⑬
Yamaha(config-if)# switchport multiple-vlan group 7 ⑭
Yamaha(config-if)# exit
```

① Switch to interface mode

② Configure multiple VLAN group

③ Switch to interface mode

④ Configure multiple VLAN group

⑤ Switch to interface mode

⑥ Configure multiple VLAN group

⑦ Switch to interface mode

⑧ Configure multiple VLAN group

⑨ Switch to interface mode

⑩ Configure multiple VLAN group

⑪ Switch to interface mode

⑫ Configure multiple VLAN group

⑬ Switch to interface mode

⑭ Configure multiple VLAN group

- Associate port1.8 with multiple VLAN groups #1 to #7.

```
Yamaha(config)# interface port1.8 ①
Yamaha(config-if)# switchport multiple-vlan group 1-7 ②
Yamaha(config-if)# exit
```

① Switch to interface mode

② Specify multiple VLAN group

- This checks the multiple VLAN group settings.

```
Yamaha>show vlan multiple-vlan
GROUP ID  Name                             Member ports
======== ================================ ======================
1        GROUP0001                        port1.1 port1.8
2        GROUP0002                        port1.2 port1.8
3        GROUP0003                        port1.3 port1.8
4        GROUP0004                        port1.4 port1.8
5        GROUP0005                        port1.5 port1.8
6        GROUP0006                        port1.6 port1.8
7        GROUP0007                        port1.7 port1.8
```

Points of Caution

The points of caution regarding this function are as follows.

- The function cannot be used in conjunction with a private VLAN.
- The multiple VLAN group to associate with a link aggregation logical interface must be the same.
- A multiple VLAN group is only applicable to forwarding between ports. Voluntary packets will not be affected by the settings of a multiple VLAN group.
- Even if a multiple VLAN is configured, communication may not work correctly due to the following influences.
    - Block status of spanning tree
    - IGMP snooping/MLD snooping status
    - Blocked status of loop detection
- In inter-VLAN routing, multiple VLAN communication restrictions are applied only to packets routed by hardware processing.
  Restrictions do not apply to inter-VLAN routing through the CPU.
- YMPI frames are transmitted for managing Yamaha wireless access points if multiple VLANs are specified.
  Therefore, even if there are multiple Yamaha wireless access points associated with different multiple VLAN groups, the cluster management function or the wireless LAN controller function can be used.

Related Documentation

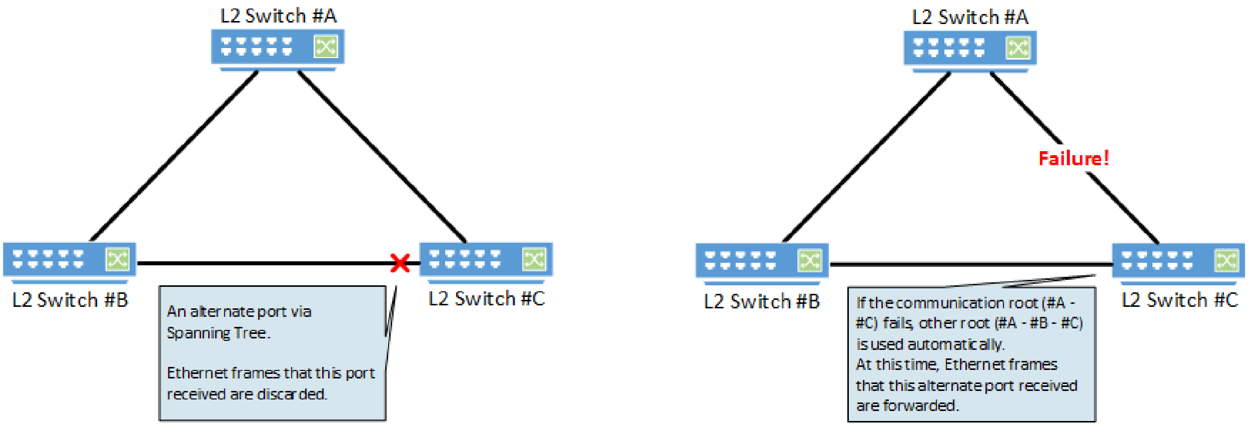
- VLAN

Spanning Tree

Function Overview

The spanning tree is a function that maintains redundancies in the network routes while preventing loops.
Normally, the L2 switch floods the adjacent network switch with the broadcast packets.
If the network is constructed as a loop, the network switches will flood each other, causing the loop to occur.
This results in a major degradation of bandwidth and CPU resources in the network switches.
The spanning tree determines the roles of each port and establishes a network construction where the broadcast packets do not keep traveling around, for networks that contain physical loops as well.
When there are problems linking, the problem is detected and the tree is reconstructed in order to restore the system.
This product supports STP, RSTP, and MSTP.

- Spanning tree function overview


L2 Switch #A
L2 Switch #B
L2 Switch #C
An alternate port via Spanning Tree.
Ethernet frames that this port received are discarded.
L2 Switch #A
Failure!
L2 Switch #B
L2 Switch #C
If the communication root (#A - #C) fails, other root (#A - #B - #C) is used automatically.
At this time, Ethernet frames that this alternate port received are forwarded.

Normal operation

Abnormal operation

Definition of Terms Used

STP：Spanning Tree Protocol (802.1d)

The spanning tree protocol (STP) exchanges BPDU (bridge protocol data unit) messages, in order to avoid loops.
This product supports **IEEE802.1d** and **RFC4188**.

RSTP：Rapid Spanning Tree Protocol (802.1w)

The rapid spanning tree protocol (RSTP) is an extension of STP. It can recover the spanning tree more quickly than STP, when the network architecture has changed or when there is a problem linking.
This product supports **IEEE802.1w** and **RFC4318**.

MSTP：Multiple Spanning Tree Protocol (802.1s)

Multiple spanning tree protocol (MSTP) is a further extension of STP and RSTP. It groups the VLAN into instances, and constructs a spanning tree for each group.
This can be used to distribute load within the network routes.
This product supports **IEEE802.1s**.

Function Details

This product supports the following functions in order to flexibly handle the construction of routes based on MSTP.

- Setting priority
    - Set bridge priority
    - Set port priority
- Set path cost
- Set timeout
    - Set forward delay time
    - Set maximum aging time
- Specify edge port (Port Fast settings)
- BPDU guard
- BPDU filtering
- Route guard

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

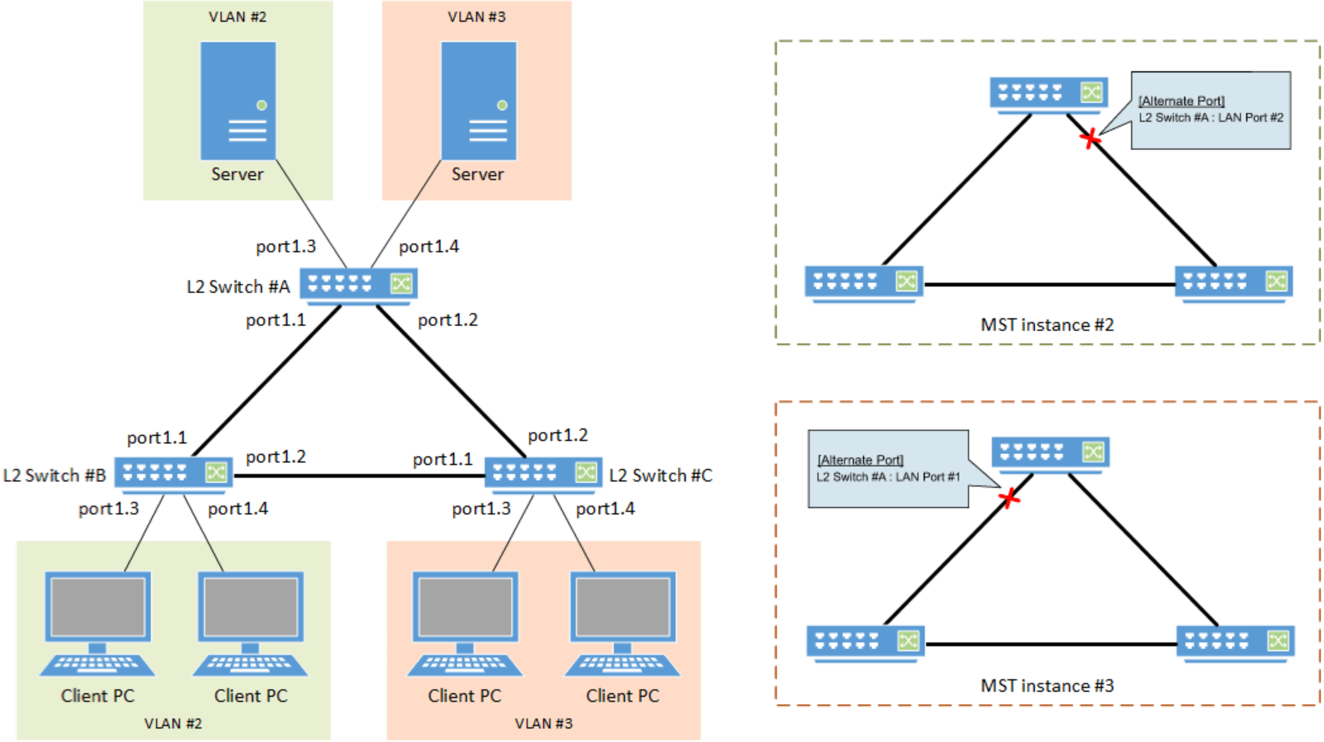
Operations	Operating commands
Set spanning tree for the system	spanning-tree shutdown
Set forward delay time	spanning-tree forward-time
Set maximum aging time	spanning-tree max-age
Set bridge priority	spanning-tree priority
Set spanning tree for an interface	spanning-tree
Set interface link type	spanning-tree link-type
Set interface BPDU filtering	spanning-tree bpdu-filter
Set interface BPDU guard	spanning-tree bpdu-guard
Set interface path cost	spanning-tree path-cost
Set interface priority	spanning-tree priority
Set edge port for interface	spanning-tree edgeport
Show spanning tree status	show spanning-tree
Show spanning tree BPDU statistics	show spanning-tree statistics
Clear protocol compatibility mode	clear spanning-tree detected protocols
Move to MST mode	spanning-tree mst configuration
Generate MST instance	instance
Set VLAN for MST instance	instance vlan
Set priority of MST instance	instance priority
Set MST region name	region
Set revision number of MST region	revision

Operations	Operating commands
Set MST instance for interface	spanning-tree instance
Set interface priority for MST instance	spanning-tree instance priority
Set interface path cost for MST instance	spanning-tree instance path-cost
Show MST region information	show spanning-tree mst config
Show MSTP information	show spanning-tree mst
Show MST instance information	show spanning-tree mst instance

Examples of Command Execution

MSTP setting example

Use this product to realize the architecture shown in the diagram below.



- In this example, MST instances are used to construct the spanning tree.
- A different route is set for each MST instance (VLAN), in order to distribute network load.
- The LAN port that is connected to the PC is set as the edge port.

■ Setting Procedure

1. [Switch #A] Define VLAN #2 and VLAN #3.

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 2 ①
Yamaha(config-vlan)#vlan 3 ②
Yamaha(config-vlan)#exit
```

① Define VLAN #2

② Define VLAN #3

2. [Switch #A] Set the CIST priority.

```
Yamaha(config)#spanning-tree priority 8192 ①
```

① Set CIST priority to 8192

3. [Switch #A] Set the MST.

```
Yamaha(config)#spanning-tree mst configuration
Yamaha(config-mst)#region Sample ①
Yamaha(config-mst)#revision 1 ②
Yamaha(config-mst)#instance 2 vlan 2 ③
Yamaha(config-mst)#instance 3 vlan 3 ④
Yamaha(config-mst)#exit
```

① Set the MST region name to “Sample”

② Set the MST revision number to 1

③ Define MST instance #2 and associate it with VLAN #2

④ Define MST instance #3 and associate it with VLAN #3

4. [Switch #A] Set LAN ports #1–#2 as trunk ports, and associate them with VLAN #2–#3.
Also, set the MST instances #2–#3.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#switchport mode trunk ①
Yamaha(config-if)#switchport trunk allowed vlan add 2,3 ②
Yamaha(config-if)#spanning-tree instance 2 ③
Yamaha(config-if)#spanning-tree instance 3 ④
Yamaha(config-if)#exit
(Also perform the above settings for LAN port #2.)
```

① Set the ports as trunk port

② Associate the ports with VLAN #2 and #3

③ Set MST instance #2

④ Set MST instance #3

5. [Switch #A] Set LAN port #3 as the access port, and associate it with VLAN #2.
Also, set the MST instance #2, and make it an edge port.

```
Yamaha(config)#interface port1.3
Yamaha(config-if)#switchport mode access ①
Yamaha(config-if)#switchport access vlan 2 ②
Yamaha(config-if)#spanning-tree instance 2 ③
Yamaha(config-if)#spanning-tree edgeport ④
Yamaha(config-if)#exit
```

① Set the port as access port

② Associate it with VLAN #2

③ Set MST instance #2

④ Set it as edge port

6. [Switch #A] Set LAN port #4 as the access port, and associate it with VLAN #3.
   Also, set the MST instance #3, and make it an edge port.

```
Yamaha(config)#interface port1.4
Yamaha(config-if)#switchport mode access ①
Yamaha(config-if)#switchport access vlan 3 ②
Yamaha(config-if)#spanning-tree instance 3 ③
Yamaha(config-if)#spanning-tree edgeport ④
Yamaha(config-if)#exit
```

① Set the port as access port

② Associate it with VLAN #3

③ Set MST instance #3

④ Set it as edge port

7. [Switch #B] Define VLAN #2 and VLAN #3.

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 2 ①
Yamaha(config-vlan)#vlan 3 ②
Yamaha(config-vlan)#exit
```

① Define VLAN #2

② Define VLAN #3

8. [Switch #B] Set the CIST priority.

```
Yamaha(config)#spanning-tree priority 16384 ①
```

① Set CIST priority to 16384

9. [Switch #B] Set the MST.

```
Yamaha(config)#spanning-tree mst configuration
Yamaha(config-mst)#region Sample ①
Yamaha(config-mst)#revision 1 ②
Yamaha(config-mst)#instance 2 vlan 2 ③
Yamaha(config-mst)#instance 2 priority 8192 ④
Yamaha(config-mst)#instance 3 vlan 3 ⑤
Yamaha(config-mst)#instance 3 priority 16384 ⑥
Yamaha(config-mst)#exit
```

① Set the MST region name to “Sample”

② Set the MST revision number to 1

③ Define MST instance #2 and associate it with VLAN #2

④ Set the priority of MST instance #2 to 8192

⑤ Define MST instance #3 and associate it with VLAN #3

⑥ Set the priority of MST instance #3 to 16384

10. [Switch #B] Set LAN ports #1−#2 as trunk ports, and associate them with VLAN #2−#3.

Also, set the MST instances #2–#3.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#switchport mode trunk ①
Yamaha(config-if)#switchport trunk allowed vlan add 2,3 ②
Yamaha(config-if)#spanning-tree instance 2 ③
Yamaha(config-if)#spanning-tree instance 3 ④
Yamaha(config-if)#exit
(Also perform the above settings for LAN port #2.)
```

① Set the ports as trunk port

② Associate the ports with VLAN #2 and #3

③ Set MST instance #2

④ Set MST instance #3

11. [Switch #B] Set LAN port #3 as the access port, and associate it with VLAN #2.
Also, set the MST instance #2, and make it an edge port.

```
Yamaha(config)#interface port1.3
Yamaha(config-if)#switchport mode access ①
Yamaha(config-if)#switchport access vlan 2 ②
Yamaha(config-if)#spanning-tree instance 2 ③
Yamaha(config-if)#spanning-tree edgeport ④
Yamaha(config-if)#exit
⑤
```

① Set the port as access port

② Associate it with VLAN #2

③ Set MST instance #2

④ Set it as edge port

⑤ Configure the settings above for LAN port #4 as well.

12. [Switch #C] Define VLAN #2 and VLAN #3.

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 2 ①
Yamaha(config-vlan)#vlan 3 ②
Yamaha(config-vlan)#exit
```

① Define VLAN #2

② Define VLAN #3

13. [Switch #C] Set the MST.

```
Yamaha(config)#spanning-tree mst configuration
Yamaha(config-mst)#region Sample ①
Yamaha(config-mst)#revision 1 ②
Yamaha(config-mst)#instance 2 vlan 2 ③
Yamaha(config-mst)#instance 2 priority 16384 ④
Yamaha(config-mst)#instance 3 vlan 3 ⑤
Yamaha(config-mst)#instance 3 priority 8192 ⑥
Yamaha(config-mst)#exit
```

① Set the MST region name to “Sample”

② Set the MST revision number to 1

③ Define MST instance #2 and associate it with VLAN #2

④ Set the priority of MST instance #2 to 16384

⑤ Define MST instance #3 and associate it with VLAN #3

⑥ Set the priority of MST instance #3 to 8192

14. [Switch #C] Set LAN ports #1–#2 as trunk ports, and associate them with VLAN #2–#3.
Also, set the MST instances #2–#3.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#switchport mode trunk ①
Yamaha(config-if)#switchport trunk allowed vlan add 2,3 ②
Yamaha(config-if)#spanning-tree instance 2 ③
Yamaha(config-if)#spanning-tree instance 3 ④
Yamaha(config-if)#exit
(Also perform the above settings for LAN port #2.)
```

① Set the ports as trunk port

② Associate the ports with VLAN #2 and #3

③ Set MST instance #2

④ Set MST instance #3

15. [Switch #C] Set LAN port #3 as the access port, and associate it with VLAN #3.
Also, set the MST instance #3, and make it an edge port.

```
Yamaha(config)#interface port1.3
Yamaha(config-if)#switchport mode access ①
Yamaha(config-if)#switchport access vlan 3 ②
Yamaha(config-if)#spanning-tree instance 3 ③
Yamaha(config-if)#spanning-tree edgeport ④
Yamaha(config-if)#exit
⑤
```

① Set the port as access port

② Associate it with VLAN #3

③ Set MST instance #3

④ Set it as edge port

⑤ Configure the settings above for LAN port #4 as well.

16. Connect the LAN cable.

17. [Switch #A] Check the CIST architecture.

```
Yamaha>show spanning-tree |include Root Id
% Default: CIST Root Id 200100a0deaeb920 ①
% Default: CIST Reg Root Id 200100a0deaeb920
```

```
Yamaha>show spanning-tree |include Role
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated - State
Forwarding
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Designated - State
Forwarding
%   port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State
Forwarding
%   port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State
Forwarding
%   port1.5: Port Number 909 - Ifindex 5005 - Port Id 0x838d - Role Disabled - State
Discarding
%   port1.6: Port Number 910 - Ifindex 5006 - Port Id 0x838e - Role Disabled - State
Discarding
%   port1.7: Port Number 911 - Ifindex 5007 - Port Id 0x838f - Role Disabled - State
Discarding
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Disabled - State
Discarding
%   port1.9: Port Number 913 - Ifindex 5009 - Port Id 0x8391 - Role Disabled - State
Discarding
%   port1.10: Port Number 914 - Ifindex 5010 - Port Id 0x8392 - Role Disabled - State
Discarding
```

① Switch #A with the higher priority becomes the root bridge of the CIST.

18. [Switch #B] Check the CIST architecture.

```
Yamaha>show spanning-tree |include Root Id
% Default: CIST Root Id 200100a0deaeb920 ①
% Default: CIST Reg Root Id 200100a0deaeb920

Yamaha>show spanning-tree |include Role
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State
Forwarding
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Designated - State
Forwarding
%   port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State
Forwarding
%   port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State
Forwarding
%   port1.5: Port Number 909 - Ifindex 5005 - Port Id 0x838d - Role Disabled - State
Discarding
%   port1.6: Port Number 910 - Ifindex 5006 - Port Id 0x838e - Role Disabled - State
Discarding
%   port1.7: Port Number 911 - Ifindex 5007 - Port Id 0x838f - Role Disabled - State
Discarding
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Disabled - State
Discarding
%   port1.9: Port Number 913 - Ifindex 5009 - Port Id 0x8391 - Role Disabled - State
Discarding
%   port1.10: Port Number 914 - Ifindex 5010 - Port Id 0x8392 - Role Disabled - State
Discarding
```

① Switch #A with the higher priority becomes the root bridge of the CIST.

19. [Switch #C] Check the CIST architecture.

```
Yamaha>show spanning-tree |include Root Id
% Default: CIST Root Id 200100a0deaeb920 ①
% Default: CIST Reg Root Id 200100a0deaeb920

Yamaha>show spanning-tree |include Role
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Alternate - State
Discarding ②
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Rootport - State
Forwarding
%   port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State
Forwarding
%   port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State
Forwarding
%   port1.5: Port Number 909 - Ifindex 5005 - Port Id 0x838d - Role Disabled - State
Discarding
%   port1.6: Port Number 910 - Ifindex 5006 - Port Id 0x838e - Role Disabled - State
Discarding
%   port1.7: Port Number 911 - Ifindex 5007 - Port Id 0x838f - Role Disabled - State
Discarding
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Disabled - State
Discarding
%   port1.9: Port Number 913 - Ifindex 5009 - Port Id 0x8391 - Role Disabled - State
Discarding
%   port1.10: Port Number 914 - Ifindex 5010 - Port Id 0x8392 - Role Disabled - State
Discarding
```

① Switch #A with the higher priority becomes the root bridge of the CIST.

② The LAN #1 port of Switch #C with the lower priority becomes the alternate port of the CIST.

20. [Switch #A] Check the architecture of MST instance #2.

```
Yamaha>show spanning-tree mst instance 2 |include Root Id
% Default: MSTI Root Id 200200a0deaeb879 ①

Yamaha>show spanning-tree mst instance 2 |include Role
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State
Forwarding
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Alternate - State
Discarding ②
%   port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State
Forwarding
```

① Switch #B with the higher priority becomes the root bridge of MST instance #2.

② The LAN #2 port of Switch #A with the lower priority becomes the alternate port of MST instance #2.

21. [Switch #B] Check the architecture of MST instance #2.

```
Yamaha>show spanning-tree mst instance 2 |include Root Id
% Default: MSTI Root Id 200200a0deaeb879 ①

Yamaha>show spanning-tree mst instance 2 |include Role
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated - State
Forwarding
```

```
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Designated - State
Forwarding
%   port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State
Forwarding
%   port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State
Forwarding
```

① Switch #B with the higher priority becomes the root bridge of MST instance #2.

22. [Switch #C] Check the architecture of MST instance #2.

```
Yamaha>show spanning-tree mst instance 2 |include Root Id
% Default: MSTI Root Id 200200a0deaeb879 ①

Yamaha>show spanning-tree mst instance 2 |include Role
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State
Forwarding
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Designated - State
Forwarding
```

① Switch #B with the higher priority becomes the root bridge of MST instance #2.

23. [Switch #A] Check the architecture of MST instance #3.

```
Yamaha>show spanning-tree mst instance 3 |include Root Id
% Default: MSTI Root Id 200300a0deaeb83d ①

Yamaha>show spanning-tree mst instance 3 |include Role
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Alternate - State
Discarding ②
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Rootport - State
Forwarding
%   port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State
Forwarding
```

① Switch #C with the higher priority becomes the root bridge of MST instance #3.

② The LAN #1 port of Switch #A with the lower priority becomes the alternate port of MST instance #3.

24. [Switch #B] Check the architecture of MST instance #3.

```
Yamaha>show spanning-tree mst instance 3 |include Root Id
% Default: MSTI Root Id 200300a0deaeb83d ①

Yamaha>show spanning-tree mst instance 3 |include Role
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated - State
Forwarding
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Rootport - State
Forwarding
```

① Switch #C with the higher priority becomes the root bridge of MST instance #3.

25. [Switch #C] Check the architecture of MST instance #3.

```
Yamaha>show spanning-tree mst instance 3 |include Root Id
% Default: MSTI Root Id 200300a0deaeb83d ①

Yamaha>show spanning-tree mst instance 3 |include Role
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated - State
Forwarding
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Designated - State
Forwarding
%   port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State
Forwarding
%   port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State
Forwarding
```

① Switch #C with the higher priority becomes the root bridge of MST instance #3.

Points of Caution

- **STP** and **RSTP** on this product are supported by **backward-compatibility provided by MSTP**.

Related Documentation

- Layer 2 Function: VLAN
- STP
  - IEEE802.1d
  - RFC4188
- RSTP
  - IEEE802.1w
  - RFC4318
- MSTP
  - IEEE802.1s

Unique Loop Detection

Function Overview

This product offers a proprietary system to detect whether there is a loop in the network environment that was configured.
This sends a proprietary loop detection frame from LAN/SFP ports and logical interfaces (hereinafter “loop detection-compatible interfaces”) to monitor whether that same frame returns or not.
If the transmitted frame returns, the system determines that there is a loop in the port in question.

Definition of Terms Used

LDF (Loop Detection Frame)

This is a Yamaha proprietary Ethernet frame that is used to detect loops.

Function Details

Loop detection operating specifications

The loop detection specifications for this product are shown below.

1. The loop detection functionality in this product can be enabled/disabled for the entire system or for specific loop detection-compatible interfaces.
   To activate loop detection at all loop detection-compatible interfaces, the loop detection function must be **enabled** for the entire system.
   - Use the **loop-detect** command in global configuration mode for the system-wide setting.
   - To activate loop detection at only specific loop detection-compatible interfaces, the **loop-detect** command must be used in the interface mode.
2. The default settings for the loop detection function are as shown below. (In the initial state, this function is not operating.)
   - System-wide setting: Disabled
   - Setting for loop detection-compatible interfaces: Enabled
3. If both loop detection and spanning tree protocol settings are set to **enabled** for the entire system, the spanning tree protocol is prioritized over the loop detection-compatible interface setting.
4. If the loop detection function is enabled for this product, the following operations are performed.
   - Loop detection frames (hereafter “LDF”) are sent **every two seconds** from linked-up loop detection-compatible interfaces.
     However, **the loop detection function is disabled** at ports with mirroring specified (mirror ports).
   - If an LDF sent from a port is received by that same port, a loop is determined to have occurred and the port that received the LDF performs the following actions.
     - **Port Shutdown**
       - If an LDF is sent and received at the same loop detection-compatible interface, the corresponding port is shut down.
       - The linkup will be made five minutes after shutdown, and LDF transmission will resume. (If a loop has occurred, this operation will repeat.)
       - When a linkup to the relevant port is desired within five minutes of monitored time, the **no shutdown** command is used.
     - **Port Blocking**
       - In any of the following cases, the port that received the LDF will block all non-LDF frames.

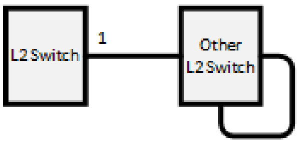
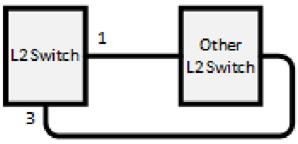
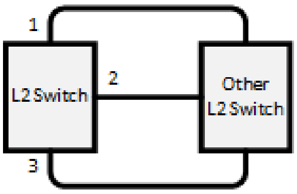
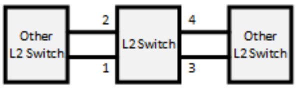
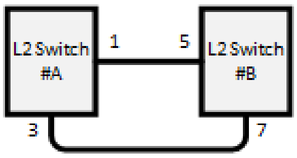
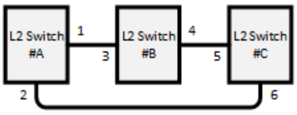
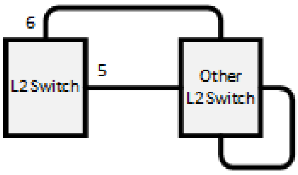
      - An LDF sent from a logical interface was received at a LAN/SFP port
      - An LDF sent from a static logical interface was received at an LACP logical interface
      - Sending or receiving interfaces are the same type and the interface with the higher number received an LDF
    - The LDF will be transmitted periodically, but LDF will not be forwarded from other devices.
    - If a blocked loop detection-compatible interface does not detect an LDF sent from itself for 5 seconds, then the loop is considered resolved and normal communications are resumed.
  - **Port Detected**
    - In any of the following cases, the port that received the LDF will continue normal communications because other ports are blocked.
      - An LDF sent from a LAN/SFP port was received at a logical interface
      - An LDF sent from an LACP logical interface was received at a static logical interface
      - Sending and receiving interfaces are the same type and the interface with the smaller number received an LDF
- When a loop is detected, the port lamp display on this product changes to a dedicated status, and the following SYSLOG message is output.
  - [LOOP]: inf: Detected Loop! : port1.1, 1.3 … , sa1,3 …, po1,3 <1>
- The port lamp display on this product is restored as communications are resumed after the loop is resolved, and the following SYSLOG message is output.
  - [LOOP]: inf: Recovered Loop! : port1.1, 1.3 … , sa1,3 …, po1,3 …

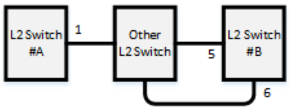
5. Shutdown and blocking actions at loop detection-compatible interfaces that have detected a loop can be overridden to perform “loop detected” actions.
   - Use the **loop-detect blocking disable** command for this setting.
   - If this setting is “enabled”, port blocking will be implemented on the next largest port number. (Shutdown operations will not occur.)
6. A force-clear can be performed on the loop detection status (detected, blocking) by using the **loop-detect reset** command. (On models equipped with a [MODE] button, this can be also done by holding down the [MODE] button for three seconds.)
   If a linkdown has occurred on the port where a loop has been detected, the detection status will be cleared. (The port lamp display is restored, and the following syslog message is outputted.)
7. The status of the loop detection function can be checked using the **show loop-detect** command. The following is displayed.
   - System Enable/disable status
   - Loop detection status display (status for a single loop detection-compatible interface)
8. When an LDF is received by a loop detection-compatible interface when the loop detection function is disabled, frames received from all other ports will be forwarded as-is.
   However, forwarding is disabled at ports with mirroring specified (mirror ports).
9. In the following kinds of situations, loops in hubs that are connected to this product might not be detected.
   - Loops are being detected in a connected hub
   - Loop detection frames are not being forwarded by a connected hub

Loop detection examples

The following shows examples of loop detection in this product.

- Loop detection examples

Loop detection case	Configuration example	Loop detection status
1		A loop is detected when a port receives the LDF that it has transmitted. port1.1: Shutdown
2		When loops are detected in multiple ports on the same terminal, the port with the largest number is blocked. port1.1: Detected port1.3: Blocking
3		The loop is avoided by blocking multiple ports. The blocking port is selected using the same rules as case 2. port1.1: Detected port1.2: Blocking port1.3: Blocking
4	 Other L2 Switch 2 1 L2 Switch 4 3 Other L2 Switch	When loops are detected in multiple groups, the port with the largest number in each group port1.1: Detected, port1.2: Blocking port1.3: Detected, port1.4: Blocking
5		When a loop occurs between two switches, one of the switches detects the loop. ○When detected in port1.3 of switch #A port1.1: Detected, port1.3: Blocking ○When detected in port1.7 of switch #B port1.5: Detected, port1.7: Blocking
6	 L2 Switch #A 1 3 L2 Switch #B 4 5 L2 Switch #C 2 6	Out of the six ports that are connected by cable, the port for which the loop is most quickly detected is the one that is blocked. ○When detected in port1.2 of switch #A port1.1: Detected, port1.2: Blocking + ○When detected in port1.4 of switch #B port1.3: Detected, port1.4: Blocking ○When detected in port1.6 of switch #C port1.5: Detected, port1.6: Blocking
7		Because the LDF transmitted from each port returns to these ports, port1.5 and port1.6 will both shut down. port1.5: Shutdown port1.6: Shutdown

Loop detection case	Configuration example	Loop detection status
8	 L2 Switch #A 1 Other L2 Switch 5 L2 Switch #B 6	Port1.6 of switch #B is blocked. Depending on the timing, port1.1 of switch #A will shut down; but the loop in port1.1 of switch #A is resolved by blocking port1.6 of switch #B. Switch #A port1.1: Shutdown Switch #B port1.5: Detected Switch #B port1.6: Blocking

Related Commands

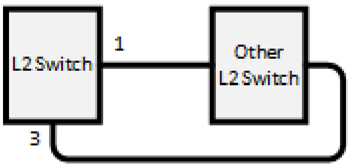
Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Enable/disable loop detection function (system)	loop-detect enable/disable
Enable/disable loop detection function (interface)	loop-detect enable/disable
Set port blocking for loop detection	loop-detect blocking enable/disable
Set port blocking duration time when a loop is detected	loop-detect blocking interval
Reset the loop detection status	loop-detect reset
Refer to the setting status of loop detection	show loop-detect

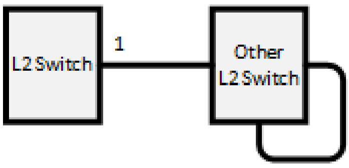
Examples of Command Execution

This example detects any loops occurring on this product using the following configuration, when the loop detection function is enabled.

- [Example 1] Loop occurring within this product



- [Example 2] Loop occurring in a third-party hub connected to this product



This sets LAN ports #1 and #3 to detect loops.

■ Setting Procedure

1. Enable the loop detection function for the entire system.

```
Yamaha(config)#loop-detect enable ①
```

① Enable the loop detection function for the entire system

2. Enable the loop detection function for LAN ports #1 and #3.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#spanning-tree disable ①
Yamaha(config-if)#loop-detect enable ②
Yamaha(config-if)#loop-detect blocking enable ③
(Also perform the above settings for LAN port #3.)
```

① Disable the spanning tree function for each LAN port

② Enable the loop detection function for each LAN port

③ Enables blocking

- The loop detection function for each LAN port and blocking are both enabled by default, so there is no need to set them.

3. Confirm that the loop detection function has been set.
   Confirm whether the loop detection function is enabled(*) for LAN ports #1 and #3.

```
Yamaha>show loop-detect
loop-detect: Enable

port      loop-detect    port-blocking           status
-------------------------------------------------------
port1.1        enable(*)        enable           Normal
port1.2        enable           enable           Normal
port1.3        enable(*)        enable           Normal
port1.4        enable           enable           Normal
port1.5        enable           enable           Normal
port1.6        enable           enable           Normal
port1.7        enable           enable           Normal
port1.8        enable           enable           Normal
port1.9        enable           enable           Normal
   :             :                :                :
-------------------------------------------------------
(*): Indicates that the feature is enabled.
```

4. If a loop has been detected, the loop detection status can be checked.

   - In the case of example 1:

```
Yamaha>show loop-detect
loop-detect: Enable

port      loop-detect    port-blocking           status
-------------------------------------------------------
port1.1        enable(*)        enable         Detected ①
port1.2        enable           enable           Normal
port1.3        enable(*)        enable         Blocking ②
port1.4        enable           enable           Normal
```

```
port1.5        enable           enable           Normal
port1.6        enable           enable           Normal
port1.7        enable           enable           Normal
port1.8        enable           enable           Normal
port1.9        enable           enable           Normal
   :             :                :                :
-------------------------------------------------------
(*): Indicates that the feature is enabled.
```

① LAN port #1 enters the detected status

② LAN port #3 enters the blocking status

- In the case of example 2:

```
Yamaha>show loop-detect
loop-detect: Enable

port      loop-detect    port-blocking          status
-------------------------------------------------------
port1.1        enable(*)        enable         Shutdown ①
port1.2        enable           enable           Normal
port1.3        enable(*)        enable           Normal
port1.4        enable           enable           Normal
port1.5        enable           enable           Normal
port1.6        enable           enable           Normal
port1.7        enable           enable           Normal
port1.8        enable           enable           Normal
port1.9        enable           enable           Normal
   :             :                :                :
-------------------------------------------------------
(*): Indicates that the feature is enabled.
```

① LAN port #1 goes into the shutdown state

Points of Caution

- All LAN/SFP ports included in the same logical interface must have the same loop detection setting (enabled, disabled, or blocked).
  - LAN/SFP ports with different loop detection settings cannot be included in the same logical interface.
  - Loop detection settings cannot be specified for LAN/SFP ports included in a logical interface.

Related Documentation

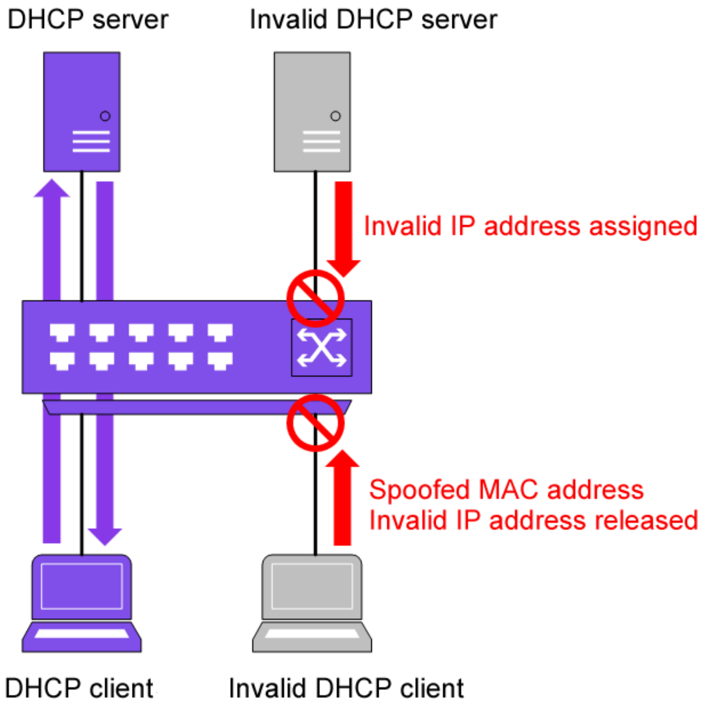
- Spanning Tree
- LED Control

DHCP Snooping

Function Overview

The DHCP snooping function monitors DHCP messages exchanged between the DHCP server and clients to filter out any invalid DHCP messages.
Using the function can be expected to improve security in the following ways.

- Deters assignment of IP addresses from invalid DHCP servers.
- Deters releasing IP addresses from invalid DHCP clients or detecting multiple IP addresses.
- Deters spoofed MAC addresses.
- Deters spoofed Option 82 actions.



Definition of Terms Used

Trusted port

Ports for which DHCP message filtering by DHCP snooping is disabled. It connects to a trusted DHCP server.

Untrusted port

Ports for which DHCP message filtering by DHCP snooping is enabled. It connects to DHCP clients.

IfIndex

Interface ID number. For IfIndex allocation, refer to Basic Interface Functions.

Function Details

Enabling DHCP snooping

To enable DHCP snooping, execute the **ip dhcp snooping enable** command in the global configuration mode. In addition, the **ip dhcp snooping enable** command must be executed in the interface mode for VLANs where DHCP snooping is to be enabled.

The status of system settings for the DHCP snooping function can be checked using the **show ip dhcp snooping** command.
The interface setting status for the DHCP snooping function can be checked using the **show ip dhcp snooping interface** command.

Binding database

If DHCP snooping is enabled, messages between the DHCP server and DHCP client can be monitored to build a binding database.
When the DHCP server assigns an IP address, the following DHCP client information is registered in the binding database.

- ID numbers of VLANs that received DHCP message from DHCP client
- Interface information for DHCP messages received from DHCP client
- DHCP client MAC address
- DHCP client IP address
- Lease time

Entry information for the binding database can be checked using the **show ip dhcp snooping binding** command.
Registered entry information is deleted when the entry lease time is finished or when a DHCP release message is received from the DHCP client.
The binding database can be cleared using the **clear ip dhcp snooping binding** command.
A maximum of **512** entries can be registered in the binding database.

DHCP snooping by port type

The **ip dhcp snooping trust** command can be used for DHCP snooping at two types of LAN/SFP ports, either “trusted” or “untrusted” ports.
Trusted ports connect to trusted DHCP servers, whereas untrusted ports connect DHCP clients.
The actions specified for each are described below.

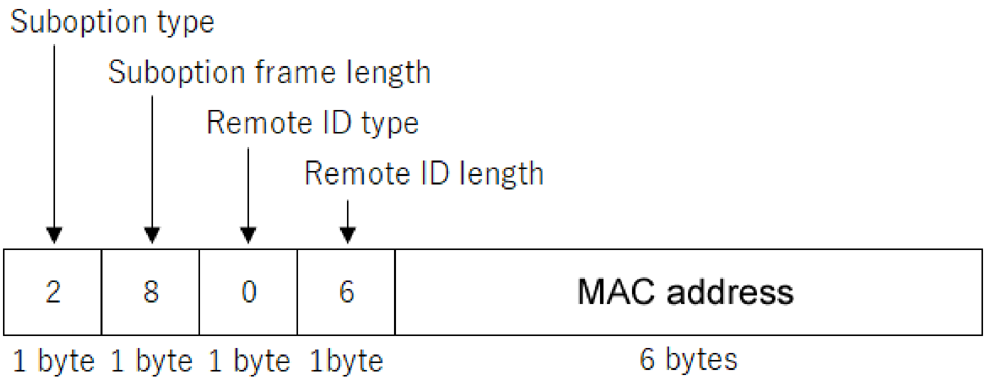
- Trusted port
    - DHCP messages are forwarded without filtering.
- Untrusted port
    - DHCP packets sent from a DHCP server are discarded.
    - If a MAC address is registered in the binding database and the following DHCP packets are received from a different interface than the registered interface, then the corresponding DHCP packets are discarded.
        - IP address release request (DHCP release)
        - Notification that a duplicate IP address was detected (DHCP decline)
    - If MAC address verification is enabled, the MAC address of the DHCP packet sender is compared to the client hardware address (chaddr). If the addresses do not match, then the corresponding DHCP packets are discarded.
    - If Option 82 is enabled and DHCP packets received from a DHCP client are already appended with Option 82 information, then the corresponding DHCP packets are discarded.

At untrusted ports, MAC address verification is **enabled** by default, but can be disabled using the **ip dhcp snooping verify mac-address** command.
If a DHCP agent needs to be connected to an untrusted port, MAC address verification must be disabled because the DHCP agent will overwrite the MAC address of DHCP clients sending DHCP packets.

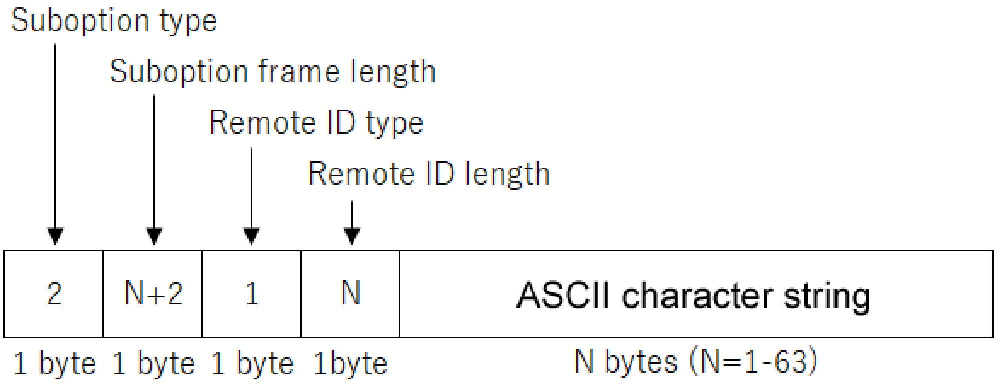
Option 82

If Option 82 is enabled when DHCP snooping is enabled, then Option 82 information is appended to DHCP packets received from DHCP clients at untrusted ports.
If a DHCP client is connected directly to an untrusted port, Option 82 information is deleted from return packets sent from the DHCP server to the DHCP client before forwarding.
Option 82 is **enabled** by default. The following Option 82 information is appended to packets.

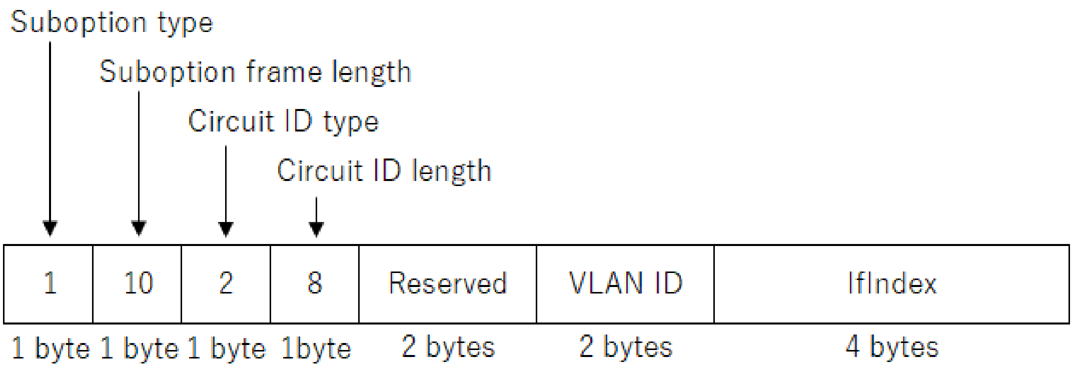
- Remote-ID
    - With default settings, packets are appended with the MAC address for the given unit.
        - Format: Suboption type=2, Remote-ID type=0 (Default)



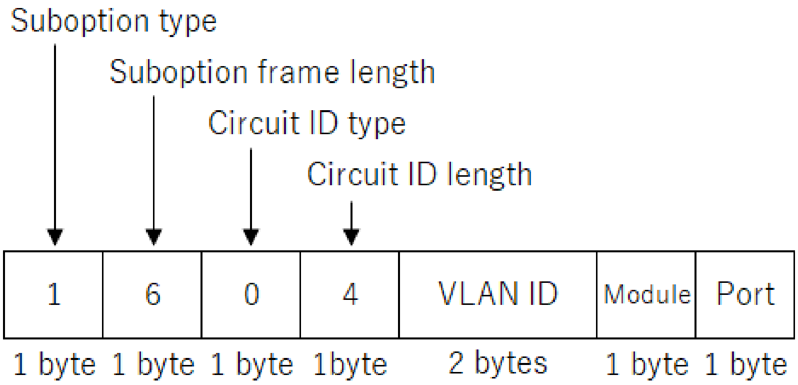
-
    - The **ip dhcp snooping information option format remote-id** command can be used to append Remote-ID values with any string (single-byte characters or symbols) up to 63 characters long.
        - Format: Suboption type=2, Remote-ID type=1



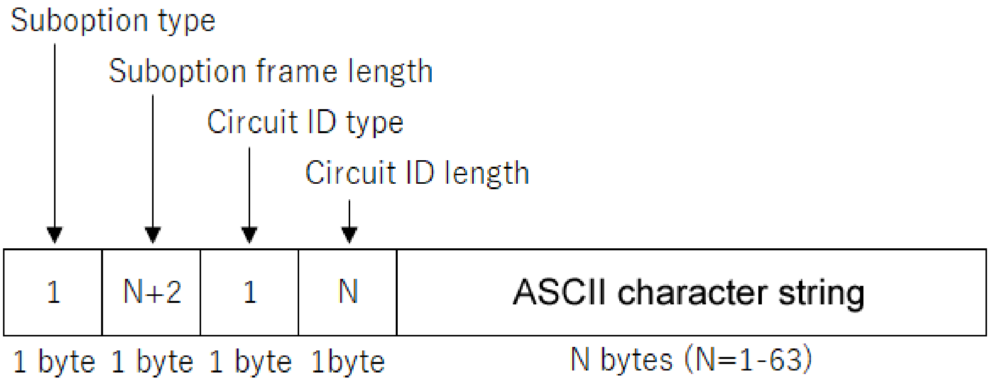
- Circuit-ID
    - With default settings, DHCP packets received from DHCP clients are appended with VLAN ID and IfIndex information.
        - Format: Suboption type=1, Circuit-ID type=2 (Default)



  - The **ip dhcp snooping information option format-type circuit-id** command can be used to change circuit-ID information to VLAN ID and port number information for DHCP packets received from DHCP clients. For physical ports, “Module” values are appended with the stack number or with a “1” setting for standalone or non-stack-compatible models. For logical ports, fixed static “0x11” and LACP “0x12” settings are specified.
    “Port” values are appended with the physical port number.
    - Format: Suboption type=1, Circuit-ID type=0



  - Any character string (single-byte characters or symbols) up to 63 characters long can also be specified for Circuit-ID values.
    - Format: Suboption type=1, Circuit-ID type=1



- Subscriber-ID
  - Not appended with default settings.
  - The **ip dhcp snooping subscriber-id** command can be used to specify any string (single-byte characters or symbols) up to 50 characters long for subscriber-ID values at applicable ports and include the string in Option 82 information.

If Option 82 is enabled and a DHCP packet already appended with Option 82 information is received at an

untrusted port, that packet is discarded to deter spoofing of Option 82 information.
In order to connect a DHCP relay agent appended with Option 82 to an untrusted port, the **ip dhcp snooping information option allow-untrusted** command must be executed to allow forwarding DHCP packets that include Option 82 at untrusted ports.

DHCP packet rate limits

If DHCP snooping is enabled, the **ip dhcp snooping limit rate** command can be used to specify the maximum number of DHCP packets that can be received per second by the overall system.
If more than the maximum DHCP packets allowed by the limit rate are received, all DHCP packets that exceed the limit rate are discarded. A limit rate is not specified in default settings.

DHCP snooping statistical information

Statistics about DHCP packets discarded by DHCP snooping can be checked using the **show ip dhcp snooping statistics** command.
However, that statistical information does not include statistics on DHCP packets discarded due to the limit rate.
The statistical information can be deleted using the **clear ip dhcp snooping statistics** command.

SYSLOG output

If DHCP packets are discarded due to a DHCP snooping inspection of DHCP packets received, the reason for discarding the packets can be included in INFO level SYSLOG output.
The SYSLOG output enable/disable setting can be specified using the **ip dhcp snooping logging** command.
SYSLOG output is enabled in default settings.
The following SYSLOG messages are output.

Level	Output conditions	SYSLOG Message
INFO	DHCP server packet received at untrusted port.	2022/07/21 09:00:00: [DHCPSN]:inf: DHCP dropped due to prohibited message type, VLAN 1, port1.1, DHCPOFFER, 1234.4567.abcd
INFO	DHCP RELEASE/DECLINE request was received from an unregistered interface.	2022/07/21 09:00:00: [DHCPSN]:inf: DHCP dropped due to source interface mismatch, VLAN 1, port1.1, DHCPRELEASE, 5c5a.c7d6.9e1e
INFO	Sender MAC and chaddr information do not match.	2022/07/21 09:00:00: [DHCPSN]:inf: DHCP dropped due to source mac mismatch, VLAN 1, port1.1, DHCPINFORM, 001c.4321.abcd
INFO	Packet appended with Option 82 was received at untrusted port.	2022/07/21 09:00:00: [DHCPSN]:inf: DHCP dropped due to option82 value, VLAN 1, port1.1, DHCPINFORM, 5c5a.c7d6.9e1e

Related Commands

Related commands are indicated below.

Operations	Operating commands
Enable/disable setting for DHCP snooping (system)	ip dhcp snooping enable/disable
Enable/disable setting for DHCP snooping (VLAN)	ip dhcp snooping enable/disable
DHCP snooping port type setting	ip dhcp snooping trust
Enable/disable setting for MAC address verification	ip dhcp snooping verify mac-address enable/disable

Operations	Operating commands
Enable/disable setting for Option 82	ip dhcp snooping information option enable/disable
Setting for allowing packets appended with Option 82 to be received at untrusted ports	ip dhcp snooping information option allow-untrusted
Remote-ID setting for Option 82	ip dhcp snooping information option format remote-id
Circuit-ID setting for Option 82	ip dhcp snooping information option format-type circuit-id
Subscriber-ID setting	ip dhcp snooping subscriber-id
DHCP packet receiving limit rate setting	ip dhcp snooping limit rate
Enable/disable setting for SYSLOG output when DHCP packets are discarded	ip dhcp snooping logging enable/disable
Shows DHCP snooping system setting information	show ip dhcp snooping
Shows DHCP snooping interface settings information	show ip dhcp snooping interface
Display Binding Database	show ip dhcp snooping binding
Shows DHCP snooping statistical information	show ip dhcp snooping statistics
Clears binding database	clear ip dhcp snooping binding
Clears DHCP snooping statistical information	clear ip dhcp snooping statistics

Examples of Command Execution

Designating trusted interfaces

This specifies trusted interfaces (LAN port #1) for connecting DHCP servers.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#ip dhcp snooping trust
Yamaha(config-if)#exit
```

Enabling DHCP snooping

This enables DHCP snooping for the system and VLAN #1.

```
Yamaha(config)#ip dhcp snooping enable
Yamaha(config)#interface vlan1
Yamaha(config-if)#ip dhcp snooping enable
Yamaha(config-if)#exit
```

Points of Caution

- None

Layer 3 Functions

IPv4/IPv6 Common Settings

Function Overview

This product is compatible with the following **network environment settings that are common to IPv4 and IPv6**, mainly for the purpose of maintenance (configuring the settings of the switch).

1. DNS client settings
2. Equal cost multipath settings

Definition of Terms Used

None

Function Details

DNS client settings

This product supports **DNS (Domain Name System) clients**.
If an **FQDN (Fully Qualified Domain Name)** has been set for an NTP server or a syslog server, an inquiry is made to the DNS server to retrieve the IPv4/IPv6 address.

This product provides the following DNS client control functions.

- Set IP address of the DNS server
- Set default domain name
- Set search domain list

Inquiries to the DNS server are **enabled** by default, and the setting can be changed by using the **dns-client enable/disable** command.

Set IP address of the DNS server

Up to three IP addresses can be set for the DNS server, using the methods shown below.

- Manual setting using the **dns-client name-server** command
    - This lets you specify the IPv4/IPv6 address.
- Automatic setting via DHCP
    - The highest default gateway value takes priority if there is more than one.
- Automatic setting via DHCPv6
    - If specifying multiple settings, the most recent is prioritized.
    - Link local addresses notified by DHCPv6 cannot be specified.
- If both DHCP and DHCPv6 are used, both settings will be overwritten when DNS server addresses are obtained.

This product **always gives priority to the information that was set via commands**.
Check the configured DNS servers by using the **show dns-client** command.

Set default domain name

Only one default domain can be set using the methods shown below. The domain can be specified using up to **256 characters**.

- Manual setting using the **dns-client domain-name** command
- Automatic setting via DHCP
  - The highest default gateway value takes priority if there is more than one.

Just as with DNS server IP addresses, this product **prioritizes information specified with commands**.
Check the default domain that was set by using the **show dns-client** command.
The use of a default domain is only allowed if there are no listings in the search domain list.

Set search domain list

This product uses a search domain list to manage the domain names used when inquiring with the DNS.
Up to six domain names can be set on the search domain list using the method below.

- Manual setting using the **dns-client domain-list** command
- Automatic setting via DHCPv6
  - If specifying multiple settings, the most recent is prioritized.

Just as with DNS server IP addresses, this product **prioritizes information specified with commands**.
The search domain list that has been set can be checked using the **show dns-client** command.
The search domain list **must be within 256 characters total for all domain names registered**.

Equal cost multipath settings

This product supports **equal-cost multi-path** settings using the following functions.

- IPv4 static routing
- IPv6 static routing
- RIPv1, RIPv2, RIPng (only on compatible models)
- OSPFv2, OSPFv3 (only on compatible models)

If multiple routes to the same destination are registered in the RIB, these multiple routes will be reflected in the FIB.
Up to eight routes leading to the same destination can be registered in the FIB. The default setting is **four routes**.
The number of equal-cost multi-paths that can be registered may be changed using the **maximum-paths** command.
The changes to the settings will not be reflected in actual operations until rebooting.

Use the **port-channel load-balance** command to configure the load balance rules for equal-cost multi-path destinations.
Caution must be used when changing the load balance rule settings using the **port-channel load-balance** command, as this has an impact on how link aggregation works.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Function types	Operations	Operating commands
DNS client settings	DNS client settings	dns-client enable/disable
	Set DNS server address	dns-client name-server
	Set default domain name	dns-client domain-name
	Set search domain list	dns-client domain-list
	Show DNS client settings	show dns-client
Equal cost multipath settings	Set the number of equal-cost multi-paths that can be registered	maximum-paths
	Display the number of equal-cost multi-paths that can be registered	show ip route summary
		show ipv6 route summary
	Set load balance function rules	port-channel load-balance

Examples of Command Execution

DNS client settings

Set DNS client settings for this product to prepare an environment for DNS queries.

- Specify 192.168.100.1 and 192.168.100.2 as the IP addresses of the servers for DNS queries.
- Specify example.com as the default domain used for DNS queries.

■ Setting Procedure

1. Enable the DNS query functionality.

   ```
   Yamaha(config)#dns-client enable
   ```

   - Since this is specified as the default value, we do not need to set this specifically.

2. Specify the DNS servers.

   ```
   Yamaha(config)#dns-client name-server 192.168.100.1
   Yamaha(config)#dns-client name-server 192.168.100.2
   ```

3. Set the default domain.

   ```
   Yamaha(config)#dns-client domain-name example.com
   ```

4. Check the DNS client information that was set.

   ```
   Yamaha#show dns-client
   ```

```
DNS client is enabled
 Default domain  : example.com
 Domain list     :
 Name Servers    : 192.168.100.1 192.168.100.2

 * - Values assigned by DHCP or DHCPv6 Client.
```

Equal-cost multi-paths

This changes the number of equal-cost multi-paths that can be registered to “5”.
Also, the source and destination IP addresses are used as load balance rules.

1. Set the number of equal-cost multi-paths that can be registered

   ```
   Yamaha(config)#maximum-paths 5
   % System Reboot is required for new Maximum-Path value to take effect.
   ```

   - A reboot is required to apply the settings.

2. Set the source and destination IP addresses as load balance rules.

   ```
   Yamaha(config)#port-channel load-balance src-dst-ip
   ```

3. Check the current number of equal-cost multi-paths that can be registered.

   ```
   Yamaha(config)#show ip route summary
   IP routing table name is Default-IP-Routing-Table(0)
   IP routing table maximum-paths   : 5
   Route Source    Networks
   connected       3
   rip             2
   Total           5
   ```

Points of Caution

None

Related Documentation

None

Basic IPv4 Settings

Function Overview

This product is compatible with the following **IPv4 network environment settings**, mainly for the purpose of maintenance (configuring the settings of the switch).

1. IPv4 address settings
2. Route information settings
3. ARP table settings
4. MTU settings

Definition of Terms Used

IPv4 Link Local Address

This is an address that is only valid within the same segment, within the range of **169.254.0.0/16 to 169.254.255.255/16**.

Function Details

IPv4 address settings

This product lets you specify the **IPv4 address and subnet mask** for a **VLAN interface**.
As the setting method, both **fixed settings** and **automatic settings via DHCP** are supported.

- To set the fixed/automatic IPv4 address, use the **ip address** command.
- The following actions occur if addresses are specified automatically by DHCP.
  - The HostName option (option code 12) can be added to the Discover/Request message.
  - The lease time requested to the DHCP server is **fixed at 72 hours**. (The actual lease time will depend on the setting of the DHCP server.)
  - If the **no ip address** command is executed with automatic settings, a release message for the IPv4 address obtained is sent to the DHCP server.
  - The information obtained from the DHCP server can be checked using the **show dhcp lease**.
- For IPv4 addresses, **1 primary address** and **4 secondary addresses** can be specified **per VLAN interface**.
  A **maximum of 8** IPv4 addresses can be specified for the **entire system**.
  The IPv4 address that is allocated to a VLAN interface can be checked using the **show ip interface** command.
- In the initial state, **192.168.100.240/24** is fixed for the **default VLAN (VLAN #1)**.

Auto IP function

As part of the IPv4 address setting functionality, this product provides an auto IP function which automatically generates IPv4 link local addresses based on the MAC address.
The auto IP function only works when an IPv4 address has not been allocated from the DHCP server. (The IPv4 address must be set to “DHCP” as a prerequisite.)
This function confirms whether the automatically-generated IPv4 link local address does not already exist on the network via ARP.
If it has been confirmed that the address does not already exist, the generated address will start to be used.
If the IPv4 address was allocated from the DHCP server after the IPv4 link local address was determined via auto IP, the IPv4 link local address is discarded, and the IP address obtained from the DHCP server is used.

- To enable the Auto IP function, use the **auto-ip enable** command.
- The Auto IP function can be enabled **for only one VLAN interface**. In the initial state, the **default VLAN (VLAN #1)** is enabled.

Route information settings

This product refers to a routing table when sending syslog messages and when sending out voluntary IPv4 packets as an IPv4 host for NTP-based time adjustments and so on.
This product uses the following functions to perform the routing table operations.

- Set VLAN interface route information
- Set default gateway
- Set static route information
- Show route information

Route information for VLAN interfaces

When an IPv4 address is set for a VLAN interface, this product automatically sets the correspondence between the network address and VLAN ID as route information.
When releasing IPv4 addresses set for the VLAN interface, the above settings will be deleted.

Set default gateway

The destination for IPv4 packets sent to network addresses that are not set in the routing table can be set as the default gateway on this product.

- To set the default gateway, use the **ip route** command.
- To show the default gateway, use the **show ip route** command.

Set static route information

A static route to the destination network address (the gateway address to which packets will be sent) can be set on this product.

- Static route information is set using the **ip route** command.
- Static route information is displayed using the **show ip route** command.

Routing table and route selection

You will use the following two types of table to specify routing information.

- RIB (Routing Information Base: IP routing table)
- FIB (Forwarding Information Base: IP forwarding table)

The roles of each are explained below.

- **RIB**
  RIB (Routing Information Base: IP routing table) is a database that stores various routing information.
  - A route is registered in the RIB in the following cases.
    - When an IPv4 address is assigned to a VLAN interface
    - When a static route or a default gateway are specified manually
    - When a default gateway is learned via a DHCP message
  - To check the RIB, use the **show ip route database** command.

- **FIB**
  FIB (Forwarding Information Base: IP forwarding table) is a database that is referenced when deciding how to forward IP packets.
  Of the routes that are registered in the RIB, the FIB registers only the route that is determined to be “optimal” and is actually used for forwarding packets.
    - The conditions by which a route is determined to be optimal are as follows.
        - The corresponding VLAN interface is in the link up state
        - If multiple routes to the same destination are registered in the RIB, only one is decided in the following order of priority
            1. A manually specified route takes priority over a route learned via a DHCP message.
            2. A route whose gateway has a higher IP address value takes priority
    - To check the FIB, use the **show ip route** command.

ARP table settings

When sending IPv4 packets, this product uses ARP (Address Resolution Protocol) to obtain the MAC addresses from the IPv4 addresses.
The correspondence between IPv4 address and MAC address is saved in the ARP table with the following specifications.

- The **ARP entries** saved in the ARP table manage the following information.
    - IPv4 address
    - MAC address
    - VLAN interface
- **Up to 508 entries** are stored in the ARP table, including dynamic and static entries.
- With the default settings, dynamic entries saved in the ARP table are maintained for **300 sec**.
  The entry timeout value can be changed using the **arp-ageing-timeout** command.
- Dynamic entries saved in the ARP table can be cleared regardless of the timeout value, by using the **clear arp-cache** command.
- Settings for the static entries in the ARP table are made using the **arp** command. Up to 255 items can be registered.
- Use the **show arp** command to check the ARP table.

MTU settings

This product enables MTU values to be specified for **VLAN interfaces**.

- Use the **mtu** command to set MTU values.
- The default MTU value is **1500 bytes**, but setting values ranging from **68 bytes** to **9216 bytes** can be specified.
  However, the setting range for VLAN interfaces with “ipv6 enable” specified is from **1280 bytes** to **9216 bytes**.
- A maximum of seven MTU values, besides the default value, can be specified.
- To route received packets, use the following steps.
    - If the IPv4 header “Total Length” field value for IPv4 packets exceeds the MTU value, then packets are forwarded divided into parts (IP fragments).
      IPv4 packets appended with a DF (don’t fragment) bit are discarded without being divided into IP fragments and an ICMP error (fragmentation needed) is returned.
    - If the IPv6 header “Payload Length” field value for IPv6 packets exceeds the MTU value, then an ICMPv6 error (packet too big) is returned and the packet is discarded.

- Packets larger than the maximum receivable frame size specified by the **mru** command are not routed. To forward extra large frames, use the **mru** command to adjust the maximum receivable frame size setting as necessary.
- *If divided (IP fragmentation) for forwarding, then software is used for forwarding, which limits the forwarding speed and also dramatically increases the CPU usage rate. *
  It is recommended that the mtu command be used to set a frame size large enough to forward extra-large frames without dividing them (IP fragmentation).

- This product forwards packets according to the following steps.
  - If the IPv4/IPv6 packet size sent is larger than the MTU value for the VLAN interface where packets are being sent, then packets are divided (IP fragmentation) based on the MTU value.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Function types	Operations	Operating commands
IPv4 address settings	IPv4 address settings	ip address
	Show IPv4 address	show ip interface
	Set dynamic IPv4 address by DHCP client	ip address dhcp
	Show DHCP client status	show dhcp lease
	Enable/disable Auto IP function	auto-ip enable/disable
Route information settings	Set default gateway	ip route
	Show default gateway	show ip route
	Set static route information	ip route
	Show static route information	show ip route
	Show route information	show ip route
ARP table settings	Show ARP table	show arp
	Set the dynamic entry hold time	arp-ageing-timeout
	Clear dynamic entries	clear arp-cache
	Set static entry	arp
MTU settings	MTU settings	mtu

Examples of Command Execution

IPv4 network environment settings (DHCP)

In this example, the IPv4 addresses are set on this product, and an environment is set up for accessing the unit from a remote terminal.

- Maintenance for this product is done using the default VLAN (VLAN #1).
- The IPv4 address is set automatically by **DHCP** for the default VLAN (VLAN #1).
- **Web/TFTP access permission** is given from a host connected to VLAN #1.

1. Check the IPv4 address that is currently set.
   If the default settings are still in effect, the fixed IPv4 address (192.168.100.240/24) is set.

```
Yamaha#show ip interface brief
Interface            IP-Address                Status                Protocol
vlan1                192.168.100.240/24        up                    up
```

2. Specify DHCP for the default VLAN (VLAN #1).

```
Yamaha#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Yamaha(config)#interface vlan1
Yamaha(config-if)#ip address dhcp
```

3. Check the information that was provided by the DHCP server.

```
Yamaha(config-if)#end
Yamaha#show dhcp lease
Interface vlan1
--------------------------------------------------------------------------------
IP Address:                  192.168.1.3
Expires:                     YYYY/MM/DD 05:08:41
Renew:                       YYYY/MM/DD 19:08:41
Rebind:                      YYYY/MM/DD 02:38:41
Server:
Options:
  subnet-mask                255.255.255.0
  default-gateway            192.168.1.1
  dhcp-lease-time            72000
  domain-name-servers        192.168.1.1
  dhcp-server-identifier     192.168.1.1
  domain-name                xxx.xxxxx.xx.xx
```

4. Set the default VLAN (VLAN #1) to permit access from HTTP servers and TFTP servers.
   Access using a remote host over the Web after settings are made.

```
Yamaha(config)#http-server interface vlan1 ①
Yamaha(config)#tftp-server interface vlan1 ②
```

① HTTP server access permission

② TFTP server access permission

Points of Caution

None

Related Documentation

- Layer 2 Function: VLAN
- Maintenance and Operation Functions: Remote Access Control

- Yamaha RTpro: What is ARP?

Basic IPv6 Settings

Function Overview

This product is compatible with the following **IPv6 network environment settings**, mainly for the purpose of maintenance (configuring the switch settings).

1. IPv6 address settings
2. Route information settings
3. Neighbor cache table settings
4. MTU settings
5. DHCPv6-PD client settings

Definition of Terms Used

RA (Router Advertisement)

This is a system that automatically sets address information and network settings on the IPv6 network for devices of the network that is associated with a router.

IPv6 address

The IPv6 address is 128 bits expressed as hexadecimal. The address is divided into eight fields delimited by ":" with 16 bits in each field.

- **2001:02f8:0000:0000:1111:2222:0000:4444**

The expression can be abbreviated according to the following rules.

- If the beginning of a field is a zero, the zero can be omitted.
- A field that consists of four zeros can be abbreviated as a single zero.
- Multiple fields consisting only of consecutive zeros can be abbreviated as "::" **in only one location for the entire address**.

Applying these rules to the above address, we get the following.

- **2001:2f8::1111:2222:0:4444**

IPv6 link-local address

This is an address that is only valid within the same segment, and is in the following range.

- [Start] **FE80:0000:0000:0000:0000:0000:0000:0000**
- [End] **FE80:0000:0000:0000:FFFF:FFFF:FFFF:FFFF**

Function Details

IPv6 address settings

This product lets you specify the **IPv6 address and prefix length** for a **VLAN interface**.
The setting method supports either **fixed settings**, **setting addresses automatically via RAs (router advertisement)**, or **setting addresses automatically by DHCPv6**.

- In order to specify an IPv6 address, IPv6 functionality must be enabled for the corresponding VLAN interface.

  - To enable IPv6 functionality, use the **ipv6 enable** command.
  - When IPv6 functionality is enabled, an IPv6 link local address is automatically assigned.
- To set a fixed/automatic IPv6 address, use the **ipv6 address** command.
- The following actions occur if addresses are specified automatically by DHCPv6.
  - Executing the **ipv6 address dhcp** command enables the DHCPv6 stateful actions (IA_NA).
  - If the **no ipv6 address dhcp** command is executed with addresses specified automatically, a message is sent to the DHCPv6 server indicating that the IPv6 addresses acquired were released.
  - The information obtained from the DHCPv6 server is checked using the **show ipv6 dhcp interface** command.
- Specifying **stateless** as the parameter for the **ipv6 address autoconfig** command used to specify addresses automatically by RA (router advertisements) enables DHCPv6 stateless actions.
- For IPv6 addresses, **up to 5 global addresses (including automatically specified addresses and IPv6 addresses specified by a DHCPv6 client or using DHCPv6-PD)** and **1 link local address** can be specified **per VLAN interface**.
  A **maximum of 8** IPv6 addresses can be specified for the **entire system**.
  The IPv6 address that is allocated to a VLAN interface can be checked using the **show ipv6 interface** command.

Route information settings

This product refers to a routing table when sending syslog messages and when sending out voluntary IPv6 packets as an IPv6 host for NTP-based time adjustments and so on.
This product uses the following functions to perform the routing table operations.

- Set VLAN interface route information
- Set default gateway
- Set static route information
- Show route information

Route information for VLAN interfaces

When setting an IPv6 address on this product for a VLAN interface, the correspondence between the network address and VLAN ID is automatically set as route information.
When releasing IPv6 addresses set for the VLAN interface, the above settings will be deleted.

Set default gateway

The destination for IPv6 packets sent to network addresses that are not set in the routing table can be set as the default gateway on this product.

- To set the default gateway, use the **ipv6 route** command.
- To show the default gateway, use the **show ipv6 route** command.
- When **ipv6 address dhcp**, **ipv6 dhcp client pd**, or **ipv6 address autoconfig** commands are specified, device addresses to which RAs were sent are automatically added to the default gateway.
  - Automatic default gateway registration by RAs can be enabled/disabled using the **ipv6 nd accept-ra-default-routes** command.

Set static route information

A static route to the destination network address (the gateway address to which packets will be sent) can be set on this product.

- Static route information is set using the **ipv6 route** command.
- Static route information is displayed using the **show ipv6 route** command.

Routing table and route selection

You will use the following two types of table to specify routing information.

- RIB (Routing Information Base: IP routing table)
- FIB (Forwarding Information Base: IP forwarding table)

The roles of each are explained below.

- **RIB**
  RIB (Routing Information Base: IP routing table) is a database that stores various routing information.
    - A route is registered in the RIB in the following cases.
        - When an IPv6 address is assigned to a VLAN interface
        - When a static route or a default gateway are specified manually
    - To check the RIB, use the **show ipv6 route database** command.
- **FIB**
  FIB (Forwarding Information Base: IP forwarding table) is a database that is referenced when deciding how to forward IP packets.
  Of the routes that are registered in the RIB, the FIB registers only the route that is determined to be "optimal" and is actually used for forwarding packets.
    - The conditions by which a route is determined to be optimal are as follows.
        - The corresponding VLAN interface is in the link up state
        - If multiple routes to the same destination are registered in the RIB, only one is decided in the following order of priority
            1. A route whose gateway has a higher IP address value takes priority
    - To check the FIB, use the **show ipv6 route** command.

Neighbor cache table settings

When sending IPv6 packets, this product uses Neighbor Discovery Protocol to obtain the MAC addresses from the IPv6 addresses.
The correspondence between IPv6 address and MAC address is saved in the neighbor cache table with the following specifications.

- The **neighbor cache entries** saved in the neighbor cache table manage the following information.
    - IPv6 address
    - MAC address
    - VLAN interface
- **Up to 128 entries** are stored in the neighbor cache table, including dynamic and static entries.
- Dynamic entries saved in the neighbor cache table can be cleared by using the **clear ipv6 neighbors** command.
- Settings for the static entries in the neighbor cache table are made using the **ipv6 neighbor** command. Up to 63 items can be registered.
- Use the **show ipv6 neighbor** command to check the neighbor cache table.

MTU settings

This product enables MTU values to be specified for **VLAN interfaces**.

- Use the **mtu** command to set MTU values.
- The default MTU value is **1500 bytes**, but setting values ranging from **68 bytes** to **9216 bytes** can be specified.
  However, the setting range for VLAN interfaces with “ipv6 enable” specified is from **1280 bytes** to **9216 bytes**.
- A maximum of seven MTU values, besides the default value, can be specified.
- To route received packets, use the following steps.
  - If the IPv4 header “Total Length” field value for IPv4 packets exceeds the MTU value, then packets are forwarded divided into parts (IP fragments).
    IPv4 packets appended with a DF (don’t fragment) bit are discarded without being divided into IP fragments and an ICMP error (fragmentation needed) is returned.
  - If the IPv6 header “Payload Length” field value for IPv6 packets exceeds the MTU value, then an ICMPv6 error (packet too big) is returned and the packet is discarded.
  - Packets larger than the maximum receivable frame size specified by the **mru** command are not routed. To forward extra large frames, use the **mru** command to adjust the maximum receivable frame size setting as necessary.
  - *If divided (IP fragmentation) for forwarding, then software is used for forwarding, which limits the forwarding speed and also dramatically increases the CPU usage rate. *
    It is recommended that the mtu command be used to set a frame size large enough to forward extra-large frames without dividing them (IP fragmentation).
- This product forwards packets according to the following steps.
  - If the IPv4/IPv6 packet size sent is larger than the MTU value for the VLAN interface where packets are being sent, then packets are divided (IP fragmentation) based on the MTU value.

DHCPv6-PD client settings

This product enables DHCPv6-PD clients to be specified for **VLAN interfaces**.
Prefixes can be obtained from a DHCPv6-PD server for specifying addresses or reassigning the user’s own DHCPv6 server.

- Executing the **ipv6 dhcp client pd** and **prefixname** commands will enable DHCPv6-PD stateful actions (IA_PD).
- Prefixes obtained with the **prefixname** command can be used for the following.
  - Using the **ipv6 address pd** command to specify IPv6 addresses using the prefixes obtained.
  - Using the **range** command in the DHCPv6 mode to specify the range of IPv6 addresses to be dynamically assigned in the DHCPv6 server using the prefixes obtained (only on models compatible with DHCPv6 server).
  - Using the **prefix-delegation** command in the DHCPv6 mode to reassign prefixes to the DHCPv6 server using the prefixes obtained (only on models compatible with DHCPv6 server).
- The information obtained from the DHCPv6 server is checked using the **show ipv6 dhcp interface** command.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Function types	Operations	Operating commands
IPv6 address settings	Enable/disable IPv6 addresses	ipv6 enable/disable
	IPv6 address settings	ipv6 address
	Specifies IPv6 addresses using DHCPv6-PD.	ipv6 address pd
	Show IPv6 address	show ipv6 interface
	Set RA setting for IPv6 address	ipv6 address autoconfig
	Specifies IPv6 addresses dynamically using a DHCPv6 client.	ipv6 address dhcp
	DHCPv6-PD client settings	ipv6 dhcp client pd
	Specifies automatic registration of default gateways using an RA.	ipv6 nd accept-ra-default-routes
	Displays status of DHCPv6 client.	show ipv6 dhcp interface
	Resets DHCPv6 client.	clear ipv6 dhcp client
	Setting for ND prefix received when setting DHCPv6 client settings	ipv6 dhcp client nd-prefix
Route information settings	Set default gateway	ipv6 route
	Show default gateway	show ipv6 route
	Set static route information	ipv6 route
	Show static route information	show ipv6 route
	Show route information	show ipv6 route
Neighbor cache settings	Set static neighbor cache entry	ipv6 neighbors
	Show neighbor cache table	show ipv6 neighbors
	Clear neighbor cache table	clear ipv6 neighbors
MTU settings	MTU settings	mtu

Examples of Command Execution

Setting up an IPv6 network environment (fixed settings)

In this example, the IPv6 addresses are manually set on this product, and an environment is set up for accessing the unit from a remote terminal.

- Maintenance for this product is done using the default VLAN (VLAN #1).
- The IPv6 address is set manually for the default VLAN (VLAN #1).
- **Web/TFTP access permission** is given from a host connected to VLAN #1.

1. This sets 2001:db8:1::2/64 for the default VLAN (VLAN #1).

```
Yamaha#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Yamaha(config)#interface vlan1
Yamaha(config-if)#ipv6 enable ①
Yamaha(config-if)#ipv6 address 2001:db8:1::2/64 ②
```

① Enable IPv6

② Specify an IPv6 address

2. Check the IPv6 address that was set.

```
Yamaha(config-if)#end
Yamaha#show ipv6 interface brief
Interface        IP-Address                                  Status
Protocol
vlan1            2001:db8:1::2/64                            up                    up
                 fe80::2a0:deff:fe:2/64
```

3. Set the default VLAN (VLAN #1) to permit access from HTTP servers and TFTP servers.
   Access using a remote host over the Web after settings are made.

```
Yamaha(config)#http-server interface vlan1 ①
Yamaha(config)#tftp-server interface vlan1 ②
```

① HTTP server access permission

② TFTP server access permission

Setting up an IPv6 network environment (automatic settings using RA)

In this example, the IPv6 addresses are automatically set on this product, and an environment is set up for accessing the unit from a remote terminal.

- Maintenance for this product is done using the default VLAN (VLAN #1).
- The IPv6 address is set automatically by **RA** for the default VLAN (VLAN #1).
- **Web/TFTP access permission** is given from a host connected to VLAN #1.

1. Specify RA for the default VLAN (VLAN #1).

```
Yamaha#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Yamaha(config)#interface vlan1
Yamaha(config-if)#ipv6 enable ①
Yamaha(config-if)#ipv6 address autoconfig ②
```

① Enable IPv6

② Set up RA

2. Check the IPv6 address that was obtained from RA.

```
Yamaha(config-if)#end
Yamaha#show ipv6 interface brief
Interface        IP-Address                                  Status
Protocol
vlan1            2001:db8::2a0:deff:fe:2/64                  up                    up
                 fe80::2a0:deff:fe:2/64
```

3. Set the default VLAN (VLAN #1) to permit access from HTTP servers and TFTP servers.
   Access using a remote host over the Web after settings are made.

```
Yamaha(config)#http-server interface vlan1 ①
Yamaha(config)#tftp-server interface vlan1 ②
```

① HTTP server access permission

② TFTP server access permission

IPv6 network environment setting (DHCPv6)

In this example, the IPv6 addresses are set on this product, and an environment is set up for accessing the unit from a remote terminal.

- Maintenance for this product is done using the default VLAN (VLAN #1).
- The IPv6 address is set automatically by **DHCPv6** for the default VLAN (VLAN #1).
- **Web/TFTP access permission** is given from a host connected to VLAN #1.

1. Specify DHCPv6 for the default VLAN (VLAN #1).

```
Yamaha#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Yamaha(config)#interface vlan1
Yamaha(config-if)#ipv6 enable ①
Yamaha(config-if)#ipv6 address dhcp ②
```

① Enable IPv6

② Set DHCPv6

2. Check the IPv6 address information obtained by DHCPv6.

```
Yamaha(config-if)#end
Yamaha#show ipv6 interface brief
Interface       IPv6-Address                                Admin-Status  Link-Status
vlan1          *2001:db8:1:aa10::dd37/128
                fe80::ae44:f2ff:fe84:efdd/64                up            up
```

3. Set the default VLAN (VLAN #1) to permit access from HTTP servers and TFTP servers.
   Access using a remote host over the Web after settings are made.

```
Yamaha(config)#http-server interface vlan1 ①
Yamaha(config)#tftp-server interface vlan1 ②
```

① HTTP server access permission

② TFTP server access permission

IPv6 network environment settings (DHCPv6-PD)

In this example, the IPv6 addresses are set on this product, and an environment is set up for accessing the unit from a remote terminal.

- Maintenance for this product is done using the default VLAN (VLAN #1).
- **DHCPv6-PD** is specified for VLAN #100 and prefixes are obtained.
- The IPv6 address is specified using a prefix obtained by DHCPv6-PD for the default VLAN (VLAN #1).
- **Web/TFTP access permission** is given from a host connected to VLAN #1.

1. Specify DHCPv6-PD for VLAN #100.

```
Yamaha#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Yamaha(config)#interface vlan100
Yamaha(config-if)#ipv6 enable
Yamaha(config-if)#ipv6 dhcp client pd PD_VLAN100           ... (Obtain a prefix using the
name PD_VLAN100)
Yamaha(config-if)#end
```

2. Check the prefix information obtained by DHCPv6-PD.

```
Yamaha#show ipv6 dhcp interface
Interface vlan100
  Client Type        : IA_PD
  Prefix name        : PD_VLAN100
  prefix             : 2001:db8:1:aaf0::/60 ①
  IAID               : 0f28924a
  DUID               : 0001000100000000a0de000000
  preferred lifetime : 604800
  valid lifetime     : 2592000
  expires            : 2023/4/19 08:08:04
```

① Obtain 2001:db8:1:aaf0::/60

3. Specify an IPv6 address for the default VLAN (VLAN #1).
Use the prefix obtained by DHCPv6-PD to specify 2001:db8:1:aaf2::1/64.

```
Yamaha#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Yamaha(config)#interface vlan1
Yamaha(config-if)#ipv6 enable ①
Yamaha(config-if)#ipv6 address pd PD_VLAN100 ::2:0:0:0:1/64 ②
```

① Enable IPv6

② Specify an IPv6 address

4. Check the IPv6 address that was set.

```
Yamaha(config-if)#end
Yamaha#show ipv6 interface brief
Interface       IP-Address                                  Admin-Status  Link-Status
vlan1          *2001:db8:1:aaf2::1/64
                fe80::ae44:f2ff:fe84:efdd/64                up            up
```

5. Set the default VLAN (VLAN #1) to permit access from HTTP servers and TFTP servers.

Access using a remote host over the Web after settings are made.

```
Yamaha(config)#http-server interface vlan1 ①
Yamaha(config)#tftp-server interface vlan1 ②
```

① HTTP server access permission

② TFTP server access permission

Points of Caution

- If opposing DHCPv6 server settings are changed while DHCPv6 client functionality is being used, the setting changes may not be applied properly in the DHCPv6 client. If that occurs, use the **clear ipv6 dhcp client** command to reset the DHCPv6 client.
- The DHCPv6 client for this product does not support the following operations.
    - Requesting an SOL_MAX_RT option for solicit messages sent by a DHCPv6 client.
    - Overwriting SOL_MAX_RT parameter settings inside a DHCPv6 client after a SOL_MAX_RT option is received.
        - Note that SOL_MAX_RT parameters inside a DHCPv6 client remain active for a fixed 120 seconds.
    - Requesting an INF_MAX_RT option for request messages sent by a DHCPv6 client.
    - Overwriting INF_MAX_RT parameter settings inside a DHCPv6 client after an INF_MAX_RT option is received.
        - Note that INF_MAX_RT parameters inside a DHCPv6 client remain active for a fixed 120 seconds.

Related Documentation

- Layer 2 Function: VLAN
- Maintenance and Operation Functions: Remote Access Control
- Yamaha RTpro: What is ARP?

Static Routing

Function Overview

In this product, static routing (static route information) can be used for route control in IP networks.

An administrator can explicitly register route information by entering a command.
You can set both static routes for IPv4 networks and static routes for IPv6 networks.

There are the following two types of static route information.

Type	Description
VLAN interface route information	Route information automatically registered by setting the IP address using the **ip/ipv6 address** command
Static route information	Route information registered by route setting by **ip/ipv6 route** command

Use the **show ip/ipv6 route** command to display the routing table.

Definition of Terms Used

None

Function Details

VLAN interface route information

Route information that is automatically registered by setting the IP address using the **ip/ipv6 address** command.
It is the route information of the network directly connected to this product and is associated with the interface.

Set 192.168.100.1/24 as the IP address for the VLAN1 interface and display the routing table.

```
Yamaha(config)# interface vlan1
Yamaha(config-if)# ip address 192.168.100.1/24
Yamaha(config-if)# exit
Yamaha(config)# exit
Yamaha#show ip route
Codes: C - connected, S - static
       * - candidate default

C       192.168.100.0/24 is directly connected, vlan1

Gateway of last resort is not set
```

Static route information

Route information registered by route setting by **ip/ipv6 route** command.

You can statically set a route to a specific network or set a default gateway.

When setting the default gateway, specify **0.0.0.0/0** as the destination network.

Up to 128 IPv4 static routes with the **ip route** command can be set.
Up to 32 IPv6 static routes with the **ipv6 route** command can be set.

Set the gateway for the route addressed to 172.16.0.0/16 to 192.168.100.254 and display the routing table.

```
Yamaha(config)# ip route 172.16.0.0/24 192.168.100.254
Yamaha(config)# exit
Yamaha# show ip route
Codes: C - connected, S - static
       * - candidate default

S       172.16.0.0/24 [1/0] via 192.168.100.254, vlan1
C       192.168.100.0/24 is directly connected, vlan1

Gateway of last resort is not set
```

Set 192.168.100.200 as the default gateway and display the routing table.

```
Yamaha(config)# ip route 0.0.0.0/0 192.168.100.200
Yamaha(config)# exit
Yamaha# show ip route
Codes: C - connected, S - static
       * - candidate default

Gateway of last resort is 192.168.100.200 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 192.168.100.200, vlan1
S       172.16.0.0/24 [1/0] via 192.168.100.254, vlan1
C       192.168.100.0/24 is directly connected, vlan1
```

Display of routing table

There are two routing tables: an IP forwarding table (FIB) in which only route information actually used for packet forwarding is registered, and an IP routing table (RIB) in which all route information is registered.
All VLAN interface route information and static route information are registered in the IP routing table. Within this, only the route information that is actually used in the packet forwarding process is registered in the IP forwarding table.

Use the **show ip/ipv6 route** command to display the IP forwarding table and the IP routing table.
In the routing table, VLAN interface route information and static route information are displayed as follows.

Type	Display
VLAN interface route information	C - connected
Static route information	S - static

If no option is specified for show ip/ipv6 route, the IP forwarding table is displayed.

You can display the IP routing table by specifying the database option with show ip/ipv6 route.
You can also display summary information and specific route information only by specifying other options.

Option	Description
IP address	Display route information used when forwarding packets to the specified IP address.
IP address and prefix	Display route information that matches the specified information.
database	Display all configured route information (IP routing table).

Option	Description
summary	Display IP routing table summary information

For details on how to use the **show ip route** command, refer to the command reference.

Route information priority (management distance)

Route information has a priority commonly called Administrative Distance.
This is used to determine which is prioritized when route information to the same destination is registered with VLAN interface route information and static route information.
The priority of route information can be applied not only to static routing but also to dynamic routing.
The priority of static routing route information can be specified in the range of 1 to 255 using the option at the end of the **ip route** command.
The smaller the value, the higher the priority. In the initial state, the priority is as follows.

Type	Initial priority	How to change priority
VLAN interface route information	None (overrides any other route information)	Settings cannot be changed.
Static route information	1	It can be specified in the range of 1 to 255 by the option at the end of the **ip/ipv6 route** command.

Enabling the routing function

Use the **ip/ipv6 forwarding** command to enable/disable the routing function.
In the initial state, the routing function is enabled for both IPv4 and IPv6.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

- List of related commands

Function types	Operations	Operating commands
Route information settings	Set static route information	ip route / ipv6 route
	Show static route information	show ip route / show ipv6 route
	Show route information	show ip route / show ipv6 route
Routing function settings	Routing function settings	ip forwarding / ipv6 forwarding
	Routing function status display	show ip forwarding / show ipv6 forwarding

Points of Caution

None

Related Documentation

None

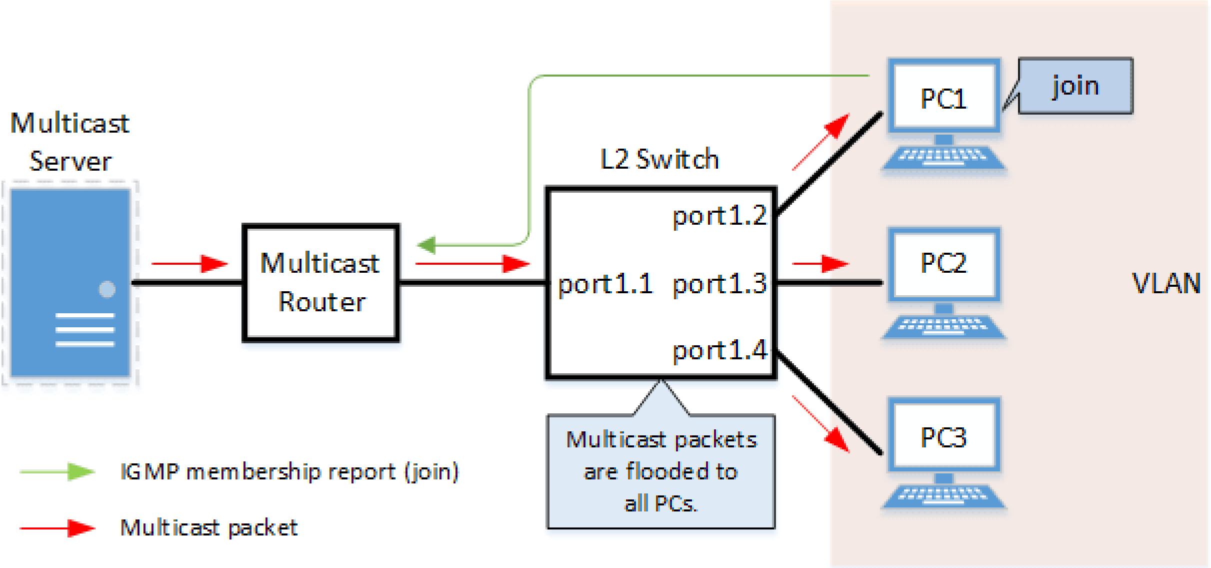
IP Multicast Functions

IGMP Snooping

Function Overview

IGMP snooping is a function to suppress consumption of network bandwidth in a VLAN environment, by controlling any surplus multicast flooding.
On an L2 switch, since multicast packets are distributed per VLAN, if there is even one device in the VLAN that wants to receive the multicast packet, the packet will be distributed to all ports within the same VLAN.

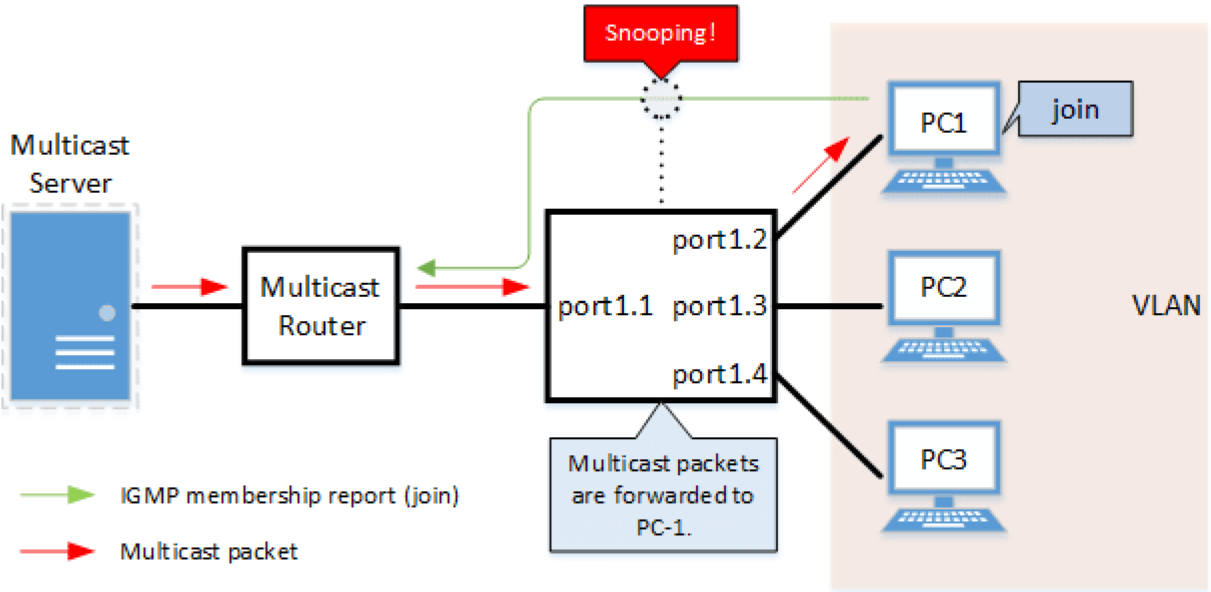
- Operations during multicast distribution (no IGMP snooping)



Multicast packets are flooded to all PCs.

When using the IGMP snooping function, the IGMP messages exchanged between the receiving device and the multicast router are monitored (snooped), the packet from the relevant group will only be distributed to the port, to which the device that wants to receive the multicast packet is connected.

- Operations during multicast distribution (using IGMP snooping)



Multicast packets are forwarded to PC-1.

Definition of Terms Used

IGMP (Internet Group Management Protocol)

This is a protocol to control multicast groups.
The multicast router can determine which hosts on the LAN are members of the multicast group, and the hosts can communicate which multicast group they belong to.
There are three protocol versions, respectively defined by **IGMPv1 (RFC1112)**, **IGMPv2 (RFC2236)** and **IGMPv3 (RFC3376)**.

Multicast Router Port

This is the LAN/SFP port to which the multicast router is connected.
The LAN/SFP port that receives the IGMP general query is automatically acquired as the multicast router port.

IGMP Report Suppression Function

This is a function where the switch controls the data transmission load between the multicast router and the hosts.
The messages gathered by this product to perform control are shown below.

- IGMP reports replied to IGMP general queries by hosts, sent from the multicast router
- IGMP leave messages notified by the host

The report suppression function works with IGMPv1/v2/v3.

Fast Leave Function

If a LAN/SFP port receives an IGMPv2/v3 leave message, this function immediately disconnects the port from ports receiving multicast traffic (deletes the FDB entry necessary for transmission).
Normally, when processing IGMPv2/v3 messages, if a leave message is received, a group-specific query is transmitted to that port to confirm that the receiver exists, but if the fast leave function is **enabled**, that action is not performed.
For this reason, the fast leave function is **effective only when there is a single receiver under the control of the LAN/SFP port**.
The fast leave function operates only when an IGMPv2/v3 leave message is received.
If the fast leave function is **enabled** and the **auto-assignment** option is specified, the port to which the switch is connected under the control of the LAN/SFP port will confirm that a receiver exists when a leave message is received.
The **auto-assignment** option allows you to use the fast leave function in a cascaded switch configuration.

IGMP Query Transmission Function (IGMP Querier)

This is a function to send IGMP general and specific queries.
It is used to enable the IGMP snooping function in an environment without a multicast router.

Data Transfer Suppression Function for Multicast Router Ports

This function controls multicast data being forwarded to the multicast router port.
Normally, all multicast group data already acquired by the product is forwarded to the multicast router port, but if this function is **enabled**, then only multicast group data acquired by receiving an IGMP report via the multicast router port is forwarded.
If unnecessary multicast data flow between switches is restricting bandwidth, the problem can be mitigated by **enabling** this function in combination with the **l2-unknown-mcast discard** command.

IGMP Report Forwarding Function

This function forwards IGMP Join/Leave messages to ports to which a switch is connected under the control of the LAN/SFP port.
By enabling this function, IGMP Join/Leave messages will be forwarded to non-querier switches in a cascaded switch configuration.
When using the **data transfer suppression function for multicast router ports** in an environment where multiple multicast data flow, we recommend that this function be **enabled**.

Function Details

The operating specifications for IGMP snooping are shown below.

1. This product offers snooping functions compatible with **IGMP v1/v2/v3**.
   You can use the **ip igmp snooping version** command to make later versions operate on this product.
   Version settings are made for the **VLAN interface**, and initial settings are for **v3**.
   The difference in operations between the configured version and received frame versions are shown in the table below.
   - If an IGMP query whose version is higher than the settings is received, the version will be lowered to the version that was configured, and the query will be forwarded.
   - If an IGMP report whose version is higher than the configured version is received, the relevant report will be discarded without being forwarded.
   - If an IGMP query and report of a lower version than the specified version is received, it is forwarded unmodified as the received version.
2. The settings to **enable/disable** IGMP snooping are made for the **VLAN interface**.
   The default value is **disabled**.
3. The IGMP snooping function can handle the following six operations.
   - Multicast router port setting
   - IGMP report suppression
   - Fast leave
   - IGMP query transmission
   - Suppression of data forwarding to multicast router port
   - IGMP report forwarding
4. Although the **multicast router port** is **automatically acquired** on VLAN interfaces where IGMP snooping is set to “**Enabled**”, the **ip igmp snooping mrouter interface** command can also be used to make static settings.
   The **show ip igmp snooping mrouter** command is used to check multicast router ports that are set for the VLAN interface.
5. The **IGMP report suppression function** is specified for VLAN interfaces using the **ip igmp snooping report-suppression** command.
   The default value is **enabled**.
   When transmitting an IGMP report or IGMP leave message using the report suppression function, the IPv4 address allocated to the VLAN interface will be used for the source IPv4 address.
   (The address will be set and transmitted as “0.0.0.0” if it has not been allocated.)
6. The **fast leave function** is set for the VLAN interface using the **ip igmp snooping fast-leave** command.
   The default value is **disabled**.
   If the fast leave function is **enabled** and the **auto-assignment** option is specified, and a network switch is connected under the control of the LAN/SFP port, the fast leave function is automatically **disabled** on that port.
   To determine whether or not a switch is connected under the control of the LAN/SFP port, the basic management TLV “System Capabilities” of the LLDP frame received on that port is checked to see if “Bridge” is contained in the TLV.

Therefore, when using the **auto-assignment** option, enable LLDP transmission and reception on both this product and the counterpart switch and add the basic management TLV to the transmitted frames.

7. The IGMP query transmission function is supported in order to allow use of IGMP snooping in environments that do not have a multicast router.
   The IGMP query transmission function is controlled with the following two parameters.
   - IGMP query transmission function Enable/disable
     - The **ip igmp snooping querier** command is used for VLAN interfaces.
     - The default value is **disabled**.
   - IGMP query transmission interval
     - This is executed using the **ip igmp snooping query-interval** command.
     - The transmission interval can be set from 20–18,000 sec., and the default value is **125 sec.**
8. When multiple devices transmit queries within a VLAN, the query is sent by the device with the lowest IPv4 address within the VLAN.
   When this product receives a query from a device whose IPv4 address is lower than its own, the query transmission function will be halted.
   The source IPv4 address that is set when a query is transmitted uses the IPv4 address allocated to the VLAN interface. If an IPv4 address has not been allocated, an IPv4 address allocated to a different VLAN interface is used instead. (If no IPv4 addresses have been allocated to any VLAN interfaces, the address will be set and transmitted as “0.0.0.0”.)
9. This product features a function that forces the TTL value of a received IGMP packet to change to “1” if the TTL value is invalid (a value other than “1”), instead of discarding the packet.
   This is defined as the **“TTL check function”**, and it can be configured for a VLAN interface by using the **ip igmp snooping check ttl** command.
   The default setting value for the **TTL check function** is **enabled (packets with invalid TTL values are discarded)**.
10. This product features a function that adds the RA (Router Alert) option to an IP header of a received IGMPv2/IGMPv3 packet that does not contain the RA option and forwards it instead of discarding.
    This is defined as the **“RA check function”**, and it can be configured for a VLAN interface by using the **ip igmp snooping check ra** command.
    The default value of the **RA check function** is set to **Disabled (forward packets that do not contain the RA option)**.
11. This product features a function that forces the ToS (Type of field) value of a received IGMPv3 packet to change to “0xc0” if the ToS value is invalid (a value other than “0xc0”), instead of discarding the packet.
    This is defined as the **“ToS check function”**, and it can be configured for a VLAN interface by using the **ip igmp snooping check tos** command.
    The default value of **ToS check function** is set to **Disabled (forward packets with invalid ToS values)**.
12. The data transfer suppression function for multicast router ports is specified for VLAN interfaces using the **ip igmp snooping mrouter-port data-suppression** command.
    The default value is **disabled**.
13. The IGMP report forwarding function is specified using the **ip igmp snooping report-forward** command for VLAN interfaces.
    The default value is **disabled**.
    When this function is **enabled** and a network switch is connected under the control of the LAN/SFP port, IGMP Join/Leave messages will be forwarded to that port.
    To determine whether or not a switch is connected under the control of the LAN/SFP port, the basic management TLV “System Capabilities” of the LLDP frame received on that port is checked to see if “Bridge” is contained in the TLV.
    Therefore, when using this function, enable LLDP transmission and reception on both this product and the counterpart switch and add the basic management TLV to the transmitted frames.

Related Commands

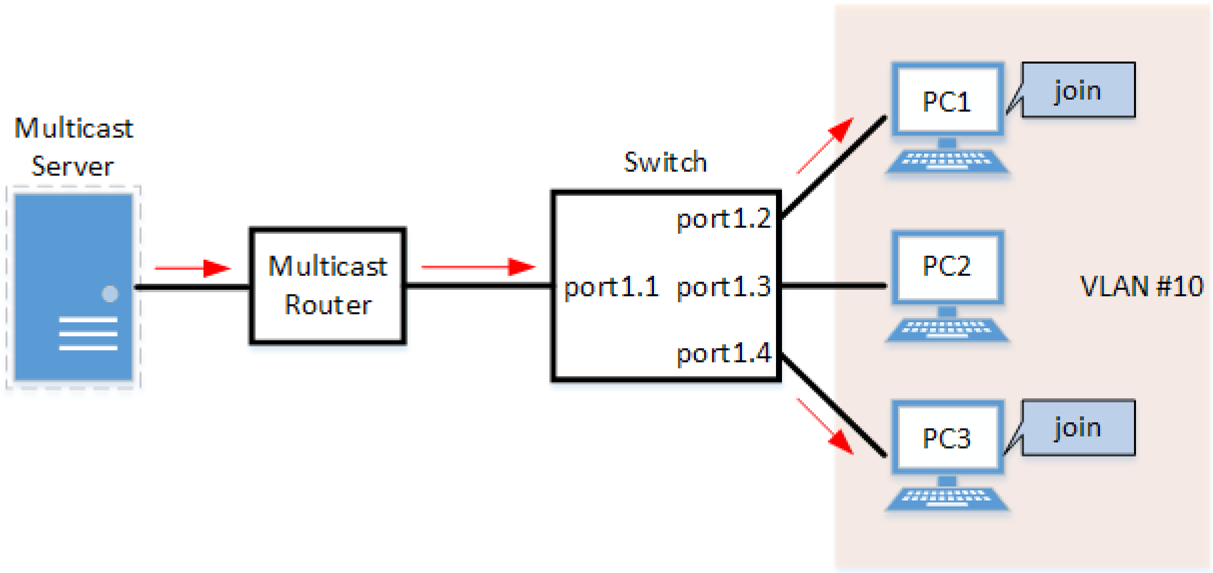
Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Enable/disable IGMP snooping	ip igmp snooping
Set IGMP snooping fast-leave	ip igmp snooping fast-leave
Multicast router port setting	ip igmp snooping mrouter interface
Set the query transmission function	ip igmp snooping querier
Set IGMP query transmission interval	ip igmp snooping query-interval
Set IGMP snooping TTL check	ip igmp snooping check ttl
Set IGMP snooping RA check	ip igmp snooping check ra
Set IGMP snooping ToS check	ip igmp snooping check tos
Set IGMP version	ip igmp snooping version
Set IGMP report suppression function	ip igmp snooping report-suppression
Set the data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression
Set IGMP report forwarding function	ip igmp snooping report-forward
Set the processing method for unknown multicast frames in the system	l2-unknown-mcast
Set forwarding of linked local multicasting addresses in the system	l2-unknown-mcast forward link-local
Set the processing method for unknown multicast frames at VLAN interfaces	l2-unknown-mcast
Set forwarding of multicasting frames at VLAN interfaces	l2-mcast flood
Show multicast router port information	show ip igmp snooping mrouter
Show IGMP multicast receiver information	show ip igmp snooping groups
Show IGMP related information for an interface	show ip igmp snooping interface
Clear IGMP group membership entries	clear ip igmp snooping

Examples of Command Execution

IGMP snooping settings (with multicast router)

In an environment with a multicast router, enable the IGMP snooping function and join a multicast group. Data is distributed only to PC1 and PC3.



- Set LAN ports #1–#4 as **access ports and associate them with VLAN #10**.
- Since there is a multicast router, leave the **IGMP query transmission function as "disabled"**.
- Set multicast router port acquisition to **automatic acquisition** only. (A static setting is not used.)
- **Enable the fast leave function**.

1. Define VLAN #10, and set IGMP snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#no ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping fast-leave ④
```

① Define VLAN #10

② Enable IGMP Snooping for VLAN #10

③ Disable the IGMP query transmission function for VLAN #10

④ Enable the IGMP fast leave function for VLAN #10

  - IGMP snooping is enabled and IGMP query transmission is disabled in default settings, so there is no need to specify those settings.

2. Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

① Configure the settings above for LAN ports #2–#4 as well.

3. Confirm the multicast router port information. (It should be connected to LAN port #1.)

```
Yamaha#show ip igmp snooping mrouter vlan10
VLAN    Interface             IP-address    Expires
-------------------------------------------------------------------
```

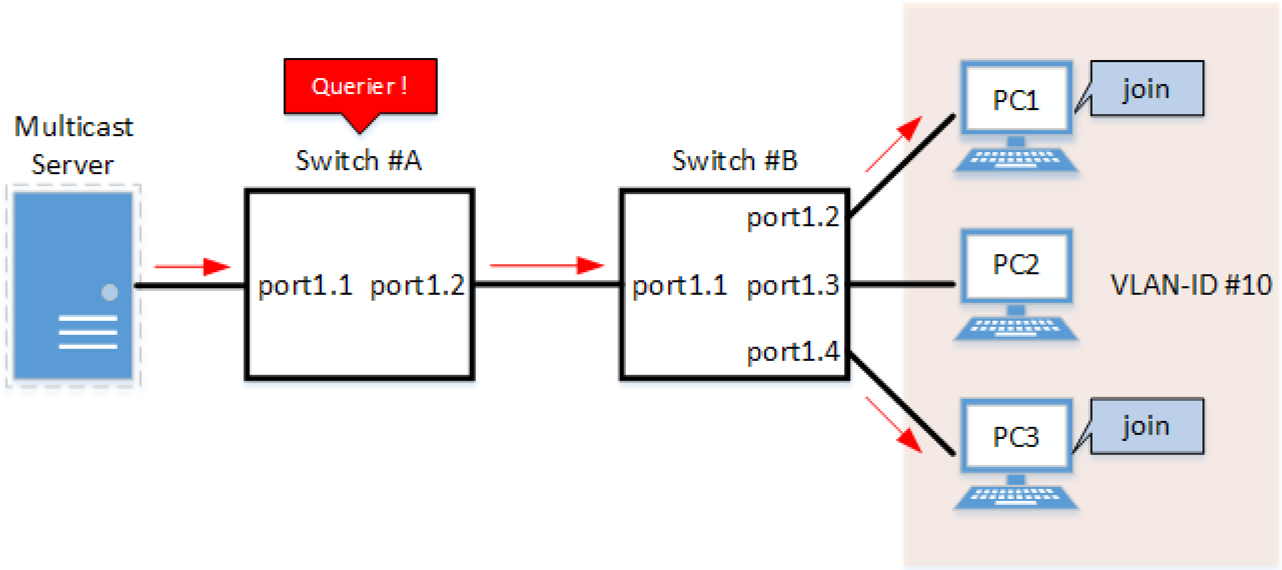
```
10      port1.1(dynamic)         192.168.100.216        00:00:49
```

4. Confirm the information for the multicast recipient.

```
Yamaha#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
10     239.0.0.1                port1.2        R      00:00:13    00:00:41 192.168.100.2
V3
10     239.0.0.1                port1.4        R      00:00:02    00:00:48 192.168.100.4
V3
```

IGMP snooping settings (without multicast router)

In an environment without a multicast router, enable the IGMP snooping function and join a multicast group. Data is distributed only to PC1 and PC3.



- Switch #A
    - Set LAN ports #1−#2 as **access ports and associate them with VLAN #10**.
    - **Enable the IGMP query transmission function**.
      Set the IGMP query transmission interval to **20 sec**.
- Switch #B
    - Set LAN ports #1−#4 as **access ports and associate them with VLAN #10**.
    - Set **multicast router port** acquisition to **automatic acquisition** only. (A static setting is not used.)
    - **Enable the fast leave function**.
    - Since there is a device that sets invalid TTL values in IGMP packets, **disable the TTL check function**.

1. [Switch #A] Define VLAN #10, and set IGMP snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping query-interval 20 ④
```

① Define VLAN #10

② Enable IGMP Snooping for VLAN #10

③ Enable the IGMP query transmission function for VLAN #10

④ Set the IGMP query transmission interval for VLAN #10 to 20 sec.

- Since IGMP snooping is enabled by default, we do not need to set this specifically.

2. [Switch #A] Set LAN ports #1–#2 as access ports, and associate them with VLAN #10.

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

① Configure the settings above for LAN port #2 as well.

3. [Switch #B] Define VLAN #10, and set IGMP snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#no ip igmp snooping querier ③
Yamaha(config-if)#no ip igmp snooping check ttl ④
Yamaha(config-if)#ip igmp snooping fast-leave ⑤
```

① Define VLAN #10

② Enable IGMP Snooping for VLAN #10

③ Disable the IGMP query transmission function for VLAN #10

④ Disable the TTL check function for VLAN #10

⑤ Enable the IGMP fast leave function for VLAN #10

- IGMP snooping is enabled and IGMP query transmission is disabled in default settings, so there is no need to specify those settings.

4. [Switch #B] Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

① Configure the settings above for LAN ports #2–#4 as well.

5. [Switch #B] Check the multicast router port information. (It should be connected to LAN port #1.)

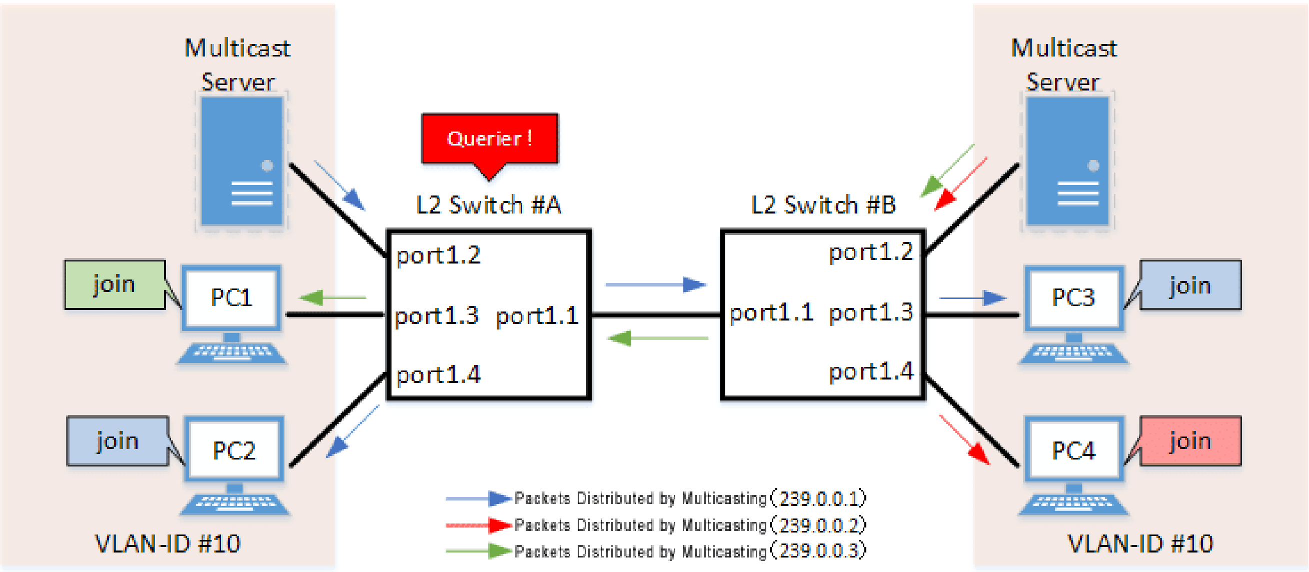
```
Yamaha#show ip igmp snooping mrouter vlan10
VLAN    Interface             IP-address    Expires
10      port1.1(dynamic)         192.168.100.216        00:00:49
```

6. [Switch #B] Check the multicast receiver information.

```
Yamaha#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
10     239.0.0.1                port1.2        R      00:00:13   00:00:41 192.168.100.2
V3
10     239.0.0.1                port1.4        R      00:00:02   00:00:48 192.168.100.4
V3
```

IGMP snooping settings (If distributing data in both directions)

In a configuration with two switches, both switches are connected to a multicast server and computer.
Each computer frequently switches between participating multicast groups to minimize the interruption time.



- Switch #A
  - Set LAN ports #1–#4 as **access ports and associate them with VLAN #10**.
  - **Enable the IGMP query transmission function**.
    Set the IGMP query transmission interval to **20 sec**.
  - **Enable the fast leave function** and perform the following operations in order to confirm the existence of multiple multicast receivers under the control of the counterpart switch.
    - **Enable LLDP transmission and reception and add the basic management TLV to the transmitted frames**.
    - **Enable the auto-assignment option**.
  - **Disable the IGMP report suppression function**.
  - Increasing the number of multicast servers or data distributions could cause port bandwidth restrictions, so **the data transfer suppression function for multicast router ports is enabled** to only

    forward the minimum data necessary.
    Also, **unknown multicast frames are set to be discarded**.

    - To forward IGMP reports to non-queriers, perform the following operations.
        - **Enable LLDP transmission and reception and add the basic management TLV to the transmitted frames**.
        - **Enable the IGMP report forwarding function**.

- Switch #B
    - Set LAN ports #1–#4 as **access ports and associate them with VLAN #10**.
    - Set **multicast router port** acquisition to **automatic acquisition** only. (A static setting is not used.)
    - **Enable the fast leave function** and perform the following operations in order to confirm the existence of multiple multicast receivers under the control of the counterpart switch.
        - **Enable LLDP transmission and reception and add the basic management TLV to the transmitted frames**.
        - **Enable the auto-assignment option**.
    - **Disable the IGMP report suppression function**.
    - Increasing the number of multicast servers or data distributions could cause port bandwidth restrictions, so **the data transfer suppression function for multicast router ports is enabled** to only forward the minimum data necessary.
      Also, **unknown multicast frames are set to be discarded**.

1. [Switch #A] Define VLAN #10, and set IGMP snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping query-interval 20 ④
Yamaha(config-if)#ip igmp snooping fast-leave auto-assignment ⑤
Yamaha(config-if)#ip igmp snooping report-suppression disable ⑥
Yamaha(config-if)#ip igmp snooping mrouter-port data-suppression enable ⑦
Yamaha(config-if)#ip igmp snooping report-forward enable ⑧
```

   ① Define VLAN #10

   ② Enable IGMP Snooping for VLAN #10

   ③ Enable the IGMP query transmission function for VLAN #10

   ④ Set the IGMP query transmission interval for VLAN #10 to 20 sec.

   ⑤ Enable the fast leave function and auto-assignment option for VLAN #10

   ⑥ Disable the report suppression function for VLAN #10

   ⑦ Enable the data transfer suppression function for multicast router ports for VLAN #10

   ⑧ Enable the report forwarding function for VLAN #10
    - Since IGMP snooping is enabled by default, we do not need to set this specifically.

2. [Switch #A] Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

① Configure the settings above for LAN ports #2–#4 as well.

3. [Switch #A] Discard unknown multicast frames.

```
Yamaha(config)#l2-unknown-mcast discard
```

4. [Switch #A] Enable LLDP transmission and reception for LAN port #1 and add the basic management TLV to the transmitted frames.

```
Yamaha(config)# lldp run
Yamaha(config)# interface port1.1
Yamaha(config-if)# lldp-agent
Yamaha(lldp-agent)# set lldp enable txrx
Yamaha(lldp-agent)# tlv-select basic-mgmt
```

5. [Switch #B] Define VLAN #10, and set IGMP snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#no ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping fast-leave auto-assignment ④
Yamaha(config-if)#ip igmp snooping report-suppression disable ⑤
Yamaha(config-if)#ip igmp snooping mrouter-port data-suppression enable ⑥
Yamaha(config-if)#ip igmp snooping report-forward enable ⑦
```

① Define VLAN #10

② Enable IGMP Snooping for VLAN #10

③ Disable the IGMP query transmission function for VLAN #10

④ Enable the fast leave function and auto-assignment option for VLAN #10

⑤ Disable the report suppression function for VLAN #10

⑥ Enable the data transfer suppression function for multicast router ports for VLAN #10

⑦ Enable the report forwarding function for VLAN #10

   - IGMP snooping is enabled and IGMP query transmission is disabled in default settings, so there is no need to specify those settings.

6. [Switch #B] Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

① Configure the settings above for LAN ports #2–#4 as well.

7. [Switch #B] Discard unknown multicast frames.

```
Yamaha(config)#l2-unknown-mcast discard
```

8. [Switch #B] Enable LLDP transmission and reception for LAN port #1 and add the basic management TLV to the transmitted frames.

```
Yamaha(config)# lldp run
Yamaha(config)# interface port1.1
Yamaha(config-if)# lldp-agent
Yamaha(lldp-agent)# set lldp enable txrx
Yamaha(lldp-agent)# tlv-select basic-mgmt
```

9. [Switch #A] Check the multicast receiver information.

```
Yamaha#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
10     239.0.0.1                port1.1        R      00:00:02   00:00:48 192.168.100.3
V3
10     239.0.0.2                port1.1        R      00:00:02   00:00:48 192.168.100.4
V3
10     239.0.0.3                port1.3        R      00:00:04   00:00:46 192.168.100.1
V3
10     239.0.0.1                port1.4        R      00:00:03   00:00:47 192.168.100.2
V3
```

10. [Switch #B] Check the multicast router port information. (It should be connected to LAN port #1.)

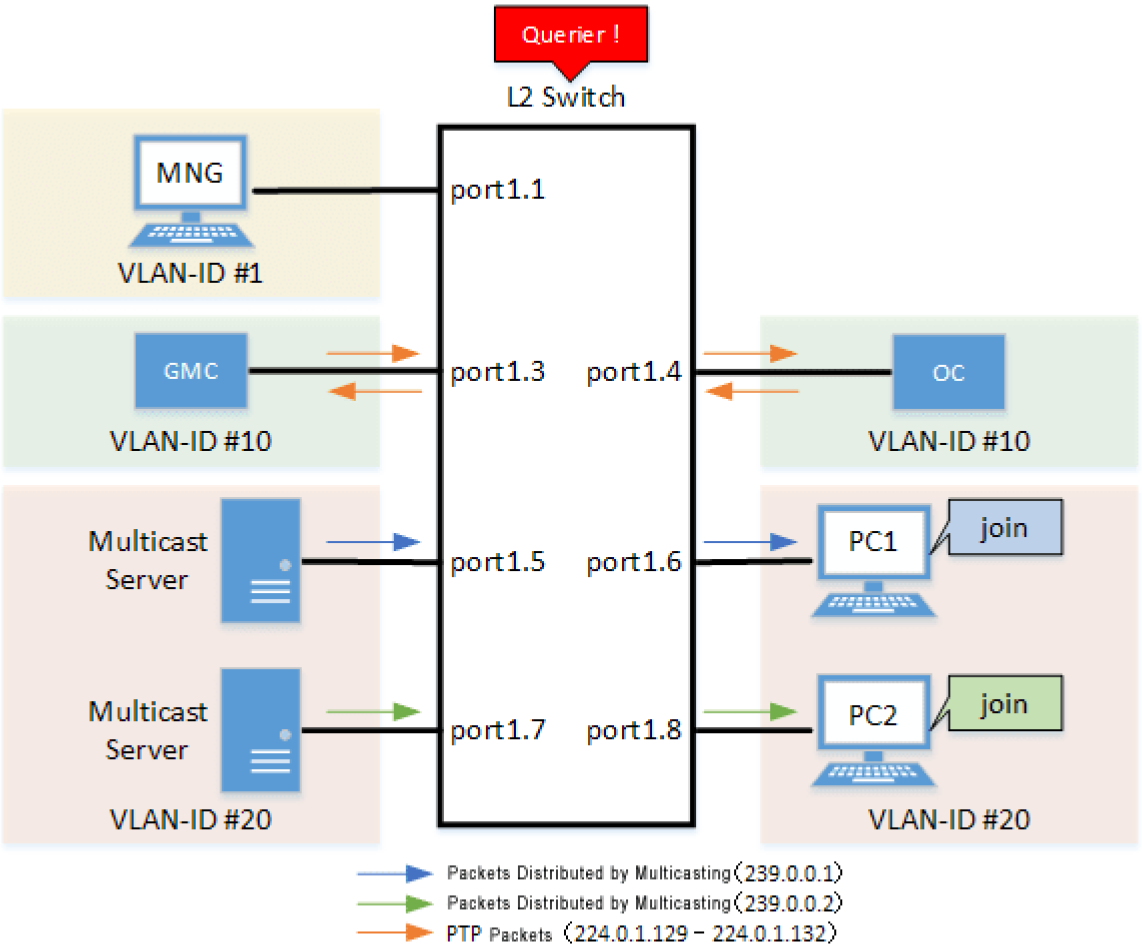
```
Yamaha#show ip igmp snooping mrouter vlan10
VLAN    Interface                 IP-address    Expires
10      port1.1(dynamic)          192.168.100.240        00:00:25
```

11. [Switch #B] Check the multicast receiver information.

```
Yamaha#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
10     239.0.0.1                port1.1        R      00:00:03   00:00:47 192.168.100.2
V3
10     239.0.0.3                port1.1        R      00:00:04   00:00:46 192.168.100.1
V3
10     239.0.0.1                port1.3        R      00:00:02   00:00:48 192.168.100.3
V3
10     239.0.0.2                port1.4        R      00:00:02   00:00:48 192.168.100.4
V3
```

IGMP snooping settings (for separating multiple multicast environments with VLANs)

Using a single network switch, multicast environments are reconfigured with synchronized times and data streams separated by VLANs.
VLAN #1 is used for management, **VLAN #10 for time synchronization**, and **VLAN #20 for streaming**.



- Entire system
  - The entire system is configured to **always forward linked local multicasting addresses**.
- VLAN #1
  - LAN port #1 is **set as the access port associated to VLAN #1**.
  - **Enable the IGMP query transmission function**.
- VLAN #10
  - LAN ports #3 to #4 are **set as access ports associated to VLAN #10**.
  - To minimize any interruptions in PTP packet streams (224.0.1.129 to 224.0.1.132), the VLAN is **always kept flooded**.
  - **Enable the IGMP query transmission function**.
- VLAN #20
  - LAN ports #5 to #8 are **set as access ports associated to VLAN #20**.
  - This **discards unknown multicast frames** to prevent restricting bandwidth due to unnecessary multicasting in VLAN #20.
  - **Enable the IGMP query transmission function**.
    Set the IGMP query transmission interval to **20 sec**.
  - **Enable the fast leave function**.

1. Configure the entire system to always forward linked local multicasting addresses.

```
Yamaha(config)#l2-unknown-mcast forward link-local
```

2. Specify IGMP snooping for VLAN #1.

```
Yamaha(config)#interface vlan1
Yamaha(config-if)#ip igmp snooping enable ①
Yamaha(config-if)#ip igmp snooping querier ②
```

① Enable IGMP snooping for VLAN #1

② Enable the IGMP query transmission function for VLAN #1
   - Since IGMP snooping is enabled by default, we do not need to set this specifically.

3. Define VLAN #10 and specify IGMP snooping and multicast forwarding.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#l2-mcast flood 224.0.1.129 ②
Yamaha(config-if)#l2-mcast flood 224.0.1.130 ③
Yamaha(config-if)#l2-mcast flood 224.0.1.131 ④
Yamaha(config-if)#l2-mcast flood 224.0.1.132 ⑤
Yamaha(config-if)#ip igmp snooping enable ⑥
Yamaha(config-if)#ip igmp snooping querier ⑦
```

① Define VLAN #10

② Always flood 224.0.1.129 on VLAN #10

③ Always flood 224.0.1.130 on VLAN #10

④ Always flood 224.0.1.131 on VLAN #10

⑤ Always flood 224.0.1.132 on VLAN #10

⑥ Enable IGMP Snooping for VLAN #10

⑦ Enable the IGMP query transmission function for VLAN #10
   - Since IGMP snooping is enabled by default, we do not need to set this specifically.

4. Set LAN ports #3–#4 as access ports, and associate them with VLAN #10.

```
Yamaha(config)# interface port1.3
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

① Configure the settings above for LAN port #4 as well.

5. Define VLAN #20 and specify IGMP snooping and multicast forwarding.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 20 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan20
Yamaha(config-if)#l2-unknown-mcast discard ②
Yamaha(config-if)#ip igmp snooping enable ③
Yamaha(config-if)#ip igmp snooping query-interval 20 ④
Yamaha(config-if)#ip igmp snooping querier ⑤
Yamaha(config-if)#ip igmp snooping fast-leave ⑥
```

① Define VLAN #20

② Discard unknown multicast on VLAN #20

③ Enable IGMP snooping for VLAN #20

④ Set the IGMP query transmission interval for VLAN #20 to 20 sec.

⑤ Enable the IGMP query transmission function for VLAN #20

⑥ Enable the fast leave function for VLAN #20
   - Since IGMP snooping is enabled by default, we do not need to set this specifically.

6. [Switch #A] Set LAN ports #5–#8 as access ports, and associate them with VLAN #20.

```
Yamaha(config)# interface port1.5
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 20
①
```

① Configure the settings above for LAN ports #6–#8 as well.

7. Confirm the information for the multicast recipient.
PTP packets (224.0.1.129 to 224.0.1.132) are not listed because they are always kept flooded at that time.

```
Yamaha#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
20     239.0.0.1                port1.6        R      00:00:02   00:00:48 192.168.100.1
V3
20     239.0.0.2                port1.8        R      00:00:02   00:00:48 192.168.100.2
V3
```

Points of Caution

- If you want to change the handling of unknown multicast frames, use the **l2-unknown-mcast** command.
- When a topology change is detected, if you want to send a query regardless of the normal transmission interval, set the **l2-mcast snooping tcn-query** command.

Related Documentation

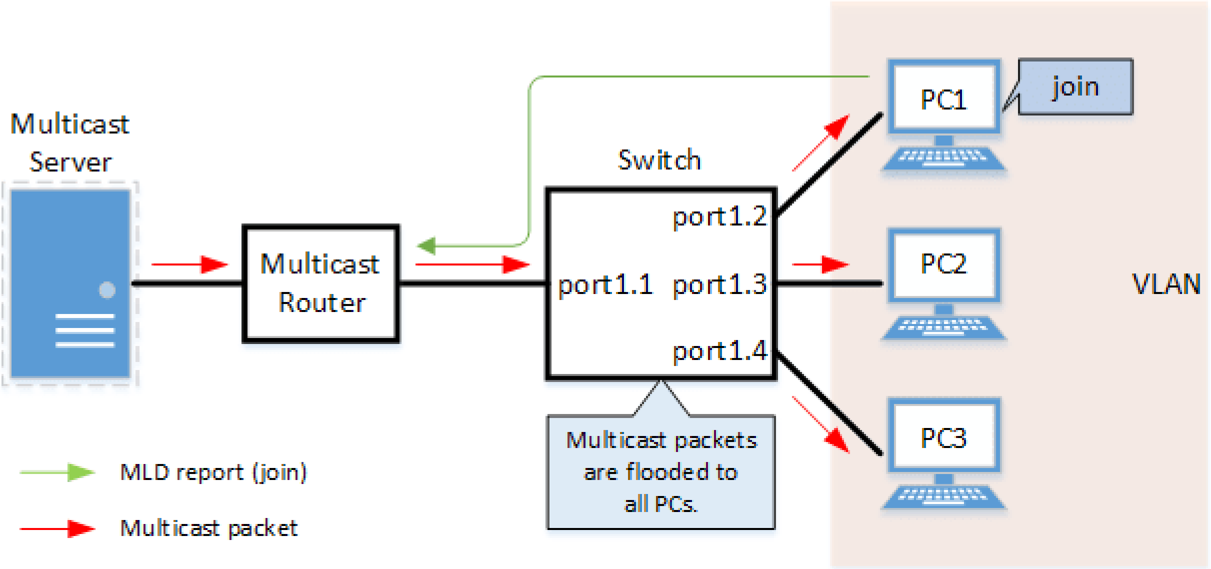
- Layer 2 Function: VLAN

MLD Snooping

Function Overview

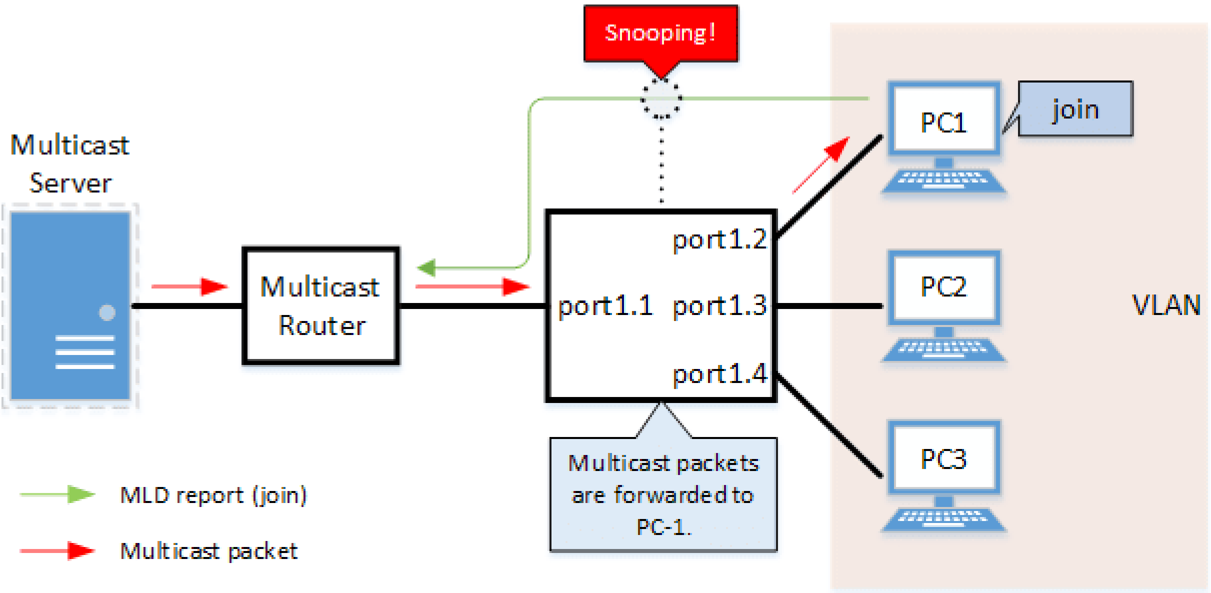
MLD snooping is a function to suppress consumption of network bandwidth in an IPv6 VLAN environment, by controlling any surplus multicast flooding.
On an L2 switch, since multicast packets are distributed per VLAN, if there is even one device in the VLAN that wants to receive the multicast packet, the packet will be distributed to all ports within the same VLAN.

- Operations during multicast distribution (no MLD snooping)



When using the MLD snooping function, the MLD messages exchanged between the receiving device and the multicast router are monitored (snooped), the packet from the relevant group will only be distributed to the port, to which the device that wants to receive the multicast packet is connected.

- Operations during multicast distribution (using MLD snooping)



Definition of Terms Used

MLD (Multicast Listener Discovery)

This is a protocol to control multicast groups using IPv6 (a sub-protocol of ICMPv6).
The multicast router can determine which hosts on the LAN are members of the multicast group, and the hosts

can communicate which multicast group they belong to.
There are two protocol versions, respectively defined by **MLDv1 (RFC2710)**, and **MLDv2 (RFC3810)**.

Multicast Router Port

This is the LAN/SFP port to which the multicast router is connected.
The LAN/SFP port that receives the MLD general query is automatically acquired as the multicast router port.

MLD Report Suppression Function

This is a function where the L2 switch controls the data transmission load between the multicast router and the hosts.
The messages gathered by this product to perform control are shown below.

- MLD reports replied to MLD general queries by hosts, sent from the multicast router
- MLD Done messages notified by the host and MLD reports (Leave)

The report suppression function works with MLDv1/v2.

MLD Fast Leave Function

This function allows for the LAN/SFP port that received an MLDv1 Done and an MLDv2 report (Leave) to immediately stop receiving multicasts (deleting the necessary FDB entry).
Previously, when an MLDv1 Done message and an MLDv2 report (Leave) was received in the course of MLD leave processing, a group-specific query was sent to check for the existence of a receiver; but if the fast leave function is **enabled**, this operation is not performed.
For this reason, the fast leave function is **effective only when there is a single receiver under the control of the LAN/SFP port**.

MLD Query Transmission Function (MLD Querier)

This is a function to send MLD general and specific queries.
It is used to enable the MLD snooping function in an environment without a multicast router.

Function Details

The operating specifications for MLD snooping are shown below.

1. This product offers snooping functions compatible with **MLD v1/v2**.
   You can use the **ipv6 mld snooping version** command to make later versions work on this product.
   Version settings are made for the **VLAN interface**, and initial settings are for **v2**.
   The difference in operations between the configured version and received frame versions are shown in the table below.
   - If an MLD query whose version is higher than the settings is received, the version will be lowered to the version that was configured, and the query will be forwarded.
   - If an MLD report whose version is higher than the configured version is received, the relevant report will be discarded without being forwarded.
2. The settings to **enable/disable** MLD snooping are made for the **VLAN interface**.
   The initial setting for the default VLAN (VLAN #1) and the initial setting after a VLAN is generated are both **disabled**.
3. The MLD snooping function can handle the following four operations.
   - Multicast router port setting
   - MLD report suppression
   - MLD fast leave

    - MLD query transmission

4. Although the **multicast router port** is **automatically acquired** on VLAN interfaces where MLD snooping is set to "**Enabled**", the **ipv6 mld snooping mrouter interface** command can also be used to make static settings.
   The **show ipv6 mld snooping mrouter** command is used to check multicast router ports that are set for the VLAN interface.
5. The **MLD report suppression function** is specified for VLAN interfaces using the **ipv6 mld snooping report-suppression** command.
   The default value is **enabled**.
   When transmitting an MLD report or MLD leave message using the report suppression function, the IPv6 link local address allocated to the VLAN interface will be used for the source IPv6 address.
   (The address will be set and transmitted as "::" if it has not been allocated.)
6. The **MLD fast leave function** is set for the VLAN interface using the **ipv6 mld snooping fast-leave** command.
   The initial setting for the default VLAN (VLAN #1) and the initial setting after a VLAN is generated are both **disabled**.
7. The **MLD query transmission function** is supported in order to allow use of MLD snooping in environments that do not have a multicast router.
   The MLD query transmission function controls the following two parameters.
    - MLD query transmission function Enable/disable
        - The **ipv6 mld snooping querier** command is used for VLAN interfaces.
        - The initial setting for the default VLAN (VLAN #1) and the initial setting after a VLAN is generated are both **disabled**.
    - MLD query transmission interval
        - This is set using the **ipv6 mld snooping query-interval** command.
        - The transmission interval can be set from 20–18,000 sec., and the default value is **125 sec.**
8. When multiple devices transmit queries within a VLAN, the query is sent by the device with the lowest IPv6 address within the VLAN.
   When this product receives a query from a device whose IPv6 address is lower than its own, the query transmission function will be halted.
   The source iPv6 address that is set when a query is transmitted uses the IPv6 link local address allocated to the VLAN interface. If an IPv6 link local address has not been allocated, an IPv6 link local address allocated to a different VLAN interface is used instead.
   (If no IPv6 link local addresses have been allocated to any VLAN interfaces, the query is not transmitted.)
9. In this product, if the Hop Limit of a received MLD packet is invalid (other than 1), the MLD packet will be discarded.
10. In this product, if a received MLD packet does not contain the Router Alert option, the MLD packet will be discarded.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

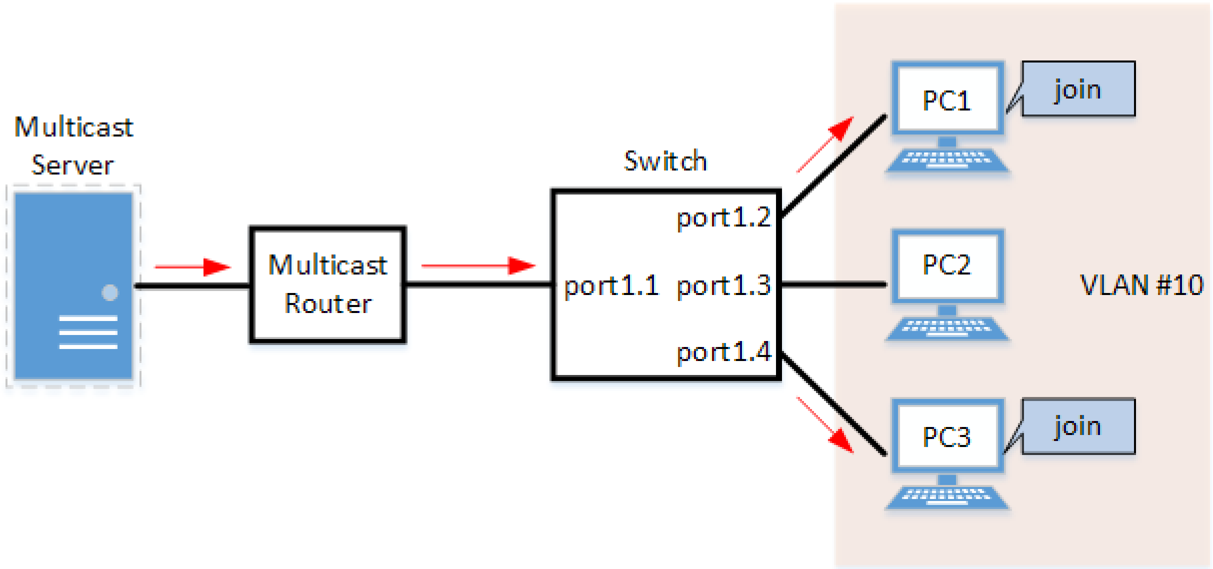
Operations	Operating commands
Enable/disable MLD snooping	ipv6 mld snooping
Set MLD snooping fast-leave	ipv6 mld snooping fast-leave
Multicast router port setting	ipv6 mld snooping mrouter interface

Operations	Operating commands
Set the query transmission function	ipv6 mld snooping querier
Set the MLD query transmission interval	ipv6 mld snooping query-interval
Set the MLD version	ipv6 mld snooping version
Set the MLD report suppression function	ipv6 mld snooping report-suppression
Show multicast router port information	show ipv6 mld snooping mrouter
Show MLD multicast recipient information	show ipv6 mld snooping groups
Show MLD related information for an interface	show ipv6 mld snooping interface
Clear the MLD group membership entries	clear ipv6 mld snooping

Examples of Command Execution

MLD snooping settings (with multicast router)

In an environment with a multicast router, enable the MLD snooping function and join a multicast group. Data is distributed only to PC1 and PC3.



- Set LAN ports #1–#4 as **access ports and associate them with VLAN #10**.
- Since there is a multicast router, leave the **MLD query transmission function as "disabled"**.
- Set **multicast router port** acquisition to **automatic acquisition** only. (A static setting is not used.)
- **Enable the MLD fast leave function**.

■ Setting Procedure

1. Define VLAN #10, and set MLD snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ipv6 enable ②
Yamaha(config-if)#ipv6 mld snooping ③
Yamaha(config-if)#no ipv6 mld snooping querier ④
Yamaha(config-if)#ipv6 mld snooping fast-leave ⑤
```

① Define VLAN #10

② Enable the IPv6 function for VLAN #10

③ Enable MLD Snooping for VLAN #10

④ Disable the MLD query transmission function for VLAN #10

⑤ Enable the MLD fast leave function for VLAN #10

- MLD snooping is enabled and the MLD query transmission function is disabled in default settings, so there is no need to specify those settings.

2. Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

① Configure the settings above for LAN ports #2–#4 as well.

3. Confirm the multicast router port information. (It should be connected to LAN port #1.)

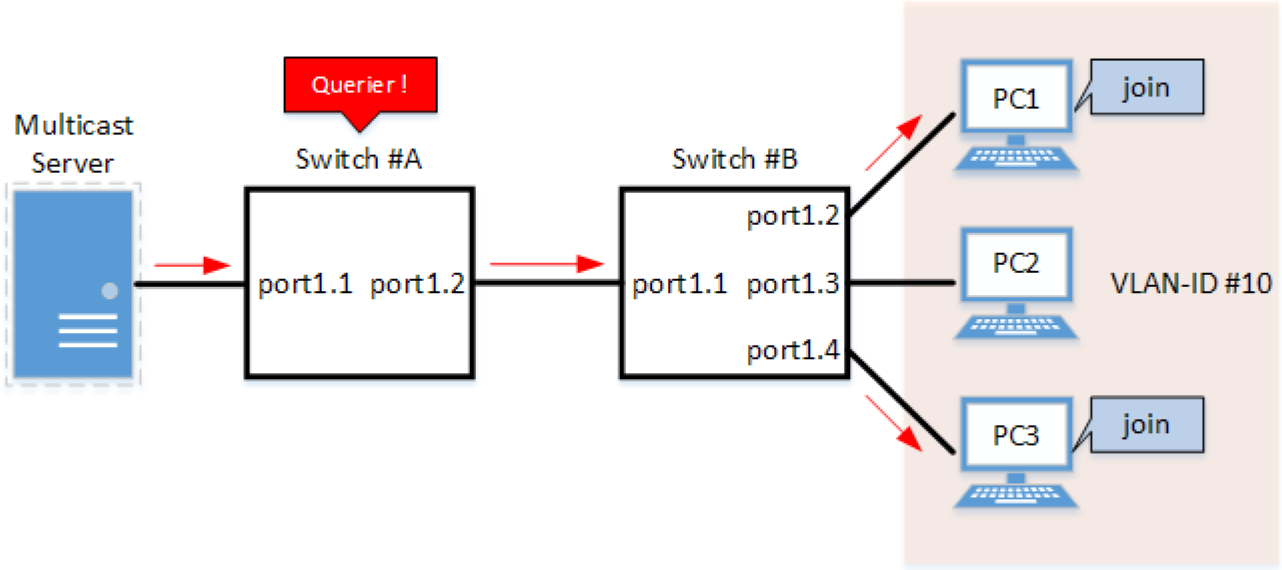
```
Yamaha#show ipv6 mld snooping mrouter vlan10
VLAN    Interface             IP-address    Expires
10      port1.1(dynamic)         fe80::2a0:deff:feae:b879       00:00:43
```

4. Confirm the information for the multicast recipient.

```
Yamaha#show ipv6 mld snooping groups
MLD Connected Group Membership
Vlan   Group Address                              Interface            Uptime   Expires
Last Reporter
10     ff15::1                                    port1.2              00:00:13 00:00:41
fe80::a00:27ff:fe8b:87e2
10     ff15::1                                    port1.4              00:00:02 00:00:48
fe80::a00:27ff:fe8b:87e4
```

MLD snooping settings (without multicast router)

In an environment without a multicast router, enable the MLD snooping function and join a multicast group. Data is distributed only to PC1 and PC3.



- Switch #A
  - Set LAN ports #1–#2 as **access ports and associate them with VLAN #10**.
  - **Enable the MLD query transmission function**.
    Set the MLD query transmission interval to* 20 sec*.
- Switch #B
  - Set LAN ports #1–#4 as **access ports and associate them with VLAN #10**.
  - Set **multicast router port** acquisition to **automatic acquisition** only. (A static setting is not used.)
  - **Enable the MLD fast leave function**.

1. [Switch #A] Define VLAN #10, and set MLD snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ipv6 enable ②
Yamaha(config-if)#ipv6 mld snooping ③
Yamaha(config-if)#ipv6 mld snooping querier ④
Yamaha(config-if)#ipv6 mld snooping query-interval 20 ⑤
```

① Define VLAN #10

② Enable the IPv6 function for VLAN #10

③ Enable MLD Snooping for VLAN #10

④ Enable the MLD query transmission function for VLAN #10

⑤ Set the MLD query transmission interval for VLAN #10 to 20 sec.

  - Since MLD snooping is enabled by default, we do not need to set this specifically.

2. [Switch #A] Set LAN ports #1–#2 as access ports, and associate them with VLAN #10.

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
```

```
①
```

① Configure the settings above for LAN port #2 as well.

3. [Switch #B] Define VLAN #10, and set MLD snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ipv6 enable ②
Yamaha(config-if)#ipv6 mld snooping ③
Yamaha(config-if)#no ipv6 mld snooping querier ④
Yamaha(config-if)#ipv6 mld snooping fast-leave ⑤
```

① Define VLAN #10

② Enable the IPv6 function for VLAN #10

③ Enable MLD Snooping for VLAN #10

④ Disable the MLD query transmission function for VLAN #10

⑤ Enable the MLD fast leave function for VLAN #10

- MLD snooping is enabled and the MLD query transmission function is disabled in default settings, so there is no need to specify those settings.

4. [Switch #B] Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

① Configure the settings above for LAN ports #2–#4 as well.

5. [Switch #B] Check the multicast router port information. (It should be connected to LAN port #1.)

```
Yamaha#show ipv6 mld snooping mrouter vlan10
VLAN    Interface             IP-address    Expires
10      port1.1(dynamic)         fe80::2a0:deff:feae:b879       00:00:43
```

6. [Switch #B] Check the multicast receiver information.

```
Yamaha#show ipv6 mld snooping groups
MLD Connected Group Membership
Vlan   Group Address                           Interface            Uptime   Expires
Last Reporter
10     ff15::1                                 port1.2              00:00:13 00:00:41
fe80::a00:27ff:fe8b:87e2
10     ff15::1                                 port1.4              00:00:02 00:00:48
fe80::a00:27ff:fe8b:87e4
```

Points of Caution

- If you want to change the handling of unknown multicast frames, use the l2-unknown-mcast command.
- When a topology change is detected, if you want to send a query regardless of the normal transmission interval, set the **l2-mcast snooping tcn-query** command.
- If the stack function is enabled, this will be **disabled** regardless of the MLD snooping settings.

Related Documentation

- Layer 2 Function: VLAN
- Layer 3 Functions: Basic IPv6 Settings

Traffic Control Functions

ACL

Function Overview

The access list (ACL) is a conditional statement that determines whether to permit or to deny the frame.
If the access list is applied to the interface, only the permitted frame will be transferred, and the denied frame will be discarded.
As this allows for only specified frames to be selected for transfer, this feature is primarily used for security purposes.
This product supports three access list types, as shown in the table below.

- Access list type

Access list type	Deciding criteria	Access list ID	Purpose of use
IPv4 access list	Source IPv4 address Destination IPv4 address IP protocol type	1–2000	Filters access from specific hosts and networks. Filters specific IP protocol types such as TCP/UDP.
IPv6 access list	Source IPv6 address	3001–4000	Filters access from specific hosts and networks.
MAC access list	Source MAC address Destination MAC address	2001–3000	Filters access and data transfer from specific devices.

Definition of Terms Used

ACL

Abbreviation of “**Access Control List**”.

Wildcard mask

Information that specifies which portion of the specified IPv4 address or MAC address is read. This is **used when specifying a range of IPv4 addresses or MAC addresses** as ACL conditions.

- When the wildcard mask bit is **“0”**: check the corresponding bit
- When the wildcard mask bit is **“1”**: do not check the corresponding bit

Examples of settings using wildcard masks are shown below. (The underlined portion is the wildcard mask.)

- To specify conditions for subnet **192.168.1.0/24**: **192.168.1.0 0.0.0.255** (specified in decimal)
- To specify conditions for vendor code **00-A0-DE---***: **00A0.DE00.0000 0000.00FF.FFFF** (specified in hexadecimal)

Function Details

Generate access list

Access lists for the number of IDs in each access list number can be generated. (Refer to the table in **1 Function Overview**.)
A **maximum of 256** control conditions can be registered per access list.
If the registered control conditions are not satisfied, forwarding occurs as usual.

Applying to the interface

The following table shows how access lists are applied to the input/output interfaces of this product.
Note that **one** access list can be applied to the IN and OUT respectively for an interface.

- Status of access list application to the interface

Access list type	LAN/SFP port		VLAN interface		Static/LACP logical interface	
	in	out	in	out	in	out
IPv4 access list	Yes	Yes (*)	Yes	Yes (*)	Yes	No
IPv6 access list	Yes	Yes	Yes	Yes	Yes	No
MAC access list	Yes	No	Yes	No	Yes	No

(*) As a limitation, an IPv4 access list that specifies a range of port numbers cannot be applied to the output (out) side of an interface.

The number of access lists that can be applied to the interface depends on the number of control parameters that are registered in the access lists.
On this product, a **maximum of 512** control conditions can be registered to the interface.
Applying an access list to the interface will use resources **“equivalent to the number of control conditions that are registered in the access list”**.

However, control conditions may also be used internally within the system in some cases, and use resources accordingly.

Settings for the LAN/SFP port and logical interface

The steps for applying an access list to a LAN/SFP port and to a logical interface are shown below.

1. Decide on the filtering parameters, and generate the access list.
    - Add explanatory text as necessary.
2. Check the access list.
3. Apply the access list to the LAN/SFP port and logical interface.
4. Check the applied access list.

A list of operation commands is given below.

- Access list operating commands (when applied to the LAN/SFP port and logical interface)

Access list type	Generate access list	Check access list	Apply access list	Check applied access list
IPv4 access list	**access-list**	**show access-list**	**access-group**	**show access-group**
IPv6 access list	**access-list**	**show access-list**	**access-group**	**show access-group**
MAC access list	**access-list**	**show access-list**	**access-group**	**show access-group**

VLAN interface settings

The steps for applying access lists to the VLAN interface are shown below.

1. Decide on the filtering parameters, and generate the access list.
    - Add explanatory text as necessary.
2. Check the access list.
3. Generate the VLAN access map.
4. Set the access list for the VLAN access map.
5. Check the VLAN access map.
6. Apply the VLAN access map to the VLAN.
7. Check the VLAN access map that was applied.

The operations in steps **1 and 2** are the same as those shown in 3.2.
The following is a list of operating commands for steps **3.** and later.

- VLAN access map operating command

Access list type	VLAN access map generation	Settings for access list used with VLAN access map	VLAN access map confirmation	VLAN access map application	Confirmation of the applied VLAN access map
IPv4 access list	**vlan access-map**	**match access-list**	**show vlan access-map**	**vlan filter**	**show vlan filter**
IPv6 access list	**vlan access-map**	**match access-list**	**show vlan access-map**	**vlan filter**	**show vlan filter**
MAC access list	**vlan access-map**	**match access-list**	**show vlan access-map**	**vlan filter**	**show vlan filter**

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Apply IPv4 access list	access-group
Generate IPv4 access list	access-list
Add IPv4 access list explanatory text	access-list description
Apply IPv4 access list	access-group
Generate IPv6 access list	access-list
Add IPv6 access list explanatory text	access-list description
Apply IPv6 access list	access-group
Generate MAC access list	access-list
Add MAC access list explanatory text	access-list description

Operations	Operating commands
Apply MAC access list	access-group
Show generated access list	show access-list
Show access list applied to interface	show access-group
Create VLAN access map	vlan access-map
Set VLAN access map parameters	match
Assign VLAN access map to VLAN	vlan filter
Show VLAN access map	show vlan access-map
Show VLAN access map filter	show vlan filter

Examples of Command Execution

IPv4 access list settings

Example of application to a LAN port

■ Specify host

Set **LAN port #1** so that access is only permitted from host: **192.168.1.1** to host: **10.1.1.1**.
With **#123** as the access list ID, add **IPV4-ACL-EX** as access list explanatory text using.

1. Generate and confirm **access list #123**.

```
Yamaha(config)#access-list 123 permit any host 192.168.1.1 host 10.1.1.1 ①
Yamaha(config)#access-list 123 deny any any any
Yamaha(config)#access-list 123 description IPV4-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ③
IPv4 access list 123
    10 permit any host 192.168.1.1 host 10.1.1.1
    20 deny any any any
Yamaha#
```

① Generate access list

② Add access list explanatory text

③ Check access list

2. Apply **access list #123** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 123 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv4 access group 123 in
```

① Apply access list

② Check access list settings

To change the access list (delete or add a setting), application of the list to the LAN port must be temporarily canceled.
For the setting indicated above, delete the setting that allows access from host: **192.168.1.1** to host: **10.1.1.1** and add a setting that allows access from host: **192.168.1.1** to host: **10.1.1.2**.

1. Temporarily cancel the application of **access list #123** from **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#no access-group 123 in ①
```

① Cancel the application of the access list

2. Delete, add, and then check the setting in **access list #123**.

```
Yamaha(config)#no access-list 123 10 ①
Yamaha(config)#access-list 123 10 permit any host 192.168.1.1 host 10.1.1.2 ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ③
IPv4 access list 123
    10 permit any host 192.168.1.1 host 10.1.1.2
    20 deny any any any
```

① Remove the setting from the access list

② Add the setting to the access list

③ Check access list

3. Apply **access list #123** to **LAN port #1** again.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 123 in ①
```

① Apply access list

■ Specify network

Set **LAN port #1** so that access is only permitted from network: **192.168.1.0/24** to host: **10.1.1.1**.
With **#123** as the access list ID, add **IPV4-ACL-EX** as access list explanatory text using.

1. Generate and confirm **access list #123**.

```
Yamaha(config)#access-list 123 permit any 192.168.1.0 0.0.0.255 host 10.1.1.1 ①
Yamaha(config)#access-list 123 deny any any any
Yamaha(config)#access-list 123 description IPV4-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show ip access-list ③
IPv4 access list 123
    10 permit any 192.168.1.0/24 host 10.1.1.1
    20 deny any any any
```

```
Yamaha#
```

① Generate access list

② Add access list explanatory text

③ Check ACL

2. Apply **access list #123** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 123 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv4 access group 123 in
```

① Apply access list

② Check access list settings

To change the access list (delete or add a setting), application of the list to the LAN port must be temporarily canceled.
The specific procedure is the same as for specifying a host.

Example of application to the VLAN interface

■ Specify host

Set **VLAN #1000** so that access is only permitted from host: **192.168.1.1** to host: **10.1.1.1**.

We will use access list ID **#123**.
The VLAN access map to be used will be **VAM-002**, and **access list #123** will be set.

1. Generate and confirm **access list #123**.

```
Yamaha(config)#access-list 123 permit any host 192.168.1.1 host 10.1.1.1 ①
Yamaha(config)#access-list 123 deny any any any
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ②
IPv4 access list 123
    10 permit any host 192.168.1.1 host 10.1.1.1
    20 deny any any any
```

① Generate access list

② Check access list

2. Generate **VLAN access map VAM-002**, and set **access list #123**.

```
Yamaha(config)#vlan access-map VAM-002 ①
Yamaha(config-vlan-access-map)#match access-list 123 ②
Yamaha(config-vlan-access-map)#end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-002
```

```
    match ipv4 access-list 123
```

① VLAN access map generation

② Register the access list

③ Check the settings for VLAN access map and access list

3. Apply **VLAN access map VAM-002** to **VLAN #1000**, and confirm the status.

```
Yamaha(config)#vlan filter VAM-002 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-002 is applied to vlan 1000 in
```

① Apply the VLAN access map to the VLAN

② Check the settings for VLAN access map

To change the access list (delete or add a setting), it is necessary to temporarily cancel applying the list to the VLAN interface and the setting in the VLAN access map.
For the setting indicated above, delete the setting that allows access from host: **192.168.1.1** to host: **10.1.1.1** and add a setting that allows access from host: **192.168.1.1** to host: **10.1.1.2**.

1. Temporarily cancel **VLAN access map VAM-002** from being applied to **VLAN #1000**.

```
Yamaha(config)#no vlan filter VAM-002 1000 in ①
```

① Cancel the application of a VLAN access map from a VLAN

2. Temporarily cancel the **access list #123** setting in **VLAN access map VAM-002**.

```
Yamaha(config)#vlan access-map VAM-002 ①
Yamaha(config-vlan-access-map)#no match access-list 123 ②
```

① Change the VLAN access map

② Cancel the registration of access list

3. Delete, add, and then check the setting in **access list #123**.

```
Yamaha(config)#no access-list 123 10 ①
Yamaha(config)#access-list 123 10 permit any host 192.168.1.1 host 10.1.1.2 ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ③
IPv4 access list 123
    10 permit any host 192.168.1.1 host 10.1.1.2
    20 deny any any any
```

① Remove the setting from the access list

② Add the setting to the access list

③ Check access list

4. Specify the **access list #123** setting in **VLAN access map VAM-002** again.

```
Yamaha(config)#vlan access-map VAM-002 ①
Yamaha(config-vlan-access-map)#match access-list 123 ②
```

① Change the VLAN access map

② Register the access list

5. Apply **VLAN access map VAM-002** to **VLAN #1000** again.

```
Yamaha(config)#vlan filter VAM-002 1000 in ①
```

① Apply the VLAN access map to the VLAN

■ Specify network

Set **VLAN #1000** so that access is only permitted from network: **192.168.1.0/24** to host: **10.1.1.1**.

We will use access list ID **#123**.
The VLAN access map to be used will be **VAM-002**, and **access list #123** will be set.

1. Generate and confirm **access list #123**.

```
Yamaha(config)#access-list 123 permit any 192.168.1.0 0.0.0.255 host 10.1.1.1 ①
Yamaha(config)#access-list 123 deny any any any
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ②
IPv4 access list 123
    10 permit any 192.168.1.0/24 host 10.1.1.1
    20 deny any any any
```

① Generate access list

② Check access list

2. Generate **VLAN access map VAM-002**, and set **access list #123**.

```
Yamaha(config)#vlan access-map VAM-002 ①
Yamaha(config-vlan-access-map)#match access-list 123 ②
Yamaha(config-vlan-access-map)#end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-002
    match ipv4 access-list 123
```

① VLAN access map generation

② Register the access list

③ Check the settings for VLAN access map and access list

3. Apply **VLAN access map VAM-002** to **VLAN #1000**, and confirm the status.

```
Yamaha(config)#vlan filter VAM-002 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-002 is applied to vlan 1000 in
```

① Apply the VLAN access map to the VLAN

② Check the settings for VLAN access map

To change the access list (delete or add a setting), it is necessary to temporarily cancel applying the list to the VLAN interface and the setting in the VLAN access map.
The specific procedure is the same as for specifying a host.

Allowing only TCP communication from one direction (example using TCP flags)

Given VLAN10 and VLAN20, this example controls TCP communication so that it occurs in one direction.

- Communication from VLAN10 to VLAN20 is possible by Telnet, etc.
- Communication from VLAN20 to VLAN10 is not possible by Telnet, etc.

1. Generate **access list #1**.
   Specify settings that only allow IPv4 TCP packets with an **ACK** or **RST** flag.

```
Yamaha(config)#access-list 1 permit tcp any any ack ①
Yamaha(config)#access-list 1 permit tcp any any rst
Yamaha(config)#access-list 1 deny any any any
Yamaha(config)#end
Yamaha#
Yamaha#show access-list ②
IPv4 access list 1
    10 permit tcp any any ack
    20 permit tcp any any rst
    30 deny any any any
```

   ① Configure access list settings

   ② Check access list settings

2. Generate **VLAN access map VAM-ESTABLISHED** and specify **access list #1**.

```
Yamaha(config)#vlan access-map VAM-ESTABLISHED ①
Yamaha(config-vlan-access-map)#match access-list 1 ②
Yamaha(config-vlan-access-map)#end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-ESTABLISHED
    match ipv4 access-list 1
```

   ① VLAN access map generation

   ② Register the access list

   ③ Check the settings for VLAN access map

3. Apply **VLAN access map VAM-ESTABLISHED** to **VLAN #20**.

```
Yamaha(config)#vlan filter VAM-ESTABLISHED 20 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-ESTABLISHED is applied to vlan 20 in
```

① Apply the VLAN access map to the VLAN

② Check the status of application to the VLAN

IPv6 access list settings

Example of application to a LAN port

■ Specify host

Set **LAN port #1** so that it only allows access from host: **2001:db8::1**.
With **#3001** as the access list ID, add **IPV6-ACL-EX** as access list explanatory text using.

1. Generate and confirm **access list #3001**.

```
Yamaha(config)#access-list 3001 permit 2001:db8::1/128 ①
Yamaha(config)#access-list 3001 deny any
Yamaha(config)#access-list 3001 description IPV6-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 3001 ③
IPv6 access list 3001
    10 permit 2001:db8::1/128
    20 deny any
```

① Generate access list

② Add access list explanatory text

③ Check access list

2. Apply **access list #3001** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 3000 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv6 access group 3001 in
```

① Apply access list

② Check access list settings

To change the access list (delete or add a setting), application of the list to the LAN port must be temporarily canceled.
For the specific procedure, refer to **Example of application to a LAN port** in **IPv4 access list settings**.

■ Specify network

Set **LAN port #1** so that it only allows access from network: **2001:db8::/64**.
With **#3001** as the access list ID, add **IPV6-ACL-EX** as access list explanatory text using.

1. Generate and confirm **access list #3001**.

```
Yamaha(config)#access-list 3001 permit 2001:db8::/64 ①
Yamaha(config)#access-list 3001 deny any
Yamaha(config)#access-list 3001 description IPV6-ACL-EX ②
Yamaha(config)#end

Yamaha# show access-list 3001 ③
IPv6 access list 3001
    10 permit 2001:db8::/64
    20 deny any
```

① Generate access list

② Add access list explanatory text

③ Check access list

2. Apply **access list #3001** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 3001 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv6 access group 3001 in
```

① Apply access list

② Check access list settings

To change the access list (delete or add a setting), application of the list to the LAN port must be temporarily canceled.
For the specific procedure, refer to **Example of application to a LAN port** in **IPv4 access list settings**.

Example of application to the VLAN interface

■ Specify host

Set **VLAN #1000** so that it only allows access from host: **2001:db8::1**.

We will use access list ID **#3001**.
The VLAN access map to be used will be **VAM-001**, and **access list #3001** will be set.

1. Generate and confirm **access list #3001**.

```
Yamaha(config)#access-list 3001 permit 2001:db8::1/128 ①
Yamaha(config)#access-list 3001 deny any
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 3001 ②
IPv6 access list 3001
    10 permit 2001:db8::1/128
    20 deny any
```

① Generate access list

② Check access list

2. Generate **VLAN access map VAM-001**, and set **access list #3001**.

```
Yamaha(config)#vlan access-map VAM-001 ①
Yamaha(config-vlan-access-map)#match access-list 3001 ②
Yamaha(config-vlan-access-map)#end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-001
    match ipv6 access-list 3001
```

① VLAN access map generation

② Configure access list settings

③ Check the settings for VLAN access map and access list

3. Apply **VLAN access map VAM-001** to **VLAN #1000**, and confirm the status.

```
Yamaha(config)#vlan filter VAM-001 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-001 is applied to vlan 1000 in
```

① Apply the VLAN access map to the VLAN

② Check the settings for VLAN access map

To change the access list (delete or add a setting), it is necessary to temporarily cancel applying the list to the VLAN interface and the setting in the VLAN access map.
For the specific procedure, refer to **Example of application to the VLAN interface** in **IPv4 access list settings**.

■ Specify network

Set **VLAN #1000** so that it only allows access from network: **2001:db8::/64**.

We will use access list ID **#3001**.
The VLAN access map to be used will be **VAM-001**, and **access list #3001** will be set.

1. Generate and confirm **access list #2**.

```
Yamaha(config)#access-list 3001 permit 2001:db8::/64 ①
Yamaha(config)#access-list 3001 deny any
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 3001 ②
IPv6 access list 3001
    10 permit 2001:db8::/64
    20 deny any
```

① Generate access list

② Check access list

2. Generate **VLAN access map VAM-001**, and set **access list #3001**.

```
Yamaha(config)#vlan access-map VAM-001 ①
Yamaha(config-vlan-access-map)#match access-list 3001 ②
Yamaha(config-vlan-access-map)#end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-001
    match ipv6 access-list 3001
```

① VLAN access map generation

② Configure access list settings

③ Check the settings for VLAN access map and access list

3. Apply **VLAN access map VAM-001** to **VLAN #1000**, and confirm the status.

```
Yamaha(config)#vlan filter VAM-001 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-001 is applied to vlan 1000 in
```

① Apply the VLAN access map to the VLAN

② Check the settings for VLAN access map

To change the access list (delete or add a setting), it is necessary to temporarily cancel applying the list to the VLAN interface and the setting in the VLAN access map.
For the specific procedure, refer to **Example of application to the VLAN interface** in **IPv4 access list settings**.

MAC access list settings

Example of application to a LAN port

■ Specify host

Set **LAN port #1** so that it only denies access from host: **00-A0-DE-12-34-56**.
With **#2001** as the access list ID, add **MAC-ACL-EX** as access list explanatory text using.

1. Generate and confirm **access list #2001**.

```
Yamaha(config)#access-list 2001 deny host 00a0.de12.3456 any ①
Yamaha(config)#access-list 2001 description MAC-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 2001 ③
MAC access list 2001
    10 deny host 00A0.DE12.3456 any
```

① Generate access list

② Add access list explanatory text

③ Check access list

2. Apply **access list #2001** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 2001 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : MAC access group 2001 in
```

① Apply access list

② Check access list settings

To change the access list (delete or add a setting), application of the list to the LAN port must be temporarily canceled.
For the specific procedure, refer to **Example of application to a LAN port** in **IPv4 access list settings**.

■ Specify vendor

Set **LAN port #1** so that it only denies access from vendor code: **00-A0-DE---*** (00-A0-DE-00-00-00 to 00-A0-DE-FF-FF-FF).
With **#2001** as the access list ID, add **MAC-ACL-EX** as access list explanatory text using.

1. Generate and confirm **access list #2001**.

```
Yamaha(config)#access-list 2001 deny 00a0.de00.0000 0000.00ff.ffff any ①
Yamaha(config)#access-list 2001 description MAC-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 2001 ③
MAC access list 2001
    10 deny 00A0.DE00.0000 0000.00FF.FFFF any
```

① Generate access list

② Add access list explanatory text

③ Check access list

2. Apply **access list #2001** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 2001 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : MAC access group 2001 in
```

① Apply access list

② Check access list settings

To change the access list (delete or add a setting), it is necessary to temporarily cancel applying the list to the VLAN interface and the setting in the VLAN access map.
For the specific procedure, refer to **Example of application to a LAN port** in **IPv4 access list settings**.

Example of application to the VLAN interface

■ Specify host

Set **VLAN #1000** so that it only denies access from host: **00-A0-DE-12-34-56**.

With **#2001** as the access list ID, add **MAC-ACL-EX** as access list explanatory text using.
The VLAN access map to be used will be **VAM-003**, and **access list #2001** will be set.

1. Generate and confirm **access list #2000**.

```
Yamaha(config)#access-list 2001 deny host 00a0.de12.3456 any ①
Yamaha(config)#access-list 2001 description MAC-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list ③
MAC access list 2001
    10 deny host 00A0.DE12.3456 any
```

① Generate access list #2001

② Add access list explanatory text

③ Check access list

2. Generate **VLAN access map VAM-003**, and set **access list #2001**.

```
Yamaha(config)# vlan access-map VAM-003 ①
Yamaha(config-vlan-access-map)# match access-list 2001 ②
Yamaha(config-vlan-access-map)# end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-003
    match mac access-list 2001
```

① VLAN access map generation

② Register the access list

③ Check the settings for VLAN access map and access list

3. Apply **VLAN access map VAM-003** to **VLAN #1000**, and confirm the status.

```
Yamaha(config)#vlan filter VAM-003 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-003 is applied to vlan 1000 in
```

① Apply the VLAN access map to the VLAN

② Check the settings for VLAN access map

To change the access list (delete or add a setting), it is necessary to temporarily cancel applying the list to the VLAN interface and the setting in the VLAN access map.
For the specific procedure, refer to **Example of application to the VLAN interface** in **IPv4 access list settings**.

■ Specify vendor

Set **VLAN #1000** so that it only denies access from vendor code: **00-A0-DE---*** (00-A0-DE-00-00-00 to 00-A0-DE-FF-FF-FF).
With **#2001** as the access list ID, add **MAC-ACL-EX** as access list explanatory text using.
The VLAN access map to be used will be **VAM-003**, and **access list #2001** will be set.

1. Generate and confirm **access list #2001**.

```
Yamaha(config)#access-list 2001 deny 00a0.de00.0000 0000.00ff.ffff any ①
Yamaha(config)#access-list 2001 description MAC-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 2001 ③
MAC access list 2001
    10 deny 00A0.DE00.0000 0000.00FF.FFFF any
```

① Generate access list #2001

② Add access list explanatory text

③ Check access list

2. Generate **VLAN access map VAM-003**, and set **access list #2001**.

```
Yamaha(config)# vlan access-map VAM-003 ①
Yamaha(config-vlan-access-map)# match access-list 2001 ②
Yamaha(config-vlan-access-map)# end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-003
    match mac access-list 2001
```

① VLAN access map generation

② Register the access list

③ Check the settings for VLAN access map and access list

3. Apply **VLAN access map VAM-003** to **VLAN #1000**, and confirm the status.

```
Yamaha(config)#vlan filter VAM-003 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-003 is applied to vlan 1000 in
```

① Apply the VLAN access map to the VLAN

② Check the settings for VLAN access map

To change the access list (delete or add a setting), it is necessary to temporarily cancel applying the list to the VLAN interface and the setting in the VLAN access map.
For the specific procedure, refer to **Example of application to the VLAN interface** in **IPv4 access list settings**.

Points of Caution

- LAN/SFP ports for which an access list is configured for received frames cannot belong to a logical interface.

- Access list settings for received frames on an interface cannot be applied to a LAN/SFP port that belongs to a logical interface. If access list settings exist for the received frame of a LAN/SFP port that belongs to a logical interface in startup config, the settings for the most recent port number will be applied to the logical interface.
- Conditions might not be determined correctly for fragment packets. Specifically, if layer 4 information (source port number, destination port number, and various TCP flags) is included in the conditions, correct information cannot be determined because the information is not included in the second and subsequent fragment packets. If there is a possibility of processing fragment packets, do not include layer 4 information in the conditions.

Related Documentation

- Layer 2 Function: VLAN

QoS

Function Overview

QoS (Quality of Service) is a technology for reserving a specified bandwidth for communications over a network, guaranteeing a fixed speed of communication.
Application data is classified and grouped, and then forwarded by group priority level, referring to the DSCP in the IP header or the CoS in the IEEE802.1Q tag.

Definition of Terms Used

CoS (IEEE 802.1p Class of Service)

This expresses priority as a 3-bit field in the VLAN tag header, with a value from 0–7.
Also called 802.1p user priority.

IP Precedence

This expresses priority as a 3-bit field in the TOS field of the IP header, with a value from 0–7.
Used to indicate the traffic class of the frame in question, for the device that receives the frame.

DSCP (Diffserv Code Point)

This expresses priority as a 6-bit field in the TOS field of the IP header, with a value from 0–63.
Since DSCP uses the same TOS field as IP precedence, it is compatible with IP-Precedence.
Used to indicate the traffic class of the frame in question, for the device that receives the frame.

Default CoS

This is the CoS value that is assigned to an untagged frame for the purpose of internal processing.

Transmission queue

This product has eight transmission queues per port. The transmission queues are numbered from ID 0–7, with larger ID numbers being given higher priority.

Trust mode

This indicates what will be the basis for deciding (trusting) the transmission queue ID.
The CoS value or DSCP value of the received frames can be used to differentiate them, or a priority order specified for each receiving port can be applied.
Settings can be configured for each LAN/SFP port and logical interface. Note that the settings for LAN/SFP ports that belong to a logical interface cannot be changed.
The default status (when QoS is enabled) is set to “CoS”.

Transmission queue ID conversion table

This is a conversion table used when deciding on the transmission queue ID from either the CoS value or the DSCP value.
There are two kinds of transmission queue ID conversion tables, the CoS-transmission queue ID conversion table and the DSCP-transmission queue ID conversion table. Each kind is used with its own trust mode.
Mapping can be freely changed by the user.

Port priority

This is the priority order assigned for each reception port. If the trust mode is “port priority,” frames received at that port are placed in the transmission queue according to the port’s priority setting.

Class map

This defines the conditions by which packets are classified into traffic classes.
Packets can be associated and used with policy maps, and QoS processing (pre-marking, transmission queue specification, metering/policing/remarking) per traffic class can be defined.

Policy map

This is an element for performing a QoS processing series on the receiving port. This cannot be used by itself, but rather is associated and used with 1–8 class maps.
When a policy map is applied to a LAN/SFP port and logical interface, traffic is classified per class map that is associated with the policy map for the packets received on the relevant port.
Also, QoS processing (pre-marking, transmission queue specification, metering/policing/remarking) set per traffic class can be performed.

Policer

This is a group series of metering/policing/remarking settings.
There are two types of policers, an individual policer for metering that targets one traffic class, and a group policer that meters multiple traffic classes by putting them together.

Function Details

Enabling or disabling QoS control

When shipped from the factory, the QoS control of this product is set to **disable**.

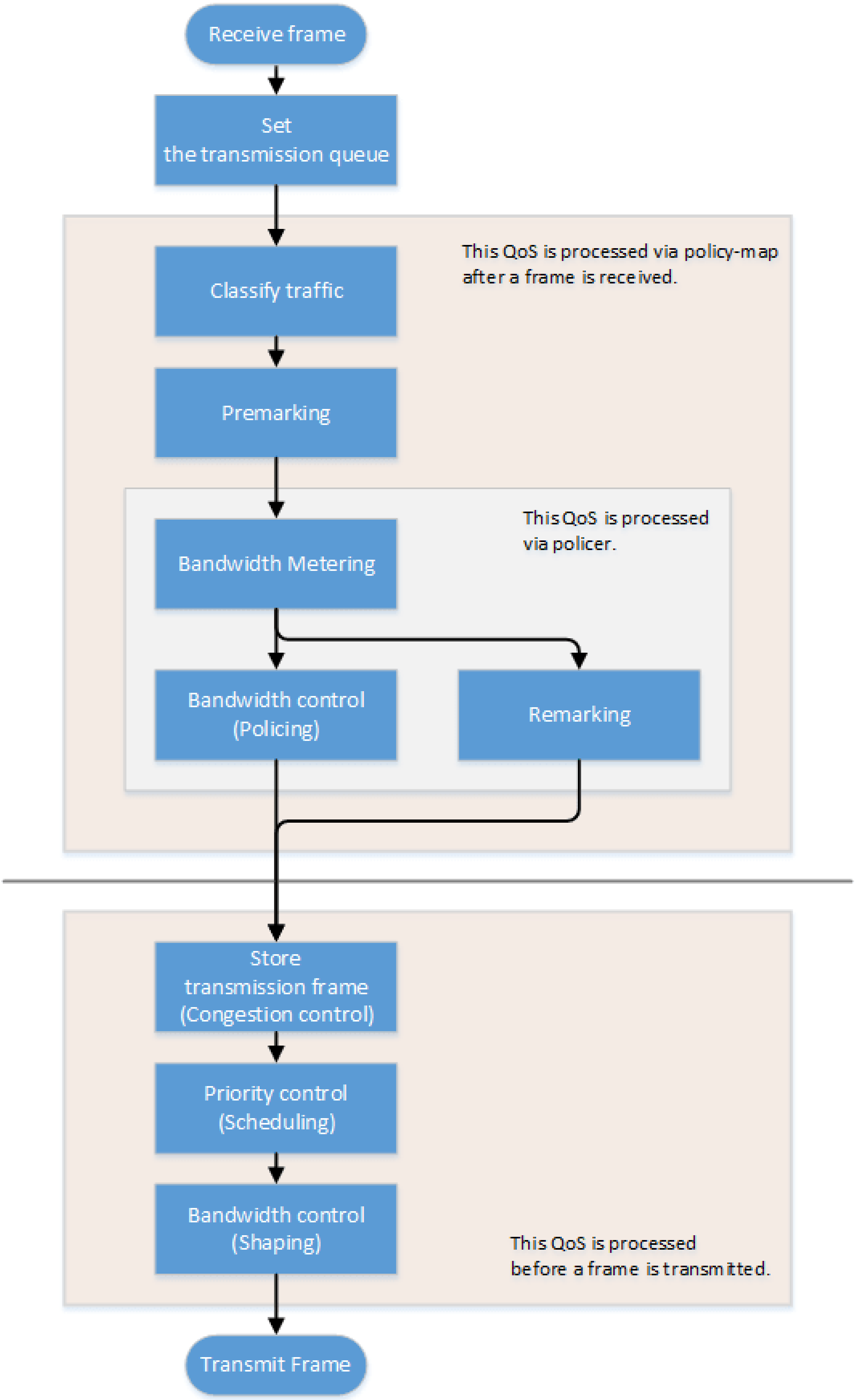
To enable QoS control, use the **qos enable** command. To disable this, use the **no qos** command.

Most QoS control commands cannot be executed if QoS is not enabled.

The QoS function status can be checked using the **show qos** command.
In order to enable QoS control, the system’s flow control must be disabled.

QoS processing flow

The QoS processing flow is shown below.


Receive frame
Set the transmission queue
Classify traffic
This QoS is processed via policy-map after a frame is received.
Premarking
Bandwidth Metering
This QoS is processed via policer.
Bandwidth control (Policing)
Remarking
Store transmission frame (Congestion control)
Priority control (Scheduling)
Bandwidth control (Shaping)
This QoS is processed before a frame is transmitted.
Transmit Frame

Transmission queue assignments

When this product receives a frame, it determines the initial value of the transmission queue ID according to the **CoS value or DSCP value** within the frame and the **port priority** of the reception port.
Of the factors such as the frame's CoS value, DSCP value, and port priority, the port's **trust mode** determines which factor will be the basis for determining the transmission queue.

The **trust mode** can be changed by the **qos trust** command. The default value (when QoS is enabled) is set to **CoS**.

The transmission queue is assigned per **trust mode**, using the following rules.

- When trust mode is "CoS"
  - When the received frame is a frame with a VLAN tag, the CoS value within the tag is used to determine the transmission queue ID.
  - When the received frame is a frame without a VLAN tag, the **default CoS** that is managed by this product is used to determine the transmission queue ID.
    The default setting (when QoS is enabled) and the **default CoS** are set to "**0**". The setting can be changed using the **qos cos** command.
  - Conversion from the CoS value to the transmission queue ID is performed by the CoS-transmission queue ID conversion table.
    One such table is maintained by the system, and with the default settings (when QoS is enabled), the settings are as follows. The setting can be changed using the **qos cos-queue** command.

CoS value	Transmission queue ID	Traffic Type
0	2	Best Effort
1	0	Background
2	1	Standard(spare)
3	3	Excellent Effort(Business Critical)
4	4	Controlled Load(Streaming Multimedia)
5	5	Video(Interactive Media) less than 100 msec latency and jitter
6	6	Voice(Interactive Media) less than 10 msec latency and jitter
7	7	Network Control(Reserved Traffic)

- When trust mode is "DSCP"
  - The DSCP value in the IP header is used to determine the transmission queue ID.
  - Conversion from the DSCP value to the transmission queue ID is performed by the DSCP-transmission queue ID conversion table.
    One such table is maintained by the system, and with the default settings (when QoS is enabled), the settings are as follows. The setting can be changed using the **qos dscp-queue** command.

DSCP value	Transmission queue ID	Traffic Type
0 - 7	2	Best Effort
8 –15	0	Background
16 - 23	1	Standard(spare)
24 - 31	3	Excellent Effort(Business Critical)
32 - 39	4	Controlled Load(Streaming Multimedia)
40 - 47	5	Video(Interactive Media) less than 100 msec latency and jitter
48 - 55	6	Voice(Interactive Media) less than 10 msec latency and jitter

DSCP value	Transmission queue ID	Traffic Type
56 - 63	7	Network Control(Reserved Traffic)

- When trust mode is “port priority”
  - The transmission queue ID is determined by the **port priority**.
  - By default (when QoS is enabled), **port priority** is set to **2**. The setting can be changed using the **qos port-priority-queue** command.

If the trust mode is “CoS” or “DSCP,” the transmission queue ID might be reassigned due to QoS processing (see below) by the policy map.
In this case, the new transmission queue ID is reassigned based on the transmission queue ID conversion table that corresponds to the port’s trust mode.

- Pre-marking
  - Refer to “**Pre-marking**” for details.
- Specify transmission queue
  - When the trust mode is “CoS”, specify the CoS value that corresponds to the transmission queue ID, using the **set cos-queue** command.
  - When the trust mode is “DSCP”, specify the DSCP value that corresponds to the transmission queue ID, using the **set dscp-queue** command.
- Remark
  - Refer to **Metering/policing/remarking** for details.

If the trust mode is “port priority,” the transmission queue ID cannot be changed by the policy map’s QoS processing. (It is not possible to apply a policy map that includes pre-marking, transmission queue specification, and remarking settings.)

Transmission queue assignments (frames sent from the network switch unit)

As an exception to the transmission queue assignments, frames sent from the network switch unit (CPU) are automatically assigned **the transmission queue determined by the system**. (They are not given transmission queue assignments based on the **trust mode**.)
The **qos queue sent-from-cpu** command can be used to change the transmission queue that is assigned, and by default the transmission queue ID is set to **7**.

Traffic classification

Traffic classification is a function to classify received frames, based on a **class map** that defines the conditions of the IP header, TCP header, and so on.
The conditions that can be classified and the commands for settings are shown in the table below.

- Conditions that can be classified, and commands for settings

Classification condition	Condition-setting command	Class map setting command	Number that can be registered per class map
Source/destination MAC address	**access-list** (*Note 3)	**match access-list**	1
Source/destination IP address			1
IP protocol type (*Note 1)			1
Ethernet frame type number	**match ethertype**		1
CoS value for VLAN tag header	**match cos**		8
Precedence value for IP header	**match ip-precedence**		8
DSCP value for IP header	**match ip-dscp**		8
VLAN ID (*Note 2)	**match vlan, match vlan-range**		30

(*Note 1) IPv6 is not subject to classification by IP protocol type.

(*Note 2) Does not include isolated or community VLANs in a private VLAN.
(*Note 3) **Up to 39** conditions can be set in the access list for traffic classification.

- Traffic is classified per **class map**.
- **One** classification condition type can be set for one **class map**. Policer-based QoS processing (metering/policing/remarking) and pre-marking, as well as specifying the transmission queue can be done for frames that match the conditions.
- If classification conditions are not specified, all frames are classified into the corresponding traffic class.
- For classification based on CoS, IP precedence, DSCP, and the VLAN ID, multiple classifications can be made for one class map.
- Associating multiple **class maps** to a **policy map** will make it possible to classify complex traffic for the receiving port. **Up to eight class maps** can be associated to one **policy map**.
- Information for the **class map** that was set can be confirmed using the **show class-map** command.
- Information for the **policy map** that was set can be confirmed using the **show policy-map** command.
- Use the **show qos map-status** command to check the port to which the **policy map** is applied, and the policy map to which the **class map** is associated.

Pre-marking

Pre-marking is a function to change (assign) the CoS, IP precedence, and DSCP values for received frames classified into traffic classes.
Pre-marking is set using the policy map and class mode commands shown below.

- Pre-marking setting commands

Pre-marking target	Command for settings
CoS	**set cos**
IP Precedence	**set ip-precedence**

Pre-marking target	Command for settings
DSCP	**set ip-dscp**

- The DSCP values that can be premarked include **the value recommended in the RFC** and those not found in the RFC, for **a total of four**. (This rule also applies to DSCP values that are used in remarking.)
- **Only one** pre-marking setting can be made for a **class map**. This cannot be used together when specifying a transmission queue (set cos-queue, set ip-dscp-queue).
- When pre-marking, the transmission queue will be reassigned based on the changed value and the **transmission queue ID conversion table** that corresponds to the trust mode.

Metering/policing/remarking

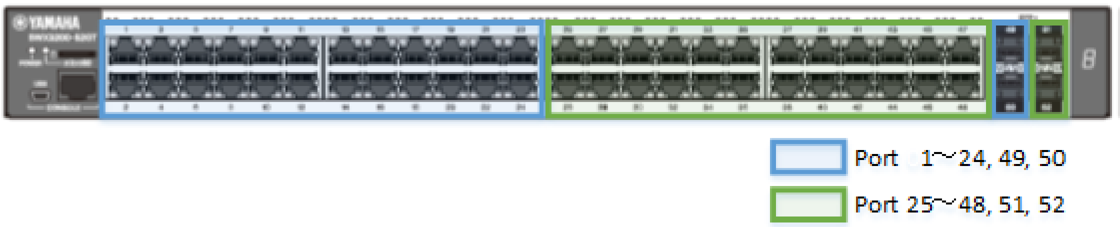
Bandwidth can be controlled by measuring the bandwidth used, and discarding or reprioritizing packets according to the measurement results.
The processing series for metering, policing and remarking is done per "**policer**".

- Processing summary for bandwidth control

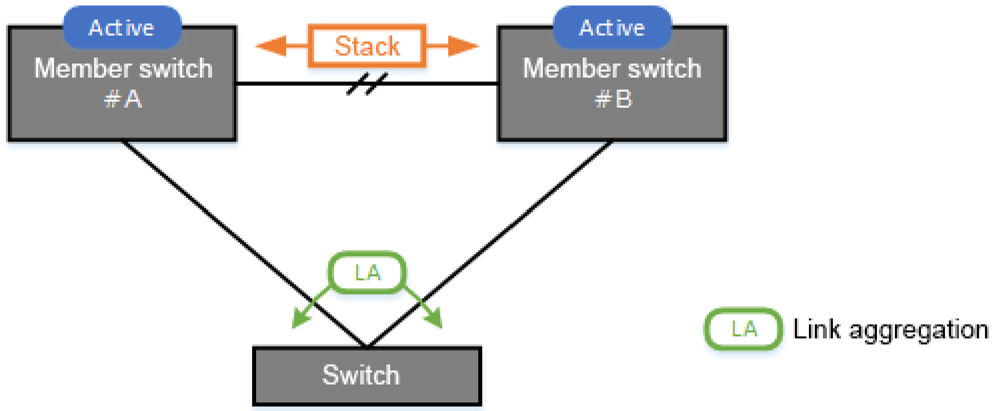
Process name	Summary
Metering	This measures how much bandwidth is being taken up by the classified traffic based on the traffic rate and burst size, and classifies this into three bandwidth classes (green, yellow and red). Actions such as discarding (policing) and remarking can be specified for each classified bandwidth class.
Policing	The bandwidth usage can be kept within a certain amount by discarding frames, using bandwidth class information.
Remark	The CoS, IP precedence, and DSCP values for a frame can be changed using the bandwidth class information.

Metering, policing, and remarking cannot be performed for the following logical interfaces.

1. Logical interfaces grouped by Ports 1 to 24, 49, and 50 (ports in the blue frame below) and Ports 25 to 48, 51, and 52 (ports in the green frame below) on SWX3200-52GT



2. Logical interface grouped across the member switches that make up the stack (green I/F below)



Policer types

There are two types of policers: an **individual policer** that performs metering/policing/remarking on one traffic class, and an **aggregate policer** that performs these actions on multiple aggregated traffic classes.

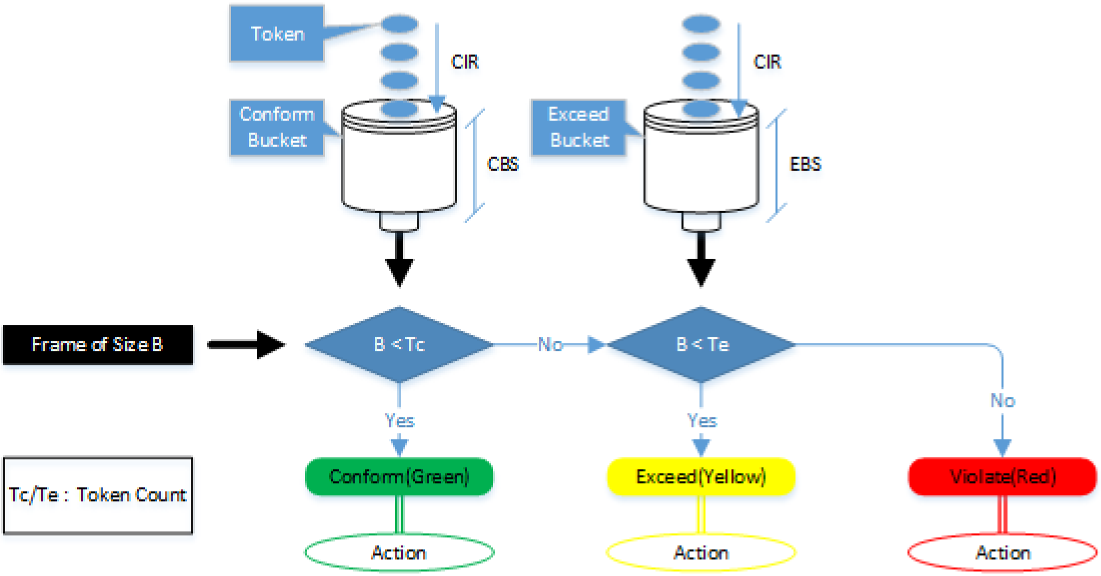
- **Individual policer**
  Metering/policing/remarking is done per traffic class.
  The settings are specified using **police** and **remark-map** commands in the policy map/class mode.
- **Aggregate policer**
  Metering/policing/remarking is done on multiple traffic classes, which are aggregated.
  The aggregate policer can be created using the **aggregate-police** command, and the content can be specified by the aggregate policer mode's **police** command and **remark-map** command.
  To apply a created aggregate policer to a traffic class, use the **police-aggregate** command.
- The commands used to make settings for an **individual policer** and an **aggregate policer** respectively are as follows.

Content of setting	Individual policer	Aggregate policer
Create policer	-	**aggregate-police**
Policer settings (Metering/policing/remarking)	**police single-rate, police twin-rate** (Policy map class mode)	**police single-rate, police twin-rate** (Aggregate policer mode)
Apply policer to traffic class		**police-aggregate**
Detailed remarking settings	**remark-map** (Policy map/class mode)	**remark-map** (Aggregate policer mode)

Metering settings

There are two types of metering: **single rate policer** (RFC2697) and **twin rate policer** (RFC2698).
The type of metering to use and the control parameters are specified using the **police** command (policy map/class mode or aggregate policer mode).

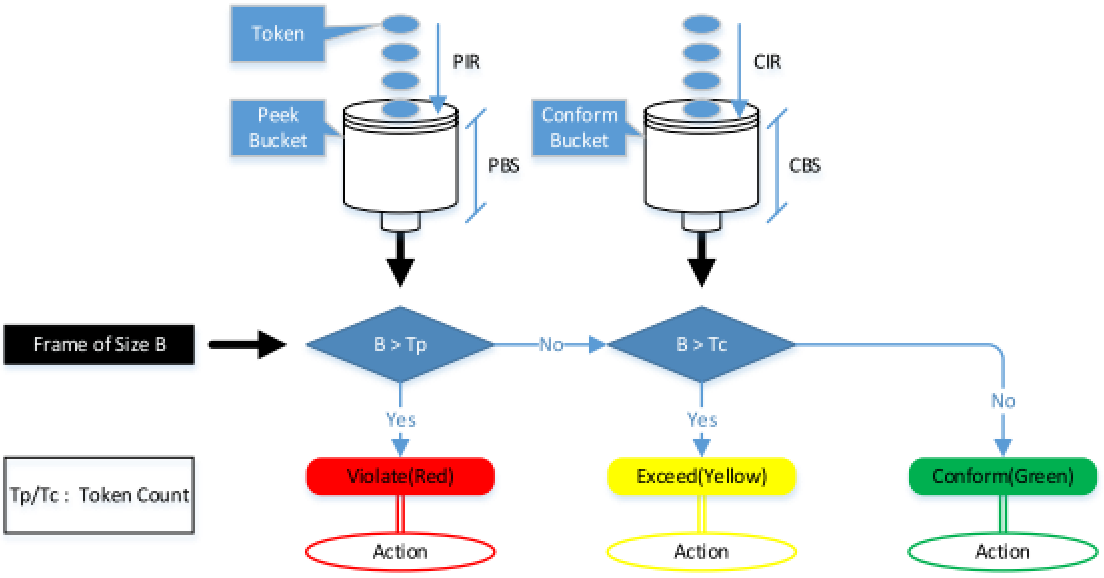
- Single rate policer (RFC2697)
  Single rate policers separate the frames within a traffic class into three bandwidth classes: **"green" (conforming)**, **"yellow" (exceeding)** or **"red" (violating)**, based on the **traffic rate (CIR)** and **burst size (CBS, EBS)**.



- Single rage policer control parameters
  If the burst size was not set appropriately, the throughput might decrease in some cases.

Parameter	Explanation
CIR (Committed Information Rate)	This is the amount of tokens that is periodically stored in buckets. The amount can be specified in the range of 1–102,300,000 kbps.
CBS (Committed Burst Size)	This is the amount of traffic that can be removed at one time from the first token bucket (a conforming token bucket). The amount can be specified in the range of 11–2,097,120 kByte.
EBS (Exceed Burst Size)	This is the amount of traffic that can be removed at one time from the second token bucket (an exceeding token bucket). The amount can be specified in the range of 11–2,097,120 kByte.

- Twin rate policer (RFC2698)
  Twin rate policers separate the frames within a traffic class into three bandwidth classes: **“green” (conforming)**, **“yellow” (exceeding)** or **“red” (violating)**, based on the **traffic rate (CIR, PIR)** and **burst size (CBS, PBS)**.



- Twin rage policer control parameters
  If the burst size was not set appropriately, the throughput might decrease in some cases.

Parameter	Explanation
CIR (Committed Information Rate)	This is the amount of tokens periodically stored in the second token bucket (confirming token bucket). The amount can be specified in the range of 1–102,300,000 kbps.
PIR (Peak Information Rate)	This is the amount of tokens periodically stored in the first token bucket (peak token bucket). The amount can be specified in the range of 1–102,300,000 kbps. However, a value smaller than the CIR cannot be specified.
CBS (Committed Burst Size)	This is the amount of token traffic that can be removed at one time from the conforming token bucket. The amount can be specified in the range of 11–2,097,120 kByte.
PBS (Peak Burst Size)	This is the amount of token traffic that can be removed at one time from the peak token bucket. The amount can be specified in the range of 11–2,097,120 kByte.

Metering action (policing/remarking) settings

To specify the action for a bandwidth class that was categorized by metering, use the **police** command (in policy map/class mode or aggregate policer mode).
This product lets you define the following actions for each bandwidth class.

- Specifying bandwidth class actions

Bandwidth class	Forward	Discard	Remark
Green	Yes	No	No
Yellow	Yes	Yes	○ (only one or the other)
Red	No	Yes	

- Detailed remarking settings are specified using the **remark-map** command (policy map/class mode or aggregate policer mode).
  As with pre-marking, remarking to DSCP values can use **the value recommended by RFC** (refer to separate table 1. “Standard PHB (RFC recommended value)” and those not found in the RFC, **for total of four**.
  When remarking, the transmission queue will be reassigned based on the changed value and the **transmission queue ID conversion table** that corresponds to the trust mode.
- If metering is not done, all frames that have been classified into traffic classes will be handled as the **green** bandwidth class.

Storing in the transmission queue

Frames are stored in the transmission queue that is finally determined through a series of QoS processing.
In order to resolve transmission queue congestion, this product provides a system to select and discard frames.

- This product uses the **tail drop** method to resolve overflow in the transmission queue.
  When the threshold values shown below for the bandwidth class that is classified by metering have been exceeded, the frame in question will be discarded.
  Frames discarded by tail drop are counted by the frame counter.

Bandwidth class	Tail drop threshold value (%)
Green + Yellow	100%
Red	60%

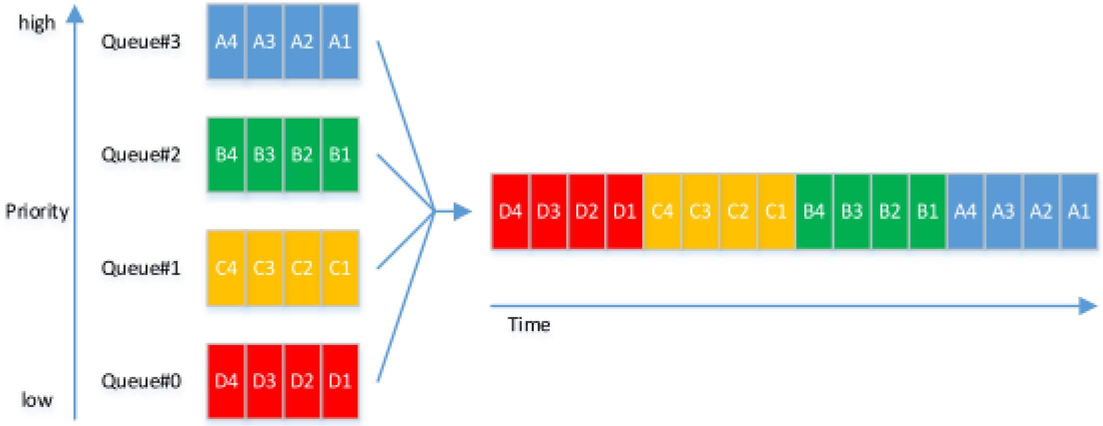
- Tail drop is disabled only if the stack function is disabled and flow control is enabled.
  It is not possible to change the threshold value.
- The usage of the transmission queue can be checked using the **show qos queue-counters** command.
- The number of packets discarded by tail drop can be checked using the **show interface, show frame-counter** command.

Scheduling

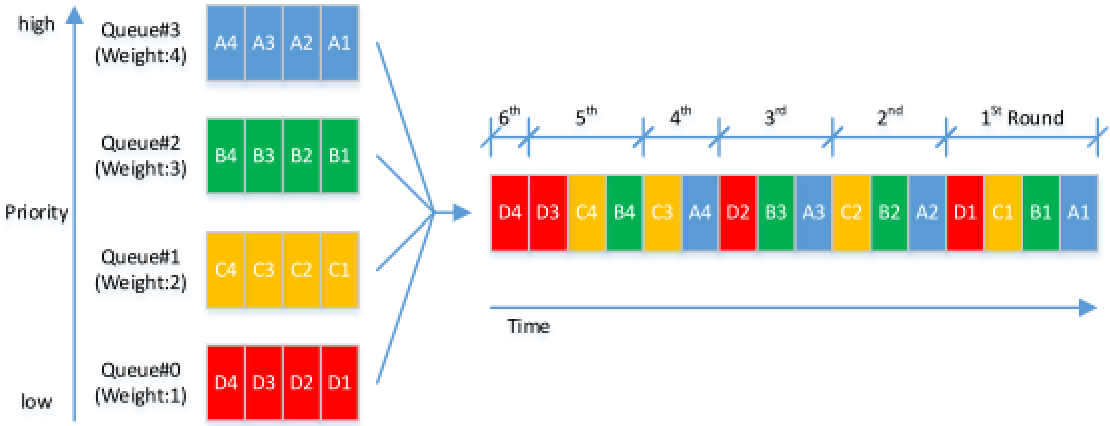
Scheduling is used to determine what rules are used to send out the frames that are stored in the transmission queue.
Appropriate control of the scheduling along with the system to control congestion will help ensure QoS. (Inappropriate scheduling will result in degradation of QoS.)

This product supports two types of scheduling for the transmission queue, the **strict priority system (SP)** and the **weighted round-robin (WRR)** system.
SP and WRR can also be integrated in the interface and used together. (When doing so, SP will be given priority during processing.)

- Strict priority system (SP: Strict Priority) The higher the queue priority, the higher the transmission priority.
  When a frame is stored in a high-priority queue, it can never be transmitted from a lower-priority queue.



- Weighted round-robin system (WRR: Weighted Round Robin)
  Each queue is assigned **a weight** and transmits frames accordingly. A weight of **1–32** can be set. Frames can also be transmitted from a lower-priority queue, within a specified percentage.



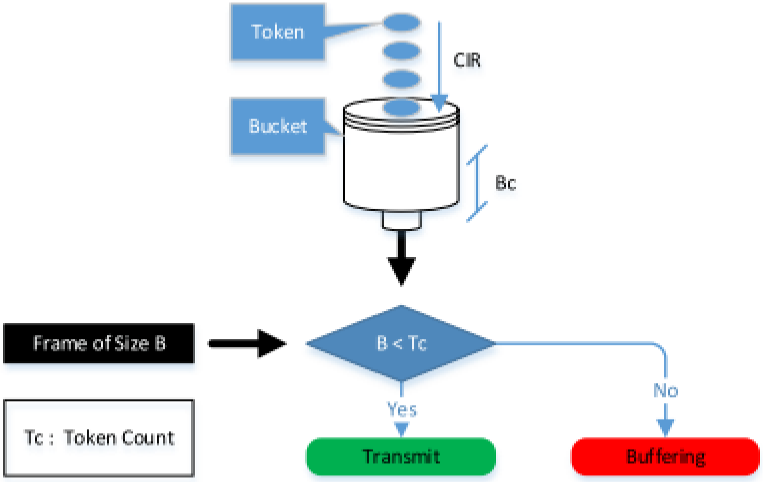
The transmission queue settings are made for the entire system, not for each interface.

Use the **qos wrr-weight** command to set the weight.
The default setting (when QoS is enabled) and the scheduling setting is “**SP**” for all queues.

Shaping

If a frame is forwarded from a broadband network to a narrowband network at the same transmission speed when connecting to a network with different bandwidth, the frame cannot be forwarded, which may result in insufficient bandwidth.
Shaping is a function that monitors the frame transmission speed, and restricts the forwarding rate to a specific amount by temporarily buffering frames with a speed that exceeds the limit, and then transmitting them.
Shaping on this product is realized by using a single token bucket.

- Single token bucket



- Shaping can be specified for individual ports and for individual queues, respectively using the following commands.

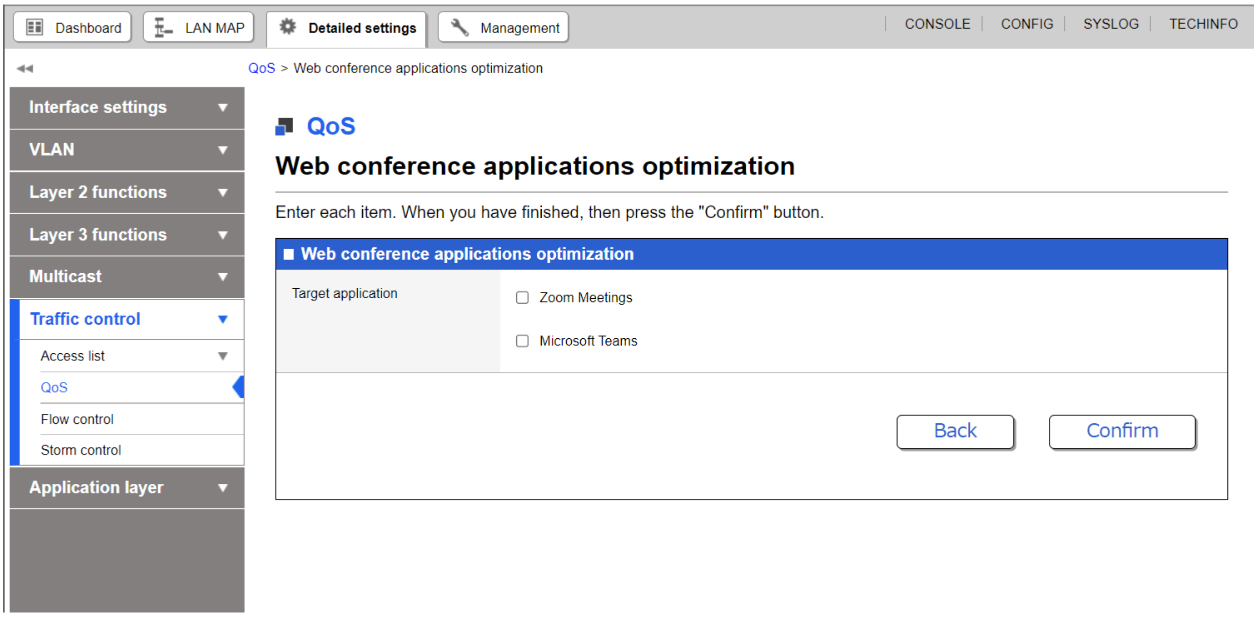
Object of shaping	Command for settings
By port	**traffic-shape rate**
By transmission queue	**traffic-shape queue rate**

- Specify the upper limit of the transmission rate (CIR) and the burst size (BC).
    - Upper limit of transmission rate (CIR): Can be specified from **18 to 1,000,000 kbps**.
    - Burst size (BC): Can be specified from **4 to 16,000 kbyte**. However, this is specified in 4 Kbyte units.
    - If shaping is used both by queue and by port, shaping by port is applied after shaping by queue.
- The default setting (when QoS is enabled) and the shaping setting is "**disable**" for all ports and all queues.

Optimizing web conference application settings

QoS settings for web conference application software can be configured easily via the Web GUI.
By merely using simple operations to select the web conference application to use, communication can be prioritized for that web conference application, such as Zoom Meetings or Microsoft Teams.

- Page for optimizing web conference application settings



QoS

Web conference applications optimization

Enter each item. When you have finished, then press the "Confirm" button.

Web conference applications optimization

Target application: □ Zoom Meetings □ Microsoft Teams

Optimizing web conference application settings involves configuring the following settings.

- Enable QoS.
- Set the trust mode for all ports to DSCP.
- Assign the DSCP value for the web conference application to be optimized to a high-priority sending queue. The DSCP values used for web conference applications are indicated below.
  To use the web conference application settings to change the DSCP value used by the web conference application to a non-default value, use the **qos dscp-queue** command to change the link between the DSCP value and sending queue.
  - Zoom Meetings
    - 56 (Audio)
    - 40 (Video/Screen sharing)
  - Microsoft Teams
    - 46 (Audio)
    - 34 (Video)
    - 18 (Application/Screen sharing)
- Assign the DSCP value not used by the web conference application being optimized to the lowest-priority sending queue.
- Change the scheduling mode for all sending queues to the absolute priority method.

This web conference application setting optimization function includes functionality for configuring QoS settings for individual switches. To fully maximize the benefits of QoS settings, they must be configured for the entire network, including the router, at the same time.
If the DSCP value for the web conference application was changed to a non-default value, also change the DSCP sending queue assignment settings separately.

Separate table 1: Standard PHB (RFC recommended value)

PHB		DSCP value	RFC
Default		0	RFC2474
CS (Class Selector)	CS0	0	RFC2474
	CS1	8	
	CS2	16	
	CS3	24	
	CS4	32	
	CS5	40	
	CS6	48	
	CS7	56	

PHB		DSCP value	RFC
AF (Assured Forwarding)	AF11	10	RFC2597
	AF12	12	
	AF13	14	
	AF21	18	
	AF22	20	
	AF23	22	
	AF31	26	
	AF32	28	
	AF33	30	
	AF41	34	
	AF42	36	
	AF43	38	
EF (Expedited Forwarding)		46	RFC2598

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Enabling or disabling QoS control	qos enable
Set default CoS	qos cos
Change trust mode	qos trust
Generate policy map for received frames	policy-map
Apply policy map for received frames	service-policy input
Show status of QoS function setting	show qos
Show QoS information for LAN/SFP port	show qos interface
Show egress queue usage ratio	show qos queue-counters
Show policy map information	show policy-map
Show map status	show qos map-status
Set CoS-transmission queue ID conversion table	qos cos-queue
Set DSCP-transmission queue ID conversion table	qos dscp-queue
Set port priority order	qos port-priority-queue
Set priority order of frames sent from the network switch unit	qos queue sent-from-cpu
Generate class map (traffic category conditions)	class-map

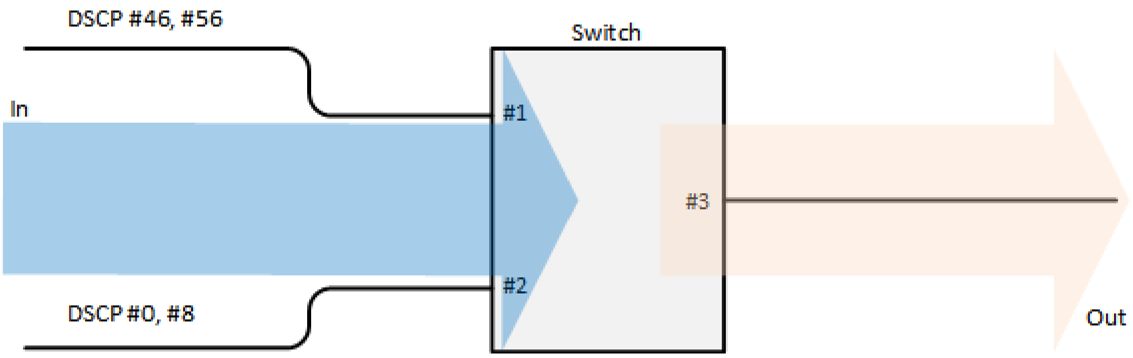
Operations	Operating commands
Associate class map	class
Set traffic classification conditions (access-group)	match access-list
Set traffic classification conditions (CoS)	match cos
Set traffic classification conditions (TOS precedence)	match ip-precedence
Set traffic classification conditions (DSCP)	match ip-dscp
Set traffic classification conditions (Ethernet Type)	match ethertype
Set traffic classification conditions (VLAN ID)	match vlan
Set traffic classification conditions (VLAN ID range)	match vlan-range
Show class map information	show class-map
Set pre-marking (CoS)	set cos
Set pre-marking (TOS precedence)	set ip-precedence
Set pre-marking (DSCP)	set ip-dscp
Set individual policer / aggregate policer (single rate)	police signle-rate
Set individual policer / aggregate policer (twin rate)	police twin-rate
Set remarking for individual policer / aggregate policer	remark-map
Create aggregate policer	aggregate-police
Show aggregate policer	show aggregate-police
Apply aggregate policer	police-aggregate
Show metering counter	show qos metering-counters
Clear metering counter	clear qos metering-counters
Set egress queue (CoS-Queue)	set cos-queue
Set egress queue (DSCP-Queue)	set ip-dscp-queue
Set egress queue scheduling	qos wrr-weight
Set traffic shaping (individual port)	traffic-shape rate
Set traffic shaping (individual queue)	traffic-shape queue rate

Examples of Command Execution

Priority control (SP) using DSCP values

This example allocates the transmission queue based on the DSCP value of the frame, for priority control (SP). When the DSCP = 56, 46, 8, 0 frame is received, large frames for DSCP values from LAN port #3 will be processed with priority by SP priority control.

- DSCP priority control (SP): setting example



- Prioritizing the input frame is done as follows.
    - DSCP = 56 frame is set at priority level 7
    - DSCP = 46 frame is set at priority level 5
    - DSCP = 8 frame is set at priority level 1
    - DSCP = 0 frame is set at priority level 0

1. Enable QoS and set the trust mode for the reception ports (LAN ports #1 and #2).

```
Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust dscp ③
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ④
Yamaha(config-if)#qos trust dscp ⑤
Yamaha(config-if)#exit
```

① Enable QoS

② Setting for LAN port #1

③ Change the trust mode to DSCP

④ Setting for LAN port #2

⑤ Change the trust mode to DSCP

2. Set the DSCP - transmission queue ID conversion table.
As the transmission queue ID corresponding to DSCP value = 46, 56 is the default, there is no need to make this setting, but it is listed for purposes of clarity.

```
Yamaha(config)#qos dscp-queue 56 7 ①
Yamaha(config)#qos dscp-queue 46 5 ②
Yamaha(config)#qos dscp-queue 8 1 ③
Yamaha(config)#qos dscp-queue 0 0 ④
```

① Store frames with DSCP = 56 in transmission queue #7

② Store frames with DSCP = 46 in transmission queue #5

③ Store frames with DSCP = 8 in transmission queue #1

④ Store frames with DSCP = 0 in transmission queue #0

3. This sets the scheduling method per transmission queue.
As this is the default, there is no need to make this setting, but it is listed for purposes of clarity.

```
Yamaha(config)# no qos wrr-weight 7 ①
Yamaha(config)# no qos wrr-weight 5 ②
Yamaha(config)# no qos wrr-weight 1 ③
Yamaha(config)# no qos wrr-weight 0 ④
```

① Queue: 7 SP method

② Queue: 5 SP method

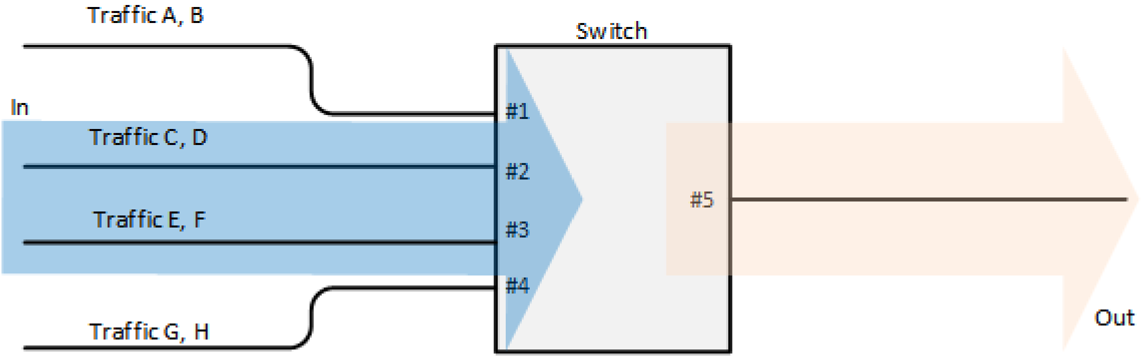
③ Queue: 1 SP method

④ Queue: 0 SP method

Priority control (SP+WRR) using an access list

This example classifies traffic by using the source IP address, and sets the priority control (WRR).

- Priority control (SP+WRR) setting example



- Classification conditions and priority setting for input frames
  - The packet from 192.168.10.2 is classified as **traffic A**, and is set with a priority level of 7 during packet transmission
  - The packet from 192.168.20.2 is classified as **traffic B**, and is set with a priority level of 6 during packet transmission
  - The packet from 192.168.30.2 is classified as **traffic C**, and is set with a priority level of 5 during packet transmission
  - The packet from 192.168.40.2 is classified as **traffic D**, and is set with a priority level of 4 during packet transmission
  - The packet from 192.168.50.2 is classified as **traffic E**, and is set with a priority level of 3 during packet transmission
  - The packet from 192.168.60.2 is classified as **traffic F**, and is set with a priority level of 2 during packet transmission
  - The packet from 192.168.70.2 is classified as **traffic G**, and is set with a priority level of 1 during packet transmission
  - The packet from 192.168.80.2 is classified as **traffic H**, and is set with a priority level of 0 during packet transmission
- Scheduling method
  Configure the settings in a combination of SP and WRR.

Queue ID	Method	Weight (%)
7	SP	-
6	SP	-

Queue ID	Method	Weight (%)
5	SP	-
4	WRR	8 (40.0%)
3	WRR	6 (30.0%)
2	WRR	3 (15.0%)
1	WRR	2 (10.0%)
0	WRR	1 (5.0%)

1. This enables QoS, defines the access lists for traffic A–H, and defines the traffic classes that will be set in the LAN ports.

```
Yamaha(config)#qos enable ①
Yamaha(config)#access-list 1 permit any 192.168.10.2 0.0.0.0 any ②
Yamaha(config)#class-map cmap-A
Yamaha(config-cmap)#match access-list 1
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 2 permit any 192.168.20.2 0.0.0.0 any ③
Yamaha(config)#class-map cmap-B
Yamaha(config-cmap)#match access-list 2
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 3 permit any 192.168.30.2 0.0.0.0 any ④
Yamaha(config)#class-map cmap-C
Yamaha(config-cmap)#match access-list 3
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 4 permit any 192.168.40.2 0.0.0.0 any ⑤
Yamaha(config)#class-map cmap-D
Yamaha(config-cmap)#match access-list 4
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 5 permit any 192.168.50.2 0.0.0.0 any ⑥
Yamaha(config)#class-map cmap-E
Yamaha(config-cmap)#match access-list 5
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 6 permit any 192.168.60.2 0.0.0.0 any ⑦
Yamaha(config)#class-map cmap-F
Yamaha(config-cmap)#match access-list 6
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 7 permit any 192.168.70.2 0.0.0.0 any ⑧
Yamaha(config)#class-map cmap-G
Yamaha(config-cmap)#match access-list 7
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 8 permit any 192.168.80.2 0.0.0.0 any ⑨
Yamaha(config)#class-map cmap-H
Yamaha(config-cmap)#match access-list 8
Yamaha(config-cmap)#exit
```

① Enable QoS

② Traffic A

③ Traffic B

④ Traffic C

⑤ Traffic D

⑥ Traffic E

⑦ Traffic F

⑧ Traffic G

⑨ Traffic H

2. This reverts the CoS - transmission queue ID conversion table to the default setting.

```
Yamaha(config)#no qos cos-queue 0
Yamaha(config)#no qos cos-queue 1
Yamaha(config)#no qos cos-queue 2
Yamaha(config)#no qos cos-queue 3
Yamaha(config)#no qos cos-queue 4
Yamaha(config)#no qos cos-queue 5
Yamaha(config)#no qos cos-queue 6
Yamaha(config)#no qos cos-queue 7
```

3. Generate and apply the policy to LAN port #1 (port1.1).
This sets a transmission queue with CoS value 7 to traffic-A, and a transmission queue with CoS value 6 to traffic-B.

```
Yamaha(config)#policy-map pmap1
Yamaha(config-pmap)#class cmap-A
Yamaha(config-pmap-c)#set cos-queue 7 ①
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-B
Yamaha(config-pmap-c)#set cos-queue 6 ②
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.1 ③
Yamaha(config-if)#service-policy input pmap1 ④
Yamaha(config-if)# exit
```

① Traffic-A is given local priority 7

② Traffic-B is given local priority 6

③ LAN port #1

④ Apply the policy to received frames

4. Generate and apply the policy to LAN port #2 (port1.2).
This sets a transmission queue with CoS value 5 to traffic-C, and a transmission queue with CoS value 4 to traffic-D.

```
Yamaha(config)#policy-map pmap2
Yamaha(config-pmap)#class cmap-C
Yamaha(config-pmap-c)#set cos-queue 5 ①
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-D
Yamaha(config-pmap-c)#set cos-queue 4 ②
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.2 ③
Yamaha(config-if)#service-policy input pmap2 ④
Yamaha(config-if)# exit
```

① Traffic-C is given local priority 5

② Traffic-D is given local priority 4

③ LAN port #2

④ Apply the policy to received frames

5. Generate and apply the policy to LAN port #3 (port1.3).
This sets a transmission queue with CoS value 3 to traffic-E, and a transmission queue with CoS value 0 to traffic-F.

```
Yamaha(config)#policy-map pmap3
Yamaha(config-pmap)#class cmap-E
Yamaha(config-pmap-c)#set cos-queue 3 ①
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-F
Yamaha(config-pmap-c)#set cos-queue 0 ②
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.3 ③
Yamaha(config-if)#service-policy input pmap3  ④
Yamaha(config-if)# exit
```

① Traffic-E is given local priority 3

② Traffic-F is given local priority 2

③ LAN port #3

④ Apply the policy to received frames

6. Generate and apply the policy to LAN port #4 (port1.4).
This sets a transmission queue with CoS value 2 to traffic-G, and a transmission queue with CoS value 1 to traffic-H.

```
Yamaha(config)#policy-map pmap4
Yamaha(config-pmap)#class cmap-G
Yamaha(config-pmap-c)#set cos-queue 2 ①
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-H
Yamaha(config-pmap-c)#set cos-queue 1 ②
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.4 ③
Yamaha(config-if)#service-policy input pmap4 ④
Yamaha(config-if)#exit
```

① Traffic-G is given local priority 1

② Traffic-H is given local priority 0

③ LAN port #4

④ Apply the policy to received frames

7. This sets the scheduling method for the transmission queue.

As the queue IDs 5, 6, and 7 are the defaults, there is no need to make this setting, but it is listed for purposes of clarity.

```
Yamaha(config)#qos wrr-weight 0 1 ①
Yamaha(config)#qos wrr-weight 1 2 ②
Yamaha(config)#qos wrr-weight 2 3 ③
Yamaha(config)#qos wrr-weight 3 6 ④
Yamaha(config)#qos wrr-weight 4 8 ⑤
Yamaha(config)#no qos wrr-weight 5 ⑥
Yamaha(config)#no qos wrr-weight 6 ⑦
Yamaha(config)#no qos wrr-weight 7 ⑧
```

① Transmission queue 0: WRR method, weight of 1

② Transmission queue 1: WRR method, weight of 2

③ Transmission queue 2: WRR method, weight of 3

④ Transmission queue 3: WRR method, weight of 6

⑤ Transmission queue 4: WRR method, weight of 8

⑥ Transmission queue 5: SP method

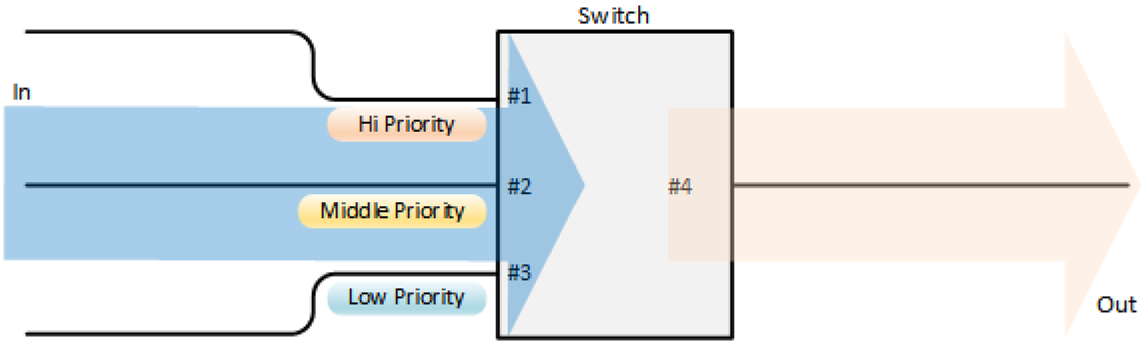
⑦ Transmission queue 6: SP method

⑧ Transmission queue 7: SP method

Priority control using port priority trust mode

The transmission queue is determined according to the port priority order that is specified for each reception port.

- Priority control using port priority: setting example



- Set priority for each reception port
  - Set LAN port #1 (port1.1) to priority order **6**.
  - Set LAN port #2 (port1.2) to priority order **4**.
  - Set LAN port #3 (port1.3) to priority order **2**.

1. Enable QoS and set the trust mode for the reception ports (LAN ports #1, #2, and #3).

```
Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust port-priority ③
Yamaha(config-if)#qos port-priority-queue 6 ④
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ⑤
Yamaha(config-if)#qos trust port-priority ⑨
Yamaha(config-if)#qos port-priority-queue 4 ⑦
Yamaha(config-if)#exit
Yamaha(config)#interface port1.3 ⑧
Yamaha(config-if)#qos trust port-priority ⑨
Yamaha(config-if)#qos port-priority-queue 2 ⑩
Yamaha(config-if)#exit
```

① Enable QoS

② Setting for LAN port #1

③ Change the trust mode to “port priority”

④ Set the port priority to 6

⑤ Setting for LAN port #2

⑥ Change the trust mode to “port priority”

⑦ Set the port priority to 4

⑧ Setting for LAN port #3

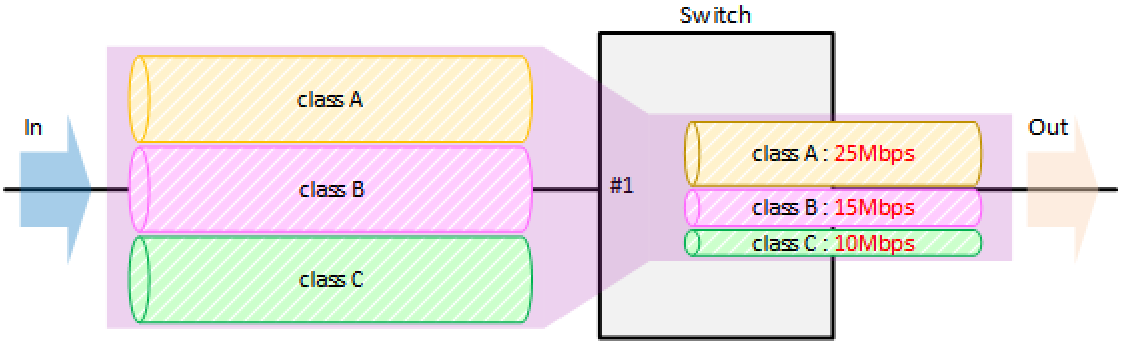
⑨ Change the trust mode to “port priority”

⑩ Set the port priority to 2

Bandwidth control using access list (twin rate / individual policer)

This example sets bandwidth control by using the source IP address. A twin rate policer and an individual policer are used for metering.

- Bandwidth control setting example



- Classification conditions and bandwidth limits for input frames
  - Packets from 192.168.10.2 are classified as **traffic A** packets, with a committed information rate (CIR) (guaranteed reception rate) of 25 Mbps.
  - Packets from 192.168.20.2 are classified as **traffic B** packets, with a committed information rate (CIR) (guaranteed reception rate) of 15 Mbps.
  - Packets from 192.168.30.2 are classified as **traffic C** packets, with a committed information rate (CIR) (guaranteed reception rate) of 10 Mbps.

1. Enable QoS, define the access lists for traffic A–C, and define the traffic classes that will be set for the LAN ports.

```
Yamaha(config)#qos enable ①
Yamaha(config)#access-list 1 permit any 192.168.10.2 0.0.0.0 any ②
Yamaha(config)#class-map cmap-A
Yamaha(config-cmap)#match access-list 1
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 2 permit any 192.168.20.2 0.0.0.0 any ③
Yamaha(config)#class-map cmap-B
Yamaha(config-cmap)#match access-list 2
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 3 permit any 192.168.30.2 0.0.0.0 any ④
Yamaha(config)#class-map cmap-C
Yamaha(config-cmap)#match access-list 3
Yamaha(config-cmap)#exit
```

① Enable QoS

② Traffic A

③ Traffic B

④ Traffic C

2. Generate and apply the policy to LAN port #1 (port1.1).
   Individually specify metering for traffic A through traffic C.
   In the twin rate policer, bandwidth for green can be allocated (guaranteed) by discarding yellow and red.

```
Yamaha(config)#policy-map pmap1
Yamaha(config-pmap)#class cmap-A ①
Yamaha(config-pmap-c)#police twin-rate 25000 25000 156 50 yellow-action drop red-action
drop
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-B ②
Yamaha(config-pmap-c)#police twin-rate 15000 15000 93 50 yellow-action drop red-action
drop
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-C ③
Yamaha(config-pmap-c)#police twin-rate 10000 10000 62 50 yellow-action drop red-action
drop
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.1 ④
Yamaha(config-if)#service-policy input pmap1 ⑤
Yamaha(config-if)#exit
```

① Traffic-A metering setting

② Traffic-B metering setting

③ Traffic-C metering setting

④ LAN port 1

⑤ Apply the policy to received frames

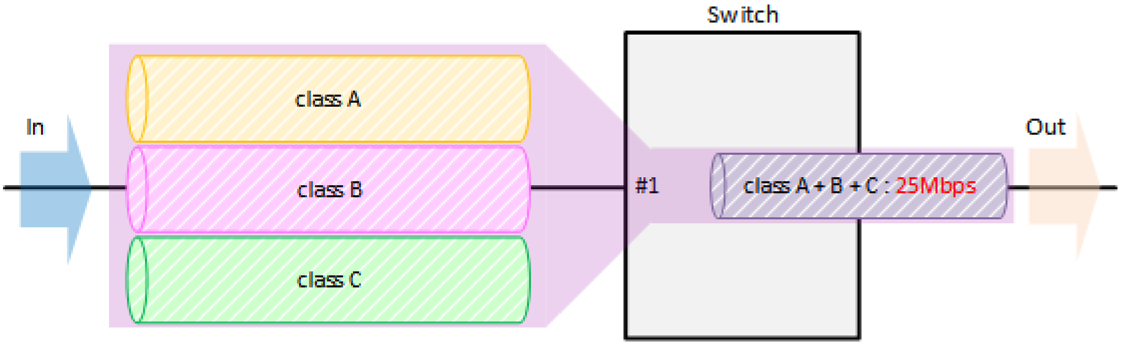
- The metering setting values are shown below.
  - Metering type: Twin rate policer
  - Traffic-A: CIR, PIR (25,000 kbps), CBS (156 kbyte), PBS (50 kbyte)
  - Traffic-B: CIR, PIR (15,000 kbps), CBS (93 kbyte), PBS (50 kbyte)
  - Traffic-C: CIR, PIR (10,000 kbps), CBS (62 kbyte), PBS (50 kbyte)

    The following calculation is used to find the CBS, with a round-trip time of 0.05 sec.
    CBS = CIR (bps) ÷ 8 (bit) × 0.05 (second)

Bandwidth control using access list (single rate / aggregate policer)

This example sets bandwidth control by using the source IP address. A single rate policer and an aggregate policer are used for metering.

- Bandwidth control setting example



- Classification conditions and bandwidth limits for input frames
  - Packets from 192.168.10.2 are classified as **traffic A**.
  - Packets from 192.168.20.2 are classified as **traffic B**.
  - Packets from 192.168.30.2 are classified as **traffic C**.
  - The reception rate is restricted to 25 Mbps for traffic A, B, and C collectively.
  - Bandwidth class “yellow” is remarked as DSCP = 0, and sent with low priority.

1. Enable QoS, define the access lists for traffic A–C, and define the traffic classes that will be set for the LAN ports.

```
Yamaha(config)#qos enable ①
Yamaha(config)#access-list 1 permit any 192.168.10.2 0.0.0.0 any ②
Yamaha(config)#class-map cmap-A
Yamaha(config-cmap)#match access-list 1
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 2 permit any 192.168.20.2 0.0.0.0 any ③
Yamaha(config)#class-map cmap-B
Yamaha(config-cmap)#match access-list 2
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 3 permit any 192.168.30.2 0.0.0.0 any ④
Yamaha(config)#class-map cmap-C
Yamaha(config-cmap)#match access-list 3
Yamaha(config-cmap)#exit
```

① Enable QoS

② Traffic A

③ Traffic B

④ Traffic C

2. Set the DSCP–transmission queue ID conversion table.
Assign the lowest-priority transmission queue to the DSCP value (0) used for remarking “yellow.”

```
Yamaha(config)#qos dscp-queue 0 0
```

3. Create an aggregate policer.

```
Yamaha(config)#aggregate-police agp1 ①
Yamaha(config-agg-policer)#police single-rate 25000 156 50 yellow-action remark red-
action drop
Yamaha(config-agg-policer)#remark-map yellow ip-dscp 0
Yamaha(config-agg-policer)#exit
```

① Create an aggregate policer

- The aggregate policer’s metering setting values are as follows.
    - Metering type: Single rate policer
    - Remark “yellow” to DSCP value = 0
    - CIR (25,000 kbps), CBS (156 kbyte), EBS (50 kbyte)

      The following calculation is used to find the CBS, with a round-trip time of 0.05 sec.
      CBS = CIR (bps) ÷ 8 (bit) × 0.05 (second)

4. Generate and apply the policy to LAN port #1 (port1.1).
   Specify metering (aggregate policer) for the aggregated traffic of A through C.

```
Yamaha(config)#policy-map pmap1
Yamaha(config-pmap)#class cmap-A ①
Yamaha(config-pmap-c)#police-aggregate agp1
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-B ②
Yamaha(config-pmap-c)#police-aggregate agp1
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-C ③
Yamaha(config-pmap-c)#police-aggregate agp1
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.1 ④
Yamaha(config-if)#service-policy input pmap1 ⑤
Yamaha(config-if)#exit
```

① Traffic-A metering setting

② Traffic-B metering setting

③ Traffic-C metering setting

④ LAN port 1

⑤ Apply the policy to received frames

Points of Caution

- LAN/SFP ports that use settings different from those shown below cannot be aggregated as a logical interface. Also, as for the settings shown below for a LAN/SFP port that belongs to a logical interface in startup config, the settings for the most recent port number will be applied to the logical interface.
    - Trust mode
    - Default CoS
    - Port priority
- LAN/SFP ports on which policy maps have been applied cannot belong to a logical interface.
- Policy maps cannot be applied to a LAN/SFP port that belongs to a logical interface. However, if a policy

map exists for a LAN/SFP port associated to a logical interface in startup config, the settings for the most recent port number will be applied to the logical interface.

- Conditions might not be determined correctly for fragment packets. Specifically, if layer 4 information (source port number, destination port number, and various TCP flags) is included in the conditions, correct information cannot be determined because the information is not included in the second and subsequent fragment packets. If there is a possibility of processing fragment packets, do not include layer 4 information in the conditions.

Related Documentation

None

Trademarks and Trade Names

- Zoom is a trademark or registered trademark of Zoom Video Communications, Inc. in the United States and other countries.
- Microsoft Teams is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.

Flow Control

Function Overview

A switching hub initially stores received frames in memory and then performs relay processing.
When many frames are sent at the same time and relay processing cannot keep up (a congested state), exceeding the available memory capacity for storage, the frames to be relayed are discarded.
This product includes the following two functions to help mitigate such congestion.

- When ports are operating at full duplex: IEEE 802.3x flow control can be enabled.
- When ports are operating at half duplex: the back pressure function will always be enabled.

Definition of Terms Used

Bit Time

On a 10BASE network, the speed is **10Mbps**, so 1 bit time = 100 nsec.
In the same way, the bit time on 100BASE is 10 nsec, and on 1000BASE is 1 nsec.

Jam Signal

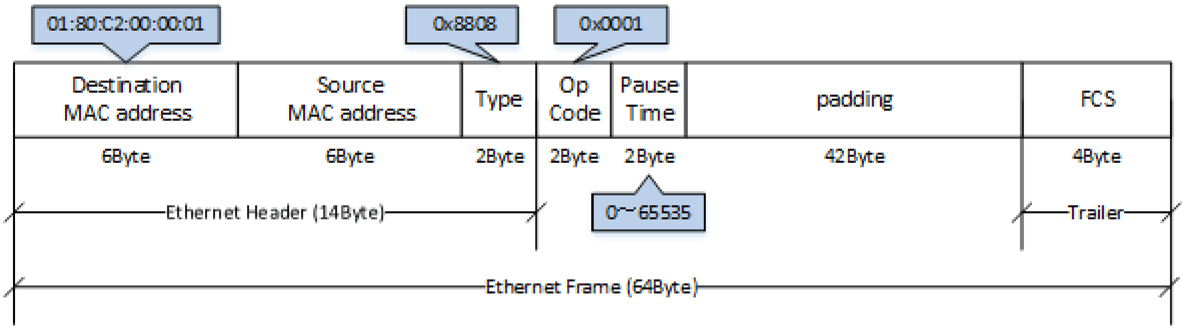
In half-duplex communications, where data cannot be transmitted and received at the same time, there is a possibility of data collision.
The transmitting device monitors the possibility of data collision during transmission. When possible data collision is detected, the device stops transmitting and sends a jam signal. After the jam signal is sent, the device waits for a random interval before resuming transmission.
Although undefined in IEEE, jam signals that use a 32-digit alternating “1” and “0” bit sequence (such as “10101010101010101010101010101010”) are often used.

Function Details

IEEE 802.3x flow control

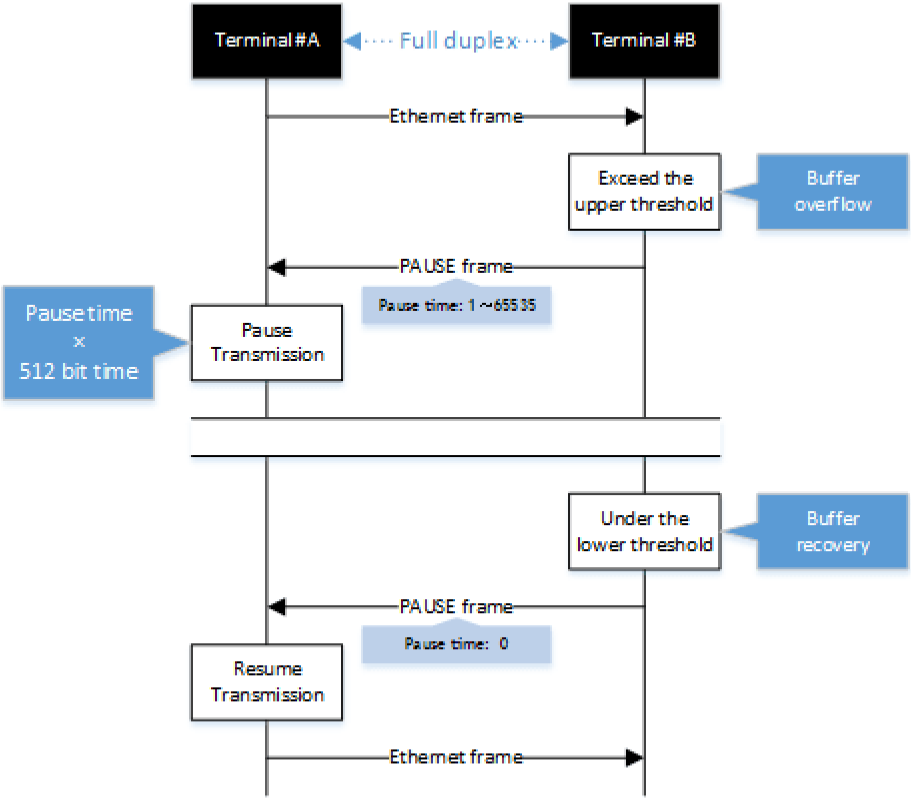
For full duplex communication, the MAC control protocol with IEEE802.3x option can be used.
The **MAC control frame** in the diagram below is used for flow control.

- MAC control frame



The following flow control operations are performed, based on the restriction start threshold and the restriction cancel threshold.

- Flow control: processing flow



This product can be used for either transmitting or receiving MAC control frames. The operations for each are shown below.

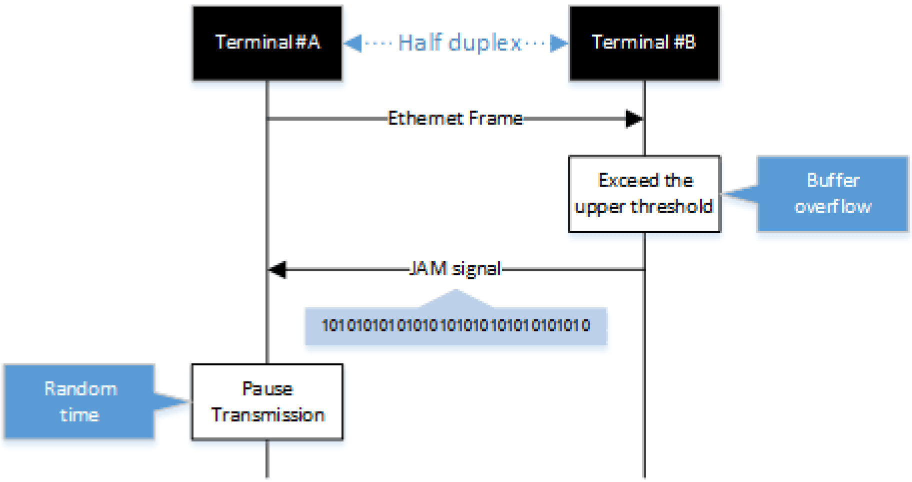
- MAC control frame transmission processing
  - Frames are stored in the received buffer. When the number of the frames exceeds the restriction start threshold, a PAUSE frame with a pause time of 65535 is sent.
  - When the overflow in the received buffer is resolved, and the number of the frames falls below the restriction cancel threshold, a PAUSE frame with a pause time of 0 is sent.
- MAC control frame reception processing
  - When a PAUSE frame with a pause time of 1–65535 is received, the transmission processing will be stopped if the corresponding bit time has elapsed, or if the a PAUSE frame with a pause time of 0 has been received.

Use the **flowcontrol** command to enable or disable the flow control (when transmitting/receiving MAC control frames).
This setting can be made for the system and for each transmitting/receiving LAN/SFP port, and is set to “disable” by factory default.
In order to enable flow control for an individual port, flow control must be enabled for the system.
The **tail drop function is disabled** when flow control is enabled in the system, except when the stack function is enabled.
If the Qos function is enabled, **flow control cannot be enabled**.
When the stack function is enabled, **only Pause frames** can be received.

Back pressure

This product sends a jam signal whenever the receiving buffer of a LAN port is about to overflow.
With this, the sender waits for a random amount of time as per the CSMA/CD, and then sends the frames.
When the LAN port is operating at **half duplex**, the **back pressure function will always be enabled**.
In addition, when the stack is enabled, jam signals are not sent for communication via the stack port.

- Back pressure processing flow



Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Set (system) flow control (IEEE 802.3x PAUSE send/receive)	flowcontrol
Set (interface) flow control (IEEE 802.3x PAUSE send/receive)	flowcontrol
Show flow control operating status	show flowcontrol

Examples of Command Execution

- Enable flow control on LAN port #1.
  After the function is enabled, check the flow control operating status.

```
Yamaha(config)#flowcontrol enable
Yamaha(config)#interface port1.1
Yamaha(config-if)#flowcontrol both
Yamaha(config-if)#end
Yamaha#show flowcontrol port1.1
Port        FlowControl       RxPause TxPause
---------   -----------       ------- -------
port1.1     Both                    0      64
```

Points of Caution

None

Related Documentation

None

Storm Control

Function Overview

This product provides a **storm control** function as a countermeasure against L2 loops and DoS attacks. Broadcast frames, multicast frames, and unicast frames addressed to an unknown destination (dlf) are monitored for each LAN/SFP port, and frames that exceed a preset threshold value are discarded.
This prevents such frames from taking up bandwidth on the LAN/SFP port.
Using this along with the **unique loop detection** and **storm control** functions **enhances the precision of loop detection (avoiding such frames in the first place)**.

Definition of Terms Used

Broadcast Storm/Multicast Storm

This means a situation where frames addressed for broadcast or multicast are continuously forwarded.
In this situation, the switch floods all ports except for the reception port with the broadcast or multicast.
When this is received by another switch, all ports except for the reception port are flooded in the same way.
When this continues, it can lead to the following symptoms.

- Bandwidth is taken up by the broadcast frames/multicast frames
- The switch's CPU load increases, making normal operations difficult
- Devices connected to the switch become unable to communicate

Unicast Storm

This means a situation where frames addressed to an unknown unicast destination (dlf: Destination Lookup Failure) are continuously forwarded.
When the MAC address of the receiving device has not been registered in the ARP table, all ports on the switch except for the reception port are flooded.
This leads to the same symptoms occurring as with a broadcast storm or multicast storm.

Function Details

The operating specifications for storm control are shown below.

1. The storm control function can be enabled for LAN/SFP ports.
   The setting is **disabled for all ports** by default.
2. Storm control on this product can be specified as a tolerance percentage for the bandwidth of the LAN/SFP ports that receive broadcast frames, multicast frames, and unicast frames addressed to an unknown destination.
   (Control can be made in two decimal points. Specifying 100% is the same as disabling the storm function.)
   The bandwidth tolerance is common for all frames, and the user can select the applicable frames.
   This setting is made using the **storm-control** command.
3. The following **SYSLOG** will be outputted **at the time that storm control is enabled or disabled**.
   - Enabled: [STORM]:inf: storm-control ENABLE (port:port1.1, type:B M U, level:50. 0%)
   - Disabled: [STORM]:inf: storm-control DISABLE (port:port1.1)
4. When frames exceeding the permitted bandwidth are received, the excessive frames are discarded.
5. Use the **show storm-control** command to check the storm control information set for the LAN/SFP port.

Related Commands

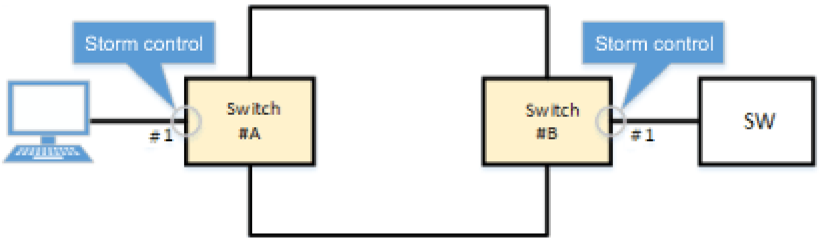
Related commands are indicated below.
For details on the commands, refer to the Command Reference.

Operations	Operating commands
Set storm control	storm-control
Show storm control reception upper limit	show storm-control

Examples of Command Execution

In this example, the receivable L2 broadcast packets for LAN port 1 are restricted to a port bandwidth of 30%.

- Storm control command setting: example



```
Yamaha(config)#interface port1.1
Yamaha(config-if)#storm-control broadcast level 30 ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show storm-control
Port        BcastLevel    McastLevel    UcastLevel
port1.1       30.00%       100.00%       100.00%
port1.2      100.00%       100.00%       100.00%
port1.3      100.00%       100.00%       100.00%
port1.4      100.00%       100.00%       100.00%
port1.5      100.00%       100.00%       100.00%
port1.6      100.00%       100.00%       100.00%
port1.7      100.00%       100.00%       100.00%
port1.8      100.00%       100.00%       100.00%
port1.9      100.00%       100.00%       100.00%
```

① Limit broadcast to 30% of bandwidth

Points of Caution

None

Related Documentation

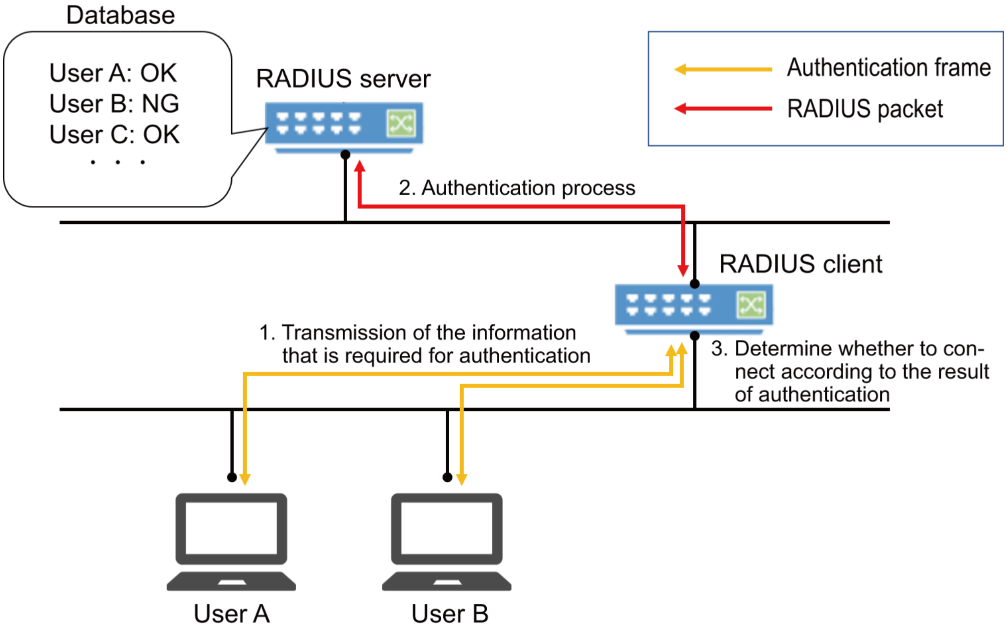
- Layer 2 Function: Unique Loop Detection

Application layer function

RADIUS server

Function Overview

The RADIUS server function manages user information and certificates, and performs authentication based on information notified from the client.
By combining with MAC authentication, 802.1X authentication, and Web authentication of this device, the authentication function can be realized with this device alone.
Also, when authenticating with a device other than this device, this device can be operated as an authentication server.


Database
User A: OK
User B: NG
User C: OK
・・・
RADIUS server
Authentication frame
RADIUS packet
2. Authentication process
RADIUS client
1. Transmission of the information that is required for authentication
3. Determine whether to connect according to the result of authentication
User A
User B

The basic performance of the RADIUS server function and the corresponding authentication method are as follows.

- **Basic performance**

Item	Performance
Number of RADIUS clients that can be registered	100
Number of users that can be registered	2000
Key strength	2048 bit
Signature algorithm	SHA256
Certificate Authority name (default value)	swx-radius

- **Supported authentication methods**

Authentication method	Application
PAP	MAC authentication
EAP-MD5	IEEE802.1X authentication, MAC authentication, WEB authentication

Authentication method	Application
EAP-TLS	IEEE802.1X authentication
EAP-TTLS	IEEE802.1X authentication
PEAP	IEEE802.1X authentication

Definition of Terms Used

PKI (Public Key Infrastructure)

Public key infrastructure. Includes digital certificates and certificate authorities (CAs) using public key cryptography.

Certificate authority (CA)

An organization that guarantees reliability. It is divided into a root Certificate Authority and an intermediate Certificate Authority.
It has a tree structure with the root Certificate Authority at the top and an intermediate Certificate Authority under it.

Intermediate certificate authority

Among Certificate Authorities (CAs), indicates a Certificate Authority whose reliability is guaranteed by a higher-level Certificate Authority (CA).

Root certificate authority

Among Certificate Authorities (CA), indicates a Certificate Authority whose reliability is guaranteed by itself.

Root certificate authority certificate

A public key certificate that has the same issuer and subject and has signed its own public key with its own private key. It is the root of a tree-structured certificate.

Digital certificate

Data that certifies that the public key issued by the Certificate Authority is the genuine issuer's public key.
When the issuer makes a certificate request to the Certificate Authority (CA) together with the public key, the Certificate Authority (CA) issues a digital certificate after scrutinizing and confirming it.

EAP-MD5 authentication method (Message digest algorithm 5)

This is an authentication method that uses a user name and password. Authenticates by exchanging an MD5 hash value instead of a plain text password.

EAP-TLS authentication method (Transport Layer Security)

An authentication method used in IEEE 802.1X, a type of EAP implementation that authenticates by exchanging digital certificates after encrypting the transport layer between the user and the RADIUS server, instead of authenticating with a user ID and password. This is defined in RFC2716 and RFC5216.

EAP-TTLS authentication method (Tunneled TLS)

An authentication method used in IEEE 802.1X, a type of EAP implementation that establishes a TLS communication channel using the server's digital certificate and authenticates the user with a password within the encrypted channel. This is defined in RFC5281.

PEAP authentication method (Protected EAP)

The operating principle is the same as EAP-TTLS (there is only a difference in the protocol in the encrypted tunnel). A TLS communication channel is established using the server's digital certificate, and the user is authenticated with a password in the encrypted communication channel.

It is trusted

A certificate indicating that the public key belongs to the issuer has been issued by a trusted third party.

RADIUS server

The host device that provides the RADIUS server function, in this case, this device.
Authenticates connected users via a RADIUS server and manages authentication/authorization information such as user IDs, passwords, MAC addresses, and associated VLANs.

Server certificate

A certificate to state that the Certificate Authority (CA) has proved that the RADIUS server is trusted.

RADIUS client

Also called a NAS or an authenticator, it relays between the user connected to the LAN/SFP port and the authentication server, and controls access to the LAN based on the success or failure of authentication.

User

A device that connects to a RADIUS client and requests authentication, or a supplicant that is software.
It is the minimum unit for identifying the person to be authenticated. There are data required for authentication and authorization, such as a unique user ID and password.

Client certificate (user certificate)

This certificate proves that the user described above is trusted by the Certificate Authority (CA).

Function Details

Root certificate authority

To use the RADIUS server function, you must first create a root Certificate Authority.
The root certificate authority is used for issuing and managing digital certificates. It can be created with the **crypto pki generate ca** command.
The certificate authority name can be specified in the **crypto pki generate ca** command argument, if omitted it becomes **swx-radius**.

The following certificates are issued and managed based on the root Certificate Authority.
All certificates have a key strength of 2048 bits and a signature algorithm of SHA256.

Root Certificate Authority certificate	Proves that this device is a trusted root Certificate Authority. Issued at the same time that the root Certificate Authority is created. The expiration date applies from 23:59:59 (JST) on December 31, 2037 from the date of certificate creation.

Server certificate	Proves that this device is a trusted server. Issued at the same time that the root Certificate Authority is created. The expiration date applies from 23:59:59 (JST) on December 31, 2037 from the date of certificate creation.
Client (user) certificate	Proves that the user is trusted.
Client revocation certificate	Proves that the client certificate has been revoked.

The root Certificate Authority is deleted or overwritten by the following operations.

- It is deleted when the **cold start** command is executed.
- It is deleted when the **no crypto pki generate ca** command is executed.
- It is deleted when the **stack enable** command is executed.
- It is deleted when the **stack disable** command is executed.
- It is deleted when the **erase startup-config** command is executed.
- It is overwritten when the **crypto pki generate ca** command is executed again.
- It is overwritten when the **restore system** command is executed.
- It is overwritten when the **copy radius-server local** command is executed.

[red]#It is necessary to keep the root certificate authority installed first consistent, so be careful not to delete it carelessly. #
Also, please take measures to back up the file in advance, in case it is deleted.

Once the root CA is deleted, even if the same CA name is set, it will be a different CA from before.
If you delete the root Certificate Authority before backup, you cannot add or revoke the certificate after that. You will have to reissue all the certificates from the beginning.

When the root certificate authority is created by the **crypto pki generate ca** command, it is automatically saved in the internal area, so there is no need to execute the **write** command.

RADIUS client settings

Use the **nas** command to specify the RADIUS clients that are permitted to access the RADIUS server.
You can specify an individual IP address or network address, and up to **100** addresses can be set.
RADIUS client operations are verified using the following products.

- Yamaha network switch (SWX series)
- Yamaha router (RTX series or NVR series)
- Yamaha wireless access point (WLX series)

The settings of the RADIUS client set by the **nas** command are not displayed in the config by **show running-config**.
There is no need to execute the **write** command because it is automatically saved in a different area from the config, but it is necessary to execute the **radius-server local refresh** command to reflect it in the actual operation.
Use the **show radius-server local nas** command to confirm the settings.

User registration

User information for authentication is registered with the **user** command.

Up to 2000 records of user information can be registered.
Items that can be set with the **user** command are as follows.

Type	Item	Summary/Remarks
Mandatory	User ID	ID for uniquely identifying user information
Password	Password used in combination with user ID If the client certificate is compressed, use this password for decompression.	Option
User name	Any character string can be set for user identification.	
MAC address	Compared when the RADIUS client notifies the Calling-Station-Id, and if it does not match, it is not authenticated.	
SSID	Compared when the RADIUS client notifies the Called-Station-Id, and if it does not match, it is not authenticated.	
Mail address	This is the address for sending the certificate by mail.	
Authentication method	The default is EAP-TLS, so you must specify it if you want to use another authentication method.	
Period of certificate validity	This is valid only when the authentication method is EAP-TLS. If omitted, it will be 23:59:59 on December 31, 2037.	

The user settings set by the **user** command are not displayed in the config by **show running-config**, etc.
There is no need to execute the **write** command because it is automatically saved in a different area from the config, but it is necessary to execute the **radius-server local refresh** command to reflect it in the actual operation.
Use the **show radius-server local user** command to confirm the settings.

Restricting the authentication method

The authentication method can be restricted by the **authentication** command.
The authentication method is not restricted by default, but you can use it when you want to temporarily disable a specific authentication method.

Enabling the RADIUS server function

To enable the RADIUS server function, use the **radius-server local enable** command.
Set the RADIUS client and user information, and enable the RADIUS server function after the necessary preparations are completed.

Reflecting settings in operation

If you add/change/delete the settings related to the RADIUS server, execute the **radius-server local refresh** command to reflect them in actual operation.
The commands reflected in the actual operation by the **radius-server local refresh** command are as follows.

- **authentication** command
- **nas** command
- **reauth interval** command
- **user** command

When you add/change/delete settings related to the RADIUS server in Web GUI, processing equivalent to the **radius-server local refresh** command is automatically performed.

Issue client certificate

Use the **certificate user** command to issue a client certificate to a user who performs authentication using a certificate (a user whose authentication method is EAP-TLS with the **user** command).
Each user can hold up to two client certificates, and issuing a third client certificate will cause the older client certificate to expire.
If you specify an individual user ID with the **certificate user** command, a client certificate for the specified user is issued.
If you do not specify individual user IDs in the **certificate user** command, client certificates are issued for all users that meet any of the following conditions.

Conditions for batch issuance of client certificates

- Client certificate has never been issued
- The password or expiration date has changed since the client certificate was issued

It takes about **15 seconds** to issue a client certificate. Although the **certificate user** command issues client certificates in the background, be aware that batch issuing client certificates for multiple users can be time consuming.
To cancel the issuance of a client certificate partway through, use the **certificate abort** command.

The method to export an issued client certificate is as follows.

- Specify the mail option in the **certificate user** command
  The client certificate can be sent to the specified mail address at the same time that the client certificate is issued.
  The client certificate is ZIP compressed and can be decompressed with the password of the **user** command.
  For details on sending a client certificate by mail, refer to **Sending a certificate by mail**.

- **certificate export sd** command
  You can copy the client certificate of any user or all users to a microSD card to export it.
  If a client certificate of any user is compressed and exported by the compress option, it can be decompressed with the password of the **user** command.
  If the client certificate for all users is compressed and exported together using the compress option, it can be decompressed without a password.

- **certificate export mail** command
  The client certificate of any user or all users can be sent to the mail address set by the **user** command.
  The client certificate is ZIP compressed and can be decompressed with the password of the **user** command.

- Access the device with Web GUI

The client certificate can be downloaded for any or all users.
Although it is ZIP compressed, no password is required for decompression.

Revoking a client certificate

To prevent authentication for the user who issued the client certificate, you must issue a revocation certificate. When a revocation certificate is issued to any user, the revocation certificate is referenced in the authentication process and reflected in the authentication result.
Revocation certificates are issued by the following process.

- Execute the **certificate revoke id** command
  A revocation certificate is issued for the client certificate with the specified certificate ID.
- Execute the **certificate revoke user** command
  Revocation certificates are issued for all client certificates of the specified user.
- Change the authentication method from EAP-TLS to other (PAP, PEAP, EAP-MD5, EAP-TTLS) with the **user** command
  Revocation certificates are issued for all client certificates of the target user.
  If you change the authentication method of the target user to EAP-TLS again, it will be subject to **the issue of client certificates**.
- Deletion of **user** command
  Revocation certificates are issued for all client certificates of the target user.
  If you register a user again with the same user ID as the target user, it will be subject to **the issue of client certificates**.
- Issue a third client certificate with the **certificate user** command
  A revocation certificate is issued for the target user’s older client certificate.
- Importing user information according to **Importing and exporting user information**
  If a user is deleted due to an import, a revocation certificate is issued for all client certificates of the deleted user.

Sending a certificate by mail

To use the client certificate mail transmission described in **Issuing a client certificate**, the following preparations are required in advance.
The settings described here are the minimum settings. Make the necessary settings according to the usage.

1. **Set SMTP server**
    1. Specify the SMTP server with the **mail server smtp host** command.
2. **Specify the mail template**
    1. Specify the template ID with the **mail template** command and switch to the template setting mode.
    2. Specify the mail server ID of the SMTP server set by the **mail server smtp host** command with the **send server** command.
    3. Specify the sender mail address with the **send from** command.
3. **Specify the mail template to use for sending certificate mails**
    1. Specify the ID of the mail template created above with the **mail send certificate** command.

The subject and body of the mail are as follows. The format cannot be changed.

Subject	`Certification Publishment`

Body	Certification is published. Name : [*NAME parameter of the user command] Account : [*USERID parameter of the user command] MAC address : XX:XX:XX:XX:XX:XX Expire : YYYY/MM/DD

Checking settings and certificates

- **Checking the RADIUS client settings**
  Use the **show radius-server local nas** command.

```
Yamaha# show radius-server local nas 192.168.100.0/24
host                                    key
-----------------------------------------------------------------------------------------
---------------
192.168.100.0/24                        abcde
```

- **Checking the user settings**
  Use the **show radius-server local user** command.

```
Yamaha# show radius-server local user

Total     1

userid                           name                             vlan mode
--------------------------------------------------------------------------------
00a0de000000                     Yamaha                              1 eap-md5
```

```
Yamaha# show radius-server local user detail 00a0de000000

Total     1

userid      : 00a0de000000
password    : secretpassword
mode        : eap-md5
name        : Yamaha
vlan        :    1
```

- **Checking the status of client certificate issuance processing**
  Use the **show radius-server local certificate status** command.

```
Yamaha# show radius-server local certificate status
certificate process: xxxx/ zzzz processing...
```

- **Checking the list of client certificates**
  Use the **show radius-server local certificate list** command.

```
Yamaha# show radius-server local certificate list detail Taro

userid                           certificate number
enddate
------------------------------------------------------------------------------------------
----
Yamaha                           Yamaha-DF598EE9B44D22CC
2018/12/31
                                 Yamaha-DF598EE9B44D22CD
2019/12/31
```

- **Checking the revocation certificate**
  Use the **show radius-server local certificate revoke** command.

```
Yamaha# show radius-server local certificate revoke

userid                           certificate number                                 reason
------------------------------------------------------------------------------------------
----
Yamaha                           Yamaha-DF598EE9B44D22CC
expired
Yamaha                           Yamaha-DF598EE9B44D22CD
revoked
```

Mail notification of expiration of client certificate

A mail notification can be sent before the client certificate expires.

The following preparations are required in advance to use advance mail notification.
The settings described here are the minimum settings. Make the necessary settings according to the usage.

1. **Set SMTP server**
    1. Specify the SMTP server with the **mail server smtp host** command.
2. **Specify the mail template**
    1. Specify the template ID with the **mail template** command and switch to the template setting mode.
    2. Specify the mail server ID of the SMTP server set by the **mail server smtp host** command with the **send server** command.
    3. Specify the sender mail address with the **send from** command.
3. **Specify the mail template to use for the certificate expiration advance mail notification**
    1. Specify the ID of the mail template created above with the **mail send certificate-notify** command.
4. **Specify when to send a certificate expiration advance mail notification**
    1. Specify the number of days before the expiration date to send the mail notification with the **mail certificate expire-notify** command.

Confirmation of the certificates that are subject to the client certificate expiration advance mail notification is performed **every day at 23:59:59**.

The subject and body of the mail are as follows. The format cannot be changed.

Subject	`Certification expiration`

Body	`Your certificate will expire in [残り日数] days.`
	`Name            : [*NAME parameter of the user command]`
	`Account         : [*USERID parameter of the user command]`
	`MAC address     : XX:XX:XX:XX:XX:XX`
	`Expire          : YYYY/MM/DD`

Importing and exporting user information

- **Exporting**

  User information can be exported from the web GUI as a CSV file.

  Users can be registered collectively by appending them to the exported CSV format file.
  User information exported by this device cannot be imported using a Yamaha wireless access point (WLX series).

- **Importing**

  User information can be imported from the web GUI.
  When importing user information, client certificates being issued due to the import can be issued at one time as a batch.
  When importing information for a large number of users, it may take time before the information is reflected in actual operations.
  User information exported by a Yamaha wireless access point (WLX series) can be imported to this device.
  However, user information cannot be imported if it includes characters that cannot be used in the unit. In that case, add each user separately.
  For details about characters not allowed by the unit, refer to Points of Caution.

Backing up and restoring all RADIUS server related information

This device can back up and restore all RADIUS server related information including the root Certificate Authority.

- **Backup**
  By specifying the microSD card as the export destination with the **copy radius-server local** command, all the RADIUS server related information can be backed up to the microSD card.
  The same backup can be performed from the Web GUI. We recommend that you make a backup in case of device failure.
  The backup file contains the setting information of the following three commands, but does not include the setting information related to other RADIUS server functions. Therefore, it is recommended that you back up configuration files along with backup files.

  - **crypto pki generate ca** command
  - **user** command
  - **nas** command

  Not all RADIUS server-related information backed up by this device can be restored using a Yamaha wireless access point (WLX series).

- **Restoration**
  By specifying the internal config number as the export destination with the **copy radius-server local** command, the data backed up above can be restored from the microSD card.
  In addition, the same restoration can be performed from the Web GUI, and it is possible to restore data obtained with any model of the SWX series.
  Note that if you perform restoration while the root Certificate Authority has been created, the root Certificate Authority will be overwritten.

Restoring RADIUS server information backed up by a Yamaha wireless access point (WLX series)

This unit can be used to restore RADIUS server information backed up by a Yamaha wireless access point (WLX series). The information can only be restored via the Web GUI.
RADIUS server functions used to operate a Yamaha wireless access point (WLX series) can be transferred to the given unit by executing the following procedure.

1. Restore the data backed up by a Yamaha wireless access point (WLX series) port in the unit.
   For the WLX402 model, the backed up data (ZIP file) can be obtained from the RADIUS server settings page on the Web GUI.
   For the WLX313 model, the backed up data (ZIP file) can be obtained from the settings (save/restore) page on the Web GUI.
2. Use the **nas** command or Web GUI to specify the RADIUS client.
3. Specify the VLAN interface to use for RADIUS authentication by the **radius-server local interface** command or via the Web GUI.
4. To send an authentication certificate via mail or send prior mail notification about the certificate expiration date, specify mail settings.
5. Enable RADIUS server functions using the **radius-server local enable** command or the Web GUI.
6. Apply the RADIUS information to actual operations using the **radius-server local refresh** command.

The procedure above eliminates the need to reissue a client certificate and can be used to transfer RADIUS server functions to the unit from a Yamaha wireless access point (WLX series).
If RADIUS server functions are transferred to the unit from a Yamaha wireless access point (WLX series), then the revocation certificate expiration date is automatically updated to 20 years from the date/time the functions are received.
The following data backed up via a Yamaha wireless access point (WLX series) can be restored.

- Root certificate authority
- Root certificate
- Server certificate
- Client certificate
- Revocation certificate
- User information

RADIUS client settings and other information not indicated above are not restored and must be set separately.
Users with information that includes characters not allowed by the unit cannot be restored. In that case, add each user separately.
For details about characters not allowed by the unit, refer to **Points of Caution**.
Certificate Authority names can be restored even if they include characters not allowed by the unit. However, disallowed characters are shown converted to the underscore (_) character in config files.

SYSLOG output information

The following information is output to the SYSLOG as a RADIUS server function.

The prefix is **[RADIUSD]**.

Type	Message	Description
INFO	RADIUS server started.	The RADIUS server function process has started.
INFO	RADIUS server stopped.	The RADIUS server function process has stopped.
INFO	Authentication succeeded.: [{ **User ID** }/<via Auth-Type = { **Authentication method** }>] (from client port { **Port number** } cli { **MAC address** })	User authentication succeeded.
INFO	Authentication failed.: [{ **User ID** }/<via Auth-Type = { **Authentication method** }>] (from client port { **Port number** } cli { **MAC address** })	User authentication failed.
INFO	MAC address is not allowed.User-ID:{ **User ID** } MAC:{ **MAC address** }	User authentication failed because the MAC address is incorrect.
INFO	Connected NAS is not allowed.IP:{ **IP address** }	An authentication request was received from an unauthorized RADIUS client.

Related Commands

Related commands are indicated below.
For details on the commands, refer to the Command Reference.

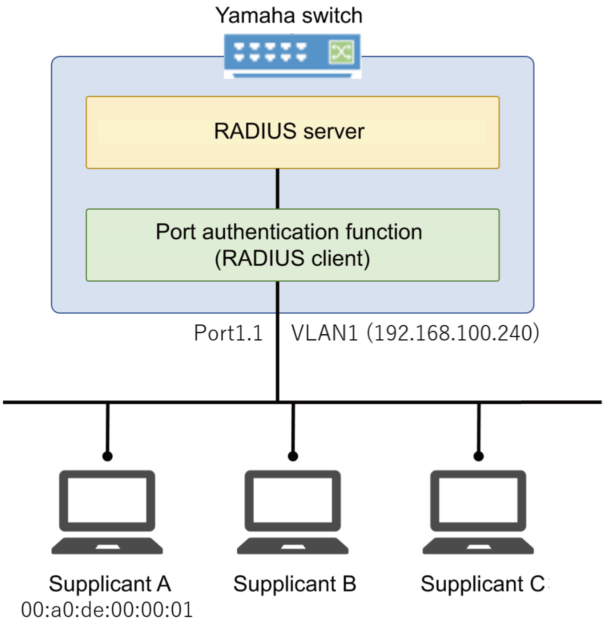
Operations	Operating commands
radius-server local enable	Setting of local RADIUS server function
radius-server local interface	Access interface settings
crypto pki generate ca	Generate root Certificate Authority
radius-server local-profile	RADIUS configuration mode
authentication	Authentication method setting
nas	RADIUS client (NAS) settings
user	Authentication user settings
reauth interval	Re-authentication interval settings
radius-server local refresh	Set data reflected on local RADIUS server
certificate user	Issue client certificate
certificate abort	Suspend client certificate issuance
certificate revoke id	Revoke client certificate with the specified certificate ID
certificate revoke user	Revoke client certificate for specified user
certificate export sd	Export client certificate (SD copy)
certificate export mail	Export client certificate (mail transmission)
copy radius-server local	Copy RADIUS data
show radius-server local nas	Show RADIUS client (NAS)

Operations	Operating commands
show radius-server local user	Show authentication user information
show radius-server local certificate status	Show issuance status of client certificate
show radius-server local certificate list	Show list of client certificates
show radius-server local certificate revoke	Show revocation list of client certificates

Setting Examples

Using RADIUS server functions and port authentication function simultaneously

Use a local RADIUS server to configure supplicants A, B, and C to authenticate with MAC, IEEE802.1X, and Web authentication, respectively.



1. Enable the local RADIUS server with the network switch and register the user.

```
Yamaha# configure terminal
Yamaha(config)# crypto pki generate ca
Generate CA? (y/n): y
Finished
Yamaha(config)# radius-server local-profile
Yamaha(config-radius)# user 00a0de000001 00a0de000001 auth peap
Yamaha(config-radius)# user 8021xuser 8021xpass auth peap
Yamaha(config-radius)# user webuser webpass auth peap
Yamaha(config-radius)# exit
Yamaha(config)# radius-server local enable
Yamaha(config)# exit
Yamaha# radius-server local refresh
```

2. Assign an IP address to VLAN #1 for web authentication

```
Yamaha# configure terminal
Yamaha(config)# interface vlan1
Yamaha(config-if)# ip-address 192.168.100.240/24
```

3. Enable MAC authentication, IEEE802.1X authentication, and Web authentication on LAN port #1.

```
Yamaha# configure terminal
Yamaha(config)# aaa authentication auth-mac
Yamaha(config)# auth-mac auth-user unformatted lower-case
Yamaha(config)# aaa authentication dot1x
Yamaha(config)# aaa authentication auth-web
Yamaha(config)# interface port1.1
Yamaha(config-if)# auth host-mode multi-supplicant
Yamaha(config-if)# auth-mac enable
Yamaha(config-if)# dot1x port-control auto
Yamaha(config-if)# auth-web enable
```

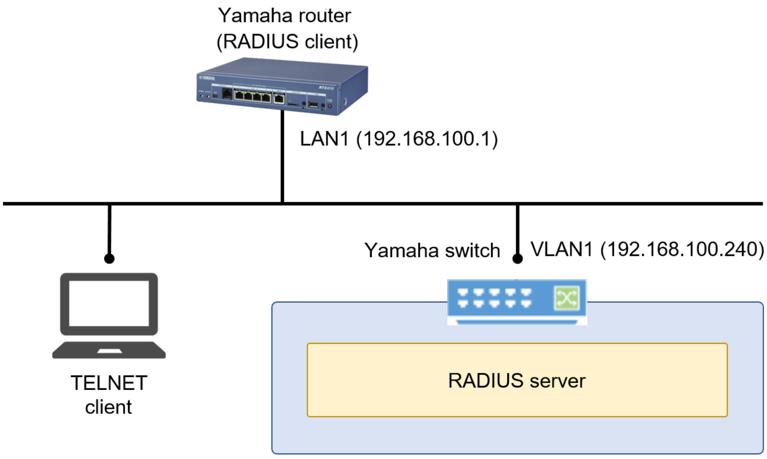
4. Set the RADIUS server used for the authentication function.

```
Yamaha# configure terminal
Yamaha(config)# radius-server host 127.0.0.1 key secret_local
```

Using RADIUS server functions for authentication of users logging in to a Yamaha router

If accessing a Yamaha router from a TELNET client, user login authentication and administrator privilege authentication are performed by the Yamaha network switch RADIUS server.

That enables user login using the user ID “**user1**” and password “**password1**”.
Users can be promoted to administrator using the password “**admin**”.



■ Yamaha network switch settings

1. Specify the IP address in the interface.

```
Yamaha# configure terminal
Yamaha(config)# interface vlan1
Yamaha(config-if)# ip address 192.168.100.240/24
Yamaha(config-if)# exit
```

2. Generate a root Certificate Authority.

```
Yamaha(config)#crypto pki generate ca
Generate CA? (y/n): y
Finished
```

3. Specify the RADIUS servers.

```
Yamaha(config)# radius-server local-profile
Yamaha(config-radius)# nas 192.168.100.1 key yamaha
Yamaha(config-radius)# user user1 password1 auth pap
Yamaha(config-radius)# user *administrator admin auth pap
Yamaha(config-radius)# exit
```

4. Specify interfaces to which RADIUS clients can connect.

```
Yamaha(config)# radius-server local interface vlan1
```

5. Enable RADIUS server functions.

```
Yamaha(config)# radius-server local enable
Yamaha(config)#exit
```

6. Apply RADIUS server settings to actual operations.

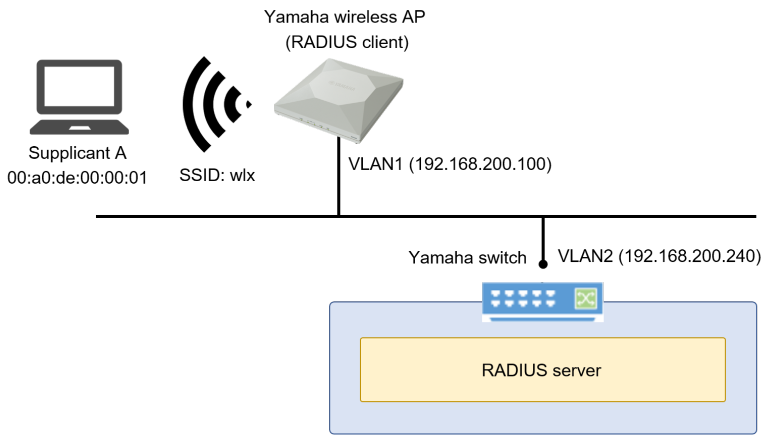
```
Yamaha#radius-server local refresh
Yamaha#
```

■ Yamaha router settings

```
login radius use on
administrator radius auth on
ip lan1 address 192.168.100.1/24
radius auth on
radius auth server 192.168.100.240
radius auth port 1812
radius secret yamaha
```

Using RADIUS server functions for MAC authentication of Yamaha wireless access points (WLX series)

The Yamaha network switch RADIUS server is used to authenticate the MAC address of supplicants connected to a Yamaha wireless access point.



■ Yamaha network switch settings

1. Specify the IP address in the interface.

```
Yamaha# configure terminal
Yamaha(config)# interface vlan2
Yamaha(config-if)# ip address 192.168.200.240/24
Yamaha(config-if)# exit
```

2. Generate a root Certificate Authority.

```
Yamaha(config)#crypto pki generate ca
Generate CA? (y/n): y
Finished
```

3. Specify the RADIUS servers.

```
Yamaha(config)# radius-server local-profile
Yamaha(config-radius)# nas 192.168.200.100 key yamaha
Yamaha(config-radius)# user 00a0de000001 00a0de000001 auth pap ssid wlx
Yamaha(config-radius)# exit
```

4. Specify interfaces permitted to connect to RADIUS clients.

```
Yamaha(config)# radius-server local interface vlan2
```

5. Enable RADIUS server functions.

```
Yamaha(config)# radius-server local enable
Yamaha(config)#exit
```

6. Apply RADIUS server settings to actual operations.

```
Yamaha#radius-server local refresh
Yamaha#
```

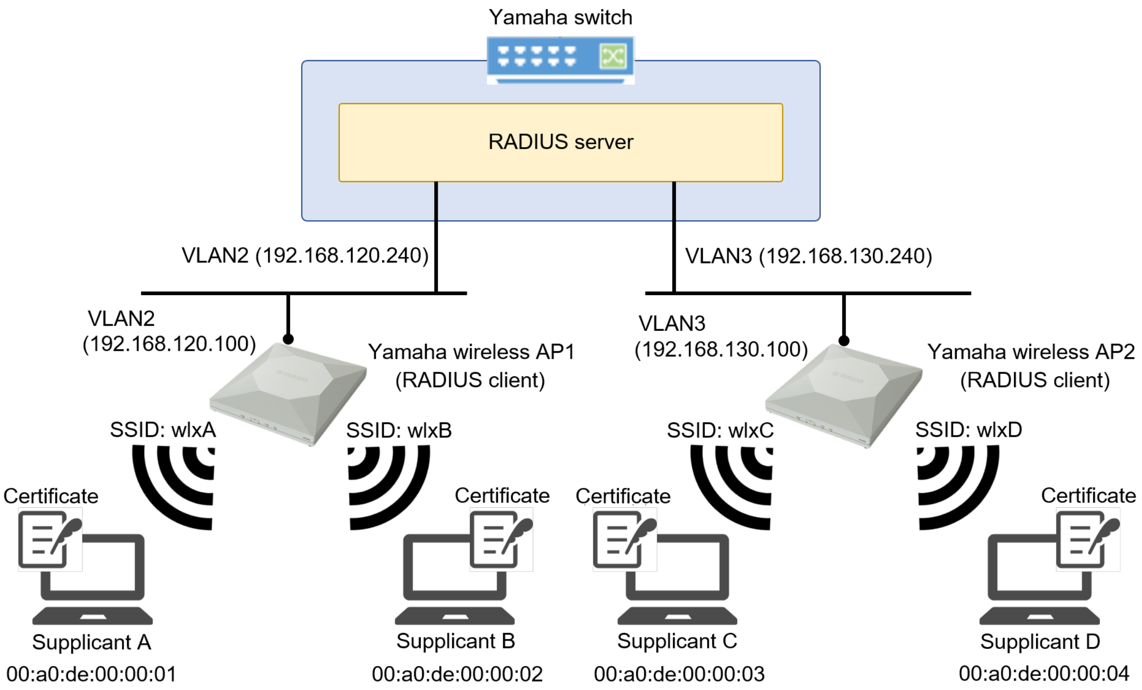
■ Yamaha wireless AP (WLX402) settings

Note: Only for settings related to authentication. Configure other settings, such as for wireless functions, separately according to the given environment.

```
ip vlan-id 1 address 192.168.200.100/24
airlink slect 1
airlink ssid wlx
airlink radius auth on
airlink radius server 192.168.200.240
airlink radius secret yamaha
airlink enable 1
```

Using RADIUS server functions to connect to a Yamaha wireless access point (WLX series) using a certificate

A supplicant with a certificate issued by the Yamaha network switch installed is used to authenticate connections to a Yamaha wireless access point.



■ Yamaha network switch settings

1. Specify the IP address in the interface.

```
Yamaha(config)# interface vlan2
Yamaha(config-if)# ip address 192.168.120.240/24
Yamaha(config-if)# exit
```

2. Generate a root Certificate Authority.

```
Yamaha(config)#crypto pki generate ca
Generate CA? (y/n): y
Finished
```

3. Specify the RADIUS servers.

```
Yamaha(config)# radius-server local-profile
Yamaha(config-radius)# nas 192.168.120.100 key yamaha1
Yamaha(config-radius)# nas 192.168.130.100 key yamaha2
Yamaha(config-radius)# user user1 pass1 ssid wlxA
Yamaha(config-radius)# user user2 pass2 ssid wlxB
Yamaha(config-radius)# user user3 pass3 ssid wlxC
Yamaha(config-radius)# user user4 pass4 ssid wlxD
Yamaha(config-radius)# exit
```

4. Specify interfaces permitted to connect to RADIUS clients.

```
Yamaha(config)# radius-server local interface vlan2
Yamaha(config)# radius-server local interface vlan3
```

5. Enable RADIUS server functions.

```
Yamaha(config)# radius-server local enable
Yamaha(config)# exit
```

6. Issue client certificates.
   Install the issued certificates in supplicants A to D, respectively.

```
Yamaha# certificate user user1
Yamaha# certificate user user2
Yamaha# certificate user user3
Yamaha# certificate user user4
```

7. Apply RADIUS server settings to actual operations.

```
Yamaha# radius-server local refresh
```

■ Yamaha wireless AP1 (WLX402) settings

Note: Only for settings related to authentication. Configure other settings, such as for wireless functions, separately according to the given environment.

```
ip vlan-id 2 address 192.168.120.100/24
 airlink select 1
  airlink ssid wlxA
  airlink vlan-id 2
  airlink radius auth on
  airlink radius server 192.168.120.240
  airlink radius secret yamaha1
 airlink enable 1
 airlink select 2
  airlink ssid wlxB
  airlink vlan-id 2
  airlink radius auth on
  airlink radius server 192.168.120.240
  airlink radius secret yamaha1
 airlink enable 2
```

■ Yamaha wireless AP2 (WLX402) settings

Note: Only for settings related to authentication. Configure other settings, such as for wireless functions, separately according to the given environment.

```
ip vlan-id 3 address 192.168.130.100/24
 airlink select 1
  airlink ssid wlxC
  airlink vlan-id 3
  airlink radius auth on
  airlink radius server 192.168.130.240
  airlink radius secret yamaha2
 airlink enable 1
 airlink select 2
  airlink ssid wlxD
  airlink vlan-id 3
  airlink radius auth on
  airlink radius server 192.168.130.240
  airlink radius secret yamaha2
 airlink enable 2
```

Points of Caution

- In the RADIUS server function, the time of the internal clock of this device is used for processing such as authentication processing and certificate issuance.
  Therefore, it is necessary to always keep the internal clock of this device at the correct time. Time synchronization with NTP server is recommended.
- It is necessary to keep the root Certificate Authority consistent from its creation, so be careful not to delete it carelessly.
  If it is deleted, the issued client certificates cannot be used, and client certificates must be reissued for all users.
  Also, almost all settings related to the RADIUS server function will be deleted.
- Even if you create a root Certificate Authority with the same name on a Yamaha network switch of the same model number, that root Certificate Authority will be a different one.
  Client certificates can only be used with Yamaha network switch authentication that has the root Certificate Authority used at the time of generation.
  To maintain the same root Certificate Authority in multiple devices, see **Backing up and restoring all RADIUS server related information**.
- Authentication cannot be performed even if a RADIUS client connects to an IPv6 link-local address.
- The characters permitted in user or other information by Yamaha network switches is different than permitted by Yamaha wireless access points (WLX series). Those differences are indicated below.
  (The characters in red are disallowed only by Yamaha network switches)

Item	Yamaha network switch restrictions	Yamaha wireless access point restrictions

Root certificate authority name (CA-NAME option for **crypto pki generate ca** command)	The following single-byte alphanumeric characters and symbols cannot be used. ‘\’ (backslash) ‘/’ ‘[’ ‘]’ ‘?’ ‘ ’ (space) ‘”’ (double quote)	The following single-byte alphanumeric characters and symbols cannot be used. ‘\’ (backslash) ‘/’ ‘[’ ‘]’
RADIUS client shared password (SECRET parameter of **nas** command)	The following single-byte alphanumeric characters and symbols cannot be used. ‘\’ (backslash) ‘[’ ‘]’ ‘?’ ‘ ’ (space) ‘”’ (double quote)	The following single-byte alphanumeric characters and symbols cannot be used. ‘\’ (backslash) ‘[’ ‘]’
User ID in user information (USERID parameter of **user** command) When the authentication method is EAP-TLS	The following single-byte alphanumeric characters and symbols cannot be used. ‘\’ (backslash) ‘/’ ‘[’ ‘]’ ':' ‘<’ ‘*’ ‘>’ ‘|’ ‘?’ ‘ ’ (space) ‘”’ (double quote)	The following single-byte alphanumeric characters and symbols cannot be used. ‘\’ (backslash) ‘/’ ‘[’ ‘]’
User ID in user information (USERID parameter of **user** command) When the authentication method is PAP or PEAP	The following single-byte alphanumeric characters and symbols cannot be used. ‘\’ (backslash) ‘[’ ‘]’ ‘?’ ‘ ’ (space) ‘”’ (double quote)	The following single-byte alphanumeric characters and symbols cannot be used. ‘\’ (backslash) ‘[’ ‘]’

Password in user information (PASSWORD parameter of **user** command)	The following single-byte alphanumeric characters and symbols cannot be used. '\' (backslash) '[' ']' '?' ' ' (space) '"' (double quote)	The following single-byte alphanumeric characters and symbols cannot be used. '\' (backslash) '[' ']'
Name in user information (NAME option of **user** command)	The following single-byte alphanumeric characters and symbols cannot be used. '?' ' ' (space) '"' (double quote)	All single-byte alphanumeric characters and symbols can be used.

Related Documentation

- Interface Control Functions: Port Authentication

Other Information

SNMP MIB Reference

For more information, see the “SNMP MIB Reference” chapter in the HTML version of this document.

- Command Referenceinclude::license.adoc[About Licenses, leveloffset = 2]

Published 02/2025
YJ-A0