P3N1-E202-01ENZ0

XG2000 series

User's Guide

FUJITSU

Preface

You have purchased the XG2000 series, a compact, 20-port 10 Gigabit Ethernet layer 2 switch that achieves unsurpassed standards of high throughput and low-latency performance.
This guide describes the XG2000 series (XG2000 / XG2000R / XG2000C / XG2000CR) functions, installation procedures, configuration operations, and maintenance procedures and should be read and understood before you start using your XG2000 series.

March, 2009

About this Manual

This section describes target readers, contents, notations, etc. of this guide.

Target Readers and Required Knowledge

This guide was written for administrators, who are in charge of network construction, maintenance, and management.
To use this guide, the following knowledge is required.

- Basic knowledge of networks, the Internet, and intranets
- Basic knowledge of system security

This guide omits explanations of network protocol terms.

Contents

This guide to the XG2000 series is composed of the following chapters.

Chapter 1. Features and Functions

Describes the features and functions.

Chapter 2. Using the CLI

Describes operating environment of CLI and how to operate CLI.

Chapter 3. Installation

Describes the necessary installation procedures.

Chapter 4. Functions and Procedures for Setting Functions

Describes how to use the console screen.

Chapter 5. Command References

Describes how to use the commands.

Chapter 6. Managing the Device

Describes the management of the device.

Chapter 7. Troubleshooting

Describes how to solve problems in the device.

Appendix A. Event Logs

Describes the contents of messages reported by the device and actions to be taken for each message.

Appendix B. SNMP Traps

Describes message format of SNMP traps.

Appendix C. List of MIBs

Describes the list of MIBs supported by the SNMP agent

Related Manuals

The following are XG2000 series related manuals. Use these manuals as necessary.

- XG2000 Series Hardware Guide

Describes the hardware of the XG2000 series.

Symbols Used in This Guide

The symbols used in this guide have the following meanings.

Point

indicates useful information related to using the XG2000 series.

Note

indicates precautions to take when using the XG2000 series.

Hint

indicates supplementary information.

Information

indicates related matters such as operation procedures, etc.

Contents

Chapter 1 Features and Functions

This chapter describes the features and functions of the device.

1.1 Features

The XG2000 series is a compact, 20-port 10 Gigabit Ethernet Layer 2 switch.
Special features of the XG2000 series are shown below:

Item	Function	Features
Basic Switch Functions	Throughput	400Gbit/s
	Latency	350ns (Exclude latency of XFPs)
	Switching mode	Either store-and-forward or cut-through is selectable.
	MAC address learning table size	16384 entries
	MAC address learning	SVL (Shared VLAN Learning), IVL (Independent VLAN Learning), user selectable.
	Jumbo frame support	Up to 16KB (16128 bytes).
	Flow control	IEEE802.3x compliant pause frame control. Possible to specify flow control options for each port.
	Storm control	Detects the broadcast storm status to prevent the traffic from overflowing the network and avoid degrading overall system performance.
	Port security	Possible to restrict port access based on a source MAC address.
	Ingress rate control	Supports by-port ingress rate control.
	Port mirroring	Possible to monitor the incoming/outgoing traffic by port mirroring.
	Link pass through	Possible to synchronize the link state of a monitored port with the link state of a single or multiple ports.
Scalability	Link aggregation (Static and LACP)	Possible to increase bandwidth and redundancy. (Up to 10 ports for each link). Also supports IEE802.3ad LACP.
	Uplink Filter	Filtering multicast, broadcast and unlearned unicast frames from leaf nodes to uplink. Possible to configure fat tree using several XG series.
Redundancy	IEEE802.1D STP, IEEE802.1w RSTP	Possible to make a redundant and loop-free network using Rapid Spanning Tree Protocol (upward compatible with Spanning Tree Protocol).
VLAN support	IEEE802.1Q VLAN	Max. 128 groups.
	Filtering	Ingress/egress filtering
	Multiple VLAN	Possible to create multiple tag-based VLAN, with user VLAN tag identifier.
QoS	IEEE802.1p QoS DiffServ	Supports 4 traffic classes based on VLAN priority or DSCP (DiffServ Code Point) of IPv4/IPv6.
	Scheduling	Strict, DRR(Deficit Round Robin), Strict+DRR
Multi-cast support	IGMP snooping	Prevents unnecessary forwarding of multicast traffic to ports to reduce unnecessary multicast traffic.
Network Management	Traffic statistics	Possible to analyze traffic and errors, using traffic statistics.
	SNMP agent	Can be used in conjunction with an SNMP manager, supporting MIBs, including Standard MIB, Bridge MIB, and RMON MIB.
Operation management	Console by serial/management LAN	Dedicated management LAN is isolated from the serial interface and 10 Gigabit ports to secure the device.
	CLI	Allows the user to provide environment settings and operation management using command line interface (CLI).
	Remote authentication	RADIUS and TACACS+

Chapter 2 Using the CLI

This chapter describes how to use the command line interface (CLI) to operate the device.

2.1 Overview of the CLI

This section describes how to use the command line interface (CLI) for the XG Series.

2.1.1 Operating Environment for the CLI

There are two ways to access the device to run commands. Up to 5 terminal sessions can access the device concurrently.

- Serial connection

Connect to the serial port of the device using RS232C cable.
The available terminal emulation type is VT100.
When initially connecting a terminal to the device, configure the serial port on the client side as shown below.

Item	Setting value
Baud rate	9600 bps (can be changed)
Character size	8 bit
Parity	None
Stop bits	1 bit
Flow control	None
Emulation	VT100
Character set	ASCII
Line feed code	Transmission: CR (carriage return) only Reception: LF is added

The baud rate can be changed to one of 9600, 19200, 38400 and 57600 (bps) using the "baud-rate" command.

- Remote connection via management LAN port

Connect a terminal using a telnet or SSH.
The following tables list the factory defaults.

Management LAN Interface initial settings

Item	Setting value
IP address	192.168.0.2
Subnet mask	255.255.255.0

Telnet server initial settings

Item	Setting value
Use telnet	Disable (can be changed)
Port number	23 (TCP)
Emulation	VT100/VT200/xterm
BackSpace key	Delete
Character set	ASCII

SSH server initial settings

Item	Setting value
Use SSH	Disable (can be changed)
Port number	22 (TCP)
Emulation	VT100/VT200/xterm
BackSpace key	Delete
Character set	ASCII
SSH Protocol	Version 2 (not support version 1)

To use the remote connection via the management LAN port, use the "management-lan ip" command to configure the management LAN port for the device and use the "telnet-server" or “ssh-server” command to enable the telnet or SSH service.
A VT100, VT200, or xterm can be used as a terminal.

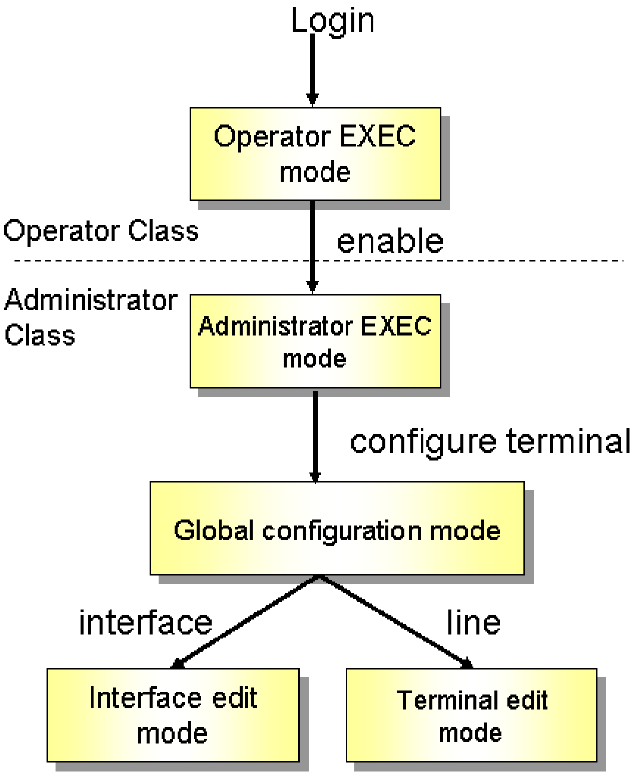
2.1.2 Command Modes and Mode Switching

The following table shows a hierarchy of command modes and mode switching.

Command Modes and Prompt Text (host name for the device: xg)	Outline
Operator class	The initial-level operating mode entered upon logging into the system.
Operator EXEC mode Prompt: `xg>`	Allows access to commands that have no effect on the switch operations. With the device, this mode is mainly used to view its status. The prompt changes to "xg>".
Administrator class	To enter this level, use the "enable" command in the operator class or type the administrator's authentication password.
Administrator EXEC mode Prompt: `xg#`	Allows users to perform operations that are related to the system management of the device, such as date/time setting and firmware update, in addition to those operations that are performed in the operator EXEC mode. The prompt changes to "xg#".
Global configuration mode Prompt: `xg(config)#`	To switch to the global configuration mode, enter the "configure terminal" command in the administrator EXEC mode. This mode allows the user to define the environment settings for the device that are to be saved in a configuration file. The prompt changes to "xg(config)#".

Interface edit mode
Prompt: `xg(config-if)#`
`xg(config-agg)# or`
`xg(config-vlan)#`
	To enter the interface edit mode, enter the "interface" command in the global configuration mode.
	This mode allows the user to configure each port or VLAN of the switch.
	The interface edit mode is represented by prompt "xg(config-if)#", while the edit mode for a port that is created with link aggregation function is represented by prompt "xg(config-agg)#". Also, The edit mode for VLAN is represented by prompt “xg(config-vlan)#”.

Terminal edit mode Prompt: `xg(config-line)#`	To enter the serial terminal edit mode, enter the "line console" command in the global configuration mode. The prompt changes to "xg(config-line)#". Baud rate of the serial terminal and screen display size can be set.



Entering a specific command allows switching from one mode to another. Entering the "exit" command returns program control to the previous mode.
Entering "end" command or pressing [Ctrl] and [Z], or [C] simultaneously in the global configuration, interface edit or terminal edit mode transfers program control to the administrator EXEC mode.

An example is given below.

`Login: admin`
`password: ********`
	Switch to operator EXEC mode by performing a login operation.
	By default, the login username is "admin" and password "password".

`xg> enable`	Use the "enable" command to switch to administrator EXEC mode.
`xg# configure terminal`	Use the "configure terminal" command to switch to global configuration mode.
`xg(config)# interface port 1`	Use the "interface" command to switch to interface edit mode.
`xg(config-if)# exit`	Use the "exit" command to return to global configuration mode.
`xg(config)# exit`	Use the "exit" command to return to administrator EXEC mode.
`xg# copy running-config startup-config`	Copy the current configuration file in memory to the startup-config in the nonvolatile memory.
`xg# exit`	User is logged out and session is disconnected.

Point

- Multiple users can use the operator and administrator EXEC modes concurrently. (Up to 5 terminals)
- Only one terminal can switch to global configuration, interface edit or terminal edit modes at a time. It is not possible for multiple terminals to simultaneously switch to global configuration mode.

Note

- Pressing [Ctrl] and [C] simultaneously in the global configuration, interface edit or terminal edit mode transfers program control to the administrator EXEC mode when “- -more- -“ is displayed in the last line in the console screen.
  (“- -more- -“ is displayed when display command, such as “show”, is executed and information exceed the console screen)

2.1.3 startup-config and running-config

The configuration information is saved to startup-config and running-config files.
This section describes the functions of the startup-config and running-config files.

- startup-config
  Startup-config is the configuration file that stores the environment settings that are enabled upon device startup. The startup-config is saved in non-volatile memory and read the next time the device is reset or power cycled.

- running-config
  Running-config is a file stored in volatile memory that represents the operating environment of the current running system. The information stored in the running-config file will be lost when the system is restarted.
  To assure the system configuration that is active in the current running-config file is enabled the next time the system is started, use the "copy" command to save it to the startup-config file.

  ```
  xg# copy running-config startup-config
  ```

  The contents of the startup-config and running-config match immediately after the device is started.

- How to upload and save the startup-config and running-config files
  To upload the configuration information to the remote server, run the "show" command.

  ```
              Syntax (upload the file on a TFTP server:)
  xg# show running-config | tftp HOST REMOTE-FILE
  or
  xg# show startup-config | tftp HOST REMOTE-FILE
              Syntax (upload the file on a SSH server:)
  xg# show running-config | scp USERNAME HOST REMOTE-FILE
  or
  xg# show startup-config | scp USERNAME HOST REMOTE-FILE
  ```

- How to download startup-config
  To download the configuration information that was uploaded to the remote server as startup-config, run the "copy" command.

  ```
              Syntax (download a file from a TFTP server:)
  xg# copy tftp HOST REMOTE-FILE startup-config
              Syntax (download a file from a SSH server:)
  xg# copy scp USERNAME HOST REMOTE-FILE startup-config
  ```

  To enable the settings downloaded to the startup-config file, restart the device using the "reset" command.

Point

- Be sure to upload the contents of the startup-config file to a remote server because the contents could be lost if the startup-config file is accidentally overwritten.
- Refer to "Uploading/Downloading a Configuration File" for details on uploading and downloading configurations.
- “scp” supports only password authentication, and this device can register up to 10 public keys of SSH servers.
- Execute “clear ssh-rhost-key” command to delete a registered public key.

2.2 Using the CLI

2.2.1 How to Enter Commands

- Command Entry Format

  Separate each command, subcommand and argument with a single space.

  <command> <subcommand> <argument 1> <argument 2> ... (" " indicates a space.)

```
xg(config)# management-interface ip 192.168.1.10/24 default-gw 192.168.1.150
xg(config)# management-interface dns-server 192.168.1.150
```

- Characters that can be entered:
  - Any letter (A-Z, a-z) and digit (0-9)
  - Space (ASCII code: 0x20)
  - Symbols: !, ". #, $, %, `, ', (,   ), _, -, ~, ^, ¥, {, }, :, +, ,, ., @, =, [,], &, *, ;, /, ?, |, >

Command and option separators are recognized as one or more space characters (ASCII code: 0x20). Enclose a parameter in quotes if it contains a blank space.
The commands are not case-sensitive. Note that some entries (password, etc.) are case-sensitive.

2.2.2 Context-Sensitive Help

Entering a question mark "?" at the command prompt displays a list of commands available for each command mode. A list of command's associated with the keywords and parameters will be displayed.

- A list of commands that are available in the current mode

  Entering a question mark "?" at the system prompt displays a list of commands and brief descriptions available for the current command mode.

```
xg # ?
Exec commands:
  boot-system   Change firmware to boot
  clear         Reset functions
  configure     Enter configuration mode
  copy          Copy from one file to another
  date          Manage the system date and time
  delete        Delete files on current system
  dir           List files on current system
      :
  (The rest is omitted.)
xg# _
```

- Word help

  Entering a question mark "?" in the middle of a command name, will list the possible command options required to complete the command. The prompt will show the letters previously typed. Enter the rest of the letters to complete the command entry.

```
xg # co?
Exec commands:
  configure      Enter configuration mode
  copy           Copy from one file to another
xg# co_
```

The CLI lists all possible commands that begin with "co".

- A list of options that are available in the current entry position

  Entering a question mark "?" followed by a space after typing a command name, will cause the CLI to list the possible commands or keywords that may be entered at the current option position. For option 2 and 3 positions, the CLI also lists options
  that can be entered at these positions. The prompt will show the letters previously typed. Enter the rest of the letters to complete the command entry.

```
xg# configure ?
terminal   Configure from the terminal

xg# configure _
```

CLI lists possible options that follow the "configure" command.

The <cr> symbol may appear in the list to indicate that the command can be executed without entering any subsequent options. Parameters enclosed in square brackets can be omitted and, therefore, the <cr> symbol does not appear.

2.2.3 Command Completion

Entering part of a command or option and pressing the [Tab] key, causes the CLI to display the remaining command or option characters.

```
xg# con<TAB>
              ↓
xg# configure _
```

For example, the only command that begins with "con" is "configure", so the CLI completes the command name as "configure". Pressing the [Tab] key, causes the CLI to list all possible commands or option names.

```
xg# co<TAB>
configure copy
xg# co_
```

Since there are two commands that begin with "co" - "configure" and "copy" - the CLI lists both commands.

2.2.4 Command Abbreviation

Commands and options can be abbreviated to the minimum number of characters as long as command or option names are unique and forward-match the entered letters.

```
xg# con t
```

For example, the "configure" command may be abbreviated to "con" because "configure" is the only command that begins with "con", and "terminal" may be abbreviated to "t" because "terminal" is the only command that begins with "t".

2.2.5 Command-Line Error Messages

The table below shows error messages that appear when a command is incorrectly entered. The "configure terminal" command is used as an example below:

Error Message	Explanation

`xg# co t`
`% Ambiguous command: "co t"`
	Insufficient characters were entered for the CLI to recognize the command.
	Re-enter the correct command string.

`xg# configure`
`% Incomplete command.`
	All of the options or values required by this command were not entered.
	Enter all necessary options and values.

`xg# configure aerminal`
`              ^`
`% Invalid input detected at '^' marker`
	The command incorrectly entered. A caret symbol (^) indicates the incorrect entry.
	Correct the entries and execute the command again.

`xg# coc?`
`% Unrecognized command`
	Part of the command was incorrectly entered.
	Re-enter the correct command string.

2.2.6 Scrolling Down or Up a Line or a Page

When the information displayed by a command contains more lines than the console screen will display, a "--More--" prompt is displayed at the bottom of the screen and the CLI waits for a user entry.

```
xg# show running-config
!
interface port 1
    :
    :
(The rest is omitted.)
    :
--More--
```

- Scrolling Up a Line
  `To scroll up one line, press the [Enter] key.`
- Scrolling Up a Page
  `To scroll up one page, press the [Space] bar.`
- Finishing Displaying
  `To finish displaying, press the [q] or [Q] key.`

The following table shows the combinations of shortcut keys, function keys and the [Ctrl] key used to edit commands.

Combinations of keys	Description
"↑" or [Ctrl] + [P]	Recalls the previous command.
"↓" or [Ctrl] + [N]	Recalls the next command.
"←" or [Ctrl] + [B]	Moves the cursor back one character.
"→" or [Ctrl] + [F]	Moves the cursor forward one character.
[Home] or [Ctrl] + [A]	Moves the cursor to the first character in line.
[End] or [Ctrl] + [E]	Moves the cursor to the last character in line.
[Esc] + [B]	Moves the cursor back one word (to the beginning of a parameter).
[Esc] + [F]	Moves the cursor forward one word (to the beginning of a parameter).
[Backspace]	Erases the character to the left of the cursor and moves the cursor back one character.
[Delete] or [Ctrl] + [D]	Deletes the character to the right of the cursor.
[Ctrl] + [W]	Records the character to the left of the cursor before deleting.
[Ctrl] + [U]	Records the command line before deleting.
[Ctrl] + [K]	Records all characters to the left of the cursor before deleting.
[Ctrl] + [Y]	Pastes a string recorded by [Ctrl]+[W], [U] or [K].
[Ctrl] + [L]	Erases the current screen.
[Ctrl] + [C]	Runs command result and aborts output.
[Enter], [Ctrl] + [J], or [Ctrl] + [M]	Completes a command entry.
[Ctrl] + [T]	Transposes the character located at the cursor with the character to the left of the cursor.

Hint

If any of the above key combinations or command completion displays using the [Tab] key do not work correctly, the correct VT100, VT200 or xterm terminal emulation type may not be selected.

2.2.7 Command History

Command history is a function that records command lines previously entered so they can be reused.
It is useful for repeatedly entering the same command line or for entering a similar command.

- To display the previous command line in the history:
  Press the up arrow key or [Ctrl]+[P] to recall the previous command in the history to the prompt.
  Repeat the key sequence to recall successively older commands.
- To display a more recent command line:
  Press the down arrow key or [Ctrl]+[N] to bring up the next line from the command history to the prompt.
  Repeat the key sequence to bring up successively more recent commands.
- To list the command history:
  Use the "show history" command to view the list of commands saved in the history:
  For each login up to 100 lines of command history can be registered.

2.2.8 Aborting Command

An executing command can be aborted by pressing [Ctrl]+[C]. Note that this key sequence may not be effective for some commands.

2.2.9 No Form of Commands

Almost every configuration command has a no form. In general, the no form is used to cancel the settings of a configuration command or restore default values.
Type "no" before entering a command name.
For details on using the no form, refer to the "Command Reference".

2.2.10 Filtering show Command Output

This function allows filtering the show command output so lines that only satisfy specific conditions (filter for strings) are displayed. This function is useful in excluding unnecessary information from a large amount of output.
To use it, a "show" command must be followed by a keyword (pipe (|), begin, include or exclude) and a regular expression (filtering condition).

Syntax

```
show ・・・・・・ | {begin | include | exclude} regular-expression
```

Keyword for filtering output	Meaning
begin	Begins output starting at the first line that contains matches to given regular expression parameters.
exclude	Does not display output lines that contain matches to given regular expression parameters.
include	Displays output lines that contain matches to given regular expression parameters.

```
xg# show history | begin 2
...skipping
2 configure terminal
3 show running-config
4 show history
5 show history | begin 2
```

```
xg# show history | exclude 2
1 enable
3 show running-config
4 show history
```

```
xg# show history | include 2
2 configure terminal
5 show history | begin 2
```

Hint

Regular expressions are case sensitive.
For example, if "| exclude strings" is entered, lines that include "String" are output, but those that include "strings" are not.

2.2.11 Redirecting show Command Output

Redirect the output of "show" commands to a file in volatile memory using ">" (pipe) or "|" (redirect).

Syntax (To redirect the output of a show command to a file in volatile memory:)

```
show ・・・・・・ > FILE-NAME
show ・・・・・・ | FILE-NAME
```

- FILE-NAME
  Specifies the file name in volatile memory that the output of the command is piped or redirected.

"| tftp" or "| scp" redirects the output of the show command to a file on a remote server.

Syntax (Redirect the output of a show command to a file on a TFTP server:)

```
show ・・・・・・ | tftp HOST REMOTE-FILE
```

Syntax (Redirect the output of a show command to a file on a SSH server:)

```
show ・・・・・・ | scp USERNAME HOST REMOTE-FILE
```

- | tftp
  Redirects the copy to a file on the TFTP server.
- | scp
  Redirects the copy to a file on the SSH server.
- USERNAME
  Specifies the username of the SSH server.
- HOST
  Specifies the host name or IP address of the TFTP server or SSH server.
- REMOTE-FILE
  Specifies the file name in the TFTP server or SSH server that the output of the command is redirected.

In the following example, the current startup-config is redirected as filename "startup_09302005", the running-config file is redirected as filename "running_09302005", and system information is redirected as filename "system_09302005".
The results of the redirection are confirmed with the "ls" command.
Then, using the "tftp" command, each of these files are moved to the TFTP server.

```
xg# show startup-config > startup_09302005
xg# show running-config > running_09302005
xg# show system information > system_09302005
xg# ls
```

(ls command output)

```
  Update-time          File-size  File-name
- 2005/09/30 11:57:27       872   system_09302005
- 2005/09/30 11:54:01     2,310    startup_09302005
- 2005/09/30 11:55:58     2,437    running_09302005
```

```
xg# tftp put remote-host1 startup_09302005 restore_startup_09302005
xg# tftp put remote-host1 running_09302005 restore_running_09302005
xg# tftp put remote-host1 system_09302005 restore_system_09302005
```

In the following example, show command output is redirected to TFTP server "remote-host1" using "| tftp".

```
xg# show startup-config | tftp remote-host1 restore_ startup_09302005
xg# show running-config | tftp remote-host1 restore_running_09302005
xg# show system information | tftp remote-host1 restore_system_09302005
```

In the following example, show command output is redirected to SSH server "remote-host2" using "| scp".

```
xg# show startup-config | scp foo remote-host2 restore_ startup_07012008
remote-host2's password:
xg# show running-config | scp foo remote-host2 restore_running_07012008
remote-host2's password:
xg# show system information | scp foo remote-host2 restore_system_07012008
remote-host2's password:
```

Point

- "scp" supports only password authentication, and this device can register up to 10 public keys of SSH servers.
- Execute "clear ssh-rhost-key" command to delete a registered public key.

2.2.12 Using the monitor Command

The monitor command provides additional key commands to perform screen navigation.
The following table shows the keys used to perform screen-related operations.

Displayed item	Meaning
ESC:exit	Press the [Esc] key to close the monitor screen.
F:refresh	Press the [F] or [f] key to refresh the screen.
U:page up	Press the [U] or [u] key to scroll up to the previous page. If the current page is the first page of the display nothing occurs.
D:page down	Press the [D] or [d] key to scroll down to the next page. If the current page is the last page of the display, nothing occurs.
L:page left	Press the [L] or [l] key to scroll the screen to the left. If there are no additional columns of data to the left to display, nothing occurs.
R:page right	Press the [R] or [r] key to scroll the screen to the right. If there are no additional columns of data to the right of the display, nothing occurs.

Chapter 3 Installation

This chapter describes the installation procedures for the device.
Refer to "Using the CLI" for details on using the CLI.
Refer to "Command Reference" for details on commands.

3.1 Workflow for Initial Setup of the Device

This section describes the procedures to setup the device.

1. **Prepare a terminal**
   Prepare a terminal for the initial configuration.
2. **Setting Up the Serial Interface**
   Connect the device and terminal with an RS232C cable. The initial baud rate setting is 9,600 bps.
3. **Turn on the device to start the system.**
   Turn on the terminal and the device to start the system.
4. **Configure Management LAN Interface**
   The initial setting of the management LAN interface is disabled.
   To use the following functions, set up the management LAN interface:
   - Telnet connection
   - SSH connection
   - SNMP manager connection
   - System log transmission
   - Time synchronization using an NTP server
   - Configuration file upload/download
   - Firmware update
   - Collection of maintenance information
5. **Telnet Connection via Management LAN Interface (Optional)**
   The initial setting of the Telnet connection via the management LAN interface is disabled.
   (IP address: 192.168.0.2, subnet address: 255.255.255.0)
6. **SSH Connection via Management LAN Interface (Optional)**
   The initial setting of the SSH connection via the management LAN interface is disabled.
7. **SNMP Configuration (Optional)**
   Initially, the SNMP agent configuration is not set.
   Set the SNMP configuration as needed.
8. **This is the end of the preparation procedure**
   Proceed with configuring the switch.

3.1.1 Setting Up the Serial Interface

Connect the device and terminal with an RS232C cable. The initial setting of baud rate setting is 9,600 bps.
Refer to "Operating Environment for the CLI" for details on settings.

For serial interfaces, only the baud rate can be changed. To change the serial interface settings, carry out the following procedure.

Command	Task

`xg login: admin`
`Password: ********`
	Login to the device from the serial terminal. The default user name is "admin". The default password is "password".

`xg> enable`	Switch to administrator EXEC mode.
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# line console`	Switch to serial terminal edit mode.
`xg(config-line)# baud-rate {9600 | 19200 | 38400 | 57600}`	Change serial baud rate. The baud rate is changed after the logout.
`xg(config-line)# exit`	Exit to global configuration mode.
`xg(config)# terminal timeout console MINUTES`	(Optional) If the terminal is idle after the timeout period (in minutes) expires the serial connection is terminated. The default is 10 minutes.
`xg(config)# exit`	Exit to administrator EXEC mode.

3.1.2 Configure Management LAN Interface

The management LAN interface is initially enabled.

```
      (IP address: 192.168.0.2, subnet address: 255.255.255.0)
```

To use the following functions, configure the management LAN interface.

- Telnet connection (enabled by default)
- SSH connection (disabled by default)
- SNMP manager connection
- System log transmission
- Time synchronization using an NTP server
- Configuration file upload/download
- Firmware update
- Collection of maintenance information

To configure the management LAN interface, carry out the following procedure.

Command	Task

`xg login: admin`
`Password: ********`
	Login to the device from the serial terminal. The default user name is "admin". The default password is "password."

`xg> enable`	Switch to administrator EXEC mode.
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# management-lan ip A.B.C.D/M [ default-gw A.B.C.D]`	Change the IP address and subnet, and set the default gateway of the management LAN interface.
`xg(config)# management-lan dns-server A.B.C.D`	(Optional) Set up DNS servers. Up to 4 DNS servers can be set up. Priority is assigned to DNS servers in the order they are defined. To change their order, delete them using the no command before doing so.
`xg(config)# management-lan domain DOMAIN-NAME`	(Optional) Set the name of the network domain.
`xg(config)# remote-host A.B.C.D HOST-NAME`	(Optional) Associate a remote host name with an IP address. This allows referencing a remote IP address with a host name without relying on a DNS server.
`xg(config)# exit`	Exit to administrator EXEC mode.

3.1.3 Telnet Connection via the Management LAN Interface (Optional)

The "Telnet server function" via the management LAN interface is initially disabled.

To change the monitoring time for the telnet connection, carry out the following procedure in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# telnet-server`	Enable Telnet connection,
`xg(config)# terminal timeout vty <0-60>`	(Optional) If the Telnet session timeout period (in minutes) expires the telnet connection is terminated.
`xg(config)# exit`	Exit to administrator EXEC mode.

3.1.4 SSH Connection via the Management LAN Interface (Optional)

This device supports the “SSH server function”. This function is remote connection like “Telnet server function”.
After executing “ssh-server” command, the “SSH-server” is enabled and authentication key is generated (It takes some time to generate authentication key).
The following shows the “SSH-server function” supported by this device.

Function	Support
Protocol Version	v2
Method of authentication	Password
Authentication key	RSA(2048bits, fixed), DSA(1024bits, fixed)
Method to generate authentication key	Automatically generated, CLI
Method of coding	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr
Terminal sessions	Maximum 4 (including Telnet connection)
Message authentication code	hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-sha1-96,hmac-md5-96

The "SSH server function" via the management LAN interface is initially disabled.
To change the monitoring time for the SSH connection, carry out the following procedure in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# ssh-server`	Enable SSH connection
`xg(config)# terminal timeout vty <0-60>`	(Optional) If the SSH session timeout period (in minutes) expires the SSH connection is terminated.
`xg(config)# exit`	Exit to administrator EXEC mode.

The “SSH-server function” supported by this device uses Open SSH free software that is published based on BSD licence.
Please refer to the following URL for more details.
http://www.openssh.com/

3.1.5 SNMP Configuration (Optional)

To operate in conjunction with an SNMP manager, the SNMP agent must be configured.
To configure the SNMP agent, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# hostname HOST-NAME`
`xg(config)# snmp-server location`
` SYSTEM-LOCATION`
`xg(config)# snmp-server contact`
`SYSTEM-CONTACT`
	Set the switch name (HOST-NAME), switch's location (SYSTEM-LOCATION), and contact (SYSTEM-CONTACT).

`xg(config)# snmp-server access host`
` {A.B.C.D|HOSTNAME} community COMMUNITY-NAME`
	Set the IP address (host name) of the SNMP manager and the community name.

`xg(config)# snmp-server trap host`
`{A.B.C.D|HOSTNAME} community COMMUNITY-NAME`
`[protocol {v1|v2c}]`
	Set the IP address (host name) of the host that is notified of SNMP traps and community name, if the SNMP trap notification is enabled.

`xg(config)# exit`	Exit to administrator EXEC mode.

Chapter 4 Switch Functions and their Configuration

This chapter describes the functions of the device and how to configure them.
Refer to "Operating Environment for the CLI" for details on using the CLI.
Refer to "Command Reference" for details on commands.

4.1 Basic Switch Functions

This section describes the basic switch functions.

4.1.1 Switching Mode

The device provides the following two switching modes.

- Store-and-forward switching mode
  After the device finishes receiving a frame, it checks the FCS (Frame Check Sequence) and performs a validity check (on packet size, etc.) before forwarding the frame. If the switch receives a frame with an error frame, it discards it.
- Cut-through switching mode
  The device transmits the frame to the destination as soon as the first 64 bytes of the frame are received with no errors. Since the device starts transmitting the frame before it receives the entire frame, this mode allows forwarding at low latency.

To change the switching modes, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# bridge forward-mode {cut-through | store-and-forward }`
`xg(config)# no bridge forward-mode`
	Select the cut-through (or store-and-forward) for the switching mode.

`xg(config)# exit`	Exit to administrator EXEC mode.

4.1.2 MAC Address Table Management

The MAC address table is a database used for managing the association between address information and destination ports. The device can learn up to 16384 entries of MAC addresses.

- MAC address table management
  The device has two methods for MAC address table management.
  - SVL(Shared VLAN Learning)
    The device learns MAC addresses common to all VLANs. Different VLANs with identical MAC addresses are treated as identical entries.
  - IVL(Independent VLAN Learning)
    The device learns MAC addresses separately for each VLAN. Identical MAC addresses with different VLANs are treated as separate entries.

  To change the MAC address table management modes, carry out the following procedures in the management EXEC mode.

Command	Task
`xg# configure terminal`	Switch to the global configuration mode.

`xg(config)# bridge learn-mode { ivl | svl }`
`xg(config)# no bridge learn-mode`
	Select IVL or SVL for the MAC address table management mode.

`xg(config)# exit`	Exit to administrator EXEC mode.
`xg# copy running-config startup-config`	Save the current settings of the device to nonvolatile memory.
`xg# reset`	If the MAC address table management mode is changed, the new setting becomes enabled after the device is restarted.

- Dynamic MAC address learning
  The device dynamically learns MAC addresses from received frames. If MAC addresses are not refreshed before the aging time expires, they will be removed from the MAC address table. To disable the dynamic learning, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# interface port 1 2 3`
`xg(config)# interface port range 1 3`
	Switch to the interface edit mode to specify the port(s) to be configured.
	In this example, the global interface configuration mode is selected for ports 1 through 3.

`xg(config-if)# suppress-address-learning`
`xg(config-if)# no suppress-address-learning`
	Enable (or disable) the dynamic MAC address learning.

`xg(config-if)# exit`	Exit to global configuration mode.
`xg(config)# exit`	Exit to administrator EXEC mode.

- Static unicast address

  By registering a unicast MAC address with the MAC address table, unicast frames are forwarded to a specified port. Static unicast addresses are not subject to MAC address removal controlled by the aging function.
  To register, change or delete a static unicast address, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# bridge mac-address-table static MAC [vlan <1-4094>] {[port <1-20>] | [agg-port <1-10>]}`
 	
`xg(config)# no bridge mac-address-table static MAC [vlan <1-4094>]`
	Register a static unicast address and destination port with the MAC address table (or remove them from it).

`xg(config)# exit`	Exit to administrator EXEC mode.

- Static multicast address

  By registering a multicast MAC address with the MAC address table, a specific multicast frame will be forwarded to a designated port.
  To register, change or delete a multicast address, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# bridge mac-address-table static MAC [vlan <1-4094>] [port <1-20> [<1-20> ・・・]] [agg-port <1-10> [<1-10> ・・・]]`
 	
`xg(config)# no bridge mac-address-table static MAC [vlan <1-4094>]`
	Register (or remove) a static multicast address table and destination port.
	For a multicast MAC address, multiple ports can be specified.

`xg(config)# exit`	Exit to administrator EXEC mode.

4.1.3 Jumbo Frame Support

The device can transmit jumbo frames of up to 16KB (16128 bytes).
To configure jumbo frame support, carry out the following procedure in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# bridge jumbo-frame [{9216 | 12288 | 15360 | 16128}]`
 	
`xg(config)# no bridge jumbo-frame`
	Enable (or disable) jumbo frame support.

`xg(config)# exit`	Exit to administrator EXEC mode.

4.1.4 Flow Control

Flow control is a function that prevents frame loss when the receive buffer in the switch overflows due to temporary traffic overload by using a PAUSE frame.
When the device receives a PAUSE frame, it temporarily stops sending frames at the receive port. If the receive buffer overflows, it is possible to restrict frame transmission from the connected device by sending a PAUSE frame.
For each port, it is possible to select whether or not to send/recive a PAUSE frame.
To change the flow control mode, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# interface port 1 2 3`
 	
`xg(config)# interface port range 1 3`
	Switch to the interface edit mode to specify the port(s) to be configured for flow control.
	In this example, the global interface configuration mode is selected for ports 1 through 3.

`xg(config-if)# flowcontrol { disable | only-receive | only-send | send-receive }`	Set the flow control mode.
`xg(config-if)# exit`	Exit to global configuration mode.
`xg(config)# exit`	Exit to administrator EXEC mode.

4.1.5 Storm Control

The device discards broadcast frames when the number of received broadcast frames are over a given threshold to prevent unnecessary waste of bandwidth due to retained broadcast frames on the network. This function is called "Storm Control".
For each port, it is possible to configure storm control.
When broadcast frames are discarded by storm control, error logs are output, and storm control logging is disabled. To re-enabled logging, these violations must be cleared with "clear violation".
To configure storm control, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# interface port 1 2 3`
`xg(config)# interface port range 1 3`
	Switch to the interface edit mode to specify the port(s) to be configured for storm control.
	In this example, the global interface configuration mode is selected for ports 1 though 3.

`xg(config-if)# storm-control`	Enable storm control.
`xg(config-if)# exit`	Exit to global configuration mode.
`xg(config)# exit`	Exit to administrator EXEC mode.

4.1.6 Port Security

Port security blocks connections attempted by unregistered hosts. When a host MAC address is registered, the device receives only those frames that use registered source addresses.
For each port, it is possible to configure port security. To register a MAC address for a host, use the "bridge mac-address-table static" command. The port that the host is connected must be registered as a member port. In Independent VLAN Learning mode, this must be done for all VLANs that permit transmission.
Either of the following two modes can be specified for a security-violating (unregistered) frame the device receives.

- Restrict mode
  Filters violating frames only, forwarding permitted frames.
- Shutdown mode
  Filters all frames upon reception of a violating frame, and the port goes link down.

Once a security violation is detected, an error log is recorded. No further detection of a violating frame will cause an error log to be recorded until security violations are reset by "clear violation".
To configure port security, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# interface port 1 2 3`
`xg(config)# interface port range 1 3`
	Switch to the interface edit mode to specify the port(s) to be configured for port security.
	In this example, the global interface configuration mode is selected for ports 1 though 3.

`xg(config-if)# port-security violation {restrict | shutdown}`	Enable Port Security.
`xg(config-if)# exit`	Exit to global configuration mode.
`xg(config)# exit`	Exit to administrator EXEC mode.
`xg# clear violation all`	Clear security violations

4.1.7 Ingress Rate Control

It is possible to set an ingress rate-limiting value for each port in approximately 40Mbps increments.
To set an ingress rate-limiting value, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# interface port 1 2 3`
`xg(config)# interface port range 1 3`
	Switch to the interface edit mode to specify the port(s) to be configured for ingress rate control.
	In this example, the global interface configuration mode is selected for ports 1 though 3.

`xg(config-if)#ingress-bandwidth <40-10000>`	Specify an ingress rate limiting value.
`xg(config-if)# exit`	Exit to global configuration mode.
`xg(config)# exit`	Exit to administrator EXEC mode.

Note

- The ingress rate is measured at 100us time intervals. Should burst transfers take place at intervals of 100us or over, the ingress rate the device actually allows may be less than the specified value.

4.2 Port Mirroring

It is possible to monitor the traffic by mirroring the frames sent or received by a port to another port.
To configure port mirroring, carry out the following procedure in the administrator EXEC mode.

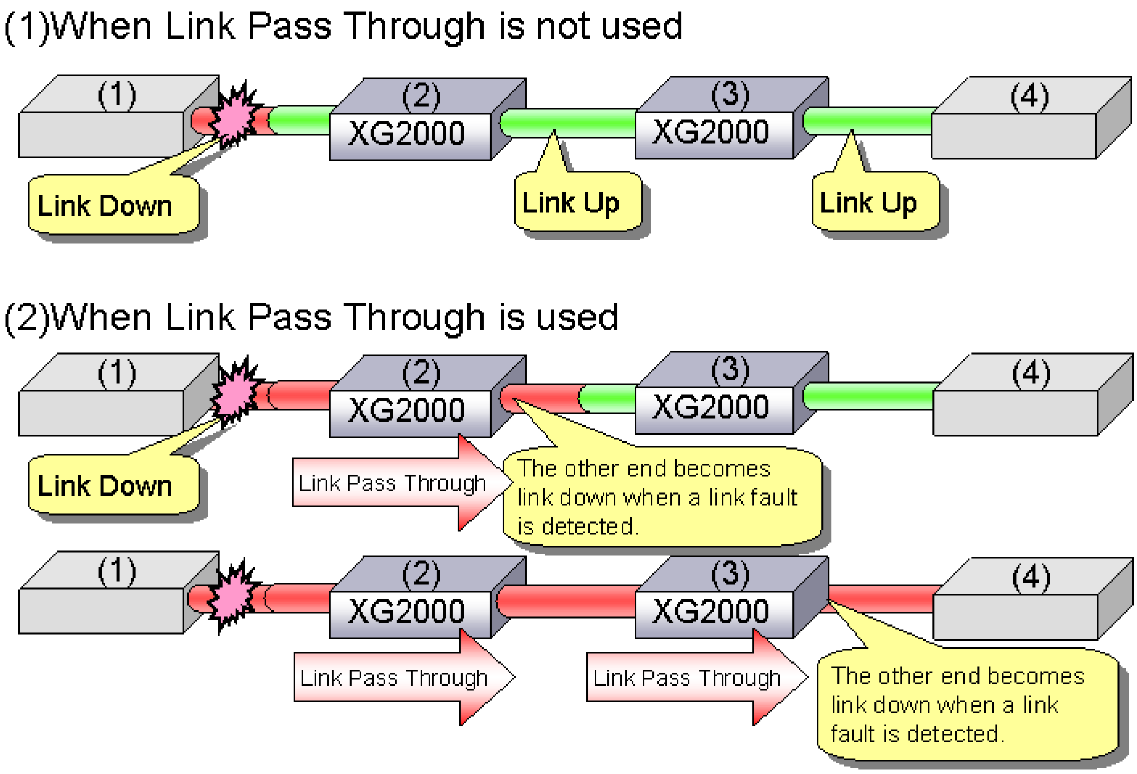
Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# mirror monitored-port <1-20>`
`[rx-mirroring-port <1-20>]`
`[tx-mirroring-port <1-20>]`
	Configure the port to be monitored and its mirror port to be mirrored.

`xg(config)# exit`	Exit to administrator EXEC mode.
`xg# show mirror`	View the status of port mirroring.

4.3 Link Pass Through

Link pass through is a function that monitors the status of a specified port link and notifies the device connected to the port via link status notification of the link status of a monitored port by synchronizing the monitored port with the link status on the port.


(1)When Link Pass Through is not used
(1)
(2)
XG2000
(3)
XG2000
(4)
Link Down
Link Up
Link Up
(2)When Link Pass Through is used
(1)
(2)
XG2000
(3)
XG2000
(4)
Link Down
Link Pass Through
The other end becomes link down when a link fault is detected.
(1)
(2)
XG2000
(3)
XG2000
(4)
Link Pass Through
Link Pass Through
The other end becomes link down when a link fault is detected.

Link Pass Through

This function allows the device to notify the port, after link status notification, of a link fault if detected at the monitored port. Link pass through communicates the link fault status to the other port by sending a remote fault (RF) signal, as prescribed in IEEE802.3ae LFS (Link Fault Signaling). When the link status of the monitored port is restored to normal, the other port is also restored to normal, thereby restoring the network link.

To configure Link pass through, carry out the following procedure in the administrator EXEC mode.

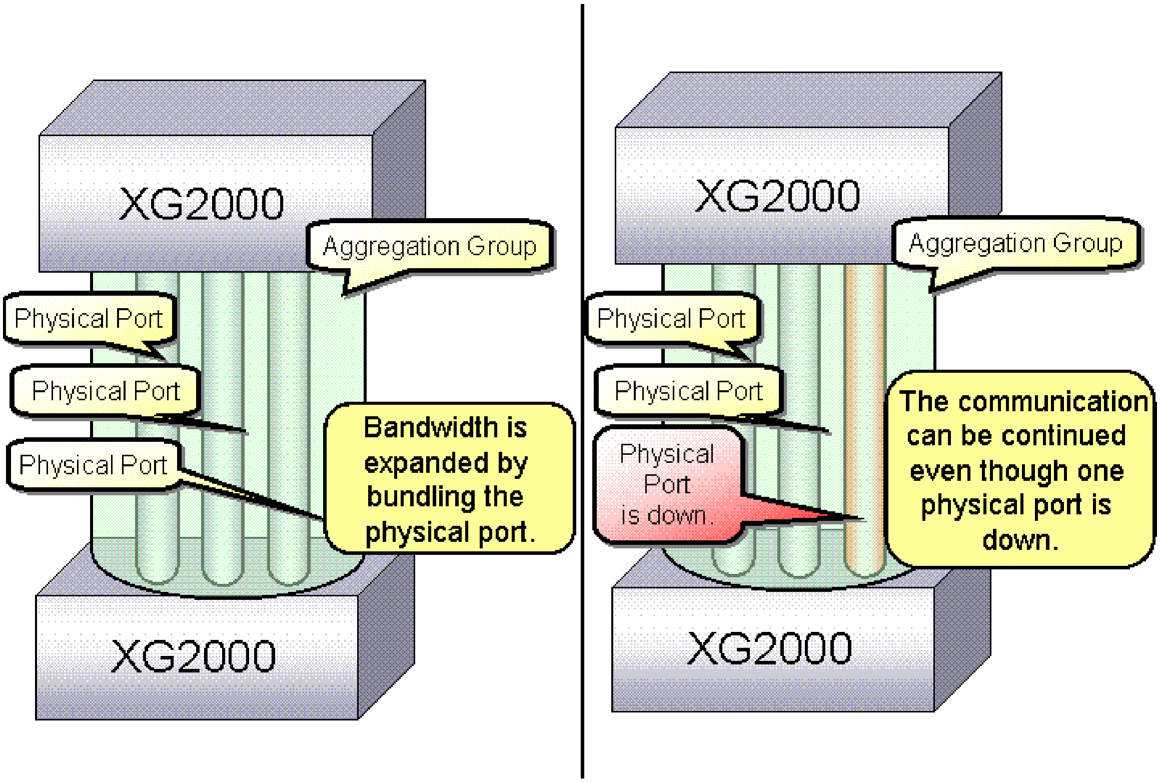
Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# link-pass-through { monitored-port <1-20> | monitored-agg-port <1-10>} [domino-port <1-20> [<1-20> ・・・]] [domino-agg-port <1-10> [<1-10> ・・・]]`	Set the relationship between the ports to be monitored and ports link status notification were sent.
`xg(config)# exit`	Exit to administrator EXEC mode.

4.4 Link Aggregation

Link aggregation is a function that combines multiple ports into a single logical link. A set of ports that comprise a logical link is called an aggregation group.
Link aggregation provides:

- Increased bandwidth
  By grouping multiple physical ports into a single logical link (an aggregation group), network traffic (data sent and received) will be balanced across the physical ports, thereby providing increased bandwidth.
- Redundancy
  Multiplexing ports allows uninterrupted network operations should one of the multiple links fail. Since the link status of the logical aggregation groups remains unchanged, there are no fluctuations in network traffic, the effect of a fault having been minimized.

Up to 10 ports can be used to create a single link aggregation group using link aggregation. Up to 10 aggregation groups can be created.



Link Aggregation

4.4.1 Configuring Link Aggregation

Either static or dynamic (also known as LACP) configuration can be selected for Link Aggregation.

- Static configuration
  Configures aggregation groups statically.
- LACP
  Configures link aggregation using Link Aggregation Control Protocol (LACP). The LACP is a switch-to-switch control protocol that enables dynamic configuration of aggregation groups and is standardized by the IEEE802.3ad. The LACP facilitates load balancing across the individual links aggregated between the devices connected.
  Either "active" or "passive" LACP mode can be selected.
  - **active**
    The device starts LACP negotiation. Since the active mode allows the reception of LACP control frames, it is possible to direct the device in "active" mode.
  - **passive**
    The device responds to LACP control frames but does not start LACP negotiation.

To configure static link aggregation, carry out the following procedure in the administrator EXEC mode.

Command	Task
xg# configure terminal	Switch to global configuration mode.
xg(config)# link-aggregation agg-port <1-10> protocol none port <1-20> <1-20> ・・・	Assign a number to the aggregation group to be created (agg-port) and the port numbers assigned to the link aggregation. Specify "none" for static configuration.
xg(config)# interface agg-port <1-10>	To change the setting of the aggregation group created, switch to the interface edit mode for the aggregation group and specify the "interface agg-port" requiring change. The prompt changes to "config-agg".
xg(config-agg)# port-vlan-id vlan 2	(Optional) Change the setting of the aggregation group as required. In this example, default VLAN ID is set to 2.
xg(config-agg)# exit	Exit to global configuration mode.
xg(config)# exit	Exit to administrator EXEC mode.

To configure LACP link aggregation, carry out the following procedure in the administrator EXEC mode.

Command	Task
xg# configure terminal	Switch to global configuration mode.
xg(config)# link-aggregation agg-port <1-10> protocol lacp lacp-mode {active | passive } port <1-20> <1-20> ・・・	Assign a number to the aggregation group to be created (agg-port) and the port numbers assigned to the link aggregation. Specify "lacp" for LACP link aggregation. Specify the desired negotiation operational mode in "lacp-mode".
xg(config)# interface agg-port <1-10>	To change the setting of the aggregation group created, switch to the interface edit mode for the aggregation group and specify the "interface agg-port" requiring change. The prompt changes to "config-agg".
xg(config-agg)# port-vlan-id vlan 2	(Optional) Change the settings of the aggregation group as required. In this example, default VLAN ID is set to 2.
xg(config-agg)# exit	Exit to global configuration mode.
xg(config)# exit	Exit to administrator EXEC mode.

4.4.2 Frame Distribution Methods in Link Aggregation

How frames are distributed across physical ports that make up an aggregation group are determined by the contents of a frame (source and destination MAC addresses).
There are three ways to specify how frames are distributed:

- Frame distribution based on destination MAC address (dst-mac)
  The destination port is determined based on the destination MAC address of the frames.
- Frame distribution based on source MAC address (src-mac)
  The destination port is determined based on the source MAC address of the frames.
- Frame distribution based on destination and source MAC addresses (dst-src-mac)
  The destination port is determined based on the destination and source MAC addresses of the frames.

> Point
>
> - If there are too few MAC addresses to be distributed across an aggregation group, the distribution of frames across the destination ports tends to become biased. To reduce such bias, use a distribution method that uses more MAC addresses.
>   For example, if a server is connected to an aggregation group and a client is connected to a different port, the "src-mac" or "dst-src-mac" parameters are recommended.

To set a distribution method, carry out the following procedure in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# link-aggregation agg-port <1-10>`
`protocol {none | lacp}`
`load-balance dst-mac|src-mac|dst-src-mac}`
`port <1-20> <1-20> ・・・`
	Specify a distribution method in the load-balance parameter of the "link-aggregation" command.

`xg(config)# exit`	Exit to administrator EXEC mode.

4.4.3 The Number of Ports That Require Linkup

It is possible to specify the number of ports that enable a linkup state for an aggregation group. If the number of active ports that make up an aggregation group in a linkup state is less than the specified number of ports, the aggregation group changes to a linkdown state.

- For static link aggregation
  If the number of ports that make up an aggregation group in a linkup state no longer satisfies the specified number of ports, the aggregation group changes to a linkdown state.

- For LACP link aggregation
  If the number of ports that make up an established LACP aggregation group changes, the aggregation group reverts to a linkdown state.

To set the number of ports in the aggregation group, carry out the following procedure in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# link-aggregation agg-port`
`<1-10>`
`protocol {none | lacp} minimum-port <1-20>`
`port <1-20> <1-20> ・・・`
	Specify the required number of ports in "minimum-port" parameter of the "link-aggregation" command.
	The default value for "minimum-port" parameter is 1.

`xg(config)# exit`	Exit to administrator EXEC mode.

4.4.4 Notes on Link Aggregation

The smallest port number in an aggregation group serves as the master port.
Port settings established after defining an aggregation group inherit the same settings as those of the master port, with some exceptions. The settings that are not inherited from the master port are.

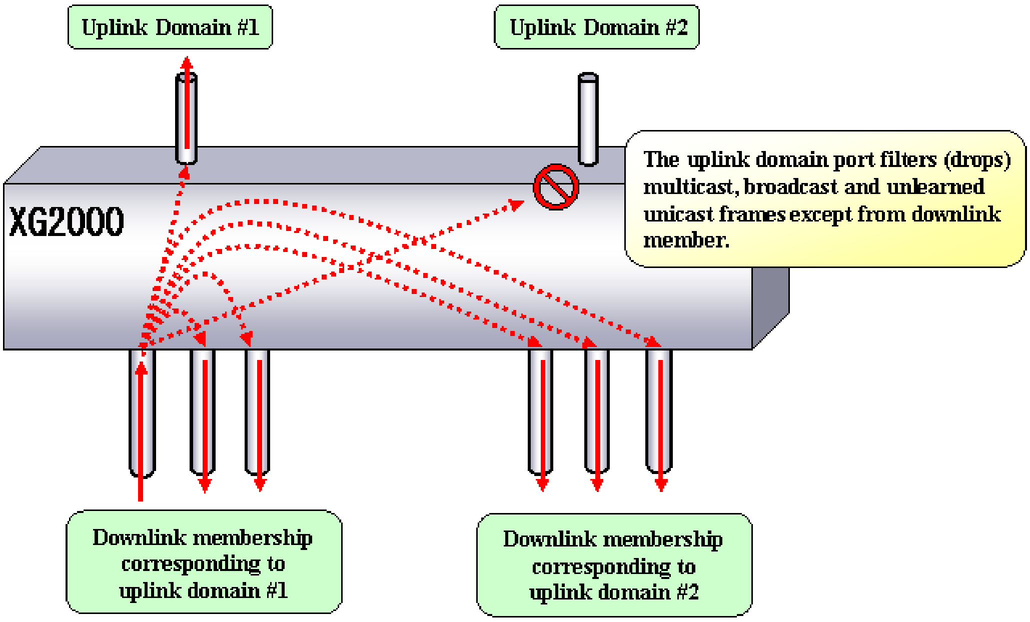
- "link-pass-through"
  `Settings for these ports are cleared.`
- The information registered in MAC address table
  `All addresses related to ports configured are cleared.`
- "spanning-tree port-path-cost"
  `Port-path-cost will be re-adjusted to match the new configuration.`

When changing the port settings for aggregation groups that have already been created, the aggregation group changes to a linkdown state, and then to a linkup state if one of the following conditions are satisfied.

- A master port was removed
- A master port changed
- The "protocol" or "lacp-mode" parameter changed

4.5 Uplink Filter

When an uplink domain is defined, the domain's uplink domain ports filter (drops) multicast, broadcast and unlearned (flooding) unicast frames from non-membership downlink ports. However it does not filter learned unicast frames that are forwarded based on the MAC address table.

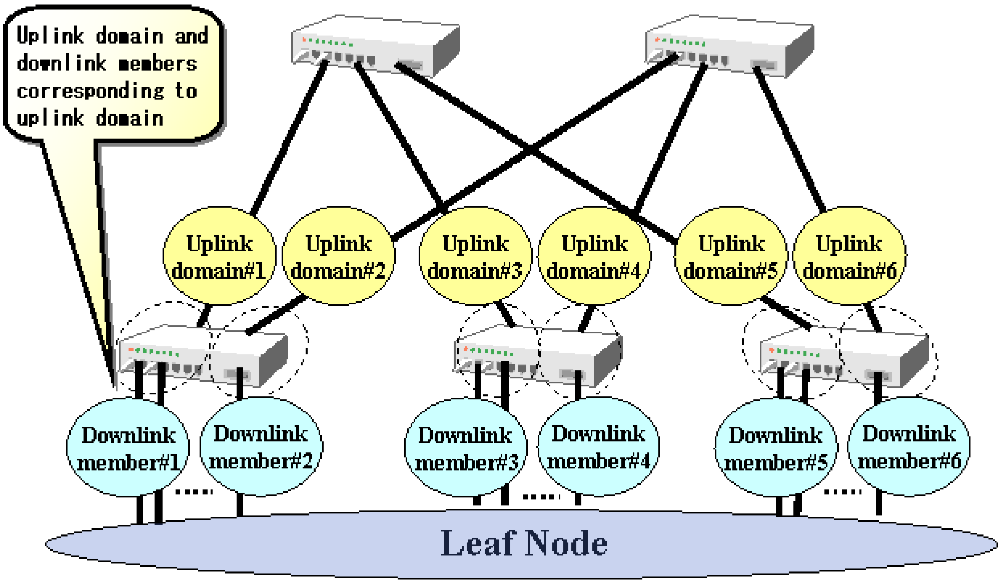

Uplink Domain #1
Uplink Domain #2
XG2000
The uplink domain port filters (drops) multicast, broadcast and unlearned unicast frames except from downlink member.
Downlink membership corresponding to uplink domain #1
Downlink membership corresponding to uplink domain #2

Uplink Filter

The uplink filter is useful in configuring large networks with multiple paths, such as a fat tree network, by cascading multiple XG-series switches.

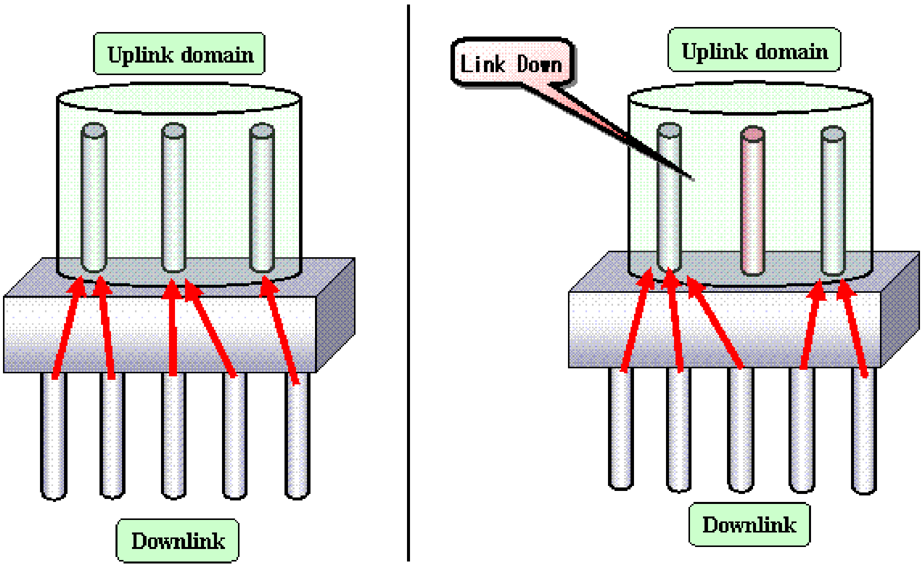
To configure an uplink filter, specify an uplink domain whose membership consists of one or more downlink ports and one or more uplink ports. For example, in a fat tree network, an uplink domain is configured such that ports connected to switches are designated as uplink ports, and leaf nodes as downlink ports. The uplink domain will then block multicast, broadcast and flooding unicast frames to other uplink domains configured within the switch and only distribute traffic from the downlink to the uplink ports within that domain.

If an uplink filter is specified to have multiple uplink ports, link aggregation and redundancy are provisioned within that domain. The uplink filter differs from link aggregation in that the uplink ports within the uplink domain can be connected to different switches or equipment to ensure redundancy within the various uplink ports.



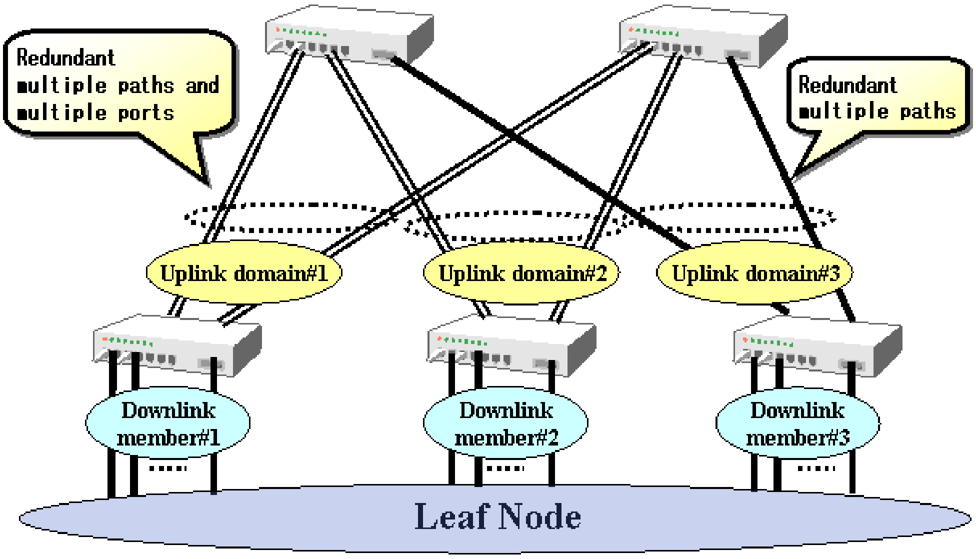
Fat tree network using uplink filter

When specifying multiple uplink ports within an uplink domain, frame distribution among the uplink ports is performed equally from port to port and not by type of frame. Frame distribution changes automatically when a fail-over or fail-back occurs, thereby providing uplink redundancy.



Frame distribution in uplink domain

The following is an example of a fat tree configuration with network redundancy.



Fat tree network with redundancy

To configure an uplink filter, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# uplink-domain 1 port 11 12`	Create an uplink domain that consists of port 11 and 12.

`xg(config)# interface port 1 2 3`
`(interface port range 1 3)`
	Switch to interface edit mode to assign downlink ports. In this example, the global interface configuration mode is selected for ports 1 through 3.

`xg(config-if)# downlink allowed uplink-domain 1`	Register each port as a downlink member of the uplink domain.
`xg(config-if)# exit`	Exit to global configuration mode.
`xg(config)# exit`	Exit to administrator EXEC mode.
`xg# show uplink`	View the state of the uplink.

Note

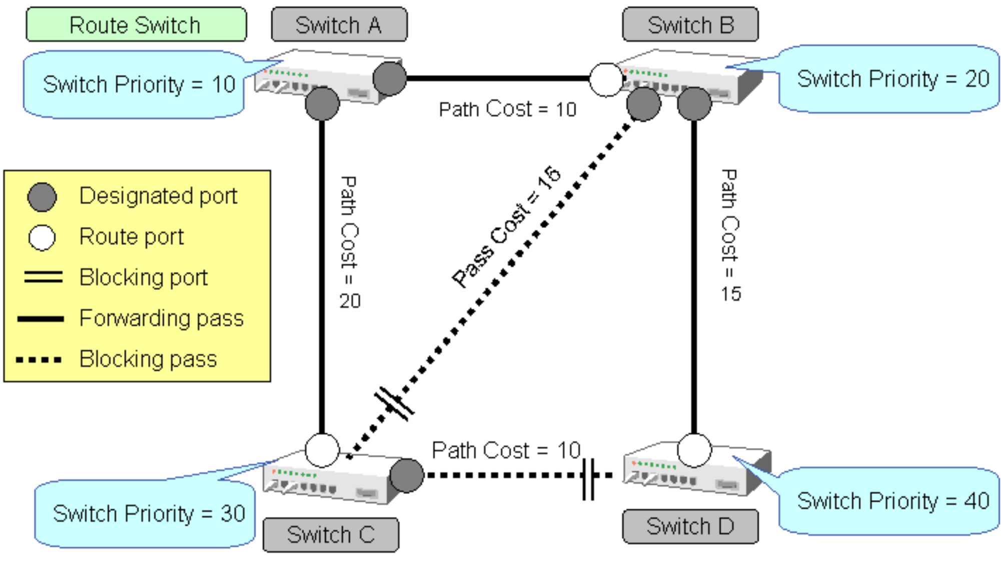
- Multicast, broadcast, and unlearned unicast frames are filtered by the uplink filter. But both statically and dynamically learned unicast frames forwarded to a specified port are not filtered.
- An uplink port is not allowed to be a member of a link aggregation group.
- STP must be disabled on uplink ports.
- The IGMP snooping and uplink filter features cannot be used at the same time.

4.6 Spanning Tree Protocol (STP)

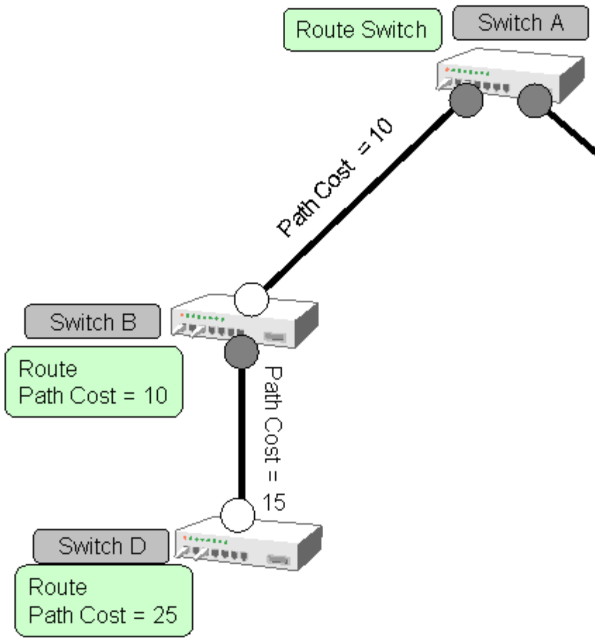
The Spanning Tree Protocol (STP) is a function that prevents loops from occurring on a network. It is also possible to provide network redundancy by intentionally creating a loop.

STP exclusively uses only one active path between network devices, and shuts out other paths, to avoid network loops. An active path is selected by comparing path costs defined on each path. After the comparison, the lowest cost path will be selected. If the selected path becomes disabled, STP will activate the lowest cost path amongst the paths remaining.

The device supports IEEE802.1w RSTP (Rapid Spanning Tree Protocol). The RSTP is upward compatible with IEEE802.1D STP (Spanning Tree Protocol) and serves as a STP if the destination device only supports STP.



Physical Topology



Logical Topology by STP

4.6.1 Port Roles Based on Spanning Tree

RSTP assigns one of these port roles to individual ports:

- Root port
  Provides the best path (lowest cost) when the switch forwards packets to the root switch.
- Designated port
  Connects to the designated switch toward the leaves of the spanning tree. The port specified connecting to the designated port serves as a root port.
- Alternate Port
  The alternative port with the second lowest path cost. In the event that the root port goes to a linkdown state, the alternate port serves as the root port. It does not always send or receive frames while in the blocking state.
- Backup Port
  Provides an alternative path to that specified. In the event that the specified port goes into a linkdown state, the backup port serves as the new designated port. It does not always send or receive frames while it is in the blocking state.
- Disabled Port
  Disabled port, it does not send or receive any frames.

4.6.2 Spanning Tree Protocol Port States

The port states defined by the STP are:

- Discard
  The port is in a "discarding state. BPDUs are only received.
- Learn
  The port is in a "learning" state. A port in the learning state learns the destination MAC address of the received frames but does not participate in frame forwarding.
- Forward
  The port is ready to transmit data traffic.

The STP states "blocking" and "listening" have been merged into a unique RSTP "discarding" state. The correspondence between STP port states and RSTP port states are shown below.

Display Format	STP(IEEE802.1D)	RSTP(IEEE802.1w)
Discard	Blocking	Discarding
Discard	Listening	Discarding
Learn	Learning	Learning
Forward	Forwarding	Forwarding

4.6.3 Configuring Spanning Tree

To configure the spanning tree protocol, carry out the following procedure in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# spanning-tree`	Enable Spanning Tree Protocol.

`xg(config)# spanning-tree priority <0-61440>`
`xg(config)# spanning-tree hello-time <1-10>`
`xg(config)# spanning-tree max-age <6-40>`
`xg(config)# spanning-tree forward-time <4-30>`
	Configure Spanning Tree Protocol parameters on the device.
	● Switch priority
	● Hello time
	● Maximum aging time (max-age)
	● Forward delay time (forward-time)

`xg(config)# interface port 1 2 3`
 	
`xg(config)# interface port range 1 3`
	Switch to interface edit mode to configure spanning tree-related parameters for a given port.
	In this example, the global interface configuration mode is selected for ports 1 through 3.

`xg(config-if)# spanning-tree port-priority <0-240>`
 	
`xg(config-if)# spanning-tree port-path-cost <1-200000000>`
	Configure the following parameters related to the spanning tree topology:
	● Port priority
	● Path cost

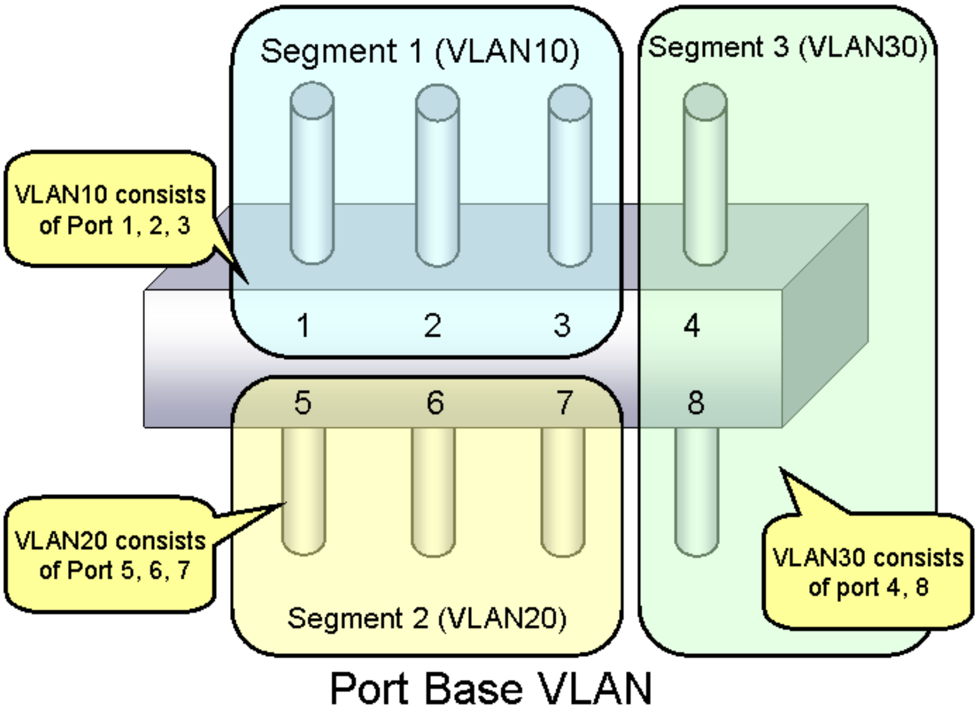
`xg(config-if)# spanning-tree portfast`	(Optional) If the port is configured as an edge port(*), this setting can reduce the time taken to transition into the forwarding state. * It is available only when the port is directly connected to an end terminal that has no influence on the spanning tree configuration.
`xg(config-if)# exit`	Exit to global configuration mode.
`xg(config)# exit`	Exit to administrator EXEC mode.
`xg# show spanning-tree [ detail ]`	View the state of the spanning tree.

4.7 VLAN

VLAN (Virtual LAN) is a technology that divides a single network into virtually separated networks.
VLANs are separate logical networks within one physical network. A VLAN capable switch can change and define new LAN network configurations without changing physical cable connections. This creates a flexible and extensible network system.
The device provides for port-based or tag-based (IEEE802.1Q) VLANs.

4.7.1 Port-Based VLAN

Port-based VLAN is a method for configuring VLAN membership on a port basis. Forwarding is based on the destination MAC addresses and related port.


Segment 1 (VLAN10)
Segment 3 (VLAN30)
VLAN10 consists of Port 1, 2, 3
1
2
3
4
5
6
7
8
VLAN20 consists of Port 5, 6, 7
VLAN30 consists of port 4, 8
Segment 2 (VLAN20)
Port Base VLAN

To configure a port-based VLAN, carry out the following procedures in the administrator EXEC mode.

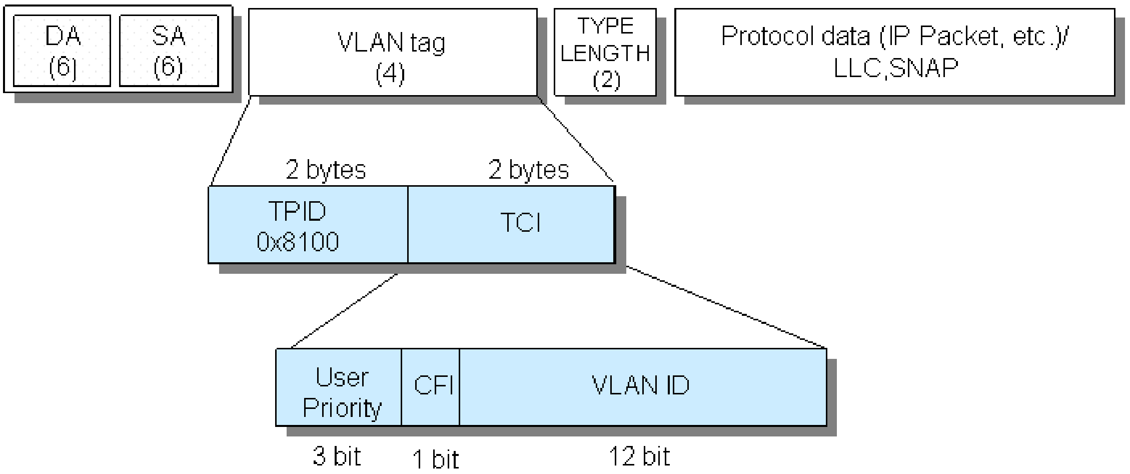
Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# vlan <1-4094> [ description VLAN_DESCRIPTION ]`	Create a VLAN to use.
`xg(config)# vlan-statistics collection <1-4094> [ <1-4094> ・・・・・]`	(Optional) Configure a VLAN that collects statistics.
`xg(config)# interface port 1 2 3 (interface port range 1 3)`	Switch to interface edit mode to assign a port to the desired port-based VLAN. In this example, the global interface configuration mode is selected for ports 1 through 3.
`xg(config-if)# port-vlan-id vlan <1-4094>`	Set the default port VLAN ID for each port.

`xg(config-if)# ingress-filter tagged-frame`
`xg(config-if)# ingress-filter untagged-frame`
	(Optional)
	Define a filter on frames received (tagged and untagged frames) if necessary.

`xg(config-if)# exit`	Exit to global configuration mode.
`xg(config)# exit`	Exit to administrator EXEC mode.
`xg# show interface`	Verify the port state. Check the information displayed in [Port Default Vlan ID] under command output [Vlan Information].
`xg# show vlan`	Verify the port VLAN membership.

4.7.2 Tag-Based (IEEE802.1Q) VLAN

Tag-based VLAN is a method of configuring VLANs so that the frame forwarding decision is based on a tag in the MAC header identifying the VLAN membership. 4 bytes of additional data in the header, called a VLAN tag, identifies the VLAN frame ownership. Using a VLAN tag enables configuring a single physical link that shares multiple VLANs.
The device’s tag-based VLAN function is based on the IEEE 802.1Q standard.
The following figure shows an Ethernet frame format including a VLAN tag as specified by the IEEE 802.1Q standard.



- TPID (Tag Protocol Identifier) (0x8100)
- TCI (Tag Control Information)
  - User Priority (3bit) : Priority of Frames (Higher priority to larger number from 0 to 7)
  - CFI (Canonical Format Indicator)(1bit): "1" when RIF field exists. Normally "0".
  - VLAN ID(12bit) : VLAN identifier (0～4095. 0 and 4095 are reserved ID)

Tag VLAN Frame Format

To configure a tag-based VLAN, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# vlan <1-4094> [ description VLAN DESCRIPTION ]`	Create a VLAN to use.
`xg(config)# vlan-statistics collection <1-4094> [ <1-4094> ・・・・・]`	(Optional) Configure a VLAN that collects statistics.

`xg(config)# interface port 1 2 3`
`(interface port range 1 3)`
	Switch to interface edit mode for the desired ports to be configured as tag-based VLAN members.
	In this example, the global interface configuration mode is selected for ports 1 though 3.

`xg(config-if)# vlan-member allowed vlan { <1-4094> | all } { egress-untagging | egress-tagging }`	Register VLAN port ownership.

`xg(config-if)# ingress-filter tagged-frame`
`xg(config-if)# ingress-filter untagged-frame`
	(Optional)
	Define a filter for frames received (tagged and untagged frames) at the ports, if necessary.

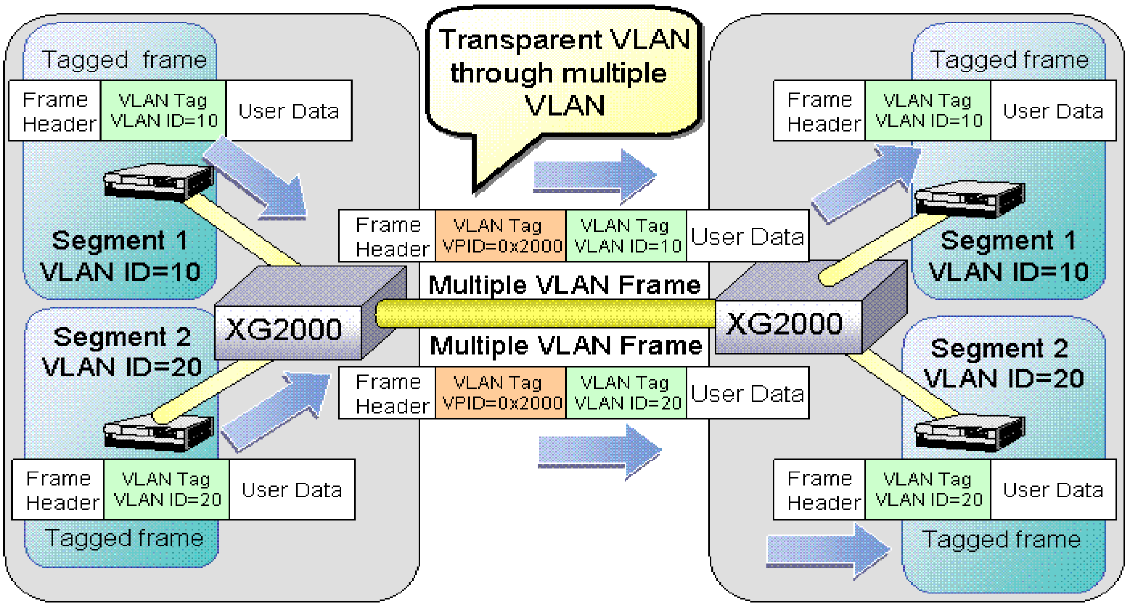
`xg(config-if)# exit`	Exit to global configuration mode.
`xg(config)# exit`	Exit to administrator EXEC mode.
`xg# show vlan`	View the port's VLAN membership state.

4.7.3 Multiple VLAN

With the user-defined VLAN tag protocol identifier, the IEEE 802.1Q standard tag can be replaced with a user-defined VPID, allowing for encapsulation of multiple tags for multiple-tagged VLANs. The standard tag identifier or TPID is 0x8100 as defined in IEEE 802.1Q.

> Information
>
> For the frame format, refer to TPID (Tag Protocol Identifier) in "Tag VLAN Frame Format".

Using multiple VLAN (also known as double tagging or Q-in-Q) allows a service provider to transparently forward customers' VLAN traffic even if the service provider assigns customer traffic to different VLANs.

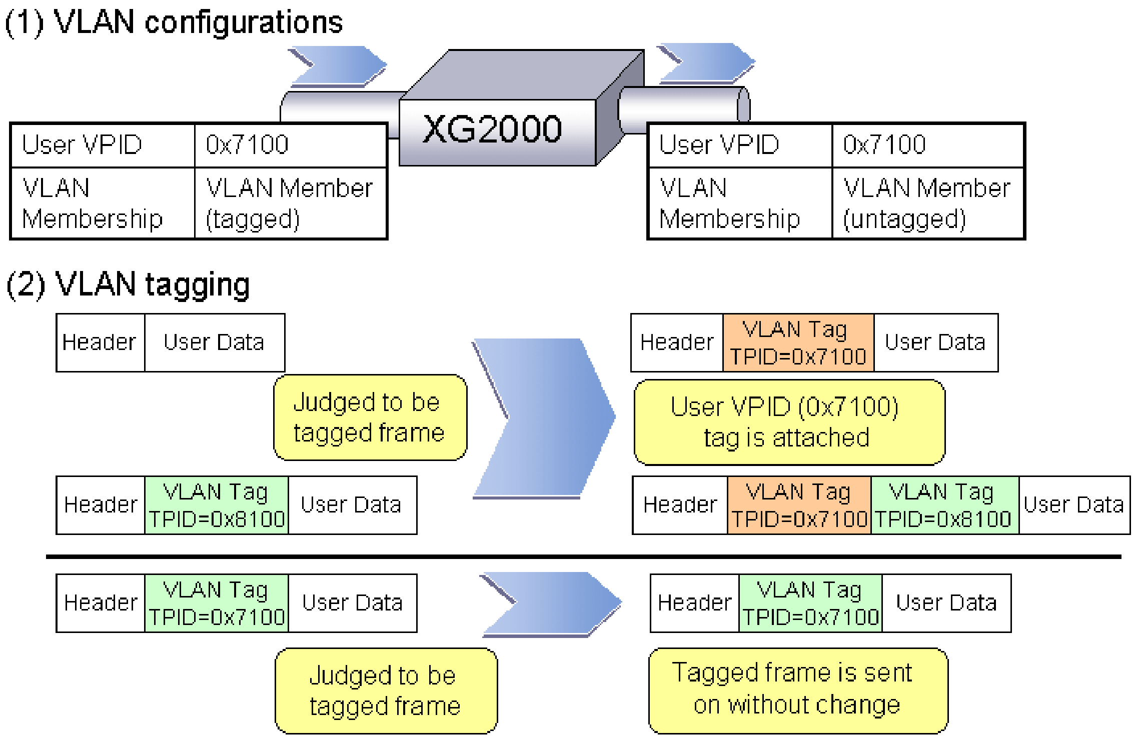

Tagged frame
Frame Header | VLAN Tag VLAN ID=10 | User Data
Segment 1
VLAN ID=10
Segment 2
VLAN ID=20
Frame Header | VLAN Tag VLAN ID=20 | User Data
Tagged frame
Transparent VLAN through multiple VLAN
Frame Header | VLAN Tag VPID=0x2000 | VLAN Tag VLAN ID=10 | User Data
Multiple VLAN Frame
XG2000
XG2000
Multiple VLAN Frame
Frame Header | VLAN Tag VPID=0x2000 | VLAN Tag VLAN ID=20 | User Data
Tagged frame
Frame Header | VLAN Tag VLAN ID=10 | User Data
Segment 1
VLAN ID=10
Segment 2
VLAN ID=20
Frame Header | VLAN Tag VLAN ID=20 | User Data
Tagged frame

Multiple VLAN

To configure multiple VLAN using a user-defined VLAN tag protocol identifier, carry out the following procedures in the administrator EXEC mode.

Command	Task
xg# configure terminal	Switch to global configuration mode.
xg(config)# vlan <1-4094> [description VLAN DESCRIPTION]	Create a VLAN to use.
xg(config)# vlan-statistics collection <1-4094> [<1-4094> ・・・・・・]	(Optional) Configure a VLAN that collects statistics.
xg(config)# interface port 1	Switch to interface edit mode to designate a port for multiple VLAN configuration. In this example, the global interface configuration mode is selected for port 1.
xg(config-if)# user-vlan-protocol-id <0x05DD ～ 0xFFFF>	Set the user-defined VLAN tag protocol identifier.
xg(config-if)# vlan-member allowed vlan { <1-4094> | all } { egress-untagging | egress-tagging }	Register the port to the VLAN. Specify "egress-tagging" for tagged output at the port. Specify "egress-untagging" for the port untagged output at the port.
xg(config-if)# ingress-filter tagged-frame xg(config-if)# ingress-filter untagged-frame	(Optional) Define a filter for frames received (tagged and untagged) for the port, if necessary.
xg(config-if)# exit	Exit to global configuration mode.
xg(config)# exit	Exit to administrator EXEC mode.
xg# show interface xg# show vlan	Verify the port state and VLAN membership state for each port.

An example of multiple VLAN and the movement of frames for a VLAN member outgoing port (VLAN-tagged frame), is shown below.

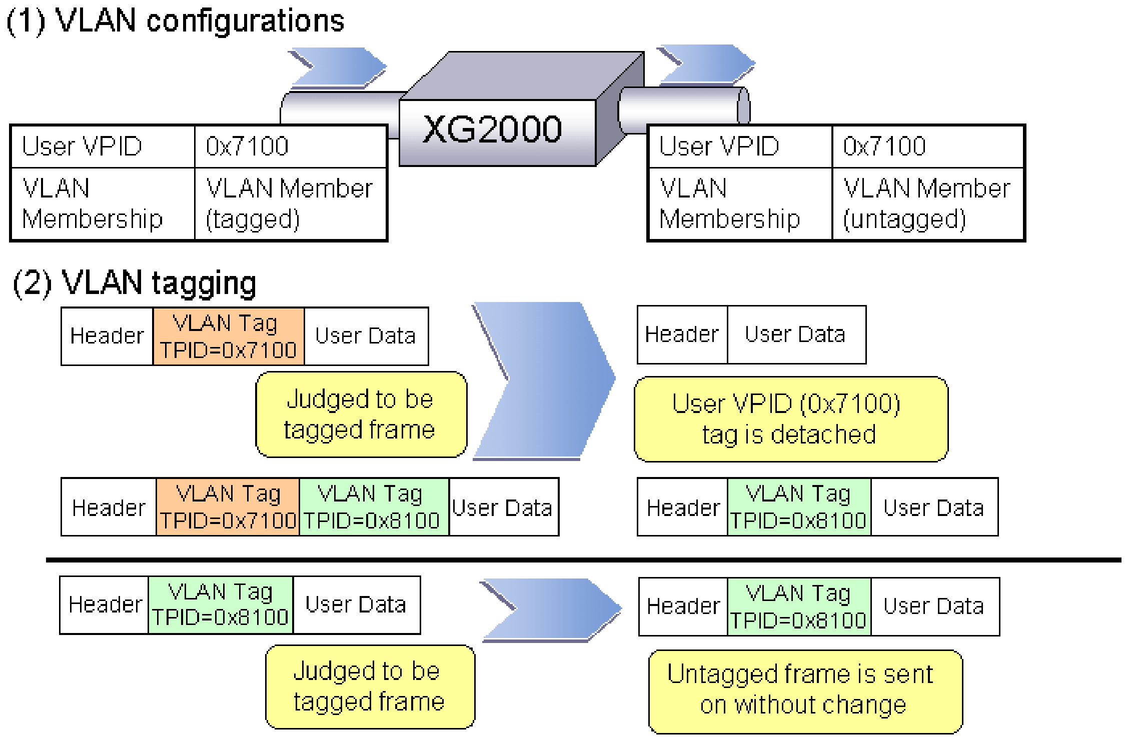


User VPID	0x7100
VLAN Membership	VLAN Member (tagged)

User VPID	0x7100
VLAN Membership	VLAN Member (untagged)

An example of multiple VLAN settings and egress rule (1)

An example of multiple VLAN and the movement of frames for a VLAN member outgoing port (VLAN-untagged frame), is shown below.

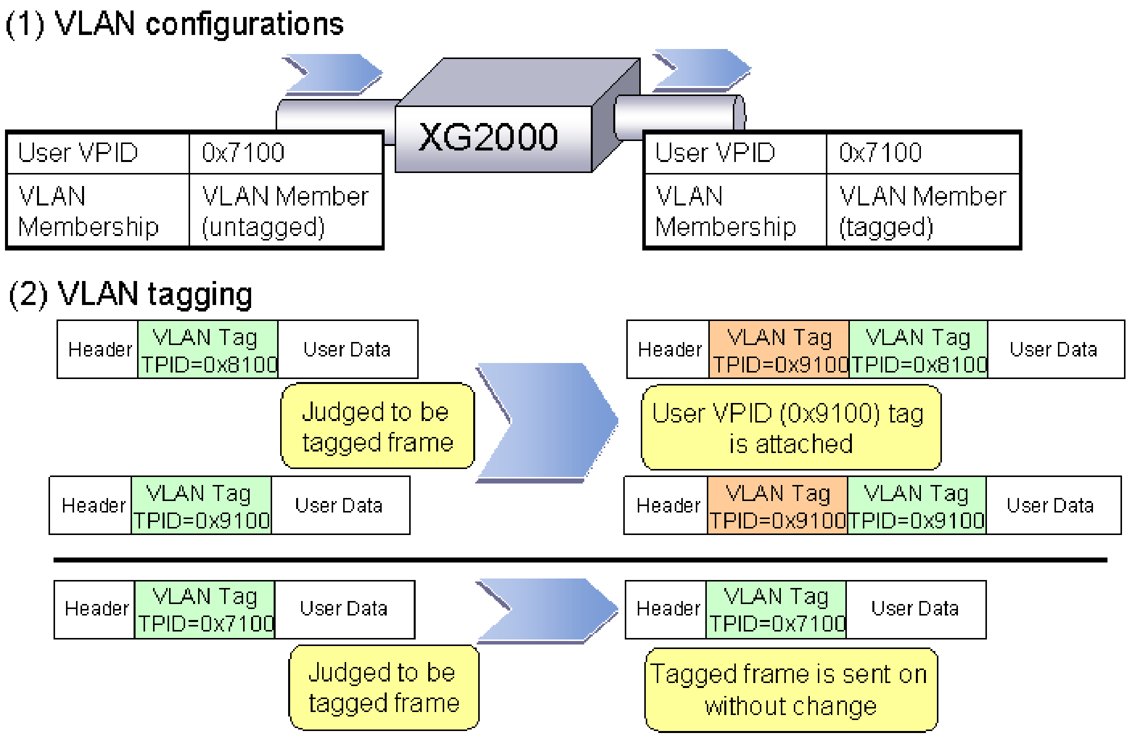


User VPID	0x7100
VLAN Membership	VLAN Member (tagged)

User VPID	0x7100
VLAN Membership	VLAN Member (untagged)

An example of multiple VLAN settings and egress rule (2)

An example of multiple VLAN and the movement of frames when the user-defined VPID of the incoming and outgoing port differ and the outgoing port is a VLAN member (VLAN-tagged frame), is shown below.


(1) VLAN configurations

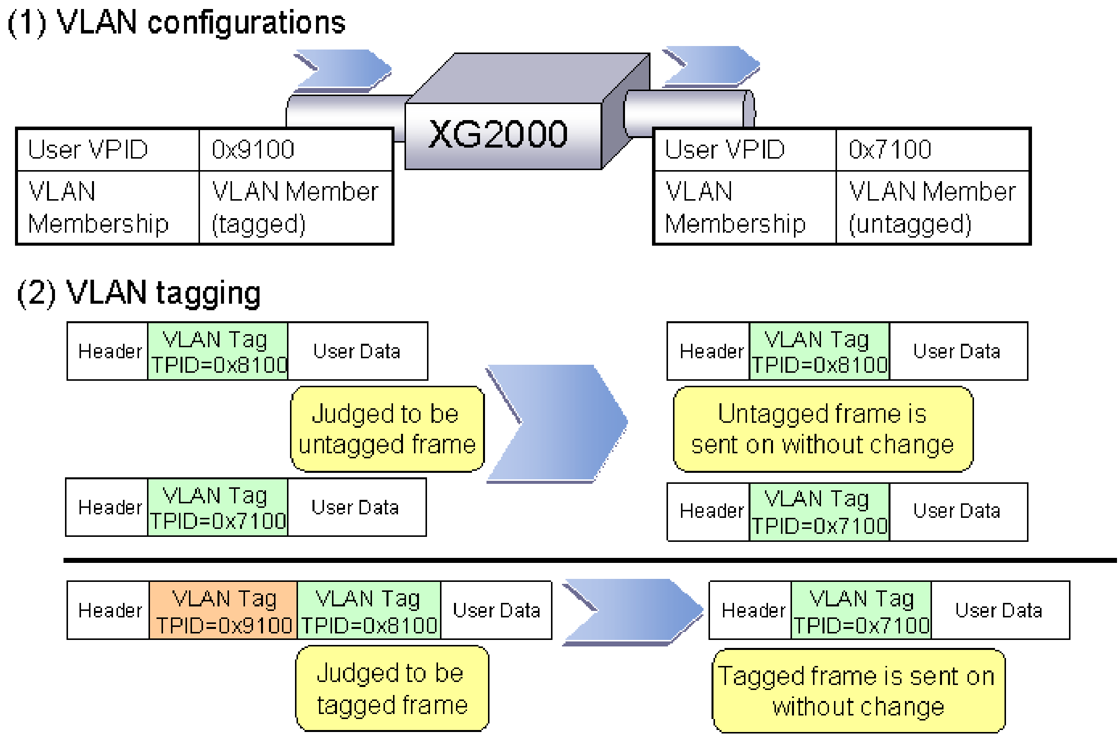
User VPID	0x7100
VLAN Membership	VLAN Member (untagged)

User VPID	0x7100
VLAN Membership	VLAN Member (tagged)

(2) VLAN tagging

An example of multiple VLAN settings and egress rule (3)

An example of multiple VLAN and the movement of frames when the user-defined VPID of the incoming and outgoing port differ and the outgoing port is not a VLAN member (VLAN-untagged frame), is shown below.


(1) VLAN configurations

User VPID	0x9100
VLAN Membership	VLAN Member (tagged)

User VPID	0x7100
VLAN Membership	VLAN Member (untagged)

(2) VLAN tagging

An example of multiple VLAN settings and egress rule (4)

4.8 Quality of Service (QoS)

The device provides Quality of Service (QoS) that is based on the IEEE802.1p standard.
The device QoS determines the priority of frames at the ingress side using DiffServ, VLAN tag (including priority tag) or a port's default priority. Their priorities are mapped to 4 output queues. The queues are processed in the order of the QoS priority precedence.
The device priorities available are:

- DiffServ
  Select QoS using the IPv4 header or DiffServ Code Point included in the IPv6 header.
- Default priority
  Set a default priority of 0 to 7 for each port.
  For frames whose priority was not set (VLAN-untagged frames), the default priority is assigned according to the value of the frame.
- Mapping to output queues
  The device is equipped with four output queues with different levels (0 to 3). Frames are transmitted in order of output queue priority.
  Each priority is mapped to a specified output queue.

To set the default priority and output queue mapping, carry out the following procedure in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# interface port 1 2 3`
`xg(config)# interface port range 1 3`
	Switch to interface edit mode and specify the port(s) to set with a default QoS priority.
	In this example, the global interface configuration mode is selected for ports 1 though 3.

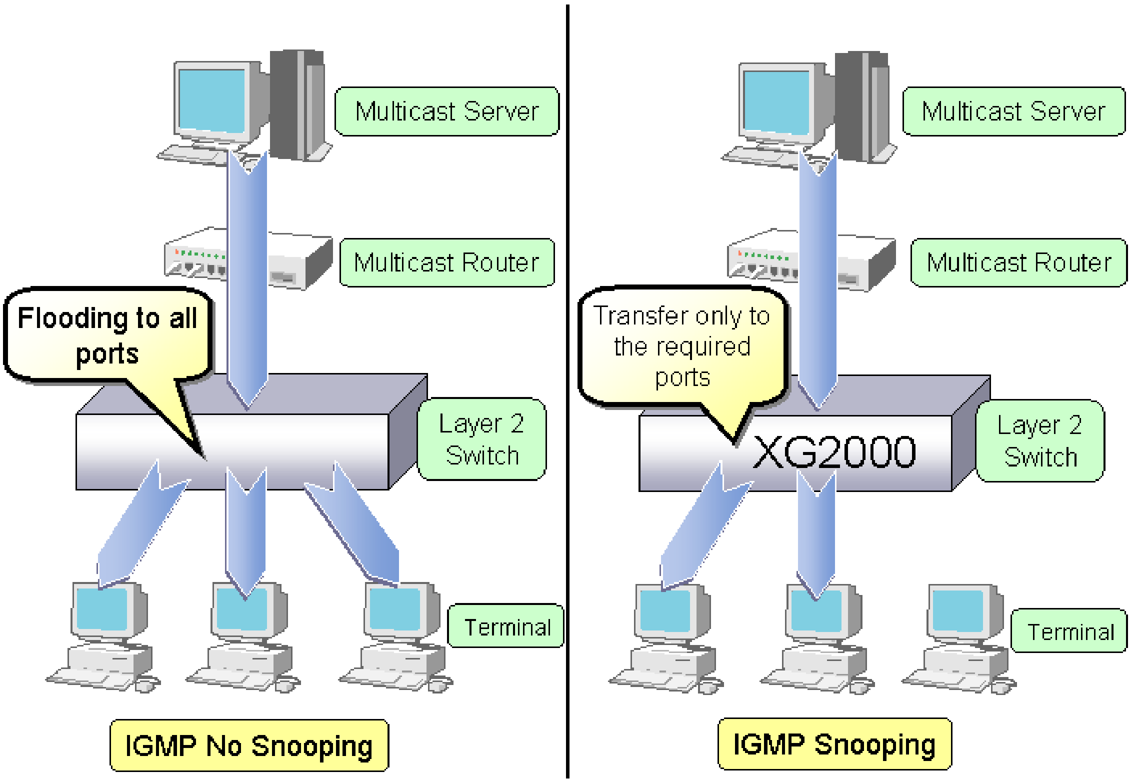
`xg(config-if)# qos default-priority <0-7>`	Set a default priority for frames whose priority was not set (VLAN-untagged frame) when received.
`xg(config-if)# exit`	Exit to global configuration mode.
`xg(config)# bridge diffserv-tos {ipv4 | ipv6}`	(Optional) Used to enable QoS based on DiffServ Code Point.
`xg(config)# qos-map priority <0-7> output-priority <0-3>`	Set the level of output queue to map to each frame that has a priority value.
`xg(config)# exit`	Exit to administrator EXEC mode.
`xg# show qos [ qos-map ]`	Show the QoS setting status.

4.9 IGMP Snooping

IP multicast is often used to distribute multimedia data, including video and voice, over a network.
A layer 2 switch floods multicast frames, absorbing unnecessary network bandwidth. A layer 3 switch that supports Internet Group Management Protocol (IGMP) manages multicast groups using IGMP packets. The device controls how IP multicast packets are forwarded to required ports by monitoring IGMP packets generated by layer 3 switches, thereby preventing unnecessary flooding. This function is called "IGMP Snooping".
The device supports IGMP snooping for IGMP v1/v2/v3.

Note

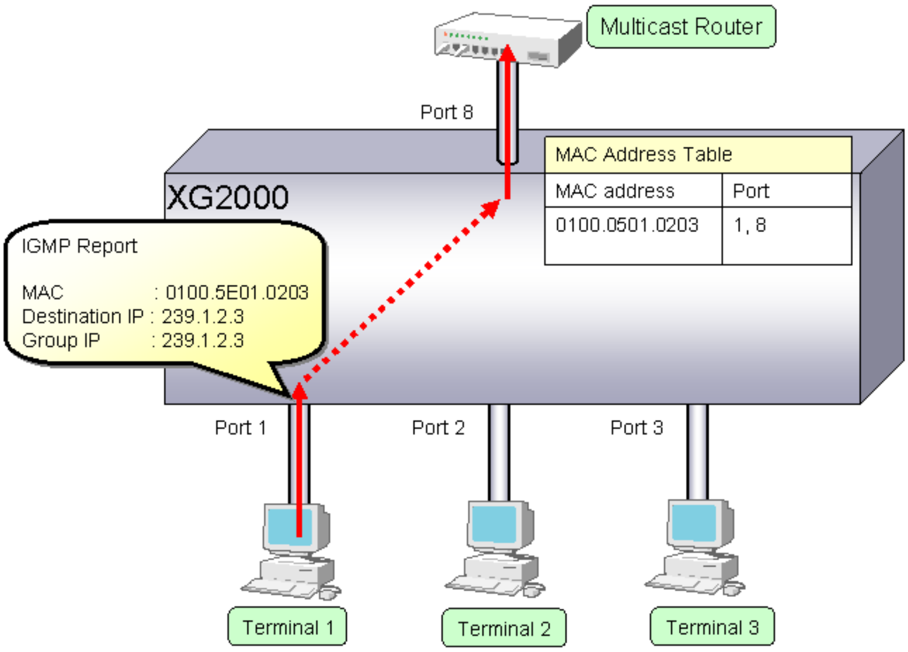
- IGMP v3 does not support source IP addressing and filtering.
- IGMP snooping and the uplink filter function cannot be used at the same time.
- The XG2000 series floods IGMP Report messages. When IGMP v1/v2 is used, it is necessary to connect a device, such as a L3 switch, that supports IGMP snooping between the XG2000 series and the IGMP hosts in order to avoid flooding.
- It is necessary to set forward-unregistered-mac or filter-unregistered-mac when IGMP snooping is used.



IGMP Snooping

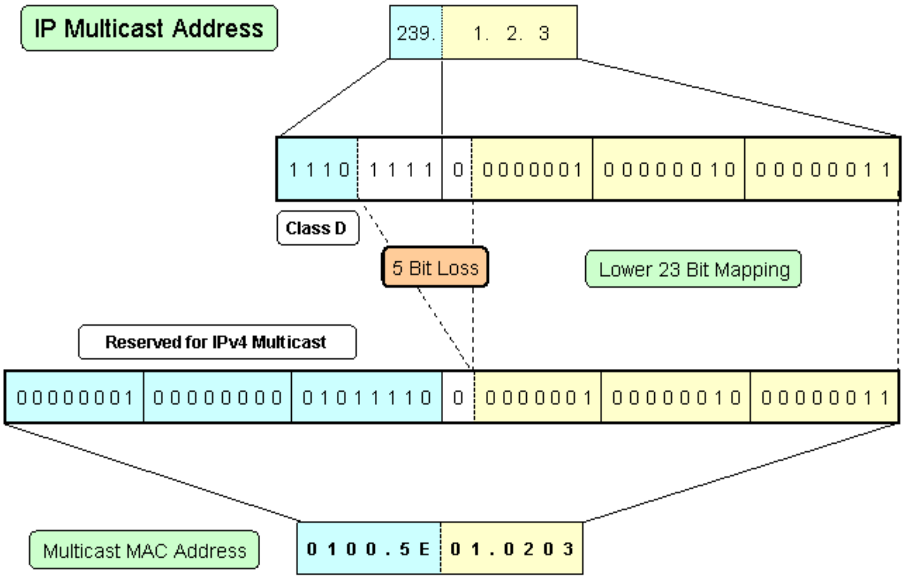
4.9.1 Registering Group Members

On receiving an IGMP Report message, the device registers a multicast MAC address with the MAC address table for the port that received the IGMP Report message and the connecting multicast router port.



Registering Group Members

The following figure shows the relationship between the registered IP multicast address and the multicast MAC address. MAC addresses that are registered with IGMP snooping are between 0100.5E00.0000 and 0100.5E7F.FFFF. An IP multicast address is 32 bits. The first 4 bits are always 1110 followed by 28 bits that represent the IP multicast address information. Of these 28 bits, the lower order 23 bits are mapped to a MAC address and the data in the higher order 5 bits is not used. Therefore 32 IP multicast addresses are mapped to the same single MAC address.

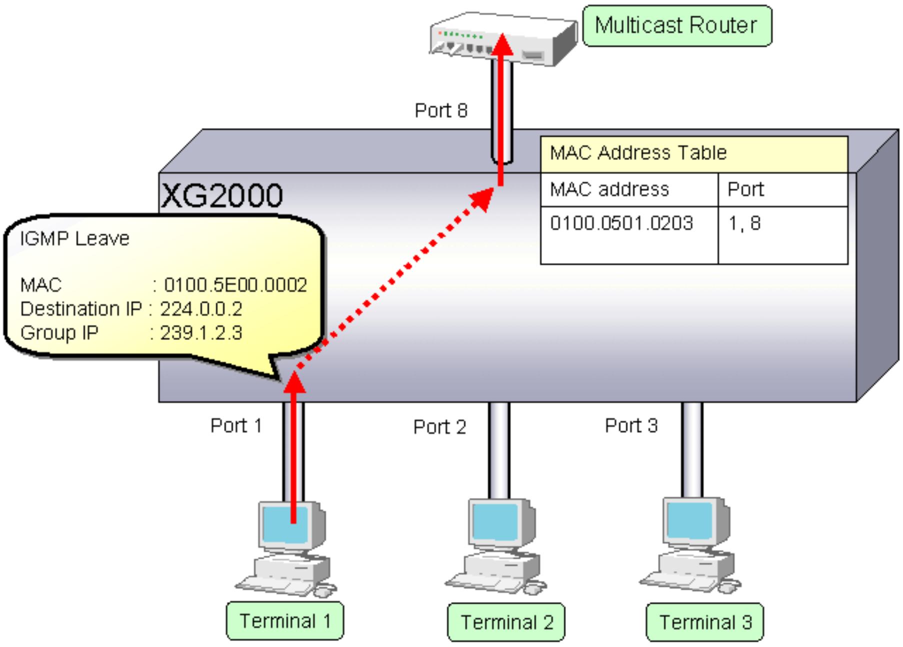


Multicast Address

4.9.2 Removing Group Members

The group members registered by IGMP snooping are removed under the following status.

- If after receiving an IGMP Report message for group registration, the group member interval expires before the device receives another IGMP Report message, the switch removes that group member. The default setting for the group member interval is 260 seconds.
- If an IGMP Leave message is sent from a host, the multicast router sends out an IGMP Specific Query (GSQ) message to determine that the host has left the group.
  If after receiving the IGMP Leave message, the last member query interval expires before the device receives another IGMP Report message, the switch removes that group member. The default setting for the last member query interval is 2 seconds.



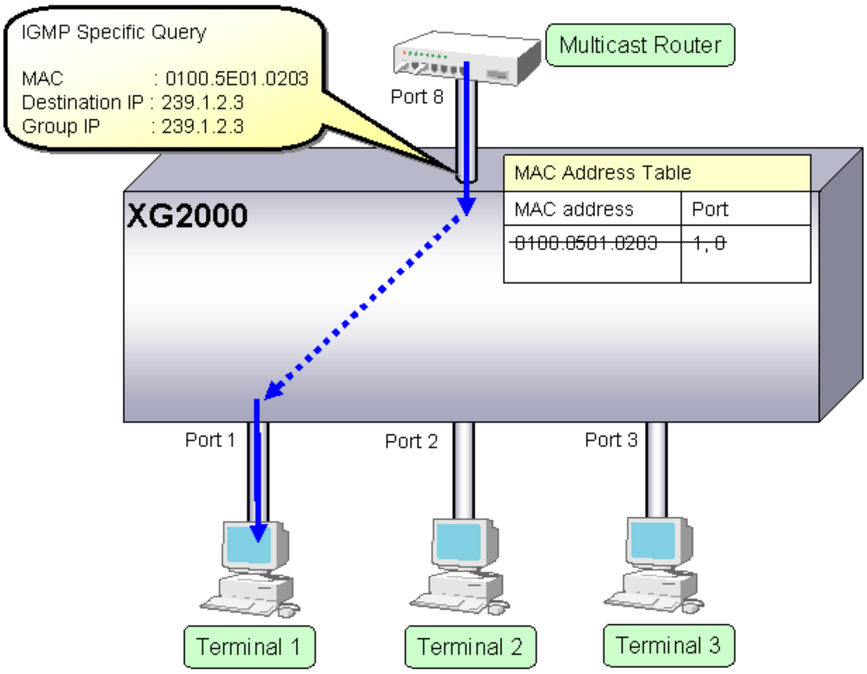
IGMP Leave

MAC : 0100.5E00.0002
Destination IP : 224.0.0.2
Group IP : 239.1.2.3

MAC Address Table

MAC address	Port
0100.0501.0203	1, 8

Removing Group Members (1)



IGMP Specific Query

MAC : 0100.5E01.0203
Destination IP : 239.1.2.3
Group IP : 239.1.2.3

MAC Address Table

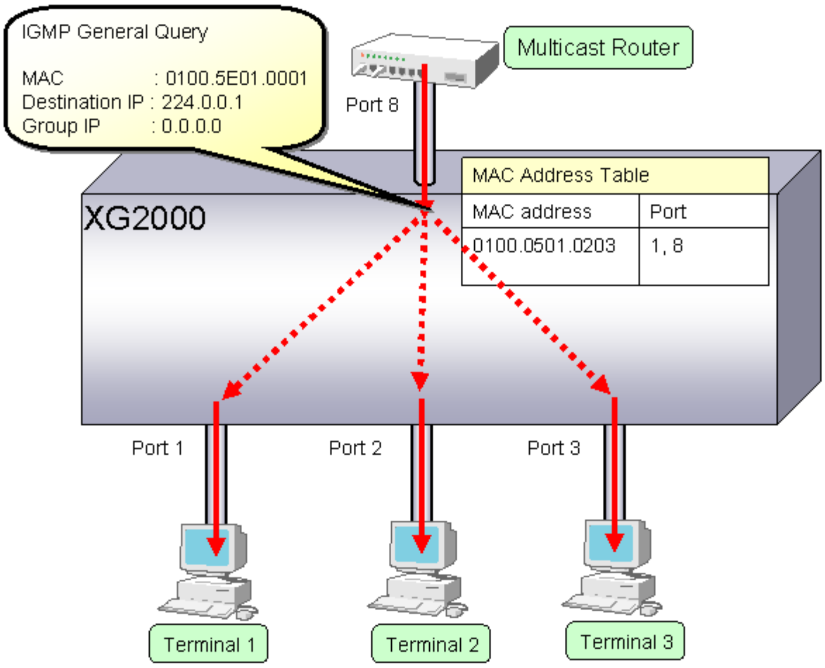
MAC address	Port
~~0100.0501.0203~~	~~1, 8~~

Removing Group Members (2)

4.9.3 Managing Group Members

When network congestion causes Leave message loss or there is a host that uses IGMPv1, the multicast router does not receive Leave messages. The multicast router sends out an IGMP General Query message to all hosts (IP address: 224.0.0.1) at intervals (query interval) to determine membership information.

Upon reception of an IGMP General Query message, the host, a member of the group, returns an IGMP Report message to maintain membership in the group.



IGMP General Query

MAC : 0100.5E01.0001
Destination IP : 224.0.0.1
Group IP : 0.0.0.0

MAC Address Table

MAC address	Port
0100.0501.0203	1, 8

Managing Group Members

In consideration of General Query or Report message loss caused by network congestion, it is recommended that the following equation be used to determine the group member interval for the device.

- Group member interval = (query interval for multicast router) × 2 + 10 (seconds)

Since RFC 3376 defines the default query interval for multicast routers as 125 seconds, the device uses 260 seconds for the default group member interval.

4.9.4 IGMP Querier

In a typical network configuration, the multicast router periodically sends out an IGMP General Query message to determine if any of the hosts on the network are members of any multicast groups. Receiving a response from a host ascertains its membership in a multicast group.

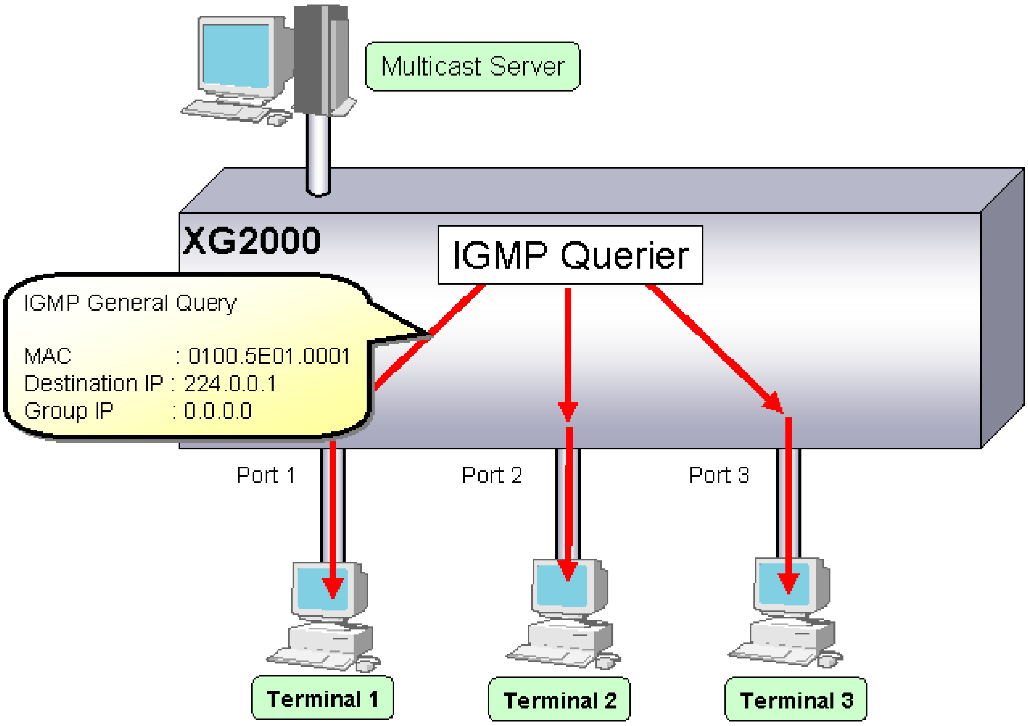
IGMP Querier is a function that acts as a proxy for a multicast router when one is not available in a network segment to send an IGMP General Query message to all hosts.

The frequency of Query messages issued is configured using the "ip snooping vlan send-query-count" command.

The frequency of the General Query messages sent (query interval) are automatically calculated by the following equation based on the send query count and the group membership interval.

- Query interval = (Group membership interval - 10)/send query count (seconds)

The default setting for the Query interval is 125 seconds.



IGMP Querier

Upon reception of an IGMP Leave message, the device sends an IGMP Specific Query (GSQ) message to determine that the host is interested in leaving the group.

If an IGMP Specific Query message is sent as many times as specified by the send query count and the host does not respond with an IGMP Report message, that host is removed.

Note

- Generally, IGMP Querier uses "0.0.0.0" for the source IP address when sending a Query message. Since some client software does not return a response for a Query message with the source IP address being set to "0.0.0.0", it is recommended that an address other than "0.0.0.0" be used.
- If a multicast router exists on the network segment, the device does not send Query message even if IGMP Querier is valid.

4.9.5 Configuring IGMP Snooping

To configure IGMP snooping, carry out the following procedure in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# ip snooping protocol igmp`	Enable global IGMP snooping on the device.
`xg(config)# ip snooping vlan <1-4094>`	Enable IGMP snooping for each VLAN separately.

`xg(config)# ip snooping vlan <1-4094>`
`group-member-interval <60-600>`
	(Optional)
	Change the group member interval.

`xg(config)# ip snooping vlan <1-4094>`
`mrouter { port <1-20> | agg-port <1-10> }`
	(Optional)
	Register the port the multicast router resides statically.

`xg(config)# ip snooping vlan <1-4094>`
`mrouter suppress-learning`
	(Optional)
	Suppress dynamic registration on the port the multicast router resides.

`xg(config)# ip snooping vlan <1-4094>`
`last-member-query-interval <1-9>`
	(Optional)
	Change the last member query interval.

`xg(config)# ip snooping vlan <1-4094>`
`send-query-count <1-3>`
	(Optional)
	Change the frequency of Query messages sent.

`xg(config)# ip snooping vlan`
`max-group <10-128>`
	(Optional)
	Change the number of multicast addresses that can be registered with IGMP snooping for each VLAN.

`xg(config)# ip snooping vlan <1-4094>`
`fast-leave`
	(Optional)
	Set the fast-leave mode used when receiving an IGMP Leave message.

`xg(config)# interface port range 1 20`	Switch to interface edit mode to designate ports to specify the forwarding method for multicast frames. `All ports are selected in this example.`

`xg(config-if)# multicast-forwarding`
`forward-unregsitered-mac`
	`Set forwarding method for multicast frames to forward-unregistered-mac.`

`xg(config)# exit`	Exit to administrator EXEC mode.

To enable IGMP query, carry out the following procedure in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# ip snooping protocol igmp`	Enable global IGMP snooping on the device.
`xg(config)# ip snooping vlan <1-4094>`	Enable IGMP snooping for each VLAN separately.

`xg(config)# ip snooping vlan <1-4094>`
`group-member-interval <60-600>`
	(Optional)
	Change the group member interval.

`xg(config)# ip snooping vlan <1-4094>`
`last-member-query-interval <1-9>`
	(Optional)
	Change the last member query interval.

`xg(config)# ip snooping vlan <1-4094>`
`send-query-count <1-3>`
	(Optional)
	Change the frequency of Query messages sent.

`xg(config)# ip snooping vlan <1-4094>`
`querier ip A.B.C.D`
	Enable IGMP query and set the source IP address for a Query message.

`xg(config)# exit`	Exit to administrator EXEC mode.

4.10 Network Management

4.10.1 Traffic Statistics

The device can display traffic statistics to analyze network operations such as traffic bytes, errors, etc.
The following are the Traffic Statistics the device provides.

- Displays traffic information on outgoing and incoming frames for each port.
- Displays traffic information on incoming frames by frame size range for each port.
- Displays traffic information on incoming frames for each VLAN.
- Displays incoming traffic information by QoS priority for each port.
- Displays information related to data flow for each port.
- Displays information about errors that occur during transmission/reception for each port.

To display traffic statistics, monitor and show commands are provided.

- "monitor" command
  Displays real-time traffic statistics.
- "show statistics" command
  Outputs details of the current accumulated traffic statistics.
  Enter this command followed by "> FILE_NAME" or "| redirect FILE_NAME" to output the results to a file in volatile memory.

To display traffic statistics, run the following commands in the operator EXEC mode or in the administrator EXEC mode.

Command	Task

`xg> monitor traffic-counts`
`{ current | total } [interval <3-60>]`
`xg> monitor traffic-bytes`
`{ current | total } [interval <3-60>]`
	View incoming and outgoing traffic statistics (number of frames and number of bytes) for each port.

`xg> show statistics traffic-counts`
`xg> show statistics traffic-bytes`	

`xg> monitor framesize-traffic-counts`
`{ current | total } [interval <3-60>]`
	View traffic statistics (number of frames) by frame size range for each port.

`xg> show statistics framesize-traffic-counts`	

`xg> monitor vlan-traffic-counts`
`{ current | total } [interval <3-60>]`
`xg> monitor vlan-traffic-bytes`
`{ current | total } [interval <3-60>]`
	View traffic statistics (number of frames and number of bytes) on incoming frames for each VLAN.

`xg> show statistics vlan-traffic-counts`
`xg> show statistics vlan-traffic-bytes`	

`xg> monitor qos-priority-traffic-counts`
`{ current | total } [interval <3-60>]`
`xg> monitor qos-priority-traffic-bytes`
`{ current | total } [interval <3-60>]`
	View incoming traffic statistics (number of frames and number of bytes) by QoS priority for each port.

`xg> show statistics`
`qos-priority-traffic-counts`
`xg> show statistics`
`qos-priority-traffic-bytes`	

`xg> monitor dataflow`
`{ current | total } [interval <3-60>]`
`xg> show statistics dataflow`
	View traffic statistics (number of frames) related to data flow during frame forwarding for each port.

`xg> monitor error`
`{ current | total } [interval <3-60>]`
`xg> show statistics error`
	View information about errors that occur during transmission/reception for each port.

`xg> enable`
`xg# clear statistics`
	Clear cumulative traffic statistics collected after system startup.

4.10.2 SNMP Agent

SNMP (Simple Network Management Protocol) is a protocol that monitors and manages devices on a network.
The device supports the SNMP (v1/v2c) function to collect management information blocks (MIBs) from a remote network manager (SNMP manager). For operations via SNMP manager, only read-only operations are allowed. For the MIBs supported, refer to Appendix C. The device can be configured for up to 4 SNMP managers and up to 4 SNMP trap destinations.
To configure the SNMP agent, carry out the following procedures in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.

`xg(config)# hostname HOST-NAME`
`xg(config)# snmp-server location SYSTEM-LOCATION`
`xg(config)# snmp-server contact SYSTEM-CONTACT`
	Set the system name (HOST-NAME), system's location (SYSTEM-LOCATION), and contact (SYSTEM-CONTACT).

`xg(config)# snmp-server access host HOST community COMMUNITY-NAME`	Set the IP address (host name) of the SNMP manager and the community name.
`xg(config)# snmp-server trap host HOST community COMMUNITY-NAME [protocol {v1|v2c}]`	Set the SNMP trap receiver IP address (host name) and the community name.
`xg(config)# exit`	Exit to administrator EXEC mode.

4.10.3 RMON

Remote Monitoring (RMON) is a function provided to monitor communications over a network, such as traffic and errors. RMON, used in conjunction with the SNMP agent, allows the remote monitoring of traffic on a LAN segment.
The device supports 4 RMON groups (Statistics, History, Alarm and Event).

- Statistics group
  Collects traffic statistics for each port.
- History group
  Records traffic statistics for each port at specified time intervals.
- Alarm group
  Monitors MIBs at specified time intervals and, if the monitored MIB object value exceeds or falls below a specified threshold, a RMON event is executed.
- Event group
  Specifies an event operation that is executed by an alarm. Possible event operations include creation of a log entry and generation of a SNMP trap.

To configure RMON, carry out the following procedure in the administrator EXEC mode.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# rmon collection history <1-65535> port <1-20> [buckets <1-20>] [interval <1-3600>] [owner OWNERNAME]`	(Optional) Enable a RMON history group.
`xg(config)# rmon alarm <1-65535> VARIABLE interval <2-65535> {absolute | delta} rising-threshold <0-2147483647> [<1-65535>] falling-threshold <0-2147483647> [<1-65535>] [owner OWNERNAME]`	(Optional) Enable a RMON alarm group.
`xg(config)# rmon event <1-65535> [log] [trap COMMUNITY] [description DESCRIPTION-STRING] [owner OWNERNAME]`	(Optional) Enable a RMON event group.
`xg(config)# exit`	Exit to administrator EXEC mode.

4.11 RADIUS/TACACS+ authentication

RADIUS (Remote Authentication Dial In User Service) or TACACS (Terminal Access Controller Access Control System) is used to manage authentication, authorization, accounting remotely. XG2000 supports RADIUS/TACACS+ authentication using PAP (User Password) for login authentication. An administrator can unify the authentications of various devices, which support RADIUS/TACACS+ clients functions through a RADIUS/TACACS+ server.

4.11.1 RADIUS Attributes

It displays RADIUS attributes.

Attribute	Value of attribute	Content
User-Name	1	The username to authenticate
User-Password	2	Password to authenticate
NAS-IP-ADDRESS	4	IP address of the device (management LAN)
Service Type	6	AuthenticateOnly(8)
NAS-Identifier	32	Hostname of the device

4.11.2 TACACS+ Attributes

It displays TACACS+ attributes.

Category	Content
action	TAC_PLUS_AUTHEN_LOGIN (0x01)
priv_lvl	TAC_PLUS_PRIV_LVL_MIN (0x00)
authen_type	TAC_PLUS_AUTHEN_TYPE_PAP (0x02)
service	TAC_PLUS_AUTHEN_SVC_LOGIN (0x01)
user_len	Size of user field
rem_addr_len	0
data_len	Size of data field
user	Username to authenticate
data	Password of the user to authenticate

4.11.3 Configuring RADIUS/TACACS+

To configure RADIUS/TACACS+ authentication, carry out the following procedure.

Command	Task
`xg# configure terminal`	Switch to global configuration mode.
`xg(config)# radius-server key KEY`	(Optional) Specifies a global secret key which is used as a default parameter when RADIUS server is registered with no key parameter.
`xg(config)# tacacs-server key KEY`	(Optional) Specifies a global secret key which is used as a default parameter when TACACS+ server is registered with no key parameter.
`xg(config)# radius-server timeout <1 - 15>`	(Optional) Specifies the timeout(sec) for authentication requests.
`xg(config)# radius-server host HOST [auth-port PORT] [key KEY]`	Register a RADIUS server.
`xg(config)# tacacs-server host HOST [key KEY]`	Register a TACACS+ server.
`xg(config)# aaa authentication login {console | ssh} {local | radius | tacacs} {local | none}`	Set login authentication method.
`xg(config)# exit`	Exit to administrator EXEC mode.
`xg# account user001 class admin`	(Optional) Register the same account for using RADIUS/TACACS+ authentication on XG2000 XG2000 cannot use an unregistered account.
`xg# show radius`	Displays the information of RADIUS server
`xg# show tacacs`	Displays the information of TACACS+ server
`xg# show authentication`	Displays the setting status of login authentication method
`xg# show account`	Lists the all accounts registered in the device.

Note

- It is needed to register RADIUS/TACACS+ user accounts to XG2000 before enabling RADIUS/TACACS+ authentication. XG2000 does not allow any account except for "admin" for the default configuration.
- RADIUS/TACACS+ authentication is only available if primary login is RADIUS/TACACS+ authentication and secondary login is disable by "aaa authentication login" command. Any user can not login XG2000 under RADIUS/TACACS+ authentication is only available if RADIUS/TACACS+ server does not work. It is recommended to test RADIUS/TACACS+ authentication under local authentication is available.
- XG2000 requests authentication in order of the lists displayed by "show radius", "show tacacs" command. Up to 4 access requests are transmitted for each RADIUS servers and 1 access for TACACS+ servers until receiving the reply from the RADIUS/TACACS+ server.

Chapter 5 Command Reference

5.1 About Command Reference

This section describes how to read command references.

5.1.1 Command System

The following is the system of commands provided in the device:

Item	Function
Management LAN Interface Configuration commands	These are used to configure functions related to the management LAN interface.
Serial/telnet/SSH configuration commands	These are used to configure functions related to serial, telnet and SSH connections.
System Basic Operation commands	These are necessary commands for system operation such as the system time setting, password setting, and file operations.
Configuration Information Operation commands	These are used for displaying or saving configuration information (running-config and startup-config) in the device.
Switch Basic Configuration commands	These are used to configure the basic functions of the device.
Link Aggregation Configuration commands	These are used to create/delete aggregation groups.
Switch Port Configuration commands	These are used to set the operating characteristics of each switch port.
Spanning Tree Protocol (STP) Setup commands	These are used to configure STP (Spanning Tree Protocol).
Virtual LAN (VLAN) Configuration commands	These are used to configure virtual LAN (VLAN).
Quality of Service (QoS) Setup commands	These are used to configure QoS (Quality of Service) configuration.
Port Mirroring Setup commands	These are used to configure port mirroring.
IGMP Snooping Setup commands	These are used to configure IGMP Snooping.
Statistics commands	These are used to display various operational statistics.
SNMP Configuration commands	These are used to configure SNMP.
RMON Configuration commands	These are used to configure RMON.
System Status Display commands	These are used to display the system status of the device and the operational status of its hardware.
Maintenance commands	These are necessary for maintenance of the device.

5.1.2 Configuration of Command Reference

This section describes the configuration of command reference and descriptive content.

Function

Explains the functions of the commands.

Prompt

Indicates the prompt of the operational mode.

Command syntax

Describes the command syntax. The notation of the command syntax is as follows:

Notation	Meaning	Example of description
Lower-case characters	Indicate fixed strings such as command names and keyword names.	enable
Upper-case characters	Indicate parameters specifying any strings.	delete FILE-NAME
[ ] (Enclosed in a pair of square brackets)	Indicate omissible parameters.	date [YYYYMMDD-hhmmss]
{ | } (Enclosed in a pair of curly brackets with a vertical line in-between)	Indicate parameters wherein at least one alternative must be chosen.	baudrate { 9600|19200|38400|57600 }
< > (Enclosed in a pair of angle brackets)	Indicate parameters with a condition of numerical range.	interface port <1-20>

Parameter

Explains how to specify command parameters, and their meanings.

Command type

Indicates configuration commands that retain configuration information in startup-config and running-config or operation management commands that are related to configuration of the device, such as status display or time setting.

Default

Indicates the factory default of this command.

Output form

Explains the meaning of output (or input) results, when there is a command output (or input).

Message

Explains messages displayed when executing a command, their solution, and significance.

Note

Explains notes for commands.

Example

Describes how to use commands, using examples.

5.2 Management LAN Interface Configuration Commands

This section explains configuration commands related to the Management LAN Interface.

5.2.1 show remote-host

Function

Displays the relationship between the remote hostname and IP address.

Prompt

xg> or xg#

Command syntax

```
show remote-host
```

Command type

Operation management commands.

Output form

```
xg# show remote-host
Remote Host  2008/02/05-11:37:34
================================
IP Address     Host Name
--------------- --------------------------------------------------------------
11.22.33.45    HOST005
11.22.33.46    HOST006
```

- IP Address
  Display the IP address of remote host
- Host Name
  Display the hostname which is related to the IP address

Example

Display the list of hostname and the IP address.

```
xg# show remote-host
```

5.2.2 management-lan ip

Function

Sets the IP address and default gateway, when the Management LAN Interface is used.
Use the no form to disable the Management LAN Interface.

Prompt

xg(config)#

Command syntax

```
management-lan ip A.B.C.D/M [default-gw A.B.C.D]
no management-lan ip
```

Parameter

- ip A.B.C.D/M
  Specifies the IP address and subnet mask bit length of the Management LAN Interface in the A.B.C.D/M format.
  Specifies an IP address of A.B.C.D, and a subnet mask bit length to M.
  IP addresses that can be set are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- default-gw A.B.C.D
  Specifies the IP address of the default gateway.

Command type

Configuration command

Default

192.168.0.2/24

Message

```
% Invalid IP-address.
```

Explanation

The specified format of the IP address or specified content is incorrect.

Solution

Specify the IP address in a correct format and execute the command again.

Note

- When the IP address is changed from a telnet/SSH terminal using this command, the telnet/SSH connection will be disconnected. Connect again with a new address.

Example

Make the Management LAN Interface usable by setting IP address to "12.34.56.25," subnet mask bit length to "24" (255.255.255.0), and default gateway address to "12.34.56.1".

```
xg(config)# management-lan ip 12.34.56.25/24 default-gw 12.34.56.1
```

5.2.3 management-lan dns-server

Function

Registers the IP address of a DNS (Domain Name Service) server used for host name resolution. Up to three DNS servers can be registered.
Use the no form to delete registered DNS servers.

Prompt

xg(config)#

Command syntax

```
management-lan dns-server A.B.C.D
no management-lan dns-server [A.B.C.D]
```

Parameter

- dns-server A.B.C.D
  Sets the IP address to register as a DNS server in A.B.C.D format.
  IP addresses that can be set are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- (no management-lan) dns-server [A.B.C.D]
  Deletes registered DNS server(s). Specifies IP address in A.B.C.D format.
  When IP address is omitted, all registered DNS servers will be deleted.

Command type

Configuration command

Default

None

Message

```
% Not exist IP-address of DNS server
```

Explanation

The specified IP address is not found.

Solution

Specify the IP address of a registered DNS server.

```
% Number of DNS server is over (max=3)
```

Explanation

The upper limit of the number of registrable DNS servers was surpassed.

Solution

After deleting unnecessary DNS server information, execute the command again.

```
% Invalid IP-address.
```

Explanation

The specified format of the IP address or specified content is incorrect.

Solution

Specify the IP address in a correct format and execute the command again.

Note

- Since DNS server(s) connect via the Management LAN Interface, the Management LAN Interface must be configured beforehand via the management-lan ip command.
- If DNS server is registered, the new setting becomes enabled after executing “copy running-config startup-config” command and restart the device.

Example

Register DNS servers with IP addresses "12.34.56.76" and "12.34.56.77".

```
xg(config)# management-lan dns-server 12.34.56.76
xg(config)# management-lan dns-server 12.34.56.77
```

Delete all registered DNS servers.

```
xg(config)# no management-lan dns-server
```

5.2.4 management-lan domain

Function

Sets the default domain name when referring to a DNS (Domain Name Service) server.
For example, when the host name is "hostname1," and "abc.jp" is specified as the default domain name, perform a search for the address with an FQDN (Fully Qualified Domain Name) of "hostname1.abc.jp."
Use the no form to delete the set domain name.

Prompt

xg(config)#

Command syntax

```
management-lan domain DOMAIN-NAME
no management-lan domain
```

Parameter

- domain DOMAIN-NAME

  Specifies the default domain name.

  > Point
  >
  > Follow these rules for specifying a domain name:
  >
  > – Characters usable for the name
  >   Alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), hyphen (-), and period (.)
  > – First character
  >   Alphabet ([a - z], [A - Z])
  > – Last character
  >   Alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), and period (.)

Command type

Configuration command

Default

None

Note

- If the default domain name is changed, the new setting becomes enabled after executing “copy running-config startup-config” command and restart the device.

Example

Specify "corp.co.jp" for the default domain name of a DNS server.
Then, return to the operator exec mode, specify "hostname1" for a TFTP server name, and execute the "tftp" command. The default domain name is added to "hostname1," and the IP address can be referenced from the DNS server with the FQDN name of "hostname1.corp.co.jp."

```
xg(config)# management-lan domain corp.co.jp
xg(config)# exit
xg# tftp get hostname1 remotefile localfile
```

5.2.5 hostname

Function

Changes the hostname of the device.
Use the no form to return to the default ("xg").

Prompt

xg(config)#

Command syntax

```
hostname HOST-NAME
no hostname
```

Parameter

- HOST-NAME
  Specifies the hostname of the device. Specify the hostname using 63 characters or less, with an alphabet character at the beginning.

> Point
>
> Follow these rules for specifying the hostname:
>
> – Characters usable for the name
> Alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), hyphen (-), and period (.)
>
> – First character
> Alphabet ([a - z], [A - Z])
>
> – Last character
> Alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), and period (.)

Command type

Configuration command

Default

"xg"

Example

Specify the hostname of the device to be "xg2."
The prompt will change to "xg2."
Switching to the administrator exec mode and displaying the system status will confirm that the System Name was changed to "xg2."

```
xg(config)# hostname xg2
xg2(config)# exit
xg2# show system information
```

```
System Information  2007/01/22-11:04:54
==============================================
 System Name (hostname)  :  xg2
 System Location         : (none)
  . . .
  . . .
```

5.2.6 remote-host

Function

Registers remote host information and shows the relationship between the remote hostname and IP address.
By registering the IP address of a remote host that is used frequently, the name can be specified instead of the IP address. The relationship between the registered hostname and IP address is given priority over the DNS server configuration.
Use the no form to delete registered remote host information.

Prompt

xg(config)#

Command syntax

```
remote-host A.B.C.D HOST-NAME
no remote-host [ A.B.C.D ]
```

Parameter

- A.B.C.D
  Specifies the IP address of a remote host in A.B.C.D format.
  IP addresses that can be set are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- HOST-NAME
  Specifies the remote hostname to register. Specify the hostname using 63 characters or less, with an alphabet character at the beginning.

> Point
>
> Follow the rules below for the hostname and domain name:
> - Characters usable for the name
>   Alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), hyphen (-), and period (.)
> - First character
>   Alphabet ([a - z], [A - Z])
> - Last character
>   Alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), and period (.)

- (no remote-host) [A.B.C.D]
  Deletes the registered remote host. Specify the IP address in A.B.C.D format.
  When IP address is omitted, all registered remote hosts will be deleted.

Command type

Configuration command

Default

None

Message

% Invalid IP-address.

Explanation
The specified format of the IP address or specified content is incorrect.

Solution
Specify the IP address in a correct format and execute the command again.

% Number of remote-host is over (max=10)

Explanation
The upper limit of the number of registrable remote hosts was surpassed.

Solution
After deleting unnecessary hosts, execute the command again.

% Already exist name of remote host

Explanation
A remote hostname with the same IP address was previously registered.

Solution
Change the remote hostname of the IP address to the correct name, or register it again after deleting it.

% Not exist IP-address of remote host

Explanation
The specified host definition is not registered.

Solution
Specify a registered IP address and execute the command again.

Note

- If a remote host is registered or deleted, the new setting becomes enabled after executing “copy running-config startup-config” command and restart the device.

Example

Register the IP address "11.22.33.45" as the hostname of "HOST005," and then "11.22.33.46" as the hostname of "HOST006." Using the show remote-host command, registration of "HOST005" and "HOST006" can be confirmed.

```
xg(config)# remote-host 11.22.33.45 HOST005
xg(config)# remote-host 11.22.33.46 HOST006
xg(config)# exit
xg# show remote-host
```

```
Remote Host  2007/01/22-11:45:46
================================
IP Address     Host Name
---------- ------------------------------------------
11.22.33.45    HOST005
11.22.33.46    HOST006
```

5.3 Serial/Telnet/SSH Configuration Commands

This section explains configuration commands related to a serial connection/telnet/SSH connection.

5.3.1 terminal pager

Function

Enables or disables the pager function of the serial/telnet/SSH terminal.

Prompt

xg> or xg#

Command syntax

```
terminal pager { on | off }
```

Parameter

- pager { on | off }
  Specifies enable/disable of the pager.
  - on
    Enables the pager.
  - off
    Disables the pager.

Command type

Operation management commands

Default

on

Note

- This command is effective until the terminal is disconnected.

5.3.2 line

Function

Switches to the terminal edit mode

Prompt

xg(config)#

Command syntax

```
line console
```

Parameter

- console
  Switches to the terminal edit mode of the serial connection.

Command type

Configuration command

Example

Switch from the administrator exec mode to the terminal edit mode with the serial interface.

```
xg# configure terminal
xg(config)# line console
```

5.3.3 baud-rate

Function

Sets the serial baud rate (bps).

Prompt

xg(config-line)#

Command syntax

```
baud-rate { 9600 | 19200 | 38400 | 57600 }
```

Parameter

- { 9600 | 19200 | 38400 | 57600 }
  Specifies any of 9600/19200/38400/57600 as the serial baud rate (bps).

Command type

Configuration command

Default

9600

Note

- When the serial baud rate is newly set, it will become valid after logging out of the serial terminal session and re-connecting.

Example

Switch from the global configuration mode to the terminal edit mode using the "line console" command. And then change the serial baud rate to 38400bps.

```
xg(config)# line console
xg(config-line)# baud-rate 38400
```

5.3.4 terminal timeout

Function

Sets the monitoring idle time for a serial connection, or telnet and SSH connections.
When there is no operation from the terminal within the monitoring time specified with this command, the terminal will be logged out automatically.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
terminal timeout { console | vty } <0-60>
no terminal timeout { console | vty }
```

Parameter

- timeout { console | vty }
  Specifies the type of the terminal.
  - **console**
    Sets the monitoring idle time for a serial connection.
  - **vty**
    Sets the monitoring idle time for a telnet and SSH connections.
- <0-60>
  Specifies the monitoring idle time. Specified in the range of 0 to 60 minutes.
  When 0 is specified, no-operation monitoring is performed, and the terminal will not be logged out automatically.

Command type

Configuration command

Default

10 minutes

Note

- While the "monitor" command or the "update-system" command is being executed, no-operation monitoring is deterred.
- The setting of this command will become valid after login.

Example

Set the monitoring idle time for the serial connection, and Telnet and SSH connections to 10 minutes and 5 minutes respectively.

```
xg# configure terminal
xg(config)# terminal timeout console 10
xg(config)# terminal timeout vty 5
```

5.3.5 telnet-server

Function

Enables telnet connections with the device.
Use the no form to disable telnet connections.

Prompt

xg(config)#

Command syntax

```
telnet-server
no telnet-server
```

Command type

Configuration command

Default

Disabled

Example

Enable telnet connections to the device.

```
xg(config)# telnet-server
```

5.3.6 ssh-server

Function

Enables SSH connections with the device. Up to 4 terminal sessions can access the device concurrently.
Use the no form to disable SSH connections.

Prompt

xg(config)#

Command syntax

```
ssh-server
no ssh-server
```

Command type

Configuration command

Default

None

Note

- The device supports password authentication.
- The device supports only version 2.

Example

Enable SSH connections to the device.

```
xg(config)# ssh-server
```

5.3.7 ssh-auto-key-generation

Function

Regenerate authentication key when enables SSH connection.
Use the no form not to regenerate authentication key.

Prompt

xg(config)#

Command syntax

```
ssh-auto-key-generation
no ssh-auto-key-generation
```

Command type

Configuration command

Default

None

Example

The following enables to regenerate authentication key.

```
xg(config)# ssh-auto-key-generation
```

5.3.8 show ssh-host-key

Function

Shows authentication key.

Prompt

xg> or xg#

Command syntax

```
show ssh-host-key
```

Command type

Operation management commands

Output form

```
xg# show ssh-host-key
SSH Host Key                                        2007/09/07-17:10:33
===============================================================================
ssh-dss AAAAB3NzaC1kc3MAAACBALZunL9ymdBEx4QFOsKhwwCf7WpCwpLne6ZNgc7keG/2Yf0OY4Yx
MwOgf1Dm5SSaN/pSdfKotT/zN3ywpDQywlNVjNxF7IYk/p3Q/jABPa245A1Mu9l9a8IiOZhV+w0vMI8N
vTi4Cqk2S+tSDzf2vXQ58KCAijeyGDrEi71bZPgbAAAAFQDjkiO5/EupRfrKMc2HHpM7OWtF+QAAAIBR
c1CGq9Wt60LV6DkzrYhLNcRgkRNi/XFARzyyFX3TWm2LPBDd8/nbp3zc+N5poNKHBJ/61somWzqKVrTA
nR/AQDEyftltVgr4vWn1IDEtu6IZzShZGfgFDk2aZIVP3jFr0BEz5GV+eoGkQb4Be3qJHKiomIjNi+As
vrSYfBqSnQAAAIBj+rJ2lZcTRtzgkmeJvjf0q52sHFL+zSC27e24c/BU7V+Hr2xw50I+bVZNbxHGMWtb
Ma9mQmBbKmotWq8wRxHluBsQ/5ZktlQrT60M0F8zF+vBFYV3PPG+LvpA8MTYDvjXkZ7w0ZypU/ShRqiZ
R8X0wyVvA2GoBCiPlXj1VfmZHA== admin@xg

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA1qtD/sBupdj89yRApm2o3pZCpaodDwljdmgW8iBfmtmO
SUnLYcszHW+dNTg7QXeoEyU+MyZMzYxQH1kABB3Wl+rfP0dZ7Ri4nCm+fYWN6QCX8M5hHVuALz5ITmBA
sWxhQUvxDxI+VdpUB3ta4xgKiPOMFfVBjdr4M6Upr9+jaVG6pyWCDGtkEL4qbLUXTx1XqFsNtuLwembg
ZUWTXo3cU6BXZ2B+wo8mpgsvcabcN1gZiTycAs3WIj/0V8lp0hglQKsfOqIF8b9pNWEi2NqIMbDSG+yz
BzXNqwg6IbpCUMxdBMeij97YafJTl1+h5zJvxP2AsrannGlIdeYJxXYaWQ== admin@xg
===============================================================================
```

Example

The following shows authentication key.

```
xg# show ssh-host-key
```

5.3.9 show ssh-rhost-key

Function

Shows registered public key of SSH remote host.

Prompt

xg> or xg#

Command syntax

```
show ssh-rhost-key
```

Command type

Operation management commands

Output form

```
xg# show ssh-rhost-key
SSH Remote Host Key                                        2008/07/07-04:24:24
===============================================================================
192.168.1.10 ssh-rsa  AAAAB3NzaC1yc2EAAAABIwAAAIEA0hyfbg54vUvQD8aUkpxTaSeRPFUdk
vKDGkXy+LBf+JWV2XZB4cINAJll6rn3HbkzEiJRrAG+Pwzn35FHRuW7sWjiyMmaRVXnWRrryFJwUKaAB
R2XchMbRLn3cz22ioA8H89OUvQj4JIGGYF3qjCxFz2rNPpU27Z18YczflvHHVM=yuyussh-rsaAAAAB3
NzaC1yc2EAAAABIwAAAIEA0hyfbg54vUvQD8aUkpxTaSeRPFUdkvKDGkXy+LBf+JWV2XZB4cINAJll6r
n3HbkzEiJRrAG+Pwzn35FHRuW7sWjiyMmaRVXnWRrryFJwUKaABR2XchMbRLn3cz22ioA8H89OUvQj4
JIGGYF3qjCxFz2rNPpU27Z18YczflvHHVM=
===============================================================================
```

Example

The following shows registered public key.

```
xg# show ssh-rhost-key
```

5.3.10 clear ssh-rhost-key

Function

Delete registered public key of SSH remote host.

Prompt

xg#

Command syntax

```
clear ssh-rhost-key [ HOST ]
```

Parameter

- HOST

  Specifies the host name or IP address of a SSH server.
  If this parameter is omitted, all public keys will be deleted.

Command type

Operation management commands

Example

Delete the public key for the SSH server whose IP address is “192.168.1.10”

```
xg# clear ssh-rhost-key 192.168.1.10
```

5.3.11 generate ssh-host-key

Function

Generate authentication key. If it has already been made, it is regenerated.

Prompt

xg#

Command syntax

```
generate ssh-host-key
```

Command type

Operation management commands

Example

The following generates authentication key.

```
xg# generate ssh-host-key
```

5.3.12 terminal window

Function

Sets the screen display size of the serial connection terminal.
Use the no form to return to the default setup.
For a telnet or SSH connection, the screen size will be obtained automatically from the client terminal.

Prompt

(config-line)#

Command syntax

```
terminal window <50-200> <12-100>
```

Parameter

- <50-200>
  Specifies the number of columns (horizontal) of the screen. It can be set in the range of 50 to 200.
- <12-100>
  Specifies the number of lines (vertical) of the screen. It can be set in the range of 12 to 100.

Command type

Configuration command

Default

80 columns by 24 lines

5.4 System Basic Operation Commands

This section explains the basic commands of the device CLI (Command Line Interface).

5.4.1 enable

Function

Switches from the operator exec mode to the administrator exec mode.
When a password is set for the "enable" command, a password is required. When there is an error in entering the password, re-entering the password will be allowed up to three times. Additionally, after successful authentication of the password, for a given login session, the user will not be prompted for the password until they exit the administrator exec mode and re-enter the mode.

Prompt

xg>

Command syntax

```
enable
```

Command type

Operation management commands

Example

Switch from the operator exec mode to the administrator exec mode using the "enable" command.
The prompt character will change to "xg#."

```
xg> enable
xg#
```

When a password is set for the "enable" command, enter the password.
When password authentication is successful, control switches to the administrator exec mode, and the prompt character will change to "xg#."

```
xg> enable
Password:                      ←Enter the password to "enable."
xg#                             (The entered password is not displayed.)
```

5.4.2 show history

Function

Displays the history of executed commands since logged into the device.

Prompt

xg> or xg#

Command syntax

```
show history
```

Command type

Operation management commands

Output form

```
xg# show history
   1 enable
   2 show system information
   3 date
   4 show system information
   5 show history
```

Note

- If the same command is executed continuously, it is treated as one command.
- Up to 100 history will be displayed.

Example

Displays the history of executed commands.

```
xg# show history
```

5.4.3 disable

Function

Switch from the administrator exec mode to the operator exec mode.

Prompt

xg#

Command syntax

```
disable
```

Command type

Operation management commands

Example

Switch from the administrator exec mode to the operator exec mode using the "disable" command.
The prompt character will change to "xg>."

```
xg# disable
xg>
```

5.4.4 configure terminal

Function

Switch from the administrator exec mode to the global configuration mode.

Prompt

xg#

Command syntax

```
configure terminal
```

Command type

Operation management commands

Message

```
Configuration is locked by other.
```

Explanation

A switch in state is not possible because a terminal session in global configuration mode exists.

Solution

After switching the terminal session from global configuration mode to administrator EXEC mode, re-execute the command.

Example

Switch from the administrator exec mode to the global configuration mode using the "configure terminal" command.
The prompt character will change to "xg(config)#."

```
xg# configure terminal
xg(config)#
```

5.4.5 exit

Function

Returns to the prior command mode level.
The relationship between the current command mode and the command mode status after executing the "exit" command is as follows:

Current command mode	Status after exit
Operator exec mode	Log out
Administrator exec mode	Log out
Global configuration mode	Administrator exec mode
Interface	Global configuration mode
Terminal edit mode	Global configuration mode

Prompt

xg>, xg#, xg(config)# , xg(config-if)# , xg(config-agg)# , xg(config-vlan)# , xg(config-line)#

Command syntax

```
Exit
```

Command type

Operation management commands

Example

Switch from the global configuration mode to the administrator exec mode using the "exit" command.
The prompt character will change to "xg#."

```
xg#(config)# exit
xg#
```

5.4.6 logout / quit

Function

Logs out and disconnects the terminal session.

Prompt

xg> or xg#

Command syntax

```
Logout
```

Command type

Operation management commands

Example

Log out and disconnect the terminal session.

```
xg# logout
Connection closed by foreign host.
```

5.4.7 do

Function

Executes administrator exec mode commands from the global configuration mode.
Using this command saves the trouble of having to return to the administrator exec mode.

Prompt

xg(config)#

Command syntax

```
do LINE
```

Parameter

- LINE
  Specifies the command line for the administrator exec mode to execute.

Command type

Operation management commands

Message

Can't execute this command.

Explanation

The specified command cannot be executed with the do command.

Solution

Execute the command in an appropriate mode without using the do command.

Example

Set "bridge aging-time" from the global configuration mode. And then, without returning to the administrator exec mode, check the setting status using the "show bridge" command.

```
xg(config)# bridge aging-time 200
xg(config)# do show bridge
```

```
Switch Basic Information                     2007/01/22-12:16:17
================================================================
Aging Time                : 200 (sec)
Cut-through Switching     : Enabled
Jumbo Frame Support       : Enabled  Max Frame Size: 9216 (byte)
Independent-vlan-learning: Enabled
DiffServ ToS              : Disabled
================================================================
```

5.4.8 help

Function

Displays help on how to use the CLI.

Prompt

xg>, xg#, xg(config)# , xg(config-if)# , xg(config-agg)# , xg(config-vlan)# , xg(config-line)#

Command syntax

```
Help
```

Command type

Operation management commands

5.4.9 show account

Function

Displays information about the user.

Prompt

xg> or xg#

Command syntax

```
show account
```

Command type

Operation management commands

Output form

```
xg# show account
Username Information                                      2007/10/04-14:33:42
=============================================================================
Username                          Class
--------------------------------- ----------
admin                             admin
operator1                         operator
user0001                          admin
=============================================================================
```

- Username
  Display the username.
- Class
  Display the class that the user can access to.
  operator : The user can access operator class only.
  admin   : The user can access both operator and administrator class.

Example

Display the user status.

```
xg# show account
```

5.4.10 account

Function

Create a new user.
Use the no form to delete the specified user.

Prompt

xg#

Command syntax

```
account USERNAME class { operator | admin }
no account USERNAME
```

Parameter

- USERNAME
  Specify a username with a length in the range of 2 to 16 characters, with an alphabet character at the beginning.

  > Follow these rules for specifying a username:
  > - Characters usable for the username
  >   Alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), hyphen (-), underscore (_), and period (.)
  > - First character
  >   Alphabet ([a - z], [A - Z])

- class { operator | admin }
  Specify the class that the user can access to.
  - operator
    The user can access operator class only.
  - admin
    The user can access both operator and administrator class.

Command type

Operation management commands

Default

admin (username) is admin class

Message

```
% The length of user name is invalid.
```
Explanation
The length of the username is invalid.
Solution
Specify the username between 2 and 16 characters.

```
% First character is invalid.
```
Explanation
The first character of the username is invalid.
Solution
Specify the first character of the username to be an alphabet.

```
% Invalid character is included.
```
Explanation
Invalid character is included in the username.
Solution
Specify characters usable for the username.

```
% USERNAME already exists.
```
Explanation
The user could not be added because specified username is already used.
Solution
Change the username or delete the user and execute the command again.

```
% cannot add user.
```
Explanation
The user could not be added.
Solution
Review the password and execute the command again.

```
% USERNAME does not exist.
```
Explanation
The user could not be deleted because it does not exist.
Solution
Review if the username exists.

```
% 4 users already exist.
```
Explanation
The maximum number of users was exceeded.
Solution
After deleting unnecessary users, execute the command again.

```
% The user name is reserved.
```
Explanation
Reserved username is specified.
Solution
Change the username and execute the command again.

Note

- Specify a password with a length in the range of 5 to 16 characters.
- The maximum number of users that can register to this device is 4.

Example

Add user0001 as the username and specify operator class:

```
xg# account user0001 class operator
Changing password for user0001
Enter the new password (minimum of 5, maximum of 16 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:******      ← Enter the password.
                               (The entered password is not displayed.)
Re-enter new password: ******** ← Enter the new password again for confirmation
Password changed.              (The entered password is not displayed.)
```

5.4.11 password (Operator EXEC mode)

Function

Change the login password of logged in user to the device.

Prompt

xg>

Command syntax

```
password
```

Command type

Operation management commands

Message

```
Bad password: too short.
```

Explanation

```
The password is too short.
```

Solution

```
Specify a password using five or more characters.
```

```
Bad password: too long.
```

Explanation

```
The password is too long.
```

Solution

```
Specify a password using 16 or less characters.
```

Note

- This command (password command for Administrator exec mode) is executable only when the user can access operator class only (see account command for the details).
- Specify a password with a length in the range of 5 to 16 characters.
- Make a note of the changed password and retain it. Refer to Section 7.1.3, Restoring Factory Defaults for recovery of lost or forgotten passwords.
- Login password information is not included in the configuration information. Therefore, even when the configuration information is downloaded to another device, the password information will not be displayed or transferred.

Example

operator1 that can access only operator class logged in the device and change own login password.

```
xg> password
Changing password for operator1
Enter the new password (minimum of 5, maximum of 16 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Re-enter new password:
Password changed.
```

5.4.12 password (Administrator EXEC mode)

Function

Change the login password of the device.

Prompt

xg#

Command syntax

```
password [USERNAME]
```

Parameter

- USERNAME
  Specify the username to change its login password. When USERNAME is omitted, the login password of own user is changed.

Command type

Configuration command

Message

```
Bad password: too short.
```

Explanation

```
The password is too short.
```

Solution

```
Specify a password using five or more characters.
```

```
Bad password: too long.
```

Explanation

```
The password is too long.
```

Solution

```
Specify a password using 16 or less characters.
```

Note

- This command (password command for Global configuration mode) is executable only when the user can access both operator and administrator class (see account command for the details).
- Specify a password with a length in the range of 5 to 16 characters.
- Make a note of the changed password and retain it. Refer to Section 7.1.3, Restoring Factory Defaults for recovery of lost or forgotten passwords.
- Login password information is not included in the configuration information. Therefore, even when the configuration information is downloaded to another device, the password information will not be displayed or transferred.

Example

Change the login password of the user that username is operator1.

```
xg# password operator1
Changing password for operator1
Enter the new password (minimum of 5, maximum of 16 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Re-enter new password:
Password changed.
```

5.4.13 reset

Function

Restarts the device.

Prompt

```
xg#
```

Command syntax

```
reset [ factory-default ]
```

Parameter

- **[factory-default]**
  When this parameter is specified, the contents of startup-config, log, and login password will be returned to the factory default.

Command type

Operation management commands

Note

- When the system is restarted without having saved the running-config to startup-config, the information set in running-config will be lost.
- When the device is restarted, the telnet and SSH sessions will be disconnected. Reconnect after restart of the system is complete.

Example

Restart the device using the "reset" command.
When the "reset" command is executed, the confirmation message is displayed.

```
xg# reset
Do you restart system? (y/n) :  Confirmation message is displayed.
```

When "y" or "Y" is entered, the reboot process will be performed. When "n" or "N" is entered, the reboot process will be cancelled.

5.4.14 system shutdown

Function

Stops the device system and prepares it for power off.
After executing this command and the STATUS-LED goes out, turn off the power to the device.

Prompt

xg#

Command syntax

```
system shutdown
```

Command type

Operation management commands

Note

- When power to the device is turned off without executing the system shutdown command, the maintenance information will not be properly stored. Furthermore, if the power is turned off while data is being written to nonvolatile memory, it may be corrupted, and the system might not restart correctly on powerup.
- When the system is shut down without saving running-config to startup-config, the information set in running-config will be lost.

Example

When the "system shutdown" command is executed, the confirmation message is displayed.

```
xg# system shutdown
Do you shutdown system? (y/n) : ← Confirmation message is displayed.
```

When "y" or "Y" is entered, the system shutdown process will be performed. When "n" or "N" is entered, the system shutdown process will be canceled.

5.4.15 date

Function

Displays the date/time of the current system clock.

Prompt

xg> or xg#

Command syntax

```
Date
```

Command type

Operation management commands

Output form

The current date and time is displayed in the form of "year/month/date-hour:minutes:seconds."

```
xg# date
2007/01/22-14:31:02
```

5.4.16 date set

Function

Changes the date/time of the current system clock.

Prompt

xg#

Command syntax

```
date set DATE-TIME
```

Parameter

- DATE-TIME

  Enter the date and time in the form of "MMDDhhmm[[CC]YY][.ss]."

  - **MM**

    Specify the month to set in the range of 1 to 12.
  - **DD**

    Specify the day to set in the range of 1 to 31.
  - **hh**

    Specify the hour to set in the range of 0 to 23.
  - **mm**

    Specify the minutes to set in the range of 0 to 59.
  - **[[CC]YY]**

    Specify the first two digits of the four digits of the year for CC. When it is omitted 20 will be specified.
    Specify the last two digits of the four digits of the year for YY.
    If CC and YY are both omitted, the year will not be changed.
  - **[.ss] (second <0 - 59>)**

    Specify the seconds to set in the range of 0 to 59.

Command type

Operation management commands

Message

% invalid date %1$.

Explanation

The specified parameter of the date and time is incorrect.
[[Inserted string]]%1$: specified date and time

Solution

Check that no mistakes have been made in the date and time parameter.

Example

Set the date and time of the system to 20:25:30, June 30, 2005.

```
xg# date set 06302025.30        (Year omitted)
or
xg# date set 0630202505.30      (Year specified with the last two digits)
or
xg# date set 063020252005.30    (Year specified with four digits)
```

5.4.17 date timezone

Function

Sets the time zone of the device.
Use the no form to return to the default setup.

Prompt

xg#

Command syntax

```
Date timezone gmt OFFSET
No date timezone
```

Parameter

- gmt [OFFSET]
  Specifies the time zone as the difference from GMT (Greenwich Mean Time).
  The time difference from GMT is specified in the form of "+hhmm" (+ can be omitted) when setting forward from GMT.
  It is specified in the form of "-hhmm" when setting backward from GMT.
  - **hh**
    Specifies the hour difference from GMT.
  - **mm**
    Specifies the minute difference from GMT.

  It can be set in the range of -1200 to +1300.

Command type

Operation management commands

Default

0000

Message

```
% invalid input %1$.
```

Explanation

The specified parameter for the time difference is incorrect.
[[Inserted string]]%1$: specified time difference

Solution

Check that no mistakes have been made in the time difference parameter.

Note

- The setting will be valid after restarting the system.
- Use the "show system information" command to confirm the settings.
- The setting will not be included in the configuration information. Therefore, even if the configuration information was restored by another device, the timezone setting will be invalid.

Example

Set the time zone to +9:00 (JST: Japan Standard Time) from GMT.

```
xg# date timezone gmt +0900
or
xg# date timezone gmt 0900
```

Then set the time zone to -1:30 from GMT.

```
xg# date timezone gmt -0130
```

5.4.18 date summer-time

Function

Sets Daylight Saving Time.
Use the no form to return to the default setup.

Prompt

xg#

Command syntax

```
date summer-time START_DAY[/TIME] END_DAY[/TIME] [OFFSET]
no date summer-time
```

Parameter

- START_DAY[/TIME]

  Specifies the day/time to start Daylight Saving Time in any form of "Mm.w.d/hhmm," "Jn/hhmm," or "n/hhmm."

  - **Mm.w.d**

    Specifies the day to start Daylight Saving Time in m, w, and d.
    Specify month for m (1 to 12), week for w (1 to 5), and the day of the week for d (0 to 6).
    w = 1 means the first week where d exists, and w = 5 means the last week.
    d = 0 means Sunday.

  - **Jn**

    Specifies the day to start Daylight Saving Time in day-of-year (Julian day). In leap years, February 29th is not counted. Specify a number in the range of 1 to 365 for n.

  - **n**

    Specifies the day to start Daylight Saving Time in day-of-year. In leap years, February 29th is counted. Specify a number in the range of 1 to 366 for n.
    Specifies the following values, for the first day of each month in "Jn" specification and "n" specification.

Month/Day	Jn specification	specification	
		Common year	Leap year
January 1st	J1	1	1
February 1st	J32	32	32
March 1st	J60	60	61
April 1st	J91	91	92
May 1st	J121	121	122
June 1st	J152	152	153
July 1st	J182	182	183
August 1st	J213	213	213
September 1st	J244	244	245
October 1st	J274	274	275
November 1st	J305	305	306
December 1st	J335	335	336

  - **hh**

    Specifies the hour to start Daylight Saving Time.

  - **mm**

    Specifies the minute to start Daylight Saving Time.

  When hhmm is omitted, "0100" (an hour) is specified.

- END_DAY[/TIME]

  Specifies the day/time to end Daylight Saving Time. The description format is the same as "START_DAY/TIME."

- OFFSET

  Specifies the time set forward during Daylight Saving Time in the form of "hhmm."

  - **hh**

    Specifies the hour set forward during Daylight Saving Time with a two-digit number. It can be set in the range of 00 to 23.

  - **mm**

    Specifies the minute set forward during Daylight Saving Time with a two-digit number. It can be set in the range of 00 to 59.

  When this parameter is omitted, "0100" (an hour) is specified.

Command type

Operation management commands

Default

None

Message

```
% DATE '%1$' is invalid
```

Explanation

The specified date/time is incorrect.
[[Inserted string]]%1$: incorrect parameter value is displayed.

Solution

Correct the error in the parameter, and execute the command again.

```
% OFFSET '%1$' is invalid
```

Explanation

The specified OFFSET is incorrect.
[[Inserted string]]%2$: incorrect parameter value is displayed.

Solution

Correct the error in the parameter, and execute the command again.

```
% Parameter '%1$' is too long
```

Explanation

The parameter specified is too long.
[[Inserted string]]%1$: incorrect parameter value is displayed.

Solution

Correct the error in the parameter, and execute the command again.

```
% DATE '%1$' is too long
```

Explanation

The date specified is too long.
[[Inserted string]]%1$: incorrect parameter value is displayed.

Solution

Correct the error in the parameter, and execute the command again.

```
% Type of start-day and end-day is inconsistency
```

Explanation

Different formats are specified for start date and end date parameters of Daylight Saving Time.

Solution

Make the formats of the start date and end date of Daylight Saving Time (Mm.w.d/ Jn/ n) consistent, and execute the command again.

Note

- The setting will be valid after restarting the system.
- Use the "show system information" command to confirm the settings.
- The setting will not be included in the configuration information. Therefore, even if the configuration information was restored by another device, the timezone setting will be invalid.

Example

Set Daylight Saving Time period (from 2:00, Sunday, the first week in April, through to 02:00, Sunday, the fifth week in October, with a time difference of an hour).

```
xg# date summer-time M4.1.0/0200 M10.5.0/0200 0100
```

5.4.19 ping

Function

Checks if communication with the specified host is possible by sending ICMP Echo Request packets to a specified host from the manage LAN interface and observing the reception of ICMP Echo Reply packets.

Prompt

xg> or xg#

Command syntax

```
ping HOST [ count <1-100> ]
```

Parameter

- HOST
  Specifies the hostname or IP address to check.
- count <1-100>
  Sets the count to transmit. 1 to 100. If omitted, 10 will be specified.
  Press Ctrl + C to abort the ping process.

Command type

Operation management commands

Output form (when the host to check is working normally)

```
xg# ping white
PING white (192.168.1.1) from 192.168.1.2 : 56(84) bytes of data.
64 bytes from white (192.168.1.1): icmp_seq=1 ttl=64 time=0.780 ms ← There is a response.
64 bytes from white (192.168.1.1): icmp_seq=2 ttl=64 time=0.592 ms ← There is a response.
........
........
--- white ping statistics ---        ← Displayed after aborting the process pressing Ctrl+ C.
5 packets transmitted, 5 received, 0% loss, time 4041ms
rtt min/avg/max/mdev = 0.549/0.619/0.724/0.060 ms
```

Output form (when the host to check is in trouble)

```
xg# ping blue
PING blue (192.168.1.3) from 192.168.1.2 : 56(84) bytes of data.← There is no response.
292 packets transmitted, 0 received, 100% loss, time 293516ms ← Displayed after aborting the process
                                                                pressing Ctrl+ C.
```

Message

```
ping: unknown host %1$.
```

Explanation

The specified hostname is incorrect.
[[Inserted string]]%1$: specified hostname

Solution

Review the hostname, and execute the command again.

5.4.20 enable password

Function

Sets the password for the enable command.
Use the no form to disable the password protection.

Prompt

xg(config)#

Command syntax

```
enable password

no enable password
```

Parameter

- password
  Specifies the password to associate with the enable command.
  After executing the command, entry of a password will be prompted. (Enter twice for confirmation.)
  Specify a password with a length in the range of 5 to 16 characters.

Command type

Configuration command

Default

None

Note

- The password will be encrypted and reflected in running-config.
- The password will not be displayed by any means after executing the command. Make a note of the set password and retain it.

Example

Set the enable password from the global configuration mode using the "enable password" command.
Then, return to the administrator exec mode and execute "show running-config." The encoded password will be displayed.

```
xg(config)# enable password
Enter password:             ← Enter the password.
                              (The entered password is not displayed.)
Re-enter password:          ← Enter the password again for confirmation.
                              (The entered password is not displayed.)
xg(config)# exit
xg# show running-config
```

```
. . . .
. . . .
enable encryption-password 4DUzjKbFg9.iU  ← The password is encoded and output.
!
. . . .
```

5.4.21 banner

Function

Sets the banner string to be displayed when logging in to the device.
Use the no form to delete the banner string.

Prompt

xg(config)#

Command syntax

```
banner login LINE
banner login default

no banner
```

Parameter

- login LINE
  Sets a banner string. No need to enclose a parameter in quotes if it contains a blank space.
- login default
  Returns the banner string to its default ("Product name firmware identification information").

Command type

Configuration command

Default

"Product name(XG2000, XG2000R, XG2000C or XG2000CR) firmware identification information"

The firmware identification information is the same information displayed in FirmWare[1] or FirmWare[2] of the "show system information" command.

Example

Set the banner string to "Welcome to XG2000."

```
xg(config)# banner login Welcome to XG2000
```

5.4.22 ntp-server

Function

Synchronizes the system time to a specified NTP server's time, using NTP (Network Time Protocol) Version3. Up to four NTP servers can be registered.
Use the no form to return the setting to its default.

Prompt

xg(config)#

Command syntax

```
ntp-server host HOST
ntp-server polling MINUTES
ntp-server timeout SECONDS

no ntp-server host HOST
no ntp-server polling
no ntp-server timeout
```

Parameter

- host HOST
  Specifies the hostname or IP address of an NTP server.
  IP addresses that can be set are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- polling MINUTES
  Specifies the time interval for synchronizing the device time with an NTP server in minutes. The value can be set in the range of 1 to 1440.
- timeout SECONDS
  Specifies the response latency of an NTP server in seconds. The value can be set in the range of 1 to 4.

Command type

Configuration command

Default

host : None
polling: 60 minutes
timeout: 1 second

Message

`% hostname can register up to 4.`

Explanation

The number of hosts that can be set to an NTP server was exceeded.

Solution

After deleting unnecessary NTP servers, execute the command again.

`% Cannot find %1$`

Explanation

The specified host cannot be found.
[[Inserted string]]%1$: specified hostname

Solution

Check that the hostname is correct, or the hostname is registered.

`% Hostname is too long`

Explanation

The specified hostname is too long.

Solution

Check that the hostname is correct.

`% Invalid IP-address.`

Explanation

The specified format of the IP address or specified content is incorrect.

Solution

Specify the IP address in a correct format and execute the command again.

Note

- Set the time zone and Daylight Saving Time to a correct value beforehand, and reboot the system. Then, NTP servers can be registered.
- If several NTP servers' IP addresses are registered by this command, the order of accessing to NTP servers are shown in "show running-config" command.
- If the host name is specified instead of IP address, changing the NTP server's IP address at DNS server will not be enabled. It is necessary to restart the device after DNS server's IP address has been changed.

Example

Register an NTP server with IP address "192.168.1.1" and set the interval for time synchronization to 600 minutes.

```
xg(config)# ntp-server host 192.168.1.1
xg(config)# ntp-server polling 600
```

5.5 RADIUS/TACACS+

This section explains the commands related to RADIUS/TACACS+.

5.5.1 show authentication

Function

Displays the setting status of authentication method.

Prompt

xg#

Command syntax

```
show authentication
```

Command type

Operation management commands.

Output form

```
xg# show authentication
Authentication Information                                  2008/05/20-16:23:25
===============================================================================
Serial/Telnet(console)
====================================
Login Primary   : Local
Login Secondary : none

SSH(ssh)
====================================
Login Primary   : RADIUS
Login Secondary : none
===============================================================================
```

- Login Primary
  Displays the primary login authentication method.
  - Local
    Local authentication based on the account information stored in the device is used.
  - RADIUS
    RADIUS authentication using PAP(User Password) is used.
  - TACACS+
    TACACS+ authentication using PAP(User Password) is used.
- Login Secondary
  Displays the secondary login authentication method. Secondary login authentication is used if primary login authentication is failed.
  - Local
    Local authentication based on the account information stored in the device is used.
  - none
    Secondary login authentication is disabled.

Example

Displays the setting status of authentication method.

```
xg# show authentication
```

5.5.2 aaa authentication login

Function

Configure login authentication method.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
aaa authentication login { console | ssh } { local | radius | tacacs } [{ local |
none }]
no aaa authentication login { console | ssh }
```

Parameter

- { console | ssh }
  Select a service to login.
  - console
    Configure the authentication method for serial console or telnet login.
  - ssh
    Configure the authentication method for SSH login.
- { local | radius | tacacs }
  Specify the primary login method.
  - local
    Local authentication based on the account information stored in the device is used.
  - radius
    RADIUS authentication using PAP(User Password) is used.
  - tacacs
    TACACS+ authentication using PAP(User Password) is used.

- { local | none }
  Specify the secondary login authentication method. Secondary login authentication is used if primary login authentication is failed.
  - local
    Local authentication based on the account information stored in the device is used.
  - none
    Secondary login authentication is disabled.

  This parameter is valid when RADIUS/TACACS+ is set as the primary login method.
  When this parameter is omitted, "local" is specified.

Command type

Configuration command

Default

Primary login is local and Secondary login is none for all services

Note

- It is needed to register RADIUS/TACACS+ user accounts to XG2000, using "account" command, before enabling RADIUS/TACACS+ authentication. XG2000 does not allow any account except for "admin" for the default configuration.
- Before local authentication is disabled, It is recommended to test RADIUS/TACACS+ authentication under local authentication is available.

Example

The following configuration enables RADIUS authentication as primary method and local authentication as secondary method for SSH login authentication.

```
xg(config)# aaa authentication login ssh radius local
```

5.5.3 show radius

Function

Displays the information of RADIUS server.

Prompt

xg#

Command syntax

```
show radius
```

Command type

Operation management command

Output form

```
xg# show radius
RADIUS Information                                          2008/05/20-16:26:00
================================================================================
Global Parameters
===============================================
Secret Key     : radius-b1
Timeout(sec)   : 3

Server Information
=============================================================================
 [No.1]
  Host      : 192.168.0.10
  Auth Port : 1812
  Secret Key: alkdje
[No.2]
  Host      : 192.168.0.11
  Auth Port : 1812
  Secret Key: dkaaff
[No.3]
  Host      : back-radius-server
  Auth Port : 1645
  Secret Key: owqkz
[No.4]
  Host      : sample.com
  Auth Port : 1812
  Secret Key: poiure123
================================================================================
```

Global Parameters

Displays the common information for configuring RADIUS servers.

- Secret Key
  Displays a secret key which is used as a default parameter when the RADIUS server is registered without secret key.
- Timeout (sec)
  Displays timeout for access replay from a RADIUS server in seconds.

Server Information

Displays the current settings of RADIUS servers.

- [No. 1]
  Indicates the register number of the RADIUS server. Access requests to RADIUS servers are transmitted in order of the number.
- Host
  Displays IP address or hostname of the RADIUS server.
- Auth Port
  Displays UDP port number of the RADIUS server.
- Secret Key
  Displays a secret key used by the device and the RADIUS server.

Note

- Displayed secret keys are not encrypted.

Example

Displays the information of RADIUS server.

```
xg# show radius
```

5.5.4 radius-server host

Function

Registers a RADIUS server. Up to four RADIUS servers can be registered.
Use the no form to delete registered RADIUS servers.

Prompt

xg(config)#

Command syntax

```
radius-server host HOST [ auth-port <1 - 65535> ] [ key KEY ]
no radius-server host HOST
```

Parameter

- host HOST
  Specifies the hostname or IP address of a RADIUS server. IP addresses that can be set are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254. This device accesses to RADIUS servers in order which is shown in "show radius" command.
- auth-port <1 - 65535>
  Specifies UDP port number of a RADIUS server. It can be set in the range of 1 to 65535. 1812 is specified if this parameter is omitted.
- key KEY
  Specifies a secret key in ASCII character. Printable characters except for "?" and a space(ASCII code 0x20) can be specified and its length should be less than 33. A global secret key is specified if this parameter is omitted.

Command type

Configuration command

Default

None

Message

% Authentication server can register up to 4.

Explanation

Four RADIUS servers have already been registered.

Solution

Delete unnecessary RADIUS servers and execute the command again.

% Secret key is too long.

Explanation

The specified secret key is more than 32 characters.

Solution

Specifies the secret key under 33 characters.

% Invalid IP-address.

Explanation

The specified format of the IP address or the IP address is incorrect.

Solution

Specify the IP address in a correct format.

% Invalid secret key.

Explanation

A secret key is not specified, or an invalid character is set.

Solution

Specifies a secret key using available characters. If the secret key is not specified, a global secret key should be configured by "radius-server key" command before executing this command.

% Cannot find %1$

Explanation

The specified host cannot be found.
[[Inserted string]]%1$: specified hostname

Solution

Check that the hostname is correct, or the hostname is registered.

Example

The following example registers a RADIUS server as IP address is 192.168.0.10 and UDP port number is 1812 and secret key is “radius-bl” .

```
xg(config)# radius-server host 192.168.0.10 auth-port 1812 key radius-b1
```

5.5.5 radius-server key

Function

Specifies a global secret key which is used as a default parameter when the RADIUS server is registered without secret key. Use the no form to delete a global secret key.

Prompt

xg(config)#

Command syntax

```
radius-server key KEY
no radius-server key
```

Parameter

- key KEY
  Specifies a global secret key in ASCII character. Printable characters except for "?" and a space(ASCII code 0x20) can be specified and its length should be less than 33.

Command type

Configuration command

Default

None

Message

```
% Secret key is too long.
```

Explanation

The specified secret key is more than 32 characters.

Solution

Specifies the secret key under 33 characters.

```
% Invalid secret key.
```

Explanation

An invalid character is set.

Solution

Specifies a secret key using available characters.

Note

- A global secret key is referred only when a RADIUS server is registered without specifying a secret key.
- A secret key for a RADIUS server will synchronize to a new global secret key when the same secret key is specified.
- A global secret key for a RADIUS server will not be deleted even when no command is committed.

Example

The following example specifies a global secret key.

```
xg(config)# radius-server key radius-b1
```

5.5.6 radius-server timeout

Function

Specifies timeout for access replay from a RADIUS server.
Use the no form to return the setting to its default.

Prompt

xg(config)#

Command syntax

```
radius-server timeout <1 – 15>
no radius-server timeout
```

Parameter

- timeout <1 - 15>
  Specifies timeout for access replay from a RADIUS server in seconds.

Command type

Configuration command

Default

None

Note

- The timeout is referred only when a RADIUS server is registered. It is necessary to register RADIUS servers again if the timeout is changed so that RADIUS servers use new setting.

Example

The following example specifies the timeout in 10 seconds.

```
xg(config)# radius-server timeout 10
```

5.5.7 show tacacs

Function

Displays the information of TACACS+ server.

Prompt

xg#

Command syntax

```
show tacacs
```

Command type

Operation management command

Output form

```
xg# show tacacs
TACACS+ Information                                           2008/06/18-12:12:15
================================================================================
Global Parameters
===============================================
Secret Key     : tacacs-b1

Server Information
=============================================================================
 [No.1]
 Host      : 192.168.0.10
 Secret Key: alkdje
[No.2]
 Host      : 192.168.0.11
 Secret Key: dkaaff
[No.3]
 Host      : back-tacacs-server
 Secret Key: owqkz
[No.4]
 Host      : sample.com
 Secret Key: poiure123
================================================================================
```

Global Parameters

Displays the common information for configuring TACACS+ servers.

- Secret Key

  Displays a secret key which is used as a default parameter when the TACACS+ server is registered without secret key.

Server Information

Displays the current settings of TACACS+ servers.

- [No. 1]

  Indicates the register number of the TACACS+ server. Access requests to TACACS+ servers are transmitted in order of the number.
- Host

  Displays IP address or hostname of the TACACS+ server.
- Secret Key

  Displays a secret key used by the device and the TACACS+ server.

Note

- Displayed secret keys are not encrypted.

Example

Displays the information of TACACS+ server.

```
xg# show tacacs
```

5.5.8 tacacs-server host

Function

Registers a TACACS+ server. Up to four TACACS+ servers can be registered.
Use the no form to delete registered TACACS+ servers.

Prompt

xg(config)#

Command syntax

```
tacacs-server host HOST [ key KEY ]
no tacacs-server host HOST
```

Parameter

- host HOST

  Specifies the hostname or IP address of a TACACS+ server. IP addresses that can be set are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254. This device accesses to TACACS+ servers in order which is shown in "show tacacs" command.
- key KEY

  Specifies a secret key in ASCII character. Printable characters except for "?" and a space(ASCII code 0x20) can be specified and its length should be less than 33. A global secret key is specified if this parameter is omitted.

Command type

Configuration command

Default

None

Message

% Authentication server can register up to 4.

Explanation

Four TACACS+ servers have already been registered.

Solution

Delete unnecessary TACACS+ servers and execute the command again.

% Secret key is too long.

Explanation

The specified secret key is more than 32 characters.

Solution

Specifies the secret key under 33 characters.

% Invalid IP-address.

Explanation

The specified format of the IP address or the IP address is incorrect.

Solution

Specify the IP address in a correct format.

% Invalid secret key.

Explanation

A secret key is not specified, or an invalid character is set.

Solution

Specifies a secret key using available characters. If the secret key is not specified, a global secret key should be configured by "tacacs-server key" command before executing this command.

% Cannot find %1$

Explanation

The specified host cannot be found.
[[Inserted string]]%1$: specified hostname

Solution

Check that the hostname is correct, or the hostname is registered.

Example

The following example registers a TACACS+ server as IP address is 192.168.0.10 and secret key is “tacacs-bl” .

```
xg(config)# tacacs-server host 192.168.0.10 key tacacs-b1
```

5.5.9 tacacs-server key

Function

Specifies a global secret key which is used as a default parameter when the TACACS+ server is registered without secret key. Use the no form to delete a global secret key.

Prompt

xg(config)#

Command syntax

```
tacacs-server key KEY
no tacacs-server key
```

Parameter

- key KEY
  Specifies a global secret key in ASCII character. Printable characters except for "?" and a space(ASCII code 0x20) can be specified and its length should be less than 33.

Command type

Configuration command

Default

None

Message

```
% Secret key is too long.
```

Explanation

The specified secret key is more than 32 characters.

Solution

Specifies the secret key under 33 characters.

```
% Invalid secret key.
```

Explanation

An invalid character is set.

Solution

Specifies a secret key using available characters.

Note

- A global secret key is referred only when a TACACS+ server is registered without specifying a secret key.
- A secret key for a TACACS+ server will synchronize to a new global secret key when the same secret key is specified.
- A global secret key for a TACACS+ server will not be deleted even when no command is committed.

Example

The following example specifies a global secret key.

```
xg(config)# tacacs-server key tacacs-b1
```

5.6 Configuration File Operation Commands

This section explains the commands related to configuration files and file operations within volatile memory.

5.6.1 copy running-config startup-config

Function

Stores the configuration file (running-config) in volatile memory to the startup-config file in nonvolatile memory.
After changing running-config, use this command to use the same configuration file after restarting the system.

Prompt

xg#

Command syntax

```
copy running-config startup-config
```

Command type

Operation management command

Note

- When the system is restarted without saving the information of running-config into startup-config, the information set in running-config will be lost.
- Be sure to upload the contents of the existing startup-config file to a remote server prior to saving running-config as the contents of startup-config will be overwritten.

Example

Store running-config in startup-config. Then, check the information in startup-config using the show command.

```
xg# copy running-config startup-config
xg# show startup-config
```

5.6.2 show running-config

Function

Displays the configuration information (running-config) currently operating in volatile memory.

Prompt

xg#

Command syntax

```
show running-config
```

Command type

Operation management commands

Example

Display the contents of running-config.

```
xg# show running-config
```

5.6.3 show running-config (redirect)

Function

Copies the configuration information (running-config) in the currently operating volatile memory to the volatile memory. Also, it can be copied directly to a file in the remote server using the "tftp" or "scp" command.

Prompt

xg#

Command syntax

```
show running-config > CONFIG-FILE
show running-config | redirect CONFIG-FILE
```

```
show running-config | { tftp | scp USERNAME } HOST REMOTE-FILE
```

Parameter

- > CONFIG-FILE
  Specifies the file name to copy in the volatile memory.
- | redirect CONFIG-FILE
  Specifies the file name to copy in the volatile memory. It means the same as "> CONFIG-FILE."

> Point
>
> Follow the rules below in specifying file names:
> - File names must start with alphabet ([a - z], [A - Z]).
> - Characters usable for file names are: alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), underscore (_), and period (.)

- | tftp
  Redirects the copy to a file on the TFTP server.
- | scp
  Redirects the copy to a file on the SSH server.
- USERNAME
  Specifies the username of the SSH server.
- HOST
  Specifies the hostname or IP address of the TFTP server or SSH server.
  IP addresses that can be set are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- REMOTE-FILE
  Specifies the file name to copy onto the TFTP server or SSH server.

Command type

Operation management commands

Message

`% tftp: %1$: Host name lookup failure`

Explanation

The specified hostname does not exist.
[[Inserted string]]%1$: specified hostname

Solution

Check whether the specified hostname is correct.

`% tftp: server says: %1$`

Explanation

An error was received from the TFTP server.
[[Inserted string]]%1$: content of error message received from the TFTP server.
The content of message depends on the type of the TFTP server. For example, there is a message as below.

- File not found: There are no files in the TFTP server.
- Access violation: File permission error occurred in the TFTP server.
- Not allowed to overwrite existing files: The file in the TFTP server cannot be overwritten.
- Could not open requested file for reading: There are no files in the TFTP server.
- File already exists: There are files in the TFTP server.
- Unknown transfer ID: Process will be aborted in time out.

Solution

Take actions in accordance with the message received from the TFTP server.

`% tftp: last timeout`

Explanation

There is no response from the TFTP server. There is a possibility of network communication error with the management LAN, or the setting of time out of the TFTP server may be too short.

Solution

Check whether there is no problem in network connection with the TFTP server using the "ping" command. If the problem persists, review the setting of time out of the TFTP server.

% Invalid IP-address.

Explanation

The specified format of the IP address or specified content is incorrect.

Solution

Specify the IP address in a correct format and execute it again.

% Cannot find %1$

Explanation

An incorrect host name was specified.
[[Inserted string]]%1$: Specified host name.

Solution

Specify the correct host name, or specify the IP address.

% The length of user name is invalid.

Explanation

The length of the username is invalid.

Solution

Specify the username 16 or less characters.

lost connection

Explanation

It failed to access to specified SSH server.

Solution

Specify the correct host name, IP address, or username.

No more remote host public key can be registered.

Explanation

Specified remote host public key could not be registered.

Solution

Delete a public key by using "clear ssh-rhost key" command, then execute the command again.

%1$: No such file or directory

Explanation

Specified file does not exist.
[[Inserted string]]%1$: Specified file name.

Solution

Specify the correct file name.

scp: %1$: No such file or directory

Explanation

Specified file does not exist.
[[Inserted string]]%1$: Specified file name.

Solution

Specify the correct file name.

scp: %1$: Permission denied

Explanation

There was no access permission to the SSH server.
[[Inserted string]]%1$: Specified file name.

Solution

Check the access permission to the SSH server.

ssh: connect to host %1$ port 22: No route to host

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: Network is unreachable

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: Connection refused

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: connection timed out

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

%1$: invalid user name

Explanation

Specified username is invalid.
[[Inserted string]]%1$: Specified username.

Solution

Specify the correct username.

% Cannot create output file %1$

Explanation

There is not enough free space to create output file on the device. A temporary file may remain on the device.

Solution

After deleting the files, processed for import, and unnecessary files using the "delete" command, execute the command again.

Note

- When copied in the volatile memory, the information will be lost when the system is restarted. If uploading is necessary, restart the system after storing the data in the TFTP server using the "tftp" command.
- If there are no files in the TFTP server, or directories are specified, an error may occur. (it depends on the functionality of the TFTP server)
- If timeout setting of the TFTP server is too short, an error may occur. (it depends on the functionality of the TFTP server)
- “scp” supports only password authentication, and this device can register up to 10 public keys of SSH servers.
- Execute “clear ssh-rhost-key” command to delete a registered public key.
- A temporary file which form is "show_(number)” is created when “scp” is specified. It may remain on the device when the command is not executed correctly. In this case, use “delete” command to delete the temporary file.

Example

Copy the content of running-config to the file name "run_conf."
Then, upload the copied "run_conf" file with the file name "run_conf_20070122" in the TFTP server called "host1."

```
xg# show running-config > run_conf
xg# tftp put host1 run_conf run_conf_20070122
```

Copy the content of running-config directly to a file in the TFTP server "host1."

```
xg# show running-config | tftp host1 run_conf_20070122
```

Copy the content of running-config directly to a file in the SSH server "host2"

```
xg# show running-config | scp foo host2 run_conf_20080701
host2's password:
```

5.6.4 show startup-config

Function

Displays the configuration information (startup-config) stored in the nonvolatile memory of the device.

Prompt

xg#

Command syntax

```
show startup-config
```

Command type

Operation management commands

Example

Display the content of startup-config.

```
xg# show startup-config
```

5.6.5 show startup-config (redirect)

Function

Copies the startup-config file stored in nonvolatile memory to volatile memory. The configuration file can also be copied directly to a file on a remote server using the "tftp" or “scp” command.

Prompt

xg#

Command syntax

```
show startup-config > CONFIG-FILE
show startup-config| redirect CONFIG-FILE
```

```
show startup-config | { tftp | scp USERNAME } HOST REMOTE-FILE
```

Parameter

- > CONFIG-FILE
  Specifies the file name of the copy to be created in volatile memory.
- | redirect CONFIG-FILE
  Specifies the file name of the copy to be created in volatile memory. It means the same as "> CONFIG-FILE."

> Point
>
> Follow the rules below in specifying file names:
> - File names must start with alphabet ([a - z], [A - Z]).
> - Characters usable for file names are: alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), underscore (_), and period (.)

- | tftp
  Redirects the copy to a file on a TFTP server.
- | scp
  Redirects the copy to a file on the SSH server.
- USERNAME
  Specifies the username of the SSH server.
- HOST
  Specifies the hostname or IP address of the TFTP server or SSH server.
  IP addresses that can be set are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- REMOTE-FILE
  Specifies the file name to copy onto the TFTP server or SSH.

Command type

Operation management commands

Message

% tftp: %1$: Host name lookup failure

Explanation

The specified hostname does not exist.
[[Inserted string]]%1$: specified hostname

Solution

Check whether the specified hostname is correct.

% tftp: server says: %1$

Explanation

An error was received from the TFTP server.
[[Inserted string]]%1$: content of error message received from the TFTP server.
The content of message depends on the type of TFTP server. For example, there is a message as below.

- File not found: There are no files on the TFTP server.
- Access violation: File permission error occurred in the TFTP server.
- Not allowed to overwrite existing files: The file in the TFTP server cannot be overwritten.
- Could not open requested file for reading: There are no files in the TFTP server.
- File already exists: There are files on the TFTP server.
- Unknown transfer ID: Process will be aborted in time out.

Solution

Take actions in accordance with the message(s) received from the TFTP server.

% tftp: last timeout

Explanation

There is no response from the TFTP server. A network communication error with the management LAN occurred, or the time out setting of the TFTP server may be too short.

Solution

Check the network connection with the TFTP server using the "ping" command. If the problem persists, review the time out setting of the TFTP server.

% Invalid IP-address.

Explanation

The specified format of the IP address or specified content is incorrect.

Solution

Specify the IP address in a correct format and execute the command again.

% Cannot find %1$

Explanation

An incorrect host name was specified.

[[Inserted string]]%1$: Specified host name.

Solution

.Specify the correct host name, or specify the IP address.

% The length of user name is invalid.

Explanation

The length of the username is invalid.

Solution

Specify the username 16 or less characters.

lost connection

Explanation

It failed to access to specified SSH server.

Solution

Specify the correct host name, IP address, or username.

No more remote host public key can be registered.

Explanation

Specified remote host public key could not be registered.

Solution

Delete a public key by using "clear ssh-rhost key" command, then execute the command again.

%1$: No such file or directory

Explanation

Specified file does not exist.

[[Inserted string]]%1$: Specified file name.

Solution

Specify the correct file name.

scp: %1$: No such file or directory

Explanation

Specified file does not exist.

[[Inserted string]]%1$: Specified file name.

Solution

Specify the correct file name.

scp: %1$: Permission denied

Explanation

There was no access permission to the SSH server.

[[Inserted string]]%1$: Specified file name.

Solution

Check the access permission to the SSH server..

ssh: connect to host %1$ port 22: No route to host

Explanation

It failed to access to specified SSH server.

[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.

Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: Network is unreachable

Explanation

It failed to access to specified SSH server.

[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.

Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: Connection refused

Explanation

It failed to access to specified SSH server.

[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.

Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: connection timed out

Explanation

It failed to access to specified SSH server.

[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.

Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

```
%1$: invalid user name
```

Explanation

```
Specified username is invalid.
[[Inserted string]]%1$: Specified username.
```

Solution

```
Specify the correct username.
```

```
% Cannot create output file %1$
```

Explanation

```
There is not enough free space to create output file on the device. A temporary file
may remain on the device.
```

Solution

```
After deleting the files, processed for import, and unnecessary files using the "delete"
command, execute the command again.
```

Note

- When copied into volatile memory, the file will be lost when the system is restarted.
  If uploading is necessary, restart the system after storing the data on a TFTP server using the "tftp" command.
- If there are no files on the TFTP server, or directories are not specified, an error may occur depending upon the functionality of the TFTP server.
- If the timeout setting of the TFTP server is too short, an error may occur during transfer.
- “scp” supports only password authentication, and this device can register up to 10 public keys of SSH servers.
- Execute “clear ssh-rhost-key” command to delete a registered public key.
- A temporary file which form is "show_(number)” is created when “scp” is specified. It may remain on the device when the command is not executed correctly. In this case, use “delete” command to delete the temporary file.

Example

Copy the content of running-config to a file named "run_conf."
Then, upload the copied "run_conf" file with the file name "run_conf_20070122" to the TFTP server called "host1."

```
xg# show startup-config > start_conf
xg# tftp put host1 start_conf start_conf_20070122
```

Copy the content of running-config directly to a file on the TFTP server "host1."

```
xg# show startup-config | tftp host1 start_conf_20070122
```

Copy the content of startup-config directly to a file in the SSH server "host2”

```
xg# show startup-config | scp foo host2 start_conf_20080701
host2's password:
```

5.6.6 copy・・・startup-config

Function

Saves the configuration information stored in volatile memory to nonvolatile memory as startup-config. Also, startup-config can be loaded from a remote server using the "tftp" or “scp” command.
After executing this command, it is necessary to restart the system using the "reset" command in order for the new startup-config to take effect.

Prompt

xg#

Command syntax

```
copy local CONFIG-FILE startup-config
copy { tftp | scp USERNAME } HOST REMOTE-FILE startup-config
```

Parameter

- local CONFIG-FILE
  Specifies the file name in volatile memory that data is copied.

> Point
> Follow the rules below in specifying file names:
> – File names must start with alphabet ([a - z], [A - Z]).
> – Characters usable for file names are: alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), underscore (_), and period (.)

- tftp
  Transfers the file stored on the TFTP server.
- scp
  Transfers the file stored on the SSH server.
- USERNAME
  Specifies the username of the SSH server.
- HOST
  Specifies the hostname or IP address of the TFTP server or SSH server for HOST.
  IP addresses that can be set are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- REMOTE-FILE
  Specifies the file name stored on the TFTP server or SSH server.

Command type

Operation management commands

Message

```
% Not found file: %1$
```

Explanation

The specified file cannot be found.
[[Inserted string]]%1$: specified file name

Solution

Check the file name, and execute the command again.

```
% Config-file(header) is invalid: %1$
```

Explanation

The specified file is not in a configuration file format.
[[Inserted string]]%1$: specified file name

Solution

Check the content of the file.

```
% Config-file(version/level) is invalid: %1$
```

Explanation

The configuration file firmware revision does not match the firmware revision installed on the device.
[[Inserted string]]%1$: specified file name

Solution

Check the content of the file.

```
% tftp: %1$: Host name lookup failure
```

Explanation

The specified hostname does not exist.
[[Inserted string]]%1$: specified hostname

Solution

Check whether the specified hostname is correct.

`% tftp: server says: %1$`

Explanation

An error was received from the TFTP server.
[[Inserted string]]%1$: content of error message received from the TFTP server.
The content of message depends on the type of TFTP server. For example:

- File not found: There are no files on the TFTP server.
- Access violation: File permission error occurred on the TFTP server.
- Not allowed to overwrite existing files: The file in the TFTP server cannot be overwritten.
- Could not open requested file for reading: There are no files in the TFTP server.
- File already exists: There are files in the TFTP server.
- Unknown transfer ID: Process will be aborted in time out.

Solution

Take actions in accordance with the message received from the TFTP server.

`% tftp: write: No space left on device`

Explanation

There is no free space for files to use as a work area on the device. Partial copies of the files being imported may remain in the device.

Solution

Delete the files on the device being processed for import, and unnecessary files using the "delete" command, and execute the command again.

`% tftp: last timeout`

Explanation

There is no response from the TFTP server. There is a possibility of network communication error with the management LAN, or the setting of time out of the TFTP server may be too short.

Solution

Check the network connection to the TFTP server using the "ping" command. If the problem persists, review the time out setting of the TFTP server.

`% Invalid IP-address.`

Explanation

The specified format of the IP address or specified content is incorrect.

Solution

Specify the IP address in a correct format and execute the command again.

`% Cannot find %1$`

Explanation

An incorrect host name was specified.
[[Inserted string]]%1$: Specified host name.

Solution

.Specify the correct host name, or specify the IP address.

`% The length of user name is invalid.`

Explanation

The length of the username is invalid.

Solution

Specify the username 16 or less characters.

`No more remote host public key can be registered.`

Explanation

Specified remote host public key could not be registered.

Solution

Delete a public key by using "clear ssh-rhost key" command, then execute the command again.

`scp: %1$: No such file or directory`

Explanation

Specified file does not exist.
[[Inserted string]]%1$: Specified file name.

Solution

Specify the correct file name.

`scp: %1$: Permission denied`

Explanation

There was no access permission to the SSH server.
[[Inserted string]]%1$: Specified file name.

Solution

Check the access permission to the SSH server.

`%1$: No space left on device`

Explanation

This device does not have enough space to copy the file. Incomplete copied file may remain on the device.
[[Inserted string]]%1$: Specified file name.

Solution

Delete incomplete copied file and unnecessary files by using "delete" command, then execute the command again.

`ssh: connect to host %1$ port 22: No route to host`

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

```
ssh: connect to host %1$ port 22: Network is unreachable
```

Explanation

```
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
```

Solution

```
Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network
connection to the SSH server
```

```
ssh: connect to host %1$ port 22: Connection refused
```

Explanation

```
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
```

Solution

```
Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network
connection to the SSH server.
```

```
ssh: connect to host %1$ port 22: connection timed out
```

Explanation

```
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
```

Solution

```
Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network
connection to the SSH server.
```

Note

- The startup-config uploaded using a new version of firmware may not be downloaded with an old version of firmware.
- “scp” supports only password authentication, and this device can register up to 10 public keys of SSH servers.
- Execute “clear ssh-rhost-key” command to delete a registered public key.

Example

Import the "start_conf_20070122" file stored on the TFTP server "host1" with the file name "start_conf."
Then copy the imported "start_conf" file to startup-config.

```
xg# tftp get host1 start_conf_20070122 start_conf
xg# copy local start_conf startup-config
```

Download the "start_conf_20070122" file stored on the TFTP server "host1 directly to startup-config.

```
xg# copy tftp host1 start_conf_20070122 startup-config
```

Download the "start_conf_20080701" file stored on the SSH server "host2 directly to startup-config.

```
xg# copy scp foo host2 start_conf_20080701 startup-config
host2's password:
```

5.6.7 dir/ls

Function

Lists the files in the volatile memory of the device.

Prompt

xg#

Command syntax

```
dir
ls
```

Command type

Operation management commands

Output form

```
xg# dir
  Update-time           File-size  File-name
- 2007/01/22 19:23:03         913  system_info_20070122
- 2007/01/22 19:22:41       2,604  start_conf_20070122
- 2007/01/22 19:22:19       2,655  run_conf_20070122

 unused: 14,639,104 bytes
```

- Update-time
  Displays the file update time.
- File-size
  Displays the file size (byte).
- File-name
  Displays the file name.
- unused
  Displays the size of free memory.

Example

Copy running-config, startup-config and the system information to files in volatile memory, then list the files in volatile memory.

```
xg# show running-config > run_conf_20070122
xg# show startup-config > start_conf_20070122
xg# show system information > system_info_20070122
xg# ls
```

```
  Update-time           File-size  File-name
- 2007/01/22 19:23:03         913  system_info_20070122
- 2007/01/22 19:22:41       2,604  start_conf_20070122
- 2007/01/22 19:22:19       2,655  run_conf_20070122

 unused: 14,639,104 bytes
```

5.6.8 delete

Function

Deletes the files in the volatile memory of the device.

Prompt

xg#

Command syntax

```
delete FILE-NAMES
```

Parameter

- FILE-NAMES
  Specifies the name of the file to delete in the volatile memory.
  Specify a generic designation with "*" (asterisk) for the file name, and files whose "*" part corresponds to the file name of arbitrary strings will be deleted.

Command type

Operation management commands

Message

```
% cannot remove `%1$': No such file or directory
```

Explanation

The specified file does not exist.
[[Inserted string]]%1$: specified file name

Solution

Check whether the specified file name is correct.

Example

Delete a file with the file name "run_conf_20070122".

```
xg# delete run_conf_20070122
```

Specify a generic target for deletion with "run_conf_*". All files whose file name starts with "run_conf_" will be deleted.

```
xg# delete run_conf_*
```

Specify "*" to delete all user files in the volatile memory.

```
xg# delete *
```

5.6.9 rename

Function

Changes the file names in volatile memory.

Prompt

xg#

Command syntax

```
rename FROM-NAME TO-NAME
```

Parameter

- FROM-NAME
  Specifies the file name to change.
- TO-NAME
  Specifies the new file name.

> Point
>
> Follow the rules below in specifying file names:
> - File names must start with alphabet ([a - z], [A - Z]).
> - Characters usable for file names are: alphabet ([a - z], [A - Z]), numerical characters ([0 - 9]), underscore (_), and period (.)

Command type

Operation management commands

Message

```
% unable to rename `%1$': No such file or directory
```

Explanation

The specified file does not exist.
[[Inserted string]]%1$: specified file name

Solution

Check whether the specified file name is correct.

Example

Change a file with the file name "run_conf_20070122" to "run_conf."

```
xg# rename run_conf_20070122 run_conf
```

5.6.10 tftp get

Function

Downloads files on the TFTP server into volatile memory.

Prompt

xg#

Command syntax

```
tftp get HOST REMOTE-FILE [ LOCAL-FILE ]
```

Parameter

- HOST
  Specify the hostname of the TFTP server or IP address.
  IP addresses that can be specified are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- REMOTE-FILE
  Specifies the file name stored on the TFTP server.
- [LOCAL-FILE]
  Specifies the file name to save in volatile memory.
  When this parameter is omitted, the "REMOTE-FILE" file name will be used.

Command type

Operation management commands

Message

% tftp: %1$: Host name lookup failure

Explanation

The specified hostname does not exist.
[[Inserted string]]%1$: specified hostname

Solution

Check whether the specified hostname is correct.

% tftp: server says: %1$

Explanation

An error was received from the TFTP server.
[[Inserted string]]%1$: content of error message received from the TFTP server.
The content of the message depends on the type of TFTP server. For example.

- File not found: There are no files in the TFTP server.
- Access violation: File permission error occurred in the TFTP server.
- Not allowed to overwrite existing files: The file in the TFTP server cannot be overwritten.
- Could not open requested file for reading: There are no files in the TFTP server.
- File already exists: There are files in the TFTP server.
- Unknown transfer ID: Process will be aborted in time out.

Solution

Take actions in accordance with the message received from the TFTP server.

% tftp: write: No space left on device

Explanation

There is not enough free space to store the files on the device. Portion of the files being imported may be present.

Solution

After deleting the files, processed for import, and unnecessary files using the "delete" command, execute the command again.

% tftp: last timeout

Explanation

There is no response from the TFTP server. A network communication error with the management LAN occurred, or the time out setting of the TFTP server may be too short.

Solution

Check the network connection with the TFTP server using the "ping" command. If the problem persists, review the time out setting of the TFTP server.

% local file: No such file or directory

Explanation

The specified file does not exist on the device.

Solution

Check the status of the file on the device.

% Invalid IP-address.

Explanation

The specified format of the IP address or specified content is incorrect.

Solution

Specify the IP address in a correct format and execute the command again.

% Cannot find %1$

Explanation

An incorrect host name was specified.
[[Inserted string]]%1$: Specified host name.

Solution

Specify the correct host name, or specify the IP address.

Example

Copy the file "start_conf_20070122"on the TFTP server "host1", to the device using the file name "start_conf".
Then, check whether the file size of the file imported with the "tftp" command is consistent with the original using the dir/(ls) command.

```
xg# tftp get host1 start_conf_20070122 start_conf
xg# ls
  Update-time          File-size  File-name
- 2007/01/22 19:22:41      2,604  start_conf
```

5.6.11 scp get

Function

Downloads files on the SSH server into volatile memory.

Prompt

xg#

Command syntax

```
scp get USERNAME HOST REMOTE-FILE [ LOCAL-FILE ]
```

Parameter

- USERNAME
  Specifies the username of the SSH server.
- HOST
  Specify the hostname of the SSH server or IP address.
  IP addresses that can be specified are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- REMOTE-FILE
  Specifies the file name stored on the SSH server.
- [LOCAL-FILE]
  Specifies the file name to save in volatile memory.
  When this parameter is omitted, the "REMOTE-FILE" file name will be used.

Command type

Operation management commands

Message

% The length of user name is invalid.

Explanation

The length of the username is invalid.

Solution

Specify the username 16 or less characters.

No more remote host public key can be registered.

Explanation

Specified remote host public key could not be registered.

Solution

Delete a public key by using "clear ssh-rhost key" command, then execute the command again.

scp: %1$: No such file or directory

Explanation

Specified file does not exist.
[[Inserted string]]%1$: Specified file name.

Solution

Specify the correct file name.

scp %1$: Permission denied

Explanation

There was no access permission to the SSH server.
[[Inserted string]]%1$: Specified file name.

Solution

Check the access permission to the SSH server.

%1$: No space left on device

Explanation

This device does not have enough space to copy the file. Incomplete copied file may remain on the device.
[[Inserted string]]%1$: Specified file name.

Solution

Delete incomplete copied file and unnecessary files by using "delete" command, then execute the command again.

ssh: connect to host %1$ port 22: No route to host

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: Network is unreachable

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: Connection refused

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.

ssh: connect to host %1$ port 22: connection timed out

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.

ssh: connect to host %1$ port 22: connection timed out

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

Note

- “scp” supports only password authentication, and this device can register up to 10 public keys of SSH servers.
- Execute “clear ssh-rhost-key” command to delete a registered public key.

Example

Copy the file "start_conf_20080701" on the SSH server "host2", to the device using the file name "start_conf".
Then, check whether the file size of the file imported with the "scp" command is consistent with the original using the dir/(ls) command.

```
xg# scp get foo host2 /tmp/start_conf_20080701 start_conf
host2's password:
xg# ls
  Update-time         File-size  File-name
- 2008/07/01 19:22:41     2,604  start_conf
```

5.6.12 tftp put

Function

Uploads the files in volatile memory to the TFTP server.

Prompt

xg#

Command syntax

```
tftp put HOST LOCAL-FILE [ REMOTE-FILE ]
```

Parameter

- HOST
  Specify the hostname of the TFTP server or IP address.
  IP addresses that can be specified are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- LOCAL-FILE
  Specifies a file name to upload.
- [REMOTE-FILE]
  Specifies the file name to use on the TFTP server.
  When this parameter is omitted, the "LOCAL-FILE" file name will be used.

Command type

Operation management commands

Message

`% tftp: %1$: Host name lookup failure`

Explanation

The specified hostname does not exist.
[[Inserted string]]%1$: specified hostname

Solution

Check whether the specified hostname is correct.

`% tftp: server says: %1$`

Explanation

An error was received from the TFTP server.
[[Inserted string]]%1$: content of error message received from the TFTP server.
The content of the message depends on the type of TFTP server. For example.

- File not found: There are no files in the TFTP server.
- Access violation: File permission error occurred on the TFTP server.
- Not allowed to overwrite existing files: The file on the TFTP server cannot be overwritten.
- Could not open requested file for reading: There are no files in the TFTP server.
- File already exists: There are files on the TFTP server.
- Unknown transfer ID: Process will be aborted in time out.

Solution

Take actions in accordance with the message received from the TFTP server.

`% tftp: last timeout`

Explanation

There is no response from the TFTP server. A network communication error with the management LAN occurred, or the time out setting of the TFTP server may be too short.

Solution

Check the network connection with the TFTP server using the "ping" command. If the problem persists, review the time out setting of the TFTP server.

`% local file: No such file or directory`

Explanation

The specified file does not exist on the device.
[[Inserted string]]%1$: specified file name

Solution

Check the status of the file on the device.

`% Invalid IP-address.`

Explanation

The specified format of the IP address or specified content is incorrect.

Solution

Specify the IP address in a correct format and execute it again.

Note

- If there are no specified files on the TFTP server, or incorrect directories are specified, an error may occur depending upon the functionality of the TFTP server.
- When transferring a file with a large file size, if the time out is set short on the TFTP server, an error may occur.
- In order to check whether the file was transferred successfully, check that the file size displayed by the "dir" or "ls" command is identical to the size of the file on the TFTP server.

Example

Copy the content of running-config to the file name "run_conf."
Then, upload the "run_conf" file to "run_conf_20070122" on the TFTP server called "host1."

```
xg# show running-config > run_conf
xg# tftp put host1 run_conf run_conf_20070122
```

5.6.13 scp put

Function

Uploads the files in volatile memory to the SSH server.

Prompt

xg#

Command syntax

```
scp put USERNAME HOST LOCAL-FILE [ REMOTE-FILE ]
```

Parameter

- USERNAME
  Specifies the username of the SSH server.
- HOST
  Specify the hostname of the SSH server or IP address.
  IP addresses that can be specified are: 1.0.0.1 - 126.255.255.254, 128.0.0.1 - 191.255.255.254, and 192.0.0.1 - 223.255.255.254.
- LOCAL-FILE
  Specifies a file name to upload.
- [REMOTE-FILE]
  Specifies the file name to use on the SSH server.
  When this parameter is omitted, the "LOCAL-FILE" file name will be used.

Command type

Operation management commands

Message

```
% The length of user name is invalid.
```
Explanation
The length of the username is invalid.
Solution
Specify the username 16 or less characters.

```
lost connection
```
Explanation
It failed to access to specified SSH server.
Solution
Specify the host name, IP address, or username.

```
No more remote host public key can be registered.
```
Explanation
Specified remote host public key could not be registered.
Solution
Delete a public key by using "clear ssh-rhost key" command, then execute the command again.

```
%1$: No such file or directory
```
Explanation
Specified file does not exist.
[[Inserted string]]%1$: Specified file name.
Solution
Specify the correct file name.

```
scp: %1$: No such file or directory
```
Explanation
Specified file does not exist.
[[Inserted string]]%1$: Specified file name.
Solution
Specify the correct file name.

```
scp: %1$: Permission denied
```
Explanation
There was no access permission to the SSH server.
[[Inserted string]]%1$: Specified file name.
Solution
Check the access permission to the SSH server.

```
ssh: connect to host %1$ port 22: No route to host
```
Explanation
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
Solution
Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

```
ssh: connect to host %1$ port 22: Network is unreachable
```
Explanation
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
Solution
Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

`ssh: connect to host %1$ port 22: Connection refused`

Explanation

```
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
```

Solution

```
Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network
connection to the SSH server.
```

`%1$: invalid user name`

Explanation

```
Specified username is invalid.
[[Inserted string]]%1$: Specified username.
```

Solution

```
Specify the correct username.
```

`ssh: connect to host %1$ port 22: connection timed out`

Explanation

```
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
```

Solution

```
Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network
connection to the SSH server.
```

Note

- “scp” supports only password authentication, and this device can register up to 10 public keys of SSH servers.
- Execute “clear ssh-rhost-key” command to delete a registered public key.

Example

Copy the content of running-config to the file name "run_conf".
Then, upload the "run_conf" file to "run_conf_20080701" on the SSH server called "host2".

```
xg# show running-config > run_conf
xg# scp put foo host2 run_conf /tmp/run_conf_20080701
host2's password:
```

5.7 Switch Basic Configuration Commands

This section explains configuration commands related to general operation of the switch.

5.7.1 clear bridge mac-address-table

Function

Deletes dynamically-learned MAC addresses from the MAC address table.

Prompt

xg#

Command syntax

```
#clear bridge mac-address-table dynamic { all | port <1-20> | agg-port <1-10> }
```

Parameter

- dynamic { all | port <1-20> | agg-port <1-10> }

  Specifies the port to delete the MAC address.

  - all

    Deletes MAC addresses dynamically-learned at every port.
  - port <1-20>

    Deletes MAC addresses dynamically-learned for a specific port.
  - agg-port <1-10>

    Deletes MAC addresses dynamically-learned for a specific aggregation group.

Command type

Operation management commands

Message

```
% Aggregation-port not bound to bridge
```

Explanation

The specified aggregation group was not created.

Solution

Check whether the specified aggregation group number is correct.

```
% Can't clear port which belongs to an aggregation port
```

Explanation

A port with link aggregation membership cannot be specified and deleted.

Solution

Specify an aggregation group and delete the MAC addresses.

Example

Delete all dynamically-learned MAC addresses.

```
xg# clear bridge mac-address-table dynamic all
```

5.7.2 show bridge

Function

Displays the basic function configuration of the switch.

Prompt

xg> or xg#

Command syntax

```
show bridge
```

Command type

Operation management commands

Output form

```
xg# show bridge
Switch Basic Information                                2007/01/22-12:12:15
=========================================================================
Aging Time                 : {Disabled | <10-1756> } (sec)
Cut-through Switching      : {Disabled | Enabled }
Jumbo Frame Support        : {Disabled | Enabled   Max Frame Size: 9216 (byte) }
Independent-vlan-learning  : {Disabled | Enabled }
DiffServ ToS               : {Disabled | Enabled }
=========================================================================
```

- Aging Time
  Displays the ageing time of the MAC address entries.
  - Disabled
    Aging is disabled.
  - <10-1756> (sec)
    Aging time (the time until a dynamically-learned MAC address expires) is displayed.
- Cut-through Switching
  The switching state is displayed.
  - Disabled
    The switching method is store-and-forward.
  - Enabled
    The switching method is cut-through.
- Jumbo Frame Support
  The jumbo frame support state is displayed.
  - Disabled
    Jumbo frames are not forwarded.
  - Enabled   Max Frame Size
    Displays the maximum size of a jumbo frame that will be forwarded.
- Independent-vlan-learning
  The IVL (Independent Vlan Learning) is displayed.
  - Disabled
    The learning mode is SVL (Shared Vlan Learning).
  - Enabled
    The learning mode is IVL (Independent Vlan Learning).
- DiffServ ToS
  The DiffServ state based on ToS is displayed.
  - Disabled
    DiffServ is disabled.
  - IPv4
    DiffServ of IPv4 is enabled.
  - IPv6
    DiffServ of IPv6 is enabled.

Example

Display the basic function configuration of the switch.

```
xg# show bridge
```

5.7.3 show bridge mac-address-table

Function

Displays the MAC address information registered in the MAC address table.

Prompt

xg> or xg#

Command syntax

```
show bridge mac-address-table [ { static | dynamic | igmp-snooping | port <1-20> | agg-port <1-10> |
  vlan <1-4094> } ]
```

Parameter

- static
  Displays only static MAC addresses.
- dynamic
  Displays only dynamic MAC addresses.
- igmp-snooping
  Displays MAC addresses registered in IGMP snooping.
- port <1-20>
  Specifies the port number of the switch to display.
- agg-port <1-10>
  Specifies the aggregation group number of the switch to display.
- Vlan <1-4094>
  Specifies the vlan number of the switch to display.

When the parameters are omitted, all MAC addresses will be displayed.

Command type

Operation management commands

Output form

```
xg# show bridge mac-address-table
Mac Address Table Information                          2007/01/22-12:12:15
Static Mac-address Table
------------------------------------------------------------------------
Mac-address   Vlan-id  Destination-port
-------------- -------- --------------------
0001.123a.4321 vlan-1   port 2
0002.123a.4321 vlan-1   port 4
0003.123a.4321 vlan-3   filter
ef01.123a.4321 vlan-3   port 1 2 3 4 5 6 7 8

Dynamic Mac-address Table
----------------------------------------------------------------
Mac-address   Vlan-id  Destination-port
-------------- -------- --------------------
0004.123a.4321 vlan-1   port 4

IGMP snooping learning group Mac-address Table
----------------------------------------------------------------
Mac-address    Vlan-id   Destination-port
-------------- --------- -------------------------------------
 (nothing)
================================================================
```

MAC addresses are sorted in the ascending order.

- Mac-address
  The destination MAC address is displayed.
- Vlan-id
  The associated VLAN ID is displayed.
  When the learning mode of the MAC address table is SVL (Shared Vlan Learning), "-------" is displayed.
- Destination-port
  The associated destination port number is displayed.
  - port <1-20>
    The destination port number is shown. For multicast MAC addresses, multiple port numbers are displayed.
  - filter
    The MAC addresses are filtered.

Message

% IGMP snooping is not enabled.

Explanation

Since Global IGMP snooping is disabled, igmp-snooping cannot be specified.

Solution

After enabling IGMP snooping, specify igmp-snooping.

Example

Display the content of all MAC address tables.

```
xg# show bridge mac-address-table
Mac Address Table Information 2007/01/22-12:12:15
===================================================================
Static Mac-address Table
-------------------------------------------------------------------
Mac-address   Vlan-id  Destination-port
-------------- -------- --------------------
0001.123a.4321 vlan-1   port 2
0002.123a.4321 vlan-1   port 4
0003.123a.4321 vlan-3   filter
ef01.123a.4321 vlan-3   port 1 2 3 4 5 6 7 8

Dynamic Mac-address Table
-------------------------------------------------------------------
Mac-address   Vlan-id  Destination-port
-------------- -------- --------------------
0004.123a.4321 vlan-1   port 4

IGMP snooping learning group Mac-address Table
-------------------------------------------------------------------
Mac-address   Vlan-id   Destination-port
-------------- --------- -----------------------------------------
(nothing)
===================================================================
```

By using the "| include" command, output lines which are matched with the parameter will be displayed. Display the information whose MAC address is 0002.123a.4321.

```
xg# show bridge mac-address-table | include port 4
0002.123a.4321 vlan-1   port 4
```

View the MAC address information forwarded to port 4 among static MAC addresses.

```
xg# show bridge mac-address-table static | include port 4
0002.123a.4321 vlan-1   port 4
0004.123a.4321 vlan-1   port 4
```

5.7.4 bridge forward-mode

Function

The device supports two types of frame forwarding, store-and-forward and cut-through.

- Store-and-forward
  After a full frame is received, an error check is performed before forwarding.
- Cut-through
  After reading the first 64 bytes of a received frame, forwarding is immediately performed.
  Basically, FSC errors are not checked, allowing low latency forwarding.
  Use the no form to return to store-and-forward.

Prompt

xg(config)#

Command syntax

```
bridge forward-mode { cut-through | store-and-forward }
no bridge forward-mode
```

Parameter

- forward-mode { cut-through | store-and-forward }
  Specifies the switching method.
  - cut-through
    Specifies Cut-through forwarding.
  - store-and-forward
    Specifies store-and-forward forwarding.

Command type

Configuration command

Default

cut-through

Note

The no form command does not return the forwarding mode to its default setting.

Example

Set the switching method to cut-through.

```
xg(config)# bridge forward-mode cut-through
```

5.7.5 bridge jumbo-frame

Function

Sets the maximum frame size of jumbo frames. The maximum frame size that can be forwarded is 16128 byte.
Use the no form to disable jumbo frame.

Prompt

xg(config)#

Command syntax

```
bridge jumbo-frame [ { 9216 | 12288 | 15360 | 16128 } ]
no bridge jumbo-frame
```

Parameter

- jumbo-frame [{ 9216 | 12288 | 15360 | 16128 }]

  Specifies the maximum frame size of the jumbo frame.

  - 9216

    Sets the permitted jumbo frame size to 9216 byte.
  - 12288

    Sets the permitted jumbo frame size to 12288 byte.
  - 15360

    Sets the permitted jumbo frame size to 15360 byte.
  - 16128

    Sets the permitted jumbo frame size to 16128 byte.

  When this parameter is omitted, 9216 is specified.

Command type

Configuration command

Default

9216

Note

- Forwardable frame sizes

  The following shows the forwardable frame size when jumbo frame forwarding is disabled.

Frame status	Forwardable frame size
VLAN-untagged	1518 bytes
VLAN-tagged	1522 bytes
User VLAN + VLAN-tagged	1526 bytes

When jumbo frame forwarding is permitted, the forwardable frame size will include the additional bytes required for VLAN tagged and user VLAN tagged frames.

Example

Set jumbo frame to permit up to 9216 byte frames.

```
xg(config)# bridge jumbo-frame 9216
```

5.7.6 bridge learn-mode

Function

Sets the MAC address table learning mode.
The device supports two learning modes: SVL (Shared Vlan Learning) and IVL (Independent VLAN Learning).

- SVL (Shared VLAN Learning)
  Regardless of the VLAN of frame ownership, it is learned as a MAC address entry (mapping of MAC address to port) common to every VLAN.
- IVL (Independent VLAN Learning)
  A MAC address entry (mapping of MAC address for port) is learned for each VLAN.

Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
bridge learn-mode { ivl | svl }
no bridge learn-mode
```

Parameter

- learn-mode { ivl | svl }
  Specifies the MAC address table learning mode.
  - ivl
    Specifies IVL (Independent Vlan Learning).
  - svl
    Specifies SVL (Shared Vlan Learning).

Command type

Configuration command

Default

svl

Note

- When changing from SVL to IVL, MAC addresses registered statically in SVL will be registered in VLAN ID 1. Also, when changing from IVL to SVL, MAC addresses registered statically in IVL will be all cleared, except for the ones registered in VLAN ID 1.

Example

This example sets the MAC address table learning mode to IVL (Independent VLAN Learning).

```
xg(config)# bridge learn-mode ivl
```

5.7.7 bridge mac-address-table

Function

By registering static MAC addresses to the MAC address table, frames with specific destination MAC addresses can be forwarded to a specified port.
When a unicast static MAC address is registered, dynamic MAC addresses will not be learned, even when frames sent from the same MAC address are received from a different port. Also, by registering multicast static MAC addresses, frames to be sent to specific multicast nodes can be assigned so that they will be forwarded only to the port specified. In this case, set the multicast forwarding mode to "forward-unregistered-mac" or "filter-unregistered-mac" using the "multicast-forwarding" command.
Use the no form to delete registered static MAC addresses.

Prompt

xg(config)#

Command syntax

```
bridge mac-address-table static MAC [ vlan <1-4094> ] [ port <1-20> [ <1-20> ・・・ ] ]
 [ agg-port <1-10> [ <1-10> ・・・ ] ]
no bridge mac-address-table static MAC [ vlan <1-4094> ]
```

Parameter

- static MAC

  Specifies static MAC addresses. When a frame with this destination address is received, it will be forwarded to the port specified.
  The MAC address format is "HHHH.HHHH.HHHH," a 12-digit hexadecimal number with a period (.) inserted between every four digits.

  Point

  - A unicast MAC address can register the information for only one port in the MAC address table. (As for IVL, one port per VLAN) Therefore, if the same unicast MAC address is already assigned to a different port, the entry will be replaced if the same MAC address and different port are specified in a subsequent “mac-address-table static” command.
  - A multicast MAC address can registered for multiple ports in the MAC address table. If the same multicast MAC address is already set to a port, subsequent assignments of the MAC address to additional ports will be appended to the address table.
  - A broadcast address (FFFF.FFFF.FFFF) can be registered to multiple ports. However, the entry will be replaced with subsequent commands registering non-broadcast addresses to the ports previously assigned.
  - The following reserved multicast addresses, prescribed in IEEE802.1D, cannot be registered.
    - In the range of 0180.C200.0000 - 0180.C200.0010
    - In the range of 0180.C200.0020 - 0180.C200.002F

- vlan <1-4094>

  Specifies a VLAN to register with the MAC address. Specify a VLAN in the range of 1 to 4094. This parameter is valid only when the learning mode of the MAC address table is IVL (Independent Vlan Learning). For SVL (Shared Vlan Learning), this parameter is not necessary.
- port <1-20> [<1-20> ・・・]

  Specifies the port number for the forwarded frame. This parameter is specified in the range of 1 to the maximum number of ports (=20).
  Additionally, when static multicast MAC addresses are registered (including broadcast addresses), multiple ports can be specified by separating the port numbers with a " " (space).
- agg-port <1-10> [<1-10>・・・]

  Specifies the aggregation group number for the forwarded frame. This parameter is specified in the range of 1 to 10.
  Additionally, when static multicast MAC addresses are registered (including broadcast addresses), multiple aggregation groups can be specified by separating the aggregation group numbers with a " " (space).

Command type

Configuration command

Default

Only broadcast address (FFFF.FFFF.FFFF) is registered.

Message

% Unable to translate mac address %1$

Explanation

The specified format of the MAC address is incorrect.
[[Inserted string]]%1$: specified MAC address

Solution

After reviewing the specified format of the MAC address, execute the command again.

% Can't set vlan in case of shared-vlan-learning.

Explanation

When the bridge learn-mode is SVL, VLANs cannot be specified.

Solution

Omit the vlan parameter, and execute the command again.

% Vlan id is not found. vid=%1$

Explanation

The specified VLAN is not created.
[[Inserted string]]%1$: VLAN ID

Solution

Review the vlan specified then execute the command again.

% Port is not vlan member. port %1$ vid=%2$

Explanation

The port is not a member of the specified VLAN.
[[Inserted string]]%1$: port number
[[Inserted string]]%2$: VLAN ID

Solution

Assign the specified port to the intended vlan then execute the command again.

% Aggregation port is not vlan member. agg-port %1$ vid=%2$

Explanation

The specified aggregation group is not a VLAN member.
[[Inserted string]]%1$: port number
[[Inserted string]]%2$: VLAN ID

Solution

Assign the specified aggregation group to the intended vlan then execute the command again.

% Can't set mac-address-table. %1$ vid=%2$

Explanation

The maximum number of table entries was exceeded.
[[Inserted string]]%1$: specified port number
[[Inserted string]]%2$: VLAN ID

Solution

After deleting unnecessary MAC addresses, execute the command again.

% In case of a unicast address, can set only one port.

Explanation

For a unicast MAC address, only one port can be specified.

Solution

After the specified port information then execute the command again.

% port is a member of aggregation group. port %1$

Explanation

A port with link aggregation membership cannot be specified.
[[Inserted string]]%1$: port number

Solution

Specify an aggregation group then execute the command again.

% Aggregation port is not found. agg-port %1$

Explanation

The specified aggregation group does not exist.
[[Inserted string]]%1$: specified aggregation group number

Solution

Review the specified aggregation group number then execute the command again.

% MAC address is reserved by IEEE802.1D %s.

Explanation

MAC addresses reserved under the IEEE802.1D cannot be specified.
[[Inserted string]]%1$: MAC address

Solution

Review the specified MAC address.

% Can't remove mac-address from static forwarding-table.

Explanation

The specified MAC address cannot be deleted.

Solution

Review the specified VLAN or MAC address.

Note

- The maximum number of unicast MAC addresses or multicast MAC addresses that can be statically registered to the device are 128 addresses for each types of address. Additionally, since MAC addresses are managed with a hash table, a message saying an address cannot be registered may be displayed before reaching the maximum number.
- If there is possibility that a multicast group might be received, do not register statically.

Example

The following example shows how to add a static MAC address 0001.2300.4567.

```
xg(config)# bridge mac-address-table static 0001.2300.4567 port 2
```

Register a static MAC address c1b1.123a.4321 belonging to VLAN3. When a frame with this MAC address as its destination is received from VLAN3, it will be forwarded to the specified port.

```
xg(config)# bridge mac-address-table static c1b1.123a.4321 vlan 3 port 4
```

All registered MAC address information can be checked using the show mac address-table command. Combine with the "| include" command, information for a specific MAC address can be output.

```
xg# show bridge mac-address-table static
Static Mac-address Table
--------------------------------------------------------------
Mac-address    Vlan-id  Destination-port
-------------- --------- -------------------------------------
0001.123a.4321 vlan-1   port 2
0002.123a.4321 vlan-1   port 4
0100.5e00.1001 vlan-1   port 1 2 3 4 5 6 7 8
ffff.ffff.ffff vlan-1   port 1 2 3 4 5 6 7 8 9 10 11 12
0003.123a.4321 vlan-2   port 4
ffff.ffff.ffff vlan-2   port 1 2 3 4 5 6 7 8 9 10 11 12

xg# show bridge mac-address-table static | include 0001.123a.4321
0001.123a.4321 vlan-1   port 2
```

5.7.8 bridge mac-address-table filter

Function

By registering a MAC address to filter, a frame with a specific destination MAC address will be discarded.
When filtering of a MAC address is specified, dynamic learning of the MAC address will not be performed, even when frames sent from the same MAC address are received on a different port.
Use the no form to delete the MAC address to filter.

Prompt

xg(config)#

Command syntax

```
bridge mac-address-table static MAC [ vlan <1-4094> ] filter
no bridge mac-address-table static MAC [ vlan <1-4094> ]
```

Parameter

- static MAC
  Specifies the destination MAC address to filter.
  The MAC address format is "HHHH.HHHH.HHHH," a 12-digit hexadecimal number, with a period (.) inserted between every four digits.
- vlan <1-4094>
  Specifies the VLAN to filter. Specify a VLAN in the range of 1 to 4094.
  This parameter is valid only when the learning mode of the MAC address table is IVL (Independent Vlan Learning). For SVL (Shared Vlan Learning), this parameter is not necessary.

Command type

Configuration command

Default

None

Message

% Unable to translate mac address %1$

Explanation

The specified format of the MAC address is incorrect. Broadcast addresses cannot be registered.
[[Inserted string]]%1$: specified MAC address

Solution

After edit the specified format of the MAC address, execute the command again.

% Can't set vlan in case of shared-vlan-learning.

Explanation

When bridge learn-mode is SVL, a VLAN cannot be specified.

Solution

Omit the specified vlan and parameter then execute the command again.

% Vlan id is not found. vid=%1$

Explanation

The specified VLAN does not exist.
[[Inserted string]]%1$: VLAN ID

Solution

Review the specified vlan then execute the command again.

% port is a member of aggregation group. port %1$

Explanation

A port with membership in a link aggregation group cannot be specified.
[[Inserted string]]%1$: port number

Solution

Specify an aggregation group then execute the command again.

% Aggregation port is not found. agg-port %1$

Explanation

The specified aggregation group does not exist.
[[Inserted string]]%1$: specified aggregation group number

Solution

Review the specified aggregation group number then execute the command again.

% MAC address is reserved by IEEE802.1D %s.

Explanation

MAC addresses reserved under the IEEE802.1D cannot be specified.
[[Inserted string]]%1$: MAC address

Solution

Review the specified MAC address.

% Can't set mac-address-table. vid=%1$

Explanation

The maximum number of table entries was exceeded.
[[Inserted string]]%1$: VLAN ID

Solution

After deleting unnecessary MAC addresses, execute the command again.

Note

- The maximum number of unicast MAC addresses or multicast MAC addresses that can be statically registered to the device are 128 addresses for each type of address including filtered addresses also included in these. Additionally, since MAC addresses are managed with a hash table, a message saying an address cannot be registered may be displayed before reaching the maximum number.
- If there is possibility that a multicast group might be received, do not register statically.

Example

The following example filters MAC address 0001.2300.4567.

```
xg(config)# bridge mac-address-table static 0001.2300.4567 filter
```

Filter MAC address c1b1.123a.4321 belonging to VLAN3. Frames, with this MAC address destination are discarded.

```
xg(config)# bridge mac-address-table static c1b1.123a.4321 vlan 3 filter
```

Using the show mac address-table command, filtered MAC address and all registered MAC address information will be displayed. Combined with the "| include" command, information for filtered MAC addresses can be output.

```
xg# show bridge mac-address-table static
```

```
Mac Address Table Information                          2005/06/23-07:18:06
==================================================================
Static Mac-address Table
----------------------------------------------------------------------------
---
Mac-address    Type    Vlan-id  Destination-port
-------------- ------- -------- --------------------
0001.123a.4321 static   vlan-1   port 2
0002.123a.4321 static   vlan-1   port 4
0003.123a.4321 static   vlan-3   filter
ef01.123a.4321 static   vlan-3   port 1 2 3 4 5 6 7 8
==================================================================
```

```
xg# show bridge mac-address-table static | include filter
```

```
0003.123a.4321 static  vlan-3   filter
```

5.7.9 bridge aging-time

Function

Sets the aging time (the remaining time before the MAC address dynamically learned in the MAC address table expires and then is deleted). The aging time is applied to all VLANs.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
bridge aging-time { 0 | <10-1756> }
no bridge aging-time
```

Parameter

- aging-time 0
  Dynamically learned MAC addresses will not expire, and will be permanently retained in the MAC address table.
- aging-time <10-1756>
  Specifies the aging time for a dynamically learned MAC address in seconds. It can be set to a value in the range of 10 to 1756 (seconds).

Command type

Configuration command

Default

300 seconds

Note

- The maximum error between the value of aging time and the time a MAC address actually expires in the device is ±1.7 seconds.

Example

Set the aging time to 400 seconds.

```
xg(config)# bridge aging-time 400
```

Disable the aging time.

```
xg(config)# bridge aging-time 0
```

5.8 Link Aggregation Configuration Commands

This section explains the commands associated with link aggregation.

5.8.1 show link-aggregation

Function

Displays the state of an aggregation group.

Prompt

xg> or xg#

Command syntax

```
show link-aggregation [ agg-port <1-10> ]
```

Parameter

- agg-port <1-10>
  Specifies the aggregation group number. The value can be set in the range of 1 to 10.
  When this parameter is omitted, the state of all aggregation groups will be displayed.

Command type

Operation management commands

Output form (in case of static link aggregation)

```
xg# show link-aggregation
Link Aggregation Information                          2007/01/22-14:30:35
===============================================================================
 System Priority : 32768
 System ID       : 0080.17c2.2144

-------------------------------------------------------------------------------
[agg-port 1]
  Master port                  : port <1-20>
  Management packet send port  : port <1-20>
  Mac address                  : 0080.17c2.2144
  Protocol                     : None
  Distribution algorithm       : { Destination address | Source address
                                 | Destination address & Source address
                                 | Vlan | IP Hash }
                                  { Destination IP | Source IP
                                    | Destination port | Source port }・・・
  Distribution parameter       : <0-3>
  The minimum number of ports  : 1

  [port 1]
    Port Status                : {Active | Inactive }
  [port 2]
    Port Status                : {Active | Inactive }

-------------------------------------------------------------------------------
[agg-port 2]
  ・・・・・・・
  ・・・・・・・
================================================================================
```

Link aggregation group common information
Link aggregation information related to the switch in general will be displayed.

- System Priority
  The system priority used by LACP is displayed.
- System ID
  The identification information used by LACP is displayed.

The state of each aggregation group will be displayed.

[agg-port 1]
Indicates the aggregation group number being displayed.

- Master port
  Displays the master port number of the aggregation group.
  Of the ports belonging to a link aggregation group, the one with the smallest port number will be the master port.
- Management packet send port
  The port number, transmitting the control protocol between switches such as BPDU and IGMP, are displayed.
  Normally, of the ports belonging to an aggregation group, the one with the smallest port number among the ports in a link up state will be the management packet send port.
- Mac address
  Displays the MAC address of the aggregation group. This MAC address will be the same value as that of the master port.

- Protocol
  The control protocol utilized by the link aggregation group is displayed.
  - None
    A static link aggregation group.
  - LACP - Active
    Uses LACP as the control protocol for link aggregation in Active mode.
  - LACP - Passive
    Uses LACP as the control protocol for link aggregation in Passive mode.
- Distribution algorithm
  Displays the distribution method for frame forwarding across the aggregated ports.
  - Destination address
    This is a distribution method based on the destination MAC address of a frame.
  - Source address
    This is a distribution method based on the transmitted frame MAC address.
  - Destination address & Source address
    This is a distribution method based on the information of the destination MAC address of a frame and the transmitted frame MAC address.
  - Vlan
    This is a distribution method based on the VLAN membership of a frame.
  - IP Hash
    This is a distribution method based on the following frame information.
    - Destination IP
      Frames are distributed based on destination IP address.
    - Source IP
      Frames are distributed based on source IP address.
    - Destination port
      Frames are distributed based on destination TCP/UDP port.
    - Source port
      Frames are distributed based on source TCP/UDP port.
- Distribution parameter
  Displays the parameter used to calculate the distribution of frames.
- The minimum number of ports
  Displays the port minimum number of ports that must be in a link up required to maintain a link up state for the aggregation group.

Static link aggregation specific information
The state of each port belonging to a static link aggregation group is then listed.
[port 1]
Indicates the port number being displayed.

- Port Status
  The status of the port is displayed.
  - Active
    The port is usable.
  - Inactive
    The port is not usable.

Output form (in case of LACP link aggregation)

```
xg# show link-aggregation
Link Aggregation Information                          2005/04/24-16:16:36
==============================================================================
System Priority : 32768
System ID       : 0080.17c2.05e2
------------------------------------------------------------------------------
[agg-port 1]
 Master port                 : port <1-20>
 Management packet send port : port <1-20>
 Mac address                 : 0080.17c2.2144
 Protocol                    : { LACP - Active | LACP - Passive }
 Distribution algorithm      : { Destination address | Source address
                               | Destination address & Source address
                               | Vlan | IP Hash }
                                { Destination IP | Source IP
                                  | Destination port | Source port }・・・
 The minimum number of ports : 1

 Actor System Key            : 1
 Partner System Priority     : 32768
 Partner System ID           : 0080.17c2.05e2
 Partner Key                 : 2

[port 1]
 Port Status                 : {Active | Inactive }
 Port Priority               : 32768
 Synchro State               : { Sync | No Sync }
 Receive State               : { Invalid | Initialize | Port Disabled | LACP Disabled| Expired
                               | Defaulted| Current}
 Periodic Tx State           : { Invalid | No Periodic | Fast Periodic | Slow Periodic }
 Actor System Key            : 1
 Partner System Priority     : 32768
 Partner  System ID           : 0080.17c2.05e2
 Partner  Key                 : 2
 Partner Port Priority       : 32768
 Partner Port Number         : 10011
 Partner Synchro State       : { Sync | No Sync }
 [port 2]
 Port Status                  : { Active | Inactive }
 Port Priority                : 32768
 Synchro State                : { Sync | No Sync }
 Receive State                : { Invalid | Initialize | Port Disabled | LACP Disabled | Expired
                               | Defaulted| Current}
 Periodic Tx State            : { No Periodic | Fast Periodic | Slow Periodic }
 Actor System Key            : 1
 Partner System Priority     : 32768
 Partner  System ID           : 0080.17c2.05e2
 Partner  Key                 : 2
 Partner Port Priority        : 32768
 Partner Port Number          : 11
 Partner Synchro State        : { Sync | No Sync }
 [agg-port 2]
  ・・・・・・・
  ・・・・・・・
 ==============================================================================
```

Link aggregation common information
Link aggregation information related to the switch in general will be displayed. The display content is the same as the case of a static link aggregation group.

LACP Link aggregation specific information
Items common to each aggregation group that will be displayed.

- Actor System Key
  The system key used by LACP is displayed.
- Partner System Priority
  LACP system priority will be displayed. This system priority is from the device which is connected by LACP shown in this command.
- Partner System ID
  LACP system ID will be displayed. This system priority is from the device which is connected by LACP shown in this command.
- Partner System Key
  LACP system key will be displayed. This system priority is from the device which is connected by LACP shown in this command.

The state of each port belonging to an LACP link aggregation group is then listed.
[port 1]
Indicates the port number being displayed.

- Port Priority
  The status of the port is displayed.
  - Active
    The port is usable.
  - Inactive
    The port is not usable.

- Synchro State
  The synchronization status of the port is displayed.
  - Sync
    The link state of LACP with the destination device connection is in a synchronized state.
  - No Sync
    The link state of LACP with the destination device connection is not in a synchronized state.
- Receive State
  Displays the reception status of LACP protocol.
  - Invalid
    The LACP port destination device connection is in trouble.
  - Initialize
    The LACP port destination device connection is in initializing.
  - Port Disabled
    The LACP port of the destination device connection is disabled.
  - LACP Disabled
    LACP at the connection destination device is disabled.
  - Expired
    LACP information with for destination device connection expired.
  - Defaulted
    The LACP port of the destination device is about to be connected.
  - Current
    The LACP port of the destination device is an LACP connected state.
- Periodic Tx State
  The state of the LACP transmit interval control frame is displayed.
  - No Periodic
    An LACP control frame will not be sent.
  - Fast Periodic
    LACP control frames are sent at short intervals.
  - Slow Periodic
    LACP control frames are sent at long intervals.
- Partner System Priority
  LACP system priority will be displayed. This system priority is from the device which is connected by a port.
- Partner System ID
  LACP system ID will be displayed. This system priority is from the device which is connected by a port.
- Partner System Key
  LACP system key will be displayed. This system priority is from the device which is connected by a port.
- Partner Port Priority
  The port priority value of the connection's destination device is displayed.
- Partner Port Number
  The port number of the connection's destination device is displayed.
- Partner Synchro State
  The port synchronization status of the connection destination device is displayed.
  - Sync
    The LACP link state is synchronized.
  - No Sync
    The LACP link state is not synchronized.

Note

- In the case of LACP link-aggregation, make sure to confirm “Partner System Priority”, “Partner System ID”, “Partner System Key” .are matched for each port of a LACP aggregation member. If not matched, it is necessary to connect correctly and reissue the command.

Example

Display the state of all aggregation groups.

```
xg> show link-aggregation
```

5.8.2 link-aggregation

Function

Link aggregation is a function wherein multiple ports within a switch act as one logical link (aggregated group). This command is used to set up a link aggregation group.
There are two types of link aggregation: static link and LACP.

- Static link aggregation
  An aggregation group is created statically.
- LACP link aggregation
  An aggregation group in compliance with IEEE802.3ad LACP (Link Aggregation Control Protocol) is created. LACP is a control protocol among switches for dynamically assembling an aggregation group.

Use the no form to delete an aggregation group.

Prompt

xg(config)#

Command syntax

```
link-aggregation agg-port <1-10> [protocol {none | lacp}] [lacp-mode {active | passive}]
[load-balance {dst-mac | src-mac | dst-src-mac | vlan | ip-hash}]
[ distribution-parameter <0-3> ]
[minimum-port <1-10>] port <1-20> <1-20> [ <1-20> ・・・]

no link-aggregation agg-port <1-10>
```

Parameter

- agg-port <1-10>
  Specifies the aggregation group number to create. Specify a number in the range of 1 to 10.
- protocol {none | lacp}
  Specifies the protocol type of the link aggregation.
  - none
    A static link aggregation group.
  - lacp
    A link aggregation group using IEEE802.3ad LACP as the control protocol between switches.

  When this parameter is omitted, "none" is assumed.
- lacp-mode {active | passive}
  Specifies the operational mode of LACP negotiation.
  - active
    Negotiation of LACP is started from the device. Also, since the active mode can receive LACP packets, a connection between two LACP active mode enabled switches is possible.
  - passive
    The device will be in the passive mode of the LACP protocol. The switch responds to LACP packets, but will not start negotiation.

  This parameter can be specified only when "lacp" is specified as the "protocol" parameter.
  When this parameter is omitted, "active" is assumed.
- load-balance { dst-mac | src-mac | dst-src-mac | vlan | ip-hash }
  Specifies the frame distribution method for each port in the aggregation group
  - dst-mac
    Determines the forwarding destination port, based on the destination MAC address of the frames.
  - src-mac
    Determines the forwarding destination port, based on the source MAC address.
  - dst-src-mac
    Determines the forwarding destination port, based on the destination MAC address of a frame and the source MAC address.
  - vlan
    Determines the forwarding destination port, based on VLAN membership.
  - Ip-hash
    Determines the forwarding destination port, based on the IP hash information.

  When this parameter is omitted, "dst-mac" is assumed.

Point

- If there are not many MAC addresses to be distributed across an aggregation group, the distribution among the destination ports tends to become biased. To reduce such bias, use a distribution method that uses more MAC addresses.
  If a server is connected to an aggregation group and a client is connected to a different port, it is recommended that either "src-mac" or "dst-src-mac" be used.
- If the load balancing of frame forwarding is questioned, the traffic state of each port can be checked by using the "monitor traffic-bytes" or the "monitor traffic-counts" commands.

- distribution-parameter <0-3>
  Specifies a parameter used in calculating of frame distribution method.
  When this parameter is omitted, "0" is assumed.

> Point
>
> - Under certain circumstances, load balance bias may not be resolved, when the distribution method is changed. By changing the distribution parameter value, the bias can be minimized.
>   However, this value affects the distribution patterns only. Changing the value does not guarantee resolution of frame distribution bias.

- minimum-port <1-10>
  Specifies the minimum number of ports in a link up state required to maintain the link up state of the aggregation group.
  When the number of ports in a link up state within an aggregation group is less than the minimum number of ports specified, the aggregation group changes to a link down state.
  When this parameter is omitted, 1 is assumed.
- port <1-20> <1-20> [<1-20> ・・・]
  Assigns port numbers to an aggregation group. Separate each port number with a " " (space).
  Specify two or more port numbers.

Command type

Configuration command

Default

None

Message

% agg-port %1$ already exists

Explanation

An aggregation group with the same number already exists.
[[Inserted string]]%1$: specified aggregation group number

Solution

Review the specified aggregation group number, and execute the command again.

% protocol is not LACP

Explanation

Although the protocol specified was not lacp, lacp-mode was specified.

Solution

When the protocol is not lacp, do not specify lacp-mode.

% The maximum number of member ports is 10

Explanation

The number of specified ports was more than 10.

Solution

Set the number of ports to 10 or less.

% port %1$ is already member of aggregation group

Explanation

The specified port already belongs to another aggregation group.
[[Inserted string]]%1$: specified port number

Solution

Specify a port not belonging to any aggregation groups.

% Same port number is found %1$

Explanation

The duplicate port numbers were specified.
[[Inserted string]]%1$: port number duplicated

Solution

Edit the port numbers then execute the command again.

% Minimum-port is too large %1$

Explanation

The number of ports specified in minimum-port surpasses the number of ports constituting the aggregation group.
[[Inserted string]]%1$: specified number of ports

Solution

Specify a minimum-port value equal to or less than the total number of ports within the aggregation group. Then execute the command again.

% port %1$ is membership of uplink-domain %2$.

Explanation

The specified port already belongs to an uplink domain.
[[Inserted string]]%1$: specified port number
[[Inserted string]]%2$: uplink domain number

Solution

Specify a port not belonging to any uplink domains. Or remove the port from an uplink domain.

Note

- Among the ports belonging to an aggregation group, the port with the smallest port number will be the master port. Ports added to an aggregation group immediately after a link aggregation group is initially created will inherit the same settings as that of the master port. The values different from the master port are as follows:
  - "link-pass-through" settings for each appended port will be cleared.
  - The MAC address table entries for each appended port will be cleared.
  - The values for "spanning-tree port-path-cost" will change in accordance with the number of member ports.
- When changing the setting of an aggregation group already created, if the following conditions are met, the aggregation group will change temporarily to a link down state and then to link up again and the port setting becomes default.
  - When the master port is deleted.
  - When the master port is changed.
  - When protocol or lacp-mode parameters are changed.
- A port belonging to an uplink domain cannot be assigned to a link aggregation group.
- Do not specify a port as a member of an aggregation group if the port is monitored by “rx-mirroring-port” or “tx-mirroring-port”.

Example

Set up a static link aggregation group with ports 1 and 2 as aggregation group number 1.
Then move to the interface edit mode of the aggregation group, and assign a VLAN ID of 2.

```
xg(config)# link-aggregation agg-port 1 protocol none port 1 2
xg(config)# interface agg-port 1
xg(config-agg)# port-vlan-id vlan 2
```

Set up an LACP link aggregation group of LACP with ports 3, 4, and 5 as aggregation group number 2.

- Port Members : 3, 4, 5
- LACP mode : active
- Distribution method : distribution by destination MAC
- Link up condition minimum number of ports: 2

```
xg(config)# link-aggregation agg-port 2 protocol lacp lacp-mode active
load-balance dst-mac minimum-port 2 port 3 4 5
```

5.8.3 lacp system-priority

Function

Sets the system priority used by LACP.
The system priority is used as information for identifying switches via LACP. Typically, it is not necessary to change its value from the default.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
lacp system-priority <1-65535>
no lacp system-priority
```

Parameter

- system-priority <1-65535>
  Assigns the LACP system priority value in the range of 1 to 65535.

Command type

Configuration command

Default

32768

Example

Set the LACP system priority to 10000.

```
xg(config)# lacp system-priority 10000
```

5.8.4 lacp port-priority

Function

Sets the priority of LACP ports.
The LACP port priority is used as information for identifying ports via LACP. Typically, it is not necessary to change its value from the default.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
lacp port-priority port <1-20> priority <1-65535>
no lacp port-priority port <1-20>
```

Parameter

- port <1-20>
  Specifies a port number in the range of 1 to 20 to assign an LACP port priority.
- priority <1-65535>
  Specifies an LACP port priority value in the range of 1 to 65535.

Command type

Configuration command

Default

32768

Example

Set LACP port priority to 10000 for Port 2.

```
xg(config)# lacp port-priority port 2 priority 10000
```

5.8.5 link-aggregation load-balance ip-hash-selection

Function

Set the parameter(s) used by the link aggregation IP hash frame distribution function.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
link-aggregation load-balance ip-hash-selection {src-ip | dst-ip | src-port |
dst-port}
no link-aggregation load-balance ip-hash-selection
```

Parameter

- ip-hash-selection {src-ip | dst-ip | src-port | dst-port}
  Specifies the IP hash parameter used for frame distribution function within a link aggregation group. These parameters can be combined.
  src-ip
  Frames are distributed based on source IP address.
  dst-ip
  Frames are distributed based on destination IP address.
  src-port
  Frames are distributed based on TCP/UDP source port number.
  dst-port
  Frames are distributed based on TCP/UDP destination port number.

Command type

Configuration command

Default

src-ip

Message

```
% Cannot set same IP-Hash method.
```

Explanation

Parameters are duplicated.

Solution

Set non-duplicate parameters.

Example

Specifies destination IP address for the IP hash frame distribution function.

```
xg(config)# link-aggregation load-balance ip-hash-selection src-ip
```

5.9 Uplink Filter Commands

This section explains the commands related to uplink filter configuration.

5.9.1 show uplink

Function

Display the configuration of uplink domains and the state of downlink member ports.

Prompt

xg>, or xg#

Command syntax

```
show uplink
```

Command Type

Operation management command

Output form

```
xg(config)# show uplink
Uplink Domain Information                                          2006/03/17-14:35:25
================================================================================
Domain Port-Function    Ports-Membership
------ ---------------- -------------------------------------------------------
     1 Uplink(Active)   port 1 10 11
       Uplink(Inactive) port 2
       Downlink         port 5 6
                        agg-port 2 3
     2 Uplink(Active)   port 3 4
       Uplink(Inactive) None
       Downlink         port 5
                         agg-port 2
================================================================================
```

- Domain
  The domain ID of the uplink group is displayed.
- Port-Function
  The port state belonging to the uplink domain is displayed.

Display	Meaning
Uplink(Active)	Defined Uplink port and link status is good.
Uplink(Inactive)	Defined Uplink port and is NOT working. When the port becomes active, the port status will change.
Downlink	Describes the member of downlink ports.

- Port-Membership
  Display the port membership of the uplink domain.

Example

Display the uplink domain configuration.

```
xg# show uplink
```

5.9.2 uplink-domain

Function

Create an uplink domain and assign member uplink ports.
Use the no form to release the domain membership.

Prompt

xg(config)#

Command syntax

```
uplink-domain <1-20> port <1-20> [ <1-20> ・・・ ]
no uplink-domain <1-20>
```

Parameter

- uplink-domain <1-20>
  Specify a domain ID. The domain ID can be an integer of 1 to 20.
- port <1-20> [<1-20> ・・・]
  Register or delete member uplink ports.
  When specifying multiple ports, list them separated with " "(space).

Command type

Configuration command

Default

None

Message

```
% STP is enabled on uplink port. port %1$
```

Explanation

Uplink port assignments are not allowed for ports with STP enabled.
[[Inserted string]]%1$:port number

Solution

After disabling STP or configuring the port as portfast, execute the command again.

```
% port %1$ is member of aggregation-group.
```

Explanation

Uplink port assignments are not allowed for aggregation ports.
[[Inserted string]]%1$:port number

Solution

After releasing the ports from the aggregation group, execute the command again.

```
% port %1$ is included another uplink-domain.
```

Explanation

This uplink port is already a member of another uplink domain.
[[Inserted string]]%1$:port number

Solution

After releasing the uplink domain that includes the specified port, execute the command again.

```
% port %1$ is already downlink port in same uplink-domain.
```

Explanation

This port is a member of the downlink.
[[Inserted string]]%1$:port number

Solution

After releasing the member from the downlink, execute the command again.

```
% IGMP snooping is enabled.
```

Explanation

IGMP snooping is enabled.

Solution

After disabling IGMP snooping, execute the command again.

Note

- Use this function only for ports to be configured after STP is disabled or portfast is enabled.
- The member of an uplink domain is not permitted to be a member of an aggregation group.
- When releasing an uplink domain using the no form, the members of downlink are also released.
- IGMP snooping and the uplink function cannot be used at the same time. Execute "no ip snooping protocol igmp" command before configuring an uplink domain.

Example

The following is an example of configuring port 3 and 4 as uplink ports of domain 3, and then, displaying the uplink domain information by using "show" command.

```
xg(config)# uplink-domain 3 port 3 4
xg# show uplink
Uplink Domain Information                                   2006/03/17-14:35:25
===============================================================================
Domain Port-Function    Ports-Membership
------ ---------------- -------------------------------------------------------
     3 Uplink(Active)   port 3 4
       Uplink(Inactive) None
       Downlink         None
===============================================================================
```

5.9.3 downlink allowed uplink-domain

Function

Configure the downlink ports belonging to the uplink domain.
Use the no form to release the membership.

Prompt

xg(config-if)#, or xg(config-agg)#

Command syntax

```
downlink allowed uplink-domain { <1-20> | all }
no downlink allowed uplink-domain { <1-20> | all }
```

Parameter

- uplink-domain { <1-20> | all }
  Specify the uplink domain ID for the member downlink ports.
  - <1-20>
    Specify a domain ID. The domain ID can be an integer of 1 to 20.
  - all
    Register or delete all uplink domains.

Command type

Configuration command

Default

None

Message

`% Uplink-Domain %1$ is not configured. port %2$`

Explanation
the uplink domain does not exist.
[[Inserted string]]%1$:uplink domain number
[[Inserted string]]%2$:port number

Solution
Create the uplink domain before executing this command.

`% port %1$ is already uplink port in same uplink-domain.`

Explanation
This port is a member of another uplink domain.
[[Inserted string]]%1$:port number

Solution
After releasing the port from the other uplink domain, execute the command again.

Note

- The member of an uplink domain is not allowed to be the member of the corresponding downlink.
- Aggregation groups can be assigned as a member of downlink.
- If adding ports that are members of an aggregation group all port members of the aggregation group will automatically be made members of downlink.
- When removing ports from an aggregation group that are also members of downlink, downlink membership does not automatically change.

Example

The following is an example of configuring port 3 as a member of uplink domain 1 and register port 4 as a downlink member of domain 1 then display the uplink domain information by using "show" command.

```
xg(config)# uplink-domain 1 port 3
xg(config)# interface port 4
xg(config-if)# downlink allowed uplink-domain 1
xg(config-if)# exit
xg(config)# exit
xg# show uplink
Uplink Domain Information                                  2006/03/17-14:35:25
===============================================================================
Domain Port-Function    Ports-Membership
------ ---------------- -------------------------------------------------------
     1 Uplink(Active)    port 3
       Uplink(Inactive) None
       Downlink         port 4
===============================================================================
```

5.10 Switch Port Configuration Commands

This section explains the port specific commands of the switch.

5.10.1 show interface

Function

Displays the port state of the specified switch.

Prompt

xg> or xg#

Command syntax

```
show interface [ { port <1-20> | agg-port <1-10> } ]
```

Parameter

- port <1-20>
  Specifies the port number of the switch to display.
- agg-port <1-10>
  Specifies the aggregation group number of the switch to display.

When the "port" parameter or "agg-port" parameter are omitted, the state of all ports will be displayed.

Command type

Operation management commands

Output form

```
xg# show interface
Interface Information                                2007/01/22-12:12:15
===============================================================================
[port 1]
Generic Information
   Description                 : port_name1
   MAC Address                 : 000C.123a.4321
   Link State                  : { Link-up | Link-down }
     Link Status Detail        : detail information
   STP State                   : { Discard | Learn | Forward }
   Flow Control                : { Disabled | Rx Only | Tx Only | Rx and Tx }
   Address Learning            : { Enabled | Disabled }
   Multicast Forwarding        : { Forward-all | Forward-unregistered-mac
                                     | Filter-unregistered-mac }
   Port Security               : { Shutdown | Restrict | Disabled }
   Storm Control               : { Enabled | Disabled }
   Default Qos Priority        : <0-7>
   Qos Egress Scheduling       : { Strict | DRR | DRR-Strict }
   Qos Bandwidth
     Output Priority 0         : <0-10000>
     Output Priority 1         : <0-10000>
     Output Priority 2         : <0-10000>
     Output Priority 3         : <0-10000>
   Ingress Bandwidth           : <40-10000> (total:<400-100000>)

Vlan Information
   Port Default Vlan ID         : <1-4094>
   Vlan Member(tagged frame)    : { None | Vlan-1 Vlan-2 ・・・}
   Vlan Member(untagged frame)  : { None | Vlan-1 Vlan-2 ・・・}
   User Vlan Protocol ID        : <0x05DD ~ 0xFFFF>
Filter Information
   Ingress Filter(no vlan member): {Disabled | Enabled}
   Ingress Filter(tagged frame)  : {Disabled | Enabled}
   Ingress Filter(untagged frame): {Disabled | Enabled}
-------------------------------------------------------------------------------
[port 2]
   ・・・・・・・
   ・・・・・・・
===============================================================================
```

The configuration and status of each switch port will be displayed.

[port 1]
The number of the switch port for the following information is displayed.
In the case of an aggregation group, the aggregation group number such as [agg-port 1] is displayed.

Generic Information

- Description
  Port description is displayed.
- MAC Address
  The MAC address of the port is displayed.
- Link State
  - Link-up
    Shows the port is in a link down state.
  - Link-down
    Shows the port is in a link up state.

- Link Status Detail
  Details of the port are displayed:

Display	Meaning
PLUG-OUT	The XFP is not installed.
LOW-PWR	The XFP is in low power state.
PHY	Access to the XFP failed.
CLI	The shutdown command was executed.
TMR	Since the shutdown command and link-aggregation command were executed, the port is down for a certain period of time.
AGG-MIN	The number of ports in a link up state comprising an aggregation group became less than the minimum number of ports required to maintain a link up state.
LF	A local fault was detected.
RF	A remote fault was detected.
LPT	A link down state notification through the link pass through function occurred.
SDL	Frame discarding due to broadcast storm control was detected.
PSL	Frame discarding due to a port security violation was detected.
LAL	Frame discarding due to a loop back alert was detected.
SYS	An internal system contradiction was detected.

- STP State
  - Disabled
    The port is in a state to discard data traffic.
  - Learn
    The port is in the learning state. It prepares for forwarding data traffic. It discards data traffic.
  - Forward
    The port is ready to transmit data traffic.
- Flow Control
  - Disabled
    PAUSE flow control is disabled.
  - Rx Only
    Rx PAUSE flow control is enabled.
  - Tx Only
    Tx PAUSE flow control is enabled.
  - Rx and TX
    Rx and Tx PAUSE flow control is enabled.
- Address Learning
  - Enabled
    Dynamic MAC address learning is enabled.
  - Disabled
    Dynamic MAC address learning is disabled.
- Multicast Forwarding
  - Forward-all
    All multicast frames will be forwarded (flooded).
  - Forward-unregistered-mac
    Multicast addresses yet to be registered in the static MAC address table, and multicast addresses registered will be forwarded (flooded).
  - Filter-unregistered-mac
    Only Multicast addresses registered in the static MAC address table will be forwarded.
- Port Security
  - Shutdown
    When a violating frame is detected, the port enters a violation state and goes link down.
  - Restrict
    When a violating frame is detected, the port enters a violation state, and the violating frame is discarded.
  - Disabled
    Port security is disabled.
- Storm Control
  - Enabled
    Broadcast storm control is enabled.
  - Disabled
    Broadcast storm control is disabled.
- Default Qos Priority
  The QoS priority <0-7> is displayed.
- Qos Egress Scheduling
  - Strict
    Forwarding is scheduled using strict priority.
  - DRR
    Forwarding is scheduled using round robin.
  - DRR-Strict
    Forwarding is scheduled using both strict priority and round robin.
- Qos Bandwidth
  Bandwidth for each output queue priority is displayed
- Ingress Bandwidth
  The ingress rate limiting value of the port is displayed in Mbps.
  For an aggregation group, the ingress rate limiting value total "(total:<240-60000>)," is displayed.

Vlan Information

- Port Default Vlan ID
  The default VLAN ID of the port is displayed.
- Vlan Member (tagged frame)
  Registered VLAN membership (tagged), is displayed.
  If not registered as a VLAN member (tagged), "None" is displayed.
- Vlan Member (untagged frame)
  Registered VLAN membership (untagged), is displayed.
  If not registered as a VLAN member (untagged), "None" is displayed.
- User Vlan Protocol ID
  User defined VLAN protocol identifier (User VLAN Protocol ID) is displayed as a hexadecimal value starting with 0x.

Filter Information

- Ingress Filter (no vlan member)
  The state of ingress filtering by VLAN ID is displayed.
  - Disabled
    The ingress filtering by VLAN ID is disabled.
  - Enabled
    The ingress filtering by VLAN ID is enabled.
    Discards frames with VLAN ID that are not members, when received.
- Ingress Filter (tagged frame)
  The state of ingress filtering of a tagged frame is displayed.
  - Disabled
    The ingress filtering of a tagged frame is disabled.
  - Enabled
    The ingress filtering of a tagged frame is enabled.
    Discards tagged frames when received.
- Ingress Filter (untagged frame)
  The state of ingress filtering of an untagged frame is displayed.
  - Disabled
    The ingress filtering of an untagged frame is disabled.
  - Enabled
    The ingress filtering of an untagged frame is enabled.
    Discards untagged frames when they received.

Example

Display the state of the switch port 3.

```
xg> show interface port 3
```

5.10.2 show port-description

Function

Displays information about port description.

Prompt

xg> or xg#

Command syntax

```
show port-description
```

Command type

Operation management commands.

Output form

```
xg# show port-description
Port Description Information                                      2007/05/10-17:50:54
=================================================================================
[agg-port 1]
 Description: agg_name1
[agg-port 2]
 Description: agg_name2
[port 1]
 Description: port_nam1
[port 2]
 Description: port_name2
[port 3]
 Description: port_name3
=================================================================================
```

[port 1]

The number of the switch port for the following information is displayed.
In the case of an aggregation group, the aggregation group number such as [agg-port 1] is displayed.

- Description

  Port description is displayed

Example

Display the list of port description.

```
xg> show port-description
```

5.10.3 shutdown (Administrator exec mode)

Function

Shuts down the port of a switch from the administrator exec mode, and turns off the optical signal at the XFP.
Use the no form to enable the port again.

Prompt

xg#

Command syntax

```
shutdown port <1-20> [ <1-20> ] ・・・
no shutdown port <1-20> [ <1-20> ・・・]
```

Parameter

- port <1-20> [<1-20>]・・・
  Specifies the port number to shut down or enable.
  When specifying multiple port numbers, list them separated with " " (space).

Command type

Operation management commands

Example

Shut down switch ports 3 and 4. Then, make them usable again.

```
xg# shutdown port 3 4
xg# no shutdown port 3 4
```

5.10.4 clear violation

Function

When a violation due to port security, loop back alert, and broadcast storm control is detected, an error log entry for the violation is output only once, and the target port will be set to a violation state. Violations can be checked with the "Link Status Detail" displayed by the "show interface" command.
By using this command, the violation state of the port will be cleared.
If a violation state occurs, execute this command after eliminating the cause of the violation. If the cause of the violation is not fully eliminated, the violation state will recur.

Prompt

xg#

Command syntax

```
clear violation { all | port <1-20> | agg-port <1-10> }
```

Parameter

- all
  Clears the violation state of all ports.
- port <1-20>
  Specifies the port to be cleared.
- agg-port <1-10>
  Specifies the aggregation group number to be cleared.

Command type

Operation management commands

Example

Clear the violation state of all ports.

```
xg# clear violation all
```

5.10.5 interface port

Function

Switches from the global configuration mode to the interface edit mode wherein ports are configured.
Multiple ports can be configured collectively.

Prompt

xg(config)#

Command syntax

```
interface port <1-20> [ <1-20> ] ・・・
interface port range <1-20> <1-20>

interface agg-port <1-10>
```

Parameter

- port <1-20> [<1-20>] ・・・
  Specifies the port to configure. When specifying multiple ports, list them separated with " " (space).
- port range <1-20> <1-20>
  Specifies the range of multiple ports to configure by separating with " " (space).
- agg-port <1-10>
  Specifies the aggregation group number to configure. Multiple aggregation groups cannot be specified.

Command type

Configuration command

Message

```
% duplicate port number: %1$
```

Explanation

The specified port number was duplicated.
[[Inserted string]]%1$: specified switch port number

Solution

Specify a switch unique port numbers.

Note

- When multiple ports are collectively configured, their settings are individually displayed when using such commands as "copy running-config startup-config" or "show running-config".

Example

Switch to the collective interface edit mode using port numbers in the range of 1 to 8.

```
xg(config)# interface port range 1 8
xg(config-if)#
```

Switch to the collective interface edit mode using port numbers 1, 3, 5, and 7.

```
xg(config)# interface port 1 3 5 7
xg(config-if)#
```

Switch to the interface edit mode using aggregation group number 1.

```
xg(config)# interface agg-port 1
xg(config-agg)#
```

When configuring an aggregation group, the prompt is displayed as (config-agg).

5.10.6 description

Function

Describes the port information.
Use the no form to delete the port description.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
description DESCRIPTION
no description
```

Parameter

- description_DESCRIPTION

  `Describes the port information using ASCII characters. The description can be up to 64 alphanumeric characters in length.`
  `No need to enclose a parameter in quotes if it contains a blank space.`

Command type

Configuration command.

Default

None.

Message

`% Port description length is max over.`

Explanation

`The port description length exceeded 64 characters.`

Solution

`Specify a port description consisting of up to 64 alphanumeric characters.`

Note

Port descriptions are not checked for duplication.

Example

Describes port 3 as “port_name3”.

```
xg(config)# interface port 3
xg(config-if)# description port_name3
```

5.10.7 flowcontrol

Function

Configures PAUSE flow control .
Use the no form to return to the default setup.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
flowcontrol { disable | only-receive | | only-send | send-receive }
no flowcontrol
```

Parameter

- disable
  `Disalbe PAUSE flow control.`
- only-receive
  `Enables Rx PAUSE flow control.`
- only-send
  `Enables Tx PAUSE flow control.`
- send-receive
  `Enables Tx and Rx PAUSE flow control.`

Command type

Configuration command

Default

only-receive

Example

Enable Tx and Rx PAUSE flow control .

```
xg(config-if)# flowcontrol send-receive
```

5.10.8 storm-control

Function

Enables broadcast storm control for the designated ports.
Use the no form to disable storm control.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
storm-control
no storm-control
```

Command type

Configuration command

Default

None

Note

- When a broadcast storm condition is detected, the port will be in a violation state. After eliminating the cause of the condition, clear the violation state with the "clear violation" command.

Example

Enable broadcast storm control for Port 3 of the switch.

```
xg(config)# interface port 3
xg(config-if)# storm-control
```

5.10.9 suppress-address-learning

Function

Disables the dynamic learning of the MAC address table for switch ports.
Use the no form to enable learning.

Prompt

xg(config-if)#, or xg(config-agg)#

Command syntax

```
suppress-address-learning
no suppress-address-learning
```

Command type

Configuration command

Default

None

Example

Disable dynamic learning for the MAC address table.

```
xg(config-if)# suppress-address-learning
```

5.10.10 shutdown (Interface edit mode)

Function

Shuts down the ports so that they cannot be used.
Use the no form to enable the ports again.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
shutdown
no shutdown
```

Command type

Configuration command

Default

None

Note

- When this command is invoked, the port becomes disabled but the optical signal from the XFP is not stopped.

Example

Shut down switch port 3. Then, make it usable again.

```
xg(config)# interface port 3
xg(config-if)# shutdown
xg(config-if)# no shutdown
```

5.10.11 shutdown (Global configuration mode)

Function

Shuts down the ports from the global configuration mode so that they cannot be used.
Use the no form to enable the ports again.

Prompt

xg(config)#

Command syntax

```
shutdown port <1-20> [ <1-20> ] ・・・
no shutdown port <1-20> [ <1-20> ] ・・・
```

Parameter

- port <1-20> [<1-20>] ・・・
  Specifies the port number to shut down or enable.
  When specifying multiple ports, list them separated with " " (space).

Command type

Configuration command

Default

None

Note

- When this command is invoked, the port becomes disabled, but the optical signal from the XFP is not stopped.
- To shut down an aggregation group, use the interface edit mode shutdown command.

Example

Shut down switch ports 3 and 4 then, make them usable again.

```
xg(config)# shutdown port 3 4
xg(config)# no shutdown port 3 4
```

5.10.12 port-security

Function

Sets port security based on the source MAC address.
When port security is enabled, register the MAC addresses permitted using the "bridge mac-address-table" command.
Use the no form to disable port security.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
port-security violation { restrict | shutdown }
no port-security
```

Parameter

- violation { restrict | shutdown }
  Specifies the action when receiving a violating frame.
  - restrict
    When a violating frame is detected an error log entry is recorded, and an SNMP trap message is sent.
    The violating frame is discarded, and the port set to a violation state.
  - shutdown
    When a violating frame is detected an error log entry is recorded, and an SNMP trap message is sent.
    The port is set to a violation state then goes link down.

Command type

Configuration command

Default

None

Note

- When a security violation is detected, the port is set to a in violation state. The "Link Status Detail" of the "show interface" command will display "PSL".
  After eliminating the cause of the violation, clear the violation state with the "clear violation" command to return the port to usable state.
- When port security is enabled, throughput decreases by about 10%, since the forwarding overhead increases. Also, receiving a frame that causes a security violation affects transmission from the port. Therefore, in an environment where security violations occur frequently, a decrease in the transmission rate should be anticipated.

Example

Set port security to switch port 3.
Then, when port 3 is in violation, check the port state using the "show interface" command.
After eliminating the cause of violation, make it usable again using the "clear violation" command.

```
xg(config)# interface port 3
xg(config-if)# port-security violation shutdown
xg(config-if)#exit
xg(config)#exit
      -        ← When the port is in violation state.
xg#show interface port 3
      -        ← When link Status Detail is "PSL."
xg# clear violation port 3
```

5.10.13 link-pass-through

Function

Link pass through is a function that monitors the link state of a specific port, and, by synchronizing the link state of the specified port, promptly notifies changes of the link state to devices connected to the notification (domino) port.
This command specifies the link state monitoring port and the notification port.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
link-pass-through { monitored-port <1-20> | monitored-agg-port <1-10>}
[domino-port <1-20> [<1-20> ・・・]] [domino-agg-port <1-10> [<1-10> ・・・]]

no link-pass-through { monitored-port <1-20> | monitored-agg-port <1-10>}
```

Parameter

- monitored-port <1-20>
  Specifies a port to monitor the link state.
- monitored-agg-port <1-10>
  Specifies an aggregation group to monitor the link state.
- domino-port <1-20> [<1-20> ・・・]
  Specifies the port number for the link state notification.
  When specifying multiple port numbers, list them separated with " " (space).
- domino-agg-port <1-10> [<1-10> ・・・]
  Specifies the aggregation group number for the link state notification.
  When specifying multiple aggregation group numbers, list them separated with " " (space).

Command type

Configuration command

Default

None

Message

% Agg-port %1$ does not exist.

Explanation

The specified aggregation group is not created.
[[Inserted string]]%1$: specified aggregation group number

Solution

Review the specified aggregation group numbers.

% monitored-port and domino-port cannot specify a port belonging to an aggregation port. port=%d

Explanation

Ports within a link aggregation group cannot be specified as monitored and domino ports.
[[Inserted string]]%1$: port number specified to monitored-port or domino-port

Solution

Review the ports specified as monitored and domino ports.

% Cannot set same port number in monitored-port and domino-port. port %1$

Explanation

The same port number cannot be set to a monitored port and a domino port.
[[Inserted string]]%1$: port number

Solution

Review the parameter specified for the monitored port or domino port.

% Cannot set same aggregation port number in monitored-agg-port and domino-agg-port. agg-port %1$

Explanation

The same aggregation group number cannot be set to a monitored port and a domino agg-port.
[[Inserted string]]%1$: aggregation group number

Solution

Review the parameters specified for the monitored port or domino agg-port.

% Cannot set same port number in domino-port. port %1$

Explanation

The same port number cannot be set as the domino port.
[[Inserted string]]%1$: port number

Solution

Review the parameter specified for the domino port.

% Cannot set same aggregation port number in domino-agg-port. agg-port %1$

Explanation

The same aggregation group number cannot be set as the domino agg-port.
[[Inserted string]]%1$: aggregation group number

Solution

Review the parameter specified for the domino agg-port.

Example

Monitor the link state of aggregation group 1 and set ports 4 and 5 to receive link state notification.

```
xg(config)# link-pass-through monitored-agg-port 1 domino-port 4 5
```

5.10.14 ingress-bandwidth

Function

Sets the ingress rate limiting value for the designated ports.
When reception traffic exceeds the ingress rate limiting value, received frames will be discarded.
Use the no form to return to the default setup.

Prompt

xg(config)# or xg(config-agg)#

Command syntax

```
ingress-bandwidth <40-10000>
no ingress-bandwidth
```

Parameter

- <40-10000>
  Specifies the ingress rate limiting value in the range of 40 to 10000 Mbps. The value must be an integer divisible by 40.
  For an aggregation group, the specified ingress rate limiting value applies to each port comprising the aggregation group. The total ingress rate limiting value for the aggregation group will be the specified ingress rate limiting value multiplied by the number of ports.

Command type

Configuration command

Default

10000

Message

% The set value is not step of 40.

Explanation

The specified ingress rate limiting value is not an integer divisible by 40.

Solution

Specify the ingress rate limiting value with an integer divisible by 40.

Note

- For the specified ingress rate limiting value x, the actual ingress rate limiting value used is expressed in the approximation below.
  Actual ingress rate limiting value = {integral part of (rate × 256 / 10000)} × 10000 / 256
- Measurement of the ingress rate is done in increments of 100μs. Therefore, when burst transfers are performed that exceed 100μs, the actual permitted ingress rate will be smaller than the specified value.

Example

Set the ingress rate of port 3 to 5Gbps.

```
xg(config)# interface port 3
xg(config-if)# ingress-bandwidth 5000
```

5.10.15 multicast-forwarding

Function

Sets the forwarding method for multicast frames.
Use the no form to return to the default setup.

Prompt

xg(config)# or xg(config-agg)#

Command syntax

```
multicast-forwarding { forward-all | forward-unregistered-mac |
filter-unregistered-mac }
no multicast-forwarding
```

Parameter

- { forward-all | forward-unregistered-mac | filter-unregistered-mac }
  Specifies the forwarding method for multicast frames.
  - Forward-all
    All multicast frames will be forwarded (flooded).
  - Forward-unregistered-mac
    Multicast addresses yet to be registered in the static MAC address table, and multicast addresses registered will be forwarded (flooded). Multicast addresses registered as non-member ports will be filtered.
  - Filter-unregistered-mac
    Only Multicast addresses registered as member ports in the static MAC address table will be forwarded.

Command type

Configuration command

Default

forward-all

Example

Enter the interface edit mode using switch ports 1 to 3, then set them to the unregistered multicast forwarding mode.

```
xg(config)# interface port range 1 3
xg(config-if)# multicast-forwarding forward-unregistered-mac
```

5.11 Spanning Tree Protocol (STP) Configuration Commands

This section explains the commands related to the Spanning Tree Protocol.

5.11.1 show spanning-tree

Function

Displays the state of the Spanning Tree Protocol.

Prompt

xg> or xg#

Command syntax

```
show spanning-tree [ detail [ { port <1-20> | agg-port <1-10> } ] ]
```

Parameter

- detail
  `Displays the state of the Spanning Tree Protocol configuration in detail.`
  `When this parameter is omitted, the display will be simplified.`
- port <1-20>
  `Specifies the ports to display.`
- agg-port <1-10>
  `Specifies the aggregation groups to display.`

When "port" parameter and "agg-port" parameter are omitted, the state of all ports will be displayed.

Command type

Operation management commands

Output form (simplified display)

```
xg# show spanning-tree
Spanning Tree Information                             2007/01/22-12:12:15
===============================================================================
Switch Information for Spanning Tree
 -------------------------------------------------------------
  Spanning Tree       : {Enabled | Disabled}
  Root Switch Priority: 32768
  Root Switch ID      : 8000.0080.17C2.0511
  Root Path Cost      : 0
  Root Port           : port1
  Switch Priority     : 32768
  Switch ID           : 8001.0080.17C2.0512
  Max Age             : 20 (sec)
  Hello Time          :  2 (sec)
  Forward Time        : 15 (sec)
  Topology Changes    : 0
  Last Topology Change: 2007/01/22-12:12:15
  portfast errdisable : {enabled | disabled}
  timeout
  portfast errdisable : 300 sec
  timeout interval
-----------------------------------------------------------------
Ports Information for Spanning Tree
-----------------------------------------------------------------
  Port State      Mode Cost  Pri  PortID  Flags  Designated Switch
  ---- ---------- ---- ----  ---  ------  ------ -------------------
     1  Forward    RSTP 2000 128  32769   Rpp-w  8000.0080.17C2.0511
     2  Discard    RSTP 2000 128  32770   Bpp-w  8000.0080.17C2.0511
     3  Learn      RSTP 2000 128  32771   Bpp-w  8001.0080.17C2.0512
     4  Forward    RSTP 2000 128  32772   Dpp--  8001.0080.17C2.0512
     5  Down      RSTP     0 128  32773   -----  0000.0000.0000.0000
     6  Down      None     0 128  32774   -----  0000.0000.0000.0000
     7  Down      None     0 128  32775   -----  0000.0000.0000.0000
     8  Down      None     0 128  32776   -----  0000.0000.0000.0000
     9  Down      None     0 128  32777   -----  0000.0000.0000.0000
    10  Down      None     0 128  32778   -----  0000.0000.0000.0000
    11  Down      None     0 128  32779   -----  0000.0000.0000.0000
    12  Down      None     0 128  32780   -----  0000.0000.0000.0000
-----------------------------------------------------------------
Flags
1: (Port role)      R=Root, D=Designated, A=Alternate, B=Backup
2: (Config type)    p=Point-to-point, s=Shared
3: (Oper. type)     p=Point-to-point, s=Shared
4: (Proposal state) p=Proposing
5: (Received BPDU)  d=802.1d, w=802.1w
===============================================================================
```

Switch Information for Spanning Tree

General Spanning Tree Protocol information is displayed.

- Spanning Tree
  The operational state of the Spanning Tree Protocol is displayed.
  - Disabled
    Spanning Tree Protocol is disabled.
  - Enabled
    Spanning Tree Protocol is enabled.
- Root Switch Priority
  The priority value for the switch selected as the root switch is displayed as a decimal number.
- Root Switch ID
  The switch identifier selected as the root switch is displayed.
  The first four digits representing the priority of the root switch are displayed as a hexadecimal number.
  The remaining 12 digits representing the MAC address of the root switch are displayed as a hexadecimal number.
- Root Path Cost
  The path cost value from the device to the root switch.
  When the device is the root switch, "0" is displayed.
- Root Port
  The switch port number of the root port of the device is displayed.
  When the device is the root switch, "---" is displayed.
- Switch Priority
  The priority value of the device is displayed as a decimal number.
- Switch ID
  The switch identifier priority for the device is displayed.
  The first four digits representing the priority of the device are displayed as a hexadecimal number.
  The remaining 12 digits representing the MAC address of the device are displayed as a hexadecimal number.
- Max Age
  The maximum valid time (seconds) for BPDU's are displayed.
- Hello Time
  The transmit interval (seconds) for BPDU's are displayed.
- Forward Time
  The time a port requires to switch states.
- Topology Changes
  The number of times the topology changed is displayed.
- Last Topology Change
  The latest date and time the topology change occurred is displayed.
- portfast errdisable timeout
  The state of errdisable-timeout function is displayed.
  - disabled
    The errdisable-timeout function is disabled.
  - enabled
    The errdisable-timeout function is enabled.
- portfast errdisable timeout interval
  The timeout value (seconds) for canceling a port down condition when the errdisable-timeout function is enabled is displayed.

Ports Information for Spanning Tree

The Spanning Tree Protocol information for each switch port is displayed.

- Port
  The switch port number is displayed.
- Port State
  The STP state of the switch port is displayed.
  - Down
    Indicates that the switch port is in link down state.
  - Discard
    The switch port does not send/receive frames other than BPDUs.
  - Learn
    The switch port is in learning state. The source MAC address for received frames is learned, but frames are not forwarded.
  - Forward
    The switch port is ready to transmit data traffic.

For RSTP (IEEE802.1w), "Blocking" and "Listening" states of STP are merged as the "Discarding" State. The port states between STP (IEEE802.1D) and RSTP (IEEE802.1w) correspond as follows:

Display format	STP(IEEE802.1D)	RSTP(IEEE802.1w)
Block	Blocking	Discarding
Listen	Listening	Discarding
Learn	Learning	Learning
Forward	Forwarding	Forwarding

Point

For a switch port that does not use STP, the state will be either "Forward" or "Down."

- Mode
  The switch port mode of the Spanning Tree Protocol is displayed.
  - STP
    The switch port is operating in STP (IEEE 802.1D Spanning Tree Protocol) mode.
  - RSTP
    The switch port is operating in RSTP (IEEE 802.1w Rapid Spanning Tree Protocol) mode.
  - None
    STP is not applicable to the switch port.
- Cost
  The path cost value of the port is displayed.
- Pri
  The priority value of the switch port is displayed.
- PortID
  The port ID of the switch port is displayed.
- Flags
  Flags indicating the state of the switch port are displayed. Each flag has the following meaning:
  - First flag (Port role)
    Indicates the role of the port.
    - R
      The Root port.
    - D
      The Designated port.
    - A
      The Alternate port.
    - B
      The Backup port.
  - Second flag (Config link type)
    Indicates the link type of the line configured in the device.
    - p
      A point-to-point link.
    - s
      A shared line.

    In the device Point-to point "p" is always used.
  - Third flag (Oper link type)
    Indicates the link type in operation.
    - p
      A point-to-point link.
    - s
      A shared link.
  - Fourth flag (Proposal state)
    Indicates a Spanning Tree was proposed by an adjacent switch.
    - p
      Building a Spanning Tree was proposed.
    - (None)
      Building a Spanning Tree request was accepted by the adjacent switch.
  - Fifth flag (Received BPDU)
    The Spanning Tree Protocol mode for the received BPDU.
    - d
      STP(IEEE802.1D).
    - w
      RSTP(IEEE802.1w).

> Point
>
> If the destination switch port is operating in STP (IEEE802.1D) mode, the connected device switch port will operate in STP mode regardless of its setting.

- Designated Switch
  Displays the switch identifier for the specified switch that sent a BPDU to the specified port.
  The first four digits representing the priority of the designated switch are displayed as a hexadecimal number. The remaining 12 digits representing the MAC address of the designated switch are displayed as a hexadecimal number.

Output form (detailed display)

```
xg# show spanning-tree detail
Spanning Tree Information                              2007/01/22-12:12:15
===============================================================================
Switch Information for Spanning Tree
---------------------------------------------------------------
  Spanning Tree       : {Enable | Disable}
  Root Switch Priority: 32768
  Root Switch ID      : 8000.0080.17C2.0511
  Root Path Cost      : 6
  Root Port           : port-1
  Switch Priority     : 32769
  Switch ID           : 8001.0080.17C2.0512
  Max Age             : 20 (sec)
  Hello Time          :  2 (sec)
  Forward Time        : 15 (sec)
  Topology Changes    : 0
  Last Topology Change: 2007/01/22-12:12:15
  portfast errdisable : {enabled | disabled}
  timeout
  portfast errdisable : 300 sec
  timeout interval
----------------------------------------------------------------

Ports Information for Spanning Tree
-----------------------------------------------------------------------------
[Port 1]
  STP State           : {Down | Discard | Learn | Forward }
  STP Mode            : {STP | RSTP | None}
  Port ID             : 32772
  Role                : {Root | Designated | Alternate | Backup}
  Path Cost           : 2
  Link Type           : { Point-to-point | Shared }
  Forward-Transitions : 0
  Portfast            : {Disabled | Enabled}
  Portfast bpdu-guard : {Disabled | Enabled}
  Portfast bpdu-filter: {Disabled | Enabled}

  BPDU Parameter
    Designated Path Cost: 0
    Designated Port ID  : 0
    Designated Priority : 128
    Designated Root ID  : 0000.0000.0000.0000
    Designated Switch ID: 0000.0000.0000.0000
    Max Age             : 20 (sec)
    Message Age         : 0 (sec)
    Message Age Timer   : 0 (sec)
    Hello Time          : 2 (sec)
    Hello Timer         : 0 (sec)
    Forward Time        : 15 (sec)
    Forward Timer       : 0 (sec)
    Received STP Protocol: None

[Port 2]
  . . . . . . . . . . . . . .
-----------------------------------------------------------------------------
=============================================================================
```

Switch Information for Spanning Tree

General Spanning Tree Protocol information is displayed.
The display content is the same as that of the simplified display except for some additional items.

Port Information for Spanning Tree

Spanning Tree Protocol information for each port is displayed.

- [Port 1]
  The switch port number is displayed.
- STP State
  The state of the port is displayed.
  The display content is the same as that of the simplified display.
- STP Mode
  The Spanning Tree Protocol mode is displayed. The display content is the same as that of the simplified display.
- Port ID
  The Port ID of the switch port is displayed.
- Role
  The role of the port is displayed.
  - Root
    The root Port.
  - Designated
    The designated port.
  - Alternate
    The alternate port.
  - Backup
    The backup port.
- Path Cost
  The path cost for the port is displayed.

- Link Type
  Indicates the state of the current link.
  - Point-to-point
    A point-to-point link.
  - Shared
    A shared link.
- Forward-Transitions
  Displays the number of times the port changed to forwarding state.
- Portfast
  The Portfast state is displayed.
  - Disabled
    The Portfast function is disabled.
  - Enabled
    The Portfast function is enabled.
- Portfast bpdu-guard
  The state of the BPDU guard function is displayed.
  - Disabled
    The BPDU guard function is disabled.
  - Enabled
    The BPDU guard function is enabled.
- Portfast bpdu-filter
  The state of the BPDU filter function is displayed.
  - Disabled
    The BPDU filter function is disabled.
  - Enabled
    The BPDU filter function is enabled.

BPDU Parameter

Displays the information about the BPDU send/receive.
This is only displayed when the "STP State" of the specified port is not "Down".

- Designated Path Cost
  The root path cost to the destination port is displayed.
- Designated Port ID
  The Port ID of the destination port is displayed.
- Designated Priority
  The priority value of the destination port is displayed,
- Designated Root ID
  The switch identifier of the root switch registered in the destination switch is displayed. The first four digits representing the priority of the root switch are displayed as a hexadecimal number. The remaining 12 digits representing the MAC address of the root switch are displayed as a hexadecimal number.
- Designated Switch ID
  The switch identifier of the destination switch is displayed.
  The first four digits representing the priority of the designated switch are displayed as a hexadecimal number.
  If the "Designated Root ID" and the "Designated Switch ID" are the same, the destination switch is the root switch.
- Max Age
  The maximum valid time (seconds) for BPDU's for the destination switch is displayed.
- Message Age
  Displays the time (seconds) lapsed since the last BPDU message from the destination switch was received.
- Message Age Timer
  Displays the timeout value (seconds) for BPDU messages sent form the destination switch.
- Hello Time
  Displays the hello time (seconds) sent from the destination switch.
- Hello Timer
  Displays the remaining seconds for the Hello Timer. When it decrements to 0, a BPDU is sent.
- Forward Time
  Displays the Forward Time (seconds) sent from the destination switch.
- Forward Timer
  Displays the remaining seconds for the Forward Timer. When it decrements to 0, the status of the port is changed.
- Received STP Protocol
  Displays the Spanning Tree Protocol (STP) mode of the destination switch.
  - STP
    The connection destination switch is operating in STP (IEEE 802.1D) mode.
  - RSTP
    The connection destination switch is operating in RSTP (IEEE 802.1w) mode.
  - None
    STP is not enabled on the destination switch.

Example

Displays the detailed information for the Spanning Tree Protocol state:

```
xg# show spanning-tree detail
```

5.11.2 spanning-tree

Function

Enables the Spanning Tree Protocol (STP).
Use the no form to disable Spanning Tree Protocol.

Prompt

xg(config)#

Command syntax

```
spanning-tree
no spanning-tree
```

Command type

Configuration command

Default

None

Message

```
% port %1$ is membership of uplink-domain %2$.
```

Explanation

The specified port already belongs to an uplink domain.
[[Inserted string]]%1$: specified port number
[[Inserted string]]%2$: uplink domain number

Solution

Specify a port not belonging to an uplink domain or remove the port from an uplink domain.

Note

- STP cannot be used on uplink ports. STP port fast, however, is allowed on uplink ports.

Example

Enable Spanning Tree Protocol.

```
xg(config)# spanning-tree
```

5.11.3 spanning-tree priority

Function

Sets the switch priority of the Spanning Tree Protocol.
Whichever switch priority is smallest is selected as the root switch for the Spanning Tree.
Use the no form to return to the default state.

Prompt

xg(config)#

Command syntax

```
spanning-tree priority <0-61440>
no spanning-tree priority
```

Parameter

- priority <0-61440>
  Sets the switch priority value. It must be an integer divisible by 4096. Values can be set in the range of 0 to 61440.

Command type

Configuration command.

Default

32768

Message

```
% Priority is not step of 4096
```

Explanation

The priority is not a multiple of 4096.

Solution

Specify an integer divisible by 4096.

Example

Set the switch priority to 4096.

```
xg(config)# spanning-tree priority 4096
```

5.11.4 spanning-tree hello-time

Function

The hello time is a time interval between BPDUs. Periodic BPDUs inform all the other switches on the network of the root switch routing information.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
spanning-tree hello-time <2-10>
no spanning-tree hello-time
```

Parameter

- hello-time <2-10>
  `Specify a hello time in seconds.`

Command type

Configuration command

Default

2 seconds

Message

```
% Can't set hello-time
```

Explanation

`An unsettable value was specified. The settable range of "hello-time" differs depending on the values of "forward-time" and "max-age".`

Solution

`Set a value which satisfies the conditions specified in this Section's Notes.`

Note

- If the hello time is short, topology changes can be detected more quickly, but STP traffic and STP processing overhead will increase.
- The settable range of hello-time differs depending on the values set with the "spanning-tree max-age" command and the "spanning-tree forward-time" command. The value must also satisfy the following conditions:

```
2 × (forward_time - 1) ≥ max_age
max_age ≥ 2 × (hello_time + 1)
```

Example

Set the hello time value of the Spanning Tree switch to 3 seconds.

```
xg(config)# spanning-tree hello-time 3
```

5.11.5 spanning-tree max-age

Function

The maximum age (max-age) of the Spanning Tree is the maximum valid time interval between received BPDUs. When BPDUs are not received within that time, the topology of the Spanning Tree will be recalculated, and the switch that timed out will send BPDUs acting as a root switch.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
spanning-tree max-age <6-40>
no spanning-tree max-age
```

Parameter

- max-age <6-40>
  Sets the timeout value for the received BPDUs. When the switch does not receive BPDUs within this period, the topology of the Spanning Tree will be recalculated. Values can be set in the range of 6 to 40 seconds.

Command type

Configuration command

Default

20 seconds

Message

% Can't set max-age.

Explanation

An unsettable value was specified. The settable range of max-age differs depending on the values of "hello-time" and "forward-time".

Solution

Set a value, which satisfies the conditions as detailed in this Section's Notes.

Note

- The settable range of maximum age differs depending on the value set with the "spanning tree hello-time" command and the "spanning tree forward-time" command. The value must also satisfy the following conditions:

```
2× (forward_time -1) ≥ max_age
max_age ≥ 2 × (hello_time + 1)
```

Example

Specify the maximum age (max-age) value of the Spanning Tree to 30 seconds.

```
xg(config)# spanning-tree max-age 30
```

5.11.6 spanning-tree forward-time

Function

The forward delay time of the Spanning Tree is the time required for the ports to change to a forwarding state.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
spanning-tree forward-time <4-30>
no spanning-tree forward-time
```

Parameter

- forward-time <4-30>

  Specifies the forward delay time for the Spanning Tree in seconds. Values can be set in the range of 4 to 30 seconds.

Command type

Configuration command

Default

15 seconds

Message

```
% Can't set forward-time.
```

Explanation

An unsettable value was specified. The settable range of "forward-time" differs depending on the values of "hello-time" and "max-age".

Solution

Set a value, which satisfies the conditions in this Section's Notes.

Note

- The settable range of forward delay time differs depending on the values set with the "spanning-tree hell-time" command and the "spanning-tree max-age" command. The value must also satisfy the following conditions:

```
2 × (forward_time - 1) ≥ max_age
max_age ≥ 2 × (hello_time + 1)
```

Example

Specify the forward delay time value to 17 seconds.

```
xg(config)# spanning-tree forward-time 17
```

5.11.7 spanning-tree port-priority

Function

Sets a port priority within the Spanning Tree.
A smaller value has a higher priority.
Use the no form to return to the default setup.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
spanning-tree port-priority <0-240>
no spanning-tree port-priority
```

Parameter

- port-priority <0-240>
  Specifies a port priority value within the Spanning Tree. Specify a value divisible by 16. It can be within the range of 0 to 240.

Command type

Configuration command

Default

128

Message

```
% Priority is not step of 16
```

Explanation

The priority value specified is not an integer divisible by 16.

Solution

Specify a priority value divisible by 16.

Example

Set the priority of port2 to 160.

```
xg(config)# interface port 2
xg(config-if)# spanning-tree port-priority 160
```

5.11.8 spanning-tree port-path-cost

Function

Sets a path cost for each port.
Use the no form to return to the default setup.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
spanning-tree port-path-cost <1-200000000>
no spanning-tree port-path-cost
```

Parameter

- port-path-cost <1-200000000>
  Sets a path cost for each port. It can be within the range of 1 to 200000000.
  The following path cost values are recommended by IEEE802.1D.

Link speed	IEEE802.1D (16bit)		IEEE802.1D (32bit)	
	Recommended range	Recommended value	Recommended range	Recommended value
100M bps	10 - 60	19	20000 - 2000000	200000
1G bps	3 - 10	4	2000 - 200000	20000
10G bps	1 - 5	2	200 - 20000	2000

Command type

Configuration command

Configuration command Default

2 (16bit)
2000 (32bit)

Example

Set the path cost for port 2 to 3:

```
xg(config)# interface port 2
xg(config-if)# spanning-tree port-path-cost 3
```

5.11.9 spanning-tree path-cost-default

Function

Sets the version of path cost (IEEE802.1D: 16bits or IEEE802.1D:32bits) to be used for the Spanning Tree Protocol.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
spanning-tree path-cost-default { 16bit | 32bit }
no spanning-tree path-cost-default
```

Parameter

- path-cost-default { 16bit | 32bit }
  - 16bit
    IEEE802.1D (16bits) will be used for the path cost. The default path cost is 2.
  - 32bit
    IEEE802.1D (32bits) will be used for the path cost. The default path cost is 2000.

Command type

Configuration command

Default

32bit

Message

% The Setting becomes an availableness by doing REBOOT.

Explanation

The settings changed will become valid when the system is restarted.

Solution

To make the settings valid, issue the "copy running-config startup-config" command first. Then, issue the "reset" command to restart the system.

Example

Use the 32-bit path cost:

```
xg(config)# spanning-tree path-cost-default 32bit
```

5.11.10 spanning-tree portfast

Function

The “portfast” function reduces the transition time required to transition to a "Forwarding" state. When the function is enabled, the port state is directly changed from "Discarding" to "Forwarding" and does not transition to a "Listening" or Learning" state.
This function can only be used with an edge port that is directly connected to a terminal node.
Use the no form to return to the default setup.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
spanning-tree portfast
no spanning-tree portfast
```

Parameter

- portfast
  `Enables the portfast function.`

Command type

Configuration command

Default

None

Message

```
% port %1$ is membership of uplink-domain %2$.
```

Explanation

```
The specified port already belongs to an uplink domain.
[[Inserted string]]%1$: specified port number
[[Inserted string]]%2$: uplink domain number
```

Solution

```
Specify a port not belonging to an uplink domain or remove the port from its uplink domain.
```

Note

- Use this function only for ports connected as an edge switch or for a port directly connected to a terminal node.
  If this function is applied to other ports, an unrecoverable loop condition will occur thereby affecting the switch and network operations may be affected.
- The port must be removed from an uplink domain before enabling the STP portfast function.

Example

Enable portfast for switch port 2.

```
xg(config)# interface port 2
xg(config-if)# spanning-tree portfast
```

5.11.11 spanning-tree portfast bpdu-guard

Function

Enable the BPDU guard function for a port within portfast enabled.
When BPDU guard enabled port receives a BPDU, the port is shut down and its communication fails. During this time, the received BPDU is not processed.
If the port is shut down, re-enable the communication either by using the “no shutdown” command or the “spanning-tree portfast errdisable-timeout” command thereby automatically restarting the communication after the err-disable timeout.
Use the no form to return to the default setup.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
spanning-tree portfast bpdu-guard
no spanning-tree portfast bpdu-guard
```

Parameter

- portfast bpdu-guard
  Enables the BPDU guard.

Command type

Configuration command

Default

None

Note

- The function is enabled for the port only if portfast was previously enabled on the port.

Example

Enables the portfast function and BPDU guard function for port 2.

```
xg(config)# interface port 2
xg(config-if)# spanning-tree portfast
xg(config-if)# spanning-tree portfast bpdu-guard
```

5.11.12 spanning-tree portfast errdisable-timeout

Function

Starts the timer that automatically releases a port from a shutdown state. This function is only valid for ports in wherein the portfast function and the BPDU guard function is enabled. This command is also used to specify a timer value.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
spanning-tree portfast errdisable-timeout [ interval <10-1000000> ]
no spanning-tree portfast errdisable-timeout
```

Parameter

- errdisable-timeout
  Enables the timer to release the port automatically from the shutdown status using the BPDU card.
- interval <10-1000000>
  Specifies the timeout value that automatically releases the port from a shutdown state. The value must be within the range of 10 to 1000000 seconds.
  If this parameter is omitted, the value is set to 300 seconds.

Command type

Configuration command

Default

None

Note

- Use this function only for ports connected to as an edge switch or for ports directly connected to a terminal node.
  If this function is applied to other ports an unrecoverable loop condition will occur thereby affecting the switch and network operations.

Example

Enable the automatic release timer for the port in a shutdown state.

```
xg(config)# spanning-tree portfast errdisable-timeout
```

5.11.13 spanning-tree portfast bpdu-filter

Function

Enable the BPDU filter for a portfast enabled port.
If BPDU filtering in enabled, the port does not send or receive a BPDU.
Use the no form to return to the default setup.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
spanning-tree portfast bpdu-filter
no spanning-tree portfast bpdu-filter
```

Parameter

- portfast bpdu-filter
  `Enables the BPDU filter for the port specified.`

Command type

Configuration command

Default

None

Note

- This function is only valid for portfast enabled ports.

Example

Enable BPDU filtering for port 2:

```
xg(config)# interface port 2
xg(config-if)# spanning-tree portfast
xg(config-if)# spanning-tree portfast bpdu-filter
```

5.12 Virtual LAN (VLAN) Setup Commands

This section explains the configuration commands related to Virtual LANs (VLAN).

5.12.1 show vlan

Function

Displays information about available VLANs and their member ports.

Prompt

xg> or xg#

Command syntax

```
show vlan [ <1-4094> ]
```

Parameter

- vlan <1-4094>
  Display specified VLAN and its total VLAN description.

When parameter is omitted, the state of all VLANs will be displayed. (VLAN description is displayed up to 19 characters)

Command type

Operation management command

Output form (no parameter)

```
xg# show vlan
Vlan Information                                                    2007/01/22-14:35:25
==================================================================================
VID  Vlan-Description     Tag   Ports-Membership
---- -------------------- ----- -------------------------------------------------
   1 default              TAG   agg-port 1 2 3 4 5 6
                                port 1 2 3 4 5 6 7 8 9 10
                          UNTAG port 11 12 13 14 15 16 17 18 19 20
   2 VLAN002              TAG   port 1 2 3
   3 VLAN003              UNTAG port 1 2 3
   4 VLAN004              ---   None
==================================================================================
```

Output form (parameter is specified)

```
xg# show vlan 2
Vlan Information                                                    2007/01/22-14:35:25
==================================================================================
VID 2
  Vlan-Description: VLAN0002

  Tag   Ports-Membership
  ----- -------------------------------------------------------
  TAG   port 1 2 3
==================================================================================
```

- VID
  Displays the VLAN ID (VID).
- Vlan-Description
  Displays the description assigned to the VLAN. If no description is set, a description consisting of "VLAN" and a 4-digit VID number will be assigned.
- Tag
  Displays the VLAN tag configuration.

Items displayed	Meaning
---	Non-VLAN member
TAG	VLAN member (with a tag) A frame having a VLAN tag will be forwarded.
UNTAG	VLAN member (without a tag) A frame having no VLAN tag will be forwarded.

- Ports-Membership
  Displays the member ports. If there are no member ports, "None" is displayed.

Example

Display the VLAN status.

```
xg# show vlan
```

5.12.2 vlan

Function

Creates a VLAN. Also, a VLAN description may be specified to allow easy identification.
Up to 128 VLANs can be created.
Use the no form to delete the VLAN.

Prompt

xg(config)#

Command syntax

```
vlan <1-4094> [ {description|name} VLAN_DESCRIPTION ]
no vlan <2-4094>
```

Parameter

- vlan <1-4094>
  Specifies an ID for the VLAN to be created. The VLAN ID (or VID) can be an integer in the range of 1 to 4094.
  The default VLAN (VID = 1 and description “default”) cannot be deleted.
- description|name VLAN_DESCRIPTION
  Describes the VLAN using ASCII characters. The description can be up to 256 alphanumeric characters in length.
  The default VLAN description is “VLAN****” (where, **** is the VID). No need to enclose a parameter in quotes if it contains a blank space.

Command type

Configuration command

Default

The default VLAN (VID=1, VLAN description =default) is initially registered with all ports as members.

Message

% Argument is too long

Explanation

The VLAN description length exceeded 256 characters.

Solution

Specify a VLAN description consisting of up to 256 alphanumeric characters.

% Can't add vlan. Max entry over.

Explanation

No more VLANs can be created. The maximum VLAN entries (128 entries) allowed are registered on the system.

Solution

Delete unnecessary VLANs and reissue the command.

% Can't delete vlan. same pvid entry

Explanation

The VLAN cannot be deleted because the specified port was set to port VLAN ID (“port-vlan-id”).

Solution

Make sure that each port VID is not the same as the VLAN ID. If not required, delete the port VID using the “no port-vlan-id” command. Then, delete the VLAN.

Note

- VLAN descriptions are not checked for duplication. Specify a unique description for each VLAN on the network.

Example

First, create a VLAN having VID 2 and VLAN description “vlan-floor1”. Second, create a VLAN having VID 3 and VLAN description “vlan-floor2”.
Finally, check the VLAN descriptions using the “show vlan” command.

```
xg(config)# vlan 2 description vlan-floor1
xg(config)# vlan 3 name vlan-floor2
xg(config)# exit
xg# show vlan
Vlan Information                                               2007/01/22-16:20:15
===================================================================================
VID  Vlan-Description    Tag   Ports-Membership
---- ------------------- ----- -----------------------------------------------------
   1 default            UNTAG port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
                                   20
   2 vlan-floor1         ---   None
   3 vlan-floor2         ---   None
===================================================================================
```

5.12.3 Interface vlan

Function

Switches from the global configuration mode to the interface edit mode wherein VLANs are configured.
Multiple VLANs can be configured collectively.

Prompt

xg(config)#

Command syntax

```
interface vlan <1-4094> [ <1-4094> ] ・・・
```

Parameter

- vlan <1-4094> [<1-4094>]・・・
  Specifies the VLAN to configure. When specifying multiple VLANs, list them separated with " " (space). Up to 8 VIDs can be specified.

Command type

Configuration command

Message

% duplicate vlan number: %1$

Explanation

The specified VID was duplicated.
[[Inserted string]]%1$: duplicated VID

Solution

Specify a unique VID.

% Can't set vlan id. Over max entry number. [8]

Explanation

The maximum number of VID was exceeded.

Solution

Specify no more than 8 VIDs and execute the command again..

% VLAN %1$ not configured.

Explanation

The specified VLAN is not created.
[[Inserted string]]%1$: specified VID

Solution

Create VID by "vlan” command.

Note

- Every command wherein VLAN edit mode is not displayed in “show running-config” command since equivalent commands are already exist.

Example

Switch to the collective interface edit mode using VLANs.

```
xg(config)# interface vlan 1 2 3
xg(config-vlan)#
```

5.12.4 egress

Function

Registers a port as a VLAN member.
Use the no form to release the VLAN membership.

Prompt

xg(config-vlan)#

Command syntax

```
egress { untagging | tagging } { port <1-20> | agg-port <1-10> }
no egress { port <1-20> | agg-port <1-10> }
```

Parameter

- untagging
  `Deletes a VLAN tag during frame transmission.`
- tagging
  `Adds a VLAN tag during frame transmission.`
- port <1-20>
  `Specifies a port for membership registration or deletion.`
- agg-port <1-10>
  `Specifies an aggregation group for membership registration or deletion.`

Command type

Configuration command

Default

Registers all ports with “egress-untagging” (the default VLAN).
Not set (except for the default VLAN)

Message

`% cannot found port interface: %1$`

Explanation

`The specified port number is not found.`
`[[Inserted string]]%1$: Port number`

Solution

`Assign the specified port not to be a member of an aggregation group.`

`% cannot found agg-port interface: %1$`

Explanation

`The specified aggregation group is not found.`
`[[Inserted string]]%1$: Aggregation group number`

Solution

`Check whether the specified aggregation group number is correct.`

`% duplicate port number: %1$`

Explanation

`The specified port number was duplicated.`
`[[Inserted string]]%1$: specified switch port number`

Solution

`Specify a switch unique port numbers.`

`% duplicate agg-port number: %1$`

Explanation

`The specified aggregation group number was duplicated.`
`[[Inserted string]]%1$: specified aggregation group number`

Solution

`Specify a unique aggregation group number.`

`% Can't remove vlan from port. Same pvid entry. %1$`

Explanation

`The specified VID cannot be deleted because it is identical to the default PVID.`
`[[Inserted string]]%1$: Port number`

Solution

`Change the default PVID and reissue the command.`

Example

The following example shows registering port 20 as members of VLAN 1, 2 and 3 (with untag).

```
xg(config)# interface vlan 1 2 3
xg(config-vlan)# egress untagging port 20
```

5.12.5 port-vlan-id

Function

The port-vlan-id command allows assigning a port to explicitly belong to a VLAN and configure the VLAN as a group of ports. However, when a frame with VLAN tags is received, the VLAN tag information has precedent over the port VID.
This command sets the default port VID (PVID) of the switch port. Also, the command registers it as a VLAN member port (without a tag).
Use the no form to return to the default value.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
port-vlan-id vlan <1-4094>
no port-vlan-id
```

Parameter

- vlan <1-4094>
  Specifies the default port VLAN ID (PVID). The PVID can be an integer of 1 to 4094.

Command type

Configuration command

Default

1

Message

```
% VLAN %1$ not configured. %2$
```

Explanation

```
The specified VLAN was not created.
[[Inserted string]]%1$: VID
[[Inserted string]]%2$: Port number
```

Solution

```
Create the VLAN first then reissue the command.
```

Note

When this command is issued, the port is registered as a member of the specified VLAN (having no tag). The frame having no tag is sent during egressing. To change the rule during egressing to “transfer tagged frames,” issue “vlan-member allowed vlan <1-4094> egress-tagging”.

Example

Set the default PVID of switch ports 2 and assign it to “vlan-floor2”, VID=3.
Then, display the VLAN information using the “show vlan” command and make sure that VID 3 was registered with port 2 as a member (untagged frames during egressing).

```
xg(config)# interface port 2
xg(config-if)# port-vlan-id vlan 3
xg(config-if)# exit
xg(config)# exit
xg# show vlan
Vlan Information                                               2007/01/22-16:20:15
==================================================================================
VID  Vlan-Description     Tag   Ports-Membership
---- ------------------- ----- ---------------------------------------------------
   1 default             UNTAG port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
                                    20
   2 vlan-floor1         ---   None
   3 vlan-floor2         UNTAG port 2
==================================================================================
```

5.12.6 vlan-member allowed

Function

Registers a port as a VLAN member.
Use the no form to release the VLAN membership.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
vlan-member allowed vlan { <1-4094> | all } { egress-untagging | egress-tagging }
no vlan-member allowed vlan { <1-4094> | all }
```

Parameter

- vlan <1-4094>
  Specifies a VLAN ID (or VID) for membership registration or VLAN ID deletion. The VID can be an integer of 1 to 4094.
- vlan all
  Registers or deletes member ports for all registered VLANs.
- egress-untagging
  Deletes a VLAN tag during frame transmission.
- egress-tagging
  Adds a VLAN tag during frame transmission.

Command type

Configuration command

Default

Registers all ports with "egress-untagging" (the default VLAN).
Not set (except for the default VLAN)

Message

```
% VLAN %1$ not configured. %2$
```

Explanation

```
The specified VLAN was not created.
[[Inserted string]]%1$: VID
[[Inserted string]]%2$: Port number
```

Solution

```
Create a VLAN first then reissue the command.
```

```
% Can't remove vlan from port. Same pvid entry. %1$
```

Explanation

```
The specified VID cannot be deleted because it is identical to the default PVID.
[[Inserted string]]%1$: Port number
```

Solution

```
Change the default PVID and reissue the command.
```

Example

Enter the interface edit mode for ports 1 to 3 and register the ports as VLAN members (with tags) of VID 3.
Then, use the "show vlan" command to display the VLAN information. Check that ports 1 to 3 have been registered as members of the VLAN (VID 3).

```
xg(config)# interface port range 1 3
xg(config-if)# vlan-member allowed vlan 3 egress-tagging
xg(config-if)# exit
xg(config)# exit
xg# show vlan
Vlan Information                                               2007/01/22-16:20:15
==================================================================================
VID  Vlan-Description    Tag   Ports-Membership
---- ------------------ ----- ---------------------------------------------------
   1 default             UNTAG port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
                                    20
   2 vlan-floor1          ---   None
   3 vlan-floor2          TAG   port 1 2 3
==================================================================================
```

5.12.7 user-vlan-protocol-id

Function

The VLAN tag protocol ID (VPID or TPID) used for VLAN tag identification can be changed to the user-defined value of each port.
The standard VLAN tag protocol ID was defined as 0x8100 in IEEE 802.1Q. However, the standard IEEE 802.1Q tag for multiple-tag VLAN encapsulated with the user-defined VPID (or TPID) tag (*) can be used.
*: Similar functions are called Stacked VLAN, Nested VLAN, VLAN tunneling and 802.1Q in 802.1Q (Q-in-Q).

Information

- For the frame format, see the TPID (Tag Protocol Identifier) in "Tag VLAN Frame Format".
- For the multiple-tag VLAN setup example and the frame flow, see "Multiple VLAN".

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
user-vlan-protocol-id <0x05DD ~ 0xFFFF>
no user-vlan-protocol-id
```

Parameter

- user-vlan-protocol-id <0x05DD ~ 0xFFFF>
  Specify the VPID (or TPID) using a hexadecimal integer beginning with 0x. It can be an integer in the range of 0x05DD to 0xFFFF.

Command type

Configuration command

Default

0x8100

Example

Enter the interface edit mode for ports 1 to 3 and set the VPID (or TPID) to 0x2000.

```
xg(config)# interface port range 1 3
xg(config-if)# user-vlan-protocol-id 0x2000
```

5.12.8 ingress-filter no-vlan-member-frame

Function

Enables VLAN ingress filtering. If the VLAN ingress filter is enabled, frames from non-member ports of a VLAN are discarded.
Use the no form to disable the ingress filtering.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
ingress-filter no-vlan-member-frame
no ingress-filter no-vlan-member-frame
```

Parameter

- no-vlan-member-frame
  Discards frames from non-member ports of a VLAN.

Command type

Configuration command

Default

None

Example

Enter the Edit Interface mode for switch ports 1 to 3 and enable VLAN ingress filtering.

```
xg(config)# interface port range 1 3
xg(config-if)# ingress-filter no-vlan-member-frame
```

5.12.9 ingress-filter tagged-frame

Function

Specifies that designated port VLAN-tagged frames will be discarded.
Use the no form to disable frame discarding.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
ingress-filter tagged-frame
no ingress-filter tagged-frame
```

Parameter

- tagged-frame
  Discards VLAN-tagged frames when they are received.

Command type

Configuration command

Default

None

Note

- If the user VPID is specified by the “user-vlan-protocol-id,” a tag having the same tag ID as the user VPID is considered to be the VLAN tag.
- If both “ingress-filter tagged-frame” and “ingress-filter untagged-frame” are specified, all frames received at this switch port are discarded.

Example

Enter the interface edit mode for ports 1 to 3 and specify to discard VLAN-tagged frames.

```
xg(config)# interface port range 1 3
xg(config-if)# ingress-filter tagged-frame
```

5.12.10 ingress-filter untagged-frame

Function

Specifies that designated port VLAN untagged frames will be discarded.
Use the no form to disable frame discarding.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
ingress-filter untagged-frame
no ingress-filter untagged-frame
```

Parameter

- untagged-frame
  Discards VLAN untagged frames when they are received.

Command type

Configuration command

Default

None

Note

- If the user VPID is specified by the “user-vlan-protocol-id,” a tag having the same tag ID as the user VPID is considered to be the VLAN tag.
- If both “ingress-filter tagged-frame” and “ingress-filter untagged-frame” are specified, all frames received at this port are discarded.
- When using the Spanning Tree Protocol (STP), do not specify the “ingress-filter untagged-frame” command.

Example

Enter the interface edit mode for ports 1 to 3 and specify to discard VLAN untagged frames.

```
xg(config)# interface port range 1 3
xg(config-if)# ingress-filter untagged-frame
```

5.12.11 vlan-statistics collection

Function

Configures the specified VLANs to collect statistics information. Up to 32 VLANs can be set.
Use the no form to cancel collecting the VLAN statistics information.

Prompt

xg(config)#

Command syntax

```
vlan-statistics collection <1-4094> [ <1-4094> ・・・・・ ]
no vlan-statistics
```

Parameter

- collection <1-4094> <1-4094>・・・・・

  Specifies the ID of the VLAN to collect statistics information.
  To collect the statistics information on multiple VLANs, specify multiple VIDs by separating them with a “ ” (space). Up to 32 VLANs can be specified.

Command type

Configuration command

Default

None

Message

% Can't set vlan id. Over max entry number. [%1$]

Explanation

No more VLANs can be specified for collection. The maximum allowed VLANs (32) have been specified.
[[Inserted string]]%1$: Limit value

Solution

Delete VLANs whose information is no longer required then reissue the command.

Note

- If a VID of an uncreated VLAN is specified, the command is terminated normally. However, the statistics information of an uncreated VLAN is not collected.

Example

Specify VIDs 1, 10, 20, 30 and 40 for VLAN statistics collection.
Then, change the VIDs to 1, 10, 20 and 30 only to collect their VLAN statistics information.

```
xg(config)# vlan-statistics collection 1 10 20 30 40
xg(config)# vlan-statistics collection 1 10 20 30
```

5.13 QoS Setup Commands

This section explains the Quality of Service (QoS) configuration commands.

5.13.1 show qos

Function

Displays the current Quality of Service (QoS) status.

Prompt

xg> or xg#

Command syntax

```
show qos [ qos-map ]
```

Parameter

- qos-map

  Displays the QoS priority mapping information (that is, the output queue information for each priority).
  There are four levels of output queues (levels 0 to 3). A higher value has the higher output priority.
  If this parameter is omitted, all QoS information is displayed.

Command type

Operation management command

Output form

```
xg# show qos
QoS Information                                      2007/01/22-12:12:15
==============================================================================
Priority Output Queue Mapping
-----------------------------------------
Qos Priority:      0  1  2  3  4  5  6  7
----------------- -- -- -- -- -- -- -- --
Output Priority:   1  0  0  1  2  2  3  3
-----------------------------------------
==============================================================================
```

QoS Priority Mapping Information

- Qos Priority

  Displays the QoS priority (0 to 7).
- Output Priority

  Displays the output queue level for each priority (0 to 3).

Example

Display the QoS status:

```
xg# show qos
```

5.13.2 qos default-priority

Function

Sets the default priority for frames having no priority information (such as VLAN untagged frames).
Use the no form to return to the default setup.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
qos default-priority <0-7>
no qos default-priority
```

Parameter

- default-priority <0-7>
  Sets the default priority for frames having no priority information.

Command type

Configuration command

Default

0

Example

Enter the interface edit mode for switch ports 1 and 3, and set the default priority to 1.

```
xg(config)# interface port 1 3
xg(config-if)# qos default-priority 1
```

5.13.3 qos-map priority

Function

The system has four priority levels of output queues for frame transmission processing.
This command maps the frame priorities to the output queue levels.
Use the no form to reset the entire mapping information to the default setup.

Prompt

xg(config)#

Command syntax

```
qos-map priority <0-7> output-priority <0-3>
no qos-map
```

Parameter

- priority <0-7>
  Specifies a frame priority within the range of 0 to 7.
- output-priority <0-3>
  Specifies the output queue level to be associated with the specified priority within the range of 0 to 3.

Command type

Configuration command

Default

priority	output-priority
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Example

Map the priority “0” to the output queue “2”.

```
xg(config)# qos-map priority 0 output-priority 2
```

5.13.4 bridge diffserv-tos

Function

Enables Quality of Service using the DiffServ code point.
When priority control by DiffServ codes is enabled, any priority included in a VLAN tag and the default priority are ignored.
Use the no form to disable DiffServ code control.

Prompt

xg(config)#

Command syntax

```
bridge diffserv-tos { ipv4 | ipv6 }
no bridge diffserv-tos
```

Parameter

- diffserv-tos { ipv4 | ipv6 }
  Enables Quality of Service using the DiffServ code point.
  - ipv4
    Enables IPv4 Quality of Service.
  - ipv6
    Enables IPv6 Quality of Service.

Command type

Configuration command

Default

None

Example

Enable Quality of Service using the DiffServ code point for IPv4.

```
xg(config)# bridge diffserv-tos ipv4
```

5.13.5 qos egress-scheduling

Function

Sets the egress scheduling algorithm.
Use the no form to reset to default.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
qos egress-scheduling {strict | drr | drr-strict}
no qos egress-scheduling
```

Parameter

- egress-scheduling

  Specify the egress scheduling algorithm

  - strict

    Frames are forwarded based on strict priority scheduling. Higher priority frames always precede those of lower priority.
  - drr

    Frames are forwarded based on deficit round robin (DRR) algorithm. Minimum bandwidth for each output queue can be specified by "qos bandwidth" command.
  - drr-strict

    Frames are forwarded based on the combination of strict priority scheduling and DRR algorithm. Strict priority scheduling is used for output queue "0" and "1", and DRR algorithm for output queue "2" and "3".

Command type

Configuration command

Default

Strict

Example

Sets strict method to the algorithm that schedules priority.

```
xg(config-if)# qos egress-scheduling strict
```

5.13.6 qos bandwidth

Function

Sets a band width value for an output queue. Each output queue can be assured sufficient output traffic rate.
Use the no form to reset to default.

Prompt

xg(config-if)# or xg(config-agg)#

Command syntax

```
qos bandwidth <0-10000> output-priority <0-3>
no qos bandwidth
```

Parameter

- bandwidth <0-10000>

  Specifies the bandwidth of an output queue in the range of 0 to 10000 Mbps. The value must be an integer divisible by 100.
- output-priority <0-3>

  Specifies the output queue within the range of 0 to 3 to associate with the bandwidth value.

Command type

Configuration command

Default

0 (Sets the band width of the output queue to be equal)

Message

```
% The set value is not step of 100
```

Explanation

The specified the band width value is not an integer divisible by 100.

Solution

Sets a band width value with an integer divisible by 100.

```
% The total value exceeded 10000
```

Explanation

The sum of the bandwidth values of each output queue is exceeds 10Gbps.

Solution

Changes the bandwidth values so the total does not exceed 10Gbps.

Note

- Residual bandwidth is assigned to each output queue without specified bandwidth. Enabling jumbo frames and the frame size established affects minimum bandwidth assignments across all output queues. The "The total value exceeded 10000" error message may be displayed despite the fact the total bandwidth assigned a given queue does not exceed 10Gbps.
- Setting bandwidth 0 is same as no form, so the configuration is cleared.

Example

Sets 4Gbps for output queue "0" s.

```
xg(config-if)# no qos bandwidth
xg(config-if)# qos bandwidth 4000 output-priority 0
```

5.14 Port Mirroring Setup Commands

This section explains the configuration commands for port mirroring.

5.14.1 show mirror

Function

Displays the current mirroring configuration for send and receive frames.

Prompt

xg> or xg#

Command syntax

```
show mirror
```

Command type

Operation management command

Output form

```
xg# show mirror
Mirror Information                                   2007/01/22-12:12:15
===============================================================================
Monitored Port     Rx Mirroring Port
--------------     -----------------
Port-1        ===> Port-2

Monitored Port     Tx Mirroring Port
--------------     -----------------
Port-1        ===> Port-3
===============================================================================
```

- Monitored Port
  Displays the port number of the monitored switch.
- Rx Mirroring Port
  Displays the destination port number for mirroring of frames received at the monitored port.
- Tx Mirroring Port
  Displays the destination port number for mirroring of frames sent from the monitored port.

Example

Display the port mirroring status.

```
xg> show mirror
```

5.14.2 mirror

Function

Configures port mirroring for specific ports.
Use the no form to cancel the port mirroring setup.

Prompt

xg(config)#

Command syntax

```
mirror monitored-port <1-20> [rx-mirroring-port <1-20>] [tx-mirroring-port <1-20>]
no mirror
```

Parameter

- monitored-port <1-20>
  Specifies a port number to be monitored.
- rx-mirroring-port <1-20>
  Specifies the destination port number for mirroring of received frames. It must be different from the port specified by "monitored-port/tx-mirroring-port".
- tx-mirroring-port <1-20>
  Specifies the destination port number for mirroring of sent frames. It must be different from the port specified by "monitored-port/rx-mirroring-port".

Command type

Configuration command

Default

None

Message

% Cannot set same port.

Explanation

Identical port numbers for the "monitored-port", "rx-mirroring-port" or "tx-mirroring-port" have been specified.

Solution

Specify different port numbers by reviewing the "monitored-port", "rx-mirroring-port" and "tx-mirroring-port" values then reissue the command.

% Mirroring port %1$ is a member of aggregation group.

Explanation

The command was not executed since the port, specified by "rx-mirroring-port" or "tx-mirroring-port", is a member of an aggregation group.
[[Inserted string]]%1$: The port number specified by "rx-mirroring-port" or "tx-mirroring-port".

Solution

Delete the specified port from the aggregation group then reissue the command.

Note

- If port mirroring was enabled before issuing this command, the impacted ports are reassigned in accordance with the most recent command.

Example

Mirror the frames received at port 1 to port 2, and mirror the frames sent from port 1 to port 3.

```
xg(config)# mirror monitored-port 1 rx-mirroring-port 2 tx-mirroring-port 3
```

Mirror the frames received at port 1 to port 2.

```
xg(config)# mirror monitored-port 1 rx-mirroring-port 2
```

5.15 IGMP Snooping Setup Commands

This section explains the IGMP snooping configuration commands.

5.15.1 show ip snooping

Function

Displays the IGMP snooping configuration.

Prompt

xg> or xg#

Command syntax

```
show ip snooping [vlan <1-4094> ]
show ip snooping mrouter [vlan <1-4094>]
show ip snooping group [vlan <1-4094>]
```

Parameter

- [vlan <1-4094>]
  Displays the IGMP snooping configuration for the specified VLAN.
  If this parameter is omitted, all of the VLANs configuration information is displayed.
- mrouter [vlan <1-4094>]
  Displays only the multicast router information for the IGMP snooping configuration.
  If "vlan" is omitted, all of the VLANs' configuration information is displayed.
- group [vlan <1-4094>]
  Displays only the registered multicast group information for the IGMP snooping configuration.
  If "vlan" is omitted, all of the VLANs' configuration information is displayed.

Command type

Operation management command

Output form

```
xg# show ip snooping
IGMP Snooping Information                                 2007/01/22-22:17:04
===============================================================================
Global IGMP snooping          : { Enabled | Disabled }

[vlan-1]
 IGMP snooping                 : { Enabled | Disabled }
 Registered group number       : 0 (Current) / 32 (Maximum)
 Multicast router auto learning: { Enabled | Disabled }
 Fast leave                    : { Enabled | Disabled }
 Group Membership interval     : 260 (sec)
 Last Member Query interval    : 2 (sec)
 Send Query count              : 2 (times)
 IGMP snooping querier         : { Enabled | Disabled }
   General Query interval      : 125 (sec)
   Querier IP address          : 0.0.0.0

 Multicast Router Information
 -----------------------------------------------------------------------------
 Vlan Type    Mrouter ports
 ---- ------- ------------
    1  static  port 5
 -----------------------------------------------------------------------------

 Multicast Group Information
 -----------------------------------------------------------------------------
 Vlan Multicast Group Ver Member ports
 ---- -------------- --- ------------------------------------------------------
    1  225.10.10.1      2   port 1 5
-------------------------------------------------------------------------------

[vlan-2]
   . . . . . .
   . . . . . .
```

- Global IGMP snooping
  The operational state of IGMP snooping for the device is displayed.
  - Enabled
    IGMP snooping is enabled.
  - Disabled
    IGMP snooping is disabled.

[vlan 1]
The VIDs of applicable VLANs are displayed.

- IGMP snooping
  The IGMP operational state for the applicable VLANs are displayed.
  - Enabled
    IGMP snooping is enabled.
  - Disabled
    IGMP snooping is disabled.
- Registered group number
  The number of registered multicast groups detected through IGMP snooping are displayed.
  - (Current)
    The number of currently registered groups is displayed.
  - (Maximum)
    The maximum number of groups that can be registered for the applicable VLANs is displayed.
- Multicast router auto learning
  The status of the Automatic Learning mode for the multicast router is displayed.
  - Enabled
    Automatic learning for the multicast router is enabled.
  - Disabled
    Automatic learning for the multicast router is disabled.
- Fast leave
  The status of the Immediate Leave mode is displayed.
  - Enabled
    The Immediate Leave mode is enabled.
  - Disabled
    The Immediate Leave mode is disabled.
- Group Membership interval
  The valid interval time (in seconds) for the registered multicast group is displayed.
- Last Member Query interval
  The monitoring time (in seconds) for leaving confirmation when an IGMP Leave message is received is displayed.
- Send Query count
  The transmission frequency of query messages by the IGMP query function is displayed.
- IGMP snooping querier
  The operation state of IGMP query function is displayed.
  - Enabled
    The IGMP query function is enabled.
  - Disabled
    The IGMP query function is disabled.
- General Query interval
  The transmission interval (in seconds) of query messages sent by the IGMP query function is displayed.
- Querier IP address
  Source IP address of the query message sent by the IP querier is displayed.

Multicast Router Information
The multicast router status is displayed.

- Vlan
  The ID of the applicable VLAN is displayed.
- Type
  The identified type of multicast router is displayed.
  - static
    This is a multicast router statically set by the CLI.
  - dynamic
    This is a multicast router port dynamically learned by IGMP snooping.
- Mrouter ports
  The port numbers registered with the multicast router are displayed.
  For an aggregation group, the group number is displayed immediately after the "agg-port" information.

Multicast Group Information
The state of the registered multicast groups detected through IGMP snooping are displayed.

- Vlan
  The ID of the applicable VLAN is displayed.
- Multicast Group
  The addresses of registered IP multicast groups are displayed.
- Ver
  The version of the received IGMP protocol is displayed.
- Member ports
  The port numbers of the registered multicast group is displayed.
  For an aggregation group, the group number is displayed immediately after the "agg-port" information.

Output form (if “mrouter” is specified)

Only the multicast router information is extracted from the IGMP snooping information and displayed.

```
xg# show ip snooping mrouter
IGMP Snooping Information(Multicast Router)              2005/04/24-22:19:52
===============================================================================
  Vlan Type    Mrouter ports
  ---- ------- -------------
     1 static  port 5
     2 dynamic port 6
----------------------------------------------------------------------------
===============================================================================
```

Output form (if “group” is specified)

Only the multicast group information is extracted from the IGMP snooping information and displayed.

```
xg# show ip snooping group
IGMP Snooping Information(Multicast Group)               2005/04/24-22:20:56
===============================================================================
  Vlan  Multicast Group Ver Member ports
  ---- --------------- --- ---------------------------------------------------
    1  225.0.0.1        2   port 1 5
    2  225.0.0.2        2   port 1 5
----------------------------------------------------------------------------
===============================================================================
```

5.15.2 ip snooping protocol

Function

Enables global IGMP snooping.
Use the no form to disable the snooping.

Prompt

xg(config)#

Command syntax

```
ip snooping protocol igmp
no ip snooping protocol igmp
```

Parameter

- protocol igmp
  `Enables global IGMP snooping for the device.`

Command type

Configuration command

Default

None

Message

```
% port %1$ is membership of uplink-domain %2$.
```

Explanation

```
The displayed port is used as an uplink.
[[Inserted string]]%1$: Port number
[[Inserted string]]%2$: Uplink domain number
```

Solution

```
Clear the uplink domain before enabling IGMP snooping.
```

Note

- IGMP snooping and the uplink filter function cannot be used at the same time.

Example

Enable IGMP snooping of the device.

```
xg(config)# ip snooping protocol igmp
```

5.15.3 ip snooping vlan

Function

Enables IGMP snooping for a specified VLAN.
IGMP snooping can be enabled for each VLAN only after enabling global IGMP snooping using the “ip snooping protocol” command.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
ip snooping vlan <1-4094>
no ip snooping vlan <1-4094>
```

Parameter

- vlan <1-4094>
  Enables IGMP snooping for the specified VLAN.

Command type

Configuration command

Default

Enabled (for the default VLAN)
Disabled (for all VLANs other than the default VLAN)

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the “ip snooping protocol” command first then reissue the “ip snooping vlan” command.

```
% Vlan id is not found. vid=%1$
```

Explanation

The specified VLAN was not created.
[[Inserted string]]%1$: VID of the specified VLAN

Solution

Create a VLAN using the “vlan” command first then reissue the “ip snooping vlan” command.

```
% More than 128 total max-group per system.
```

Explanation

The registration number of multicast addresses allowed on the entire system exceeded the limit (128 addresses).

Solution

Reduce the maximum number of VLANs using the “ip snooping vlan max-group” command, or disable the IGMP snooping function for other VLANs.

Example

Enable IGMP snooping of VLAN 2:

```
xg(config)# ip snooping vlan 2
```

5.15.4 ip snooping vlan max-group

Function

Defines the number of multicast groups that can be registered for IGMP snooping on each VLAN.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
ip snooping vlan <1-4094> max-group <10-128>
no ip snooping vlan <1-4094> max-group
```

Parameter

- vlan <1-4094>
  Changes the IGMP snooping setup for the specified VLAN.
- max-group <10-128>
  Sets the maximum number of multicast groups that can be registered. It can be any integer between 10 and 128.

Command type

Configuration command

Default

32

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the "ip snooping protocol" command first, then reissue the "ip snooping vlan" command.

```
% Vlan id is not found. vid=%1$
```

Explanation

The specified VLAN was not created.
[[Inserted string]]%1$: VID of the specified VLAN

Solution

Create a VLAN using the "vlan" command first then reissue the "ip snooping vlan" command.

```
% IGMP snooping vlan-%1$ is not enabled.
```

Explanation

IGMP snooping for the specified VLAN is disabled.
[[Inserted string]]%1$: VID of the specified VID

Solution

Enable the IGMP snooping for the VLAN using the "ip snooping vlan" command first then reissue the "ip snooping vlan max-group" command.

```
% More than 128 total max-group per system.
```

Explanation

The number of registration of multicast addresses allowed on the entire system exceeded the limit (128 addresses).

Solution

Reduce the maximum number of VLANs using the "ip snooping vlan max-group" command, or disable the IGMP snooping function for other VLANs.

Note

- Up to 128 multicast MAC addresses can be registered on the entire system.
  Therefore, if IGMP snooping is used by multiple VLANs, care must be taken not to exceed the limit number of multicast MAC addresses.
- Sets the maximum number of multicast groups not to exceed the number of multicast groups that Is registered currently.

Example

Set the number of groups that can be registered for IGMP snooping on VLAN 2 to 50.

```
xg(config)# ip snooping vlan 2 max-group 50
```

5.15.5 ip snooping vlan mrouter

Function

Automatically learns the IGMP query message receiving port as a multicast router port.
This command can statically set multicast router ports. Also, it can change the automatic learning mode of multicast router ports.
Set multicast router ports statically to register more than one multicast router port.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
ip snooping vlan <1-4094> mrouter { port <1-20> | agg-port <1-10> }
no ip snooping vlan <1-4094> mrouter { port <1-20> | agg-port <1-10> }

ip snooping vlan <1-4094> mrouter suppress-learning
no ip snooping vlan <1-4094> mrouter suppress-learning
```

Parameter

- vlan <1-4094>
  Specifies the VLAN to change.
- mrouter port <1-20>
  Specifies a port number to be set statically as the multicast router port.
- mrouter agg-port <1-10>
  Specifies an aggregation group number to be set statically as the multicast router port.
- mrouter suppress-learning
  Disables automatic learning on the multicast router ports.

Command type

Configuration command

Default

None

Message

% Global IGMP snooping is not enabled.

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the “ip snooping protocol” command first then reissue the “ip snooping vlan” command.

% Vlan id is not found. vid=%1$

Explanation

The specified VLAN was not created.
[[Inserted string]]%1$: Specified VID

Solution

Create a VLAN using the “vlan” command first then reissue the “ip snooping vlan” command.

% IGMP snooping vlan-%1$ is not enabled.

Explanation

IGMP snooping of the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID

Solution

Enable IGMP snooping on the VLAN using the “ip snooping vlan” command first, then reissue the “ip snooping vlan max-group” command.

% Port is not vlan member. vid=%1$

Explanation

The specified port is not a VLAN member.
[[Inserted string]]%1$: Specified VID

Solution

Set the port as a VLAN member using the “vlan-member allowed” command first, then reissue the “ip snooping vlan mrouter” command.

% Aggregation-port is not vlan member. vid=%1$

Explanation

The specified aggregation group is not a VLAN member.
[[Inserted string]]%1$: Specified VLAN ID

Solution

Set the aggregation group as a VLAN member using the “vlan-member allowed” command first, then reissue the “ip snooping vlan mrouter” command.

% Aggregation-port not bound to bridge.

Explanation

The specified aggregation group does not exist.

Solution

Configure a link aggregation group by using the “link-aggregation” command first then specify the “agg-port” using the “ip snooping vlan mrouter” command.

% Can't set mrouter on a port which belongs to an aggregation port.

Explanation

A port belonging to a link aggregation group cannot be specified as an mrouter port.

Solution

Review the specified port number and reissue the command. When registering an aggregation group specify "agg-port".

% Multicast router port %1$ could not be deleted

Explanation

The specified port is not set to be an multicast router port.
[[Inserted string]]%1$: Specified port number

Solution

Review multicast router information and execute the command again.

Example

Set aggregation group 1 as a multicast router port:

```
xg(config)# ip snooping vlan 2 mrouter agg-port 1
```

5.15.6 ip snooping vlan group-member-interval

Function

Sets a valid time interval (in seconds) for the IP multicast group which was registered for IGMP snooping.
The registered IP multicast group is deleted if an IGMP Report message is not received within the valid time.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
ip snooping vlan <1-4094> group-member-interval <60-600>
no ip snooping vlan <1-4094> group-member-interval
```

Parameter

- vlan <1-4094>

  Specifies a VLAN to change.

- group-member-interval <60-600>

  Specifies the valid time period in seconds for the registered IP multicast group.

> Point
>
> It is recommended "group member interval" be set by considering the message transmission interval of the multicast router connected to the system. (This interval is called the "query interval" and its default is 125 seconds in RFC.) The recommended value is as follows.
>
> Group-member-interval = Query Interval × 2 + 10 (seconds)

Command type

Configuration command

Default

260 seconds

Message

% Global IGMP snooping is not enabled.

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the "ip snooping protocol" command first then reissue the "ip snooping vlan group-member-interval" command.

% Vlan id is not found. vid=%1$

Explanation

The specified VLAN was not created.
[[Inserted string]]%1$: Specified VID

Solution

Create a VLAN using the "vlan" command first then reissue the "ip snooping vlan group-member-interval" command.

% IGMP snooping vlan-%1$ is not enabled.

Explanation

IGMP snooping on the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID

Solution

Enable IGMP snooping on the VLAN using the "ip snooping vlan" command first, then reissue the "ip snooping vlan group-member-interval" command.

Example

Set the valid time interval for the IP multicast group learned at VLAN 1 to 300 seconds (5 minutes).

```
xg(config)# ip snooping vlan 1 group-member-interval 300
```

5.15.7 ip snooping vlan fast-leave

Function

Set the Fast Leave mode on the IP multicast group port where the IGMP Leave message is received. In the Fast Leave mode, the exit is not checked when the IGMP Leave message is received.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
ip snooping vlan <1-4094> fast-leave
no ip snooping vlan <1-4094> fast-leave
```

Parameter

- vlan <1-4094>
  Specifies a VLAN to change.
- fast-leave
  Enables the Fast Leave mode.

Command type

Configuration command

Default

None

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the “ip snooping protocol” command first then reissue the “ip snooping vlan fast-leave” command.

```
% Vlan id is not found. vid=%1$
```

Explanation

The specified VLAN was not created.
[[Inserted string]]%1$: Specified VID

Solution

Create a VLAN using the “vlan” command first then reissue the “ip snooping vlan fast-leave” command.

```
% IGMP snooping vlan-%1$ is not enabled.
```

Explanation

IGMP snooping of the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID

Solution

Enable IGMP snooping on the VLAN using the “ip snooping vlan” command first then reissue the “ip snooping vlan fast-leave” command.

Example

Enable the Fast Leave mode on VLAN 1.

```
xg(config)# ip snooping vlan 1 fast-leave
```

5.15.8 ip snooping vlan last-member-query-interval

Function

Sets the monitoring time (in seconds) for checking on the exit of the last member of a IP multicast group. If an IGMP Report message is not issued within the monitoring time after reception of an IGMP Leave message, the IP multicast group is deleted. Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
ip snooping vlan <1-4094> last-member-query-interval <1-9>
no ip snooping vlan <1-4094> last-member-query-interval
```

Parameter

- vlan <1-4094>
  Specifies a VLAN to change.
- last-member-query-interval <1-9>
  Specifies the monitoring time (in seconds) to check for member exit.

Command type

Configuration command

Default

2 seconds

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the “ip snooping protocol” command first then reissue the “ip snooping vlan last-member-query-interval” command.

```
% Vlan id is not found. vid=%1$
```

Explanation

The specified VLAN was not created.
[[Inserted string]]%1$: Specified VID

Solution

Create a VLAN using the “vlan” command first then reissue the “ip snooping vlan” command.

```
% IGMP snooping vlan-%1$ is not enabled.
```

Explanation

IGMP snooping of the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID

Solution

Enable IGMP snooping on the VLAN using the “ip snooping vlan” command first, then reissue the “ip snooping vlan last-member-query-interval” command.

Example

Set the monitoring time to check for member exit on VLAN 2 to 3 seconds.

```
xg(config)# ip snooping vlan 2 last-member-query-interval 3
```

5.15.9 ip snooping vlan send-query-count

Function

Sets a query message transmission frequency.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
ip snooping vlan <1-4094> send-query-count <1-3>
no ip snooping vlan <1-4094> send-query-count
```

Parameter

- vlan <1-4094>
  Specifies a VLAN to change.
- send-query-count <1-3>
  Sets a query message transmission frequency.

Command type

Configuration command

Default

2

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the “ip snooping protocol” command first then reissue the “ip snooping vlan send-query-count” command.

```
% Vlan id is not found. vid=%1$
```

Explanation

The specified VLAN was not created.
[[Inserted string]]%1$: Specified VID

Solution

Create a VLAN using the “vlan” command first then reissue the “ip snooping vlan send-query-count” command.

```
% IGMP snooping vlan-%1$ is not enabled.
```

Explanation

IGMP snooping of the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID

Solution

Enable IGMP snooping on the VLAN using the “ip snooping vlan” command first, then reissue the “ip snooping vlan send-query-count” command.

Example

Set the query message transmission frequency on VLAN 2 to 3:

```
xg(config)# ip snooping vlan 2 send-query-count 3
```

5.15.10 ip snooping vlan querier

Function

The IGMP Querier function sends an IGMP General Query message to each terminal node instead of the multicast router if no multicast router exists on the network segment.
This command enables the IGMP querier. The query message transmission interval (called “Query interval”) is calculated based on the query message transmission frequency and the group valid time interval (called “Group member interval”) as follows.

- Query interval = (Group-membership-interval – 10) / send-query-count (seconds)

The device does not send Query messages when there is a multicast router on the network.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
ip snooping vlan <1-4094> querier ip A.B.C.D
no ip snooping vlan <1-4094> querier
```

Parameter

- vlan <1-4094>
  Specifies a VLAN to change.
- querier
  Enables the IGMP querier function.
- ip A.B.C.D
  Specifies the source IP address of Query messages to be sent by the IGMP querier.
  The IP address can be 0.0.0.0 or within the range of 1.0.0.1 to 126.255.255.254, 128.0.0.1 to 191.255.255.254, or 192.0.0.1 to 223.255.255.254.

Command type

Configuration command

Default

None

Message

```
% Global IGMP snooping is not enabled.
```

Explanation
Global IGMP snooping is disabled on the system.
Solution
Enable global IGMP snooping using the “ip snooping protocol” command first then reissue the “ip snooping vlan querier” command.

```
% Vlan id is not found. vid=%1$
```

Explanation
The specified VLAN was not created.
[[Inserted string]]%1$: Specified VLAN ID
Solution
Create a VLAN using the “vlan” command first then reissue the “ip snooping vlan querier” command.

```
% IGMP snooping vlan-%1$ is not enabled.
```

Explanation
IGMP snooping on the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID
Solution
Enable IGMP snooping on the VLAN using the “ip snooping vlan” command first, then reissue the “ip snooping vlan querier” command.

```
% Invalid IP-address.
```

Explanation
The IP address was specified in an incorrect format or an incorrect address was specified.
Solution
Specify the IP address in the correct format and reissue the command.

Example

Enable an IGMP querier on VLAN 1 and set the query transmission source IP address to "192.168.1.200.”

```
xg(config)# ip snooping vlan 1 querier ip 192.168.1.200
```

5.15.11 ip snoop

Function

Enables IGMP snooping for specified VLANs. This command is enabled after enabling global IGMP snooping using the “ip snooping protocol” command.
Use the no form to return to the default setup.

Prompt

xg(config-vlan)#

Command syntax

```
ip snooping
no ip snooping
```

Command type

Configuration command

Default

Enabled (for the default VLAN)
Disabled (for all VLANs other than the default VLAN)

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the “ip snooping protocol” command first then execute the command again.

```
% More than 128 total max-group per system.
```

Explanation

The registered number of multicast addresses allowed on the entire system exceeded the limit (128 addresses).

Solution

Reduce the maximum number of VLANs using a command such as “ip snooping vlan max-group”, or disable the IGMP snooping function for other VLANs.

Example

Enable IGMP snooping of VLAN 2 and 3.

```
xg(config)# interface vlan 2 3
xg(config-vlan)# ip snooping
```

5.15.12 ip snooping max-group

Function

Defines the number of multicast groups that can be registered for IGMP snooping on specified VLANs.
Use the no form to return to the default setup.

Prompt

xg(config-vlan)#

Command syntax

```
max-group <10-128>
no ip snooping max-group
```

Parameter

- max-group <10-128>
  Sets the maximum number of multicast groups that can be registered. It can be any integer between 10 and 128.

Command type

Configuration command

Default

32

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the "ip snooping protocol" command first then execute the command again.

```
% More than 128 total max-group per system.
```

Explanation

The registered number of multicast addresses allowed on the entire system exceeded the limit (128 addresses).

Solution

Reduce the maximum number of VLANs using a command such as "ip snooping vlan max-group", or disable the IGMP snooping function for other VLANs.

```
% IGMP snooping vlan-%1$ is not enabled.
```

Explanation

IGMP snooping is not valid on specified VLAN ID.
[[Inserted string]]%1$: Specified VID

Solution

Valid IGMP snooping on specified VLAN by "ip snooping vlan" or "ip snooping" command.

Note

- Up to 128 multicast MAC addresses can be registered on the entire system.
  Therefore, if IGMP snooping is used by multiple VLANs, care must be taken not to exceed the limit number of multicast MAC addresses.
- Sets the maximum number of multicast groups not to exceed the number of multicast groups that Is registered currently.

Example

Set the number of groups, that can be registered for IGMP snooping on VLAN 2 and 3, to 30.

```
xg(config)# interface vlan 2 3
xg(config-vlan)# ip snooping max-group 30
```

5.15.13 ip snooping mrouter

Function

Automatically learns the IGMP query message receiving port as a multicast router port.
This command can statically set multicast router ports. Also, it can change the automatic learning mode of multicast router ports.
Set multicast router ports statically to register more than one multicast router port.
Use the no form to return to the default setup.

Prompt

xg(config-vlan)#

Command syntax

```
ip snooping mrouter { port <1-20> | agg-port <1-10> }
no ip snooping mrouter { port <1-20> | agg-port <1-10> }

ip snooping mrouter suppress-learning
no ip snooping mrouter suppress-learning
```

Parameter

- mrouter port <1-20>
  Specifies a port number to be set statically as the multicast router port.
- mrouter agg-port <1-10>
  Specifies an aggregation group number to be set statically as the multicast router port.
- mrouter suppress-learning
  Disables automatic learning on the multicast router ports.

Command type

Configuration command

Default

None

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the "ip snooping protocol" command first then execute the command again.

```
% IGMP snooping vlan-%1$ is not enabled.
```

Explanation

IGMP snooping of the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID

Solution

Enable IGMP snooping on the VLAN using the "ip snooping vlan" command first, then execute the command again.

```
% Port is not vlan member. vid=%1$
```

Explanation

The specified port is not a VLAN member.
[[Inserted string]]%1$: Specified VID

Solution

Set the port as a VLAN member using the "vlan-member allowed" command first, then execute the command again.

```
% Aggregation-port is not vlan member. vid=%1$
```

Explanation

The specified aggregation group is not a VLAN member.
[[Inserted string]]%1$: Specified VLAN ID

Solution

Set the aggregation group as a VLAN member using the "vlan-member allowed" command first, then execute the command again.

```
% Aggregation-port not bound to bridge.
```

Explanation

The specified aggregation group does not exist.

Solution

Configure a link aggregation group by using the "link-aggregation" command first then execute the command again.

```
% Can't set mrouter on a port which belongs to an aggregation port.
```

Explanation

A port belonging to a link aggregation group cannot be specified as an mrouter port.

Solution

Review the specified port number and reissue the command. When registering an aggregation group specify "agg-port".

```
% Multicast router port %1$ could not be deleted
```

Explanation

The specified port is not set to be an multicast router port.
[[Inserted string]]%1$: Specified port number

Solution

Review multicast router information and execute the command again.

Example

Set port 1 as a multicast router port at VLAN 2 and 3

```
xg(config)# interface vlan 2 3
xg(config-vlan)# ip snooping mrouter port 1
```

5.15.14 ip snooping group-member-interval

Function

Sets a valid time interval (in seconds) for the IP multicast group which was registered for IGMP snooping.
The registered IP multicast group is deleted if an IGMP Report message is not received within the valid time.
Use the no form to return to the default setup.

Prompt

xg(config-vlan)#

Command syntax

```
ip snooping group-member-interval <60-600>
no ip snooping group-member-interval
```

Parameter

- group-member-interval <60-600>

  Specifies the valid time period in seconds for the registered IP multicast group.

> It is recommended "group member interval" be set by considering the message transmission interval of the multicast router connected to the system. (This interval is called the "query interval" and its default is 125 seconds in RFC.) The recommended value is as follows.
> Group-member-interval = Query Interval × 2 + 10 (seconds)

Command type

Configuration command

Default

260 seconds

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the "ip snooping protocol" command first then execute the command again.

```
% IGMP snooping vlan-%1$ is not enabled.
```

Explanation

IGMP snooping on the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID

Solution

Enable IGMP snooping on the VLAN using the "ip snooping vlan" command first, then execute the command again.

Example

Set the valid time interval for the IP multicast group learned at VLAN 2 and 3 to 300 seconds (5 minutes).

```
xg(config)# interface vlan 2 3
xg(config-vlan)# ip snooping group-member-interval 300
```

5.15.15 ip snooping fast-leave

Function

Set the Fast Leave mode on the IP multicast group port where the IGMP Leave message is received. In the Fast Leave mode, the exit is not checked when the IGMP Leave message is received.
Use the no form to return to the default setup.

Prompt

xg(config-vlan)#

Command syntax

```
ip snooping fast-leave
no ip snooping fast-leave
```

Parameter

- fast-leave
  Enables the Fast Leave mode.

Command type

Configuration command

Default

None

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the “ip snooping protocol” command first then execute the command again.

```
% IGMP snooping vlan-%1$ is not enabled.
```

Explanation

IGMP snooping of the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID

Solution

Enable IGMP snooping on the VLAN using the “ip snooping vlan” command first then execute the command again.

Example

Enable the Fast Leave mode on VLAN 2 and 3.

```
xg(config)# interface vlan 2 3
xg(config-vlan)# ip snooping fast-leave
```

5.15.16 ip snooping last-member-interval

Function

Sets the monitoring time (in seconds) for checking on the exit of the last member of a IP multicast group. If an IGMP Report message is not issued within the monitoring time after reception of an IGMP Leave message, the IP multicast group is deleted. Use the no form to return to the default setup.

Prompt

xg(config-vlan)#

Command syntax

```
ip snooping last-member-interval <1-9>
no ip snooping last-member-interval
```

Parameter

- last-member-interval <1-9>
  `Specifies the monitoring time (in seconds) to check for member exit.`

Command type

Configuration command

Default

2 seconds

Message

`% Global IGMP snooping is not enabled.`

Explanation

`Global IGMP snooping on the device is disabled.`

Solution

`Enable global IGMP snooping using the “ip snooping protocol” command first then execute the command again.`

`% IGMP snooping vlan-%1$ is not enabled.`

Explanation

`IGMP snooping of the specified VLAN is disabled.`
`[[Inserted string]]%1$: Specified VID`

Solution

`Enable IGMP snooping on the VLAN using the “ip snooping vlan” command first, then execute the command again.`

Example

Set the monitoring time to check for member exit on VLAN 2 to 3 seconds.

```
xg(config)# interface vlan 2
xg(config-vlan)# ip snooping last-member-interval 3
```

5.15.17 ip snooping send-query-count

Function

Sets a query message transmission frequency.
Use the no form to return to the default setup.

Prompt

xg(config-vlan)#

Command syntax

```
ip snooping send-query-count <1-3>
no ip snooping send-query-count
```

Parameter

- send-query-count <1-3>
  Sets a query message transmission frequency.

Command type

Configuration command

Default

2

Message

```
% Global IGMP snooping is not enabled.
```

Explanation

Global IGMP snooping on the device is disabled.

Solution

Enable global IGMP snooping using the “ip snooping protocol” command first then execute the command again.

```
% IGMP snooping vlan-%1$ is not enabled.
```

Explanation

IGMP snooping of the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID

Solution

Enable IGMP snooping on the VLAN using the “ip snooping vlan” command first, then execute the command again.

Example

Set the query message transmission frequency on VLAN 2 to 3:

```
xg(config)# interface vlan 2
xg(config-vlan)# ip snooping send-query-count 3
```

5.15.18 ip snooping querier

Function

The IGMP Querier function sends an IGMP General Query message to each terminal node instead of the multicast router if no multicast router exists on the network segment.
This command enables the IGMP querier. The query message transmission interval (called “Query interval”) is calculated based on the query message transmission frequency and the group valid time interval (called “Group member interval”) as follows.

- Query interval = (Group-membership-interval – 10) / send-query-count (seconds)

The device does not send Query messages when there is a multicast router on the network.
Use the no form to return to the default setup.

Prompt

xg(config-vlan)#

Command syntax

```
ip snooping querier ip A.B.C.D
no ip snooping querier
```

Parameter

- querier
  Enables the IGMP querier function.
- ip A.B.C.D
  Specifies the source IP address of Query messages to be sent by the IGMP querier.
  The IP address can be 0.0.0.0 or within the range of 1.0.0.1 to 126.255.255.254, 128.0.0.1 to 191.255.255.254, or 192.0.0.1 to 223.255.255.254.

Command type

Configuration command

Default

None

Message

% Global IGMP snooping is not enabled.

Explanation

Global IGMP snooping is disabled on the system.

Solution

Enable global IGMP snooping using the “ip snooping protocol” command first then execute the command again.

% IGMP snooping vlan-%1$ is not enabled.

Explanation

IGMP snooping on the specified VLAN is disabled.
[[Inserted string]]%1$: Specified VID

Solution

Enable IGMP snooping on the VLAN using the “ip snooping vlan” command first, then execute the command again.

% Invalid IP-address.

Explanation

The IP address was specified in an incorrect format or an incorrect address was specified.

Solution

Specify the IP address in the correct format and execute the command.

Example

Enable an IGMP querier on VLAN 2 and set the query transmission source IP address to "192.168.1.200.”

```
xg(config)# interface vlan 2
xg(config-vlan)# ip snooping querier ip 192.168.1.200
```

5.16 Statistics Commands

The device provides a wide variety of statistical displays.
Statistics can be displayed using the “monitor” command, which periodically updates the display information, or by using the “show statistics” command which displays a snapshot.

Point

The transmission byte statistics information does not include preambles (framing bytes).

Note

Set the terminal screen size to 50 columns by 12 lines or more when issuing the “monitor” command.
If the terminal screen size is too small, the following message is displayed.

```
% terminal line is too small
```

or

```
% terminal width is too short
```

Point

The number of statistics display lines vary depending upon the counter used.
If the line length exceeds the limit, the following unit is displayed at the right of the displayed value. The unit indicates a multiplier for the value displayed.

K:	1,000
M:	1,000,000
G:	1,000,000,000
T:	1,000,000,000,000

5.16.1 monitor traffic-bytes

Function

Displays the transmission frame length (in bytes) at each port.

Prompt

xg> or xg#

Command syntax

```
monitor traffic-bytes { current | total } [interval <3-60>]
```

Parameter

- { current | total }
  Specifies the statistics to be displayed.
  – current
    Displays the accumulated byte count of transmission frames after startup of this command.
  – total
    Displays the accumulated byte count of transmission frames after startup of the system.
- interval <3-60>
  Specifies the update interval (in seconds).
  The default interval is 3 seconds.

Command type

Operation management command

Output form (if "current" is specified)

```
xg# monitor traffic-bytes current
Traffic Statistics(Current Frame Bytes)           2007/01/22-12:12:15
====================================================================>
Port Link State/    Tx Rate    Rx Rate   Tx-Frame      Rx-Frame
     STP State     Bits/Sec   Bits/Sec   Bytes         Bytes
---- ------------- ---------- ---------- ------------ -----------
   1 Up/Discard    12345678K  12345678K  1234567890K  1234567890K
   2 Down                  0          0            0            0
   3 Up/Discard          923        923  1234567890K  1234567890K
   4 Up/Learn        999123K    999123K  1234567890M  1234567890M
   5 Up/Forward          999        999  1234567890G  1234567890G
   6 Up/Forward      999999K    999999K  1234567890T  1234567890T
   7 Down                  0          0            0            0
   8 Down                  0          0            0            0
====================================================================>
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

```
(continues)
Traffic Statistics(Current Frame Bytes)              2007/01/22-12:12:15
<=======================================================================
Port-Description

------------------------------------
port_name1
port_name2
port_name3
port_name4
port_name5
port_name6
port_name7

<=======================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

- Port
  Displays port numbers. Statistics for each port are displayed on one line.
- Link State/STP State
  Displays the port state in the Link State or STP State format.
  The Link State may indicate one of the following link states.
  – Down
    The port link is down.
  – Up
    The port link is up.
  The STP State displays the current port status based on the STP (Spanning Tree Protocol).
  Note that the STP State is not displayed if the Link State is down.
  For port status details, see "Spanning Tree Protocol Port States".
- Tx Rate Bits/Sec
  Displays the transmission rate (in bps) using an 8-digit, right-justified value.
- Rx Rate Bits/Sec
  Displays the receive rate (in bps) using an 8-digit, right-justified value.
- Tx-Frame Bytes
  Displays the accumulated transmission byte count after execution of this command, using a 10-digit, right-justified value.
- Rx-Frame Bytes
  Displays the accumulated receive byte count after execution of this command, using a 10-digit, right-justified value.

- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 33 characters can be displayed.

Output form (if "total" is specified)

```
xg# monitor traffic-bytes total
Traffic Statistics(Total Frame Bytes)                      2007/01/22-12:12:15
==============================================================================
Port Link State/   Tx-Frame     Rx-Frame    Port-Description
     STP State     Bytes        Bytes
---- ------------- -----------  ------------ ---------------------------------
   1 Up/Discard    1234567890K  1234567890K port_name1
   2 Down          1234567890G  1234567890G port_name2
   3 Up/Discard    1234567890M  1234567890M port_name3
   4 Up/Learn      1234567890T  1234567890T port_name4
   5 Up/Forward     1234567890   1234567890 port_name5
   6 Up/Forward     1234567890   1234567890 port_name6
   7 Down           1234567890   1234567890 port_name7
   8 Down           1234567890   1234567890
==============================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

- Port
  Same as the display description for the “current” option
- Link State/STP State
  Same as the display description for the “current” option
- Tx-Frame Bytes
  Displays the accumulated transmission byte count after system startup, using a 10-digit, right-justified value.
- Rx-Frame Bytes
  Displays the accumulated receive byte count after system startup, using a 10-digit, right-justified value.
- Port-Description
  Same as the display description for the “current” option

5.16.2 monitor traffic-counts

Function

Displays the transmission frame count at each port.

Prompt

xg> or xg#

Command syntax

```
monitor traffic-counts { current | total } [interval <3-60>]
```

Parameter

- { current | total }
  Specifies the statistics to be displayed.
  - current
    Displays the number of accumulated transmission frames after startup of this command.
  - total
    Displays the number of accumulated transmission frames after startup of the system.
- interval <3-60>
  Specifies the update interval (in seconds).
  The default interval is 3 seconds.

Command type

Operation management command

Output form (if "current" is specified)

```
xg# monitor traffic-counts current
Traffic Statistics(Current Frame Counts)                     2007/01/22-12:12:15
===============================================================================>
Port  Link State/ Tx-Frame    Rx-Frame    Tx-Frame    Rx-Frame     Rx-Bcast
       STP State  Counts/S    Counts/S    Counts      Counts       Counts
----  ----------  ----------  ----------  ----------  ------------ -----------
   1  Up/Discard   12345678K   12345678K  1234567890K 1234567890K   1234567890K
   2  Down                 0           0            0           0             0
   3  Up/Discard         923         923  1234567890K 1234567890K   1234567890K
   4  Up/Learn        999123      999123  1234567890M        256M          256M
   5  Up/Forward         999         999  1234567890G        256G          256G
   6  Up/Forward      999999      999999  1234567890T        256T          256T
===============================================================================>
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

```
(continues)
Traffic Statistics(Current Frame Counts)                       2007/01/22-12:12:15
<=================================================================================
Rx-Mcast     Port-Description
Counts
----------- ------------------------------------
1234567890K  port_name1
          0  port_name2
1234567890K  port_name3
       256M  port_name4
       256G  port_name5
       256T
<=================================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

- Port
  Displays the port numbers. Statistics for each port are displayed on one line.
- Link State/STP State
  Displays the port state in the Link State or STP State format.
  The Link State may indicate one of the following link states.
  - Down
    The port link is down.
  - Up
    The port link is up.

  The STP State displays the current port status based on the STP (Spanning Tree Protocol).
  Note that the STP State is not displayed if the Link State is down.
  For port status details, see "Spanning Tree Protocol Port States".
- Tx-Frame Counts/S
  Displays the transmission frame rate (in fps) using an 8-digit, right-justified value.
- Rx-Frame Counts/S
  Displays the receive frame rate (in fps) using an 8-digit, right-justified value.
- Tx-Frame Counts
  Displays the number of accumulated transmission frames after execution of this command, using a 10-digit, right-justified value.
- Rx-Frame Counts
  Displays the number of accumulated receive frames after execution of this command, using a 10-digit, right-justified value.

- Rx-Bcast Counts
  Displays the number of accumulated receive broadcast frames after execution of this command, using a 10-digit, right-justified value.
- Rx-Mcast Counts
  Displays the number of accumulated receive multicast frames after execution of this command, using a 10-digit, right-justified value.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 36 characters can be displayed.

Output form (if “total” is specified)

```
xg# monitor traffic-counts total
Traffic Statistics(Total Frame Counts)            2007/01/22-12:12:15
=======================================================================>
Port Link State/  Tx-Frames     Rx-Frames     Rx-Bcast     Rx-Mcast
     STP State    Counts        Counts        Counts       Counts
---- ------------ -----------   -----------   -----------  -----------
   1 Up/Discard   1234567890K   1234567890K   1234567890K   1234567890K
   2 Down                   0             0             0             0
   3 Up/Discard   1234567890K   1234567890K   1234567890K   1234567890K
   4 Up/Learn     1234567890K   1234567890K   1234567890K   1234567890K
   5 Up/Forward   1234567890K   1234567890K   1234567890K   1234567890K
   6 Up/Forward   1234567890K   1234567890K   1234567890K   1234567890K
   7 Down         1234567890K   1234567890K   1234567890K   1234567890K
   8 Down         1234567890K   1234567890K   1234567890K   1234567890K
======================================================================>
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

```
(continues)
Traffic Statistics(Total Frame Counts)             2007/01/22-12:12:15
<======================================================================
Port-Description

------------------------------------
port_name1
port_name2
port_name3
port_name4
port_name5
port_name6
port_name7

<======================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

- Port
  Same as the display described for the “current” option
- Link State/STP State
  Same as the display described for the “current” option
- Tx-Frame Counts
  Displays the number of accumulated transmission frames after system startup, using a 10-digit, right-justified value.
- Rx-Frame Counts
  Displays the number of accumulated receive frames after system startup, using a 10-digit, right-justified value.
- Rx-Bcast Counts
  Displays the number of accumulated receive broadcast frames after system startup, using a 10-digit, right-justified value.
- Rx-Mcast Counts
  Displays the number of accumulated receive multicast frames after system startup, using a 10-digit, right-justified value.
- Port-Description
  Same as the display description for the “current” option

5.16.3 monitor framesize-traffic-counts

Function

Displays a frame count and size range for frames which have been sent or received at each port.

Prompt

xg> or xg#

Command syntax

```
monitor framesize-traffic-counts { current | total } [interval <3-60>]
```

Parameter

- { current | total }
  Specifies the statistics to be displayed.
  – current
    Displays the number of accumulated frames after startup of this command.
  – total
    Displays the number of accumulated frames after startup of the system.
- interval <3-60>
  Specifies the update interval (in seconds).
  The default interval is 3 seconds.

Command type

Operation management command

Output form (if "current" is specified)

```
xg# monitor framesize-traffic-counts current
Framesize Traffic Statistics(Current Frame Counts)          2007/01/22-12:12:15
===============================================================================>
Port Link State/ FrameSize    FrameSize     FrameSize   FrameSize     FrameSize
     STP State    0-64         65-127       128-255      256-511       512-1023
---- ---------   ----------   ----------   -----------  -----------  -----------
 1   Up/Discard   1234567890K 1234567890K  1234567890K  1234567890K  1234567890K
 2   Down                   0           0            0            0            0
 3   Up/Discard   1234567890K 1234567890K  1234567890K  1234567890K  1234567890K
 4   Up/Learn     1234567890M      25690M       25690M       25690M       25690M
 5   Up/Forward   1234567890G      25690G       25690G       25690G       25690G
 6   Up/Forward   1234567890T      25690T       25690T       25690T       25690T
 7   Down                   0           0            0            0            0
 8   Down                   0           0            0            0            0
===============================================================================>
ESC:exit     F:refresh
U:page up    D:page down   L:page left  R:page right
```

```
(continues)
Framesize Traffic Statistics(Current Frame Counts)      2007/01/22-12:12:15
<==========================================================================
FrameSize   Port-Description
1024-1518
----------- ------------------------------------------
1234567890K port_name1
          0 port_name2
1234567890K port_name3
      25690 port_name4
     25690G port_name5
     25690T port_name6
          0 port_name7
          0

<==========================================================================
ESC:exit     F:refresh
U:page up    D:page down   L:page left  R:page right
```

- Port
  Displays the port numbers. Statistics for each port are displayed on one line.
- Link State/STP State
  Displays the port state in the Link State or STP State format.
  The Link State may indicate one of the following link states.
  – Down
    The port link is down.
  – Up
    The port link is up.
  The STP State displays the current port status based on the STP (Spanning Tree Protocol).
  Note that the STP State is not displayed if the Link State is down.
  For port status details, see "Spanning Tree Protocol Port States".
- FrameSize 0-64
  Displays the number of accumulated 64-byte frames sent or received after the command execution.
- FrameSize 65-127
  Displays the number of accumulated 65- to 127-byte frames sent or received after the command execution.
- FrameSize 128-255
  Displays the number of accumulated 128- to 255-byte frames sent or received after the command execution.

- FrameSize 256-511
  Displays the number of accumulated 256- to 511-byte frames sent or received after the command execution.
- FrameSize 512-1023
  Displays the number of accumulated 512- to 1023-byte frames sent or received after the command execution.
- FrameSize 1024-1518
  Displays the number of accumulated 1024- to 1518-byte frames sent or received after the command execution.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 44 characters can be displayed.

Output form (if "total" is specified)

```
xg# monitor framesize-traffic-counts total
Framesize Traffic Statistics(Total Frame Counts)           2007/01/22-12:12:15
=============================================================================>
Port Link State/  FrameSize    FrameSize   FrameSize    FrameSize    Framesize
     STP State   0-64         65-127     128-255      256-511     512-1023
---- -----------  ----------- ----------- ----------- ----------- -----------
   1 Up/Discard   1234567890K 1234567890K 1234567890K 1234567890K 1234567890K
   2 Down                   0           0           0           0           0
   3 Up/Discard   1234567890K 1234567890K 1234567890K 1234567890K 1234567890K
   4 Up/Learn     1234567890M      25690M      25690M      25690M      25690M
   5 Up/Forward   1234567890G      25690G      25690G      25690G      25690G
   6 Up/Forward   1234567890T      25690T      25690T      25690T      25690T
   7 Down                   0           0           0           0           0
   8 Down                   0           0           0           0           0
=============================================================================>
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

```
(continues)
Framesize Traffic Statistics(Total Frame Counts)        2007/01/22-12:12:15
<==========================================================================
 FrameSize   Port-Description
 1024-1518
 ----------- --------------------------------------------
 1234567890K port_name1
           0 port_name2
 1234567890K port_name3
       25690 port_name4
      25690G port_name5
      25690T port_name6
           0 port_name7
           0
<==========================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

- The displayed values are the ones accumulated after the system startup. Other values are the same as those displayed if the “current” option were specified.

5.16.4 monitor qos-priority-traffic-bytes

Function

Displays the number of bytes received at each port for each QoS priority.

Prompt

xg> or xg#

Command syntax

```
monitor qos-priority-traffic-bytes { current | total } [interval <3-60>]
```

Parameter

- { current | total }
  Specifies the statistics to be displayed.
  - current
    Displays the number of bytes in each QoS priority received after startup of this command.
  - total
    Displays the number of bytes in each QoS priority received after the system startup.
- interval <3-60>
  Specifies the update interval (in seconds).
  The default interval is 3 seconds.

Command type

Operation management command

Output form (if "current" is specified)

```
xg# monitor qos-priority-traffic-bytes current
Qos Priority Traffic Statistics(Current Frame Bytes)           2007/01/22-12:12:15
=================================================================================>
Port Priority-0  Priority-1  Priority-2  Priority-3  Priority-4  Priority-5  Priority-6
     Bytes       Bytes       Bytes       Bytes       Bytes       Bytes       Bytes
---- ----------- ----------- ----------- ----------- ----------- ----------- -----------
   1 1234567890K 1234567890K  1234567890  1234567890  1234567890  1234567890  1234567890
   2           0           0           0           0           0           0           0
   3 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K
   4 1234567890M     256890M     256890M     256890M     256890M     256890M     256890M
   5 1234567890G     256890G     256890G     256890G     256890G     256890G     256890G
   6 1234567890T     256890T     256890T     256890T     256890T     256890T     256890T
   7           0           0           0           0           0           0           0
   8           0           0           0           0           0           0           0
=================================================================================>
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

```
(continues)
Qos Priority Traffic Statistics(Current Frame Bytes)           2007/01/22-12:12:15
<================================================================================
Priority-7  Port-Description
Bytes
----------- ---------------------------------------------------
 1234567890  port_name1
          0  port_name2
1234567890K  port_name3
    256890M  port_name4
    256890G  port_name5
    256890T  port_name6
          0  port_name7
          0
<================================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

- Port
  Displays the port numbers. Statistics for each port are displayed on one line.
- Priority-0 Bytes - Priority-7 Bytes
  Display the accumulated number of bytes for each of priority 0 through 7 received at each port after the command execution, using 10-digit, right-justified values.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 51 characters can be displayed.

Output form (if "total" is specified)

```
xg# monitor qos-priority-traffic-bytes total
Qos Priority Traffic Statistics(Total Frame Bytes)            2007/01/22-12:12:15
===============================================================================>
Port Priority-0  Priority-1   Priority-2  Priority-3   Priority-4  Priority-5  Priority-6
     Bytes       Bytes        Bytes       Bytes        Bytes       Bytes       Bytes
---- ----------- ----------- ----------- ----------- ----------- ----------- -----------
   1 1234567890K 1234567890K  1234567890  1234567890   1234567890  1234567890  1234567890
   2           0           0           0           0           0           0           0
   3 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K
   4 1234567890M     256890M     256890M     256890M     256890M     256890M     256890M
   5 1234567890G     256890G     256890G     256890G     256890G     256890G     256890G
   6 1234567890T     256890T     256890T     256890T     256890T     256890T     256890T
   7           0           0           0           0           0           0           0
   8           0           0           0           0           0           0           0
===============================================================================>
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

```
(continues)
Qos Priority Traffic Statistics(Total Frame Bytes)           2007/01/22-12:12:15
<==========================================================================
Priority-7  Port-Description
Bytes
----------- ------------------------------------------------
 1234567890  port_name1
          0  port_name2
1234567890K  port_name3
    256890M  port_name4
    256890G  port_name5
    256890T  port_name6
          0  port_name7
          0
<==========================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

The bytes displayed in the “Bytes” column are the ones accumulated after the system startup. Other values are the same as those displayed if the “current” option were specified.

5.16.5 monitor qos-priority-traffic-counts

Function

Displays the number of frames received at each port for each QoS priority.

Prompt

xg> or xg#

Command syntax

```
monitor qos-priority-traffic-counts { current | total } [interval <3-60>]
```

Parameter

- { current | total }
  Specifies the statistics to be displayed.
  - current
    Displays the accumulated number of frames in each QoS priority received after startup of this command.
  - total
    Displays the accumulated number of frames in each QoS priority received after the system startup.
- interval <3-60>
  Specifies the update interval (in seconds).
  The default interval is 3 seconds.

Command type

Operation management command

Output form (if "current" is specified)

```
xg# monitor qos-priority-traffic-counts current
Qos Priority Traffic Statistics(Current Frame Counts)           2007/01/22-12:12:15
=================================================================================>
Port Priority-0  Priority-1  Priority-2  Priority-3  Priority-4  Priority-5  Priority-6
      Counts      Counts      Counts      Counts      Counts      Counts      Counts
---- ----------- ----------- ----------- ----------- ----------- ----------- -----------
   1 1234567890K 1234567890K  1234567890  1234567890  1234567890  1234567890  1234567890
   2           0           0           0           0           0           0           0
   3 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K
   4 1234567890M     256890M     256890M     256890M     256890M     256890M     256890M
   5 1234567890G     256890G     256890G     256890G     256890G     256890G     256890G
   6 1234567890T     256890T     256890T     256890T     256890T     256890T     256890T
   7           0           0           0           0           0           0           0
   8           0           0           0           0           0           0           0
=================================================================================>
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

```
(continues)
Qos Priority Traffic Statistics(Current Frame Counts)       2007/01/22-12:12:15
<=============================================================================
Priority-7  Port-Description
Counts
----------- ---------------------------------------------------
1234567890  port_name1
         0  port_name2
1234567890K port_name3
    256890M port_name4
    256890G port_name5
    256890T port_name6
          0 port_name7
          0
<=============================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

- Port
  Displays the port numbers. Statistics for each port are displayed on one line.
- Priority-0 Counts to Priority-7 Counts
  Display the accumulated number of frames for each priority 0 through 7 received at each port after the command execution, using 10-digit, right-justified values.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 51 characters can be displayed.

Output form (if "total" is specified)

```
xg# monitor qos-priority-traffic-counts total
Qos Priority Traffic Statistics(Total Frame Counts)          2007/01/22-12:12:15
=========================================================================================>
Port Priority-0  Priority-1   Priority-2  Priority-3   Priority-4  Priority-5  Priority-6
     Counts      Counts       Counts      Counts       Counts      Counts      Counts
---- ----------- ----------- ----------- ----------- ----------- ----------- -----------
   1 1234567890K 1234567890K  1234567890  1234567890   1234567890  1234567890   1234567890
   2           0           0           0           0           0           0           0
   3 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K 1234567890K
   4 1234567890M     256890M     256890M     256890M     256890M     256890M     256890M
   5 1234567890G     256890G     256890G     256890G     256890G     256890G     256890G
   6 1234567890T     256890T     256890T     256890T     256890T     256890T     256890T
   7           0           0           0           0           0           0           0
   8           0           0           0           0           0           0           0
=========================================================================================>
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

```
(continues)
Qos Priority Traffic Statistics(Total Frame Counts)     2007/01/22-12:12:15
<==========================================================================
Priority-7  Port-Description
Counts
----------- -----------------------------------------------
 1234567890 port_name1
          0 port_name2
1234567890K port_name3
    256890M port_name4
    256890G port_name5
    256890T port_name6
          0 port_name7
          0
<==========================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

The values displayed in the “Counts” column are the ones accumulated after the system startup. Other values are the same as those displayed if the “current” option were specified.

5.16.6 monitor vlan-traffic-bytes

Function

Displays the received byte count of each VLAN.

Prompt

xg> or xg#

Command syntax

```
monitor vlan-traffic-bytes { current | total } [interval <3-60>]
```

Parameter

- { current | total }
  Specifies the statistics to be displayed.
  - current
    Displays the accumulated byte count of received frames for each VLAN after startup of this command.
  - total
    Displays the accumulated byte count of received frames for each VLAN after the system startup.
- interval <3-60>
  Specifies the update interval (in seconds).
  The default interval is 3 seconds.

Command type

Operation management command

Output form (if "current" is specified)

```
xg# monitor vlan-traffic-bytes current
VLAN Traffic Statistics(Current Frame Bytes) 2007/01/22-12:12:15
================================================================
VID    Rx-Frame    Rx-NonUcast
        Bytes      Bytes
---- ----------- ------------
   1  1234567890    1234567890
  10           0             0
  20 1234567890K  1234567889K
  30      25690M        25690M
  40      25690G        25690G
4094           0             0
================================================================
ESC:exit     F:refresh
U:page up    D:page down   L:page left  R:page right
```

- VID
  Displays the VID of the VLAN set for statistics collection. Statistics of each VLAN are displayed on one line.

Point
Specify the VLAN to collect its statistics using the "vlan-statistics collection" command.

- Rx-Frame Bytes
  Displays the accumulated byte count of frames received at the specified VLAN after the startup of this command, using a 10-digit, right-justified value.
- Rx-NonUcast Bytes
  Displays the accumulated byte count of multicast or broadcast frames received at the specified VLAN after the startup of this command, using a 10-digit, right-justified value.

Output form (if "total" is specified)

```
xg# monitor qos-priority-traffic-bytes total
VLAN Traffic Statistics(Total Frame Bytes) 2007/01/22-12:12:15
==============================================================
VID   Rx-Frame     Rx-NonUcast
       Bytes       Bytes
---- ----------- ------------
   1  1234567890   1234567890
  10           0            0
  20 1234567890K  1234567889K
  30      25690M       25690M
  40      25690G       25690G
4094           0            0
==============================================================
ESC:exit     F:refresh
U:page up    D:page down   L:page left  R:page right
```

The bytes displayed in the “Bytes” column are the ones accumulated after the system startup. Other values are the same as those displayed if the “current” option were specified.

5.16.7 monitor vlan-traffic-counts

Function

Displays the received frame count of each VLAN.

Prompt

xg> or xg#

Command syntax

```
monitor vlan-traffic-counts { current | total } [interval <3-60>]
```

Parameter

- { current | total }
  Specifies the statistics to be displayed.
  - current
    Displays the accumulated number of frames for each VLAN received after startup of this command.
  - total
    Displays the accumulated number of frames for each VLAN received after the system startup.
- interval <3-60>
  Specifies the update interval (in seconds).
  The default interval is 3 seconds.

Command type

Operation management command

Output form (if "current" is specified)

```
xg# monitor vlan-traffic-counts current
VLAN Traffic Statistics(Current Frame Counts) 2007/01/22-12:12:15
=================================================================
VID  Rx-Frame     Rx-NonUcast
     Counts       Counts
---- ----------- -----------
   1  1234567890  1234567890
  10           0           0
  20 1234567890K 1234567890K
  30      25690M      25690M
  40      25690G      25690G
4094           0           0
=================================================================
ESC:exit     F:refresh
U:page up    D:page down   L:page left  R:page right
```

- VID
  Displays the VID of the VLAN set for statistics collection. Statistics for each VLAN are displayed on one line.

> Point
> Specify the VLAN to collect its statistics using the "vlan-statistics collection" command.

- Rx-Frame Counts
  Displays the accumulated number of frames received at the specified VLAN after the startup of this command, using a 10-digit, right-justified value.
- Rx-NonUcast Counts
  Displays the accumulated number of multicast or broadcast frames received at the specified VLAN after the startup of this command, using a 10-digit, right-justified value.

Output form (if "total" is specified)

```
xg# monitor vlan-traffic-counts total
VLAN Traffic Statistics(Total Frame Counts) 2007/01/22-12:12:15
===============================================================
VID  Rx-Frame    Rx-NonUcast
     Counts      Counts
---- ----------- -----------
   1  1234567890   1234567890
  10           0            0
  20 1234567890K  1234567890K
  30      25690M       25690M
  40      25690G       25690G
4094           0            0
===============================================================
ESC:exit     F:refresh
U:page up    D:page down   L:page left  R:page right
```

The values displayed in the “Counts” column are the ones accumulated after the system startup. Other values are the same as those displayed if the “current” option were specified.

5.16.8 monitor dataflow

Function

Displays statistics including both pause frame transmission to and from each port and the results of transmission processing.

Prompt

xg> or xg#

Command syntax

```
monitor dataflow { current | total } [interval <3-60>]
```

Parameter

- { current | total }
  Specifies the statistics to be displayed.
  - current
    Displays the accumulated data count after startup of this command.
  - total
    Displays the accumulated data count after the system startup.
- interval <3-60>
  Specifies the update interval (in seconds).
  The default interval is 3 seconds.

Command type

Operation management command

Output form (if "current" is specified)

```
xg# monitor dataflow current
Dataflow Statistics(Current Counts)                 2007/01/22-12:12:15
=====================================================================>
Port Link State/  Flow-Ctl Forward     Flood       Rx-Pause     Tx-Pause
     STP State    Mode     Counts      Counts      Counts       Counts
---- ------------ ------- ----------- ----------- ----------- -----------
   1 Up/Discard    Rx & Tx   1234567890  1234567890   1234567890  1234567890
   2 Down          Rx                 0           0            0           0
   3 Up/Discard    Rx & Tx  1234567890K 1234567890K 1234567890K 1234567890K
   4 Up/Learn      Rx & Tx  1234567890M      25690M      25690M      25690M
   5 Up/Forward    Rx & Tx  1234567890G      25690G      25690G      25690G
   6 Up/Forward    Rx & Tx  1234567890T      25690T      25690T      25690T
   7 Down          Rx                 0           0            0           0
   8 Down          Rx                 0           0            0           0
=====================================================================>
ESC:exit     F:refresh
U:page up    D:page down   L:page left  R:page right
```

```
 (continues)
Dataflow Statistics(Current Counts)                 2007/01/22-12:12:15
<=====================================================================
Full-Drop    VLAN-Drop  Port-Description
Counts       Counts
----------- ----------- ----------------------------
1234567890   1234567890  port_name1
         0            0  port_name2
1234567890K 1234567890K  port_name3
    25690M       25690M  port_name4
     25690G       25690G  port_name5
    25690T       25690T  port_name6
         0            0  port_name7
         0            0
<=====================================================================
ESC:exit     F:refresh
U:page up    D:page down   L:page left  R:page right
```

- Port
  Displays the port numbers. Statistics for each port are displayed on one line.
- Link State/STP State
  Displays the port state in the Link State or STP State format.
  The Link State may indicate one of the following link states.
  - Down
    The port link is down.
  - Up
    The port link is up.

  The STP State indicates the current port status based on the STP (Spanning Tree Protocol).
  Note that the STP State is not displayed if the Link State is down.
  For port status details, see "Spanning Tree Protocol Port States".
- Flow-Ctl Mode
  Displays the flow control setup for each port.
  - Rx & Tx
    Both transmission and reception of pause frames are enabled.
  - Rx
    Only the reception of pause frames is enabled.
- Forward Counts
  Displays the accumulated number of frames forwarded normally (the unicast frames received at each port after the startup of this command).

- Flood Counts
  Displays the accumulated number of flooded frames among the unicast frames received at each port after the startup of this command.
- Rx-Pause Counts
  Displays the accumulated number of pause frames received at each port after the startup of this command.
- Tx-Pause Counts
  Displays the accumulated number of pause frames sent from each port after the startup of this command.
- Full-Drop Counts
  Displays the number of frames discarded due to the saturated port input buffer of the system after startup of this command.
- VLAN-Drop Counts
  Displays the number of frames discarded due to the reception of non-VLAN member frames that are not allowed to be forwarded among those received at each port after the startup of this command.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 29 characters can be displayed.

Output form (if "total" is specified)

```
xg# monitor dataflow total
Dataflow Statistics(Total Counts)                     2007/01/22-12:12:15
=========================================================================>
Port Link State/ Flow-Ctl Forward     Flood       Rx-Pause    Tx-Pause
     STP State   Mode     Counts      Counts      Counts      Counts
---- ----------- -------- ----------- ----------- ----------- -----------
   1 Up/Discard  Rx & Tx  1234567890  1234567890  1234567890  1234567890
   2 Down        Rx                0           0           0           0
   3 Up/Discard  Rx & Tx  1234567890K 1234567890K 1234567890K 1234567890K
   4 Up/Learn    Rx & Tx  1234567890M      25690M      25690M      25690M
   5 Up/Forward  Rx & Tx  1234567890G      25690G      25690G      25690G
   6 Up/Forward  Rx & Tx  1234567890T      25690T      25690T      25690T
   7 Down        Rx                0           0           0           0
   8 Down        Rx                0           0           0           0
=========================================================================>
ESC:exit     F:refresh
U:page up    D:page down    L:page left  R:page right
```

```
(continues)
Dataflow Statistics(Total Counts)   2007/01/22-12:12:15
<=========================================================
Full-Drop   VLAN-Drop   Port-Description
Counts      Counts
----------- ----------- ----------------------------
1234567890  1234567890   port_name1
         0           0  port_name2
1234567890K 1234567890K port_name3
     25690M      25690M port_name4
     25690G      25690G port_name5
     25690T      25690T port_name6
         0           0  port_name7
         0           0
<=========================================================
ESC:exit     F:refresh
U:page up    D:page down    L:page left  R:page right
```

The values displayed in the “Counts” column are the ones accumulated after the system startup. Other values are the same as those displayed if the “current” option were specified.

5.16.9 monitor error

Function

Displays error traffic statistics for each port.

Prompt

xg> or xg#

Command syntax

```
monitor error { current | total } [interval <3-60>]
```

Parameter

- { current | total }
  Specifies the statistics to be displayed.
  - current
    Displays the accumulated error count after startup of this command.
  - total
    Displays the accumulated error count after the system startup.

> Point
> If the error count reaches 4294967295, it is returned to 0 when incremented.

- interval <3-60>
  Specifies the update interval (in seconds).
  The default interval is 3 seconds.

Command type

Operation management command

Output form (if "current" is specified)

```
xg# monitor error current
Error Statistics(Current Counts)                                2007/01/22-12:12:15
===================================================================================>
Port Rx         Rx & Tx    Rx & Tx    Rx & Tx    Rx & Tx     Rx         Total
     CRC        Over       Under      Fragment   Jabber      Align      Lost
--- ---------- ---------- ---------- ---------- ---------- ---------- ----------
  1 1234567890 1234567890 1234567890 1234567890 1234567890 1234567890 1234567890
  2        123         12         34         34         56         78         90
  3        123         12         34         34         56         78         90
  4        123         12         34         34         56         78         90
  5        123         12         34         34         56         78         90
  6        123         12         34         34         56         78         90
  7        123         12         34         34         56         78         90
  8        123         12         34         34         56         78         90
==================================================================================>
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

```
(continues)
Error Statistics(Current Counts)                    2007/01/22-12:12:15
<======================================================================
Port-Description

------------------------------------
port_name1
port_name2
port_name3
port_name4
port_name5
port_name6
port_name7

<=======================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

- Port
  Displays the port numbers. Statistics for each port are displayed on one line.
- Rx CRC
  Displays the accumulated number of FCS (Frame Check Sequence) error frames received after startup of this command.
- Rx & Tx Over
  Displays the accumulated number of frames whose size exceeds 1518 bytes (excluding the VLAN tag) after startup of this command.
- Rx & Tx Under
  Displays the accumulated number of transmission frames whose size is less than 64 bytes after startup of this command.
- Rx & Tx Fragment
  Displays the accumulated number of FCS (Frame Check Sequence) error frames whose size is less than 64 bytes sent or received after startup of this command.
- Rx & Tx Jabber
  Displays the accumulated number of FCS (Frame Check Sequence) error frames whose size exceeds 1518 bytes (excluding the VLAN tag) sent or received after startup of this command.

- Rx Align
  Displays the accumulated number of 64- to 1518-byte alignment error frames whose bit size is not a multiple of 8 received after startup of this command.
- Total Lost
  Displays the accumulated number of frames received but discarded at each port after startup of this command.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 31 characters can be displayed.

Output form (if "total" is specified)

```
xg# monitor error total
Error Statistics(Total Counts)                                    2007/01/22-12:12:15
==================================================================================>
Port Rx        Rx & Tx    Rx & Tx    Rx & Tx    Rx & Tx    Rx          Total
     CRC       Over       Under      Fragment   Jabber     Align       Lost
---- --------  ---------  ---------  ---------  ---------  ---------   ----------
  1 1234567890 1234567890 1234567890 1234567890 1234567890 1234567890  1234567890
  2        123         12         34         34         56         78          90
  3        123         12         34         34         56         78          90
  4        123         12         34         34         56         78          90
  5        123         12         34         34         56         78          90
  6        123         12         34         34         56         78          90
  7        123         12         34         34         56         78          90
  8        123         12         34         34         56         78          90
==================================================================================>
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

```
(continues)
Error Statistics(Current Counts)                    2007/01/22-12:12:15
<======================================================================
Port-Description

------------------------------------
port_name1
port_name2
port_name3
port_name4
port_name5
port_name6
port_name7

<=======================================================================
ESC:exit    F:refresh
U:page up   D:page down   L:page left  R:page right
```

The displayed values are the ones accumulated after the system startup. Other values are the same as those displayed if the “current” option were specified.

5.16.10 show statistics traffic-bytes

Function

Displays the accumulated number of bytes sent or received to and from each port after the system startup.

Prompt

xg> or xg#

Command syntax

```
show statistics traffic-bytes
```

Command type

Operation management command

Output form

```
xg# show statistics traffic-bytes
Traffic Statistics(Total Frame Bytes)  2007/01/22-19:22:55
==========================================================
[No.1]
  Port                   : 1
  Link State/ STP State : Up/Forward
  Tx-Frame Bytes        : 71872
  Rx-Frame Bytes        : 63424
  Port-Description      : port_name1

[No.2]
  . . .
  . . .
```

- [No.]
  Displays statistics for each port.
- Port
  Displays the port numbers.
- Link State/STP State
  Displays the port state in the Link State or STP State format.
  The Link State may indicate one of the following link states.
  - Down
    The port link is down.
  - Up
    The port link is up.

  The STP State displays the current port status based on the STP (Spanning Tree Protocol).
  Note that the STP State is not displayed if the Link State is down.
  For port status details, see "Spanning Tree Protocol Port States".
- Tx-Frame Bytes
  Displays the accumulated number of bytes sent after the system startup.
- Rx-Frame Bytes
  Displays the accumulated number of bytes received after the system startup.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything.
  Up to 33 characters can be displayed.

5.16.11 show statistics traffic-counts

Function

Displays the accumulated number of frames sent or received to and from each port after the system startup.

Prompt

xg> or xg#

Command syntax

```
show statistics traffic-counts
```

Command type

Operation management command

Output form

```
xg# show statistics traffic-counts
Traffic Statistics(Total Frame Counts)    2007/01/22-19:41:39
=============================================================
[No.1]
 Port                 : 1
 Link State/ STP State: Up/Forward
 Tx-Frame Counts      : 367
 Rx-Frame Counts      : 300
 Rx-Bcast Counts      : 0
 Rx-Mcast Counts      : 300
 Port-Description     : port_name1

[No.2]
  . . .
  . . .
```

- [No.]
  Displays statistics for each port.
- Port
  Displays the port numbers.
- Link State/STP State
  Displays the port state in the Link State or STP State format.
  The Link State may indicate one of the following link states.
  - Down
    The port link is down.
  - Up
    The port link is up.

  The STP State displays the current port status based on the STP (Spanning Tree Protocol).
  Note that the STP State is not displayed if the Link State is down.
  For port status details, see "Spanning Tree Protocol Port States".
- Tx-Frame Counts
  Displays the accumulated number of frames sent after the system startup.
- Rx-Frame Counts
  Displays the accumulated number of frames received after the system startup.
- Rx-Bcast Counts
  Displays the accumulated number of broadcast frames received after the system startup.
- Rx-Mcast Counts
  Displays the accumulated number of multicast frames received after the system startup.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything.
  Up to 36 characters can be displayed.

5.16.12 show statistics framesize-traffic-counts

Function

Displays traffic statistics for each port in different frame size groups.

Prompt

xg> or xg#

Command syntax

```
show statistics framesize-traffic-counts
```

Command type

Operation management command

Output form

```
xg# show statistics framesize-traffic-counts
Framesize Traffic Statistics(Total Frame Counts)  2007/01/22-19:44:11
=====================================================================
[No.1]
 Port                 : 1
 Link State/ STP State: Up/Forward
 FrameSize 0-64       : 805
 FrameSize 65-127      : 0
 FrameSize 128-255     : 0
 FrameSize 256-511     : 0
 FrameSize 512-1023    : 0
 FrameSize 1024-1518   : 0
 Port-Description       : port_name1

[No.2]
  . . .
  . . .
```

- [No.]
  Displays statistics for each port.
- Port
  Displays the port numbers.
- Link State/STP State
  Displays the port state in the Link State or STP State format.
  The Link State may indicate one of the following link states.
  - Down
    The port link is down.
  - Up
    The port link is up.

  The STP State displays the current port status based on the STP (Spanning Tree Protocol).
  Note that the STP State is not displayed if the Link State is down.
  For port status details, see "Spanning Tree Protocol Port States".
- FrameSize 0-64
  Displays the accumulated number of 64-byte frames sent or received at each port after the system startup.
- FrameSize 65-127
  Displays the accumulated number of 65- to 127-byte frames sent or received at each port after the system startup.
- FrameSize 128-255
  Displays the accumulated number of 128- to 255-byte frames sent or received at each port after the system startup.
- FrameSize 256-511
  Displays the accumulated number of 256- to 511-byte frames sent or received at each port after the system startup.
- FrameSize 512-1023
  Displays the accumulated number of 512- to 1023-byte frames sent or received at each port after the system startup.
- FrameSize 1024-1518
  Displays the accumulated number of 1024- to 1518-byte frames sent or received at each port after the system startup.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything.
  Up to 44 characters can be displayed.

5.16.13 show statistics qos-priority-traffic-bytes

Function

Displays the traffic (the number of frames) for each port with different QoS priorities after system startup.

Prompt

xg> or xg#

Command syntax

```
show statistics qos-priority-traffic-bytes
```

Command type

Operation management command

Output form

```
xg# show statistics qos-priority-traffic-bytes
Qos Priority Traffic Statistics(Total Frame Bytes)  2007/01/22-19:46:24
======================================================================
[No.1]
 Port              : 1
 Priority-0 Bytes : 26560
 Priority-1 Bytes : 145366784370
 Priority-2 Bytes : 234554675423423
 Priority-3 Bytes : 34346331246523
 Priority-4 Bytes : 1234114235453466
 Priority-5 Bytes : 0
 Priority-6 Bytes : 0
 Priority-7 Bytes : 0
 Port-Description : port_name1

[No.2]
  ・・・
  ・・・
```

- [No.]
  Displays statistics for each port.
- Port
  Displays the port numbers.
- Priority-0 Bytes to Priority-7 Bytes
  Displays the accumulated number of frames with different QoS priorities received from the startup of this command.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 51 characters can be displayed.

5.16.14 show statistics qos-priority-traffic-counts

Function

Displays the traffic (the number of frames) for each port with different QoS priorities after system.

Prompt

xg> or xg#

Command syntax

```
show statistics qos-priority-traffic-counts
```

Command type

Operation management command

Output form

```
xg# show statistics qos-priority-traffic-counts
Qos Priority Traffic Statistics(Total Frame Counts)  2007/01/22-19:49:53
========================================================================
[No.1]
 Port                : 1
 Priority-0 Counts : 12345678901234567890
 Priority-1 Counts : 2354235234
 Priority-2 Counts : 235434250
 Priority-3 Counts : 12314657
 Priority-4 Counts : 235477689352374
 Priority-5 Counts : 246364564564546
 Priority-6 Counts : 1234453456
 Priority-7 Counts : 1436434623
 Port-Description  : port_name1
[No.2]
  . . .
  . . .
```

- [No.]
  Displays statistics for each port.
- Port
  Displays the port numbers.
- Priority-0 Counts to Priority-7 Counts
  Displays the accumulated number of frames with different QoS priorities received from the startup of this command.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 51 characters can be displayed.

5.16.15 show statistics vlan-traffic-bytes

Function

Displays the traffic (the number of bytes) for each VLAN after system startup.

Prompt

xg> or xg#

Command syntax

```
show statistics vlan-traffic-bytes
```

Command type

Operation management command

Output form

```
xg# show statistics vlan-traffic-bytes
VLAN Traffic Statistics(Total Frame Bytes)  2007/01/22-19:55:34
===============================================================
[No.1]
 VID              : 40
 Rx-Frame Byte    : 0
 Rx-NonUcast Byte: 0
[No.2]
  . . .
  . . .
```

- [No.]
  Displays statistics for each VLAN.
- VID
  Displays the VID of the VLAN set for statistics collection.

  > Point
  >
  > Specify the VLAN for statistics collection using the "vlan-statistics collection" command.

- Rx-Frame Bytes
  Displays the accumulated byte count of frames received at the specified VLAN (after the startup of this command), using a 10-digit, right-justified value.
- Rx-NonUcast Bytes
  Displays the accumulated byte count of multicast/broadcast frames received at the specified VLAN after the startup of this command, using a 10-digit, right-justified value.

5.16.16 show statistics vlan-traffic-counts

Function

Displays the traffic (the number of frames) for each VLAN after system startup.

Prompt

xg> or xg#

Command syntax

```
show statistics vlan-traffic-counts
```

Command type

Operation management command

Output form

```
xg# show statistics vlan-traffic-counts
VLAN Traffic Statistics(Total Frame Counts)  2007/01/22-19:58:31
================================================================
[No.1]
  VID                 : 40
  Rx-Frame Counts     : 0
  Rx-NonUcast Counts: 0
[No.2]
  . . .
  . . .
```

- [No.]
  Displays statistics for each VLAN.
- VID
  Displays the VID of the VLAN set for statistics collection.

  > Point
  > Specify the VLAN for statistics collection using the "vlan-statistics collection" command.

- Rx-Frame Counts
  Displays the accumulated count of frames received at the specified VLAN (after the system startup), using a 10-digit, right-justified value.
- Rx-NonUcast Counts
  Displays the accumulated count of non-unicast frames received at the specified VLAN after the system startup, using a 10-digit, right-justified value.

5.16.17 show statistics dataflow

Function

Displays statistics including the transmission and reception of pause frames at each port and the data transmission type.

Prompt

xg> or xg#

Command syntax

```
show statistics dataflow
```

Command type

Operation management command

Output form

```
xg# show statistics dataflow
Dataflow Statistics(Total Counts)  2007/01/22-19:59:17
[No.1]
 Port                   : 1
 Link State/ STP State: Up/Forward
 Flow-Ctl Mode          : disabled
 Forward Counts         : 0
 Flood Counts           : 0
 Rx-Pause Counts        : 0
 Tx-Pause Counts        : 0
 Full-Drop Counts       : 0
 VLAN-Drop Counts       : 0
 Port-Description       : port_name1

[No.2]
  . . .
  . . .
```

- [No.]
  Displays statistics for each port.
- Port
  Displays the port numbers.
- Link State/STP State
  Displays the port state in the Link State or STP State format.
  The Link State may indicate one of the following link states.
  - Down
    The port link is down.
  - Up
    The port link is up.

  The STP State displays the current port status based on the STP (Spanning Tree Protocol).
  Note that the STP State is not displayed if the Link State is down.
  For port status details, see "Spanning Tree Protocol Port States".
- Flow-Ctl Mode
  Displays the flow control setup for each port.
  - Rx & Tx
    Both transmission and reception of pause frames are enabled.
  - Rx
    Only the reception of pause frames is enabled.
- Forward Counts
  Displays the accumulated number of frames forwarded normally (among the unicast frames received at each port after the system startup).
- Flood Counts
  Displays the accumulated number of flooded frames (among the unicast frames received at each port after the system startup).
- Rx-Pause Counts
  Displays the accumulated number of pause frames received at each port after the system startup.
- Tx-Pause Counts
  Displays the accumulated number of pause frames sent from each port after the system startup.
- Full-Drop Counts
  Displays the number of frames discarded due to the saturated port input buffer of the system after the system startup.
- VLAN-Drop Counts
  Displays the number of frames discarded due to the reception of non-VLAN member frames that are not allowed to be forwarded among those received at each port after the system startup.
- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 29 characters can be displayed.

5.16.18 show statistics error

Function

Displays statistics for errors occurring at each port after system startup.

Prompt

xg> or xg#

Command syntax

```
show statistics error
```

Command type

Operation management command

Output form

```
xg# show statistics error
Error Statistics(Total Counts)  2007/01/22-20:21:35
===================================================
[No.1]
 Port               : 1
 Rx CRC             : 0
 Rx & Tx Over       : 0
 Rx & Tx Under      : 0
 Rx & Tx Fragment   : 0
 Rx & Tx Jabber     : 0
 Rx Align           : 0
 Total Lost         : 0
 Port-Description   : port_name1

[No.2]
  . . .
  . . .
```

- [No.]
  Displays statistics for each port.
- Port
  Displays the port numbers.
- Rx CRC
  Displays the accumulated number of FCS (Frame Check Sequence) error frames received after the system startup.
- Rx & Tx Over
  Displays the accumulated number of transmission frames whose size exceeds 1518 bytes (excluding the VLAN tag) after the system startup.
- Rx & Tx Under
  Displays the accumulated number of transmission frames whose size is less than 64 bytes after the system startup.
- Rx & Tx Fragment
  Displays the accumulated number of FCS (Frame Check Sequence) error frames whose size is less than 64 bytes sent or received after the system startup.
- Rx & Tx Jabber
  Displays the accumulated number of FCS (Frame Check Sequence) error frames whose size exceeds 1518 bytes (excluding the VLAN tag) sent or received after the system startup.
- Rx Align
  Displays the accumulated number of 64- to 1518-byte alignment error frames whose bit size is not a multiple of 8 received after the system startup.
- Total Lost
  Displays the accumulated number of frames received but discarded at each port after the system startup.

> Point
>
> If the error count reaches 4294967295, the value is reset to 0 when incremented.

- Port-Description
  Displays port descriptions. If the port is not described, it will not display anything. Up to 31 characters can be displayed.

5.16.19 clear statistics

Function

Clears all statistics stored since system startup.
The following statistics are cleared.

- Traffic statistics: traffic-bytes, traffic-counts and framesize-traffic-counts
- QoS traffic statistics: qos-priority-traffic-bytes and qos-priority-traffic-counts
- VLAN traffic statistics: vlan-traffic-bytes and vlan-traffic-counts
- Data flow statistics: dataflow
- Error traffic statistics: error

Prompt

xg#

Command syntax

```
clear statistics
```

Command type

Operation management command

Note

- If this command is issued during execution of the “monitor” command in “current” mode, the “monitor” command may temporarily display incorrect statistics. If this occurs, reissue the “monitor” command. The “monitor” command will then display the correct statistics.

Example

Clear all statistics stored since system startup.

```
xg# clear statistics
```

5.17 SNMP Setup Commands

This section explains the SNMP configuration settings.

5.17.1 show snmp-server

Function

Displays the current SNMP settings.

Prompt

xg> or xg#

Command syntax

```
show snmp-server
```

Command type

Operation management command

Output form

```
xg# show snmp-server
SNMP Information                                     2007/01/22-06:04:41
================================================================================
SNMP Manager Information
--------------------------------------------------------------------------------
[No.1]
  Host      : 192.168.41.24
  Community : public
[No.2]
  Host      : 192.168.41.29
  Community : public
--------------------------------------------------------------------------------

SNMP Trap Manager Information
--------------------------------------------------------------------------------
[No.1]
  Host      : 192.168.41.24
  Community : public
  Version   : { v1 | v2c }
[No.2]
  Host      : 192.168.41.29
  Community : public
  Version   : { v1 | v2c }
================================================================================
```

SNMP Manager Information

Displays the current settings of the SNMP manager.

- [No.1]
  Indicates the number of the SNMP manager displayed. A maximum of four may be defined.
- Host
  Displays the host name or the IP address of the SNMP manager.
- Community
  Displays the community name of the SNMP manager.

SNMP Trap Manager Information

Displays the destination SNMP trap being set from the system.

- [No.1]
  Indicates the number of the SNMP trap item displayed.
- Host
  Displays the host name or the IP address of the SNMP manager for trap notification.
- Community
  Displays the community name of the SNMP manager for trap notification.
- Version
  Displays the SNMP protocol version to be used for trap notification as follows:
  - v1
    The SNMP v1 protocol is used for trap notification.
  - v2c
    The SNMP v2c protocol is used for trap notification.

5.17.2 snmp-server location

Function

Sets the installation location for the device.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
snmp-server location SYSTEM-LOCATION
no snmp-server location
```

Parameter

- SYSTEM-LOCATION

  Specifies the installation location of the device. The location name can be up to 255 alphanumeric characters.
  No need to enclose a parameter in quotes if it contains a blank space.

Command type

Configuration command

Default

None

Message

% SYSTEM-LOCATION is too long.

Explanation

The location name specified by SYSTEM-LOCATION exceeded the length limit.

Solution

Reduce the length of system location name and reissue the command.

% SYSTEM-LOCATION cannot be used.

Explanation

An illegal character was used in the SYSTEM-LOCATION name.

Solution

Review the system location name setting and reissue the command.

Example

Specify the system installation location as “3F West”:

```
xg(config)# snmp-server location 3F West
```

5.17.3 snmp-server contact

Function

Sets the installation contact name for the device.
Use the no form to return to the default setup.

Prompt

xg(config)#

Command syntax

```
snmp-server contact SYSTEM-CONTACT
no snmp-server contact
```

Parameter

- SYSTEM-CONTACT

  Specifies the system contact name for the device. The contact name can be up to 255 alphanumeric characters.
  No need to enclose a parameter in quotes if it contains a blank space.

Command type

Configuration command

Default

None

Message

% SYSTEM-CONTACT is too long.

Explanation

The contact name specified by "SYSTEM-CONTACT" exceeded the length limit.

Solution

Reduce the length of the system contact name and reissue the command.

% SYSTEM-CONTACT cannot be used.

Explanation

An illegal character was used in the "SYSTEM-CONTACT" name.

Solution

Review the system contact name setting and reissue the command.

Example

Specify the system contact address as “administrator tel: 012-3456-7890.”

```
xg(config)# snmp-server contact administrator tel:012-3456-7890
```

5.17.4 snmp-server access

Function

Sets an SNMP agent. The SNMP manager has read-only access privileges. Up to four access-enabled SNMP managers can be registered.
Use the no form to delete the existing SNMP managers.

Prompt

xg(config)#

Command syntax

```
snmp-server access host HOSTNAME community COMMUNITY-NAME
no snmp-server access host HOSTNAME
```

Parameter

- host HOSTNAME
  Specifies the host name or the IP address of the SNMP manager.
  The IP address can be within the range of 1.0.0.1 to 126.255.255.254, 128.0.0.1 to 191.255.255.254, or 192.0.0.1 to 223.255.255.254.
- community COMMUNITY-NAME
  Specifies a community name for the SNMP manager. The community name can be up to 255 alphanumeric characters.

Command type

Configuration command

Default

None

Message

```
% SNMP Manager can register up to 4.
```

Explanation

Four SNMP managers have already been registered.

Solution

Delete unnecessary SNMP managers then reissue the command.

```
% Cannot find %1$
```

Explanation

The name cannot be resolved. An incorrect host name was specified.
[[Inserted string]]%1$: Specified host name

Solution

Review the host name then reissue the command by specifying a correct host name or IP address.

```
% Hostname is too long.
```

Explanation

The specified host name exceeded the length limit.

Solution

Reduce the host name length then reissue the command.

```
% COMMUNITY-NAME is too long.
```

Explanation

The specified community name exceeded the length limit.

Solution

Reduce the community name length then reissue the command.

```
% COMMUNITY-NAME cannot be used.
```

Explanation

An illegal character was used in the community name.

Solution

Review the community name setting then reissue the command.

```
% Invalid IP-address.
```

Explanation

The IP address was specified in an incorrect format or an incorrect address was specified.

Solution

Specify the correct IP address in the correct format then reissue the command.

Note

- If a previously defined host name is specified with a new community name the prior community name is overwritten.
- If the host name is specified instead of IP address, changing the NTP server's IP address at SNMP manager will not be enabled. It is necessary to restart the device after DNS server's IP address has been changed.
- The following message might be output if there is a SNMP request from a SNMP manager when the device is starting up and in the process of executing initial settings. It is not necessary to review the SNMP permission in this case. .
  - XG INFO[S8500]: SNMP authentication failure.

Example

Allow access from the SNMP manager having the IP address "192.168.1.10" and the community name "xgpublic".

```
xg(config)# snmp-server access host 192.168.1.10 community xgpublic
```

5.17.5 snmp-server trap

Function

Sets the destination for SNMP trap notifications. Up to four (4) destinations can be registered.
Use the no form to delete the existing destination names.

Prompt

xg(config)#

Command syntax

```
snmp-server trap host HOSTNAME community COMMUNITY-NAME [ protocol {v1|v2c} ]
no snmp-server trap host HOSTNAME
```

Parameter

- host HOSTNAME
  Specifies a host name or an IP address for the destination SNMP manager.
  The IP address can be within the range of 1.0.0.1 to 126.255.255.254, 128.0.0.1 to 191.255.255.254, or 192.0.0.1 to 223.255.255.254.
- community COMMUNITY-NAME
  Specifies a community name for the destination SNMP manager. The community name can be up to 255 alphanumeric characters.
- [protocol {v1|v2c}]
  Specifies the SNMP protocol to be used.
  - v1
    The SNMP v1 protocol is used for trap notification.
  - v2c
    The SNMP v2c protocol is used for trap notification.

  The SNMP v2c protocol is the default if not specified.

Command type

Configuration command

Default

None

Message

% SNMP Trap Manager can register up to 4.

Explanation

Four SNMP trap managers have already been registered.

Solution

Delete unnecessary SNMP trap managers then reissue the command.

% Cannot find %1$

Explanation

The name cannot be resolved. An incorrect host name was specified.
[[Inserted string]]%1$: Specified host name

Solution

Review the host name then reissue the command by specifying the correct hostname or IP address.

% Hostname is too long.

Explanation

The specified host name exceeded the length limit.

Solution

Reduce the host name length then reissue the command.

% COMMUNITY-NAME is too long.

Explanation

The specified community name exceeded the limit length.

Solution

Review the community name length then reissue the command.

% COMMUNITY-NAME cannot be used.

Explanation

An illegal character was used in the community name.

Solution

Review the community name setting then reissue the command.

% Invalid IP-address.

Explanation

The IP address was specified in an incorrect format or an incorrect address was specified.

Solution

Specify the correct IP address in the correct format then reissue the command.

Note

- If a previously defined host name is specified with new parameters the prior parameters are overwritten.
- If the host name is specified instead of IP address of the destination for SNMP trap notifications, changing the NTP server's IP address at the destination for SNMP trap notifications will not be enabled. It is necessary to restart the device after DNS server's IP address has been changed.

Example

Specify trap notification using the SNMP v2c protocol for the SNMP manager with the IP address “192.168.1.10” and the community name “xgpublic”.

```
xg(config)# snmp-server trap host 192.168.1.10 community xgpublic protocol v2c
```

5.18 RMON Setup Commands

This section explains the RMON configuration settings.

5.18.1 show rmon

Function

Displays the current RMON settings.

Prompt

xg> or xg#

Command syntax

```
show rmon
```

Command type

Operation management command

Output form

```
xg# show rmon
RMON Information                                    2007/01/22-06:03:09
=============================================================================
History Information
-----------------------------------------------------------------------------
[History 1]
  Port    : port-1
  Buckets : 10
  Interval: 1800
  Owner   : Administer
-----------------------------------------------------------------------------
Alarm Information
-----------------------------------------------------------------------------
[Alarm 1]
  Monitored OID      : .1.3.6.1.2.1.16.1.1.1.7.1
  Monitoring Interval: 10
  Sample Type        : { Absolute | Delta }
  Rising Threshold   : 1000
  Rising Event       : 1
  Falling Threshold  : 0
  Falling Event      : 0
  Owner              : Administer
-----------------------------------------------------------------------------

Event Information
-----------------------------------------------------------------------------
[Event 1]
  Event Type
    Log          : { Enabled | Disabled }
    Trap         : { Enabled | Disabled }
  Trap Community : public
  Description    : Traffic alarm event
  Owner          : Admin
=============================================================================
```

History Information

Displays the current RMON history settings.

- [History 1]
  Indicates an index number that identifies the history group (historyControlTable).
- Port
  Displays the port number for the collected RMON history group information.
- Buckets
  Indicates the stored data unit count for the RMON history group.
- Interval
  Indicates an interval (in seconds) for collecting the RMON history group data.
- Owner
  Displays the owner name of the RMON history group.

Alarm Information

Displays the current RMON alarm settings.

- [Alarm 1]
  Indicates a unique ID assigned to the RMON alarm.
- Monitored OID
  Indicates an OID within the MIB object to be monitored.
- Monitoring Interval
  Indicates an interval (in seconds) for threshold check of the MIB to be monitored.
- Sample Type
  Displays the threshold evaluation method.
  - Absolute
    The value obtained from the MIB is evaluated based on the absolute value.
  - Delta
    The difference between the value obtained from the previous MIB and the value obtained from the current MIB is evaluated.

- Rising Threshold
  Indicates the threshold upper limit (or the rising threshold).
- Rising Event
  Indicates a number for the event notification if the value obtained exceeded the threshold limit.
  Event does not occur if the value is 0.
- Falling Threshold
  Indicates the threshold lower limit (or the falling threshold).
- Falling Event
  Indicates a number for the event notification if the value obtained dropped below the threshold limit.
  Event does not occur if the value is 0.
- Owner
  Displays the owner name of the RMON alarm group.

Event Information

Displays the contents of the RMON event.

- [Event 1]
  Indicates an index number that identifies the RMON event entry.
- Event Type
  log
  Displays the status of the RMON log entry creation when a RMON event occurred.
  - Enabled
    A RMON log entry was created.
  - Disabled
    No RMON log entry was created.

  Trap
  Displays the trap notification status.
  - Enabled
    SNMP trap notification occurs.
  - Disabled
    No SNMP trap notification occurs.
- Trap Community
  Displays a community name for the SNMP trap.
- Description
  Displays a character string that explains the RMON event entry.
- Owner
  Displays the owner name of the RMON event entry.

5.18.2 rmon collection history

Function

Sets an RMON history. Up to 40 entries can be set.
Use the no form to delete the information set.

Prompt

xg(config)#

Command syntax

```
rmon collection history INDEX { port <1-20> | agg-port <1-10> }
 [buckets BUCKET-NUM] [interval SECOND] [owner OWNERNAME]

no rmon collection history INDEX
```

Parameter

- INDEX
  Specifies an entry index number for the history within the range of 1 to 65535.
- port <1-20>
  Specifies a port number for collection of the RMON history group.
- agg-port <1-10>
  Specifies an aggregation group number for collecting of the RMON history group.
- buckets BUCKET-NUM
  Specifies the data storage unit count of the RMON history entry group within the range of 1 to 20.
  If omitted, the default storage count is 10 data sets.
- interval SECOND
  Specifies a time interval for collecting the RMON history group data within the range of 1 to 3600 seconds.
  If omitted, the default interval is 1800 seconds (or 30 minutes).
- owner OWNERNAME
  Specifies an owner name of the entry using up to 127 characters.
  If omitted, no owner name is set.

Command type

Configuration command

Default

None

Message

% RMON collection history can register up to 40

Explanation

The RMON history group data entry registration limit was exceeded.

Solution

Delete unnecessary RMON history groups then reissue the command.

% RMON collection history %1$ is not set.

Explanation

An attempt was made to delete a non-existing RMON history group.
[[Inserted string]]%1$: Index number

Solution

Review the specified index then reissue the command.

% OWNERNAME is too long.

Explanation

The specified “ownername” exceeded the length limit.

Solution

Reduce the “ownername” length then reissue the command.

% Agg-port %1$ does not exist

Explanation

The specified aggregation group was not created.
[[Inserted string]]%1$: Specified aggregation group number

Solution

Review the “agg-port” settings then reissue the command.

% OWNERNAME cannot be used.

Explanation

An illegal character was specified in the "ownername".

Solution

Review the specified “ownername” then reissue the command.

% It failed in the snmpset command.

Explanation

It fails to set RMON because the command was executed while the SNMP manager was accessing.

Solution

While the SNMP is not accessing, execute the no command and set RMON again.

Example

Set the data collection interval to 30 minutes (default value) and the data storage count to 20 data sets for the RMON history for port 1. The 10-hour history statistics will be logged.

```
xg(config)# rmon collection history 1 port 1 buckets 20
```

5.18.3 rmon alarm

Function

Sets RMON alarms. Up to 30 entries can be set.
Use the no form to delete entries previously set.

Prompt

xg(config)#

Command syntax

```
rmon alarm INDEX VARIABLE interval VALUE {absolute | delta}
 rising-threshold VALUE [EVENT-NUM]  falling-threshold VALUE [EVENT-NUM]
 [owner OWNERNAME]

no rmon alarm INDEX
```

Parameter

- INDEX
  Specifies an entry index number for the RMON alarm within the range of 1 to 65535.
- VARIABLE
  Specifies an OID for the MIB object to be monitored.
  A name such as “ifEntry.10.2” cannot be set for the OID. The OID must be a string of decimal integers separated by a period (.). An example: “1.3.6.1.2.1.1.2.2.1.10.2”.
- interval VALUE
  Specifies an interval (in seconds) for threshold checks on the MIB to be monitored. The VALUE can be an integer of 2 to 65535.
- {absolute | delta}
  Specifies a threshold evaluation method as follows.
  - absolute
    The value obtained from the MIB is evaluated based on the absolute value.
  - delta
    The difference between the value obtained from the previous MIB and the value obtained from the current MIB is evaluated.
- rising-threshold VALUE [EVENT-NUM]
  The VALUE specifies the threshold upper limit or the “rising threshold”.
  The EVENT-NUM specifies an index for the event to be executed if the rising threshold is exceeded.
  If EVENT-NUM is omitted, event will not occur.
- falling-threshold VALUE [EVENT-NUM]
  The VALUE specifies the threshold lower limit or the “falling threshold”.
  The EVENT-NUM specifies an index for the event to be executed if the falling threshold is exceeded.
  If EVENT-NUM is omitted, event will not occur.
- owner OWNERNAME
  Specifies an owner name for the entry using up to 127 alphanumeric characters.
  If omitted, no owner name is set.

Command type

Configuration command

Default

None

Message

% RMON alarm can register up to 30

Explanation

The RMON alarm group data entry registration limit was exceeded.

Solution

Delete unnecessary RMON alarm groups then reissue the command.

% RMON alarm %1$ is not set.

Explanation

An attempt to delete a non-existing RMON alarm group occurred.
[[Inserted string]]%1$: Specified index

Solution

Review the specified index then reissue the command.

% OWNERNAME is too long.

Explanation

The “ownername” length limit was exceeded.

Solution

Reduce the “ownername” length then reissue the command.

% OID cannot be used.

Explanation

An illegal character was specified in the OID.

Solution

Review the specified OID then reissue the command.

% OWNERNAME cannot be used.

Explanation

An illegal character was specified in the "ownername".

Solution

Review the specified “ownername” then reissue the command.

```
% It failed in the snmpset command.
```

Explanation

It fails to set RMON because the command was executed while the SNMP manager was accessing.

Solution

While the SNMP is not accessing, execute the no command and set RMON again.

Example

Set RMON alarms:

```
xg(config)# rmon alarm 10 .1.3.6.1.2.1.16.1.1.1.7.1 interval 60 absolute
          rising-threshold 15 1 falling-threshold 0 1 owner "admin"
```

5.18.4 rmon event

Function

Sets an RMON event. Up to 60 entries can be set.
Use the no form to delete the information set.

Prompt

xg(config)#

Command syntax

```
rmon event INDEX [ log ] [ trap COMMUNITY ] [ description DESCRIPTION-STRING ]
 [owner OWNERNAME]

no rmon event INDEX
```

Parameter

- INDEX
  Specifies an entry index number for the RMON event within the range of 1 to 65535.
- log
  Delete unnecessary RMON events then reissue the command.
- trap COMMUNITY
  This option notifies a trap if an event occurred. The COMMUNITY name can be up to 127 alphanumeric characters.
  If omitted, no traps are notified.
- description DESCRIPTION-STRING
  Specifies a character string that explains the events. The description string can be up to 127 alphanumeric characters.
- owner OWNERNAME
  Specifies an owner name for the entry using up to 127 alphanumeric characters.
  If omitted, no owner name is set.

Command type

Configuration command

Default

None

Message

```
% RMON event can register up to 60
```

Explanation

The RMON event group data entry registration limit was exceeded.

Solution

Delete unnecessary RMON events then reissue the command.

```
% RMON event %1$ is not set.
```

Explanation

An attempt to delete a non-existing RMON event group occurred.
[[Inserted string]]%1$: Specified index

Solution

Review the specified index then reissue the command.

```
% OWNERNAME is too long.
```

Explanation

The “ownername” length limit was exceeded.

Solution

Reduce the “ownername” length then reissue the command.

```
% COMMUNITY is too long.
```

Explanation

The specified “community” name length limit was exceeded.

Solution

Reduce the “community” name length then reissue the command.

```
% DESCRIPTION is too long.
```

Explanation

The “description” specified exceeded the length limit.

Solution

Review the “description” length and reissue the command.

```
% COMMUNITY cannot be used.
```

Explanation

An illegal character was specified in the “community” name.

Solution

Review the specified “community” name then reissue the command.

```
% DESCRIPTION cannot be used.
```

Explanation

An illegal character was specified in the "description".

Solution

Review the specified “description” then reissue the command.

```
% OWNERNAME cannot be used.
```

Explanation

An illegal character was specified in the "ownername".

Solution

Review the specified “ownername” then reissue the command.

```
% It failed in the snmpset command.
```

Explanation

It fails to set RMON because the command was executed while the SNMP manager was accessing.

Solution

While the SNMP is not accessing, execute the no command and set RMON again.

Note

An RMON event entry must be created using the "rmon event" command for log creation or SNMP trap notification to occur.

Example

Set RMON events:

```
xg(config)# rmon event 1 log trap public description "event test1" owner "admin"
xg(config)# rmon event 2 log description "event test2" owner "admin"
```

5.19 System Operation Display Commands

This section explains commands that display the system's operational status.

5.19.1 show system status

Function

Displays the hardware operational status.
For explanations and actions to be taken for each item, see the "Verifying Hardware Status".

Prompt

xg> or xg#

Command syntax

```
show system status
```

Command type

Operation management command

Output form

```
xg# show system status
System Status Information  2007/01/25-12:16:19
==============================================
[Temperature]
   Internal      : good

[Power Supply]
  PWR-0 (AC)       : good
  PWR-1 (AC)       : good

[Voltage]
   Voltage        : good

[Fan]
   Rear Fan-0     : good (normal-speed)
   Rear Fan-1     : good (normal-speed)
   PWR-0 Fan      : good
   PWR-1 Fan      : good

[XFP]
   port  1 (VENDER-NAME.    :S  ) : good
   port  2 (VENDER-NAME.    :L  ) : good
   port  3 (VENDER-NAME.    :S  ) : good
   port  4 (VENDER-NAME.    :L  ) : good
   port  5 (VENDER-NAME.    :S  ) : good
   port  6 (VENDER-NAME.    :L  ) : good
   port  7 (VENDER-NAME.    :S  ) : good
   port  8 (VENDER-NAME.    :L  ) : good
   port  9 (VENDER-NAME.    :S  ) : good
   port 10 (VENDER-NAME.    :L  ) : good
   port 11 (VENDER-NAME.    :S  ) : good
   port 12 (VENDER-NAME.    :L  ) : good
   port 13 (VENDER-NAME.    :S  ) : good
   port 14 (VENDER-NAME.    :L  ) : good
   port 15 (VENDER-NAME.    :S  ) : good
   port 16 (VENDER-NAME.    :L  ) : good
   port 17 (VENDER-NAME.    :S  ) : good
   port 18 (VENDER-NAME.    :L  ) : good
   port 19 (VENDER-NAME.    :S  ) : good
   port 20 (VENDER-NAME.    :L  ) : good
```

- Temperature
  Displays the temperature status of the system hardware.
  - Internal
    Internal temperature sensor
- Power Supply
  Displays the operational status of the power supplies.
  - PWR-0
    Displays the operational status of power supply 0.
  - PWR-1
    Displays the operational status of power supply 1.
- Voltage
  Displays the supply voltage status. If all the voltages are normal, no information is displayed.
  - VDP
    Displays the VDP voltage status.
  - VDE
    Displays the VDE voltage status.
  - VDR
    Displays the VDR voltage status.
  - VDD
    Displays the VDD voltage status.
  - VDN
    Displays the VDN voltage status.

  - 1.5V
    Displays the 1.5V voltage status on the CPU board.
  - 3.3V
    Displays the 3.3V voltage status on the CPU board.
  - 12V
    Displays the 12V voltage status on the CPU board.
  - 3.3V
    Displays the 3.3V voltage status on the switch ASIC board.
  - 12V
    Displays the 12V voltage status on the switch ASIC board.

- Fan
  Displays the fan operational status.
  - Rear Fan-0
    Displays the operational status of rear fan 0.
  - Rear Fan-1
    Displays the operational status of rear fan 1.
  - PWR-0 Fan
    Displays the operational status of the fan mounted in power supply 0.
  - PWR-1 Fan
    Displays the operational status of the fan mounted in power supply 1.
- XFP
  Displays the XFP status for each port.
  - port xx (yy-zz)
    Displays the XFP status of port xx. The vender name, yy, and PHY type, zz, are also displayed.
    The number of displayed ports is depend on the device. 20 ports are displayed for XG2000 and XG2000R and 4 ports for XG2000C and XG2000CR.

5.19.2 show system information

Function

Displays the operational status of the device.

Prompt

xg> or xg#

Command syntax

```
show system information
```

Command type

Operation management command

Output form

```
xg# show system information
System Information  2007/01/22-21:06:11
=======================================
 System Name (hostname) : xg
 System Location        : (none)
 System Contact         : (none)
 Default Banner         : XG2000 E10L11 Z01
 Startup Time           : 2007/01/22-19:28:24
 Startup-config Modified : 2007/01/22-19:54:01
 Firmware Information
  Firmware[1]           : E10L10 Z01 2007/01/21-18:42:52
   Updated Time         : 2007/01/21-22:08:12
  Firmware[2]           : E10L11 Z01 2007/01/22-19:27:12
   Updated Time         : 2007/01/23-10:57:53
  Current Firmware      : [2]
  Next Startup Firmware : [2]
  Boot Loader           : E10L10 Z01
 Timezone               : gmt +0900
  (Next Boot)           : gmt -800
 Summer-Time            : (none)
  (Next Boot)           : M4.1.0/0200 M10.5.0/0200 0100
 RS232C Baud-Rate       : 9600
 Management LAN Information
  MAC Address           : 0080.17c2.0500
  IP Address/Mask       : 192.168.41.22/24
  Default Gateway       : 192.168.41.1
  DNS Server            : 192.168.77.20
  Domain Name           : abc.efg.com
 System Load Information
  CPU Used Ratio        : 1%
  Memory Used Size      : 36,429,824 bytes (57%)
```

- System Name (hostname)
  Displays the system name (host name) of the device.
- System Location
  Displays the installation location of the device.
- System Contact
  Displays the contact information of the device.
- Default Banner
  Displays the default banner string displayed during user login.
- Startup Time
  Displays the date and time when the system was started up.
- Startup-config Modified
  Displays the date and time when the “startup-config” setup was last updated.
- Firmware Information
  Displays the firmware status of the device.
  The system retains up to two sets of firmware information (old and new firmware information) and firmware images.
  - Firmware[1] / Firmware[2]
    Displays the firmware information of firmware partitions 1 and 2 and the firmware update status.
    (No display other than revision and revision date)
    The new firmware is not being updated.
    (writing)
    The new firmware is being updated.
    (new)
    The firmware was updated.
    (incomplete)
    The switch fails to update the new firmware.
    Retry to update the new firmware.
  - Updated Time
    Displays the date and time when the firmware was last updated.
  - Current Firmware
    Displays the partition number of the firmware currently being used for system startup.
  - Next Startup Firmware
    Displays the partition number of the firmware to be used for the next system startup.
  - Boot Loader
    Displays boot loader revision.

- Timezone
  Displays the current time zone settings.
  If the time zone settings were changed, the new settings are displayed in the “Next Boot” area. Once the system is restarted the new settings appear as the Timezone setting.
- Summer-Time
  Displays the current summer time settings.
  If the summer time settings were changed, the new settings are displayed in the “Next Boot” area. Once the system is restarted the new settings appear as the Summer-time setting.
- RS232C Baud-Rate
  Displays the serial (RS-232C) baud rate.
- Management LAN Information
  Displays the current status of the management LAN interface.
  - MAC Address
    Displays the MAC address.
  - IP Address/Mask
    Displays the IP address and the subnet mask bit length.
  - Default Gateway
    Displays the IP address of the default gateway.
  - DNS Server
    Displays the IP address of the DNS server.
  - Domain Name
    Displays the domain name.
- System Load Information
  - CPU Used Ratio
    Displays the CPU usage ratio.
  - Memory Used Size
    Displays both the currently used size of memory and the current memory usage ratio.

5.19.3 show optical-module sensor

Function

Displays the sensor values which is installed on the optical module.

Prompt

xg> or xg#

Command syntax

```
show optical-module sensor [ dbm ]
```

Parameter

- dbm

  `Display the strength of the laser in “dBm”.`

When parameter is omitted, the strength will be displayed in “mW”

Command type

Operation management command

Output form (no parameter)

```
xg# show optical-module sensor
Optical Module Monitoring Data  2008/06/23-12:16:19
===================================================
           [Tx power]  [Rx power]  [Temperature]
                (mW)        (mW)     (degree C)
port 1  :      0.5221     0.5970           27.0
port 2  :      0.5392     0.4754           35.9
port 3  :      0.4524     0.3950           37.0
port 4  :      0.4150     0.4548           37.0
port 5  : (unmounted)
port 6  : (unmounted)
port 7  : (unmounted)
port 8  : (unmounted)
port 9  : (unmounted)
port 10 : (unmounted)
port 11 : (unmounted)
port 12 : (unmounted)
port 13 : (unmounted)
port 14 : (unmounted)
port 15 : (unmounted)
port 16 : (unmounted)
port 17 : (unmounted)
port 18 : (unmounted)
port 19 : (unmounted)
port 29 : (unmounted)
```

Output form (parameter is specified)

```
xg# show optical-module sensor dbm
Optical Module Monitoring Data  2008/06/23-12:16:19
===================================================
           [Tx power]  [Rx power]  [Temperature]
                (dBm)       (dBm)     (degree C)
port 1  :      -2.837      -2.261           27.0
port 2  :      -2.683      -3.224           35.9
port 3  :      -3.456      -4.034           37.0
port 4  :      -3.820      -3.422           37.0
port 5  : (unmounted)
port 6  : (unmounted)
port 7  : (unmounted)
port 8  : (unmounted)
port 9  : (unmounted)
port 10 : (unmounted)
port 11 : (unmounted)
port 12 : (unmounted)
port 13 : (unmounted)
port 14 : (unmounted)
port 15 : (unmounted)
port 16 : (unmounted)
port 17 : (unmounted)
port 18 : (unmounted)
port 19 : (unmounted)
port 29 : (unmounted)
```

- port xx

  `Displays each port. The number of ports are depend on the device.`
- Tx power

  `Displays the strength of the output laser.`
- Rx power

  `Displays the strength of the input laser.`
- Temperature

  `Displays the temperature of the optical module.`

5.20 System Maintenance Commands

5.20.1 clear log

Function

Initializes the system log.

Prompt

xg#

Command syntax

```
clear log [ { info | warning | error | critical } ]
```

Parameter

- { info | warning | error | critical }

  Specifies the type of system log to be initialized.

  - info

    Initializes the INFO log.
    The INFO log stores informational (INFO) messages that report on the system status of the device.
  - warning

    Initializes the WARNING log.
    The WARNING log stores warning (WARNING) messages that report on the system status of the device.
  - error

    Initializes the ERROR log.
    The ERROR log stores error (ERROR) messages that report on the system status of the device.
  - critical

    Initializes the CRITICAL log.
    The CRITICAL log stores critical (CRITICAL) messages that report on the system status of the device.

  If this log-type parameter is omitted, all logs are initialized.

Command type

Operation management command

Example

Initialize the INFO log:

```
xg# clear log info
```

5.20.2 show log

Function

Displays system logs.

Prompt

xg#

Command syntax

```
show log { info | warning | error | critical } [ latest <1-10000> ]
```

Parameter

- { info | warning | error | critical }
  Specifies the type of system log to be displayed.
  - info
    Displays the INFO log.
    The INFO log stores informational (INFO) messages that report on the system status of the device.
  - warning
    Displays the WARNING log.
    The WARNING log stores warning (WARNING) messages that report on the system status of the device.
  - error
    Displays the ERROR log.
    The ERROR log stores error (ERROR) messages that report on the system status of the device.
  - critical
    Displays the CRITICAL log.
    The CRITICAL log stores critical (CRITICAL) messages that report on the system status of the device.
- latest <1-10000>
  Specifies the number of most current log entries to be displayed within the range of 1 to 10000.
  If omitted, all logs are displayed.

Command type

Operation management command

Output form

```
xg# show log info latest 1
May 25 22:08:33 xghost xgsh: XG INFO[P4001]: cmd-exec[3388]: show log info
 |    |    |         |      |         |      |           |
Month | Hours Min Sec |  Function name  Severity |        Message text
     Day            The device's              MessageID
                    Host name
```

- Month
  Displays the month when the event occurred.
- Day
  Displays the day when the event occurred.
- Hours Min Sec
  Displays the time (hours, minutes and seconds) when the event occurred.
- Host name of the device
  Displays the host name of the XG2000 series.
- Function name
  Displays the function name.
- Severity
  Indicates the severity of the message.
  - CRITICAL
    Critical level.
    The system failed to continue its operation. Follow the instructions given by the message.
  - ERROR
    Error level.
    A portion of the system functions have failed although the system can continue operation. Follow the instructions given by the message.
  - WARNING
    Warning level.
    There is no problem with the system operations although an error or a warning event was detected. Check the message information and determine the actions necessary to take.
  - INFO
    Informational level.
    This is an informational message displaying a system status change. No response is necessary.
- MessageID
  Displays the message ID in the "S message number" or "P message number" format.
  - S
    Indicates that the message is an SNMP trap notification.
  - P
    Indicates that the message is not an SNMP trap notification.

- Message number
  Displays a unique number for message identification. Read this message number to locate the message and take necessary actions.
- Message text
  Displays the message text.

Example

Display 10 entries of the latest INFO log:

```
xg# show log info latest 10
```

5.20.3 log send

Function

Transfers the system log from the device to a remote host.

Prompt

xg(config)#

Command syntax

```
log send HOST { info | warning | error | critical } [ { udp | tcp } ]
no log send
```

Parameter

- HOST
  Specifies the host name, domain name or IP address of the system log destination.
  When specifying the host name or the domain name, set the DNS server or register the host name in advance.
  The IP address can be within the range of 1.0.0.1 to 126.255.255.254, 128.0.0.1 to 191.255.255.254, or 192.0.0.1 to 223.255.255.254.

> Point
>
> If transferring system logs to a Linux host, log information can be received by specifying "–syslogd -r".

- { info | warning | error | critical }
  Specifies the type of system logs to be transferred.
  - info
    Transfers the CRITICAL, ERROR, WARNING and INFO messages.
  - warning
    Transfers the CRITICAL, ERROR and WARNING messages.
  - error
    Transfers the CRITICAL and ERROR messages.
  - critical
    Transfers the CRITICAL level messages.
- { udp | tcp }
  Selects a protocol for transmission of system logs. The "udp" (User Datagram Protocol) is selected by default.

Command type

Operation management command

Message

% Invalid IP-address.

Explanation

The IP address was specified in an incorrect format or an incorrect address was specified.

Solution

Specify the correct IP address in the correct format then reissue the command.

% Cannot find %1$

Explanation

An incorrect host name was specified.
[[Inserted string]]%1$: Specified host name.

Solution

.Specify the correct host name, or specify the IP address.

Note

- If the host name is specified instead of IP address, changing the DNS server's IP address at a remote host will not be enabled. It is necessary to restart the device after DNS server's IP address has been changed.

5.20.4 save maintenance

Function

Stores the current internal system status in non-volatile memory.

Prompt

xg#

Command syntax

```
save maintenance
```

Command type

Operation management command

Message

`% Cannot execute simultaneously.`

Explanation

"save maintenance" is executed while it is being executed in other console.

Solution

Do not execute "save maintenance" while it is being executed in other console.

Note

- Up to 5 maintenance information is saved, and the oldest maintenance information is overwritten when exceeded.
  The detail of 5 maintenance information is following.
  - system dump: 1
  - process dump: 1
  - system state: 1

5.20.5 show maintenance

Function

Displays the maintenance information.

Prompt

xg#

Command syntax

```
show maintenance
```

Command type

Operation management command

Output form (if "current" is specified)

```
xg# show maintenance
Maintenance Information      2007/01/22-20:58:17
====================================================
NO  Type                          Occurred Time
--- ------------------------- ---------------------
  1 system dump                   2007/01/22-18:21:23
  2 system dump(dump switch)      2007/01/22-19:57:58
  3 system dump(machine check)    2007/01/22-19:58:14
====================================================
```

- NO
  Displays the maintenance information number. The oldest maintenance information is displayed first.
- Type
  Displays the maintenance information type.
  - system dump
    A system dump was logged during system failure
  - system dump(dump switch)
    A system dump was forcibly logged by the "dump" switch
  - system dump(machine check)
    A system dump was logged due to a hardware machine check
  - process dump
    The process dump was logged during a partial system failure
  - system state
    The system operational status information output by the "save maintenance" command
- Occurred Time
  Displays the date and time when the maintenance information was logged.

> Point
> Nothing is displayed if maintenance information does not exist.

5.20.6 tftp put-maintenance

Function

Transfers the system maintenance information to a TFTP server.
The file size of the maintenance information is displayed on the screen.

Prompt

xg#

Command syntax

```
tftp put-maintenance HOST [ REMOTE-FILE ]
```

Parameter

- HOST
  Specifies the host name or the IP address of the TFTP server.
  The IP address can be within the range of 1.0.0.1 to 126.255.255.254, 128.0.0.1 to 191.255.255.254, or 192.0.0.1 to 223.255.255.254.
- REMOTE-FILE
  Specifies the path and file name the maintenance information will reside in once transferred to the TFTP server. If the file name is omitted, the following file name is generated automatically:
  "mainte_2007_01_31_13_30_59” (date and time when obtained).

Command type

Operation management command

Message

% tftp: %1$: Host name lookup failure

Explanation

The specified host name does not exist.
[[Inserted string]]%1$: Specified host name

Solution

Check the host name for an error.

% tftp: server says: %1$

Explanation

An error was reported from the TFTP server.
[[Inserted string]]%1$: Error messages sent from the FTP server
The message contents vary depending on the TFTP server type used. Typical messages are as follows.

- File not found: No file is found on the TFTP server.
- Access violation: An error of file access authority occurred on the TFTP server.
- Not allowed to overwrite existing files: The file in the TFTP server cannot be overwritten.
- Could not open requested file for reading: There are no files in the TFTP server.
- File already exists: The specified file already exists on the TFTP server.
- Unknown transfer ID: The process is interrupted due to the timeout.

Solution

Take actions by following the message instructions sent from the TFTP server.

% tftp: last timeout

Explanation

There is no response by the TFTP server. The network communication with the management LAN may have failed or too short a timeout was set on the TFTP server.

Solution

Issue a “ping” command to check the network connection to the TFTP server. If an error recurs, change the timeout value of the TFTP server.

% Invalid IP-address.

Explanation

The IP address was specified in an incorrect format or an incorrect address was specified.

Solution

Specify the correct IP address in the correct format then reissue the command.

% Cannot find %1$

Explanation

An incorrect host name was specified.
[[Inserted string]]%1$: Specified host name.

Solution

.Specify the correct host name, or specify the IP address.

Note

- If the file or directory specified by REMOTE-FILE does not exist on the TFTP server, an error may occur (it depends on the TFTP server functions).
- If too short a timeout was set on the TFTP server, an error may occur (it depends on the TFTP server functions).
- To ensure the transmission of all the maintenance information, compare the file size displayed on the screen and the size of the file saved on the TFTP server.

Example

Save the current system status data as a maintenance information file in non-volatile memory then check the logged status of the maintenance information using the “show maintenance” command.

Transfer the maintenance information to the “host1” TFTP server by naming it as the “mainte_collected date and time” file.

Compare the file size of the maintenance information displayed on the screen to the size of the file stored on the TFTP server.

```
xg# save maintenance
xg# show maintenance
Maintenance Information       2007/01/22-20:58:17
==================================================
NO  Type                       Occurred Time
--- -------------------------- -------------------
  1 system dump                 2007/01/22-18:21:23
  2 system dump(dump switch)    2007/01/22-20:57:58
  3 system dump(machine check)  2007/01/22-20:58:14
==================================================
xg# tftp put-maintenance host1
Total file size: 480711 (bytes)
```

5.20.7 scp put-maintenance

Function

Transfers the system maintenance information to a SSH server.
The file size of the maintenance information is displayed on the screen.

Prompt

xg#

Command syntax

```
scp put-maintenance USERNAME HOST [ REMOTE-FILE ]
```

Parameter

- USERNAME
  Specifies the username of the SSH server.
- HOST
  Specifies the host name or the IP address of the SSH server.
  The IP address can be within the range of 1.0.0.1 to 126.255.255.254, 128.0.0.1 to 191.255.255.254, or 192.0.0.1 to 223.255.255.254.
- REMOTE-FILE
  Specifies the path and file name the maintenance information will reside in once transferred to the SSH server. If the file name is omitted, the following file name is generated automatically:
  "mainte_2008_07_01_13_30_59” (date and time when obtained).

Command type

Operation management command

Message

% The length of user name is invalid.

Explanation

The length of the username is invalid.

Solution

Specify the username 16 or less characters.

lost connection

Explanation

It failed to access to specified SSH server.

Solution

Specify the correct host name, IP address, or username.

No more remote host public key can be registered.

Explanation

Specified remote host public key could not be registered.

Solution

Delete a public key by using “clear ssh-rhost key” command, then execute the command again.

%1$: No such file or directory

Explanation

Specified file does not exist.
[[Inserted string]]%1$: Specified file name.

Solution

Specify the correct file name.

scp: %1$: No such file or directory

Explanation

Specified file does not exist.
[[Inserted string]]%1$: Specified file name.

Solution

Specify the correct file name.

scp: %1$: Permission denied

Explanation

There was no access permission to the SSH server.
[[Inserted string]]%1$: Specified file name.

Solution

Check the access permission to the SSH server.

ssh: connect to host %1$ port 22: No route to host

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: Network is unreachable

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: Connection refused

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

ssh: connect to host %1$ port 22: connection timed out

Explanation

It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.

Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

%1$: invalid user name

Explanation

Specified username is invalid.
[[Inserted string]]%1$: Specified username.

Solution

Specify the correct username.

Note

- "scp" supports only password authentication, and this device can register up to 10 public keys of SSH servers.
- Execute "clear ssh-rhost-key" command to delete a registered public key.

Example

Save the current system status data as a maintenance information file in non-volatile memory then check the logged status of the maintenance information using the "show maintenance" command.
Transfer the maintenance information to the "host2" SSH server by naming it as the "mainte_collected date and time" file.
Compare the file size of the maintenance information displayed on the screen to the size of the file stored on the SSH server.

```
xg# save maintenance
xg# show maintenance
Maintenance Information       2008/06/30-20:58:17
==================================================
NO  Type                       Occurred Time
--- -------------------------- -------------------
  1 system dump                  2008/06/30-18:21:23
  2 system dump(dump switch)     2008/06/30-20:57:58
  3 system dump(machine check)   2008/06/30-20:58:14
==================================================
xg# scp put-maintenance foo host2
ssh-host2's password:
Total file size: 480711 (bytes)
```

5.20.8 clear maintenance

Function

Clears the maintenance information from non-volatile memory on the device.

Prompt

xg#

Command syntax

```
clear maintenance
```

Command type

Operation management command

Note

- Issue the “clear maintenance” command only after checking for a successful file transfer to the remote server using the “tftp put-maintenance” or “scp put-maintenance” command.

Example

Clear the maintenance information from non-volatile memory:

```
xg# clear maintenance
```

5.20.9 update-system

Function

Updates the firmware on the device.
The device stores two firmware images. This command updates the standby firmware. The updated firmware is made valid after the next system startup.

Prompt

xg#

Command syntax

```
update-system local FILE-NAME
update-system { tftp | scp USERNAME } HOST REMOTE-FILE
```

Parameter

- local FILE-NAME
  Specifies the firmware image file that was downloaded from the TFTP server to non-volatile memory in the device.
- tftp
  Directly updates the firmware from the firmware image file stored on the TFTP server.
- scp USERNAME
  Specifies the username of the SSH server.
- HOST
  Specify the host name or the IP address of the TFTP server or SSH server.
  The IP address must be within the range of 1.0.0.1 to 126.255.255.254, 128.0.0.1 to 191.255.255.254, or 192.0.0.1 to 223.255.255.254.
- REMOTE-FILE
  Specifies the firmware image file residing on the TFTP server or SSH server.

Command type

Operation management command

Message

% File not found.

Explanation

The specified file was not found.

Solution

Check the file name for an error.

% Reading the file failed.

Explanation

The specified file could not be read.

Solution

Check that the file is read enabled.

% Checksum error: %1$ in the file

Explanation

A data error was detected in the specified file.
[[Inserted string]]%1$: Firmware configuration module

Solution

Check the file for an error in its contents.
If the file contents are OK, an error may have occurred during file transmission. Transfer the file again.

% Checksum error: whole file

Explanation

A data error (a checksum error of the entire file) was detected.

Solution

Check the file for an error in its contents.
If the file contents are OK, an error may have occurred during file transmission. Transfer the file again.

% Version of the format of the file is not suitable for this system.

Explanation

The firmware revision of the specified file cannot be used with the system hardware.

Solution

Specify the correct file to update the system firmware.

% The file is not for this system.

Explanation

The firmware revision of the specified file cannot be used with the system hardware.

Solution

Specify the correct file to update the system firmware.

% Reading boot loader partition in FlashROM failed.

Explanation

An error occurred during a read of flash ROM data.

Solution

Retry firmware updating.
If the error recurs, contact the sales representative.

% Writing %1$ into FlashROM failed.

Explanation

An error occurred while writing to flash ROM.
[[Inserted string]]%1$: Firmware configuration module

Solution

Retry firmware updating.
If the error recurs, contact the sales representative.

% Checksum error: %1$ in FlashROM

Explanation

An error occurred while writing to flash ROM.
[[Inserted string]]%1$: Firmware configuration module

Solution

Retry firmware updating.
If the error recurs, contact the sales representative.

% %1$ in SRAM is invalid.

Explanation

An inconsistency in non-volatile (SRAM) memory data was detected.
[[Inserted string]]%1$: Abnormal memory contents

Solution

Restart the system using the "reset" command. Then, retry firmware updating.
If the error recurs, contact the sales representative.

% tftp: %1$: Host name lookup failure

Explanation

The specified host name does not exist.
[[Inserted string]]%1$: Specified host name

Solution

Check the host name for an error.

% tftp: server says: %1$

Explanation

An error was reported from the TFTP server.
[[Inserted string]]%1$: Error messages sent from the FTP server
The message contents vary depending on the TFTP server type used. Typical messages are as follows.

- File not found: No file is found on the TFTP server.
- Access violation: A file access violation occurred on the TFTP server.
- Not allowed to overwrite existing files: The file in the TFTP server cannot be overwritten.
- Could not open requested file for reading: The file does not exist on the TFTP server.
- File already exists: There are files in the TFTP server.
- Unknown transfer ID: Process will be aborted in time out.

Solution

Take actions by following the message instructions sent from the TFTP server.

% tftp: write: No space left on device

Explanation

The non-volatile memory on the device has insufficient work area. A portion of the file being downloaded may remain in the non-volatile memory.

Solution

Delete the downloaded file and unnecessary files on the system using the "delete" command. Then, reissue the "update-system" command.

% tftp: last timeout

Explanation

There is no response from the TFTP server. The network may have failed or too short a timeout was set on the TFTP server.

Solution

Issue a "ping" command to check the network connection to the TFTP server. If the error recurs, change the timeout value on the TFTP server.

% Invalid IP-address.

Explanation

The IP address was specified in an incorrect format or an incorrect address was specified.

Solution

Specify the correct IP address in the correct format then reissue the command.

% Cannot find %1$

Explanation

An incorrect host name was specified.
[[Inserted string]]%1$: Specified host name.

Solution

.Specify the correct host name, or specify the IP address.

% The length of user name is invalid.

Explanation

The length of the username is invalid.

Solution

Specify the username 16 or less characters.

No more remote host public key can be registered.

Explanation

Specified remote host public key could not be registered.

Solution

Delete a public key by using "clear ssh-rhost key" command, then execute the command again.

```
scp: %1$: No such file or directory
```
Explanation

```
Specified file does not exist.
[[Inserted string]]%1$: Specified file name.
```
Solution

```
Specify the correct file name.
```
```
scp: %1$: Permission denied
```
Explanation

```
There was no access permission to the SSH server.
[[Inserted string]]%1$: Specified file name.
```
Solution

```
Check the access permission to the SSH server.
```
```
%1$: No space left on device
```
Explanation

This device does not have enough space to copy the file. Incomplete copied file may remain on the device.

```
[[Inserted string]]%1$: Specified file name.
```
Solution

Delete incomplete copied file and unnecessary files by using "delete" command, then execute the command again.

```
ssh: connect to host %1$ port 22: No route to host
```
Explanation

```
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
```
Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

```
ssh: connect to host %1$ port 22: Network is unreachable
```
Explanation

```
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
```
Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

```
ssh: connect to host %1$ port 22: Connection refused
```
Explanation

```
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
```
Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

```
ssh: connect to host %1$ port 22: connection timed out
```
Explanation

```
It failed to access to specified SSH server.
[[Inserted string]]%1$: Specified IP address or host name.
```
Solution

Specify the correct IP address or host name.
Check the setting and status of SSH server and whether there is no problem in network connection to the SSH server.

Note

- “scp” supports only password authentication, and this device can register up to 10 public keys of SSH servers.
- Execute “clear ssh-rhost-key” command to delete a registered public key.

Example

Download the firmware image file into the system volatile memory using the “tftp get” command. Check the size of the downloaded firmware image file using the “ls” command.
Then, update the firmware using the “update-system” command.

```
xg# tftp get tftp-host1 firm_upd_file
xg# ls
```

```
  Update-time        File-size  File-name
- 2007/01/31 13:52:54  5,754,559 firm_upd_file

 unused: 8,888,320 bytes
```

```
xg# update-system local firm_upd_file
```

Update the firmware directly from the TFTP server.

```
xg# update-system tftp tftp-host1 firm_upd_file
```

Update the firmware directly from the SSH server.

```
xg# update-system scp foo ssh-host1 firm_upd_file
host1's password:
```

After the firmware was updated successfully, check the firmware version (E/L) and make sure that the system firmware was set to “(new)” using the “show system information” command.
Also, check the “Next Startup Firmware” value. This firmware image will be booted during the next system startup.

```
xg# show system information
```

```
・・・
・・・
Firmware Information
  Firmware[1]          : E10L10 Z01 2007/01/21-18:42:52
   Updated Time        : 2007/01/21-22:08:12
  Firmware[2]          : E10L11 Z01 2007/01/22-19:27:12 {(writing)|(new)}
   Updated Time        : 2007/01/23-10:57:53                    ↑
  Current Firmware     : [1]                 The updating status is displayed.
  Next Startup Firmware: [2]
・・・
・・・
```

After the updating process completes, restart the system hardware.

```
xg# reset
```

5.20.10 boot-system

Function

Switches the firmware image to be used for the next system startup.
Use this command only if a problem occurred using new firmware.

Prompt

xg#

Command syntax

```
boot-system { 1 | 2 }
```

Parameter

- {1|2}
  Specifies the number of the firmware partition to be used during the next system startup.
  The applicable firmware version can be checked by the “show system information” command.
  – 1
    Uses firmware 1 for the next system startup.
  – 2
    Uses firmware 2 for the next system startup.

Command type

Operation management command

Message

% Attempted to change to invalid firmware. Command failed.

Explanation

The previous firmware update may not have completed successfully. The firmware partition is unusable.

Solution

Update the firmware again.
If the error recurs, contact the sales representative.

% 1$ in SRAM is invalid.

Explanation

An inconsistency in non-volatile (SRAM) memory data was detected.
[[Inserted string]]%1$: Abnormal memory contents

Solution

"Restart the system using the “reset” command. Then, retry the firmware update.
If the error recurs, contact the sales representative.

Example

Change the firmware to be used for the next system startup using the “boot-system” command.
Check that the firmware information (Next Startup Firmware) to be used for the next system startup changed using the “show system information” command.

```
xg# boot-system 1
xg# show system information
```

```
. . .
. . .
Firmware Information
  Firmware[1]           : E10L10 Z01 2007/01/23-18:42:52
   Updated Time         : 2007/01/21-22:08:12
  Firmware[2]           : E10L11 Z01 2007/01/31-19:27:12
   Updated Time         : 2007/01/31-19:57:53
  Current Firmware      : [2]
  Next Startup Firmware: [1]
. . .
. . .
```

Chapter 6 Managing the Device

This chapter describes the management of the device.

6.1 Verifying the Device Operations

This chapter describes the management of the device.

- Hardware status
- System status
- Log messages

6.1.1 Verifying Hardware Status

Verify the status of hardware by entering the "show system status" command in the operator EXEC mode or in the administrator EXEC mode. The following example shows the information that is displayed when the "show system status" command is entered.

```
xg# show system status
```

```
System Status Information  2007/01/25-12:16:19
=============================================
[Temperature]
   Internal      : good

[Power Supply]
  PWR-0 (AC)      : good
  PWR-1 (AC)      : good

[Voltage]
   Voltage        : good

[Fan]
   Rear Fan-0     : good (normal-speed)
   Rear Fan-1     : good (normal-speed)
   PWR-0 Fan      : good
   PWR-1 Fan      : good

[XFP]
   port  1 (VENDER-NAME.    :S  ) : good
   port  2 (VENDER-NAME.    :L  ) : good
   port  3 (VENDER-NAME.    :S  ) : good
   port  4 (VENDER-NAME.    :L  ) : good
   port  5 (VENDER-NAME.    :S  ) : good
   port  6 (VENDER-NAME.    :L  ) : good
   port  7 (VENDER-NAME.    :S  ) : good
   port  8 (VENDER-NAME.    :L  ) : good
   port  9 (VENDER-NAME.    :S  ) : good
   port 10 (VENDER-NAME.    :L  ) : good
   port 11 (VENDER-NAME.    :S  ) : good
   port 12 (VENDER-NAME.    :L  ) : good
   port 13 (VENDER-NAME.    :S  ) : good
   port 14 (VENDER-NAME.    :L  ) : good
   port 15 (VENDER-NAME.    :S  ) : good
   port 16 (VENDER-NAME.    :L  ) : good
   port 17 (VENDER-NAME.    :S  ) : good
   port 18 (VENDER-NAME.    :L  ) : good
   port 19 (VENDER-NAME.    :S  ) : good
   port 20 (VENDER-NAME.    :L  ) : good
```

The following table provides descriptions of items displayed when the "show system status" command is entered and an explanation of each error message.

Item	Item displayed	Message explanation/Solution
Temperature		Displays the temperature inside the chassis.
	Internal (internal temperature sensor)	● good The temperature is within normal operating range. ● caution The temperature is high, but within normal operating range. The system will be shutdown if it reaches the alarm threshold. – Check that the air vent is not blocked. – Check that the temperature of the switch location is within the limits specified. ● Temperature is out of range. (xx yy) The temperature is out of normal operating range. If the temperature exceeds high alarm threshold, the system will be shutdown. – Check that the air vent is not blocked. – Check that the temperature of the set up location is within the limits set out by the operation guarantee. If the same message is displayed after re-examining the set up of the device, contact the sales representative.
Power Supply		Display the status of power supply unit.
	PWR - 0 (status of power supply unit 0)	● good The power supply unit 0 is properly installed and functional. ● Removed The power supply unit 0 was removed. If this message appears with the power supply unit 0 installed, check that the unit is properly installed. ● Off Line Power is not reaching the power supply unit 0. Check the AC inputs. ● Alarm Detected. A power supply error was detected. Replace the unit.
	PWR - 1 (status of power supply unit 1)	Displays the status of power supply unit 1.The messages and actions to take are the same as those described for power supply unit 0.
Voltage		Displays status of the CPU board supply voltages.
	Voltage	● Good The voltage supplies are within normal operating range. ● VDP: Out of range. (xx) A VDP voltage error was detected. Contact the sales representative. ● VDE: Out of range. (xx) A VDE voltage error was detected. Contact the sales representative. ● VDR: Out of range. (xx) A VDR voltage error was detected. Contact the sales representative. ● VDD: Out of range. (xx) A VDD voltage error was detected. Contact the sales representative. ● VDN: Out of range. (xx) A VDN voltage error was detected. Contact the sales representative. ● 1.5V : Out of range. (xx) A 1.5V power supply error was detected on the CPU board. Contact the sales representative. ● 3.3V : Out of range. (xx) A 3.3V power supply error was detected on the CPU board. Contact the sales representative. ● 12V : Out of range. (xx) A 12V power supply error was detected on the CPU board. Contact the sales representative. ● 3.3V (I/F): Out of range. (xx) A 3.3V power supply error was detected on the switch board. Contact the sales representative. ● 12V (I/F): Out of range. (xx) A 12V power supply error was detected on the switch board. Contact the sales representative.

Fan		Displays the status of the fans.
	Rear Fan-0	● good (normal-speed) The fan is working at a normal speed. ● good (high-speed) The fan is working at a high speed. ● Removed The fan was removed. Check that the fan is installed. ● Speed is below the Low Limit. (xx yy) The fan speed is below the low limit. Replace the fan unit. ● Messages other than those above The fan is not working properly. Replace the fan unit.
	Rear Fan-1	Status of rear fan 1 The messages and actions to take are the same as those described for Rear Fan-0
	PWR-0 Fan (fan installed in power supply unit 0)	● Good The fan is working properly. ● Speed is below the Low Limit. (xx yy) The fan speed is below the low limit. It is also displayed when the PSU is removed. Replace the power supply unit if the message is displayed even though it is working properly.
	PWR-1 Fan (fan installed in power supply unit 1)	Status of the fan installed in power supply unit 1 The messages are the same as those described for PWR-0 fan.
XFP		Displays the vender name, PHY type and status for each XFP. The vender name is read from the XFP device while the PHY type is based of "XFP MSA4.5".
	port xx (status of port xx) (The number of ports are depend on the device.)	● Good The XFP is working properly. ● Low Power The XFP is in power down mode. ● Alarm (xx) An XFP alarm was detected. If high temperature alarm is detected, the device shut down the XFP. Check the XFP insertion and the temperature around the XFP. If the same message is displayed after taking appropriate action, note the message contents and contact the sales representative. ● PHY Device Error An XFP access error occurred. Check the XFP insertion. If the same message is displayed after taking appropriate action, note the the message contents and contact the sales representative. ● No messages An XFP was removed. If this message appears with the XFP in the slot, check that it is properly installed.

6.1.2 Verifying System Status

Verify the system status by entering the "show system information" command in the operator EXEC mode or in the administrator EXEC mode.
The following example shows the information that is displayed when the "show system information" command is entered.

```
xg# show system information
```

```
System Information  2007/02/22-21:06:11
=======================================
 System Name (hostname) : xg
 System Location        : (none)
 System Contact         : (none)
 Default Banner         : XG2000 E10L11 Z01
 Startup Time           : 2007/02/22-19:28:24
 Startup-config Modified: 2007/02/22-19:54:01
 Firmware Information
  Firmware[1]           : E10L10 Z01 2007/01/21-18:42:52
   Updated Time         : 2007/01/21-22:08:12
  Firmware[2]           : E10L11 Z01 2007/02/22-19:27:12
   Updated Time         : 2007/02/23-10:57:53
  Current Firmware      : [2]
  Next Startup Firmware : [2]
  Boot Loader           : E10L10 Z01
 Timezone               : gmt +0900
  (Next Boot)           : gmt -800
 Summer-Time            : (none)
  (Next Boot)           : M4.1.0/0200 M10.5.0/0200 0100
 RS232C Baud-Rate       : 9600
 Management LAN Information
  MAC Address           : 0080.17c2.0500
  IP Address/Mask       : 192.168.41.22/24
  Default Gateway       : 192.168.41.1
  DNS Server            : 192.168.77.20
  Domain Name           : abc.efg.com
 System Load Information
  CPU Used Ratio        : 1%
  Memory Used Size      : 36,429,824 bytes (28%)
```

Check the version of firmware. Verify the system status based on CPU load and memory usage.

6.1.3 Reviewing Log Messages

Log messages from the device are classified into 4 levels -- CRITICAL, ERROR, WARNING, and INFO -- in accordance with the severity of events.
To display event logs, run the "show log" command in the operator EXEC mode or in the administrator EXEC mode.

6.1.3.1 Format of Log Message

An example of the format of a log message displayed by the "show log" command is shown below.

```
xg# show log info latest 1
May 25 22:08:33 xghost xgsh: XG INFO[P4001]: cmd-exec[3388]: show log info latest 1
 |    |     |       |     |            |     |          |
Month |   HH:MM:SS  |   Function name  Severity  |          Message text
     Day          Host name                 Message ID
                  for the device
```

- Month
  Displays the date (month) of the event.
- Day
  Displays the date (day) of the event.
- HH:MM:SS
  Displays the time (hours:minutes:seconds) of the event.
- Host name of the device
  Displays the host name.
- Function name
  Indicates the function name.
- Severity
  Indicates the severity of the message.
  - CRITICAL
    The system encountered a serious condition that prevented it from continuing its operation. Take appropriate action in response to this message.
  - ERROR
    Does not stop system operation but some functions are inoperable. Take appropriate action in response to this message.
  - WARNING
    An error or critical condition was detected, but it does not affect normal operation of the device. Determine whether an action must be taken by examining the message.
  - INFO
    A message provides information about the system status. No action is necessary.
- Message ID
  Message ID is displayed in a form that begins with an "S" or "P".
  - S
    A message that receives SNMP trap notification.
  - P
    A message that does not receive SNMP trap notification.
  - Message number
    Displays a unique number used to identify a message within the device.
    Verify the meaning of the message and actions to take based on the message number.
- Message text
  Displays message text.

6.1.3.2 Reviewing Fault Logs

If a fault occurred, review the fault log to check fault messages (CRITICAL, ERROR, or WARNING).
To review fault logs, enter the "show log" command in the operator EXEC mode or in the administrator EXEC mode. For the meaning of messages and actions to take for the errors, refer to "Appendix A.2 List of Event Logs".
The following examples show the information that is displayed when the "show log" command is entered.

```
xg# show log critical
Aug 22  03:33:51 xg kernel:  XG CRITICAL[S1000]: Abnormal reset occurred (WatchDog Reset: code=1)
Aug 22 03:33:51 xg kernel: XG CRITICAL[S1900]: Core dumped 359
xg# show log error
Aug 22 03:33:51 xg env: XG ERROR[S0101]: Internal Temperature is out of rage. (65)
Aug 22 03:33:51 xg env: XG ERROR[S0115]: port 1 is not present.
xg# show log warning
Aug 22 03:33:51  xg env:  XG WARNING[S0109]: Front Fan-1 Speed is below the Low Limit. (2150 6675)
Aug 22 03:33:51 xg npm: XG WARNING[S3005]: port 1 detected port security violation.
Aug 22 03:33:51 xg npm: XG WARNING[S3202]: Received IGMP packet without IP header.
```

6.1.3.3 Verifying the Device Status Change

To verify changes in the device status, review INFO log messages.
Enter the "show log" command in the operator EXEC mode or in the administrator EXEC mode. For the meaning of messages, refer to "List of System Logs". The following examples show the information that is displayed when the "show log" command is entered.

```
xg# show log info
Aug22 10:07:57 xg xgsh: XG INFO[P4001]: cmd-exec[893]: show system information
Aug22 10:08:01 xg xgsh: XG INFO[P4002]: cmd-result[893]: success
Aug22 10:08:01 xg xgsh: XG INFO[P4001]: cmd-exec[893]: show spanning-tree
Aug22 10:08:01 xg xgsh: XG INFO[P4002]: cmd-result[893]: success
Aug22 10:08:02 xg xgsh: XG INFO[P4001]: cmd-exec[893]: show remote-host
Aug22 10:08:02 xg xgsh: XG INFO[P4002]: cmd-result[893]: success
Aug22 10:08:34 xg ntp : XG INFO[P8602]: time server 192.168.41.1 offset -0.000543 sec
Aug22 10:08:34 xg xgsh: XG INFO[P4002]: cmd-result[893]: success
Aug22 10:10:34 xg ntp : XG INFO[P8602]: time server 192.168.41.1 offset -0.000660 sec
Aug22 10:45:32 xg xgsh: XG INFO[P4001]: cmd-exec[592]: exit
Aug22 10:45:32 xg xgsh: XG INFO[P4002]: cmd-result[592]: success
```

- Display log for each component
  To display a log associated with a specific component only, specify the name of that component with "| include " after entering "show log" command.
  In the following example, the CLI displays only messages that include "cmd-exec".

```
xg# show log info | include cmd-exec
Aug22 10:07:57 xg xgsh: XG INFO[P4001]: cmd-exec[893]: show system information
Aug22 10:08:01 xg xgsh: XG INFO[P4001]: cmd-exec[893]: show spanning-tree
Aug22 10:08:02 xg xgsh: XG INFO[P4001]: cmd-exec[893]: show remote-host
Aug22 10:45:32 xg xgsh: XG INFO[P4001]: cmd-exec[592]: exit
```

6.2 Uploading/Downloading a Configuration File

The configuration file, generated in the device, can be uploaded to a remote server. Also, when an uploaded configuration file is downloaded from a remote server, the configuration of the device can be restored.
This section describes the procedures involved in uploading/downloading a configuration file.

6.2.1 Preparing the remote Server

Before uploading and/or downloading configuration files using a TFTP server or SSH server, carry out the following procedures.

- Check that the management LAN and the workstation or other machine operating as the TFTP server or SSH server is set up appropriately. Verify communication between the TFTP or SSH server and the management LAN is error-free.
- Check that the access privilege of the root directory is readable/writable in the TFTP server or SSH server.
- When downloading the configuration file, check that the configuration file uploaded to the TFTP server or SSH server is located in the correct directory.

6.2.2 Uploading a Configuration File

This section describes the procedure for uploading the configuration (startup-config) file to a TFTP server or SSH server.

1. After logging into the device, use the "enable" command to switch to administrator EXEC mode.

```
xg> enable
```

2. Upload the configuration (startup-config) file to the TFTP server "host1" as filename "start_conf".

```
xg# show startup-config | tftp host1 start_conf
```

Upload the configuration (startup-config) file to the SSH server "host2" as filename "start_conf".

```
xg# show startup-config | scp foo host12 start_conf
host2's password:
```

3. Check that the size of configuration file uploaded to a remote server is the same as that of the source configuration file.

6.2.3 Downloading a Configuration File

This section describes the procedure for downloading the configuration file from a remote server to the device as the startup-config file.

1. After logging into the device, use the "enable" command to switch to administrator EXEC mode.

```
xg> enable
```

2. Using the "copy ... startup-config" command, download the saved file from the remote server to the device.
In the following example, "start_conf" file saved on the TFTP server "host1" is downloaded to the startup-config file in the device.

```
xg# copy tftp host1 start_conf startup-config
```

In the following example, "start_conf" file saved on the SSH server "host2" is downloaded to the startup-config file in the device.

```
xg# copy scp foo host2 start_conf startup-config
remote-host2's password:
```

3. Using the "show startup-config" command, check that the contents of the startup-config changed.
Using the "show system information" command, check that the last updated date and time (Startup-config Modified) for the startup-config file changed.

```
xg# show startup-config
xg# show system information
```

```
System Information  2007/01/22-15:02:54
=======================================
 System Name (hostname) : xg
 System Location        : (none)
 System Contact         : (none)
 Default Banner         : XG2000 E10L10 Z01
 Startup Time           : 2007/01/22-19:28:24
 Startup-config Modified: 2007/01/22-19:54:01     ← Last updated date and time
  . . . .
  . . . .
```

4. To enable the downloaded startup-config, reboot the device using the "reset" command.

```
xg# reset
```

```
Do you restart system? (y/n) :   ← A confirmation message is displayed.
```

6.3 Updating Firmware

The device can hold two versions of firmware. If a firmware update is performed, the inactive firmware will be updated. The device automatically uses the new firmware (updated version) during reboot after the firmware update. If the switch fails to start the new firmware, it automatically uses the old version (the one that was not updated). If problems occur with the new version, the old version can be manually selected.

First, prepare and update the firmware.

- Preparing the remote Server (as listed in "Preparing the remote Server" in "Uploading/Downloading a Configuration File")
- Updating Firmware

Then, select the firmware to use.

- Selecting Firmware

6.3.1 Updating Firmware

This section describes the procedure involved when updating firmware using a remote server.

1. After logging into the device, use the "enable" command to switch to administrator EXEC mode.

```
xg> enable
```

2. Using the "update-system" command, perform a firmware update.

```
If a firmware update is performed, the inactive firmware will be updated.
In the following example, the firmware is updated using the firmware file "XF10100" stored
on the TFTP server "host1".
```

```
xg# update-system tftp host1 XF10100
```

```
In the following example, the firmware is updated using the firmware file "XF10100" stored
on the SSH server "host2".
```

```
xg# update-system scp foo host2 XF10100
remote-host2's password:
```

3. Upon successful completion of the firmware update, verify the version number of the updated firmware (E#/L#) changed using the "show system information" command. During the update, the command output changes to"(writing)". When the firmware update completes successfully, the updated firmware selection number is displayed in "Next Startup Firmware".

```
xg# show system information
```

```
・・・
 Firmware Information
  Firmware[1]           : E10L10 Z01 2007/01/21-18:42:52
   Updated Time         : 2007/01/21-22:08:12
  Firmware[2]           : E10L11 Z01 2007/02/22-19:27:12
   Updated Time         : 2007/02/23-10:57:53        ↑
  Current Firmware      : [1]                  Displays the status of update.
  Next Startup Firmware : [2]
```

4. Upon completion of the firmware update, reboot the device using the "reset" command.

```
xg# reset
```

```
Do you restart system? (y/n) :   ← A confirmation message is displayed.
```

If the reboot (starting the new firmware) fails, the old version is automatically selected and booted. If this is the case, the following message is output to the log.

```
XG WARNING[S7520]: init-firmup: Booting new firmware failed. Old firmware '%1$' is now running.
```

Explanation

```
Old firmware was run because the new updated firmware can not successfully initialize.
[[Inserted string]]%1$: Firmware version information
```

6.3.2 Selecting Firmware

This section describes the procedures for selecting the firmware to use.

1. After logging into the device, use the "enable" command to switch to administrator EXEC mode.

```
xg> enable
```

2. Using the "show system information" command, check the status of the firmware.
   Note the firmware information (Firmware[1] and [2]), the currently active firmware (Current Firmware), and firmware that will run the next time (Next Startup Firmware) the switch is rebooted.

```
xg# show system information
・・・
・・・
 Firmware Information
  Firmware[1]           : E10L10 Z01 2007/01/21-18:42:52
   Updated Time         : 2007/01/21-22:08:12
  Firmware[2]           : E10L11 Z01 2007/02/22-19:27:12
   Updated Time         : 2007/02/23-10:57:53
  Current Firmware      : [2]
  Next Startup Firmware: [2]
  Boot Loader           : E10L10 Z01
・・・
・・・
```

3. Using the "boot-system" command, change the Next Startup Firmware image.
   Using the "show system information" command again, check that the "Next Startup Firmware" changed.

```
xg# boot-system 1
xg# show system information
・・・
・・・
Firmware Information
  Firmware[1]           : E10L10 Z01 2007/01/21-18:42:52
   Updated Time         : 2007/01/21-22:08:12
  Firmware[2]           : E10L11 Z01 2007/02/22-19:27:12
   Updated Time         : 2007/02/23-10:57:53
  Current Firmware      : [2]
  Next Startup Firmware: [1]
・・・
・・・
```

4. Reboot the device using the "reset" command.

```
xg# reset
Do you restart system? (y/n) :   ← A confirmation message is displayed.
```

6.4 Extracting of Maintenance Information

If a fault occurred, maintenance information may be requested by the device sales representative to investigate the cause of the fault. This section provides procedures for extracting maintenance information.
Depending on the situations shown below, extract maintenance information using the described procedures.

- System/Subsystem failure
  If an unrecoverable error occurred in the device's system or subsystem, the system automatically saves maintenance information and restarts the system operations.
- System loop
  If the system entered an endless loop and CLI command entry is not accessible, use the "dump" switch on the front panel to save maintenance information and restart the system.
- The device malfunctions
  If a function configured for the device malfunctions, save maintenance information using the Extract Information command.

6.4.1 Procedure for Extracting Maintenance Information when a System /Subsystem Failure Occurred

This section describes the procedures for extracting maintenance information when a system or subsystem failure occurred.

- A system/subsystem failure occurred.
  If an unrecoverable error, including a system or subsystem failure, occurred in the device, the system automatically saves maintenance information and restarts the system operations. If a system failure occurred, a system dump file and a process dump file are generated.
- System logs and SNMP traps
  After the system restarts, a system log entry is generated to indicate that a system/subsystem failure generated a dump file. Configuring an SNMP trap in advance causes the system/subsystem failure to be reported to a system administrator.
- Viewing maintenance information history
  Using the "show maintenance" command, check that the maintenance information was saved.

```
xg# show maintenance
Maintenance Information       2007/01/22-15:55:20
==================================================
NO  Type                      Occurred Time
--- ------------------------- -------------------
  1 system dump               2007/01/22-18:21:23
  2 process dump              2007/01/22-20:57:58
==================================================
```

The "show maintenance" command displays one of the following types of maintenance information in "Type".

  - system dump
    System dump recorded when a system failure occurred.
  - system dump(dump switch)
    Forced system dump caused by the "dump" switch.
  - system dump(machine check)
    System dump triggered by a hardware machine check.
  - process dump
    Process dump generated when a failure occurred in a subsystem.

- Extracting maintenance information
  Using the "tftp put-maintenance" or "scp put-maintenance" command, forward the maintenance information to an external remote server.
- Contact the sales representative.

6.4.2 Procedure for Extracting Maintenance Information when an endless System Loop Occurred

This section describes the procedures for extracting maintenance information when an endless system loop occurs.

- A system loop occurred.
  If a CLI command entry is not accepted for an extended period of time, a system loop may exist.
- Press the "dump" switch on the device's front panel.
  The maintenance information is automatically saved when the "dump" switch is pressed, and then the system restarts.
- ***Reporting system logs on dump outputs/Reporting traps
  After the system retorts, a system log is issued to indicate that a forced system dump was generated. Configuring an SNMP trap in advance causes a trap indicating the occurrence of a system failure to be reported to a system administrator.*** Use previously edited bullet***
- Viewing maintenance information history
  Using the "show maintenance" command, check that the maintenance information was saved.

```
xg# show maintenance
Maintenance Information        2007/01/22-15:55:20
==================================================
NO  Type                        Occurred Time
--- --------------------------- -------------------
  1 system dump(Dump switch)    2007/01/22-18:21:23
==================================================
```

  The maintenance information that was saved by the "dump" switch is represented by "system dump(Dump switch)" under the "Type" column.
- Extracting maintenance information
  Using the "tftp put-maintenance" or "scp put-maintenance" command, forward the maintenance information to a remote server.
- Contact the sales representative.

6.4.3 Procedure for Extracting Maintenance Information when a Malfunction Occurs

This section describes the procedures for extracting maintenance information when a malfunction occurs.

- A malfunction occurred.
  When a function configured for the device fails to operate properly, the maintenance information can be extracted.
- Using the "save maintenance" command, save the maintenance information.
- Viewing maintenance information history
  Using the "show maintenance" command, check that the maintenance information was saved.

```
xg# show maintenance
Maintenance Information        2007/01/22-15:55:20
==================================================
NO  Type                        Occurred Time
--- --------------------------- -------------------
  1 system state               2007/01/22-20:58:14
==================================================
```

  The maintenance information that was saved by the "save maintenance" command is represented by "system state" under the "Type" column.
- Extracting maintenance information
  Using the "tftp put-maintenance" or "scp put-maintenance" command, forward the maintenance information to a remote server.
- Contact the sales representative.

Chapter 7 Troubleshooting

This chapter describes how to solve problems that might be encountered when using the device.

7.1 Restoring Factory Defaults

7.1.1 Resetting startup-config to Factory Defaults

To reset all settings in the device's startup-config file to the factory defaults:

- Using the "reset factory-default" command, reset the contents of the startup-config file to the factory defaults.

When the command is executed, a message appears requesting confirmation of the restart.

```
xg# reset factory-default
Do you restart system with setting to factory-default? (y/n) : ←A confirmation message is
                                                                 displayed.
```

If the response is "y" or "Y", the contents of the startup-config file are reset to the factory defaults and the system restarts. To cancel the process, respond to this question with any keys other than "y " and "Y".

Note

- The login password is not stored in the startup-config file. To change the login password, the "password" command must be used.
- Timezone and summer time settings will be re-initialized. After restarting the system set the timezone and summer time settings as necessary.

7.1.2 Selecting the Alternate Firmware Image

When the system successfully starts up, the firmware image to be run can be selected by following the procedure described in "Selecting Firmware".

If the system fails to start up, select the alternate firmware for reboot by executing the following sequence immediately after turning on the device.

- Connect the device to an active serial terminal.
- Turn on the device.
- Hold down the [#] key and the following message will appear on the serial terminal screen.

```
Preparing to boot
```

- At the XG_LOADER> prompt, type "boot", and then specify the firmware image number to run.

```
XG_LOADER> boot { 1 | 2 }
```

To determine the firmware number to specify, use the "firminfo" command. The "firminfo" command allows checking the firmware versions (E#/L#) and the number that corresponds to the firmware image to run.

For the firmware versions (E#/L#), check the "Firm EL of region 1" and "Firm EL of region 2" fields. For the number that corresponds to the firmware image to run, check the number that appears in the "Region being used now" field. Specify the other firmware number in the "boot" command.

In the following example, 2 is specified for the firmware number in the "boot" command (1 is assigned to the firmware image that is to be run).

```
XG_LOADER> firminfo
Firm EL of region 1     : 10.11 Z01 (1121772145)
Firm EL of region 2     : 10.10 Z01 (1121770019)
Boot loader version     : 10.10 Z01
Region being used now   : 1
Region to be used next  : 1
Status flag of region 1: CURRENT FIRM
Status flag of region 2: OLD FIRM
```

7.1.3 Restoring Factory Defaults

If the system still fails to start up with another firmware image selected, perform the following procedure to restore the device to factory defaults.

(Step 1)

- Connect the device to a serial terminal.
- Turn on the device.
- Hold down the [#] key and the following message will appear on the serial terminal screen.

```
Preparing to boot
```

- At the XG_LOADER> prompt, enter the following command.

```
XG_LOADER> boot init
```

When the above command is executed, the startup-config, time zone and summer time settings, and password of the device are restored to the factory defaults and the system restarts,

If the system still fails to start up, perform the following procedure.

(Step 2)

- Turn off the device and on again.
- Hold down the [#] key and the following message will appear on the serial terminal screen.

```
Preparing to boot
```

- At the XG_LOADER> prompt, enter the following command.

```
XG_LOADER> clear setup
```

When Step 2 is executed following Step 1, all settings in the device are re-initialized. The system then restarts. Entering the "clear setup" command displays the following message:

```
Are you sure to continue [y/<n>]?
```

Explanation

If the response is "y" or "Y", the device's all settings are reset to the factory defaults and the system restarts. To cancel the process, respond to this message with "n" or "N".

- The following message appears while the system is rebooting. Note that it does not indicate a failure if it appears after the command was executed.

```
*** Warning - bad CRC, using default environment
```

Explanation

The boot loader's system startup data area was initialized.

```
XG WARNING[S7521]: init-firmup: Firmware update information is initialized for region %1$.
```

Explanation

The firmware update information area was initialized.
[[Inserted string]]%1$: Firmware number

Note

- Timezone and summer time settings will be re-initialized. After restarting the system, set the timezone and summer time settings as necessary.
- There is a case that Alarm lamp turns on after executing this command. Restart the device to turn off it.

APPENDICES

Appendix A Event Logs

This appendix describes event logs that are extracted from the device, including message IDs, severities, message content details, and actions to take.
The severities of the event logs are classified into 4 levels -- CRITICAL, ERROR, WARNING, and INFO.
To display event logs, run the "show log" command in the operator EXEC mode or in the administrator EXEC mode.

A.1 Overview of Event Logs

This section summarizes messages that are written to logs.
The message ID format is defined as described in "Format of Log Message".

- Message numbers, each starting with an "S", are events that received SNMP trap notifications
- Message numbers, each starting with a "P", are events that did not receive SNMP trap notifications

The following table lists the abbreviated function names and message numbers.

Abbreviated function name	Message number range	Description
env	0 - 999	Health monitoring
kernel	1000 - 1999	Basic control
swc	2000 - 2999	Layer 2 basic control
npm	3000 - 3299	Network protocol control
clim	3300 - 3999	Basic CLI control
xgsh	4000 - 4499	CLI command history
rstp	4500 - 4999	Rapid Spanning Tree (RSTP) control
lacp	5000 - 5499	LACP control
sys	7400 - 7499	Maintenance support function
update	7500 - 7999	Firmware update
snmp	8500 - 8599	SNMP control
ntp	8600 - 8699	NTP (Network Time Protocol) control

A.2 List of Event Logs

This section provides an explanation of message contents and actions to take for the associated message ID and severity in ascending numerical order. There is no solution provided for messages that do not required action.

A.2.1 env (Health Monitoring: 0-999)

Message ID Severity	Message/Explanation/Solution

S0101
ERROR
	`%1$ Temperature is out of range. (%2$ %3$)`
	
	Explanation
	The temperature is out range for normal operation.
	● [[Inserted string]]%1$: Location of detected temperature error.
	`Internal: The temperature inside the chassis`
	● [[Inserted string]]%2$, %3$: Temperature value
	
	Solution
	Confirm the following checks on the device:
	● Check that the air vent is not blocked.
	● Check that the temperature of the switch environment is within the limits specified.
	If there is no air vent blockage and the ambient temperature is within specifications, note the message contents and contact the sales representative.

S0102 WARNING	`PWR-%1$ ALARM is detected.` **Explanation** A power supply error was detected. ● [[Inserted string]]%1$: Power supply unit number **Solution** Replace the power supply unit.
S0104 WARNING	`PWR-%1$ is Off Line.` **Explanation** AC power is not reaching one of the power supply units. ● [[Inserted string]]%1$: Power supply unit number **Solution** Check the AC cable and plugs.
P0105 INFO	`PWR-%1$ is On Line.` **Explanation** Power was restored to the power supply unit. ● [[Inserted string]]%1$: Power supply unit number
S0106 INFO	`PWR-%1$ is Removed.` **Explanation** The power supply unit was removed. ● [[Inserted string]]%1$: Power supply unit number **Solution** If this message is received at times other than during hot swap, check for proper installation.
P0107 INFO	`PWR-%1$ is Inserted.` **Explanation** A power supply unit was installed. ● [[Inserted string]]%1$: Power supply unit number **Solution** If this message is received at times other than during hot swap, check for proper installation.
S0108 ERROR	`%1$ is out of range. (%2$)` **Explanation** A supply voltage error was detected. ● [[Inserted string]]%1$: Displays the types of power supply fault(s) (VDP/VDE/VDR/VDD/VDN/3.3V Main/12V/3.3V(IF)/12V(IF)). ● [[Inserted string]]%2$: Value that represents the power supply fault **Solution** Note the message contents and contact the sales representative.

Message ID Severity	Message/Explanation/Solution
S0109 WARNING	`%1$ Speed is below the Low Limit. (%2$ %3$)` **Explanation** The speed of a fan is below limit. ● [[Inserted string]]%1$: Displays the location of the detected fan speed error. Rear Fan-0: Rear fan 0 Rear Fan-1: Rear fan 1 PWR-0 Fan: Fan installed in power supply unit 0 PWR-1 Fan: Fan installed in power supply unit 1 ● [[Inserted string]]%2$, %3$: Fan speed. **Solution** Replace the fan unit.
P0110 INFO	`%1$ Speed is good.` **Explanation** The speed of a fan returned to normal. ● [[Inserted string]]%1$: Identifies the fan whose normal speed was restored. Rear Fan-0: Rear fan 0 Rear Fan-1: Rear fan 1 PWR-0 Fan: Fan installed in power supply unit 0 PWR-1 Fan: Fan installed in power supply unit 1
S0111 INFO	`%1$ is Removed.` **Explanation** A fan was removed. ● [[Inserted string]]%1$: Identifies the fan removed. Rear Fan-0: Rear fan 0 Rear Fan-1: Rear fan 1
P0112 INFO	`%1$ is Inserted.` **Explanation** A fan was installed. ● [[Inserted string]]%1$: Identifies the fan installed. Rear Fan-0: Rear fan 0 Rear Fan-1: Rear fan 1
P0113 INFO	`port %1$ Plug-In.` **Explanation** An XFP was installed. ● [[Inserted string]]%1$: The port number of the installed XFP
P0114 INFO	`port %1$ Plug-Out.` **Explanation** An XFP was removed. ● [[Inserted string]]%1$: The port number of the XFP removed
P0120 INFO	`Fan Speed was changed into high speed.` **Explanation** The fan speed changed from normal to high speed.
P0121 INFO	`Fan Speed was changed into normal speed.` **Explanation** The fan speed changed from high to normal speed.
S0122 ERROR	`port %1$ PHY Alarm is detected. (%2$)` **Explanation** An XFP alarm was detected. If a high temperature is detected, the device will shut down the XFP. ● [[Inserted string]]%1$: Number assigned to the port that detected the alarm. ● [[Inserted string]]%2$: Displays additional information on the alarm. **Solution** Check the XFP connection and temperature around the XFP. If the same message is displayed after taking appropriate action, note the message contents and contact the sales representative.
S0123 WARNING	`port %1$ PHY Warning is detected. (%2$)` **Explanation** An XFP warning was detected. ● [[Inserted string]]%1$: Number assigned to the port that detected the warning. ● [[Inserted string]]%2$: Displays additional information on the warning. **Solution** The XFP is still good, but a failure may occur if the condition persists. Check the XFP connection and temperature around the XFP. If the same message is displayed after taking appropriate action, note the message contents and contact the sales representative.

Message ID Severity	Message/Explanation/Solution
S0124 Info	`Internal Temperature is high. (%1$ %2$)` **Explanation** The temperature is high. The system will be shut down if the temperature rises. ● [[Inserted string]]%1$, %2$: Temperature value **Solution** Perform the following checks on the device: ● Check that the air vent is not blocked. ● Check the temperature of the switch environment is within the limits specified.
S0125 CRITICAL	`Shutdown the system because of high temperature alarm. (%1$ %2$)` **Explanation** The system was shut down because of high temperature alarm. ● [[Inserted string]]%1$, %2$: Temperature value **Solution** Perform the following checks on the device: ● Check that the air vent is not blocked. ● Check the temperature of the switch environment is within the limits specified. If the message is displayed even though the device was properly installed, note the message contents and contact the sales representative.
S0126 ERROR	`AC and DC PSUs are mounted.` **Explanation** The device mounts both AC PSU and DC PSU. **Solution** AC PSU and DC PSU should not be mounted simultaneously. Make sure to mount the same type of PSU.

A.2.2 kernel (Basic Control: 1000-1999)

Message ID Severity	Message/Explanation/Solution
S1000 CRITICAL	`Abnormal reset occurred (WatchDog Reset: code=%1$)` **Explanation** The fault monitor control detected an error and rebooted the device. ● [[Inserted string]]%1$: Additional information that indicates the cause of the reset. **Solution** Obtain maintenance information using the "tftp put-maintenance" or "`scp put-maintenance`" command after restarting the system then note the message content before contacting the sales representative.
S1001 CRITICAL	`MAC address in EEPROM is invalid.` **Explanation** An error occurred in the device that stores the device's MAC addresses. **Solution** Note the message contents and contact the sales representative.
P1100 INFO	`%1$: config: auto-negotiation on, %2$` **Explanation** Management LAN auto-negotiation is being performed. ● [[Inserted string]]%1$: Name of target network interface ● [[Inserted string]]%2$: Displays supported features (speed and duplex).
P1101 INFO	`%1$: status: link %2$` **Explanation** The link status of the management LAN changed. ● [[Inserted string]]%1$: Name of target network interface ● [[Inserted string]]%2$: Displays details of the current link state.
S1900 CRITICAL	`Core dumped %1$` **Explanation** A critical firmware error was detected and a process dump was output. ● [[Inserted string]]%1$: Process number **Solution** Obtain maintenance information using the "tftp put-maintenance" or "`scp put-maintenance`" command then take note of the message content before contacting the sales representative.

Message ID Severity	Message/Explanation/Solution
S1960 ERROR	`Too many DRAM SBE detected.(%1$)` **Explanation** The software detected too many DRAM single bit errors. No more events will be logged. ● [[Inserted string]]%1$: Details about error **Solution** The device supports single bit ECC, so the error is corrected. But a failure may occur if the error happens again after a system reset. Note this message and those displayed above and below it then contact the sales representative. This message type may not be recorded in the log.
S1970 WARNING	`DRAM SBE detected.` **Explanation** The software detected DRAM single bit error. **Solution** The device supports single bit ECC, so the error is corrected.

A.2.3 swc (Layer 2 Basic Control: 2000-2999)

Message ID Severity	Message/Explanation/Solution
S2103 ERROR	`Output Queue MBE detected. %1$` **Explanation** An uncorrectable error was detected in the switch chip. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** Note the message contents and contact the sales representative.
S2104 ERROR	`Disabling port %1$.` **Explanation** A failure occurred on the switch chip communication port. The port was disabled. ● [[Inserted string]]%1$: Port number **Solution** Note the message contents and contact the sales representative.
S2105 ERROR	`Tag Memory MBE detected. %1$` **Explanation** An uncorrectable error was detected in the switch chip. ● [[Inserted string]]%1$: Port number **Solution** Note the message contents and contact the sales representative.
S2106 ERROR	`Input Buffer Tag Memory MBE detected. %1$` **Explanation** An uncorrectable error was detected in the switch chip. ● [[Inserted string]]%1$: Port number **Solution** Note the message contents and contact the sales representative.
S2107 ERROR	`Too Many Input Queue Tag Memory MBE Errors. LOG Disabled.` **Explanation** An uncorrectable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** Note the message contents and contact the sales representative.
S2110 ERROR	`CM Buffer MBE detected. %1$` **Explanation** An uncorrectable error was detected in the switch chip. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** Note the message contents and contact the sales representative.
S2111 ERROR	`Drop Queue MBE detected. %1$` **Explanation** An uncorrectable error was detected in the switch chip. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** Note the message contents and contact the sales representative.

Message ID Severity	Message/Explanation/Solution
S2112 ERROR	`ME Halt detected. %1$` **Explanation** An uncorrectable error was detected in the switch chip. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** Note the message contents and contact the sales representative.
S2200 WARNING	`MAC Table Error detected. %1$` **Explanation** An uncorrectable error was detected in the MAC address management table. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** Note the message contents and contact the sales representative.
S2201 WARNING	`Too Many MAC Table Error. Reset Switch LSI.` **Explanation** An uncorrectable error was repeatedly detected in the MAC address management table. The switch chip was reset. **Solution** Note the message contents and contact the sales representative.
S2202 WARNING	`VLAN Table MBE detected. %1$` **Explanation** An uncorrectable error was detected in the VLAN management table. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** Note the message contents and contact the sales representative.
S2203 WARNING	`VLAN Table SBE detected. %1$` **Explanation** An uncorrectable error was detected in the VLAN management table. It is automatically corrected by hardware. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** If the same message reappears after restarting the switch, note the message contents and contact the sales representative.
S2204 WARNING	`Too Many VLAN Table MBE Errors. Reset Switch LSI.` **Explanation** An uncorrectable error was repeatedly detected in the VLAN management table. The switch chip was reset. **Solution** If the same message reappears after restarting the switch, note the message contents and contact the sales representative.
S2205 WARNING	`Too Many VLAN Table SBE Error. Log Disabled.` **Explanation** A correctable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** Note the message contents and contact the sales representative.
S2206 WARNING	`Multicast State Table Error detected. %1$` **Explanation** An uncorrectable error was detected in the switch chip. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** Note the message contents and contact the sales representative.
S2207 WARNING	`Too Many MST Errors. Reset Switch LSI.` **Explanation** An uncorrectable error was repeatedly detected in the switch chip. The switch chip was reset. **Solution** Note the message contents and contact the sales representative.

Message ID Severity	Message/Explanation/Solution
S2208 WARNING	`Stream Memory Tag MBE detected. %1$` **Explanation** An uncorrectable error was detected in the switch chip. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** Note the message contents and contact the sales representative.
S2209 WARNING	`Too Many SMT MBE Errors. LOG Disabled.` **Explanation** An uncorrectable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** If the same message reappears after restarting the switch, note the message contents and contact the sales representative.
S2210 WARNING	`Stream Memory Tag SBE detected. %1$` **Explanation** A correctable error was detected in the switch chip. It is automatically corrected by hardware. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** If the same message reappears after restarting the switch, note the message contents and contact the sales representative.
S2211 WARNING	`Too Many SMT SBE Errors. LOG Disabled.` **Explanation** A correctable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** Note the message contents and contact the sales representative.
S2212 WARNING	`Output Queue SBE detected. %1$` **Explanation** A correctable error was detected in the switch chip. It is automatically corrected by hardware. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** Note the message contents and contact the sales representative.
S2213 WARNING	`Too Many Output Queue SBE Errors. LOG Disabled.` **Explanation** A correctable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** Note the message contents and contact the sales representative.
S2214 WARNING	`Tag Memory SBE detected. %1$` **Explanation** A correctable error was detected in the switch chip. It is automatically corrected by hardware. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** If the same message reappears after restarting the switch, note the message contents and contact the sales representative.
S2215 WARNING	`Too Many Tag Memory SBE Errors. LOG Disabled.` **Explanation** A correctable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** Note the message contents and contact the sales representative.
S2216 WARNING	`Input Buffer Tag Memory SBE detected. %1$` **Explanation** A correctable error was detected in the switch chip. It is automatically corrected by hardware. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** If the same message reappears after restarting the switch, note the message contents and contact the sales representative.

Message ID Severity	Message/Explanation/Solution
S2217 WARNING	`Too Many Input Queue Tag Memory SBE Errors. LOG Disabled.` **Explanation** A correctable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** Note the message contents and contact the sales representative.
S2218 WARNING	`MAC address learning failed.` **Explanation** Failed to learn the MAC address. **Solution** Delete the unused static MAC address. Since MAC addresses are managed with a hashing algorithm, a message stating the address cannot be registered may be displayed even though the number of addresses registered is less than the number that can be registered. If the message is displayed even though no static MAC address is unregistered, note the message contents and contact the sales representative.
S2219 WARNING	`Drop Queue SBE detected. %1$` **Explanation** A correctable error was detected in the switch chip. It is automatically corrected by hardware. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** If the same message reappears after restarting the switch, note the message contents and contact the sales representative.
S2220 WARNING	`Too Many Drop Queue SBE Errors. LOG Disabled.` **Explanation** A correctable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** Note the message contents and contact the sales representative.
S2221 WARNING	`MAC Table SBE detected. %1$` **Explanation** A correctable error was detected in the switch chip. It is automatically corrected by hardware. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** If the same message reappears after restarting the switch, note the message contents and contact the sales representative.
S2222 WARNING	`Too Many MAC Table SBE Error. LOG Disabled.` **Explanation** A correctable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** Note the message contents and contact the sales representative.
S2223 WARNING	`Multicast State Table SBE detected. %1$` **Explanation** A correctable error was detected in the switch chip. It is automatically corrected by hardware. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** If the same message reappears after restarting the switch, note the message contents and contact the sales representative.
S2224 WARNING	`Too Many MST SBE Errors. LOG Disabled.` **Explanation** A correctable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** Note the message contents and contact the sales representative.
S2225 WARNING	`CM Buffer SBE detected. %1$` **Explanation** A correctable error was detected in the switch chip. It is automatically corrected by hardware. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** If the same message reappears after restarting the switch, note the message contents and contact the sales representative.

Message ID Severity	Message/Explanation/Solution
S2226 WARNING	`Too Many CM Buffer SBE Errors. LOG Disabled.` **Explanation** A correctable error was repeatedly detected in the switch chip. Logging for this event is disabled. **Solution** Note the message contents and contact the sales representative.
S2401 ERROR	`System Error: %1$` **Explanation** A system error of Layer2 basic management module was detected. ● [[Inserted string]]%1$: Supplementary code for the error **Solution** Note the message contents and contact the sales representative.

A.2.4 npm (Network Protocol Control: 3000-3299)

Message ID Severity	Message/Explanation/Solution
S3001 INFO	`Cold Start or Warm Start.` **Explanation** The system was turned on.
S3002 INFO	`Link down %1$. (%2$)` **Explanation** Port status changed from a link up to a link down state. ● [[Inserted string]]%1$: Information on the port whose status changed to a link down. ● [[Inserted string]]%2$: Cause of link down. For details, refer to "Link Status Detail" of the "show interface" command.
S3003 INFO	`Link up %1$.` **Explanation** Port status changed to a link up state. ● [[Inserted string]]%1$: Information on the port whose status changed to link up.
S3004 WARNING	`%1$ detected storm drop.` **Explanation** A broadcast storm was detected. ● [[Inserted string]]%1$: Information on the port that dropped broadcast frames. **Solution** A loop topology may exist on the network. Review the network configuration.
S3005 WARNING	`%1$ detected port security violation.` **Explanation** A violating packet was detected by Port Security enabled. ● [[Inserted string]]%1$: Information on the port that detected the violating packet. **Solution** Investigate the cause for receiving violating packets.
S3006 WARNING	`%1$ detected loopback alert.` **Explanation** A packet loop was detected. ● [[Inserted string]]%1$: Information on the port that detected the loop. **Solution** A loop topology may exist on the network. Review the network configuration. A loopback alert can occur when the destination MAC address of a received frame was registered in the MAC address table with the receiving port registered as a destination. In other words, a loopback alert can occur even if there is no loop in the network.
P3009 INFO	`%1$ has been attached to %2$.` **Explanation** The physical port was attached to a link aggregation group. ● [[Inserted string]]%1$: Physical port information ● [[Inserted string]]%2$: Aggregation group information
P3010 INFO	`%1$ has been detached.` **Explanation** The physical port was detached from a link aggregation group. ● [[Inserted string]]%1$: Information on physical port detached

Message ID Severity	Message/Explanation/Solution
P3011 INFO	`%1$ link status details change %2$.` **Explanation** The link status of the port changed. ● [[Inserted string]]%1$: Port information ● [[Inserted string]]%2$: New status of the port
P3012 INFO	`%1$ state is changed to %2$.` **Explanation** The STP port state changed. ● [[Inserted string]]%1$: Port information ● [[Inserted string]]%2$: New state of the STP port
P3013 INFO	`Change ingress-bandwidth %1$ %2$` **Explanation** The value set in "ingress-bandwidth" changed. ● [[Inserted string]]%1$: Port information ● [[Inserted string]]%2$: New value of "ingress-bandwidth"
P3100 INFO	`%1$ has been created.` **Explanation** A link aggregation group was added. ● [[Inserted string]]%1$: Aggregation group information
P3101 INFO	`%1$ has been deleted.` **Explanation** A link aggregation group was deleted. ● [[Inserted string]]%1$: Aggregation group information
P3102 INFO	`Initialize LPT setting %1$.` **Explanation** The link pass through setting was initialized. ● [[Inserted string]]%1$: Port information
P3103 INFO	`Released LPT setting %1$ from %2$.` **Explanation** The link pass through setting configured for the port was removed when the port was configured as a member of a link aggregation group. ● [[Inserted string]]%1$: Information on the removed port (link status information was sent) ● [[Inserted string]]%2$: Information on the monitored port that was removed.
P3200 INFO	`Learned an IGMP multicast router automatically. vlan-%1$ agg-port %2$` **Explanation** IGMP snooping learned a multicast router. ● [[Inserted string]]%1$: VLAN ID ● [[Inserted string]]%2$: Learned aggregation group information
P3201 INFO	`Learned an IGMP multicast router automatically. vlan-%1$ port %2$` **Explanation** IGMP snooping learned a multicast router.
P3202 WARNING	`Received IGMP packet without IP header.` **Explanation** Received a frame with a size smaller than that described in the IP header. **Solution** Investigate the cause of faulty frames being sent to the device.
P3203 WARNING	`Received IGMP packet with illegal IP version.` **Explanation** Received a frame with an illegal IP header version. **Solution** Investigate the cause of faulty frames being sent to the device.
P3204 WARNING	`Received IGMP packet with wrong checksum in IP header.` **Explanation** Received a frame with an incorrect IP header checksum. **Solution** Investigate the cause of faulty frames being sent to the device.
P3205 WARNING	`Received IGMP packet with wrong checksum in IGMP header.` **Explanation** Received a frame with an incorrect IGMP header checksum. **Solution** Investigate the cause of faulty frames being sent to the device.

Message ID Severity	Message/Explanation/Solution
P3206 WARNING	`Destination IP-address doesn't match with IGMP group address in IGMP report message.` **Explanation** Received a frame containing at destination IP address that does not match the IGMP group address in an IGMP Report message. **Solution** Investigate the cause of faulty frames being sent to the device.
P3207 WARNING	`Received illegal IGMP packet.` **Explanation** Received a frame from an undefined IGMP type. **Solution** Investigate the cause of faulty frames being sent to the device.
P3208 WARNING	`Bad destination IP-address in IGMP leave message.` **Explanation** Received a frame containing an incorrect destination address in an IGMP Leave message. **Solution** Investigate the cause of faulty frames being sent to the device.
P3209 WARNING	`Received invalid multicast group address in IGMP packet. group address(%1$) from(%2$)` **Explanation** Received a frame containing a non-multicast group address in an IGMP Report message. ● [[Inserted string]]%1$: IP group address ● [[Inserted string]]%2$: Source IP address **Solution** Investigate the cause of faulty frames being sent to the device.
P3210 WARNING	`Cannot register group address more than max-group($1$) per VLAN(%2$) by IGMP snooping.` **Explanation** Since the number of group addresses that can be registered using IGMP Snooping reached the upper limit specified in "max-group", no more group addresses can be registered. ● [[Inserted string]]%1$: The maximum number of groups that can be registered using the relevant VLAN ● [[Inserted string]]%2$: VLAN ID **Solution** Increase the maximum number of groups using the "ip snooping vlan max-group" command.
P3211 INFO	`IGMP snooping has added multicast group address. group(%1$) vlan-%2$ agg-port %3$` **Explanation** IGMP snooping added a multicast group MAC address. ● [[Inserted string]]%1$: Registered IP group address ● [[Inserted string]]%2$: Registered VLAN ID ● [[Inserted string]]%3$: Learned aggregation group information
P3212 INFO	`IGMP snooping has added multicast group address. group(%1$) vlan-%2$ port %3$` **Explanation** IGMP snooping added a multicast group MAC address. ● [[Inserted string]]%1$: Registered IP group address ● [[Inserted string]]%2$: Registered VLAN ID ● [[Inserted string]]%3$: Registered port number
P3213 INFO	`IGMP snooping has added multicast group address of mrouter. group(%1$) vlan-%2$ agg-port %3$` **Explanation** IGMP snooping added a multicast group MAC address to a multicast router port. ● [[Inserted string]]%1$: Registered IP group address ● [[Inserted string]]%2$: Registered VLAN ID ● [[Inserted string]]%3$: Aggregation group number assigned to the registered multicast router
P3214 INFO	`IGMP snooping has added multicast group address of mrouter. group(%1$) vlan-%2$ port %3$` **Explanation** IGMP snooping added a multicast group MAC address to a multicast router port. ● [[Inserted string]]%1$: Registered IP group address ● [[Inserted string]]%2$: Registered VLAN ID ● [[Inserted string]]%3$: Port number assigned to the registered multicast router
P3215 INFO	`IGMP snooping has deleted multicast group address. group(%1$) vlan-%2$ agg-port %3$` **Explanation** IGMP snooping deleted a multicast group MAC address. ● [[Inserted string]]%1$: Deleted IP group address ● [[Inserted string]]%2$: Deleted VLAN ID ● [[Inserted string]]%3$: Deleted aggregation group number

Message ID Severity	Message/Explanation/Solution
P3216 INFO	`IGMP snooping has deleted multicast group address. Group(%1$) vlan-%2$ port %3$` **Explanation** IGMP snooping deleted a multicast group MAC address. ● [[Inserted string]]%1$: Deleted IP group address ● [[Inserted string]]%2$: Deleted VLAN ID ● [[Inserted string]]%3$: Deleted port number
P3217 INFO	`IGMP snooping has deleted multicast group address of mrouter. group(%1$) vlan-%2$ agg-port %3$` **Explanation** IGMP snooping deleted a multicast group MAC address from a multicast router port. ● [[Inserted string]]%1$: Deleted IP group address ● [[Inserted string]]%2$: Deleted VLAN ID ● [[Inserted string]]%3$: Aggregation group number assigned to the deleted multicast router
P3218 INFO	`IGMP snooping has deleted multicast group address of mrouter. group(%1$) vlan-%2$ port %3$` **Explanation** IGMP snooping deleted a multicast group MAC address from a multicast router port. ● [[Inserted string]]%1$: Deleted IP group address ● [[Inserted string]]%2$: Deleted VLAN ID ● [[Inserted string]]%3$: Port number assigned to the deleted multicast router
P3219 WARNING	`Cannot register group address more than %1$ per system by IGMP snooping. vlan($2$)` **Explanation** Since the number of group addresses that can be registered using IGMP Snooping reached the upper limit, no more group addresses can be registered. ● [[Inserted string]]%1$: The maximum number of groups that can be registered for the entire switch ● [[Inserted string]]%2$: Failed VLAN registration **Solution** Review the registered multicast group addresses using the "show bridge mac-address-table" command to delete unnecessary multicast addresses.

A.2.5 clim (Basic CLI Control: 3300-3999)

Message ID Severity	Message/Explanation/Solution
P3300 INFO	`cmd-exec[startup]: %1$` **Explanation** The command in the startup-config was executed. ● [[Inserted string]]%1$: Command string executed in the startup-config.
P3301 INFO	`cmd-result[startup]: success` **Explanation** The command in the startup-config was successfully completed.
P3302 INFO	`cmd-result[startup]: error` **Explanation** The command in the startup-config failed.
P3303 INFO	`startup-config start.` **Explanation** Starts startup-config file processing.
P3304 INFO	`startup-config end.` **Explanation** Startup-config file processing was successfully completed.
P3305 INFO	Line has connected. line-ID=%1$ **Explanation** The telnet or SSH terminal was connected. ● [[Inserted string]]%1$: Terminal ID
P3306 INFO	`startup-config end(none).` **Explanation** The startup-config file was not found.
P3307 INFO	`startup-config end(error).` **Explanation** Startup-config file processing failed.
P3308 INFO	`cmd-result[startup]: skip` **Explanation** Since the attempt to execute the previous command in startup-config resulted in an error, execution of the next command was skipped.
P3309 INFO	`Line has disconnected. line-ID=%1$` **Explanation** The telnet or SSH terminal was disconnected. ● [[Inserted string]]%1$: Terminal ID
P3310 WARNING	`Cannot find host %1$.` **Explanation** Failed to find an IP address for the host name specified with the "log send" command. ● [[Inserted string]]%1$: Host name specified with the "log send" command **Solution** Review the host name defined. Check that DNS was configured.

A.2.6 xgsh (CLI Command History: 4000-4499)

Message ID Severity	Message/Explanation/Solution
P4001 INFO	`%1$ cmd-exec[%2$]: %3$` **Explanation** The command was executed. ● [[Inserted string]]%1$: Username ● [[Inserted string]]%2$: Terminal ID ● [[Inserted string]]%3$: Command string to be executed
P4002 INFO	`%1$ cmd-result[%2$]: success` **Explanation** The command was successfully completed. ● [[Inserted string]]%1$: Username ● [[Inserted string]]%2$: Terminal ID
P4003 INFO	`%1$ cmd-result[%2$]: error` **Explanation** The command failed. ● [[Inserted string]]%1$: Username ● [[Inserted string]]%2$: Terminal ID

A.2.7 rstp (Rapid Spanning Tree Control: 4500-4999)

Message ID Severity	Message/Explanation/Solution
S4501 WARNING	`Root bridge changed.` **Explanation** The root bridge changed.
S4502 WARNING	`Topology changed.` **Explanation** The topology changed.
S4503 WARNING	`Received BPDU on PortFast enable port. shutting down %1$.` **Explanation** A BPDU was received on a Port Fast-enabled port. ● [[Inserted string]]%1$: Name of the port that received the BPDU **Solution** Review the port connection.
P4504 WARNING	`Invalid "Forward delay time" relationship 2*(%1$ - 1) >= %2$.` **Explanation** The setting of STP Forward Delay is invalid. ● [[Inserted string]]%1$: Attempted Forward Delay value change ● [[Inserted string]]%2$: The current Max Age value **Solution** Check that the setting of Forward Delay satisfies the following condition. 2 x ((Forward Delay) - 1) ≥ (Max Age)
P4505 WARNING	`Invalid "Max age" relationship 2*(%1$ - 1) >= %2$.` **Explanation** The setting of STP Max Age is invalid. ● [[Inserted string]]%1$: The current Forward Delay value ● [[Inserted string]]%2$: Attempted Max Age value change **Solution** Check that the setting of Max Age satisfies the following condition. 2 x ((Forward Delay) - 1) ≥ (Max Age)
S4507 WARNING	`Invalid BPDU received on %1$, Bridge becoming root.` **Explanation** The reception of an invalid BPDU triggered a topology change that caused the device to become a root switch. ● [[Inserted string]]%1$: Name of the port that received the BPDU **Solution** Review the network environment for the port connection.

Message ID Severity	Message/Explanation/Solution
P4508 WARNING	`Invalid "Max age" relationship 2*(%1$ + 1) <= %2$.` **Explanation** The setting of STP Max Age is invalid. ● [[Inserted string]]%1$: The current Hello Time value ● [[Inserted string]]%2$: Attempted Max Age value change **Solution** Check that the setting of Max Age satisfies the following condition. Max Age ≥ 2 x (Hello Time + 1)
P4509 WARNING	`Invalid "Hello time" relationship 2*(%1$ + 1) <= %2$.` **Explanation** The setting of Hello Time is invalid. ● [[Inserted string]]%1$: Attempted Hello Time value change ● [[Inserted string]]%2$: The current Max Age value **Solution** Check that the setting of Hello Time satisfies the following condition. Max Age ≥ 2 x (Hello Time + 1)

A.2.8 lacp (LACP Control: 5000-5499)

Message ID Severity	Message/Explanation/Solution
P5001 WARNING	`%1$ detects loopback packet.` **Explanation** Ports being members of the same link aggregation group are connected. ● [[Inserted string]]%1$: Port information **Solution** Review the connection between port being members of the link aggregation.

A.2.9 sys (Maintenance Support Function: 7400-7499)

Message ID Severity	Message/Explanation/Solution
P7400 INFO	`Dump configuration succeeded.` **Explanation** The maintenance support function was successfully initialized.
S7410 WARNING	`Could not save a system-dump file.` **Explanation** An error occurred while storing the system dump file. **Solution** Note the message contents and contact the sales representative.
S7411 ERROR	`Could not execute system-dump.` **Explanation** An error occurred while storing the system dump file. **Solution** Note the message contents and contact the sales representative.
S7490 CRITICAL	`A system-dump has been saved. Cause: critical system error occurred.` **Explanation** An error occurred while storing the system dump file. **Solution** Obtain maintenance information using the "tftp put-maintenance" or "scp put-maintenance" command then take note of the message content before contacting the sales representative.
S7491 CRITICAL	`A system-dump has been saved. Cause: dump switch was pressed.` **Explanation** As the Dump switch was pressed, the system dump was saved. **Solution** Obtain maintenance information using the "tftp put-maintenance" or "scp put-maintenance" command then take note of the message content before contacting the sales representative.

Message ID Severity	Message/Explanation/Solution
S7492 CRITICAL	`A system-dump has been saved. Cause: machine check occurred (memory or bus data error).` **Explanation** A machine check error occurred and a system dump saved. **Solution** Obtain maintenance information using the "tftp put-maintenance" or "scp put-maintenance" command then take note of the message content before contacting the sales representative.
S7493 CRITICAL	`A system-dump has been saved. Cause: machine check occurred (bus timeout).` **Explanation** A machine check error occurred and a system dump saved. **Solution** Obtain maintenance information using the "tftp put-maintenance" or "scp put-maintenance" command then take note of the message content before contacting the sales representative.
S7494 CRITICAL	`A system-dump has been saved. Cause: machine check occurred (memory or bus data error, bus timeout).` **Explanation** A machine check error occurred and a system dump saved. **Solution** Obtain maintenance information using the "tftp put-maintenance" or "scp put-maintenance" command then take note of the message content before contacting the sales representative.
S7495 CRITICAL	`A system-dump has been saved. Cause: machine check occurred.` **Explanation** A machine check error occurred and a system dump saved. **Solution** Obtain maintenance information using the "tftp put-maintenance" or "scp put-maintenance" command then take note of the message content before contacting the sales representative.

A.2.10 update (Firmware Update: 7500-7999)

Message ID Severity	Message/Explanation/Solution
S7500 INFO	`init-firmup: New firmware '%1$' is running.` **Explanation** New updated firmware was initialized. ● [[Inserted string]]%1$: Firmware version information
S7501 INFO	`init-firmup: Firmware '%1$' is running.` **Explanation** New firmware was initialized after "boot" command was issued. ● [[Inserted string]]%1$: Firmware version information
S7520 WARNING	`init-firmup: Booting new firmware failed. Old firmware '%1$' is now running.` **Explanation** Old firmware was invoked because new updated firmware could not initialize. ● [[Inserted string]]%1$: Firmware version information **Solution** Reattempt the update process to boot the new updated firmware. If the message is repeatedly displayed, contact the sales representative.
S7521 WARNING	`init-firmup: Firmware update information is initialized for region %1$.` **Explanation** The firmware information was initialized. ● [[Inserted string]]%1$: Firmware number **Solution** No action is required if this message appears in Step 2 of "Restoring Factory Defaults". If the message is displayed every time the system is booted, contact the sales representative.
S7530 CRITICAL	`init-firmup: Internal error occurred (inconsistency in firmware update information).` **Explanation** An error occurred while processing the firmware update information. ● [[Inserted string]]%1$: Firmware version information **Solution** Note the message contents and contact the sales representative.

Message ID Severity	Message/Explanation/Solution
S7531 CRITICAL	`init-firmup: Internal error occurred (SRAM access error).` **Explanation** An error occurred while processing the firmware update information. **Solution** Note the message contents and contact the sales representative.
S7532 CRITICAL	`init-firmup: Internal error occurred (FlashROM access error).` **Explanation** An error occurred while processing the firmware update information. **Solution** Note the message contents and contact the sales representative.
S7533 CRITICAL	`init-firmup: Internal error occurred (SRAM data error: invalid boot parameter).` **Explanation** An error occurred while processing the firmware update information. **Solution** Note the message contents and contact the sales representative.
P7600 INFO	`firm-update: succeeded (%1$).` **Explanation** The firmware update completed successfully. ● [[Inserted string]]%1$: Firmware version information
P7601 INFO	`firm-update: succeeded (%1$), boot loader updated (%2$).` **Explanation** The firmware update completed successfully. ● [[Inserted string]]%1$: Firmware version information ● [[Inserted string]]%2$: Boot loader version information
S7620 ERROR	`firm-update: failed (reading file error).` **Explanation** An error occurred while updating firmware (failed to read the specified file). **Solution** Check whether the specified file is readable.
S7621 CRITICAL	`firm-update: failed (reading FlashROM error: boot loader).` **Explanation** An error occurred while updating firmware. **Solution** Reattempt the update process. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7622 CRITICAL	`firm-update: failed (writing to FlashROM error: boot loader).` **Explanation** An error occurred while updating firmware. **Solution** Reattempt the update process. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7623 CRITICAL	`firm-update: failed (verification error: boot loader).` **Explanation** An error occurred while updating firmware. **Solution** Reattempt the update process. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7624 ERROR	`firm-update: failed (writing to FlashROM error: kernel).` **Explanation** An error occurred while updating firmware. **Solution** Reattempt the update process. If the message is repeatedly displayed, note the message contents and contact the sales representative.

Message ID Severity	Message/Explanation/Solution
S7625 ERROR	`firm-update: failed (verification error: kernel).` **Explanation** An error occurred while updating firmware. **Solution** Reattempt the update process. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7626 ERROR	`firm-update: failed (writing to FlashROM error: rootfs).` **Explanation** An error occurred while updating firmware. **Solution** Reattempt the update process. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7627 ERROR	`firm-update: failed (verification error: rootfs).` **Explanation** An error occurred while updating firmware. **Solution** Reattempt the update process. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7628 ERROR	`firm-update: failed (writing to FlashROM error: EL).` **Explanation** An error occurred while updating firmware. **Solution** Reattempt the update process. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7629 CRITICAL	`firm-update: failed (SRAM access error).` **Explanation** An error occurred while updating firmware. **Solution** Reattempt the update process. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7630 CRITICAL	`firm-update: failed (SRAM data error: invalid firmware update information).` **Explanation** An error occurred while updating firmware. **Solution** Reattempting the update process after rebooting the device using the "reset" command. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7631 CRITICAL	`firm-update: failed (SRAM data error: invalid boot parameter).` **Explanation** An error occurred while updating firmware. **Solution** Reattempting the update process after rebooting the device using the "reset" command. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7632 CRITICAL	`firm-update: failed (SRAM data error: no boot command).` **Explanation** An error occurred while updating firmware. **Solution** Reattempting the update process after rebooting the device using the "reset" command. If the message is repeatedly displayed, note the message contents and contact the sales representative.
S7699 CRITICAL	`firm-update: failed (unknown error).` **Explanation** An error occurred while updating firmware. **Solution** Note the message contents and contact the sales representative.

A.2.11 snmp (SNMP Control: 8500-8599)

Message ID Severity	Message/Explanation/Solution
S8500 INFO	`SNMP authentication failure.` **Explanation** The device denied an SNMP request from a SNMP manager. **Solution** Review the SNMP permission from the SNMP manager using the "snmp access" command.

S8501
INFO
	`RMON alarm by rising-threshold.`
	` index:%1$ OID:%2$ sample:%3$ value:%4$ rising-threshold:%5$`
	
	Explanation
	The current sampled value was greater than the upper threshold defined by the "rmon alarm" command. A SNMP trap for the corresponding RMON event was generated.
	● [[Inserted string]]%1$: RMON alarm index
	● [[Inserted string]]%2$: OID of MIB object to be monitored
	● [[Inserted string]]%3$: Method of determining threshold
	1: An absolute value is used when determining threshold (absolute)
	2: The difference between the previous and current values is used when determining threshold (delta)
	● [[Inserted string]]%4$: Value of MIB object to be monitored
	● [[Inserted string]]%5$: Upper threshold of MIB object to be monitored

S8502
INFO
	`RMON alarm by falling-threshold.`
	` index:%1$ OID:%2$ sample:%3$ value:%4$ falling-threshold:%5$`
	
	Explanation
	The current sampled value was less than the lower threshold defined by the "rmon alarm" command, and a SNMP trap for the corresponding RMON event was generated.
	● [[Inserted string]]%1$: RMON alarm index
	● [[Inserted string]]%2$: OID of MIB object to be monitored
	● [[Inserted string]]%3$: Method of determining threshold
	1: An absolute value is used when determining threshold (absolute)
	2: The difference between the previous and current values is used when determining threshold (delta)
	● [[Inserted string]]%4$: Value of MIB object to be monitored
	● [[Inserted string]]%5$: Lower threshold of MIB object to be monitored

P8510 WARNING	`Cannot find host %1$.` **Explanation** Failed to find an IP address for the host name specified with the "snmp-server trap" command. ● [[Inserted string]]%1$: Host name specified with the "snmp-server trap" command **Solution** Review the host name defined. Check that DNS was configured.

A.2.12 ntp (NTP Control: 8600-8699)

Message ID Severity	Message/Explanation/Solution
P8601 WARNING	`No server suitable for synchronization found.` **Explanation** No NTP server is found. **Solution** Check the NTP server host name defined by the "ntp-server" command as well as the NTP server operating status.
P8602 INFO	`Time server %1$ offset %2$ sec.` **Explanation** Time synchronization using a NTP server was performed to correct the time. ● [[Inserted string]]%1$: Host name or IP address of the NTP server that corrected the time ● [[Inserted string]]%2$: Corrected time difference in seconds
P8603 WARNING	`Cannot find host %1$.` **Explanation** Failed to find an IP address from the host name specified with the "ntp-server host" command. ● [[Inserted string]]%1$: Host name specified with the "ntp-server host" command **Solution** Review the host name defined. Check that DNS was configured.
P8691 ERROR	`System Error: %1$` **Explanation** A system error occurred while NTP time synchronization was in progress. ● [[Inserted string]]%1$: Additional information on the error **Solution** Note the message contents and contact the sales representative.

A.3 Message Format for Forwarding syslog

The logs output from the device can be forwarded to a syslog server. The device forwards logs in a message format that conforms to the RFC3164 The BSD Syslog Protocol.
The format the device uses to forward a syslog message to the syslog server is shown below.

Format of syslog message in XG2000 series	Description	Format of syslog message in RFC3164	
Priority	Priority string	PRI part	Priority
Time	The time the message was generated (MM:DD:HH:MM:SS)	HEADER part	TimeStamp
Host name	Host name of the device		HostName
Device type	XG	MSG part	Tag
Function type	Abbreviated name for the control that output the message.		Content
Severity	Severity of the message		
Message ID	The code that uniquely identifies the message		
Message	Message text		

The device appends the Priority value at the beginning of the log message then inserts the Device type between the Host name and the Function type before forwarding the message to the specified syslog server.
The Priority value is used to identify the severity and facility of a log message.
It is added according to the following rules.

- Priority must have three, four, or five characters. It starts with an angle bracket "<", followed by a number, followed by an angle bracket ">". Example: <14>
- The Priority value is calculated from the Facility code (Facility) and the Severity code (Severity). The Priority value consists of one, two, or three decimal integers.
- The Priority value is calculated by first multiplying the Facility code by 8 and then adding the numerical value of the Severity code.

The Facility code defined in the device is:

Facility code	Type of Facility
1	random user-level messages

The Severity codes defined in the device are:

Severity code	Description of Severity
2	Critical : critical conditions
3	Error : error conditions
4	Warning : warning conditions
6	Informational : informational messages

Appendix B SNMP Traps

This appendix lists the SNMP traps supported by the device.
Standard SNMP Traps

Trap name	RFC	Trap OID
coldStart	3418	1.3.6.1.6.3.1.1.5.1
linkDown	2863	1.3.6.1.6.3.1.1.5.3
linkUp	2863	1.3.6.1.6.3.1.1.5.4
authenticationFailure	3418	1.3.6.1.6.3.1.1.5.5
risingAlarm	2819	1.3.6.1.2.1.16.0.1
fallingAlarm	2819	1.3.6.1.2.1.16.0.2
newRoot	1493	1.3.6.1.2.1.17.0.1
topologyChange	1493	1.3.6.1.2.1.17.0.2

Enterprise-specific traps that are specific to the device report the following information.
(OID becomes 1.3.6.1.4.1.211.1.127.61.108.* in case of XG2000C, 1.3.6.1.4.1.211.1.127.61.109.* in case of XG2000CR, and 1.3.6.1.4.1.211.1.127.61.110.* in case of XG2000R)

Field	OID	Object name
Trap OID	1.3.6.1.4.1.211.1.127.61.107.2.0."message number"	xg2000***
Variable list	1.3.6.1.4.1.211.1.127.61.107.2.10.1	xg2000TrapLevel
	1.3.6.1.4.1.211.1.127.61.107.2.10.2	xg2000TrapMessage

"xg2000***" differs from one event to another.

"xg2000TrapLevel" indicates the severity of an event. The severities are defined as:

Severity	Value
Critical	0
Error	1
Warning	2
Info	3

"xg2000TrapMessage" indicates a message that relates to an event.
The messages are the same as those for the event logs.

Appendix C List of MIBs

This appendix lists the MIBs supported by the device.
For a definition of each object, refer to RFC.

- MIB-II system group (RFC3418)

`iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1)`

Item number	Object identifier	SYNTAX
1	sysDescr {system 1}	DisplayString
2	sysObjectID {system 2}	OBJECT IDENTIFIER
3	sysUpTime {system 3}	TimeTicks
4	sysContact {system 4}	DisplayString
5	sysName {system 5}	DisplayString
6	sysLocation {system 6}	DisplayString
7	sysServices {system 7}	INTEGER

- IF MIB (RFC2863)

`iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).interface(2)`

Item number	Object identifier	SYNTAX
1	ifNumber {interface 1}	INTEGER32
2	ifTable {interface 2}	NOT-ACCESSIBLE
3	ifEntry {ifTable 1}	NOT-ACCESSIBLE
4	ifIndex {ifEntry 1}	InterfaceIndex
5	ifDescr {ifEntry 2}	DisplayString
6	ifType {ifEntry 3}	IANAifType
7	ifMtu {ifEntry 4}	INTEGER32
8	ifSpeed {ifEntry 5}	Gauge32
9	ifPhysAddress {ifEntry 6}	PhysAddress
10	ifAdminStatus {ifEntry 7}	INTEGER
11	ifOperStatus {ifEntry 8}	INTEGER
12	ifLastChange {ifEntry 9}	TimeTicks
13	ifInOctets {ifEntry 10}	Counter32
14	ifInUcastPkts {ifEntry 11}	Counter32
15	ifInNUcastPkts {ifEntry 12}	Counter32
16	ifInDiscards {ifEntry 13}	Counter32
17	ifInErrors {ifEntry 14}	Counter32
18	ifInUnknownProtos {ifEntry 15}	Counter32
19	ifOutOctets {ifEntry 16}	Counter32
20	ifOutUcastPkts {ifEntry 17}	Counter32
21	ifOutNUcastPkts {ifEntry 18}	Counter32
22	ifOutDiscards {ifEntry 19}	Counter32
23	ifOutErrors {ifEntry 20}	Counter32
24	ifOutQLen {ifEntry 21}	Gauge32

Item number	Object identifier	SYNTAX
25	ifSpecific {ifEntry 22}	OBJECT IDENTIFIER

- Ether-like MIB (RFC2665)

`iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).transmission(10).dot3(7)`

Item number	Object identifier	SYNTAX
1	dot3StatsTable {dot3 2}	NOT-ACCESSIBLE
2	dot3StatsEntry {dot3StatsTable 1}	NOT-ACCESSIBLE
3	dot3StatsIndex {dot3StatsEntry 1}	InterfaceIndex
4	dot3StatsAlignmentErrors {dot3StatsEntry 2}	Counter32
5	dot3StatsFCSErrors {dot3StatsEntry 3}	Counter32
6	dot3StatsSingleCollisionFrames {dot3StatsEntry 4}	Counter32
7	dot3StatsMultipleCollisionFrames {dot3StatsEntry 5}	Counter32
8	dot3StatsSQETestErrors {dot3StatsEntry 6}	Counter32
9	dot3StatsDeferredTransmissions {dot3StatsEntry 7}	Counter32
10	dot3StatsLateCollisions {dot3StatsEntry 8}	Counter32
11	dot3StatsExcessiveCollisions {dot3StatsEntry 9}	Counter32
12	dot3StatsInternalMacTransmitErrors {dot3StatsEntry 10}	Counter32
13	dot3StatsCarrierSenseErrors {dot3StatsEntry 11}	Counter32
14	dot3StatsFrameTooLongs {dot3StatsEntry 13}	Counter32
15	dot3StatsInternalMacReceiveErrors {dot3StatsEntry 16}	Counter32
16	dot3StatsEtherChipSet {dot3StatsEntry 17}	OBJECT IDENTIFIER
17	dot3StatsSymbolErrors {dot3StatsEntry 18}	Counter32
18	dot3StatsDuplexStatus {dot3StatsEntry 19}	INTEGER
19	dot3ControlTable {dot3 9}	NOT-ACCESSIBLE
20	dot3ControlEntry {dot3ControlTable 1}	NOT-ACCESSIBLE
21	dot3ControlFunctionsSupported {dot3ControlEntry 1}	BITS
22	dot3ControlInUnknownOpcodes {dot3ControlEntry 2}	Counter32
23	dot3PauseTable {dot3 10}	NOT-ACCESSIBLE
24	dot3PauseEntry {dot3PauseTable 1}	NOT-ACCESSIBLE
25	dot3PauseAdminMode {dot3PauseEntry 1}	INTEGER
26	dot3PauseOperMode {dot3PauseEntry 2}	INTEGER
27	dot3InPauseFrames {dot3PauseEntry 3}	Counter32
28	dot3OutPauseFrames {dot3PauseEntry 4}	Counter32

- MIB-II snmp group (RFC1213)

`iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).snmp(11)`

Item number	Object identifier	SYNTAX
1	snmpInPkts {snmp 1}	Counter32
2	snmpOutPkts {snmp 2}	Counter32
3	snmpInBadVersions {snmp 3}	Counter32
4	snmpInBadCommunityNames {snmp 4}	Counter32

Item number	Object identifier	SYNTAX
5	snmpInBadCommunityUses {snmp 5}	Counter32
6	snmpInASNParseErrs {snmp 6}	Counter32
7	snmpInTooBigs {snmp 8}	Counter32
8	snmpInNoSuchNames {snmp 9}	Counter32
9	snmpInBadValues {snmp 10}	Counter32
10	snmpInReadOnlys {snmp 11}	Counter32
11	snmpInGenErrs {snmp 12}	Counter32
12	snmpInTotalReqVars {snmp 13}	Counter32
13	snmpInTotalSetVars {snmp 14}	Counter32
14	snmpInGetRequests {snmp 15}	Counter32
15	snmpInGetNexts {snmp 16}	Counter32
16	snmpInSetRequests {snmp 17}	Counter32
17	snmpInGetSolutions {snmp 18}	Counter32
18	snmpInTraps {snmp 19}	Counter32
19	snmpOutTooBigs {snmp 20}	Counter32
20	snmpOutNoSuchNames {snmp 21}	Counter32
21	snmpOutBadValues {snmp 22}	Counter32
22	snmpOutGenErrs {snmp 24}	Counter32
23	snmpOutGetRequests {snmp 25}	Counter32
24	snmpOutGetNexts {snmp 26}	Counter32
25	snmpOutSetRequests {snmp 27}	Counter32
26	snmpOutGetSolutions {snmp 28}	Counter32
27	snmpOutTraps {snmp 29}	Counter32
28	snmpEnableAuthenTraps {snmp 30}	INTEGER
29	snmpSilentDrops {snmp 31}	Counter32
30	snmpProxyDrops {snmp 32}	Counter32

- RMON MIB(statistics group) (RFC2819)
  `iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).rmon(16).statistics(1)`

Item number	Object identifier	SYNTAX
1	etherStatsTable {statistics 1}	NOT-ACCESSIBLE
2	etherStatsEntry {etherStatsTable 1}	NOT-ACCESSIBLE
3	etherStatsIndex {etherStatsEntry 1}	Integer32
4	etherStatsDataSource {etherStatsEntry 2}	OBJECT IDENTIFIER
5	etherStatsDropEvents {etherStatsEntry 3}	Counter32
6	etherStatsOctets {etherStatsEntry 4}	Counter32
7	etherStatsPkts {etherStatsEntry 5}	Counter32
8	etherStatsBroadcastPkts {etherStatsEntry 6}	Counter32
9	etherStatsMulticastPkts {etherStatsEntry 7}	Counter32

Item number	Object identifier	SYNTAX
10	etherStatsCRCAlignErrors {etherStatsEntry 8}	Counter32
11	etherStatsUndersizePkts {etherStatsEntry 9}	Counter32
12	etherStatsOversizePkts {etherStatsEntry 10}	Counter32
13	etherStatsFragments {etherStatsEntry 11}	Counter32
14	etherStatsJabbers {etherStatsEntry 12}	Counter32
15	etherStatsCollisions {etherStatsEntry 13}	Counter32
16	etherStatsPkts64Octets {etherStatsEntry 14}	Counter32
17	etherStatsPkts65to127Octets {etherStatsEntry 15}	Counter32
18	etherStatsPkts128to255Octets {etherStatsEntry 16}	Counter32
19	etherStatsPkts256to511Octets {etherStatsEntry 17}	Counter32
20	etherStatsPkts512to1023Octets {etherStatsEntry 18}	Counter32
21	etherStatsPkts1024to1518Octets {etherStatsEntry 19}	Counter32
22	etherStatsOwner {etherStatsEntry 20}	OwnerString
23	etherStatsStatus {etherStatsEntry 21}	EntryStatus

- RMON MIB (history group) (RFC2819)

`iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).rmon(16).history(2)`

Item number	Object identifier	SYNTAX
1	historyControlTable {history 1}	NOT-ACCESSIBLE
2	historyControlEntry {historyControlTable 1}	NOT-ACCESSIBLE
3	historyControlIndex {historyControlEntry 1}	Integer32
4	historyControlDataSource {historyControlEntry 2}	OBJECT IDENTIFIER
5	historyControlBucketsRequested {historyControlEntry 3}	Integer32
6	historyControlBucketsGranted {historyControlEntry 4}	Integer32
7	historyControlInterval {historyControlEntry 5}	Integer32
8	historyControlOwner {historyControlEntry 6}	OwnerString
9	historyControlStatus {historyControlEntry 7}	EntryStatus
10	etherHistoryTable {history 2}	NOT-ACCESSIBLE
11	etherHistoryEntry {etherHistoryTable 1}	NOT-ACCESSIBLE
12	etherHistoryIndex {etherHistoryEntry 1}	Integer32
13	etherHistorySampleIndex {etherHistoryEntry 2}	Integer32
14	etherHistoryIntervalStart {etherHistoryEntry 3}	TimeTicks
15	etherHistoryDropEvents {etherHistoryEntry 4}	Counter32
16	etherHistoryOctets {etherHistoryEntry 5}	Counter32
17	etherHistoryPkts {etherHistoryEntry 6}	Counter32
18	etherHistoryBroadcastPkts {etherHistoryEntry 7}	Counter32
19	etherHistoryMulticastPkts {etherHistoryEntry 8}	Counter32
20	etherHistoryCRCAlignErrors {etherHistoryEntry 9}	Counter32
21	etherHistoryUndersizePkts {etherHistoryEntry 10}	Counter32

Item number	Object identifier	SYNTAX
22	etherHistoryOversizePts {etherHistoryEntry 11}	Counter32
23	etherHistoryFragments {etherHistoryEntry 12}	Counter32
24	etherHistoryJabbers {etherHistoryEntry 13}	Counter32
25	etherHistoryCollisions {etherHistoryEntry 14}	Counter32
26	etherHistoryUtilization {etherHistoryEntry 15}	Integer32

- RMON MIB (alarm group) (RFC2819)
  `iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).rmon(16).alarm(3)`

Item number	Object identifier	SYNTAX
1	alarmTable {alarm 1}	NOT-ACCESSIBLE
2	alarmEntry {alarmTable 1}	NOT-ACCESSIBLE
3	alarmIndex {alarmEntry 1}	Integer32
4	alarmInterval {alarmEntry 2}	Integer32
5	alarmVariable {alarmEntry 3}	OBJECT IDENTIFIER
6	alarmSampleType {alarmEntry 4}	INTEGER
7	alarmValue {alarmEntry 5}	Integer32
8	alarmStartupAlarm {alarmEntry 6}	INTEGER
9	alarmRisingThreshold {alarmEntry 7}	Integer32
10	alarmFallingThreshold {alarmEntry 8}	Integer32
11	alarmRisingEventIndex {alarmEntry 9}	Integer32
12	alarmFallingEventIndex {alarmEntry 10}	Integer32
13	alarmOwner {alarmEntry 11}	OwnerString
14	alarmStatus {alarmEntry 12}	EntryStatus

- RMON MIB (event group) (RFC2819)
  `iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).rmon(16).event(9)`

Item number	Object identifier	SYNTAX
1	eventTable {event 1}	NOT-ACCESSIBLE
2	eventEntry {eventTable 1}	NOT-ACCESSIBLE
3	eventIndex {eventEntry 1}	Integer32
4	eventDescription {eventEntry 2}	DisplayString
5	eventType {eventEntry 3}	INTEGER
6	eventCommunity {eventEntry 4}	OCTET STRING
7	evenvLastTimeSent {eventEntry 5}	TimeTicks
8	eventOwner {eventEntry 6}	OwnerString
9	eventStatus {eventEntry 7}	EntryStatus
10	logTable {event 2}	NOT-ACCESSIBLE
11	logEntry {logTable 1}	NOT-ACCESSIBLE
12	logEventIndex {logEntry 1}	Integer32
13	logIndex {logEntry 2}	Integer32
14	logTime {logEntry 3}	TimeTicks

Item number	Object identifier	SYNTAX
15	logDescription {logEntry 4}	DisplaySting

- Bridge MIB (RFC1493)

```
iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge (17)
```

Item number	Object identifier	SYNTAX
1	dot1dBase {dot1dBridge 1}	NOT-ACCESSIBLE
2	dot1dBaseBridgeAddress {dot1dBase 1}	MacAddress
3	dot1dBaseNumPorts {dot1dBase 2}	INTEGER
4	dot1dBaseType {dot1dBase 3}	INTEGER
5	dot1dBasePortTable {dot1dBase 4}	NOT-ACCESSIBLE
6	dot1dBasePortEntry {dot1dBasaPortTable 1}	NOT-ACCESSIBLE
7	dot1dBasePort {dot1dBasePortEntry 1}	INTEGER
8	dot1dBasePortIfIndex {dot1dBasePortEntry 2}	INTEGER
9	dot1dBasePortCircuit {dot1dBasePortEntry 3}	OBJECT IDENTIFIER
10	dot1dBasePortDelayExceededDiscards {dot1dBasePortEntry 4}	Counter32
11	dot1dBasePortMtuExceededDiscards {dot1dBasePortEntry 5}	Counter32
12	dot1dStp {dot1dBridge 2}	NOT-ACCESSIBLE
13	dot1dStpProtocolSpecification {dot1dStp 1}	INTEGER
14	dot1dStpPriority {dot1dStp 2}	INTEGER
15	dot1dStpTimeSinceTopologyChange {dot1dStp 3}	TimeTicks
16	dot1dStpTopChanges {dot1dStp 4}	Counter
17	dot1dStpDesignatedRoot {dot1dStp 5}	BridgeID
18	dot1dStpRootCost {dot1dStp 6}	INTEGER
19	dot1dStpRootPort {dot1dStp 7}	INTEGER
20	dot1dStpMaxAge {dot1dStp 8}	Timeout
21	dot1dStpHelloTime {dot1dStp 9}	Timeout
22	dot1dStpHoldTime {dot1dStp 10}	INTEGER
23	dot1dStpForwardDelay {dot1dStp 11}	Timeout
24	dot1dStpBridgeMaxAge {dot1dStp 12}	Timeout
25	dot1dStpBridgeHelloTime {dot1dStp 13}	Timeout
26	dot1dStpBridgeForwardDelay {dot1dStp 14}	Timeout
27	dot1dStpPortTable {dot1dStp 15}	NOT-ACCESSIBLE
28	dot1dStpPortEntry {dot1dStpPortTable 1}	NOT-ACCESSIBLE
29	dot1dStpPort {dot1dStpPortEntry 1}	INTEGER
30	dot1dStpPortPriority {dot1dStpPortEntry 2}	INTEGER
31	dot1dStpPortState {dot1dStpPortEntry 3}	INTEGER
32	dot1dStpPortEnable {dot1dStpPortEntry 4}	INTEGER
33	dot1dStpPortPathCost {dot1dStpPortEntry 5}	INTEGER
34	dot1dStpPortDesignatedRoot {dot1dStpPortEntry 6}	BridgeId

Item number	Object identifier	SYNTAX
35	dot1dStpPortDesignatedCost {dot1dStpPortEntry 7}	INTEGER
36	dot1dStpPortDesignatedBridge {dot1dStpPortEntry 8}	BridgeId
37	dot1dStpPortDesignatedPort {dot1dStpPortEntry 9}	OCTET STRING
38	dot1dStpPortForwardTransitions {dot1dStpPortEntry 10}	Counter
39	dot1dTp {dot1dBridge 4}	NOT-ACCESSIBLE
40	dot1dTpLearnedEntryDiscards {dot1dTp 1}	Counter
41	dot1dTpAgingTime {dot1dTp 2}	INTEGER
42	dot1dTpPortTable {dot1dTp 4}	NOT-ACCESSIBLE
43	dot1dTpPortEntry {dot1dTpPortTable 1}	NOT-ACCESSIBLE
44	dot1dTpPort {dot1dTpPortEntry 1}	INTEGER
45	dot1dTpPortMaxInfo {dot1dTpPortEntry 2}	INTEGER
46	dot1dTpPortInFrames {dot1dTpPortEntry 3}	Counter
47	dot1dTpPortOutFrames {dot1dTpPortEntry 4}	Counter
48	dot1dTpPortInDiscards {dot1dTpPortEntry 5}	Counter
49	dot1dTpHCPortTable {dot1dTp 5}	NOT-ACCESSIBLE
50	dot1dTpHCPortEntry {dot1dTpHCPortTable 1}	NOT-ACCESSIBLE
51	dot1dTpHCPortInFrames {dot1dTpHCPortEntry 1}	Counter64
52	dot1dTpHCPortOutFrames {dot1dTpHCPortEntry 2}	Counter64
53	dot1dTpHCPortInDiscards {dot1dTpHCPortEntry 3}	Counter64
54	dot1dTpPortOverflowTable {dot1dTp 6}	NOT-ACCESSIBLE
55	dot1dTpPortOverflowEntry {dot1dTpPortOverflowTable 1}	NOT-ACCESSIBLE
56	dot1dTpPortInOverflowFrames {dot1dTpPortOverflowEntry 1}	Counter32
57	dot1dTpPortOutOverflowFrames {dot1dTpPortOverflowEntry 2}	Counter32
58	dot1dTpPortInOverflowDiscards {dot1dTpPortOverflowEntry 3}	Counter32

- P-Bridge MIB (RFC2674)

`iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).pBridgeMIB(6)`

Item number	Object identifier	SYNTAX
1	pBridgeMIBObjects {pBridgeMIB 1}	NOT-ACCESSIBLE
2	dot1dExtBase {pBridgeMIBObjects 1}	NOT-ACCESSIBLE
3	dot1dDeviceCapabilities {dot1dExtBase 1}	BITS
4	dot1dTrafficClassesEnabled {dot1dExtBase 2}	TruthValue
5	dot1dPortCapabilitiesTable {dot1dExtBase 4}	NOT-ACCESSIBLE
6	dot1dPortCapabilitiesEntry {dot1dPortCapabilitiesTable 1}	NOT-ACCESSIBLE
7	dot1dPortCapabilities {dot1dPortCapabilitiesEntry 1}	BITS
8	dot1dPriority {pBridgeMIBObjects 2}	NOT-ACCESSIBLE
9	dot1dPortPriorityTable {dot1dPriority 1}	NOT-ACCESSIBLE
10	dot1dPortPriorityEntry {dot1dPortPriorityTable 1}	NOT-ACCESSIBLE
11	dot1dPortDefaultUserPriority {dot1dPortPriorityEntry 1}	INTEGER

Item number	Object identifier	SYNTAX
12	dot1dPortNumTrafficClasses {dot1dPortPriorityEntry 2}	INTEGER
13	dot1dTrafficClassTable {dot1dPriority 3}	NOT-ACCESSIBLE
14	dot1dTrafficClassEntry {dot1dTrafficClassTable 1}	NOT-ACCESSIBLE
15	dot1dTrafficClassPriority {dot1dTrafficClassEntry 1}	INTEGER
16	dot1dTrafficClass {dot1dTrafficClassEntry 2}	INTEGER

- Q-Bridge MIB (RFC2674)

`iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).QBridgeMIB(7)`

Item number	Object identifier	SYNTAX
1	qBridgeMIBObjects {qBridgeMIB 1}	NOT-ACCESSIBLE
2	dot1qBase {qBridgeMIBObjects 1}	NOT-ACCESSIBLE
3	dot1qVlanVersionNumber {dot1qBase 1}	INTEGER
4	dot1qMaxVlanId {dot1qBase 2}	VlanId
5	dot1qMaxSupportedVlans {dot1qBase 3}	Unsigned32
6	dot1qNumVlans {dot1qBase 4}	Unsigned32
7	dot1qGvrpStatus {dot1qBase 5}	EnabledStatus
8	dot1qVlan {qBridgeMIBObjects 4}	NOT-ACCESSIBLE
9	dot1qVlanNumDeletes {dot1qVlan 1}	Counter32
10	dot1qVlanCurrentTable {dot1qVlan 2}	NOT-ACCESSIBLE
11	dot1qVlanCurrentEntry {dot1qVlanCurrentTable 1}	NOT-ACCESSIBLE
12	dot1qVlanTimeMark {dot1qVlanCurrentEntry 1}	TimeFilter
13	dot1qVlanIndex {dot1qVlanCurrentEntry 2}	VlanIndex
14	dot1qVlanFdbId {dot1qVlanCurrentEntry 3}	Unsigned32
15	dot1qVlanCurrentEgressPorts {dot1qVlanCurrentEntry 4}	PortList
16	dot1qVlanCurrentUntaggedPorts {dot1qVlanCurrentEntry 5}	PortList
17	dot1qVlanStatus {dot1qVlanCurrentEntry 6}	INTEGER
18	dot1qVlanCreationTime {dot1qVlanCurrentEntry 7}	TimeTicks
19	dot1qVlanStaticTable {dot1qVlan 3}	NOT-ACCESSIBLE
20	dot1qVlanStaticEntry {dot1qVlanStaticTable 1}	NOT-ACCESSIBLE
21	dot1qVlanStaticName {dot1qVlanStaticEntry 1}	SnmpAdminString
22	dot1qVlanStaticEgressPorts {dot1qVlanStaticEntry 2}	PortList
23	dot1qVlanForbiddenEgressPorts {dot1qVlanStaticEntry 3}	PortList
24	dot1qVlanStaticUntaggedPorts {dot1qVlanStaticEntry 4}	PortList
25	dot1qVlanStaticRowStatus {dot1qVlanStaticEntry 5}	RowStatus
26	dot1qNextFreeLocalVlanIndex {dot1qVlan 4}	INTEGER
27	dot1qPortVlanTable {dot1qVlan 5}	NOT-ACCESSIBLE
28	dot1qPortVlanEntry {dot1qPortVlanTable 1}	NOT-ACCESSIBLE
29	dot1qPvid {dot1qPortVlanEntry 1}	VlanIndex
30	dot1qPortAcceptableFrameTypes {dot1qPortVlanEntry 2}	INTEGER

Item number	Object identifier	SYNTAX
31	dot1qPortIngressFiltering {dot1qPortVlanEntry 3}	TruthValue
32	dot1qPortGvrpStatus {dot1qPortVlanEntry 4}	EnabledStatus
33	dot1qPortGvrpFailedRegistrations {dot1qPortVlanEntry 5}	Counter32
34	dot1qPortGvrpLastPduOrigin {dot1qPortVlanEntry 6}	MacAddress

- IF MIB (RFC2863)
  `iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1). ifMIB (31)`

Item number	Object identifier	SYNTAX
1	ifMIBObjects {ifMIB 1}	NOT-ACCESSIBLE
2	ifXTable {ifMIBObjects 1}	NOT-ACCESSIBLE
3	ifXEntry {ifXTable 1}	NOT-ACCESSIBLE
4	ifName {ifXEntry 1}	DisplayString
5	ifInMulticastPkts {ifXEntry 2}	Counter32
6	ifInBroadcastPkts {ifXEntry 3}	Counter32
7	ifOutMulticastPkts {ifXEntry 4}	Counter32
8	ifOutBroadcastPkts {ifXEntry 5}	Counter32
9	ifHCInOctets {ifXEntry 6}	Counter64
10	ifHCInUcastPkt {ifXEntry 7}	Counter64
11	ifHCInMulticastPkts {ifXEntry 8}	Counter64
12	ifHCInBroadcastPkts {ifXEntry 9}	Counter64
13	ifHCOutOctets {ifXEntry 10}	Counter64
14	ifHCOutUcastPkts {ifXEntry 11}	Counter64
15	ifHCOutMulticastPkts {ifXEntry 12}	Counter64
16	ifHCOutBroadcastPkts {ifXEntry 13}	Counter64
17	ifLinkUpDownTrapEnable {ifXEntry 14}	INTEGER
18	ifHighSpeed {ifXEntry 15}	Gauge32
19	ifPromiscuousMode {ifXEntry 16}	TruthValue
20	ifConnectorPresent {ifXEntry 17}	TruthValue
21	ifAlias {ifXEntry 18}	DisplayString
22	ifCounterDiscontinuityTime {ifXEntry 19}	TimeTicks

- FUJITSU-XG2000-MIB

```
iso(1).org(3).dod(6)internet(1).private(4).enterprises(1).fujitsu(211).
Product(1).nonos(127).xg-switch(61).xg2000(107)
(*.xg2000(107) becomes *.xg2000(108) in case of XG2000C, *.xg2000(109) in case of XG2000CR,
and *.xg2000(110) in case of XG2000R)
```

Item number	Object identifier	SYNTAX	Description
1	xg2000Monitor {xg2000 1}	NOT-ACCESSIBLE	Object identifier of monitor information specific to the device.
2	xg2000InternalTemperature {xg2000Monitor 1}	Integer32	Indicates the temperature inside the chassis (in degree Celsius).
3	xg2000LoadAverage {xg2000Monitor 3}	Integer32	Indicates the CPU usage (in %).
4	xg2000Event {xg2000 2}	NOT-ACCESSIBLE	Object identifier of trap information specific to the device.
5	xg2000Traps {xg2000Event 0}	NOT-ACCESSIBLE	Object identifier of trap information specific to the device.
6	xg2000*** {xg2000Traps X}	NOT-ACCESSIBLE	Object identifier of message information trap. "xg2000***" differs from one event to another. "X" indicates the message number to be reported.
7	xg2000TrapInfo {xg2000Event 10}	NOT-ACCESSIBLE	Object identifier of additional information on message information trap.

8	xg2000TrapLevel
	{xg2000TrapInfo 1}
		Integer32	Specifies the severity of message.
			critical(0)
			error(1)
			warning(2)
			info(3)

9	xg2000TrapMessage {xg2000TrapInfo 2}	DisplayString	Displays message text when sending a trap.

Index

XG2000 series User's Guide

P3N1-E202-01ENZ0

Date of Issue: March 2009
Issuing authority: PFU LIMITED

- The contents of this manual may be updated without notice.
- PFU assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
-