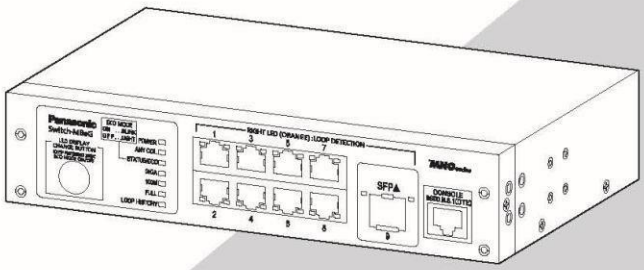
Panasonic®

Operation Manual
for Menu Interface

Switch-M8eG

Model Number: PN28080K



This operation manual is applicable to the following Switching Hubs:

Product name	Model No.	Firmware version
Switch-M8eG	PN28080K-ID PN28080K-TH PN28080K-MY PN28080K-SG	2.0.1.07 or higher

Table of Contents

1. Product Outline

Switch-M8eG is an all Giga bit Ethernet Switching Hub with management function having 8 ports of 10/100/1000BASE-T and one pair of 10/100/1000BASE-T port and SFP extension slot.

1.1. Features

- Has wire-speed Layer 2 switching function.
- Ports 1 to 8 are 10/100/1000BASE-T ports corresponding to auto negotiation. Also their speed and communication mode can be switched by configuration. Port 9 can be used corresponding to SFP extension slot.
- All twisted pair ports support straight/cross cable auto sensing function. Simply connect devices with straight cables, whether it is a terminal or a network device. (This function does not work if the port communication configuration is set at Fixed or Link Aggregation. Ports 1 to 7 are set at MDI-X. (default))
- Has a loop detection function, which notifies when a loop occurs with the corresponding port LED and automatically shuts down the looped port.
- Has a loop detection history function, which notifies when a loop occurs with the corresponding LED and enables a network administrator to identify the looped port after the loop is removed.
- VLAN function allows free grouping of up to 256 VLANs
- Use of LED indicator switching button saves power consumption of LED lamps.
- The IEEE802.1p compatible QoS function is supported.
- Has an Internet mansion function, which ensures security between each door.
- Power saving mode detects the connection status automatically and saves power consumption to minimum.
- Telnet and SSH functions facilitate remote setting change and confirmation.
- Standard MIB (MIB II, Bridge MIB, etc.) is supported, enabling remote control by using the SNMP manager. (For details, refer to Appendix A and Appendix C.)
- Link aggregation function is supported. Aggregation can be manually configured up to 8 ports.
- Reboot timer function is supported, enabling auto reboot after a scheduled time (24 hours or less).

- Equipped with energy efficient Ethernet (EEE) conforming to IEEE802.3az (LPI). When there is no data transmission at link up, the energy-saving state automatically starts so that power consumption can be reduced on each port.

1.2. Accessories

Please be sure to confirm the content. Please contact our distributor if any of the contents are insufficient.

	Quantity
Installation Guide (this document)	1
CD-ROM (PDF version of Operating Instructions)	1
Mounting bracket (for 19-inch rack)	2
Screws (for 19-inch rack)	4
Screws (for fixing the main unit and the mounting bracket)	8
Rubber foot	4
Power cord	1
Connecting bracket	2
Screws (for Connecting bracket)	8

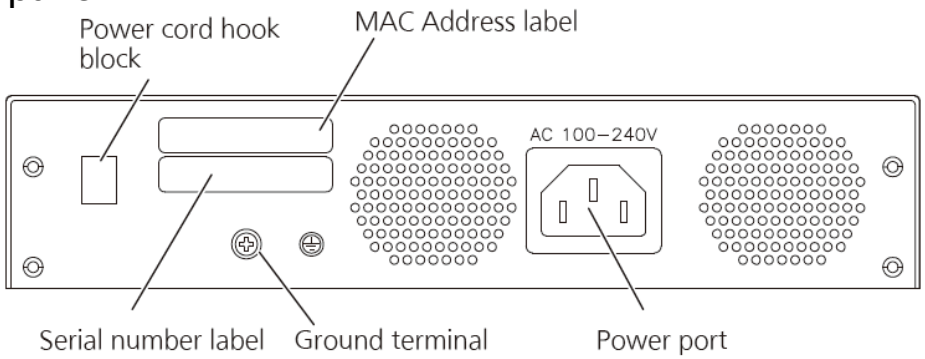
[Optional accessories]

PN54021K 1000BASE-SX SFP Module

PN54023K 1000BASE-LX SFP Module

1.3. Part Names

Back panel



Front panel

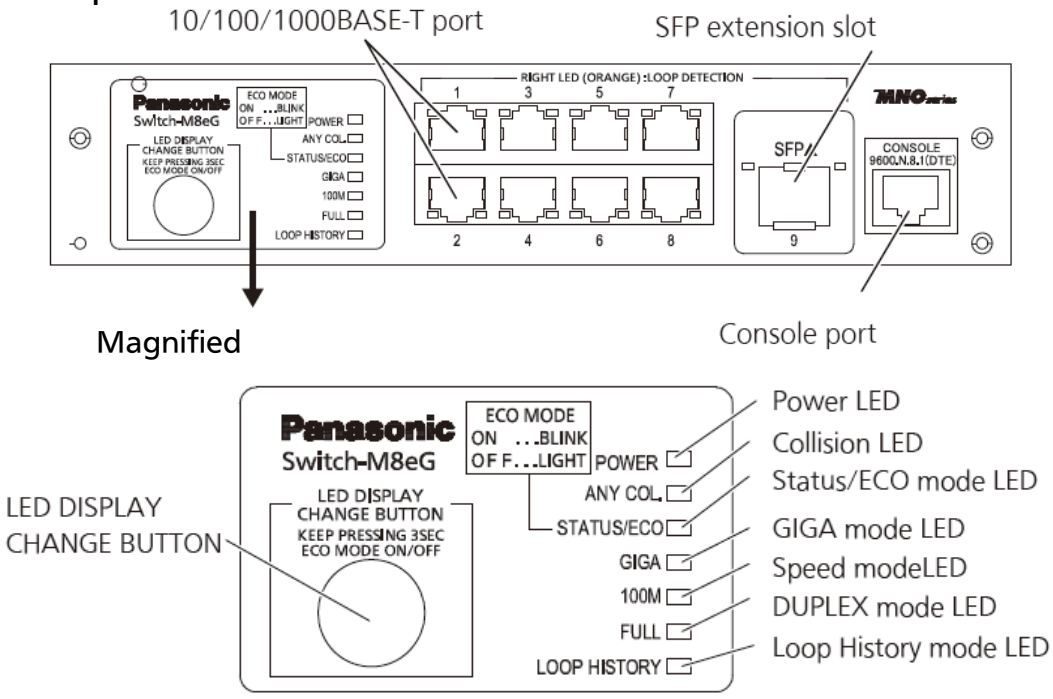


Fig. 1-3 Part Names

1.4. LED Behavior

1.4.1. LED Behavior at Start-up

Upon turning this Switching Hub on, all LEDs tentatively light up. Then, the self-diagnosis of hardware is executed. Upon finishing the diagnosis, power LED and status/ECO mode LED light in solid green. Then, the Switching Hub starts working.

1.4.2. LED Behavior while Operating

This Switching Hub has a set of LEDs for each port. These LEDs indicate the operation status of each port.

- System LED

LED	Behavior	Description
POWER LED (Power)	Green Light	Power is ON.
	Off	Power is OFF.
ANY COL. LED (Collision)	Orange Light	During half-duplex operation, packet collision is occurring in either port.
	Off	No packet collision.
STATUS/ECO LED (Status/Eco mode)	Green Light	Operating in status mode.
	Green Blink	Operating in ECO mode. **(All LEDs turn off, except POWER and STATUS/ECO LEDs during ECO mode.)**
	Off	Power is OFF.
GIGA LED (GIGA mode)	Green Light	Operating in GIGA mode.
100M LED (Speed mode)	Green Light	Operating in Speed mode.
FULL LED (DUPLEX mode)	Green Light	Operating in Duplex mode.
LOOP HISTORY LED (Loop History mode)	Green Light	Operating in Loop history mode.
	Green Blink	Loop is occurring, or occurred within the last 3 days.

● Port LED display mode LED

In the status mode described later, port LED shows linkup and communication status. By pressing the LED display switch button in the front panel, the display mode of port LED can be changed as follows.

Port LED display mode	Description
STATUS/ECO	Shows linkup and communication status.
GIGA	Shows linkup status at 1000 Mbps.
100M	Shows linkup status at 100 Mbps.
FULL	Shows linkup status at full-duplex or half-duplex.
LOOP HISTORY	Shows loop history and port shut-off status.

● Port LED

According to switchover in the port LED display mode, described previously, display of port LED in each port changes as follows.

Port LED	Display mode	Behavior	Description
Left	STATUS/ECO	Green Light	Link is established.
		Green Blink	Transmitting and receiving data.
		Off	No device connected.
	GIGA	Green Light	Link is established at 1000 Mbps.
		Off	Link is established at 100 Mbps or 10 Mbps, or no device is connected.
	100M	Green Light	Link is established at 100 Mbps.
		Off	Link is established at 1000 Mbps or 10 Mbps, or no device is connected.
	FULL	Green Light	Link is established at full-duplex.
		Off	Link is established at half-duplex or no device is connected.
	LOOP HISTORY	Green Light	Within 3 days after loop removed.
		Off	No loop detection history.
Right	—	Orange Light	Shutting down by loop detection.
		Off	Not shutting down by loop detection.

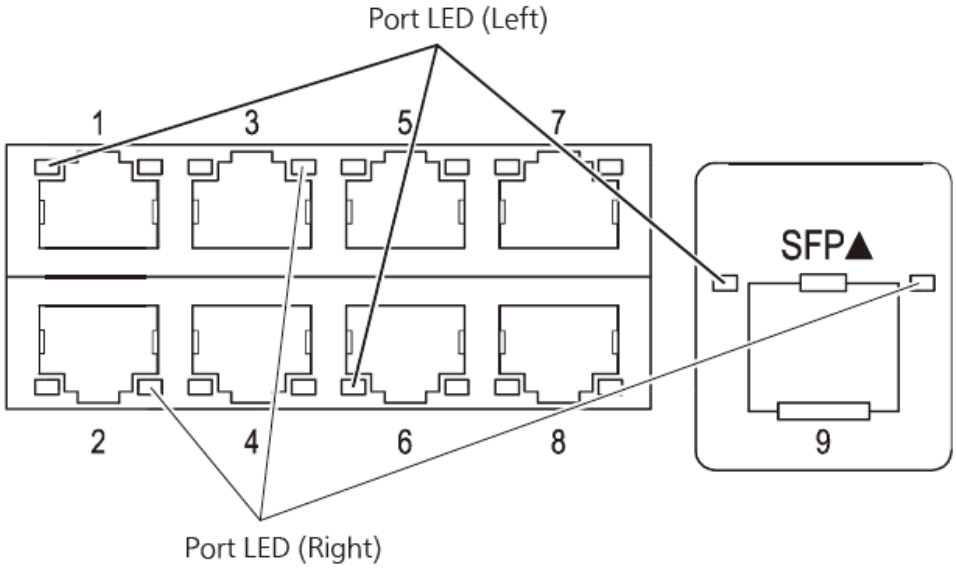


Fig. 1-4 Port LED

1.4.3. Loop detection function

Turns on the port LED with an orange light when a loop occurs in the corresponding port. At this time, the relevant port automatically shuts down (default setting: 60 sec.) to prevent loop from occurring. If the loop is still not removed, the port will shut down again. Remove the loop while the port is shut off.

The loop detection/shut-off function can be switched on/off by keeping pressing the LED display switch button for more than 10 seconds or by setting in the configuration menu. For details on the configuration menu, refer to 4.7.8. If switching properly takes place, LOOP HISTORY LED turns on to complete switchover.

The loop history can be reset by powering off the Switching Hub and then on.

1.5. LED Display Change Button

1.5.1. Setting LED Base Mode

You can select display of LEDs in this Switching Hub from two types: Status mode and Eco mode.
The mode selected at system start-up is called the base mode. The base mode can be switched by keeping pressing the LED display switch button for more than 3 seconds. After pressing the LED display switch button for more than 3 seconds, STATUS/ECO, GIGA, 100M, and FULL LEDs will turn on at once, and then the mode will switch over.

● Status mode (Factory default setting)
According to the port LED display mode, port LED shows the status of each port. In status mode, STATUS/ECO LED lights in green.

● ECO mode
Regardless of whether a device is connected or not, **all LEDs other than POWER and STATUS/ECO LEDs turn off** to save power. In ECO mode, STATUS/ECO LED flashes in green.

The base mode can be set from the configuration menu of this Switching Hub. For details, refer to 4.6.7.h.

1.5.2. LED Display Switchover

By pressing the LED display switch button on the front panel, display of port LED can be changed in the following order.

Port LED display mode	Description
STATUS/ECO	Shows link establishment and communication status.
GIGA	Shows linkup status at 1000 Mbps.
100M	Shows linkup status at 100 Mbps.
FULL	Shows linkup status at full-duplex or half-duplex.
LOOP HISTORY	Shows loop detection and port shut-off status.

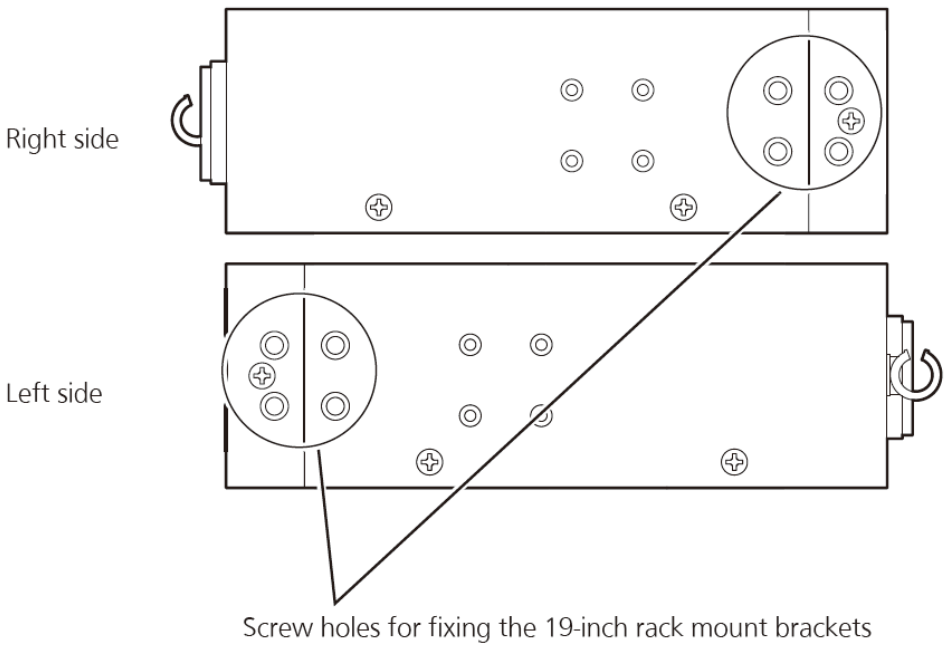
If the port LED display mode is switched to other than STATUS/ECO and then no operation is executed for more than 1 minute, the mode automatically shifts to the base mode.

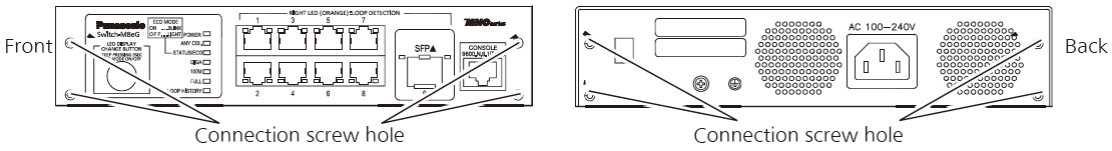
2. Installation

Switch-M16eG can be installed to a stainless steel product, a 19-inch rack, or on the wall.

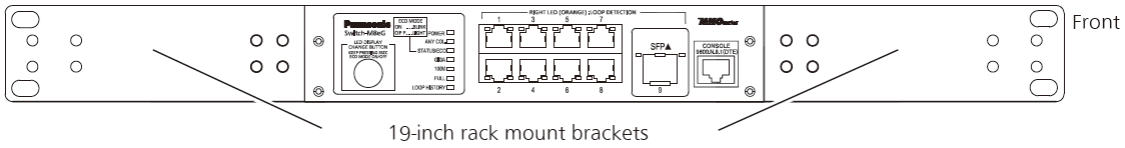
2.2. Mounting to 19-inch Rack

Use the two 19-inch rack mount brackets and eight screws (for fixing the mount brackets to the Switching Hub) to fix the mount brackets to the four holes on each side of the Switching Hub. Then securely install the Switching Hub on the rack using the four screws (for a 19-inch rack mount) or screws supplied with the rack. Up to two Switching Hubs can be connected. When connecting two Switching Hubs and installing them on a rack, use the two 19-inch rack mount brackets and eight screws (for fixing the mount brackets to the Switching Hub) to fix the mount brackets to the four holes on a side of the Switching Hubs. Then use the two connection brackets and eight screws (for fixing the connection brackets) to securely fix the connection brackets to the connection screw holes on the front and back panels, and then install the Switching Hubs on the rack.





- Installation on rack (one unit)



- Installation on rack (two units connected)

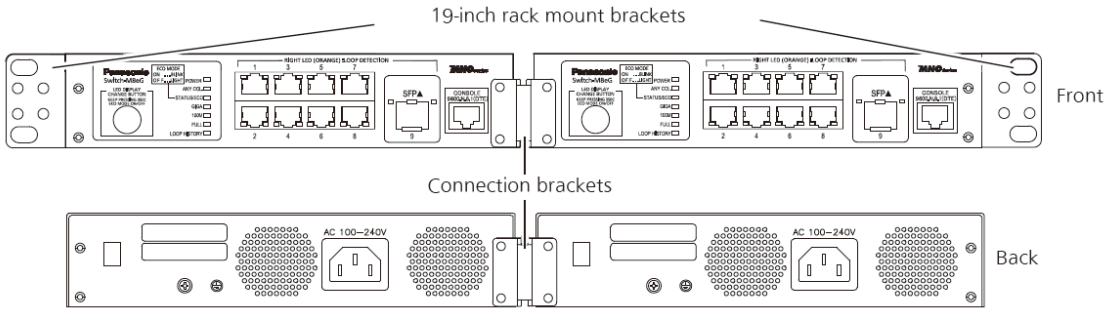


Fig. 2-2 Mounting to 19-inch Rack

3. Connection

3.1. Connection Using a Twisted Pair Port

● Connection Cable

Use a CAT5E or higher twisted pair cable with 8P8C RJ45 modular plug.

● Network Configuration

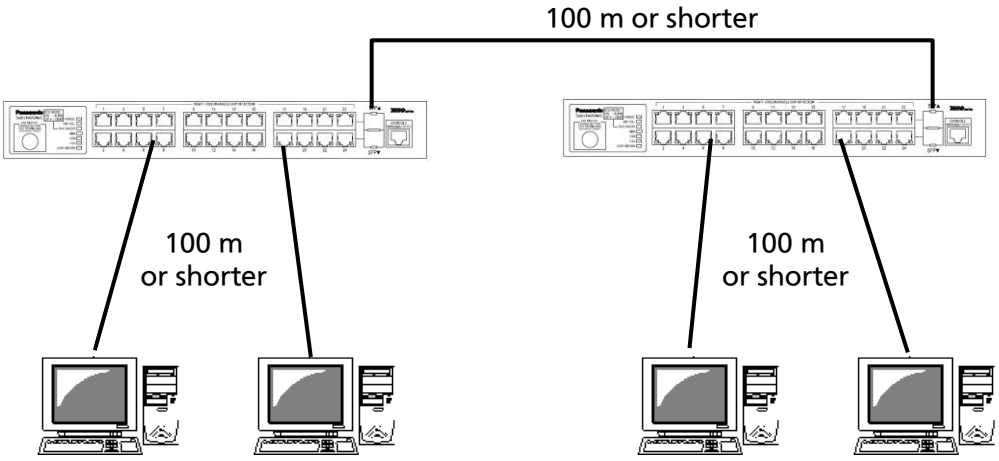


Fig. 3-1 Example of Connection

The length of the cable connecting this Switching Hub and a device must be 100 m or shorter. When a terminal or a LAN device with auto negotiation function is connected to this Switching Hub, the port is automatically configured at the highest performance mode. When a terminal or a LAN device without auto negotiation function is connected to this Switching Hub, this Switching Hub automatically determines and sets the communication speed; however, the full-duplex/half-duplex configuration is set at half-duplex because the full-duplex/half-duplex capability cannot be determined. When connecting a terminal or a LAN device without auto negotiation function, a fixed-mode port configuration needs to be set.

Note: If a fixed-ode port configuration is set, Auto-MDI/MDI-X function does not work. Therefore, use a cross cable to connect them.

3.2. Connection Using an SFP Extension Slot

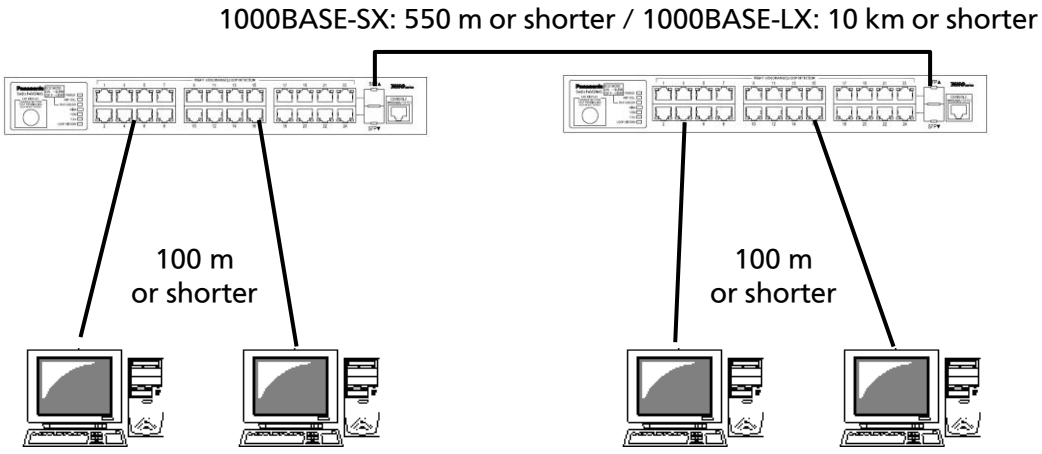


Fig. 3-2 Example of Optical Fiber Cable Connection

Plugging an SFP module (optional) into an SFP extension slot enables an optical fiber connection. Connect this Switching Hub's TX port to the RX port of the connected device and this Switching Hub's RX port to the TX port of the connected device.
If a twisted pair cable and an SFP module are simultaneously connected to combo ports that are used exclusively, SFP link has a priority.

3.3. Connection to Power

Connect the supplied power code to the power port of this Switching Hub and connect the other end into an electric outlet. This Switching Hub operates at 100-240 V (50/60 Hz).

This Switching Hub does not have a power ON/OFF switch. Plugging the power cord turns on this Switching Hub's power and the operation starts. To power off, unplug the power code from the electric outlet.

4. Configuration

Upon power on, this Switching Hub starts working as a switching hub. To use the SNMP management functionality or other unique functions, you need to configure the Switching Hub using a console port, Telnet, or SSH.
In this chapter, the configuration of this Switching Hub is explained.

Note: You need to configure an IP address to access this Switching Hub via Telnet or SSH. Therefore, configure an IP address first via the console port, before accessing via Telnet or SSH.

4.1. Connecting via Console Port

Console connection requires a DEC VT100-compatible asynchronous terminal, or a terminal capable of running a VT100-compatible terminal emulator, such as HyperTerminal on Windows XP or older. Connect a terminal of this kind to the console port of this Switching Hub.
Configure the communication mode for the asynchronous terminal as follows:

- Transmission mode: RS-232C (ITU-TS V.24 compatible)
- Emulation mode: VT100
- Transmission speed: 9600 bps
- Data length: 8 bit
- Stop bit: 1 bit
- Parity control: None
- Flow control: None

4.2. Login

If you access the Switching Hub via the console port, a screen shown in Fig. 4-2-1 appears.
If this screen does not appear, press Enter key to refresh the display or confirm that there is no error in configuration of communication mode and others.

```
================================================================================
PN28080K Local Management System Version x.x.x.xx
MAC Address: xx:xx:xx:xx:xx:xx
Serial Number:xxxxxxxxxxx
================================================================================

Login Menu

Login:
```

Fig. 4-2-1 Login Screen (Console)

If accessing the Switching Hub via Telnet, a similar login screen appears, displaying "Remote Management System Version" at the upper part of the screen, as shown in Fig. 4-2-2.

```
================================================================================
PN28080K Remote Management System Version x.x.x.xx
MAC Address:  xx:x:xx:xx:xx:xx
Serial Number:xxxxxxxxxxx
================================================================================

Login Menu

Login:
```

Fig. 4-2-2 Login Screen (Telnet)

On the screens in Fig. 4-2-1 and Fig. 4-2-2, enter the login name and password. First, enter the login name. The Switching Hub's default login name is set to "manager." Enter "manager" and press the Enter key. Then, you need to enter a password, as shown in Fig. 4-2-3. The Switching Hub's default password is the same as the login name ("manager"). Enter the password correctly and press the Enter key.

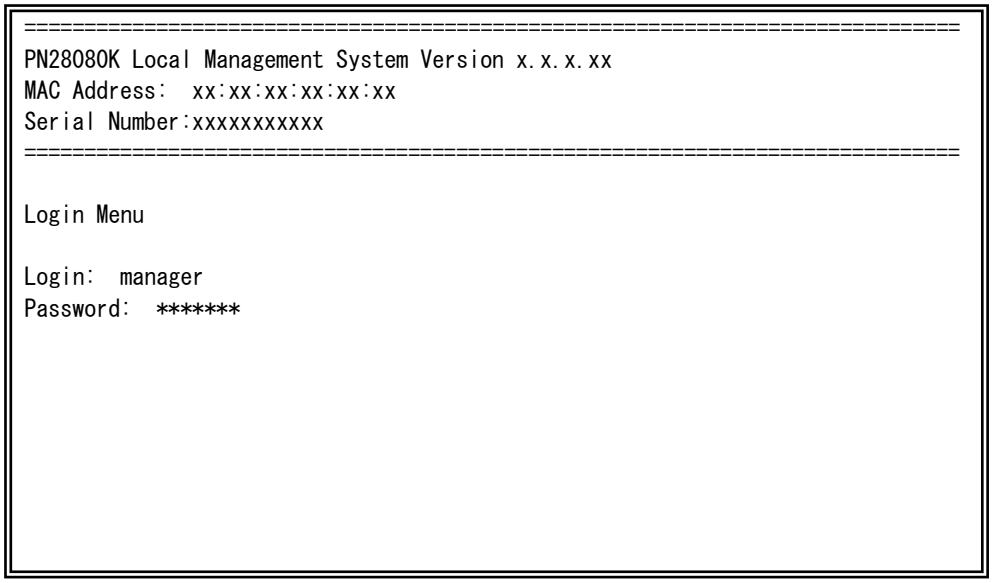


Fig. 4-2-3 Entering Password

Both the login name and password can be changed. For the detailed change procedure, refer to 4.6.7.

Note: A password is displayed with asterisks (*) as a user enters it.

Note: Up to four users can access the Switching Hub concurrently via Telnet, and two users via SSH.

Note: Follow the operating procedures for SSH client to login via SSH.

4.3. Basic Operations on the Screen

The console screen of the Switching Hub is organized as follows:

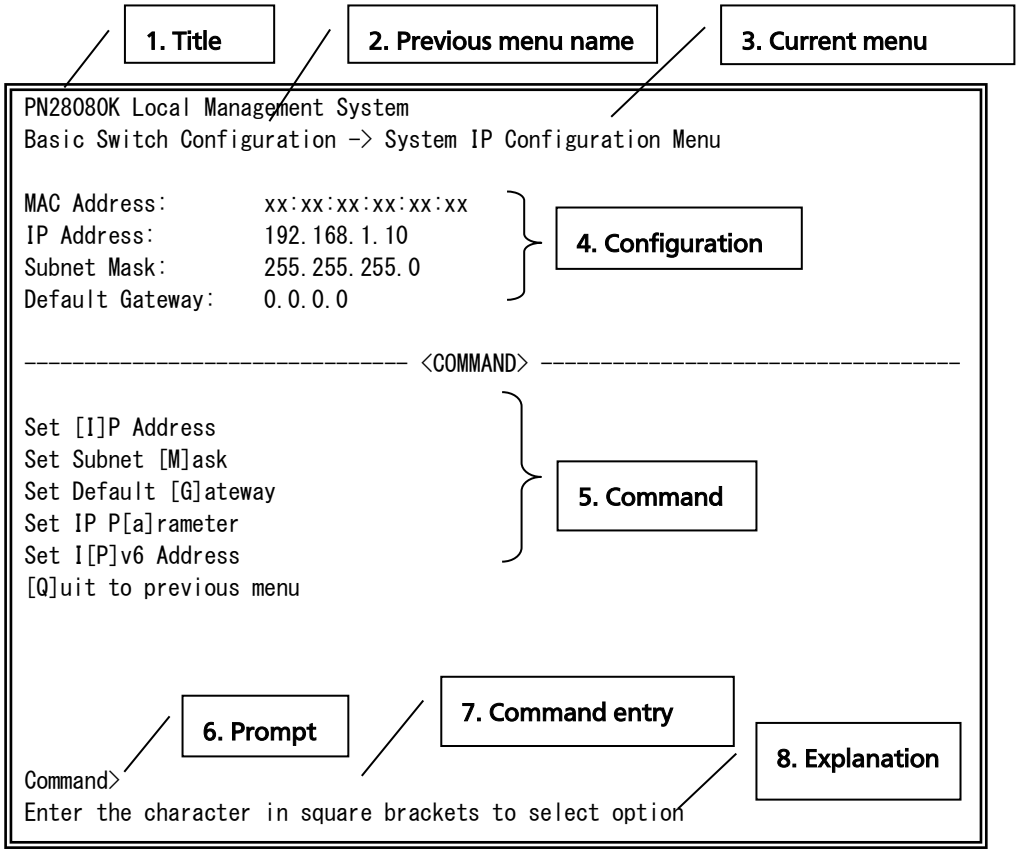


Fig. 4-3-1 Screen Structure

Screen Description

1.	Title	The title of this screen. Shows "Local Management System" while being accessed via console. Shows "Remote Management System" while being accessed via Telnet.
2.	Previous menu name	Shows the name of the previous menu. Pressing "Q," described later, opens the menu screen shown in this field.
3.	Current menu name	Shows the name of the current screen.
4.	Configuration	Shows the current configuration, set on this screen.
5.	Command	Shows the commands available on this screen. Available commands differ on each screen. Select a command from the list.
6.	Prompt	Changes as you enter a command, indicating what you need to enter next. Follow the instruction in this field.
7.	Command entry line	Enter a command or settings.
8.	Explanation	Shows the explanation of this screen or errors.

All operations on this screen are done by entering letters. Using a cursor or other operations are not available. A letter as a valid command is enclosed in square brackets in the command section of each screen. If you enter an invalid command or setting, an error message is shown in the explanation field.

4.4. Main Menu

After login, Main Menu appears, as shown in Fig. 4-4-1.
This Switching Hub has a main menu and multiple sub-menus. These menus have a tree structure, with the main menu as its root. To move to a sub-menu, enter a command letter. To return to the previous menu, enter the "Q" command. The second line from the top shows the current menu name.

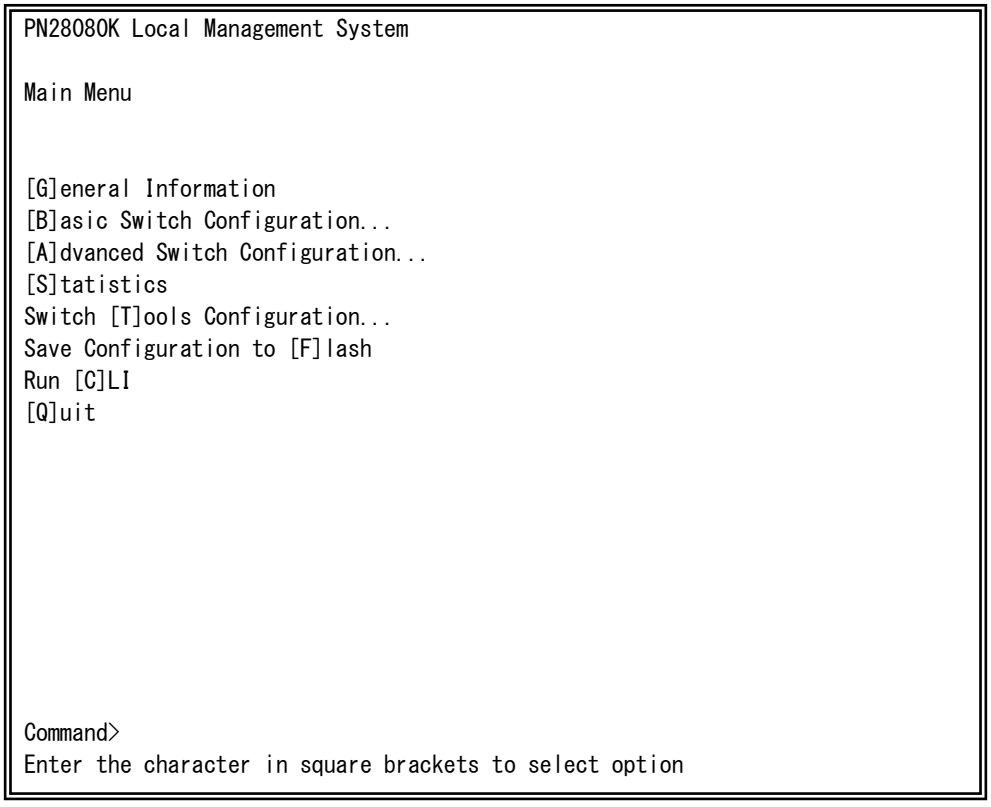


Fig. 4-4-1 Main Menu

Screen Description

General Information	Shows this Switching Hub's hardware, firmware information and address settings.
Basic Switch Configuration…	Configures this Switching Hub's basic functions (such as IP address, SNMP and port settings).
Advanced Switch Configuration…	Configures this Switching Hub's advanced functions (such as VLAN, link aggregation, and QoS).
Statistics	Shows this Switching Hub's statistical information.
Switch Tools Configuration	Configures this Switching Hub's additional tools (such as firmware update, saving/reading settings, Ping, and system log).
Save Configuration to Flash	Writes this Switching Hub's settings into its internal memory.
Run CLI	Switches to a command line interface.
Quit	Quits the main menu and returns to the login screen.

4.5. General Information Menu

On the Main Menu, pressing "G" opens the General Information Menu, as shown in Fig. 4-5-1. This screen shows this Switching Hub's basic information. You cannot edit shown information on this screen.

```
PN28080K Local Management System
Main Menu -> General Information

System up for:              0day(s), 0hr(s), 1min(s), 59sec(s)
Boot Code Version:          x.xx.xx
Runtime Code Version:       x.x.x.xx
Serial Number:              xxxxxxxxxxx
Hardware Information
  Version:                  A1
  DRAM  Size:               128MB
  Flash Size:               28MB

Administration Information
  Switch Name:
  Switch Location:
  Switch Contact:

System Address Information
  MAC Address:              xx:xx:xx:xx:xx:xx
  IP Address:               0.0.0.0
  Subnet Mask:              0.0.0.0
  Default Gateway:          0.0.0.0

Press any key to continue...
```

Fig. 4-5-1 General Information Menu

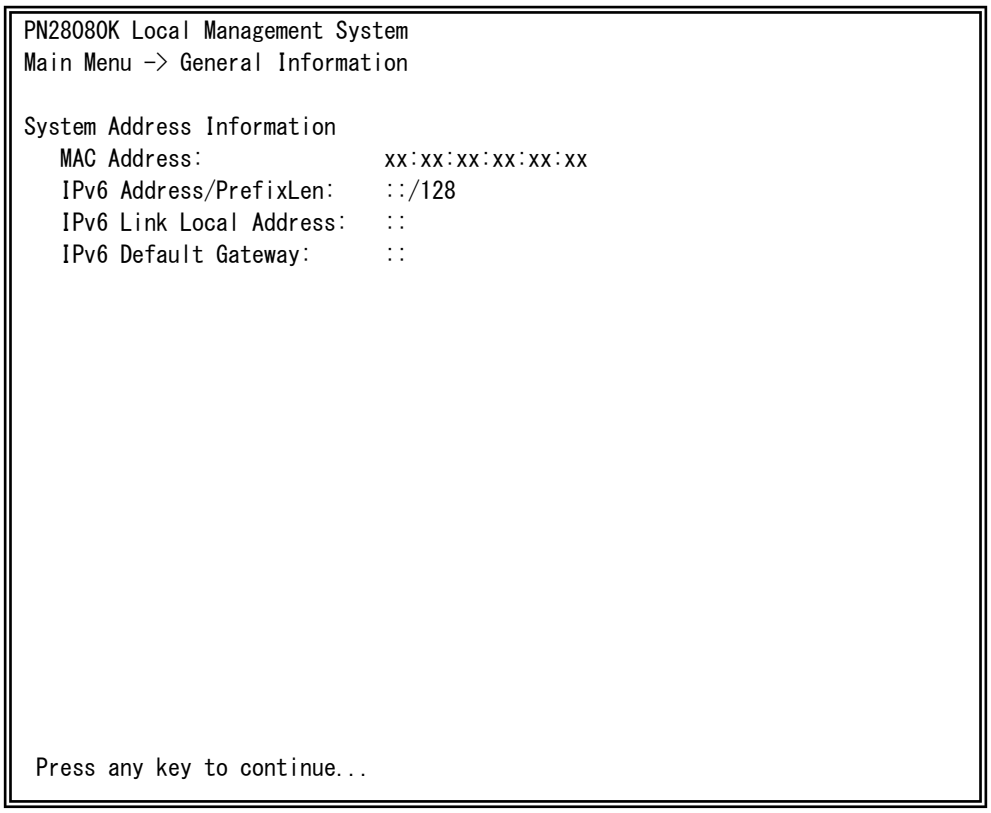


Fig. 4-5-2 General Information Menu (IPv6)

Screen Description

System up for	Shows accumulated time since the Switching Hub boot-up.	
Boot Code Version	Shows the version of Boot Code.	
Runtime Code Version	Shows the version of Runtime Code. (Upgrading firmware version described in 4.9.1 is applicable to Runtime Code.)	
Serial Number	Shows the Serial Number.	
Hardware Information	Shows the hardware information.	
	Version	Shows the hardware version information.
	DRAM / Flash Size	Shows capacities of mounted DRAM and Flash memory.
Administration Information	Items shown here are configured in accordance with "4.6.1 System Administration Configuration."	
	Switch Name	Shows the name of the Switching Hub. No information is set on shipment.
	Switch Location	Shows the installation location of the Switching Hub. No information is set on shipment.
	Switch Contact	Shows contact information of the Switching Hub. No information is set on shipment.
System Address Information	Items shown here are configured in accordance with "4.6.2 System IP Configuration."	
	MAC Address	Shows the MAC address of this Switching Hub. This value is uniquely assigned to each device and cannot be changed.
	IP Address	Shows the Switching Hub's current IP address. 0.0.0.0 is displayed because no address is set on shipment. For configuration details, refer to 4.6.2.
	Subnet Mask	Shows the Switching Hub's current subnet mask. 0.0.0.0 is displayed because no address is set on shipment. For configuration details, refer to 4.6.2.
	Default Gateway	Shows the IP address of the router for the default gateway. 0.0.0.0 is displayed because no address is set on shipment. For configuration details, refer to 4.6.2.
	IPv6 Address/PrefixLen	Shows the Switching Hub's current IPv6 address. ::/128 is displayed because no address is set on shipment. For configuration details, refer to 4.6.2a.

	IPv6 Link Local Address	Shows the Switching Hub's current IPv6 link local address. :: is displayed because no address is set on shipment. For configuration details, refer to 4.6.2a.
	IPv6 Default Gateway	Shows the IP address of the router for the default gateway. :: is displayed because no address is set on shipment. For configuration details, refer to 4.6.2a.

4.6. Basic Switch Configuration

On the Main Menu, pressing "B" opens the Basic Switch Configuration Menu, as shown in Fig. 4-6-1. On this screen, you can configure the basic configuration settings, such as
IP address, SMNP, and ports.

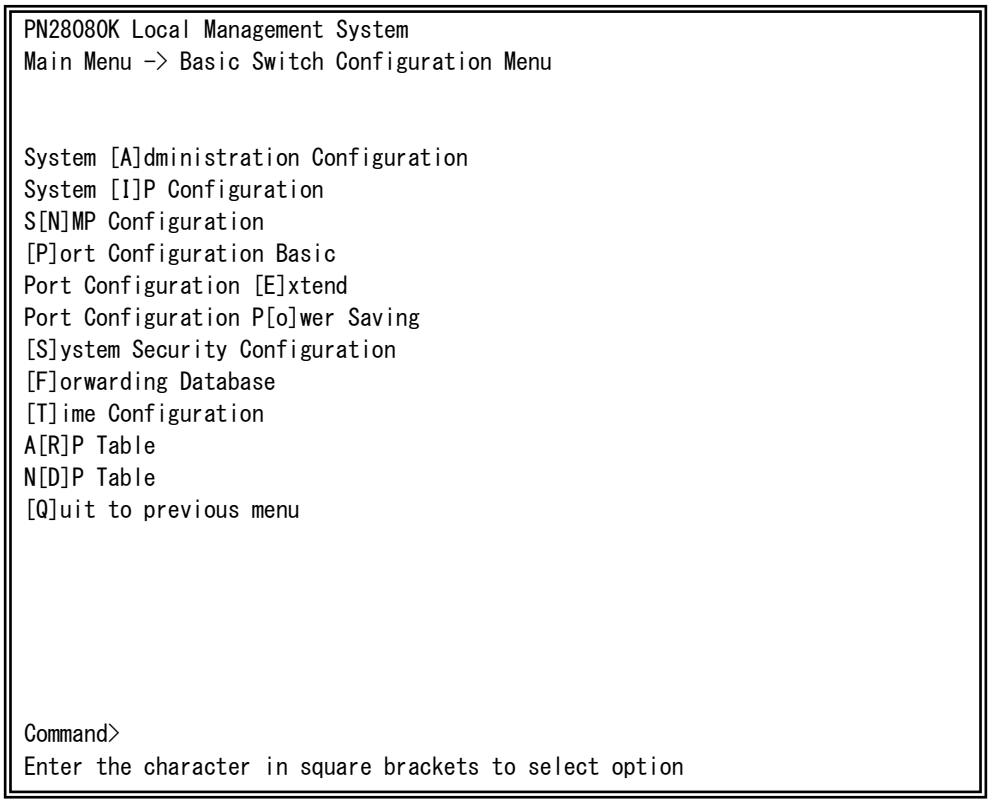


Fig. 4-6-1 Basic Switch Configuration

Screen Description

System Administration Configuration	Configures the administrative information, such as Switching Hub name, location and contact information.
System IP Configuration	Configures the IP-address-related network information.
SNMP Configuration	Configures SNMP-related settings.
Port Configuration Basic	Configures PoE for each port.
Port Configuration Extend	Configures extended port settings, such as port name.
Port Configuration Power Saving	Configures power saving mode for MNO series.
System Security Configuration	Configures the security settings, such as access control for this Switching Hub.
Forwarding Database	Shows the MAC address table.
Time Configuration	Configures the time settings, such as the SNTP-based time synchronization function and manual mode settings.
ARP Table	Shows the ARP table.
NDP Table	Shows the NDP table.
Quit to previous menu	Returns to the main menu.

4.6.1. System Administration Configuration

On the Basic Switch Configuration Menu, pressing "A" opens the System Administration Configuration Menu, as shown in Fig. 4-6-2. On this screen, you can set administrative information, such as device name.

```
PN28080K Local Management System
Basic Switch Configuration -> System Admin. Configuration Menu

Description: Switch-M8eG
Object ID:   1.3.6.1.4.1.396.5.4.2.20
Name:
Location:
Contact:

-------------------------------- <COMMAND> ----------------------------------
Set System [N]ame
Set System [L]ocation
Set System [C]ontact Information
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-6-2 System Administration Configuration

Screen Description

Description:	Shows the system information. This item is not editable.
Object ID:	Shows the corresponding ID in the MIB. This item is not editable.
Name:	Shows the system name. No information is set on shipment.
Location:	Shows the installation location. No information is set on shipment.
Contact:	Shows the contact information. No information is set on shipment.

Available commands are listed below.

N	Set/edit the system name.	
		Press "N." The command prompt changes to "Enter system name>." Enter a Switching Hub name in 50 one-byte characters or less.
L	Set/edit the installation location information.	
		Press "L." The command prompt changes to "Enter system location>." Enter a Switching Hub location in 50 one-byte characters or less.
C	Set/edit the contact information.	
		Press "C." The command prompt changes to "Enter system contact>." Enter contact information in 50 one-byte characters or less.
Q	Return to the previous menu.	

4.6.2. System IP Configuration

On the Basic Switch Configuration Menu, pressing "I" opens the System IP Configuration Menu, as shown in Fig. 4-6-3. On this screen, you can set IP-address-related settings for this Switching Hub.

```
PN28080K Local Management System
Basic Switch Configuration -> System IP Configuration Menu

MAC Address:        xx:xx:xx:xx:xx:xx
IP Address:         0.0.0.0
Subnet Mask:        0.0.0.0
Default Gateway:    0.0.0.0

------------------------------ <COMMAND> ----------------------------------

Set [I]P Address
Set Subnet [M]ask
Set Default [G]ateway
Set IP P[a]rameter
Set I[P]v6 Address
[Q]uit to previous menu




Command>
Enter the character in square brackets to select option
```

Fig. 4-6-3 System IP Configuration

Screen Description

MAC Address	Shows the MAC address of the Switching Hub. This value is a unique identifier assigned to the device. It cannot be changed.
IP Address	Shows the current IP address. 0.0.0.0 is displayed because no address is set on shipment.
Subnet Mask	Shows the current subnet mask. 0.0.0.0 is displayed because no address is set on shipment.
Default Gateway	Shows the IP address of the router, set as a current default gateway. 0.0.0.0 is displayed because no address is set on shipment.

Available commands are listed below.

I	Set/edit the IP address.	
		Press "I." The command prompt changes to "Enter IP address>." Enter an IP address for the Switching Hub.
M	Set/edit the subnet mask.	
		Press "M." The command prompt changes to "Enter subnet mask>." Enter a subnet mask for the Switching Hub.
G	Set/edit the IP address of the router for the default gateway.	
		Press "G." The command prompt changes to "Enter new gateway IP address>." Enter the IP address of the router, set as the default gateway.
A	Set the IP address, subnet mask and default gateway in succession.	
		Press "A." The command prompt changes to "Enter IP address>." Enter the IP address of the Switching Hub. Then, the command prompt changes to "Enter subnet mask>." Enter the subnet mask. Then, the command prompt changes to "Enter new gateway IP address>." Enter the IP address of a router, used as a default gateway.
Q	Return to the previous menu.	

Note: This item must be set in order to use the SNMP management functionality and to enable a remote connection by Telnet or SSH. Any IP addresses on the local network must be unique and no duplication is allowed. If you are unsure, consult the network administrator.

4.6.2.a. IPv6 Configuration

On the System IP Configuration Menu, pressing "P" opens the IPv6 Configuration Menu, as shown in Fig. 4-6-4. On this screen, you can set IPv6-address-related settings for this Switching Hub.

```
PN28080K Local Management System
System IP Configuration Menu -> IPv6 Configuration Menu

MAC Address:              xx:xx:xx:xx:xx:xx
IPv6 Status:              Disabled
IPv6 Address/PrefixLen:   ::/128
IPv6 Link Local Address:  ::
IPv6 Default Gateway:     ::

------------------------------ <COMMAND> ----------------------------------
[E]nable/Disable IPv6 Status  Set I[P]v6 Address
Set IPv6 Default Ga[t]eway    Set IPv6 Li[n]k Local Address
Set IPv6 Pa[r]ameter          [Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-6-4 System IP Configuration

Screen Description

MAC Address	Shows the MAC address of the Switching Hub. This value is a unique identifier assigned to the device. It cannot be changed.	
IPv6 Status	Shows the IPv6 status.	
	Enabled	The IPv6 status is enabled.
	Disabled	The IPv6 status is disabled.
IPv6 Address /PrefixLen	Shows the current IPv6 address and prefix length. ::/128 is displayed because no address is set on shipment.	
IPv6 Link Local Address	Shows the current IPv6 link local address. :: displayed because no address is set on shipment.	
IPv6 Default Gateway	Shows the IPv6 address of the router, set as a current default gateway. :: is displayed because no address is set on shipment.	

4.6.3. SNMP Configuration

On the Basic Switch Configuration Menu, pressing "N" opens the SNMP Configuration Menu, as shown in Fig. 4-6-5. On this screen, you can configure the SNMP agent settings.

```
PN28080K Local Management System
Basic Switch Configuration -> SNMP Configuration Menu


SNMP [M]anagement Configuration
SNMP [E]xtend Configuration
SNMP [T]rap Receiver Configuration
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-6-5 SNMP Configuration

Screen Description

SNMP Management Configuration	Configures the SNMP manager settings.
SNMP Extend Configuration	Configures the SNMP extend settings.
SNMP Trap Receiver Configuration	Configures the SNMP trap receiver settings.
Quit to previous menu	Returns to the previous menu.

Available commands are listed below.

M	Configure the SNMP manager settings.	
		Press "M." The SNMP Management Configuration Menu opens.

E	Configure the SNMP extend settings.	
		Press "E." The SNMP Extend Configuration Menu opens.
T	Configure the trap receiver settings.	
		Press "T." The SNMP Trap Receiver Configuration Menu opens.
Q	Quit the SNMP Configuration Menu and return to the previous menu.	

4.6.3.a. SNMP Management Configuration

On the SNMP Configuration Menu, pressing "M" opens the SNMP Management Configuration Menu, as shown in Fig. 4-6-6. On this screen, you can configure the SNMP manager settings.

```
PN28080K Local Management System
SNMP Configuration -> SNMP Management Configuration Menu

SNMP Manager List:
 No.   Status    Privilege     IP Address         Community
----  --------  -----------  ---------------  ----------------------------
  1   Enabled   Read-Only    0.0.0.0          public
  2   Enabled   Read-Write   0.0.0.0          private
  3   Disabled  Read-Only    0.0.0.0
  4   Disabled  Read-Only    0.0.0.0
  5   Disabled  Read-Only    0.0.0.0
  6   Disabled  Read-Only    0.0.0.0
  7   Disabled  Read-Only    0.0.0.0
  8   Disabled  Read-Only    0.0.0.0
  9   Disabled  Read-Only    0.0.0.0
 10   Disabled  Read-Only    0.0.0.0

-------------------------------- <COMMAND> ----------------------------------

Set Manager [S]tatus      Set Manager [I]P            Set Manager I[P]v6
Set Manager P[r]ivilege   Set Manager [C]ommunity     [Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-6-6 SNMP Management Configuration

Screen Description

SNMP Manager List:	Shows the current SNMP manager settings.		
	No.	Shows the entry number on the SNMP Manager List.	
	Status	Shows the SNMP manager status.	
		Enabled	The SNMP manager is enabled.
		Disabled	The SNMP manager is disabled.
	Privilege	Shows the access privilege of the SNMP manager.	
		Read-Write	Both the read and write operations are allowed.
		Read-Only	Only the read operation is allowed.
	IP Address	Shows the IP address of the SNMP manager.	
	Community	Shows the current community name.	

Available commands are listed below.

S	Set the SNMP manager status.
	Press "S." The command prompt changes to "Enter manager entry number>." Enter an SNMP manager entry number you wish to configure. Then, the command prompt changes to "Enable or Disable SNMP manger (E/D)>." Press "E" to enable the SNMP manager. Press "D" to disable it.
I	Set an IP address for an SNMP manager.
	Press "I." The command prompt changes to "Enter manager entry number>." Enter an SNMP Management entry number you wish to configure. Then, the command prompt changes to "Enter IP address for manager>." Enter an IP address.
R	Set an access privilege for an SNMP manager.
	Press "R." The command prompt changes to "Enter manager entry number>." Enter an SNMP manager entry number you wish to configure. Then, the command prompt changes to "Enter the selection>." Press "1" for read-only permission. Press "2" for read-and-write.
P	Configure the IPv6 SNMP manager settings.
	Press "P." The IPv6 SNMP Manager Menu opens. For configuration details, refer to 4.6.3.b.
C	Set a community name for an SNMP manager.
	Press "C." The command prompt changes to "Enter manager entry number>." Enter an SNMP manager entry number you wish to configure. Then, the command prompt changes to "Enter community name for manager>." Enter a community name.
Q	Return to the previous menu.

4.6.3.b. IPv6 SNMP Manager

On the SNMP Management Configuration Menu, pressing "P" opens the Set IPv6 SNMP Manager Menu, as shown in Fig. 4-6-7. On this screen, you can configure the SNMP IPv6 manager settings.

```
PN28080K Local Management System
SNMP Management Configuration Menu -> Set IPv6 SNMP Manager Menu

SNMP Manager List:
 No.    IPv6 Address
-------------------------------------------
  1    ::
  2    ::
  3    ::
  4    ::
  5    ::
  6    ::
  7    ::
  8    ::
  9    ::
 10    ::

-------------------------------- <COMMAND> ----------------------------------

Set Manager [I]Pv6        [Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-6-7 SNMP Management Configuration

Screen Description

SNMP Manager List:	Shows the current SNMP manager settings.	
	No.	Shows the entry number on the SNMP Manager List.
	IPv6 Address	Shows the IPv6 address of the SNMP manager.

Available commands are listed below.

I	Set an IP address for an SNMP manager.
	Press "I." The command prompt changes to "Enter manager entry number>." Enter an SNMP Management entry number you wish to configure. Then, the command prompt changes to " Enter new manager IPv6 address>." Enter an IPv6 address.
Q	Return to the previous menu.

4.6.3.c. SNMP Extend Configuration

On the SNMP Configuration Menu, pressing "E" opens the SNMP Extend Configuration Menu, as shown in Fig. 4-6-8. On this screen, you can configure the SNMP manager settings.

```
PN28080K Local Management System
SNMP Configuration Menu -> SNMP Extend Configuration Menu


SNMP [U]ser Configuration
SNMP [V]iew Configuration
SNMP [G]roup Configuration
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-6-8 SNMP Management Configuration

Screen Description

SNMP User Configuration	Configures the SNMP user settings.
SNMP View Configuration	Configures the SNMP View settings.
SNMP Group Configuration	Configures the SNMP Group settings.
Quit to previous menu	Returns to the previous menu.

Available commands are listed below.

U	Configure the SNMP user settings.	
		Press "U." The SNMP User Configuration Menu opens.
V	Configure the SNMP view settings.	
		Press "V." The SNMP View Configuration Menu opens.
G	Configure the SNMP Group settings.	
		Press "G." The SNMP Group Configuration Menu opens.
Q	Quit the SNMP Configuration Menu and return to the previous menu.	

4.6.3.d. SNMP User Configuration

On the SNMP Extend Configuration Menu, pressing "U" opens the SNMP User Configuration Menu, as shown in Fig. 4-6-9. On this screen, you can configure the SNMP User settings.

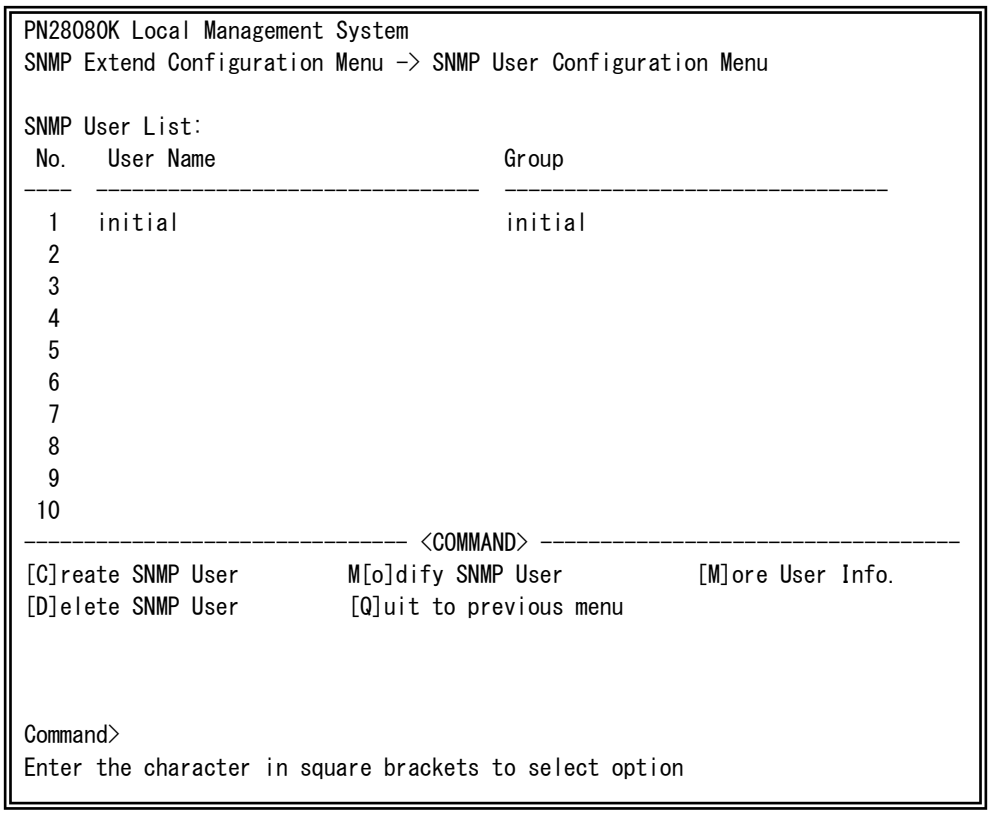


Fig. 4-6-9 SNMP User Configuration

Screen Description

SNMP User List:	Shows the current SNMP user settings.	
	No.	Shows the entry number on the SNMP User List.
	User Name	Shows the SNMP user name.
	Group	Shows the group of the SNMP user.

Available commands are listed below.

C	Go to the screen for creating SNMP user.
	Press "C." The command prompt changes to " Enter User ID>." Enter an SNMP user entry number you wish to configure. Then, the SNMP User Configuration Menu opens.
O	Go to the screen for changing SNMP user.
	Press "O." The command prompt changes to " Enter User ID>." Enter an SNMP user entry number you wish to configure. Then, the Modify SNMP User Configuration Menu opens.
M	Show additional information on a SNMP user.
	Press "M" to display information on authentication type, priviledge.
D	Delete a SNMP user.
	Press "D." The command prompt changes to " Enter User ID>." Enter User ID you wish to delete with a value of 1 to 10.
Q	Return to the previous menu.

4.6.3.e. Create SNMP User Configuration

On the SNMP User Configuration Menu, pressing "C" opens the Create SNMP User Configuration Menu, as shown in Fig. 4-6-10. On this screen, you can configure the SNMP User settings.

```
PN28080K Local Management System
SNMP User Configuration Menu -> Create SNMP User Configuration Menu

Index : 3

User Name      :
Group Name     :
   READ_VIEW   : None
   WRITE_VIEW  : None
   NOTIFY_VIEW : None
Authentication : None
Auth. key      : None
Privilege      : None
Privilege Key  : None
IP address     : 0.0.0.0

-------------------------------- <COMMAND> ----------------------------------
Set [U]ser Name          Set [G]roup Name         Set Auth. [K]ey
Set [A]uthentication     Set [P]riv. Key          Set P[r]ivilege
Set [I]P address         [Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-6-10 Create SNMP User

Screen Description

Index	Shows the entry number on the SNMP User List.	
User Name	Shows the SNMP user name.	
Group Name	Shows the group name.	
	READ_VIEW	Shows the name of view to read.
	WRITE_VIEW	Shows the name of view to write.
	NOTIFY_VIEW	Shows the name of view to notify.
Authentication	Shows the authentication method.	
Auth.key	Shows the authentication key.	
Privilege	Shows the encryption scheme.	
Privilege Key	Shows the encryption key.	

IP address	Shows the SNMP manager IP address.

Available commands are listed below.

U	Set a SNMP user name.	
		Press "U." The command prompt changes to " Enter User Name>." Enter a SNMP user name.
G	Set a name of group.	
		Press "G." The command prompt changes to " Enter Group Name>." Enter a SNMP group name.
K	Set an authentication key.	
		Press "K." The command prompt changes to " Use Password or Key>." Press "P" to enter a password. Press "K" to enter a key. If "P" is selected, the command prompt changes to " Enter Password>." Enter a password. If "K" is selected, the command prompt changes to "Enter Key>." Enter a key.
A	Set the authentication method.	
		Press "A." The command prompt changes to " Enter Authentication Type>." Press "M" to select MD5. Press "S" to select SHA.
P	Set the encryption key.	
		Press "P." The command prompt changes to " Use Password or Key>." Press "P" to enter a password. Press "K" to enter a key. If "P" is selected, the command prompt changes to " Enter Password>." Enter a password. If "K" is selected, the command prompt changes to "Enter Key>." Enter a key.
R	Set the encryption scheme.	
		Press "A." The command prompt changes to "Enter Privilege Type>." Press "D" to select DES.
I	Set the SNMP manager.	
		Press "I." The command prompt changes to "Enter User IP address>." Enter an IP address.
Q	Return to the previous menu.	

4.6.3.f. Modify SNMP User Configuration

On the SNMP User Configuration Menu, pressing "0" opens the Modify SNMP User Configuration Menu, as shown in Fig. 4-6-11. On this screen, you can configure the SNMP User settings.

```
PN28080K Local Management System
SNMP User Configuration Menu -> Modify SNMP User Configuration Menu

Index : 2

User Name      : test
Group Name     : test
   READ_VIEW   : test
   WRITE_VIEW  : test
   NOTIFY_VIEW : test
Authentication : MD5
Auth. Key      : 7b954b5c52218eebd6cdd7083a6d2d30
Privilege      : None
Privilege Key  : None
IP address     : 0.0.0.0

-------------------------------- <COMMAND> ----------------------------------
Set [U]ser Name          Set [G]roup Name         Set Auth. [K]ey
Set [A]uthentication     Set [P]riv. Key          Set P[r]ivilege
Set [I]P address         [Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-6-11 Modify SNMP User

Screen Description

Index	Shows the entry number on the SNMP User List.	
User Name	Shows the SNMP user name.	
Group Name	Shows the group of the SNMP user.	
	READ_VIEW	Shows the name of view to read.
	WRITE_VIEW	Shows the name of view to write.
	NOTIFY_VIEW	Shows the name of view to notify.
Authentication	Shows the authentication method.	
Auth.key	Shows the authentication key.	
Privilege	Shows the encryption scheme.	
Privilege Key	Shows the encryption key.	

IP address	Shows the SNMP manager IP address.

Available commands are listed below.

U	Set a SNMP user name.	
		Press "U." The command prompt changes to " Enter User Name>." Enter a SNMP user name.
G	Set a name of group.	
		Press "G." The command prompt changes to " Enter Group Name>." Enter a SNMP group name.
K	Set an authentication key.	
		Press "K." The command prompt changes to " Use Password or Key>." Press "P" to enter a password. Press "K" to enter a key. If "P" is selected, the command prompt changes to " Enter Password>." Enter a password. If "K" is selected, the command prompt changes to "Enter Key>." Enter a key.
A	Set the authentication method.	
		Press "A." The command prompt changes to " Enter Authentication Type>." Press "M" to select MD5. Press "S" to select SHA.
P	Set the encryption key.	
		Press "P." The command prompt changes to " Use Password or Key>." Press "P" to enter a password. Press "K" to enter a key. If "P" is selected, the command prompt changes to " Enter Password>." Enter a password. If "K" is selected, the command prompt changes to "Enter Key>." Enter a key.
R	Set the encryption scheme.	
		Press "A." The command prompt changes to "Enter Privilege Type>." Press "D" to select DES.
I	Set the SNMP manager.	
		Press "I." The command prompt changes to "Enter User IP address>." Enter an IP address.
Q	Return to the previous menu.	

4.6.3.g. SNMP View Configuration

On the SNMP Extend Configuration Menu, pressing "V" opens the SNMP View Configuration Menu, as shown in Fig. 4-6-12. On this screen, you can configure the SNMP View settings.

```
PN28080K Local Management System
SNMP Extend Configuration Menu -> SNMP View Configuration Menu

Total Entry : 8
View Name                        Subtree                  View Type
-------------------------------  -----------------------  ---------
restricted                       1.3.6.1.2.1.1            Included
restricted                       1.3.6.1.2.1.11           Included
restricted                       1.3.6.1.6.3.10.2.1       Included
restricted                       1.3.6.1.6.3.11.2.1       Included
restricted                       1.3.6.1.6.3.15.1.1       Included
CommunityView                    1                        Included
CommunityView                    1.3.6.1.6.3              Excluded
CommunityView                    1.3.6.1.6.3.1            Included



------------------------------ <COMMAND> ----------------------------------
[N]ext Page              [C]reate SNMP View         M[o]dify SNMP View
Pre[v]ious Page          [D]elete SNMP View          [Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-6-12 SNMP View Configuration

Screen Description

Total Entry	Shows the number of SNMP View.
View Name	Shows the SNMP View name.
Subtree	Shows the SNMP View subtree.
View Type	Shows the SNMP View type.

Available commands are listed below.

N	Show the next page.
	Press "N." The screen shows the next page.
P	Show the previous page.
	Press "P." The screen shows the previous page.
C	Go to the screen for creating SNMP view.
	Press "C." The command prompt changes to " Please enber view name>." Enter an SNMP view in 32 one-byte characters or less. Then, the Create SNMP View Configuration Menu opens.
O	Go to the screen for changing SNMP view.
	Press "O." The command prompt changes to " Please enber view name>." Enter an SNMP view in 32 one-byte characters or less. Then, the Modify SNMP View Configuration Menu opens.
D	Delete a SNMP user.
	Press "D." The command prompt changes to " Please enter view name>." Enter an SNMP view name in 32 one-byte characters or less.
Q	Return to the previous menu.

4.6.3.h. Create SNMP View Configuration

On the SNMP View Configuration Menu, pressing "C" opens the Create SNMP View Configuration Menu, as shown in Fig. 4-6-13. On this screen, you can configure the SNMP View settings.

```
PN28080K Local Management System
SNMP View Configuration Menu -> Create SNMP View Configuration Menu

View Name      : test
Subtree                                                          Type
---------------------------------------------------------------  ---------









-------------------------------- <COMMAND> ----------------------------------
[N]ext Page              [A]dd OID                [Q]uit to previous menu
Pre[v]ious Page          [D]elete OID

Command>
Enter the character in square brackets to select option
```

Fig. 4-6-13 Create SNMP View

Screen Description

View Name	Shows the SNMP View name.
Subtree	Shows the SNMP View subtree.
View Type	Shows the SNMP View type.

Available commands are listed below.

N	Show the next page.	
		Press "N." The screen shows the next page.
P	Show the previous page.	
		Press "P." The screen shows the previous page.
A	Register an additional OID in subtree.	
		Press "A." The command prompt changes to " Enter OID>." Enter an OID. Then, the command prompt changes to " Enter Type>." Press "I" to include OID. Press "E" to exclude OID.
D	Delete an OID that has been registered in subtree.	
		Press "D." The command prompt changes to " Enter OID>." Enter an OID.
Q	Return to the previous menu.	

4.6.3.i. Modify SNMP View Configuration

On the SNMP View Configuration Menu, pressing "0" opens the Modify SNMP View Configuration Menu, as shown in Fig. 4-6-14. On this screen, you can configure the SNMP view settings.

```
PN28080K Local Management System
SNMP View Configuration Menu -> Modify SNMP View Configuration Menu

View Name      : test
Subtree                                                          Type
---------------------------------------------------------------  ---------
1                                                                Included









-------------------------------- <COMMAND> ----------------------------------
[N]ext Page              [A]dd OID                [Q]uit to previous menu
Pre[v]ious Page          [D]elete OID

Command>
Enter the character in square brackets to select option
```

Fig. 4-6-14 Modify SNMP View

Screen Description

View Name	Shows the SNMP View name.
Subtree	Shows the SNMP View subtree.
View Type	Shows the SNMP View type.

Available commands are listed below.

N	Show the next page.	
		Press "N." The screen shows the next page.
P	Show the previous page.	
		Press "P." The screen shows the previous page.
A	Register an additional OID in subtree.	
		Press "A." The command prompt changes to " Enter OID>." Enter an OID. Then, the command prompt changes to " Enter Type>." Press "I" to include OID. Press "E" to exclude OID.
D	Delete an OID that has been registered in subtree.	
		Press "D." The command prompt changes to " Enter OID>." Enter an OID.
Q	Return to the previous menu.	

4.6.3.j. SNMP Group Configuration

On the SNMP Extend Configuration Menu, pressing "G" opens the SNMP Group Configuration Menu, as shown in Fig. 4-6-15. On this screen, you can configure the SNMP Group settings.

```
PN28080K Local Management System
SNMP Extend Configuration Menu -> SNMP Group Configuration Menu

Total Entry : 5
Group Name                       Ver.  Level
-------------------------------  ----  --------------
public                           v1    NoAuth/NoPriv
public                           v2c   NoAuth/NoPriv
initial                          v3    NoAuth/NoPriv
private                          v1    NoAuth/NoPriv
private                          v2c   NoAuth/NoPriv









-------------------------------- <COMMAND> ----------------------------------
[N]ext Page              [C]reate SNMP Group      M[o]dify SNMP Group
Pre[v]ious Page          [D]elete SNMP Group      [M]ore Group Info.
[Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-6-15 SNMP Group Configuration

Screen Description

Total Entry	Shows the number of SNMP Group.
Group Name	Shows the SNMP Group name.
Ver.	Shows the SNMP version.
Level	Shows the SNMP security level.

Available commands are listed below.

N	Show the next page.
	Press "N." The screen shows the next page.
P	Show the previous page.
	Press "P." The screen shows the previous page.
C	Go to the screen for creating SNMP group.
	Press "C." The command prompt changes to " Please input the SNMP Group Name>." Enter an SNMP view in 32 one-byte characters or less. Then, the command prompt changes to " Please input the SNMP Group Version>." Press "1" for SNMP v1. Press "2" for SNMP v2c. Press "3" for SNMP v3. Then, the Create SNMP Group Configuration Menu opens.
O	Go to the screen for changing SNMP group.
	Press "O." The command prompt changes to " Please input the SNMP Group Name>." Enter an SNMP view in 32 one-byte characters or less. Then, the command prompt changes to " Please input the SNMP Group Version>." Press "1" for SNMP v1. Press "2" for SNMP v2c. Press "3" for SNMP v3. Then, the Modify SNMP Group Configuration Menu opens.
D	Delete a SNMP group.
	Press "D." The command prompt changes to " Please input the SNMP Group Name>." Enter an SNMP view in 32 one-byte characters or less. Then, the command prompt changes to " Please input the SNMP Group Version>." Press "1" for SNMP v1. Press "2" for SNMP v2c. Press "3" for SNMP v3.
M	Show additional information on a SNMP group.
	Press "M" to display information on Read View Name, Write View Name, Notify View Name
Q	Return to the previous menu.

4.6.3.k. Create SNMP Group Configuration

On the SNMP Group Configuration Menu, pressing "C", input "SNMP Group name","SNMP Version", opens the Create SNMP Group Configuration Menu, as shown in Fig. 4-6-16. On this screen, you can configure the SNMP Group settings.

```
PN28080K Local Management System
SNMP Group Configuration Menu -> Create SNMP Group Configuration Menu

Group Name     : test
SNMP Version   : v3
   READ_VIEW   : None
   WRITE_VIEW  : None
   NOTIFY_VIEW : None
Security Level : NoAuth/NoPriv









-------------------------------- <COMMAND> ----------------------------------
Set [S]NMP Version       Set [R]ead View           Set [W]rite View
Set N[o]tify View        Set S[e]curity Level      [Q]uit to previous menu




Command>
Enter the character in square brackets to select option
```

Fig. 4-6-16 Create SNMP Group

Screen Description

Group Name	Shows the SNMP Group name.
SNMP Version	Shows the SNMP version.
READ_VIEW	Shows the SNMP read view.
WRITE_VIEW	Shows the SNMP write view.
NOTIFY_VIEW	Shows the SNMP notify view.
Level	Shows the SNMP security level.

Available commands are listed below.

S	Set a SNMP version.
	Press "S." The command prompt changes to " Enter SNMP version>." Press "1" for SNMP v1. Press "2" for SNMP v2c. Press "3" for SNMP v3.
O	Set a name of view to notify.
	Press "O." The command prompt changes to " Enter Notify View>." Enter an SNMP view name in 32 one-byte characters or less.
R	Set a name of view to read.
	Press "R." The command prompt changes to " Enter Read View>." Enter an SNMP view name in 32 one-byte characters or less.
E	Set a security level.
	Press "E." The command prompt changes to " Please input the Select security level(N/A/P) >." Press "N" for no authentication and no privilege. Press "A" for authentication and no priviledge. Press "P" for authentication and priviledge.
W	Set a name of view to write.
	Press "W." The command prompt changes to " Enter Write View>." Enter an SNMP view name in 32 one-byte characters or less.
Q	Return to the previous menu.

4.6.3.l. Modify SNMP Group Configuration

On the SNMP Group Configuration Menu, pressing "O", input "SNMP Group name","SNMP Version", opens the Modify SNMP Group Configuration Menu, as shown in Fig. 4-6-17. On this screen, you can configure the SNMP Group settings.

```
PN28080K Local Management System
SNMP Group Configuration Menu -> Modify SNMP Group Configuration Menu

Group Name     : test
SNMP Version   : v3
   READ_VIEW   : None
   WRITE_VIEW  : None
   NOTIFY_VIEW : None
Security Level : NoAuth/NoPriv









-------------------------------- <COMMAND> ----------------------------------
Set [S]NMP Version       Set [R]ead View          Set [W]rite View
Set N[o]tify View        Set S[e]curity Level     [Q]uit to previous menu




Command>
Enter the character in square brackets to select option
```

Fig. 4-6-17 Modify SNMP Group

Screen Description

Group Name	Shows the SNMP Group name.
SNMP Version	Shows the SNMP version.
READ_VIEW	Shows the SNMP read view.
WRITE_VIEW	Shows the SNMP write view.
NOTIFY_VIEW	Shows the SNMP notify view.
Level	Shows the SNMP security level.

Available commands are listed below.

S	Set a SNMP version.	
		Press "S." The command prompt changes to " Enter SNMP version>." Press "1" for SNMP v1. Press "2" for SNMP v2c. Press "3" for SNMP v3.
O	Set a name of view to notify.	
		Press "O." The command prompt changes to " Enter Notify View>." Enter an SNMP view name in 32 one-byte characters or less.
R	Set a name of view to read.	
		Press "R." The command prompt changes to " Enter Read View>." Enter an SNMP view name in 32 one-byte characters or less.
E	Set a security level.	
		Press "E." The command prompt changes to " Please input the Select security level(N/A/P) >." Press "N" for no authentication and no privilege. Press "A" for authentication and no priviledge. Press "P" for authentication and priviledge.
W	Set a name of view to write.	
		Press "W." The command prompt changes to " Enter Write View>." Enter an SNMP view name in 32 one-byte characters or less.
Q	Return to the previous menu.	

4.6.3.m. SNMP Trap Receiver Configuration

On the SNMP Configuration Menu, pressing "T" opens the SNMP Trap Receiver Configuration Menu, as shown in Fig. 4-6-18. On this screen, you can configure the SNMP trap receiver settings.

```
PN28080K Local Management System
SNMP Configuration -> SNMP Trap Receiver Configuration Menu

Trap Receiver List:
No.    Status    Type   IP Address        Community
---    --------  ----   ---------------   --------------------------------
  1    Disabled  v1     0.0.0.0
  2    Disabled  v1     0.0.0.0
  3    Disabled  v1     0.0.0.0
  4    Disabled  v1     0.0.0.0
  5    Disabled  v1     0.0.0.0
  6    Disabled  v1     0.0.0.0
  7    Disabled  v1     0.0.0.0
  8    Disabled  v1     0.0.0.0
  9    Disabled  v1     0.0.0.0
 10    Disabled  v1     0.0.0.0

-------------------------------- <COMMAND> ----------------------------------

Set Receiver [S]tatus     Set Receiver [I]P          In[d]ividual Trap Config
Set Trap [T]ype           Set Receiver [C]ommunity   Set Receiver I[P]v6
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-6-18 SNMP Trap Receiver Configuration

Screen Description

Trap Receiver List:	Shows the IP address and the community name for the current trap receiver.		
	No.	Shows the entry number for the trap receiver.	
	Status	Shows the trap sending setting.	
		Enabled	Sends traps.
		Disabled	Does not send traps.
	Type	Shows the trap type.	
		v1	Sends SNMP v1 traps.
		v2c	Sends SNMP v2c traps.
	IP Address	Shows the IP address of a trap receiver.	
	Community	Shows the current community name of a trap receiver.	

Available commands are listed below.

S	Enable/disable the trap receiver.	
		Press "S." The command prompt changes to "Enter manager entry number>." Enter an entry number for the trap receiver you wish to configure. Then, the command prompt changes to "Enable or Disable Trap Receiver (E/D)>." Press "E" to enable the SNMP manager. Press "D" to disable it.
I	Set an IP address for the trap receiver.	
		Press "I." The command prompt changes to "Enter manager entry number>." Enter an entry number for the trap receiver you wish to configure. Then, the command prompt changes to "Enter IP address for trap receiver>." Enter an IP address.
D	Configure the trap sending settings when the link status changes.	
		Press "D" to open the Enable/Disable Individual Trap Menu. For configuration details, refer to 4.6.3.C.
T	Set a trap type.	
		Press "T." The command prompt changes to "Enter manager entry number>." Enter an entry number for the trap receiver you wish to configure. Then, the command prompt changes to "Enter the selection>." Press "1" to select SNMPv1 traps. Press "2" to select SNMPv2 traps.
C	Set a community name for the trap receiver.	
		Press "C." The command prompt changes to "Enter manager entry number>." Enter an entry number for a trap receiver you wish to configure. Then, the command prompt changes to "Enter community name for trap receiver>." Enter a community name.
P	Configure the IPv6 Trap Receiver settings.	
	Press "P." The IPv6 Trap Receiver Menu opens. For configuration details, refer to 4.6.3.o.	
Q	Return to the previous menu.	

4.6.3.n. Enable/Disable Individual Trap

On the SNMP Trap Receiver Configuration Menu, pressing "d" opens the Enable/Disable Individual Trap Menu, as shown in Fig. 4-6-19. On this screen, you can configure the trap sending settings.

```
PN28080K Local Management System
SNMP Trap Receiver Configuration -> Enable/Disable Individual Trap Menu

Coldstart :                     Disabled
SNMP Authentication Failure :   Disabled
Login Failure :                 Disabled
Enable Link Up/Down Port:       1-9

-------------------------------- <COMMAND> ----------------------------------

Enable/Disable [C]oldstart Trap
Enable/Disable [A]uth Fail Trap
Enable/Disable [L]ogin Fail Trap
Add Link Up/Down Trap [P]orts
[D]elete Link Up/Down Trap Ports
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-6-19 Enable/Disable Individual Trap

Screen Description

Coldstart:	Shows the trap sending settings for a coldstart.	
	Enabled:	The trap sending is enabled.
	Disabled:	The trap sending is disabled. (Factory default setting)
SNMP Authentication Failure:	Shows the trap sending settings for an SNMP authentication failure.	
	Enabled:	The trap sending is enabled.
	Disabled:	The trap sending is disabled. (Factory default setting)
Login Failure:	Shows the trap sending settings for a login failure.	
	Enabled:	The trap sending is enabled.
	Disabled:	The trap sending is disabled. (Factory default setting)
Enabled Link Up/Down Port:	Shows the port number to which a trap is sent, when its link status changes. All ports are assigned at factory shipment.	

Available commands are listed below.

C	Enable/disable the trap sending at a coldstart.	
		Press "C." The command prompt changes to " Enable or Disable coldstart trap (E/D)>." Press "E" to enable the trap sending. Press "D" to disable it.
A	Enable/disable the trap sending at an SNMP authentication failure.	
		Press "A." The command prompt changes to "Enable or Disable SNMP Authentication trap (E/D)>." Press "E" to enable the trap sending. Press "D" to disable it.
L	Enable/disable the trap sending at a login failure.	
		Press "L." The command prompt changes to "Enable or Disable Login failure trap (E/D)>." Press "E" to enable the trap sending. Press "D" to disable it.
P	Add a port to which the trap is sent when its link status changes.	
		Press "P." The command prompt changes to "Enter port number>." Enter a port number. The trap is sent for this port.
D	Delete a port to which the trap is sent when its link status changes.	
		Press "D." The command prompt changes to "Enter port number>." Enter a port number. The trap is not sent for this port.
Q	Return to the previous menu.	

Note: There is no individual configuration item for loop detection trap. They are sent based on the SNMP Trap Receiver Configuration.

4.6.3.o Set IPv6 Trap Receiver

On the SNMP Trap Receiver Configuration Menu, pressing "P" opens the Set IPv6 Trap Receiver Menu, as shown in Fig. 4-6-20. On this screen, you can set SNMP trap receiver.

```
PN28080K Local Management System
SNMP Trap Receiver Configuration Menu -> Set IPv6 Trap Receiver Menu

Trap Receiver List:
 No.    IPv6 Address
-----------------------------------------------
  1    ::
  2    ::
  3    ::
  4    ::
  5    ::
  6    ::
  7    ::
  8    ::
  9    ::
 10    ::

-------------------------------- <COMMAND> -----------------------------------

Set Receiver [I]Pv6       [Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-6-20 SNMP Trap Receiver Configuration (IPv6)

Screen Description

Trap Receiver List:	Shows the current SNMP trap receiver settings.	
	No.	Shows the entry number on the SNMP trap receiver List.
	IPv6 Address	Shows the IPv6 address of the SNMP trap receiver.

Available commands are listed below.

I	Set an IPv6 address for an SNMP trap receiver.
	Press "I." The command prompt changes to "Enter manager entry number>." Enter an SNMP trap receiver entry number you wish to configure. Then, the command prompt changes to " Enter new receiver IPv6 address>." Enter an IPv6 address.
Q	Return to the previous menu.

4.6.4. Port Configuration Basic

On the Basic Switch Configuration Menu, pressing "p" opens the Port Configuration Menu, as shown in Fig. 4-6-21. On this screen, you can configure port status display settings and port settings.

```
PN28080K Local Management System
Basic Switch Configuration -> Port Configuration Basic Menu

Port  Trunk      Type      Admin     Link      Mode       Flow Ctrl  Auto-MDI
----  -----  ----------  --------   ----   ------------  ---------  --------
  1    ---      1000T     Enabled    Down   Auto          Disabled   Disabled
  2    ---      1000T     Enabled    Down   Auto          Disabled   Disabled
  3    ---      1000T     Enabled    Down   Auto          Disabled   Disabled
  4    ---      1000T     Enabled    Down   Auto          Disabled   Disabled
  5    ---      1000T     Enabled    Down   Auto          Disabled   Disabled
  6    ---      1000T     Enabled    Down   Auto          Disabled   Disabled
  7    ---      1000T     Enabled    Down   Auto          Disabled   Disabled
  8    ---      1000T     Enabled    Down   Auto          Disabled   Enabled
  9    ---      1000X     Enabled    Down   Auto          Disabled   -------




--------------------------------- <COMMAND> -----------------------------------

Set [A]dmin Status        Set [F]low Control         [Q]uit to previous menu
Set [M]ode                [S]et Auto-MDI

Command>
Enter the character in square brackets to select option
```

Fig. 4-6-21 Port Configuration

Screen Description

Port	Shows the port number.	
Trunk	Shows the group number for a trunked port.	
Type	Shows the port type.	
	100TX	The port type is 10/100BASE-TX.
	1000T	The port type is 10/100/1000BASE-T.
	1000X	The port type is SFP port.
Admin	Shows the current port status. The factory default setting is "Enabled" for all ports.	
	Enabled	The port is available for use.
	Disabled	The port is not available for use.
Link	Shows the current link status.	
	Up	Link is established successfully.
	Down	Link is not established.
Mode	Shows the communication speed and full-duplex/half-duplex settings. The factory default setting is "Auto" for all ports.	
	Auto	Auto negotiation mode
	100-FDx (100F)	100 Mbps full-duplex
	100-HDx (100H)	100 Mbps half-duplex
	10-FDx(10F)	10 Mbps full-duplex
	10-HDx(10H)	10 Mbps half-duplex
Flow Ctrl	Shows the flow control settings. The factory default setting is "Disabled" for all ports.	
	Enabled	The flow control is enabled.
	Disabled	The flow control is disabled.
Auto-MDI	Shows the Auto MDI function settings. The factory default setting is "Disabled" for ports 1 to 8. (The settings for port 9 are fixed at "Enabled.")	
	Enabled	The Auto MDI/MDI-X function is enabled.
	Disabled	The Auto MDI/MDI-X function is disabled.

Available commands are listed below.

A	Enable/disable a port.		
	Press "A." The command prompt changes to "Select port number to be changed>." Enter a port number you wish to change. Press "0" to change the settings of all ports at a time. Then, the command prompt changes to "Enable or Disable port # (E/D)>." Press "E" to enable the port. Press "D" to disable it. When you complete the setting change, the display on the screen is automatically updated.		
M	Configure the speed and full-duplex/half-duplex settings for each port.		
	Press "M." The command prompt changes to "Enter port number>." Enter a port number you wish to change. Press "0" to change the settings of all ports at a time. Then, the command prompt changes to "Enter mode for port # (A/N)>." Press "A" to enable the auto negotiation mode. Press "N" to disable it. If "N" is selected, the command prompt changes to "Enter speed for port #(10/100)>." Select a desired communication speed. Upon setting, the command prompt changes to "Enter duplex for port #(F/H)>." Select "F" for full-duplex. Select "H" for half-duplex. When you complete the setting change, the display on the screen is automatically updated.		
	Mode:	A:	Enable the auto negotiation mode.
		N:	Disable the auto negotiation mode (fixing the speed at Giga is not supported).
	Speed:	10:	Set at 10 Mbps.
		100:	Set at 100 Mbps.
	Duplex:	F:	Set at full-duplex.
		H:	Set at half-duplex.
F	Enable/disable the flow control.		
	Press "F." The command prompt changes to "Select port number to be changed>." Enter a port number you wish to change. Press "0" to change the settings of all ports at a time. Then, the command prompt changes to "Enable or Disable flow control for port # (E/D)>." Press "E" to enable the function. Press "D" to disable it. When you complete the setting change, the display on the screen is automatically updated.		
S	Enable/disable the AUTO-MDI function.		
	Press "S." The command prompt changes to "Enter port number>." Enter a port number (from 1 to 8) you wish to change. Press "0" to change the settings of all ports at a time. Then, the command prompt changes to "Enable or Disable Auto-MDI for port # (E/D)>." Press "E" to enable the function. Press "D" to disable it. As the change is applied, the display on the screen is updated automatically.		
Q	Return to the previous menu.		

Note: The screen shows the port status; however, the status is not automatically updated. To display the latest status, press any key.

4.6.5. Port Configuration Extend

On the Basic Switch Configuration Menu, pressing "e" opens the Port Configuration Menu, as shown in Fig. 4-6-22. On this screen, you can configure port status display settings and port settings.

```
PN28080K Local Management System
Basic Switch Configuration -> Port Configuration Extend Menu

Jumbo Status : Disabled
Port  Trunk      Type     Link     Port Name       EAP Pkt FW
----  -----  -----------  ----  ---------------   -------------
  1    ---      1000T     Down  PORT_1              Disabled
  2    ---      1000T     Down  PORT_2              Disabled
  3    ---      1000T     Down  PORT_3              Disabled
  4    ---      1000T     Down  PORT_4              Disabled
  5    ---      1000T     Down  PORT_5              Disabled
  6    ---      1000T     Down  PORT_6              Disabled
  7    ---      1000T     Down  PORT_7              Disabled
  8    ---      1000T     Down  PORT_8              Disabled
  9    ---      1000X     Down  PORT_9              Disabled




-------------------------------- <COMMAND> ----------------------------------
Set Port N[a]me                        Set [E]AP Packet Forwarding
[Q]uit to previous menu                Set [J]umbo Status

Command>
Enter the character in square brackets to select option
```

Fig. 4-6-22 Port Configuration

Screen Description

Jumbo	Shows the current jumbo frame settings. The factory default setting is "Disabled."	
	Enabled	Jumbo frame is enabled.
	Disabled	Jumbo frame is disabled.
Port	Shows the port number.	
Trunk	Shows the group number for a trunked port.	
Type	Shows the port type.	
	100TX	The port type is 10/100BASE-TX.
	1000T	The port type is 10/100/1000BASE-T.
	1000X	The port type is SFP extension port.
Link	Shows the current link status.	
	Up	Link is established successfully.
	Down	Link is not established.
Port Name	Shows the port name.	
EAP Pkt FW	Shows the current EAP Packet Forwarding settings. The factory default setting is “Disabled”.	
	Enabled	EAP Packet Forwarding is enabled.
	Disabled	EAP Packet Forwarding is disabled.

Available commands are listed below.

E	An EAP Packet forwarding can be assigned to each port.	
		Press "E." The command prompt changes to "Select port number to be changed>." Enter a port number you wish to change. Press "0" to change the settings of all ports at a time. Then, the command prompt changes to " Enable or Disable EAP packet forwarding for port # (E/D)>." Press "E" to enable the function. Press "D" to disable it. As the change is applied, the display on the screen is updated automatically.
A	A name can be assigned to each port.	
		Press "A." The command prompt changes to "Select port number to be changed>." Enter a port number you wish to change. Press "0" to change the settings of all ports at a time. Then, the command prompt changes to "Enter port name string>." Enter a name you wish to assign. When you complete the setting change, the display on the screen is automatically updated.
J	Enable/disable the jumbo frame forwarding function.	
		Press "J." The command prompt changes to " Enable or Disable jumbo status (E/D)>." Press "E" to enable the function. Press "D" to disable the function.
Q	Return to the previous menu.	

Note: The screen shows the port status; however, the status is not automatically updated. To display the latest status, press any key.

4.6.6. Port Configuration Power Saving

The MNO series power saving mode is our unique function for automatically detecting the port connection status and minimizing power consumption if not connected. This Switching Hub supports two modes: the Half mode for giving priority to connectivity with another device, and the Full mode for minimizing power consumption.
On the Basic Switch Configuration Menu, pressing "o" opens the Port Configuration Power Saving Menu, as shown in Fig. 4-6-23. On this screen, you can configure port status display and power saving mode.

```
PN28080K Local Management System
Basic Switch Configuration -> Port Configuration Power Saving Menu

Port  Link  Trunk     Type         Mode       Power-saving    EEE(802.3az)
----  ----  -----  ----------  ------------  --------------  ------------
  1   Down   ---      1000T     Auto            Half            Enabled
  2   Down   ---      1000T     Auto            Half            Enabled
  3   Down   ---      1000T     Auto            Half            Enabled
  4   Down   ---      1000T     Auto            Half            Enabled
  5   Down   ---      1000T     Auto            Half            Enabled
  6   Down   ---      1000T     Auto            Half            Enabled
  7   Down   ---      1000T     Auto            Half            Enabled
  8   Down   ---      1000T     Auto            Half            Enabled
  9   Down   ---      1000X     Auto            -------         -------




-------------------------------- <COMMAND> -----------------------------------

Set Power [S]aving mode                Set [E]EE Status
[Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-6-23 Port Configuration Power Saving

Screen Description

Port	Shows the port number.	
Link	Shows the current link status.	
	Up	Link is established successfully.
	Down	Link is not established.
Trunk	Shows the group number for a trunked port.	
Type	Shows the port type.	
	100TX	The port type is 10/100BASE-TX.
	1000T	The port type is 10/100/1000BASE-T.
	1000X	The port type is SFP extension port.
Mode	Shows the communication speed and full-duplex/half-duplex settings. The factory default setting is "Auto" for all ports.	
	Auto	Auto negotiation mode
	100-FDx(100F)	100 Mbps full-duplex
	100-HDx(100H)	100 Mbps half-duplex
	10-FDx(10F)	10 Mbps full-duplex
	10-HDx(10H)	10 Mbps half-duplex
Power-saving	Shows status of the MN0 series power saving mode. The factory default setting is "Half" for all ports.	
	Half	Power saving mode is enabled (Half).
	Full	Power saving mode is enabled (Full).
	Disabled	Power saving mode is disabled.
EEE(802.3az)	Shows the current EEE (Energy Efficient Ethernet) settings. The factory default setting is “Disabled”.	
	Enabled	EEE is enabled.
	Disabled	EEE is disabled.

Available commands are listed below.

S	Set the MN0 series power saving mode.	
		Press "S." The command prompt changes to "Select port number to be changed>." Enter a port number you wish to change. Press "0" to change the settings of all ports at a time. Then, the command prompt changes to "Enter Power Saving mode for port (F/H/D)>." Press "E" to enable the mode. Press "D" to disable it. Press "H" to enable the power saving mode of giving priority to connectivity with another device. As the change is applied, the display on the screen is updated automatically.
E	An EEE can be assigned to each port.	
		Press "E." The command prompt changes to "Select port number to be changed>." Enter a port number you wish to change. Press "0" to change the settings of all ports at a time. Then, the command prompt changes to " Enable, Disable for Energy Efficient Ethernet(EEE 802.3az) (E/D)>." Press "E" to enable the function. Press "D" to disable it. As the change is applied, the display on the screen is updated automatically.
Q	Return to the previous menu.	

4.6.7. System Security Configuration

On the Basic Switch Configuration Menu, pressing "S" opens the System Security Configuration screen, as shown in Fig. 4-6-24. On this screen, you can configure the access control settings to this Switching Hub for configuration and management.

```
PN28080K Local Management System
Basic Switch Configuration -> System Security Configuration

Console UI Idle Timeout:     5 Min.
Telnet UI Idle Timeout:      5 Min.

Telnet Server:               Enabled         Web Server Status: Enabled
SNMP Agent:                  Disabled
IP Setup Interface:          Enabled
Local User Name:             manager
Syslog Transmission:         Disabled
Login Method 1/2:            Local/None      Method 1 Fail Action:  Method 2
-------------------------------- <COMMAND> ----------------------------------
Set [C]onsole UI Time Out            Change Local User [N]ame
Set [T]elnet UI Time Out             Change Local [P]assword
Enable/Disable Te[l]net Server       [R]ADIUS Configuration
Enable/Disable [S]NMP Agent          L[o]gin Method
[I]P Setup Interface                 Login [M]ethod 1 Fail Action
Enable/Disable S[y]slog Transmission SS[H] Server Configuration
Syslo[g] Transmission Configuration  LED [B]ase Mode Configuration
Telnet [A]ccess Limitation           [W]eb Server Status
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-6-24 System Security Configuration

Screen Description

Console UI Idle Time Out:	Shows the idle timeout settings (in minutes) for terminating a console-connected session if no input is made. The factory default setting is 5 minutes.	
Telnet UI Idle Time Out:	Shows the idle timeout settings (in minutes) for terminating a Telnet-connected session if no input is made. The factory default setting is 5 minutes.	
Telnet Server:	Shows the Telnet access settings. The factory default setting is "Enabled."	
	Enabled	Access is enabled.
	Disabled	Access is disabled.
Web Server:	Shows the Web access settings. The factory default setting is "Disabled."	
	Enabled	Access is enabled.
	Disabled	Access is disabled.
SNMP Agent:	Shows the SNMP access settings. The factory default setting is "Disabled."	
	Enabled	Access is enabled.
	Disabled	Access is disabled.
IP Setup Interface:	Shows the access settings for the IP address configuration software. The factory default setting is "Enabled." * For instructions, refer to Appendix B.	
	Enabled:	Access is enabled.
	Disabled:	Access is disabled.
Local User Name:	Shows the current login user name. The factory default setting is "manager."	
Syslog Transmission:	Shows the settings for sending system logs to the Syslog server. The factory default setting is "Disabled.".	
	Enabled:	Sends system log to the Syslog server.
	Disabled:	Does not send system log to the Syslog server.
Login Method 1/2	Shows the method of verifying the user name and password at login. The factory default setting is "Local" for 1 and "None" for 2.	
	Local	The user name and password set in this Switching Hub is used for login.
	RADIUS	Authentication by RADIUS server is used for login.
	None	Not used. (Only for Login Method 2.)
Method 1 Fail Action	Shows the action after failed to authenticate for Method 1. The factory default setting is "Method 2".	
	Method 2	After failed to authenticate for Method 1, Method 2 is used.
	Stop	After failed to authenticate for Method 1, stop authenticating. But, in the case of no response from RADIUS server, Method 2 is used.

Available commands are listed below.

C	Configure the idle timeout settings for automatically terminating a console-connected session if no input is made.	
		Press "C." The command prompt changes to "Enter console idle timeout>." Enter a value from 0 to 60 (minutes). Entering "0" disables the automatic termination.
T	Configure the idle timeout settings for automatically terminating a Telnet-connected session if no input is made.	
		Press "T." The command prompt changes to "Enter telnet idle timeout>." Enter a value from 1 to 60 (minutes).
N	Edit the login user name.	
		Press "N." The command prompt changes to "Enter current password>." Enter the current password. After entering the correct password, the command prompt changes to "Enter new name>." Enter a new user name in 12 one-byte characters.
P	Edit the login password.	
		Press "P." The command prompt changes to "Enter old password>." Enter the current password. After entering the correct password, the command prompt changes to "Enter new password>." Enter a new password in 12 one-byte characters. After entering the password, the command prompt changes to "Retype new password>" for confirmation. Enter the new password again.
L	Configure the Telnet access settings.	
		Press "L." The command prompt changes to "Enable or Disable telnet server(E/D)>." Press "E" to enable the access. Press "D" to disable the access.
S	Configure the SNMP access settings.	
		Press "S." The command prompt changes to "Enable or Disable SNMP Agent(E/D)>." Press "E" to enable the access. Press "D" to disable the access.
Y	Configure the Syslog transmission settings.	
		Press "Y." The command prompt changes to " Enable or Disable Syslog Transmission (E/D)>." Press "E" to enable the function. Press "D" to disable the function.
R	Configure the RADIUS server access settings for login authentication.	
		Press "R." The RADIUS Configuration Menu opens. For configuration details, refer to the next section **(4.6.7.c).**
M	Configure the action after failed to authenticate for Method 1.	
		Press "M." The command prompt changes to " Enter Method 1 Fail Action (M/S)>." Press "M" to use Method 2. Press "S" to stop authenticating.
G	Set Syslog transmission.	
		Press "G." The Syslog Transmission Configuration Menu opens. For configuration details, refer to the next section **(4.6.7.e).**
A	Set Telnet accessible terminals.	
		Press "A." The Telnet Access Limitation Menu opens. For configuration details, refer to the next section **(4.6.7.a).**
I	Configures the access settings for the IP address configuration software.	
		Press "I." The command prompt changes to "Enable or Disable IP setup interface (E/D)>." Press "E" to enable the access. Press "D" to disable the access.
O	Set the verification method of the login user name and password.	
		Press "O." The command prompt changes to "Enter manager entry number>." Press "1" to change the first login method. Press "2" to change the second login method. Then, the command prompt changes to the "Select the login method." Press "L" to use the user name and password set in the Switching Hub. Press "R" to use authentication by RADIUS. Press "N" for no setting.
H	Configure the SSH server settings.	
		Press "H." The SSH Server Configuration Menu opens. For configuration details, refer to the next section **(4.6.7.g).**
B	Configure the LED base mode settings.	

		Press "B." The LED Basic Mode Configuration Menu opens. For configuration details, refer to the next section **(4.6.7.h)**.
W	Configure the Web access settings.	
		Press "W." The command prompt changes to "Enable or Disable WEB server (E/D)>." Press "E" to enable the access. Press "D" to disable the access.
Q	Return to the previous menu.	

4.6.7.a. Telnet Access Limitation Configuration

On the System Security Configuration Menu, pressing "A" opens the Telnet Access Limitation screen, as shown in Fig. 4-6-25. In this screen, you can configure limitation of equipment accessing to this Switching Hub via Telnet.

```
PN28080K Local Management System
System Security Configuration -> Telnet Access Limitation Menu

Telnet Access Limitation :   Disabled

No.      IP Address          Subnet Mask
---   ---------------     ---------------
 1     <empty>             <empty>
 2     <empty>             <empty>
 3     <empty>             <empty>
 4     <empty>             <empty>
 5     <empty>             <empty>
-------------------------------- <COMMAND> ---------------------------------

[E]nable/Disable Telnet Access Limitation
[A]dd IP Address and Subnet Mask
[D]elete IP Address and Subnet Mask
[M]odify IP Address and Subnet Mask
[S]et IPv6 Access Limitation
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-6-25 Telnet Access Limitation Configuration

Available commands are listed below.

E	Enable/Disable the access limitation from Telnet.	
	E	Set the access limitation from Telnet to Enable.
	D	Set the access limitation from Telnet to Disable.
A	Set an IP address to be permitted. Five ranges can be set up.	
		Press "A." The command prompt changes to "Enter IP address entry number>." Enter an IP address entry number between 1 and 5. The command prompt changes to "Enter IP address>." Enter an IP address to be permitted. If IP address is correct, the command prompt changes to "Enter subnet mask>." Enter a range of IP address you wish to permit accessing with mask. (Setting example) No. IP Address Subnet Mask Access permitted IP address ----- ---------- ---------- ---------- 1 192.168.1.10 255.255.255.255 192.168.1.10 (Only one unit can be accessed) 2 192.168.1.20 255.255.255.254 192.168.1.20, 192.168.1.21 (Two units can be accessed) 3 192.168.2.1 255.255.255.128 192.168.2.1 - 192.168.2.127 (127 units can be accessed) 4 192.168.3.1 255.255.255.0 192.168.3.1 - 192.168.3.254 (254 units can be accessed)
D	Delete a range of IP address that has been set up.	
		Press "D." The command prompt changes to "Enter IP address entry number>." Enter an IP address entry number you wish to delete.
M	Change a range of IP address that has been set up.	
		Press "M." The command prompt changes to "Enter IP address entry number>." Enter an IP address entry number between 1 and 5. The command prompt changes to "Enter IP address>." Enter an IP address that has been set up. The command prompt changes to "Enter subnet mask>." Enter a range of IP address you wish to permit accessing with mask.
S	Set IPv6 Telnet Access Limitation settings.	
		Press "S." The IPv6 Telnet Access Limitation Menu opens. For configuration details, refer to the next section **(4.6.7.b).**
Q	Return to the previous menu.	

4.6.7.b. IPv6 Telnet Access Limitation

On the Telnet Access Limitation Menu, pressing "S" opens the IPv6 Telnet Access Limitation Menu, as shown in Fig. 4-6-26. On this screen, you can configure limitation of equipment accessing to this Switching Hub via Telnet.

```
PN28080K Local Management System
Telnet Access Limitation Menu -> IPv6 Telnet Access Limitation Menu

Telnet Access Limitation :   Enabled

No.      IPv6 Address                                  Prefixlen
---   ----------------------------------------     --------------
 1     <empty>                                      <empty>
 2     <empty>                                      <empty>
 3     <empty>                                      <empty>
 4     <empty>                                      <empty>
 5     <empty>                                      <empty>
-------------------------------- <COMMAND> ----------------------------------

[E]nable/Disable Telnet Access Limitation
[A]dd IPv6 Address and Prefix Length
[D]elete IPv6 Address and Prefix Length
[M]odify IPv6 Address and Prefix Length
[Q]uit to previous menu



Command>
Enter the character in square brackets to select option
```

Fig. 4-6-26 IPv6 Telnet Access Limitation Configuration

Available commands are listed below.

E	Enable/Disable the access limitation from IPv6 Telnet.	
	E	Set the access limitation from IPv6 Telnet to Enable.
	D	Set the access limitation from IPv6 Telnet to Disable.
A	Set an IPv6 address to be permitted. Five ranges can be set up.	
		Press "A." The command prompt changes to "Enter IPv6 address entry number>." Enter an IPv6 address entry number between 1 and 5. The command prompt changes to "Enter IPv6 address>." Enter an IPv6 address to be permitted. If IPv6 address is correct, the command prompt changes to " Enter IPv6 Prefix Length>." Enter a range of IPv6 address you wish to permit accessing with prefix length. Access permitted IP address (Setting example) No. IPv6 Address Prefixlen Access permitted IP address --- ---------- ---------- ---------- 1 2001:1::1 128 2001:1::1 (Only one unit can be accessed) 2 2001:2::1:1 127 2001:2::1:0、2001:1:2::1:1 (Two units can be accessed) 3 2001:3::1:1 126 2001:3::1:0～2001:3::1:3 (Four units can be accessed) 4 2001:4::1:1 125 2001:4::1:0～2001:4::1:7 (Eight units can be accessed)
D	Delete a range of IPv6 address that has been set up.	
		Press "D." The command prompt changes to "Enter IPv6 address entry number>." Enter an IPv6 address entry number you wish to delete.
M	Change a range of IPv6 address that has been set up.	
		Press "M." The command prompt changes to "Enter IPv6 address entry number>." Enter an IPv6 address entry number between 1 and 5. The command prompt changes to "Enter IPv6 address>." Enter an IPv6 address that has been set up. The command prompt changes to "Enter IPv6 Prefix Length>." Enter a range of IPv6 address you wish to permit accessing with prefix length.
Q	Return to the previous menu.	

4.6.7.c. RADIUS Configuration

On the System Security Configuration Menu, pressing "R" opens the RADIUS Configuration screen, as shown in Fig. 4-6-27. On this screen, you can configure access setting to RADIUS server that is used in login authentication.

```
PN28080K Local Management System
System Security Configuration -> RADIUS Configuration Menu

NAS ID: Nas1

Index Server IP address    Shared Secret     Response Time Max Retransmission
----- ----------------- -------------------- ------------- ------------------
  1   0.0.0.0                                  10 seconds        3
  2   0.0.0.0                                  10 seconds        3
  3   0.0.0.0                                  10 seconds        3
  4   0.0.0.0                                  10 seconds        3
  5   0.0.0.0                                  10 seconds        3
------------------------------- <COMMAND> ---------------------------------
Set [N]AS ID
Set Server [I]P
Set Shared Se[c]ret
Set [E]ncrtpted Shared Secret
Set [R]esponse Time
Set [M]ax Retransmission
Set Server I[P]v6
[Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-6-27 RADIUS Configuration

Screen Description

NAS ID:	Shows the authentication ID (NAS Identifier).
Server IP Address:	Shows the IP address of RADIUS server. 0.0.0.0 is displayed because no address is set on shipment.
Shared Secret:	Shows the common key (Shared Secret) that is used in authentication. The same key must be set between the server side and the client side. In general, the system manager sets this common key. No common key is set at shipment.
Response Time:	Shows the maximum response time for authentication request to RADIUS server. The factory default setting is 10 seconds.
Max Retransmission:	Shows the number of retransmission times for authentication request to RADIUS server. The factory default setting is 3 times.

Available commands are listed below.

N	Set a NAS ID (NAS Identifier).
	Press "I." The command prompt changes to "Enter NAS ID>." Enter NAS ID within 16 one-byte characters.
I	Set an IP address of RADIUS server.
	Press "I." The command prompt changes to " Enter RADIUS server index>." Enter a RADIUS server entry number between 1 and 5. The command prompt changes to " Enter IP address for radius server>." Enter an IP address.
C	Set a common key of RADIUS server.
	Press "C." The command prompt changes to " Enter RADIUS server index>." Enter a RADIUS server entry number between 1 and 5. The command prompt changes to "Enter secret string for server>." Enter a common key within 20 one-byte characters.
E	Set an encrypted common key of RADIUS server.
	Press "E." The command prompt changes to " Enter RADIUS server index>." Enter a RADIUS server entry number between 1 and 5. The command prompt changes to " Enter secret string for server with encryption>." Enter a common key within 20 one-byte characters.
R	Set a response time until the RADIUS server responds to authentication request.
	Press "R." The command prompt changes to " Enter RADIUS server index>." Enter a RADIUS server entry number between 1 and 5. The command prompt changes to "Enter response time>." Enter the response time with a value of 1 to 120 (seconds).
M	Set the maximum number of retransmission times for authentication request.
	Press "M." The command prompt changes to " Enter RADIUS server index>." Enter a RADIUS server entry number between 1 and 5. The command prompt changes to "Enter maximum retransmission>." Enter an integer number of 1 to 254.
P	Set IPv6 RADIUS Server settings.
	Press "P." The IPv6 RADIUS Server Menu opens. For configuration details, refer to the next section **(4.6.7.d).**
Q	Return to the previous menu.

4.6.7.d. Set IPv6 RADIUS Server

On the RADIUS Configuration Menu, pressing "P" opens the Set IPv6 RADIUS Server Menu, as shown in Fig. 4-6-28. On this screen, you can configure access setting to RADIUS server that is used in login authentication.

```
PN28080K Local Management System
System Security Configuration -> Set IPv6 RADIUS Server Menu

NAS ID: Nas1

Index Server IPv6 Address
----- ---------------------------------------
  1   ::
  2   ::
  3   ::
  4   ::
  5   ::
------------------------------- <COMMAND> ---------------------------------
Set [N]AS ID
Set Server [I]Pv6
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-6-28 RADIUS Configuration

Screen Description

NAS ID:	Shows the authentication ID (NAS Identifier).
Server IPv6 Address:	Shows the IPv6 address of RADIUS server. :: is displayed because no address is set on shipment.

Available commands are listed below.

N	Set a NAS ID (NAS Identifier).
	Press "N." The command prompt changes to "Enter NAS ID>." Enter NAS ID within 16 one-byte characters.
I	Set an IPv6 address of RADIUS server.
	Press "I." The command prompt changes to " Enter RADIUS server index>." Enter a RADIUS server entry number between 1 and 5. The command prompt changes to " Enter new server IPv6 address>." Enter an IPv6 address.
Q	Return to the previous menu.

4.6.7.e. Syslog Transmission Configuration

On the System Security Configuration Menu, pressing "G" opens the Syslog Transmission Configuration screen, as shown in Fig. 4-6-29. On this screen, you can configure the setting of the Syslog server to which a system log Is sent.

```
PN28080K Local Management System
System Security Configuration -> Syslog Transmission Configuration Menu

Syslog Server List:
 No.      Status        IP Address       Facility     Include SysName/IP
----  -----------   ---------------    ----------    ------------------
  1   Disabled      0.0.0.0            Facility0
  2   Disabled      0.0.0.0            Facility0









--------------------------------- <COMMAND> -----------------------------------
Set Server [S]tatus     Set Server [I]P             [Q]uit to previous menu
Set Server [F]acility   Set S[y]sName/IP Include    [C]lear Server Information
Set Server I[P]v6

Command>
Enter the character in square brackets to select option
```

Fig. 4-6-29 Syslog Configuration

Screen Description

Status	Shows the status of each entry.	
	Enabled	Setting of the entry is enabled.
	Disabled	Setting of the entry is disabled.
IP Address	Shows the IP address of Syslog server.	
Facillity	Shows the value of Facillity.	
Include SysName/IP	Shows information to be added.	
	SysName	Adds the SysName of this switch to the system log to be transmitted.
	IP address	Adds the IP address of this switch to the system log to be transmitted.

Available commands are listed below.

S	Configure the status of Syslog transmission.
	Press "S." The command prompt changes to " Enter manager entry number>." Enter a Syslog server entry number between 1 and 2. The command prompt changes to " Enable or Disable Server (E/D)>." Press "E" to enable the server. Press "D" to disable it.
F	Set Facility.
	Press "F." The command prompt changes to " Enter manager entry number>." Enter a Syslog server entry number between 1 and 2. The command prompt changes to " Enter Server Facility>." Enter a value of 0 to 7. (Local0 to Local7)
I	Set the IP address of Syslog server.
	Press "I." The command prompt changes to " Enter manager entry number>." Enter a Syslog server entry number between 1 and 2. The command prompt changes to " Enter IP address for manager>." Enter the IP address of Syslog server.
Y	Sent information that is added to the system log to be transmitted.
	Press "Y." The command prompt changes to " Enter manager entry number>." Enter a Syslog server entry number between 1 and 2. The command prompt changes to " Enter Include Information>." Press "S" to add the SysName. Press "I" to add the IP address. Press "N" not to add the IP address.
C	Delete setting information of Syslog transmission.
	Press "C." The command prompt changes to " Enter manager entry number>." Enter a Syslog server entry number between 1 and 2. The command prompt changes to " Clear Syslog Server information>." Press "Y" to delete the server information. Press "N" not to delete it.
P	Set IPv6 Syslog Transmission settings.
	Press "P." The IPv6 Syslog Transmission Menu opens. For configuration details, refer to the next section **(4.6.7.f)**.
Q	Return to the previous menu.

4.6.7.f. Set IPv6 Syslog Server

On the System Transmission Configuration Menu, pressing "P" opens the Set IPv6 Syslog Server screen, as shown in Fig. 4-6-30. On this screen, you can configure the setting of the Syslog server to which a system log Is sent.

```
PN28080K Local Management System
 System Security Configuration -> Set IPv6 Syslog Server Menu

 Syslog Server List:
  No.     IPv6 Address
 ----  ----------------------------------------
   1   ::
   2   ::









 -------------------------------- <COMMAND> ----------------------------------
 Set Server [I]Pv6
 [Q]uit to previous menu


 Command>
 Enter the character in square brackets to select option
```

Fig. 4-6-30 Syslog Configuration

Screen Description

Server IPv6 Address:	Shows the IPv6 address of Syslog server. :: is displayed because no address is set on shipment.

Available commands are listed below.

I	Set an IPv6 address of Syslog server.
	Press "I." The command prompt changes to " Enter manager entry number>." Enter a Syslog server entry number between 1 and 2. The command prompt changes to " Enter new server IPv6 address>." Enter the IPv6 address of the Syslog server.
Q	Return to the previous menu.

4.6.7.g. SSH Server Configuration

On the System Security Configuration, pressing "H" opens the SSH Server Configuration screen, as shown in Fig. 4-6-31. On this screen, you can configure the SSH server setting. This Switching Hub supports SSHv2 only. Use and connect a client supporting SSHV2.

```
PN28080K Local Management System
System Security Configuration -> SSH Server Configuration

SSH UI Idle Timeout:          5 Min.
SSH Auth. Idle Timeout:       120 Sec.
SSH Auth. Retries Time:       5
SSH Server:                   Disabled
SSH Server key:               Key does not exist.









------------------------------ <COMMAND> ----------------------------------
[G]enerate SSH Server key              Enable/Disable SS[H] Server
Set SSH UI Time [O]ut                  Set SSH [A]uthentication Time Out
Set SSH Authentication [R]etries Time  [Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-6-31 SSH Server Configuration

Screen Description

SSH UI Idle Timeout	Shows the idle timeout settings (in minutes) for terminating an SSH remote-connected session if no input is made. The factory default setting is 5 minutes.	
SSH Auth. Idle Timeout	Shows the response time to SSH authentication. The factory default setting is 120 seconds.	
SSH Auth. Retries Time	Shows the number of retries for SSH authentication. The factory default setting is 5 times.	
SSH Server	Shows the SSH access settings. The factory default setting is "Disabled."	
	Enabled(SSH)	Access is enabled.
	Disabled	Access is disabled.
SSH Server key	Shows the status of SSH server key.	
	Key exists.	The server key exists.
	Key does not exist.	The server key does not exist.

Available commands are listed below.

G	Generate an SSH server key.
	Press "G" to generate an SSH server key.
H	Configure the SSH access setting.
	Press "H." The command prompt changes to "Enable or Disable SSH server (E/D)>." Press "E" to enable the access. Press "D" to disable the access.
O	Configure the idle timeout settings for automatically terminating an SSH-connected session if no input is made.
	Press "O." The command prompt changes to "Enter SSH UI idle timeout>." Enter a value from 1 to 60 (minutes).
A	Set the response time to SSH authentication.
	Press "A." The command prompt changes to "Enter SSH authentication idle timeout>." Enter a value from 1 to 120 (seconds).
R	Set the number of retries for SSH authentication.
	Press "R." The command prompt changes to "Enter SSH authentication retries time>." Enter a value from 0 to 5 (times).
Q	Return to the previous menu.

4.6.7.h. LED Base Mode Configuration

On the System Security Configuration, pressing "B" opens the LED Base Mode Configuration screen, as shown in Fig. 4-6-32. On this screen, you can configure the LED base mode setting.

```
PN28080K Local Management System
System Security Configuration -> LED Base Mode Configuration

System LED base-mode: Status









Note: Save Configuration to Flash will be executed when LED Base Mode changed.

-------------------------------- <COMMAND> ----------------------------------

Set LED [B]ase Mode
[Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-6-32 LED Base Mode Configuration

Screen Description

System LED base-mode	Shows the current LED base mode. This is set to the status mode (Status) on shipment.	
	Status	Operating in status mode.
	Eco	Operating in ECO mode.

Available commands are listed below.

B	Change the LED base mode.	
	Press "B." The command prompt changes to "Select LED Base Mode (S/E)>." Press "S" to change the LED base mode to the status mode. Press "E" to change it to the ECO mode.	
Q	Return to the previous menu.	

Note: If the LED base mode is changed, the configuration information is saved and all settings are stored in a built-in memory.

4.6.8. Forwarding Database

On the Basic Switch Configuration Menu, pressing "F" opens the Forwarding Database Information Menu, as shown in Fig. 4-6-33. In this screen, a list of MAC address required for transferring packets that have been learned and recorded.
Also, you can add or delete MAC address statically.

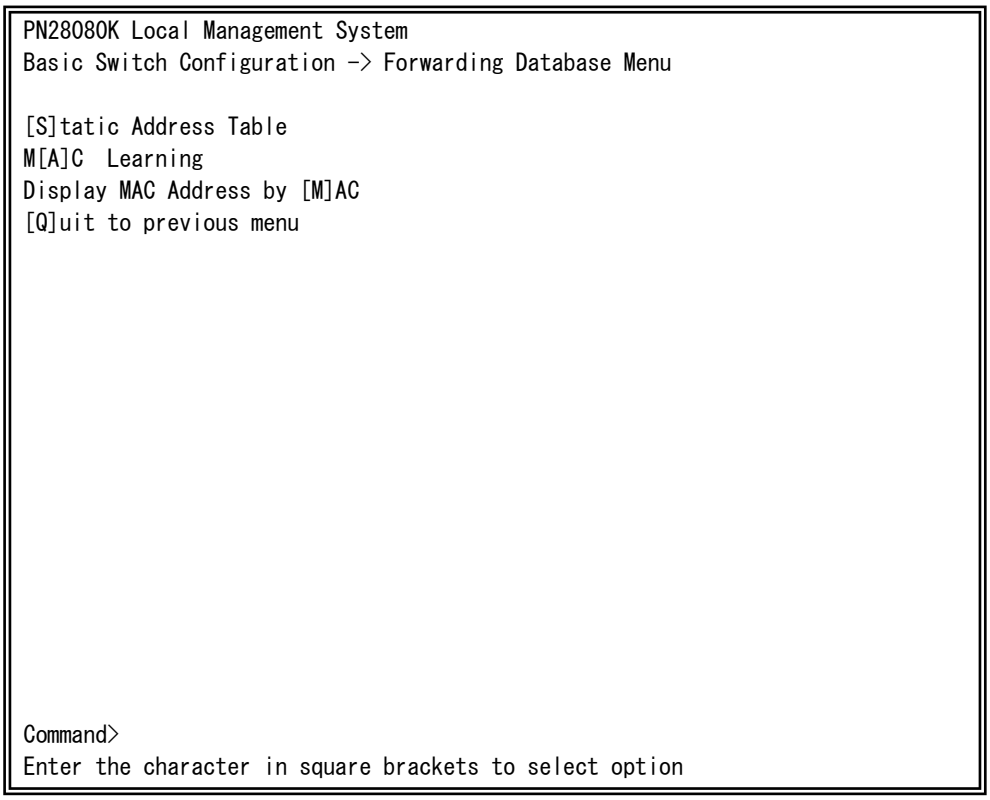


Fig.4-6-33 Forwarding Database

Screen Description

Static Address Table	Adds or deletes the MAC address of forwarding database.
MAC Learning	Sets to Auto/Off for the MAC address learning function of each port. If this is set to OFF, only MAC address registered in the Static Address Table is allowed for communications.
Display MAC Address by Port	Shows all MAC addresses that have been registered.
Quit to previous menu	Returns to the previous menu.

4.6.8.a. Adding or Deleting MAC Address

On the Forwarding Database Information Menu, pressing "S" opens the Static Address Table Menu, as shown in Fig. 4-6-34. In this screen, you can add or delete a MAC address statically.

```
PN28080K Local Management System
Forwarding Database Menu -> Static Address Table Menu

   MAC Address       Port    VLAN ID
-----------------   ------   -------
Database is empty!









--------------------------------- <COMMAND> -----------------------------------
[N]ext Page                              [D]elete Entry
[P]revious Page                          [Q]uit to previous menu
[A]dd New Entry


Command>
Enter the character in square brackets to select option
```

Fig. 4-6-34 Adding or Deleting MAC Address

Screen Description

MAC Address	Shows the MAC address in MAC address table.
Port	Shows the port to which the MAC address belongs.
VLAN ID	Shows the VLAN ID to which the MAC address belongs.

Available commands are listed below.

N	Show the next page.
	Press "N." The screen shows the next page.
P	Show the previous page.
	Press "P." The screen shows the previous page.
A	Register an additional MAC address.
	Press "A." The command prompt changes to "Enter MAC Address(xx:xx:xx:xx:xx:xx)." Enter a MAC address to be added.
D	Delete a MAC address that has been registered.
	Press "D." The command prompt changes to "Enter MAC Address(xx:xx:xx:xx:xx:xx)." Enter a MAC address to be deleted.
Q	Return to the previous menu.

4.6.8.b. Setting MAC Address Auto-learning

On the Forwarding Database Information Menu, pressing "A" opens the MAC Learning Menu, as shown in Fig. 4-6-35. On this screen, you can configure the MAC address auto-learning setting for each port and limit the number of MAC address auto-learning.

```
PN28080K Local Management System
 Forwarding Database Menu -> MAC Learning Menu

  Port   MAC Learning     MAC Learning Limit
------  ------------    -------------------
    1    Auto            Disabled
    2    Auto            Disabled
    3    Auto            Disabled
    4    Auto            Disabled
    5    Auto            Disabled
    6    Auto            Disabled
    7    Auto            Disabled
    8    Auto            Disabled
    9    Auto            Disabled




-------------------------------- <COMMAND> ----------------------------------
 [S]et MAC Learning Mode
 Set MAC Learning [L]imit
 [Q]uit to previous menu

 Command>
 Enter the character in square brackets to select option
```

Fig. 4-6-35 MAC Address Learning

Screen Description

Port	Shows the port number.	
MAC Learning	Shows the status of MAC address auto-learning.	
	Auto	MAC address auto-learning is enabled. (Factory default setting)
	Disabled	MAC address auto-learning is disabled.
MAC Learning Limit	Shows the limit number of MAC address auto-learning for each port.	
	Disabled	The number of MAC address auto-learning is not limited. (Factory default setting)
	1-256	Indicates the limit number of MAC address auto-learning.

Note: If MAC address auto-learning is disabled, communication cannot be established unless MAC address is registered statistically.

Note: Assuming that the number of learned MAC addresses reaches the limit, and if a frame with new source MAC address that has not been learned is received, this frame is discarded. To set the limit value, MAC address auto-learning must be enabled. Static MAC address is not included in the limit value.

Available commands are listed below.

N	Show the next page.
	Press "N." The screen shows the next port.
P	Show the previous page.
	Press "P." The screen shows the previous port.
S	Switches the status of auto-learning.
	Press "S." The command prompt changes to "Select Port Number to be changed>." Enter a port number you wish to change the setting. Then, the command prompt changes to "Change MAC Learning Mode for port # (specified port number)>." Press "A" to enable auto-learning. Press "D" to disable the mode.
L	Set the limit number of MAC address auto-learning.
	Press "L." The command prompt changes to "Select Port Number to be changed>." Enter a port number you wish to change setting. Then, the command prompt changes to "Enable or Disable MAC Learning Limit status for port # (specified port number) (E/D)>." Press "E" to set a limit value for the number of auto-learning. Then, the command prompt changes to "Enter MAC Limit number>." Enter a value of 1 to 256. Press "D" not to set a limit for the number of auto-learning.
Q	Return to the previous menu.

4.6.8.c. Displaying All MAC Addresses

On the Forwarding Database Information Menu, pressing "M" opens the Display MAC Address by MAC screen, as shown in Fig. 4-6-36. In this screen, you can display all MAC address tables in this Switching Hub.

```
PN28080K Local Management System
Forwarding Database Menu -> Display MAC Address by MAC

Age-Out Time:    300 Sec.

   MAC Address       Port
-----------------    ----
xx:xx:xx:xx:xx:xx     CPU









-------------------------------- <COMMAND> ----------------------------------
[N]ext Page                              Set [A]ge-Out Time
[P]revious Page                          [Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-6-36 Displaying All MAC Addresses

Screen Description

Age-Out Time:	Shows a time to store MAC address table. It is equal to the time after receiving the last packet. The factory default setting is 300 seconds (5 minutes).
MAC Address	Shows the MAC address in MAC address table.
Port	Shows the port to which the MAC address has belonged.

Available commands are listed below.

N	Show the next page.
	Press "N." The screen shows the next port.
P	Show the previous page.
	Press "P." The screen shows the previous port.
A	Set a time to store MAC address.
	Press "A." The command prompt changes to "Enter Age-Out time>." Enter Age-Out time with a value of 10 to 1000000 (seconds).
Q	Return to the previous menu.

4.6.9. Time Configuration

In this Switching Hub, it is possible to set the exact time by synchronizing the internal clock to an external SNTP server's clock with a support of SNTP (Simple Network Time Protocol).

On the Basic Switch Configuration Menu, pressing "T" opens the Time Configuration Menu, as shown in Fig. 4-6-37. In this screen, you can configure the time setting and time synchronization setting by SNTP.

```
PN28080K Local Management System
Basic Switch Configuration -> Time Configuration Menu

Time ( HH:MM:SS )   : 12:13:13
Date ( YYYY/MM/DD ) : 2001/01/01    Monday

SNTP Server IP        : 0.0.0.0
SNTP Server IPv6      : ::
SNTP Polling Interval : 1440 Min
Time Zone : (GMT+09:00) Osaka,Sapporo,Tokyo
Daylight Saving       : N/A

-------------------------------- <COMMAND> ----------------------------------
Set [C]lock Time
Set SNTP Server I[P]
Set SNTP [I]nterval
Set Time [Z]one
S[e]t Daylight Saving
Set SNTP [S]erver IPv6
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-6-37 Configuring of Time Synchronization Function: before configuration

```
PN28080K Local Management System
Basic Switch Configuration -> Time Configuration Menu

Time ( HH:MM:SS )   : 10:20:33
Date ( YYYY/MM/DD ) : 2009/04/01     Wednesday

SNTP Server IP        : 192.168.0.2
SNTP Server IPv6      : ::
SNTP Polling Interval : 1440 Min
Time Zone : (GMT+09:00) Osaka,Sapporo,Tokyo
Daylight Saving       : N/A

-------------------------------- <COMMAND> ----------------------------------
Set [C]lock Time
Set SNTP Server I[P]
Set SNTP [I]nterval
Set Time [Z]one
S[e]t Daylight Saving
Set SNTP [S]erver IPv6
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-6-38 Configuring of Time Synchronization Function: after configuration

Screen Description

Time (HH:MM:SS):	Shows the time of internal clock.
Date (YYYY/MM/DD):	Shows the date of internal clock.
SNTP Server IP	Shows the IP address of SNTP server for time synchronization.
SNTP Server IPv6	Shows the IPv6 address of SNTP server for time synchronization.
SNTP Polling Interval	Shows an interval of time synchronization with SNTP server.
Time Zone:	Shows the time zone.
Daylight Saving:	Shows the application status of Daylight Saving (Summer time).

Available commands are listed below.

C	Set the time of internal clock of this Switching Hub.	
		Press "C." The command prompt changes to "Enter Date(Year) >" and enter a year. Then, the command prompt changes to "Enter Date(Month) >" and enter a month. Then, the command prompt changes to "Enter Date(Day) >" and enter a day. Then, the command prompt changes to "Enter Time(Hour) >" and enter an hour. Then, the command prompt changes to "Enter Time(Minute) >" and enter a minute. Then, the command prompt changes to "Enter Time(Sec) >" and enter a second.
P	Set an IP address of SNTP server.	
		Press "P." The command prompt changes to "Enter new IP address>." Enter an IP address of SNTP server.
I	Set an interval of time synchronization with SNTP server.	
		Press "I." The command prompt changes to "Enter Interval Time>." Enter an interval of time synchronization with SNTP server with a value of 1 to 1440 (minutes). The factory default setting is 1440 minutes (1 day).
E	Set the application status of Daylight Saving (Summer time).	
		Press "E." The command prompt changes to "Enable or Disable Daylight Saving (E/D)>." Enter "E" to use daylight saving time. Press "D" not to use it. When the time zone is set to where daylight saving time is not applied, this setting is not available. When this Switching Hub is used domestically, this setting is not required.
Z	Set the time zone.	
		Press "Z." A list of time zones is displayed. Specify a time zone you wish to set. When this Switching Hub is used domestically, change of time zone is not required as the factory default setting is "(GMT+09:00) Osaka, Sapporo, Tokyo."
S	Set an IPv6 address of SNTP server.	
		Press "S." The command prompt changes to " Enter new server IPv6 address>." Enter an IPv6 address of SNTP server.
Q	Return to the previous menu.	

Note: If SNTP server is located outside of firewall, connection with SNTP server may be blocked depending on settings by a system administrator.
For details, ask your system administrator.
If you wish to disable time synchronization function, set SNTP server IP to 0.0.0.0. or ::.

4.6.10. ARP Table

On the Basic Switch Configuration Menu, pressing "R" opens the ARP Table screen, as shown in Fig. 4-6-39. In this screen, you can refer and configure ARP table.

```
PN28080K Local Management System
Basic Switch Configuration -> ARP Table

Sorting Method :   By IP
ARP Age Timeout : 7200  seconds
  IP Address      Hardware Address     Type
---------------   -----------------   -------









--------------------------------- <COMMAND> -----------------------------------
[N]ext Page                           [S]orting Entry Method
[P]revious Page                       [A]dd/Modify Static Entry
Set ARP Age [T]imeout                 [D]elete Entry
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-6-39 ARP Table

Screen Description

Sorting Method	Shows the order of displaying.	
	By IP	Shows the table in the order of IP address.
	By Static	Shows manually-set addresses.
	By Dynamic	Shows auto-learned addresses.
ARP Age Timeout	Shows the age-out time of ARP table.	
IP Address	Shows the IP address on ARP table.	
Hardware Address	Shows the hardware address on ARP table.	
Type	Shows the type on ARP table.	
	Static	The address is manually set.
	Dynamic	The address is auto-learned.

Available commands are listed below.

N	Show the next page.	
		Press "N." The screen shows the next page.
P	Show the previous page.	
		Press "P." The screen shows the previous page.
T	Set the age-out time of ARP table.	
		Press "T." The command prompt changes to "Enter ARP age timeout value >." Enter the age-out time of ARP table with a value of 30 to 86400 (seconds).
S	Select the order of displaying ARP table.	
		Press "S." The command prompt changes to "Select method for sorting entry to display (I/T)>." Press "I" to display in the order of IP address. Press "T" to display in the order of type. If "T" is selected, the command prompt changes to "Select type for sorting entry to display (S/D)>." Press "S" to display manually-set addresses. Press "D" to display auto-leaned addresses.
A	Add/modify an entry of ARP table.	
		Press "A." The command prompt changes to "Enter IP address>." Enter an IP address. Then, the command prompt changes to "Enter Hardware address>." Enter a MAC address as "**:**:**:**:**:**".
D	Delete an entry of ARP table.	
		Press "D." The command prompt changes to "Enter IP address>." Enter an IP address.
Q	Return to the previous menu.	

4.6.11. NDP Table

On the Basic Switch Configuration Menu, pressing "D" opens the NDP Table screen, as shown in Fig. 4-6-40. In this screen, you can refer and configure NDP table.

```
PN28080K Local Management System
Basic Switch Configuration -> NDP Table

Sorting Method:     By IP
NDP Reachable Time: 30 Seconds          NDP Stale Time: 600 Seconds
  IPv6 Address                          Hardware Address  Status     Type
------------------------------------- ----------------- ---------- -------









-------------------------------- <COMMAND> ----------------------------------
[N]ext Page                           [A]dd/Modify Static Entry
[P]revious Page                       [D]elete Entry
Set NDP [R]eachable Time              [S]orting Entry Method
Set NDP Stale [T]ime                  [Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-6-40 NDP Table

Screen Description

Sorting Method	Shows the order of displaying.	
	By IP	Shows the table in the order of IPv6 address.
	By MAC	Shows the table in the order of MAC address.
	By Static	Shows manually-set addresses.
	By Dynamic	Shows auto-learned addresses.
Type	Shows the type on ARP table.	
	Static	The address is manually set.
	Dynamic	The address is auto-learned.
NDP Reachable Time	Shows the NDP Reachable time.	
NDP State Time	Shows the NDP Stale time.	
IPv6 Address	Shows the IPv6 Address on NDP table.	
Hardware Address	Shows the hardware address on NDP table.	
Status	Shows the IPv6 neighbor cache.	
Type	Shows the type on NDP table.	
	Static	The address is manually set.
	Dynamic	The address is auto-learned.

Available commands are listed below.

N	Show the next page.	
		Press "N." The screen shows the next page.
P	Show the previous page.	
		Press "P." The screen shows the previous page.
R	Set the IPv6 Reachable time of NDP table.	
		Press "R." The command prompt changes to " Enter NDP reachable time value>." Enter the IPv6 Reachable time of NDP table with a value of 30 to 86400 (seconds).
T	Set the IPv6 Stale time of NDP table.	
		Press "T." The command prompt changes to " Enter NDP stale time value>." Enter the IPv6 Stale time of NDP table with a value of 0 to 86400 (seconds).
A	Add/modify an entry of NDP table.	
		Press "A." The command prompt changes to "Enter IPv6 address>." Enter an IPv6 address. Then, the command prompt changes to "Enter Hardware address>." Enter a MAC address as "**:**:**:**:**:**".
D	Delete an entry of NDP table.	
		Press "D." The command prompt changes to "Enter IPv6 address>." Enter an IPv6 address.
S	Select the order of displaying NDP table.	
		Press "S." The command prompt changes to " Select method for sorting entry to display (I/M/D/S)>." Press "I" to display in the order of IPv6 address. Press "M" to display in the order of MAC address. Press "D" to display auto-leaned addresses. Press "S" to display manually-set addresses.
Q	Return to the previous menu.	

4.7. Advanced Switch Configuration

On the Main Menu, pressing "A" opens the Advanced Switch Configuration Menu, as shown in Fig. 4-7-1. On this screen, you can configure settings of VLAN, link aggregation, port monitoring, access control, storm control, QoS, storm control, 802.1X Port Based Access Control, loop detection/shut-off, port grouping, digital diagnostic monitoring, and static multicast address functions.

```
PN28080K Local Management System
Main Menu -> Advaneced Switch Configuration Menu


[V]LAN Management
[L]ink Aggregation
Port [M]onitoring Configuration
[A]ccess Control Configuration
Quality of Service [C]onfiguration
St[o]rm Control Configuration
802.1[X] Port Based Access Control Configuration
Loop [D]etection Configuration Menu
[P]ort Group Configuration
Di[g]ital Diagnostic Monitoring
Static M[u]lticast Address Configuration
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-7-1 Advanced Switch Configuration

Screen Description

VLAN Management	Configures VLAN function setting.
Link Aggregation	Configures Link Aggregation setting.
Port Monitoring Configuration	Configures Port Monitoring (mirroring) setting.
Access Control Configuration	Configures Access Control setting.
Quality of Service Configuration	Configures QoS setting.
Storm Control Configuration	Configures Storm Control function setting.
802.1X Port Based Access Control Configuration	Configures IEEE802.1X Port Based Access Control setting.
Loop Detection Configuration	Configures Loop Detection/Shut-off setting.
Port Group Configuration	Configures Port Grouping setting.
Digital Diagnostic Monitoring	Configures Digital Diagnostic Monitoring setting. SFP module monitored must support SFF-8472(DMI: Diagnostic Monitoring Interface).
Static Multicast Address Configuration	Configures Static Multicast Address setting.
Quit to previous menu	Quits the Advanced Switch Configuration Menu and returns to the Main menu.

4.7.1. VLAN Management

4.7.1.a. Features

- Corresponding to IEEE802.1Q compatible Tag VLAN, a frame can be sent with a VLAN tag (hereinafter referred to as just "tag").

- Having two different parameters of VLAN ID and PVID, forwarding destination of an untagged frame is determined by a combination of these parameters.

- VLAN ID
  VLAN ID is a VLAN identifier placed on each frame in processing tagged frames. As for an untagged frame, ports are divided into groups by this ID, and the forwarding destination of the frame is determined by referring to this ID. Multiple VLANs can be assigned to each port.

- PVID (Port VLAN ID)
  Only one PVID can be set to each port. When an untagged frame is received, this ID determines to which VLAN the frame should be forwarded. As for a tagged frame, this ID is not referred and VLAN ID in the tag is used instead.

4.7.1.b. VLAN Management Menu

On the Advanced Switch Configuration Menu, pressing "V" opens the VLAN Management Menu, as shown in Fig. 4-7-2. On this screen, you can configure VLAN-related settings.

```
PN28080K Local Management System
Advanced Switch Configuration -> VLAN Management Menu

Total VLANs : 1
Internet Mansion : Disabled                Uplink      :
VLAN ID  VLAN Name                         VLAN Type    Mgmt
-------  --------------------------------  ----------   ----
1                                          Permanent    UP









-------------------------------- <COMMAND> ----------------------------------
[N]ext Page                C[o]nfig VLAN Member        Set [M]anagement Status
[P]revious Page            [S]et Port Config           [D]elete VLAN
[C]reate VLAN              Set [I]nternet Mansion      [Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-7-2 VLAN Management Menu

Screen Description

Internet Mansion	Shows the status of Internet Mansion mode.	
	Enabled	Internet Mansion mode is enabled.
	Disabled	Internet Mansion mode is disabled. (Factory default setting)
Uplink	Indicates the uplink port when Internet Mansion mode is enabled.	
VLAN ID	Shows the VLAN ID of VLAN.	
VLAN Name	Shows the VLAN name being configured.	
VLAN Type	Shows the type of VLAN.	
	Permanent	Indicates that the VLAN is the one of initial setting. This VLAN cannot be deleted.
	Static	Indicates that the VLAN is the newly configured one.
Mgmt	Shows whether the VLAN is a management VLAN or not.	
	UP	A management VLAN that is allowed to communicate with CPU.
	DOWN	Not a management VLAN.

Available commands are listed below.

N	Show the next page.
	Press "N." The screen shows the next page.
P	Show the previous page.
	Press "P." The screen shows the previous page.
C	Go to the screen for creating VLAN.
	Press "C." The VLAN Create Menu opens. For details, refer to the next section **(4.7.1.c).**
D	Delete a VLAN.
	Press "D." The command prompt changes to "Enter VLAN ID>." Enter VLAN ID you wish to delete with a value of 2 to 4094.
M	Set the management VLAN.
	Press "M." The command prompt changes to "Enter index number>." Enter a VLAN ID you wish to configure as a management VLAN with a value of 1 to 4094.
I	Set the Internet Mansion mode.
	Press "I." The command prompt changes to "Enable or Disable Internet Mansion Function? (E/D)>." Press "E" to enable the function. Press "D" to disable it. If "E" is selected, the command prompt changes to "Uplink port?>." Enter a port number you wish to configure as an uplink port. This function enables to configure all settings needed for the Internet mansion environment. Ports other than that designated as an uplink port are set as downlink ports. Communications between downlink ports are shut off. Therefore, it becomes possible to ensure security between each resident. **(There are some constrained conditions for use. Please make configuration after confirming the notes.)**
O	Go to the screen for changing VLAN.
	Press "O." The command prompt changes to "Enter VLAN ID>." Enter a VLAN ID you wish to configure with a value of 1 to 4094. Then, the VLAN Modification Menu opens. For details, refer to the next section (4.7.1.d).
S	Set and confirm PVID by port.
	Press "S." The VLAN Port Configuration Menu opens. For details, refer to the next section (4.7.1.e).
Q	Return to the previous menu.

Note: VLAN 1 is set on shipment, and all ports belong to this VLAN.
Also, the management VLAN is enabled.

Note: When creating a new VLAN, PVID (after-mentioned) is not changed in conjunction with this new creation. After registering VLAN on this screen, make sure to confirm the configuration operation and content on the configuration screen in Fig. 4-7-4 and Fig. 4-7-5.

On deletion, you cannot delete a VLAN whose ID is remained as a PVID. Delete the VLAN after changing the PVID to another ID.

Note: When Internet Mansion mode is enabled, there are constrained conditions as the followings.

Please use the Switching Hub after confirming these constrained conditions.

(1) Combined usage with Link Aggregation is not possible.

(2) Static registration to MAC Address table is not possible.

(3) Combined usage with MAC Learning is not possible.

(4) Only the uplink port belongs to management VLAN.

4.7.1.c. VLAN Creation Menu

On the VLAN Management Menu, pressing "C" opens the VLAN Creation Menu , as shown in Fig. 4-7-3. On this screen, you can create VLAN.

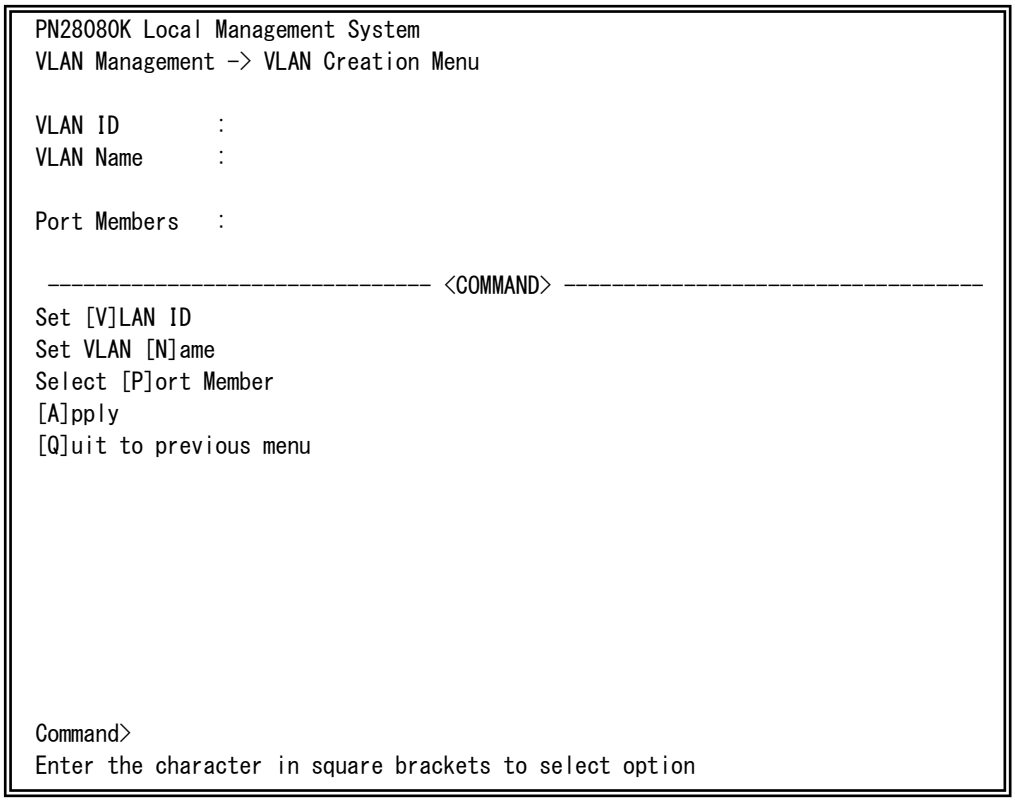


Fig. 4-7-3 VLAN Creation Menu

Screen Description

VLAN ID	Shows the VLAN ID.
VLAN Name	Shows the VLAN name.
Port Member	Shows the port number of the VLAN member.

Available commands are listed below.

S	Set a VLAN ID (VLAN Identifier).	
		Press "S." The command prompt changes to "Enter VLAN ID>." Enter a VLAN ID.
N	Set a name of VLAN.	
		Press "N." The command prompt changes to "Enter VLAN name>." Enter a VLAN name within 30 one-byte characters.
P	Set a member of VLAN.	
		Press "P." The command prompt changes to "Enter egress port number>." Enter a port number you wish to set. When entering multiple port numbers, delimit with comma with no space, or hyphenate the continuous numbers.
A	Create VLAN.	
		Press "A" to apply the setting.
Q	Return to the previous menu.	

Note: After setting a VLAN, make sure to press "A" to apply the setting. If you press "Q" without pressing "A," the setting will be discarded and VLAN will not be created.

4.7.1.d. VLAN Modification Menu

On the VLAN Management Menu, pressing "o" and specifying target VLAN ID open the VLAN Modification Menu, as shown in Fig. 4-7-4. On this screen, you can modify VLAN-related setting information.

```
PN28080K Local Management System
VLAN Management -> VLAN Modification Menu

VLAN ID        : 1
VLAN Name      :

Port Members   : 1-8
Untagged Ports : 1-8

 -------------------------------- <COMMAND> ----------------------------------
Set VLAN [N]ame
Select [P]ort Member
[A]pply
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-7-4 VLAN Modification Menu

Screen Description

VLAN ID	Shows the VLAN ID.
VLAN Name	Shows the VLAN name.
Port Member	Shows the port number of the VLAN member.
Untagged Port:	Shows the port without adding VLAN tags.

Available commands are listed below.

N	Set a name of VLAN.	
		Press "N." The command prompt changes to "Enter VLAN name>." Enter a VLAN name within 30 one-byte characters.
P	Set a member of VLAN.	
		Press "P." The command prompt changes to "Enter egress port number>." Enter a port number you wish to set. When entering multiple port numbers, delimit with comma with no space, or hyphenate the continuous numbers.
A	Apply modification of VLAN configuration.	
		Press "A" to apply the setting.
Q	Return to the previous menu.	

4.7.1.e. VLAN Port Configuration Menu

On the VLAN Management Menu, pressing "S" opens the VLAN Port Configuration Menu, as shown in Fig. 4-7-5. In this screen, you can configure VLAN-related settings by port.

```
PN28080K Local Management System
VLAN Management -> VLAN Port Configuration Menu

Port  PVID  Acceptable Frame Type
----  ----  --------------------
 1    1     Admit All
 2    1     Admit All
 3    1     Admit All
 4    1     Admit All
 5    1     Admit All
 6    1     Admit All
 7    1     Admit All
 8    1     Admit All

 -------------------------------- <COMMAND> ----------------------------------

[N]ext page                Set [F]rame Type
[P]revious Page            Set Port [V]ID
[Q]uit



Command>
Enter the character in square brackets to select option
```

Fig. 4-7-5 VLAN Port Configuration Menu

Screen Description

Port	Shows the port number.	
PVID	Shows the PVID (Port VLAN ID) being set to the port. PVID indicates VLAN ID to which an untagged packet should be forwarded when it is received. The factory default setting is 1. When a tagged packet is received, destination port will be determined according to the tag, regardless of PVID.	
Acceptable Type	Shows the type of received frame.	
	Admit All	Receives all frames.
	Tagged Only	Receives only VLAN-tagged frames.

Available commands are listed below.

N	Show the next page.	
		Press "N." The screen shows the next page.
P	Show the previous page.	
		Press "P." The screen shows the previous page.
V	Configure PVID settings.	
		Press "V." The command prompt changes to "Enter port number>." Enter a port number you wish to configure. Then, the command prompt changes to "Enter PVID for port #>." Enter a PVID with a value of 1 to 4094.
F	Set the type of received frame.	
		Press "F." The command prompt changes to "Enter port number>." Enter a port number you wish to configure. Then, the command prompt changes to "Select port acceptable frame type (A/T)>." Enter "A" to receive all frames. Enter "T" to receive only tagged frames.
Q	Return to the previous menu.	

Note: In this Switching Hub, multiple VLANs can be assigned to one port. If a new VLAN is created, a port will belong to both existing VLAN and new VLAN. To divide the domains, make sure to delete the port from the existing VLAN.

4.7.2. Link Aggregation

4.7.2.a. About Link Aggregation

Link aggregation is a function that can increase redundancy of network paths and bandwidth between Switching Hubs by grouping multiple ports to a trunk for connection.

In this Switching Hub, up to 8 ports can be assigned to 1 group, and 4 groups can be created.

When using both Link Aggregation and Access Control functions, assign a practical physical port number to a port list of access control, not a logical port created in Link Aggregation. For details, refer to 4.7.4.

Note: If port communication modes are mixed, Link Aggregation cannot be configured. In addition, Link Aggregation and Internet Mansion mode cannot be used simultaneously.

Note: Depending on number of ports in a group or the traffic condition, traffic may not be assigned uniformly to all the ports.

Note: If you shutdown one of the ports where the Link Aggregation is configured, this action shutdowns all the ports of the same group member of the Link Aggregation.

4.7.2.b. Link Aggregation Menu

On the Advanced Switch Configuration Menu, pressing "L" opens the Trunk Configuration Menu, as shown in Fig. 4-7-6. On this screen, you can configure Link Aggregation settings.

```
PN28080K Local Management System
Advanced Switch Configuration -> Link Aggregation Menu

Group   Status    Port Members
-----  --------  -------------------------------
 1     Disabled
 2     Disabled
 3     Disabled
 4     Disabled
 5     Disabled
 6     Disabled
 7     Disabled
 8     Disabled

-------------------------------- <COMMAND> ----------------------------------
[A]dd Trunk Group
[R]emove Trunk Group
[Q]uit to previous menu




Command>
Enter the character in square brackets to select option
```

Fig. 4-7-6 Link Aggregation Menu

Screen Description

Group	Shows the group number of trunking.	
Status	Shows the status of each group.	
	Enabled	Link Aggregation is enabled.
	Disabled	Link Aggregation is disabled.
Port Members	Shows the list of target ports in the group.	

Available commands are listed below.

A	Add a port to a group member.	
		Press "A." The command prompt changes to "Enter trunk group number>." Enter a target group number with a value of 1 to 8. Then, the command prompt changes to "Enter port members for group x>." Enter a port number to be added. When entering multiple port numbers, delimit with comma with no space, or hyphenate the continuous numbers.
R	Delete a group.	
		Press "R." The command prompt changes to "Enter trunk group number>." Enter a target group number with a value of 1 to 8.
Q	Return to the previous menu.	

4.7.3. Port Monitoring Configuration Menu

On the Advanced Switch Configuration Menu, pressing "M" opens the Port Monitoring Configuration Menu, as shown in Fig. 4-7-7. To analyze communications, such as by protocol analyzer, in this Switching Hub, you can monitor packets between other ports that are normally filtered and cannot be monitored. On this screen, you can configure port monitoring settings.

```
PN28080K Local Management System
Advanced Switch Configuration -> Port Monitor Configuration Menu

Monitoring Port                        Be Monitored Port(s)
---------------    ------------------------------------------------------------
       1            2

Direction             Status
---------          -------------
  Both                Disabled


-------------------------------- <COMMAND> ----------------------------------
[S]et Monitoring Port
Set Ports to be [M]onitored
Set Traffic [D]irection
[C]hange Mirror Status
[Q]uit to previous menu




Command>
Enter the character in square brackets to select option
```

Fig. 4-7-7 Port Monitoring Configuration

Screen Description

Monitoring Port	Shows the destination port number of data to be monitored.	
Be Monitored Port(s)	Shows the target port number to be monitored.	
Direction	Shows the communication direction of target packet to be monitored.	
	Tx	Monitors a transmit packet.
	Rx	Monitors a receive packet.
	Both	Monitors both transmit and receive packets. (Factory default setting)
Status	Shows the status of port monitoring.	
	Enabled	Port monitoring is enabled.
	Disabled	Port monitoring is disabled. (Factory default setting)

Available commands are listed below.

S	Set a destination port of data to be monitored (port to which analyzer, etc. is connected).
	Press "S." The command prompt changes to "Enter port number>." Enter a target port number.
M	Set a port to be monitored.
	Press "M." The command prompt changes to "Enter port number>." Enter a target port number. When entering multiple port numbers, delimit with comma with no space, or hyphenate the continuous numbers.
D	Set a communication direction of target packet to be monitored.
	Press "D." The command prompt changes to "Select port monitoring direction (R/T/B)>." Enter "R" to monitor a receive packet. Enter "T" to monitor a transmit packet. Enter "B" to monitor both receive and transmit packets.
C	Set the status of port monitoring.
	Press "C." The command prompt changes to "Enter the select(E/D)>." Enter "E" to start monitoring. Enter "D" to stop monitoring.
Q	Return to the previous menu.

4.7.4. Access Control Configuration Menu

On the Advanced Switch Configuration Menu, pressing "A" opens the Access Control Configuration Menu, as shown in Fig. 4-7-8. On this screen, you can set Access Control.

```
PN28080K Local Management System
Advanced Switch Configuration -> Access Control Configuration Menu

[C]lassifier
[I]n-Profile Action
[O]ut-Profile Action
Port [L]ist
[P]olicy
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-7-8 Access Control Configuration

Screen Description

Classifier	Sets the classifier. (Maximum configurable number: 256)
In-Profile action	Sets the action against input packet. (Maximum configurable number: 81)
Out-Profile action	Sets the action against input packet exceeding a committed rate. (Maximum configurable number: 128)
Port list	Sets the list of applicable ports. (Maximum configurable number: 128)
Policy	Sets the policy. (Maximum configurable number: 128)
Quit to previous menu	Returns to the previous menu.

4.7.4.a. Classifier Configuration Menu

On the Access Control Configuration Menu, pressing "C" opens the Classifier Configuration Menu, as shown in Fig. 4-7-9. On this screen, you can set classifier.

```
PN28080K Local Management System
Access Control Configuration -> Classifier Configuration Menu
Multifield Classifier:                Total Entries : 1
Index  Src IP Addr/Mask   Dst IP Addr/Mask  DSCP Pro. Src L4 Port Dst L4 Port
-----  ----------------- ----------------- ---- ---- ---------- ----------
    1 Ignore            Ignore            Ign  Ign  Ignore     Ignore




--------------------------------- <COMMAND> -----------------------------------
[N]ext Page                           M[o]dify Classifier
[P]revious Page                       [M]ore Classifier Info.
[C]reate Classifier                   [S]how Detailed Entry Info.
[D]elete Classifier                   [Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-9 Classifier Configuration Menu

Screen Description

Total Entries	Shows the number of classifiers (number of indexes) created.
Index	Shows the classifier index number.
Src IP Addr/Mask	Shows the source IP address.
Dst IP Addr/Mask	Shows the destination IP address.
DSCP	Shows the priority information DSCP value.
Pro.	Shows the protocol.
Src L4 Port	Shows the source port number of TCP/UDP.
Dst L4 Port	Shows the destination port number of TCP/UDP.

Available commands are listed below.

N	Show the next page.	
		Press "N." The screen shows the next page.
P	Show the previous page.	
		Press "P." The screen shows the previous page.
C	Create a classifier.	
		Press "C." The Create Classifier Configuration Menu opens. For the Create Classifier Configuration Menu, refer to the next section (4.7.4.b).
D	Delete a classifier.	
		Press "D." The command prompt changes to "Please enter classifier index>." Enter an index of the classifier to be deleted with a value of 1 to 65535.
O	Modify classifier configuration.	
		Press "O." The Modify Classifier Menu opens. Set (modify) the configuration in the same as the Create Classifier Configuration Menu.
M	Show additional information on a classifier.	
		Press "M" to display information on source MAC address, destination MAC address, 802.1p, VLAN ID, TCP SYN Flag, and ICMP type.
S	Show detailed information on a classifier.	
		Press "S" to display information on source MAC address, destination MAC address, VLAN ID, source IP address, destination IP address, 802.1p priority, DSCP, protocol type, TCP/UDP source port number, TCP/UDP destination port number, TCP SYN Flag, and ICMP type.
Q	Return to the previous menu.	

Note: In this Switching Hub, the maximum number of L4 portlist which is available in src-port or dst-port is by 16.

4.7.4.b. Create Classifier Configuration Menu

On the Classifier Configuration Menu, pressing "C" opens the Create Classifier Configuration Menu, as shown in Fig. 4-7-10. On this screen, you can create a classifier.

```
PN28080K Local Management System
Classifier Configuration -> Create Classifier Configuration Menu
Classifier Index        :
VLAN ID :       802.1p Priority :       DSCP      :          IPv6 DSCP :
Protocol:       TCP SYN Flag    :       ICMP Type :
Source MAC Address      :                   Source MAC Mask Length     :
Destination MAC Address :                   Destination MAC Mask Length:
Source IP Address       :                   Source IP Mask Length      :
Destination IP Address  :                   Destination IP Mask Length :
Source IPv6 Address     :                                        PLen :
Destination IPv6 Address:                                        PLen :
Source Layer 4 Port     :                   Destination Layer 4 Port   :
------------------------------ <COMMAND> ----------------------------------
[C]lassifier Index                      S[o]urce IP Address
[S]ource MAC Address                    D[e]stination IP Address
[D]estination MAC Address               Source IPv[6] Address
[V]LAN ID                               Desti[n]ation IPv6 Address
802.1p Pr[i]ority                       So[u]rce Layer 4 Port
DSC[P]                                  Des[t]ination Layer 4 Port
P[r]otocol                              DSCP [F]or IPv6
TCP S[Y]N Flag                          [A]pply
IC[M]P Type                             [Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-10 Create Classifier Configuration Menu

Screen Description

Classifier Index	Shows the classifier index.
VLAN ID	Shows the VLAN ID.
802.1p Priority	Shows the priority of IEEE802.1p.
DSCP	Shows the DSCP value.
IPv6 DSCP	Shows the IPv6 DSCP value
Protocol	Shows the protocol type.
TCP SYN Flag	Shows whether a TCP SYN flag is set for filtering.
ICMP Type	Shows the ICMP type.
Source MAC Address	Shows the source MAC address.
Destination MAC Address	Shows the destination MAC address.
Source MAC Mask Length	Shows the length (bits) of source MAC address.
Destination MAC Mask Length	Shows the length (bits) of destination MAC address.
Source IP Address	Shows the source IP address.
Source IP Mask length	Shows the length (bits) of source address mask.
Destination IP Address	Shows the destination IP address.
Destination IP Mask length	Shows the length (bits) of destination address mask.
Source IPv6 Address	Shows the source IPv6 address.
PLen	Shows the length (bits) of source address mask.
Destination IPv6 Address	Shows the destination IPv6 address.
PLen	Shows the length (bits) of destination address mask.
Source L4 Port	Shows the source port number of TCP/UDP.
Destination L4 Port	Shows the destination port number of TCP/UDP.

Available commands are listed below.

C	Set a classifier index.	
		Press "C." The command prompt changes to "Enter Classifier Index>." Enter a classifier index with a value of 1 to 65535.
S	Set the source MAC address to be filtered.	
		Press "S." The command prompt changes to "Enter source MAC address>." Enter the source MAC address as xx:xx:xx:xx:xx:xx. Then, the command prompt changes to "Enter source MAC address mask length>." Enter the length (bits) of address mask.
D	Set a destination MAC address to be filtered.	
		Press "D." The command prompt changes to "Enter designation MAC address>." Enter the destination MAC address as xx:xx:xx:xx:xx:xx. Then, the command prompt changes to "Enter destination MAC address mask length>." Enter the length (bits) of address mask.
V	Set a VLAN ID to be filtered.	
		Press "V." The command prompt changes to "Enter VLAN ID>." Enter a VLAN ID with a value of 1 to 4094.
P	Set a DSCP value to be filtered.	
		Press "P." The command prompt changes to "Enter DSCP value (0-63)>." Enter a DSCP value of 0 to 63.
R	Set a protocol to be filtered.	
		Press "R." The command prompt changes to "Select protocol>." Press "1" for TCP, "2" for UDP, "3" for ICMP, "4" for IGMP, "5" for RSVP, and "6" for other protocols.
O	Set the source IP address to be filtered.	
		Press "O." The command prompt changes to "Enter source IP address>." Enter a source IP address. Then, the command prompt changes to "Enter source IP address mask length>." Enter a length (bits) of address mask.
E	Set a destination IP address to be filtered.	
		Press "E." The command prompt changes to "Enter destination IP address>." Enter a destination IP address. Then, the command prompt changes to "Enter destination IP address mask length>." Enter a length (bits) of address mask.
U	Set a TCP/UDP source port number to be filtered.	
		Press "U." The command prompt changes to "Choose single port or defined port range (S/D)>." Press "S" to assign one port. Then, the command prompt changes to "Enter source layer 4 port>." Enter the source port number. Press "D" to assign ports by a range. Then, the command prompt changes to "Enter starting source port>" and "Enter final source port>." Enter the starting and final source port numbers.
T	Set a TCP/UDP destination port number to be filtered.	
		Press "T." The command prompt changes to "Choose single port or defined port range (S/D)>." Press "S" to assign one port. Then, the command prompt changes to "Enter destination layer 4 port>." Enter the destination port number. Press "D" to assign ports by a range. Then, the command prompt changes to "Enter starting destination port>" and "Enter final destination port>." Enter the starting and final destination port numbers.
I	Set the IEEE802.1p priority to be filtered.	
		Press "I." The command prompt changes to "Enter 802.1p priority>." Enter the 802.1p priority with a value of 0 to 7.
M	Set an ICMP type to be filtered. (* Protocol needs to be set to ICMP.)	
		Press "M." The command prompt changes to "Enter ICMP type>." Enter an ICMP type with a value of 0 to 18.
Y	Set a TCP SYN flag to be filtered. (* Protocol needs to be set to TCP.)	
		Press "Y." The command prompt changes to "Set TCP SYN flag (Y/N)>." Press "Y" for filter with a TCP SYN flag. Press "Y" for no filtering or to remove filter. If filtered, True is displayed. If not filtered, False is displayed.
6	Set the source IPv6 address to be filtered.	

		Press "6." The command prompt changes to "Enter source IPv6 address>." Enter a source IPv6 address. Then, the command prompt changes to "Enter source IPv6 address mask length>." Enter a length (bits) of address mask.
N	Set a destination IPv6 address to be filtered.	
		Press "N." The command prompt changes to "Enter destination IPv6 address>." Enter a destination IPv6 address. Then, the command prompt changes to "Enter destination IPv6 address mask length>." Enter a length (bits) of address mask.
F	Set a IPv6 DSCP value to be filtered.	
		Press "F." The command prompt changes to "Enter DSCP6 value (0-63)>." Enter a DSCP value of 0 to 63.
A	Apply the setting. If not applied here, the setting will be discarded.	
Q	Return to the previous menu.	

4.7.4.c. Classifier Configuration Menu

On the Classifier Configuration Menu, pressing "M" opens the More Classifier Information screen, as shown in Fig. 4-7-11 and Fig. 4-7-12. On this screen, you can refer to classifier information.

```
PN28080K Local Management System
Access Control Configuration -> Classifier Configuration Menu
Multifield Classifier:                Total Entries : 1
Index Source MAC Addr./ Mask   Destination MAC Addr./ Mask
----- ----------------------- ------------------------------------------------

    1 00:00:00:00:00:01/48     00:00:00:00:00:02/48

Press any key to continue...
```

Fig. 4-7-11 Classifier Configuration Menu 1

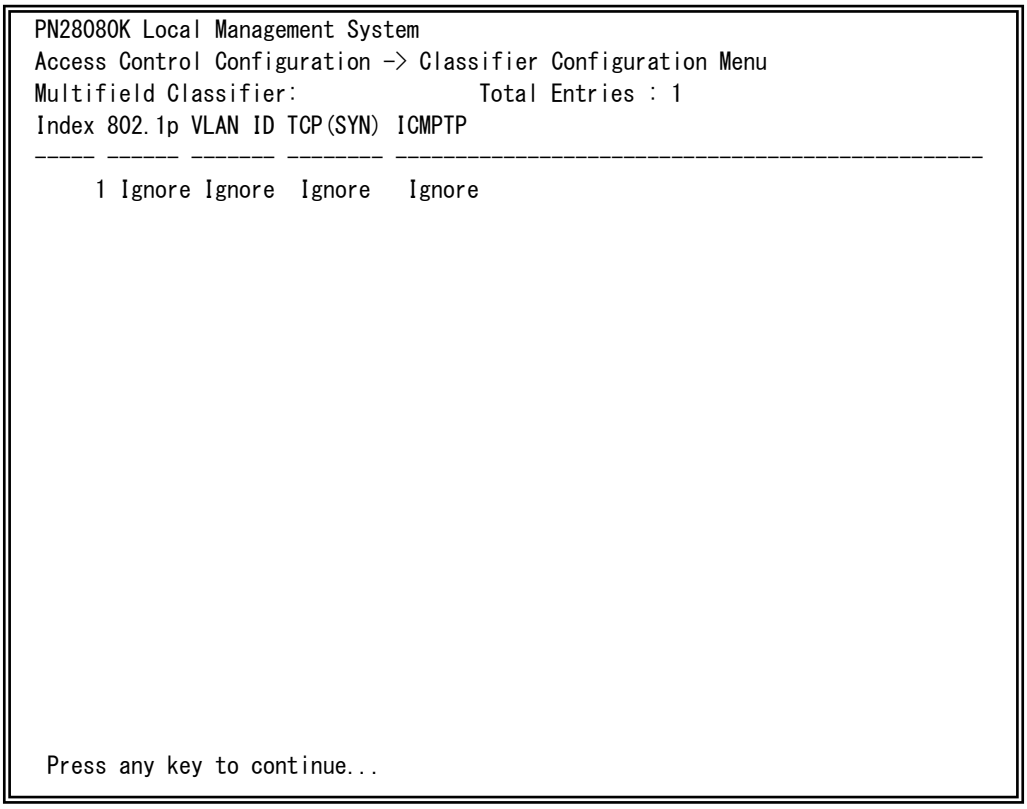


Fig. 4-7-12 Classifier Configuration Menu 2

Screen Description

Total Entries	Shows the number of classifiers (number of indexes) created.
Classifier Index	Shows the classifier index.
Source MAC Address	Shows the source MAC address.
Destination MAC Address	Shows the destination MAC address.
802.1p Priority	Shows the priority of IEEE802.1p.
VLAN ID	Shows the VLAN ID.
TCP SYN Flag	Shows whether a TCP SYN flag is set for filtering.
ICMP Type	Shows the ICMP type.

4.7.4.d. Show Detailed Entries Information Menu

On the Classifier Configuration Menu, pressing "S" opens the Show Detailed Entries Information Menu, as shown in Fig. 4-7-13. On this screen, you can refer to detailed classifier information. Classifier needs to be created before reference.

```
PN28080K Local Management System
Classifier Configuration -> Show Detailed Entry Information Menu
Detailed Classifier Information :
--------------------------------
Classifier Index                    :  1
Source MAC Address                  :  Ignore
Source MAC Address Mask Length      :  Ignore
Destination MAC Address             :  Ignore
Destination MAC Address Mask Length :  Ignore
802.1p Priority                     :  Ignore  VLAN ID         :  Ignore
Source IP Address                   :  Ignore
Source IP Address Mask Length       :  Ignore
Destination IP Address              :  Ignore
Destination IP Address Mask Length  :  Ignore
DSCP                                :  Ignore  IPv6 DSCP       :  Ignore
Protocol                            :  Ignore
Source Layer 4 Port                 :  Ignore
Destination Layer 4 Port            :  Ignore
TCP SYN Flag                        :  Ignore  ICMP Type       :  Ignore
Source IPv6 Address                 :  Ignore
Source IPv6 Address PLen            :  Ignore
Destination IPv6 Address            :  Ignore
Destination IPv6 Address PLen       :  Ignore
Press any key to continue...
```

Fig. 4-7-13 Show Detailed Entries Information Menu

Screen Description

Classifier Index	Shows the classifier index.
Source MAC Address	Shows the source MAC address.
Source Mask length	Shows the length (bits) of source address mask.
Destination MAC Address	Shows the destination MAC address.
Destination Mask length	Shows the length (bits) of destination address mask.
VLAN ID	Shows the VLAN ID.
DSCP	Shows the DSCP value.
DSCP6	Shows the IPv6 DSCP value.
Protocol	Shows the protocol type.
Source IP Address	Shows the source IP address.
Source IP Mask length	Shows the length (bits) of source address mask.
Destination IP Address	Shows the destination IP address.
Destination IP Mask length	Shows the length (bits) of destination address mask.
Source L4 Port	Shows the source port number of TCP/UDP.
Destination L4 Port	Shows the destination port number of TCP/UDP.
802.1p Priority	Shows the priority of IEEE802.1p.
TCP SYN Flag	Shows whether a TCP SYN flag is set for filtering.
ICMP Type	Shows the ICMP type.
Source IPv6 Address	Shows the source IPv6 address.
PLen	Shows the length (bits) of source address mask.
Destination IPv6 Address	Shows the destination IPv6 address.
PLen	Shows the length (bits) of destination address mask.

4.7.4.e. In-Profile Action Configuration Menu

On the Access Control Configuration Menu, pressing "I" opens the In-Profile Action Configuration Menu, as shown in Fig. 4-7-14. On this screen, you can configure in-profile setting.

```
PN28080K Local Management System
Access Control Configuration -> In-Profile Action Configuration Menu
In-Profile Action:        Total Entries : 0
Index  Deny/Permit  Policed-DSCP   Policed-Precedence  Policed-CoS
-----  -----------  -------------  ------------------  -----------









--------------------------------- <COMMAND> -----------------------------------
[N]ext Page                             [D]elete In-Profile Action
[P]revious Page                         [M]odify In-Profile Action
[C]reate In-Profile Action              [Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-14 In-Profile Action Configuration Menu

Screen Description

Total Entries	Shows the number of in-profiles (number of indexes) created.	
Index	Shows the in-profile index number.	
Deny/Permit	Shows whether a packet is denied or permitted.	
Action	Shows the execution mode in in-profile.	
	Policed-DSCP	Marks the DSCP value.
	Policed-Precedence	Marks the precedence value.
	Policed-CoS	Marks the CoS value.

Available commands are listed below.

N	Show the next page.		
		Press "N." The screen shows the next page.	
P	Show the previous page.		
		Press "P." The screen shows the previous page.	
C	Create in-profile.		
	Press "C." The Create In-Profile Action Menu opens. Refer to the next section (4.7.4.f).		
		Policed-DSCP	Mark the DSCP value.
		Policed-Precedence	Mark the precedence value.
		Policed-CoS	Mark the CoS value.
D	Delete in-profile.		
		Press "D." The command prompt changes to "Enter in-profile action index>." Enter an index number of the in-profile to be deleted.	
M	Modify in-profile.		
		Enter "M." The command prompt changes to "Enter in-profile action index>." Enter an index number of the in-profile to be modified, and modify it using the same operation as that for creating in-profile.	
Q	Return to the previous menu.		

Note: 1. Can set only one of the marking actions in In-Profile.
2. Can set precedence only in the case of IPv6.

4.7.4.f. Create In-profile Action Menu

On the In-Profile Action Configuration screen, pressing "C" opens the Create In-Profile Action Menu, as shown in Fig. 4-7-15. On this screen, you can create in-profile action.

```
PN28080K Local Management System
In-Profile Action Configuration -> Create In-Profile Action Menu
Index             : 1
Deny/Permit       : Permit
Policed-DSCP      : Ignore
Policed-Precedence: Ignore
Policed-CoS       : Ignore









-------------------------------- <COMMAND> -----------------------------------
In-Profile Action [I]ndex              Set Policed-[C]oS
Set [D]eny/Permit                      [A]pply
Set Policed-D[S]CP                     [Q]uit to previous menu
Set Policed-[P]recedence


Command>
Enter the character in square brackets to select option
```

Fig. 4-7-15 Create In-Profile Action Menu

Screen Description

Index	Shows the in-profile index number.	
Deny/Permit	Shows whether a packet is denied or permitted.	
Action	Policed-DSCP	Marks the DSCP value.
	Policed-Precedence	Marks the precedence value.
	Policed-CoS	Marks the CoS value.

Available commands are listed below.

I	Set an in-profile index number.	
		Press "I." The command prompt changes to "Enter in-profile action index>." Enter an index number with a value of 1 to 65535.
D	Deny/permit packets.	
		Press "D." The command prompt changes to "Select Deny/Permit (1-2)>." Press "1" to deny packets. Press "2" to permit them.
S	Set a DSCP value to be marked.	
		Press "S." The command prompt changes to "Enter DSCP value>." Enter a DSCP value of 0 to 63.
P	Set a precedence value to be marked.	
		Press "P." The command prompt changes to "Enter ToS precedence value>." Enter a precedence value of 0 to 7.
C	Set a CoS value to be marked.	
		Press "C." The command prompt changes to "Enter CoS value>." Enter a CoS value of 0 to 7.
A	Apply the setting. If not applied here, the setting will be discarded.	
Q	Return to the previous menu.	

4.7.4.g. Out-Profile Action Configuration Menu

On the Access Control Configuration Menu, pressing "O" opens the Out-Profile Action Configuration Menu, as shown in Fig. 4-7-16. On this screen, you can configure out-profile setting.

```
PN28080K Local Management System
Access Control Configuration -> Out-Profile Action Configuration Menu
Out-Profile Action:        Total Entries :0
Index    Committed Rate    Burst Size(KB)   Deny/Permit   Policed-DSCP
-----    ----------------  --------------   -----------   ------------









Note: Committed Rate - 1Mbps/unit, Max available rate 10/100:100, Giga:1000
-------------------------------- <COMMAND> ----------------------------------
[N]ext Page                              [D]elete Out-Profile Action
[P]revious Page                          [M]odify Out-Profile Action
[C]reate Out-Profile Action              [Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-16 Out-Profile Action Configuration Menu

Screen Description

Total Entries	Shows the number of out-profiles (number of indexes) created.
Index	Shows the out-profile index number.
Committed Rate	Shows the packet buffer rate.
Burst Size(KB)	Shows the traffic burst size that can be transmitted exceeding the committed rate. For burst size, 4K, 8K, 16K, 32K, and 64K are used.
Deny/Permit	Shows whether a packet is denied or permitted.
Policed-DSCP	Shows a DSCP value to be marked.

Available commands are listed below.

N	Show the next page.	
		Press "N." The screen shows the next page.
P	Show the previous page.	
		Press "P." The screen shows the previous page.
C	Create out-profile.	
		Press "C." The Create Out-Profile Action Menu opens. Refer to the next section (4.7.4.h).
D	Delete out-profile.	
		Press "D." The command prompt changes to "Enter out-profile action Index>." Enter an Index number of the out-profile to be deleted.
M	Modify out-profile.	
		Enter "M." The command prompt changes to "Enter out-profile action Index>." Enter an index number of the out-profile to be modified, and modify it using the same operation as that for creating out-profile.
Q	Return to the previous menu.	

Note: 1. Burst size is 64KB only. It cannot be changed.
2. Out-profile action support deny only.

4.7.4.h. Create Out-profile Action Menu

On the Out-Profile Action Configuration screen, pressing "C" opens the Create Out-Profile Action Menu, as shown in Fig. 4-7-17. On this screen, you can create out-profile action.

```
PN28080K Local Management System
Out-Profile Action Configuration -> Create Out-Profile Action Menu
Index              :
Deny/Permit        : Deny
Committed Rate     : 1
Burst Size         : 64KB









Note: Deny/Permit - deny only. Burst Size - 64KB only.
-------------------------------- <COMMAND> ----------------------------------
Out-Profile Action [I]ndex              [A]pply
Set [C]ommitted Rate                    [Q]uit to previous menu




Command>
Enter the character in square brackets to select option
```

Fig. 4-7-17 Create Out-profile Action Menu

Screen Description

Index	Shows the out-profile index number.
Deny/Permit	Shows whether a packet is denied or permitted.
Committed Rate	Shows the packet buffer rate.
Burst Size(KB)	Shows the traffic burst size that can be transmitted exceeding the committed rate. Burst size is fixed to 64K.

Available commands are listed below.

I	Set an out-profile index number.	
		Press "I." The command prompt changes to "Enter Out-Profile action index>." Enter an index number with a value of 1 to 65535.
C	Set the committed rate.	
		Press "C." The command prompt changes to "Enter committed rate>." Enter the committed rate with a value of 1 to 1000.
A	Apply the setting. If not applied here, the setting will be discarded.	
Q	Return to the previous menu.	

4.7.4.i. Port List Configuration Menu

On the Access Control Configuration Menu, pressing "L" opens the Port List Configuration Menu, as shown in Fig. 4-7-18. On this screen, you can set a port list to apply Access Control.
When using both Access Control and Link Aggregation functions, assign a practical physical port number, not a logical port created in Link Aggregation.

```
PN28080K Local Management System
Access Control Configuration -> Port List Configuration Menu
Port List:        Total Entries : 0
Index       Port List
-----     -----------------------------------------------------------------

















-------------------------------- <COMMAND> ----------------------------------
[N]ext Page                              [D]elete Port List
[P]revious Page                          [M]odify Port List
[C]reate Port List                       [Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-18 Port List Configuration Menu

Screen Description

Total Entries	Shows the number of port lists (number of indexes) created.
Index	Shows the port list index number.
Port List	Shows the port number in the port list.

Available commands are listed below.

N	Show the next page.	
		Press "N." The screen shows the next page.
P	Show the previous page.	
		Press "P." The screen shows the previous page.
C	Create a port list.	
		Press "C." The command prompt changes to "Enter port list index>." Enter an index number to be created. Then, the command prompt changes to "Enter port number>." Enter a port number to be included in the list.
D	Delete a port list.	
		Press "D." The command prompt changes to "Enter port list index>." Enter an index number of the port list to be deleted.
M	Modify a port list.	
		Enter "M." The command prompt changes to "Enter port list index>." Enter an index number of the port list to be modified, and modify it using the same operation as that for creating a port list.
Q	Return to the previous menu.	

4.7.4.j. Policy Configuration Menu

On the Access Control Configuration Menu, pressing "P" opens the Policy Configuration Menu, as shown in Fig. 4-7-19. On this screen, you can configure the policy settings.

```
PN28080K Local Management System
Access Control Configuration -> Policy Configuration Menu
Policy :                                    Total Entries : 0
Index Classifier Seq.  In-Profile Out-Profile PortList Status
----- ---------- ----- ---------- ---------- -------- --------









-------------------------------- <COMMAND> ----------------------------------
[N]ext Page                          [S]how Policy Entry
[P]revious Page                      [U]pdate Policy
[C]reate Policy                      Display Sequence [B]y Port
[D]elete Policy                      [Q]uit to previous menu
[E]nable or Disable Policy
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-19 Policy Configuration Menu

Screen Description

Total Entries	Shows the number of policies (number of indexes) created.
Index	Shows the policy index number.
Classifier	Shows the classifier index number.
Seq.	Shows the sequence number indicating the application order of policies. Policies are applied in ascending order of this sequence number.
In-Profile	Shows the in-profile index number.
Out-Profile	Shows the out-profile index number.
Port List	Shows the port list index number.
Status	Shows the application status of policy.

Available commands are listed below.

N	Show the next page.		
		Press "N." The screen shows the next page.	
P	Show the previous page.		
		Press "P." The screen shows the previous page.	
C	Create a policy.		
		Press "C." The Create Policy Configuration Menu opens. For the Create Policy Configuration Menu, refer to the next section (4.7.4.k).	
D	Delete a policy.		
		Press "D." The command prompt changes to "Enter a policy index>." Enter a policy index number to be deleted. Then the command prompt changes to "Are you sure to delete policy index xx (Y/N)>." Press "Y" to delete the policy. Press "N" to cancel the deletion.	
E	Enable/disable the policy status.		
		Press "E." The command prompt changes to "Select policy index>." Enter a policy index number to be enabled/disabled. Then, the command prompt changes to "Enable or Disable Policy Entry>." Press "E" to enable the policy. Press "D" to disable it.	
		Enabled	Enable a policy.
		Disabled	Disable a policy.
S	Show the policy information.		
		Press "S " to display detailed information on each policy.	
U	Modify a policy.		
		Press "U." The command prompt changes to "Enter policy index>." Enter an index number to be modified. Then, carry out the same operation as that for creating a policy. Remember that modification is rejected if the policy is enabled. If enabled, disable the policy and then modify it.	
B	Show a sequence number of policy applied to each port.		
		Press "B." The command prompt changes to "Enter port number>." Enter a port number to display. Then, the command prompt changes to "Select policy index order or policy sequence order (I/S)>." Press "I" to confirm a policy sequence corresponding to the policy index. Press "S" to confirm a policy index sequence corresponding to the policy sequence.	
Q	Return to the previous menu.		

4.7.4.k. Create Policy Configuration Menu

On the Policy Configuration Menu, pressing "C" opens the Create Policy Configuration Menu, as shown in Fig. 4-7-20. On this screen, you can create a policy.

```
PN28080K Local Management System
Policy Configuration -> Create Policy Configuration Menu
Policy Index             :
Classifier Index         :
Policy Sequence          :
In-Profile Action Index  :
Out-Profile Action Index :
Port List Index          :









-------------------------------- <COMMAND> -----------------------------------
Set [P]olicy Index                      Select Port [L]ist Index
Select [C]lassifier Index               [A]pply Policy
Set Policy [S]equence                   [Q]uit to previous menu
Select [I]n-Profile Action Index
Select [O]ut-Profile Action Index
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-20 Create Policy Configuration Menu

Screen Description

Policy Index	Shows the policy index number.
Classifier Index	Shows the classifier index number created in the Classifier Configuration Menu.
Policy Sequence	Shows the sequence number.
In-Profile Index	Shows the in-profile index number created in the In-Profile Action Configuration Menu.
Out-Profile Index	Shows the out-profile index number created in the Out-Profile Action Configuration Menu.
Port List Index	Shows the port list index number created in the Port List Configuration Menu.

Available commands are listed below.

P	Set a policy index number.	
		Press "P." The command prompt changes to "Enter policy index>." Enter a policy index number.
C	Set an index number of applicable classifier.	
		Press "C." The command prompt changes to "Enter classifier index>." Enter an index number of applicable classifier.
S	Set a sequence number.	
		Press "S." The command prompt changes to "Enter policy sequence>." Enter a sequence number.
I	Set an index number of applicable in-profile.	
		Press "I." The command prompt changes to "Enter in-profile index>." Enter an index number of applicable in-profile.
O	Set an index number of applicable out-profile.	
		Press "O." The command prompt changes to "Enter out-profile index>." Enter an index number of applicable out-profile. (Out-profile can be omitted.)
L	Set an index number of applicable port list.	
		Press "L." The command prompt changes to "Enter port list index>." Enter an index number of applicable port list.
A	Apply the setting. If you press "Q" without applying the setting, it will be discarded.	
Q	Return to the previous menu.	

4.7.5 Quality of Service Configuration

On the Advanced Switch Configuration Menu, pressing "S" opens the Quality of Service Configuration Menu, as shown in Fig. 4-7-21. You can configure the QoS (Quality of Service) setting of the Switching Hub.

```
PN28080K Local Management System
Main Menu -> Quality of Service Configuration Menu

[T]raffic Class Configuration
[E]gress Rate Limiting
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-7-21 QoS Configuration

Available commands are listed below.

T	Go to the configuration screen for traffic class.	
		Press "T." The Traffic Class Configuration Menu opens. For configuration details, refer to 4.7.5.a.
E	Go to the configuration screen for bandwidth.	
		Press "E." The Egress Rate Limiting Configuration Menu opens. For configuration details, refer to 4.7.5.b.
Q	Return to the previous menu.	

4.7.5.a. Traffic Class Configuration Menu

On the Quality of Service Configuration Menu, pressing "T" opens the Traffic Class Configuration screen, as shown in Fig. 4-7-22. On this screen, you can configure the traffic class setting.

```
PN28080K Local Management System
Quality of Service Configuration -> Traffic Class Configuration Menu

QoS Status: Disabled

Priority    Traffic Class
--------    -------------
   0              0
   1              0
   2              1
   3              1
   4              2
   5              2
   6              3                        0: Lowest
   7              3                        7: Highest

------------------------------- <COMMAND> ----------------------------------
[S]et QoS Status
Set Priority-Traffic Class [M]apping
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-7-22 Traffic Class Configuration Menu

Screen Description

QoS Status	Shows the status of QoS function using IEEE802.1p.	
	Enabled	QoS is enabled.
	Disabled	QoS is disabled. (Factory default setting)
Priority	Shows the priority value in a VLAN tag.	
Traffic Class	Shows the QoS priority level.	

Available commands are listed below.

S	Set the status of QoS function.	
	Press "S." The command prompt changes to "Enable or Disable QoS (E/D)>." Press "E" to enable the function. Press "D" to disable it.	
M	Assign a priority level (traffic class) to a priority value of IEEE802.1p.	
	Press "M." The command prompt changes to "Enter Priority (E/D)>." Enter a priority value (0 to 7) to be assigned. Then, the command prompt changes to "Enter traffic class for priority #>." Enter a priority level (traffic class) to be controlled by this Switching Hub with a value of 0 to 3.	
Q	Return to the previous menu.	

4.7.5.b. Egress Rate Limiting Configuration Menu

On the Quality of Service Configuration Menu, pressing "C" opens the Egress Rate Limiting Configuration Menu, as shown in Fig. 4-7-23. On this screen, you can set bandwidth control.

```
PN28080K Local Management System
Quality of Service Configuration -> Egress Rate Limiting Configuration Menu
Port   Bandwidth    Status
----  -----------  --------
  1       1000     Disabled
  2       1000     Disabled
  3       1000     Disabled
  4       1000     Disabled
  5       1000     Disabled
  6       1000     Disabled
  7       1000     Disabled
  8       1000     Disabled
  9       1000     Disabled



Note: Bandwidth - 1Mbps/unit
--------------------------------- <COMMAND> ----------------------------------
Set [B]andwidth        Set [S]tatus
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-7-23 Egress Rate Limiting Configuration Menu

Screen Description

Port	Shows the port number.	
Bandwidth	Shows the bandwidth. The factory default setting is 1000. (Unit is Mbps.)	
Status	Enables/disables the bandwidth control.	
	Enabled	Bandwidth control is enabled.
	Disabled	Bandwidth control is disabled.

Available commands are listed below.

N	Show the next page.	
		Press "N." The screen shows the next page.
P	Show the previous page.	
		Press "P." The screen shows the previous page.
B	Set a bandwidth.	
		Press "B." The command prompt changes to "Enter port number e.g.: 1, 3, 5-9>." Enter a port number to designate. Then, the command prompt changes to "Enter bandwidth>." Enter a value between 1 and 1000.
S	Set the bandwidth control.	
		Press "S." The command prompt changes to "Enter port number e.g.: 1, 3, 5-9>." Enter a port number to designate. Then, the command prompt changes to "Enable or Disable Status (E/D)>." Press "E" to enable the bandwidth control. Press "D" to disable it.
Q	Return to the previous menu.	

4.7.6. Storm Control Configuration Menu

On the Advanced Switch Configuration Menu, pressing "o" opens the Storm Control Configuration Menu, as shown in Fig. 4-7-24. You can set the storm control for unknown unicast, broadcast, and multicast traffic.

```
PN28080K Local Management System
Advanced Switch Configuration -> Storm Control Configuration Menu

Port Storm Control Setting:
 No.      DLF      Broadcast   Multicast   Threshold(pps)
----   ---------   ---------   ---------   --------------
  1    Disabled    Disabled    Disabled     0
  2    Disabled    Disabled    Disabled     0
  3    Disabled    Disabled    Disabled     0
  4    Disabled    Disabled    Disabled     0
  5    Disabled    Disabled    Disabled     0
  6    Disabled    Disabled    Disabled     0
  7    Disabled    Disabled    Disabled     0
  8    Disabled    Disabled    Disabled     0
  9    Disabled    Disabled    Disabled     0




-------------------------------- <COMMAND> ---------------------------------
Set [D]LF Status          [Q]uit to previous menu
Set [T]hreshold Value     Set [B]roadcast Status
Set [M]ulticast Status
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-24 Storm Control Configuration Menu

Screen Description

DLF	Shows the storm control setting for unknown unicast traffic.	
	Enabled	Storm control for unknown unicast is enabled.
	Disabled	Storm control for unknown unicast is disabled. (Factory default setting)
Broadcast	Shows the storm control setting for broadcast traffic.	
	Enabled	Storm control for broadcast is enabled.
	Disabled	Storm control for broadcast is disabled. (Factory default setting)
Multicast	Shows the storm control setting for multicast traffic.	
	Enabled	Storm control for multicast is enabled.
	Disabled	Storm control for multicast is disabled. (Factory default setting)
Threshold	Shows the threshold number of packets (Packet Per Second).	

Available commands are listed below.

D	Enable/disable the storm control for unknown unicast traffic.	
		Press "D." The command prompt changes to "Enter port number>." Enter a port number to designate. Then, the command prompt changes to "Enable or Disable DLF storm control status>." Press "E" to enable the unknown unicast control. Press "D" to disable it.
B	Enable/disable the storm control for broadcast traffic.	
		Press "B." The command prompt changes to "Enter port number>." Enter a port number to designate. Then, the command prompt changes to "Enable or Disable broadcast storm control status (E/D)>." Press "E" to enable the broadcast control. Press "D" to disable it.
M	Enable/disable the storm control for multicast traffic.	
		Press "M." The command prompt changes to "Enter port number>." Enter a port number to designate. Then, the command prompt changes to "Enable or Disable multicast storm control status (E/D)>." Press "E" to enable the multicast control. Press "D" to disable it.
T	Set the threshold number of packets (Packet Per Second).	
		Press "T." The command prompt changes to "Enter port number>." Enter a port number to designate. Then, the command prompt changes to "Enter threshold value>." Enter the threshold number of packets (packet per second) between 0 and 262143.
Q	Return to the previous menu.	

4.7.7. Authentication Status Configuration

On the Advanced Switch Configuration Menu, pressing "t" opens the Authentication Configuration screen, as shown in Fig. 4-7-25. On this screen, you can configure the IEEE 802.1X compatible port-based access control, MAC address-based access control, MAC authentication, and WEB authentication.

```
PN28080K Local Management System
Advanced Switch Configuration -> Authentication Configuration Menu

[A]uthentication Status Table
Authentication [L]og
[G]lobal Authentication Configuration
Local [U]ser Database Configuration
Local MA[C] Authentication Database Configuration
802.1[X] Access Control Configuration
[M]AC Authentication Configuration
[W]EB Authentication Configuration
Dynamic [V]LAN Configuration
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25 Authentication Status Configuration

Screen Description

Authentication Status Table	Displays the authentication status table.
Authentication Log	Displays the authentication log.
Global Authentication Configuration	Configures the common authentication settings.
Local User Database Configuration	Moves to the local user database configuration used in 802.1X access control or WEB authentication.
Local MAC Authentication Database Configuration	Moves to the local MAC database configuration used in MAC authentication.
802.1X Access Control Configuration	Moves to the IEEE802.1X access control configuration.
MAC Authentication Configuration	Moves to the MAC authentication configuration.
WEB Authentication Configuration	Moves to the WEB authentication configuration.
Dynamic VLAN Configuration	Moves to the dynamic VLAN configuration.
Quit to previous menu	Returns to the Advanced Switch Configuration Menu.

4.7.7.a. Authentication Status Table

On the Authentication Configuration, pressing "a" opens the Authentication Status Table screen, as shown in Fig. 4-7-25-1. On this screen, you can display the authentication status for each connected host.

```
PN28080K Local Management System
Authentication Configuration -> Authentication Status Table

Total Hosts      : 0
Authorized Hosts : 0
Auth Aging Time  : 1440 minutes

MAC Address        Port  Auth Type   Auth Status      Remaining Aging Time
-----------------  ----  ----------  ---------------  --------------------









--------------------------------- <COMMAND> -----------------------------------
[N]ext Page                  [D]elete Host            Auth [A]ging Time
[P]revious Page              [S]ort by MAC/Port
[Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-1 Authentication Status Table

Screen Description

Total Hosts	Displays the total number of hosts registered in the authentication status table. The maximum number is 1024.	
Authorized Hosts	Displays the number of authorized hosts.	
Auth Aging Time	Displays the authentication aging time in minutes. (Factory default setting: 1440)	
MAC Address	Displays the MAC address of the terminal to be authenticated.	
Port	Displays the port number to which the terminal is connected.	
Auth Type	Displays the authentication type. If Auth Status is Authorized, the authentication type when authentication succeeded is displayed. If Unauthorized, the authentication type when authentication is on standby is displayed.	
	802.1X	The authentication type is 802.1X access control.
	MAC	The authentication type is MAC authentication.
	WEB	The authentication type is WEB authentication.
	1X/MAC	The authentication type is 802.1X access control or MAC authentication.
	1X/WEB	The authentication type is 802.1X access control or WEB authentication.
	1X/MAC/WEB	The authentication type is 802.1X access control, MAC authentication, or WEB authentication.
	MAC/WEB	The authentication type is MAC authentication or WEB authentication.
Auth Status	Displays the authentication status.	
	Authorized	Authentication is authorized.
	Unauthorized	Authentication is not authorized. Communication in this state is limited in the guest VLAN.
Remaining Aging Time	Displays the remaining time (minutes) before re-authentication. If the remaining time is 0, Auth Status becomes Unauthorized, executing the authentication process again.	

Available commands are listed below.

N	Display the next page.	
		Press "N" to display the next page.
P	Display the previous page.	
		Press "P" to display to the previous page.
D	Delete a host from the authentication status table and deauthorize it.	
		Press "D." The command prompt changes to "MAC Address (XX:XX:XX:XX:XX:XX)>." Enter the MAC address of a host to be deleted.
A	Configure the authentication aging time.	
		Press "A." The command prompt changes to "Enter auth aging time >." Enter an integer number between 1 and 65535 (seconds). To disable the aging, enter 0.
S	Change the display order of the authentication status table.	
		Press "S." The command prompt changes to "Select the order type (M/P)>." Press "M" to display in the order of MAC address or "P" to display in the order of port number.
Q	Return to the parent menu.	

4.7.7.b. Authentication Log

On the Authentication Configuration, pressing "L" opens the Authentication Log screen, as shown in Fig. 4-7-25-2. On this screen, you can display the authentication log of an event that occurred in the authentication process.

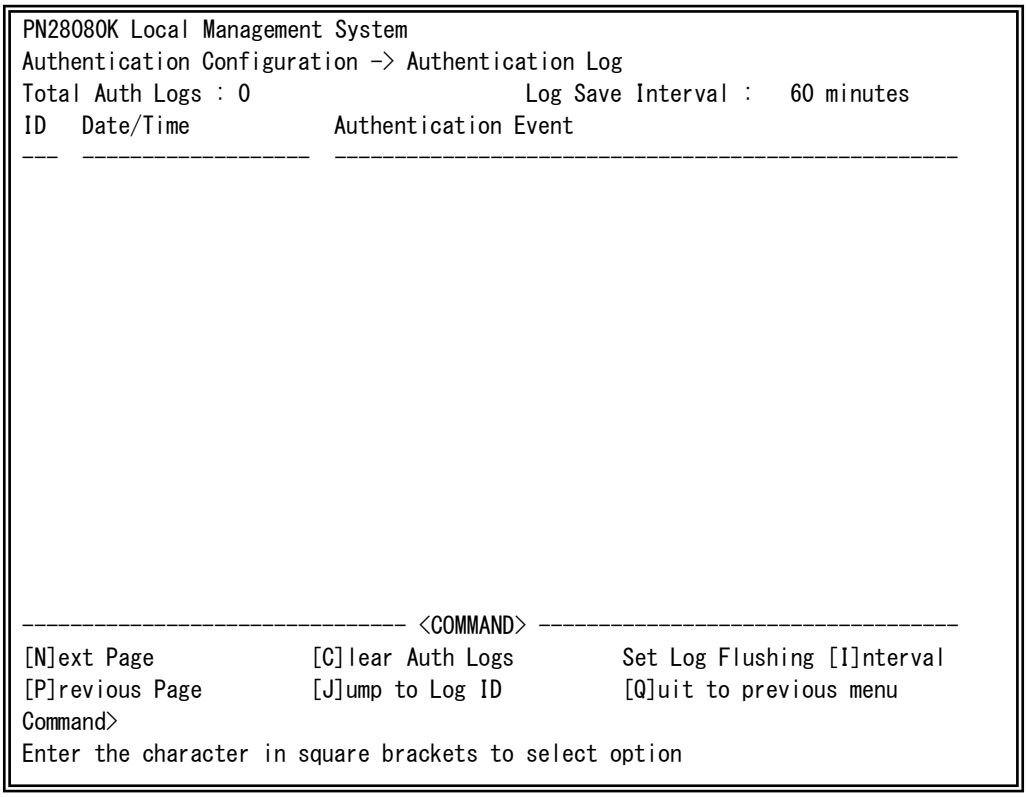


Fig. 4-7-25-2 Authentication Log

Screen Description

Total Auth Logs	Displays the total number of authentication events recorded in the authentication status table. The maximum number is 512.
Log Save Interval	Displays the waiting time in minutes until an authentication log that occurred is written to the switch. If the switch is restarted or turned off when no log is being written, an authentication log that has been recorded at that point is flushed. (Factory default setting: 60)
ID	Displays the authentication log IDs in ascending order.
Date/Time	Displays the date and time when the authentication event occurred.
Authentication Event	Displays the authentication event.

Available commands are listed below.

N	Display the next page.
	Press "N" to display the next page.
P	Display the previous page.
	Press "P" to display to the previous page.
C	Delete an authentication log.
J	Display an authentication log with the specified ID.
	Press "J." The command prompt changes to "Select log ID >." Enter an integer number between 1 and 512. Entering 0 moves to the latest authentication log.
I	Set the waiting time until an authentication log is written to the switch.
	Press "I." The command prompt changes to "Enter log flush interval in minutes >." Enter an integer number between 1 and 1440.
Q	Return to the parent menu.

The authentication events are described below.

Authentication event	Severity	Overview
[MAC](RADIUS)Authorized XX:XX:XX:XX:XX:XX on Port xx to VLAN xxxx	info	The terminal connected to a specific port succeeded in MAC authentication using the RADIUS or local database and was assigned to a specific VLAN, or it failed in authentication.
[MAC](Local)Authorized XX:XX:XX:XX:XX:XX on Port xx to VLAN xxxx	info	
[MAC](RADIUS)Rejected XX:XX:XX:XX:XX:XX on Port xx	notice	
[MAC](Local)Rejected XX:XX:XX:XX:XX:XX on Port xx	notice	
[WEB](RADIUS)Authorized user xxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx to VLAN xxxx	info	The terminal connected to a specific port succeeded in WEB authentication using the RADIUS or local database and was assigned to a specific VLAN or, it failed in authentication.
[WEB](Local)Authorized user xxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx to VLAN xxxx	info	
[WEB](RADIUS)Rejected user xxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx	notice	
[WEB](Local)Rejected user xxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx	notice	
[802.1X](RADIUS)Authorized user xxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx to VLAN xxxx	info	The terminal connected to a specific port succeeded in IEEE802.1X access control using the RADIUS or local database and was assigned to a specific VLAN, or it failed in authentication.
[802.1X](RADIUS)Rejected user xxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx	notice	
[802.1X](Local)Authorized user	info	

xxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx to VLAN xxxx		
[802.1X](Local)Rejected user xxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx	notice	
[MAC]Rejected XX:XX:XX:XX:XX:XX on Port xx (auth table was full)	notice	Authentication of a new terminal was rejected because the number of hosts registered in the authentication status table has reached the limit.
[WEB]Rejected XX:XX:XX:XX:XX:XX on Port xx (auth table was full)	notice	
[802.1X]Rejected XX:XX:XX:XX:XX:XX on Port xx (auth table was full)	notice	

4.7.7.c. Global Authentication Configuration

On the Authentication Configuration, pressing "G" opens the Global Authentication Configuration screen, as shown in Fig. 4-7-25-3. On this screen, you can configure the authentication function operations.

```
PN28080K Local Management System
Authentication Configuration -> Global Authentication Configuration Menu

Global MAC Auth Status : Disabled        Global WEB Auth Status : Disabled

802.1X Port-based Auth Ports : 1-8
802.1X MAC-based Auth Ports  :
MAC Auth Ports               :
WEB Auth Ports               :









-------------------------------- <COMMAND> ----------------------------------
Set Global [M]AC Auth Status             Set Global [W]EB Auth Status
Set 802.1X [P]ort-based Auth Ports       Set 802.1X M[A]C-based Auth Ports
Set MA[C] Auth Ports                     Set W[E]B Auth Ports

[Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-3 Global Authentication Configuration

Screen Description

Global MAC Auth Status	Displays the MAC authentication operation status of the entire device.	
	Enabled	MAC authentication is enabled.
	Disabled	MAC authentication is disabled. (Factory default setting)
Global WEB Auth Status	Displays the WEB authentication operation status of the entire device.	
	Enabled	WEB authentication is enabled.
	Disabled	WEB authentication is disabled. (Factory default setting)
802.1X Port-based Auth Ports	Displays ports with IEEE802.1X port-based access control enabled. Access control is enabled for all ports in the factory default.	
802.1X MAC-based Auth Ports	Displays ports with IEEE802.1X MAC-based access control enabled.	
MAC Auth Ports	Displays ports with MAC authentication enabled.	
WEB Auth Ports	Displays ports with WEB authentication enabled.	

Available commands are listed below.

M	Configure the MAC authentication status settings of the entire device.	
		Press "M." The command prompt changes to "Enable or Disable global MAC auth status (E/D)>." Press "E" to enable the status or "D" to disable it.
W	Configure the WEB authentication status settings of the entire device.	
		Press "W." The command prompt changes to "Enable or Disable global WEB auth status (E/D)>." Press "E" to enable the status or "D" to disable it.
P	Configure the IEEE802.1X port-based access control port settings.	
		Press "P." The command prompt changes to "Enter port number>." Enter the port number to be specified.
A	Configure the IEEE802.1X MAC-based access control port settings.	
		Press "A." The command prompt changes to "Enter port number>." Enter the port number to be specified.
C	Configure the MAC authentication port settings.	
		Press "C." The command prompt changes to "Enter port number>." Enter the port number to be specified.
E	Configure the WEB authentication port settings.	
		Press "E." The command prompt changes to "Enter port number>." Enter the port number to be specified.
Q	Return to the parent menu.	

4.7.7.d. Local User Database Configuration

On the Authentication Configuration, pressing "U" opens the Local User Database Configuration screen, as shown in Fig. 4-7-25-4. On this screen, you can configure the user account settings used in IEEE802.1X access control and WEB authentication

```
PN28080K Local Management System
Authentication Configuration -> Local User Database Configuration Menu

User Name                        Password                         VLAN AuthType
-------------------------------- -------------------------------- ---- --------









-------------------------------- <COMMAND> ----------------------------------
[N]ext Page                 [A]dd User                  [D]elete User
[P]revious Page             Add [E]ncrypted User        Modify [V]LAN ID
Modify Auth [T]ype
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-4 Local User Database Configuration

Screen Description

User Name	Displays the user name.	
Password	Displays the password. Displays [encrypted] if the password is encrypted.	
VLAN	Displays the VLAN ID to be assigned after authentication.	
Auth Type	Displays the authentication type to use the account.	
	WEB	The account is used only in WEB authentication.
	802.1X	The account is used only in 802.1X access control.
	Both	The account is used both in 802.1X access control and WEB authentication.

Available commands are listed below.

N	Display the next page.
	Press "N" to display the next page.
P	Display the previous page.
	Press "P" to display to the previous page.
A	Create a local user.
	Press "A." The command prompt changes to "Enter new user name >." Enter a user name in 32 alphanumeric characters or less. After the entry, the command prompt changes to "Enter new password >." Enter a password in 32 alphanumeric characters or less. After the entry, the command prompt changes to "Enter VLAN ID >." Enter a VLAN ID to be assigned after authentication with an integer between 1 and 4094. After the entry, the command prompt changes to "Enter Auth Type for Local User (W/X/B)>." Press "W" to use only in WEB authentication, "X" to use only in IEEE802.1X access control, or "B" to use in both.
D	Delete a local user.
	Press "D." The command prompt changes to "Enable or Disable global WEB auth status (E/D)>." Press "E" to enable the status or "D" to disable it.
E	Create a local user whose password is encrypted.
	Press "E." The command prompt changes to "Enter new user name >." Enter a user name in 32 alphanumeric characters or less. After the entry, the command prompt changes to "Enter new password >." Enter a password in 32 alphanumeric characters or less. After the entry, the command prompt changes to "Enter VLAN ID >." Enter a VLAN ID to be assigned after authentication with an integer between 1 and 4094. After the entry, the command prompt changes to "Enter Auth Type for Local User (W/X/B)>." Press "W" to use only in WEB authentication, "X" to use only in IEEE802.1X access control, or "B" to use in both.
V	Change the VLAN ID of the local user.
	Press "W." The command prompt changes to "Enter new user name >." Enter a user name in 32 alphanumeric characters or less. After the entry, the command prompt changes to "Enter VLAN ID >." Enter a VLAN ID after change with an integer between 1 and 4094.
T	Change the authentication type of the local user.
	Press "T." The command prompt changes to "Enter new user name >." Enter a user name in 32 alphanumeric characters or less. After the entry, the command prompt changes to "Enter Auth Type for Local User (W/X/B)>." Press "W" to use only in WEB authentication, "X" to use only in IEEE802.1X access control, or "B" to use in both.
Q	Return to the parent menu.

4.7.7.e. Local MAC Database Configuration

On the Authentication Configuration, pressing "C" opens the Local MAC Database Configuration screen, as shown in Fig. 4-7-25-5. On this screen, you can set the MAC address used in MAC authentication.

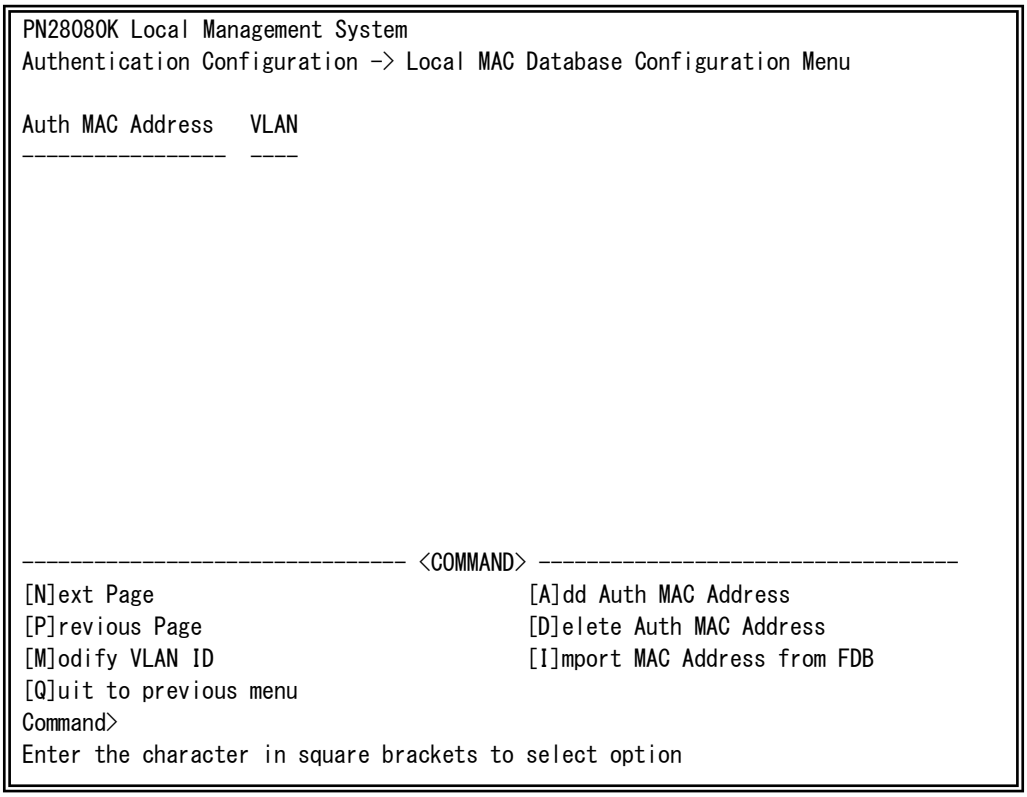


Fig. 4-7-25-5 Local MAC Database Configuration

Screen Description

Auth MAC Address	Displays the MAC address that can be authenticated.
VLAN	Displays the VLAN ID to be assigned after authentication.

Available commands are listed below.

N	Display the next page.	
		Press "N" to display the next page.
P	Display the previous page.	
		Press "P" to display to the previous page.
A	Add a MAC address that can be authenticated.	
		Press "A." The command prompt changes to "Enter the MAC Address (xx:xx:xx:xx:xx:xx)>." Enter the MAC address. After the entry, the command prompt changes to "Enter VLAN ID >." Enter a VLAN ID to be assigned after authentication with an integer between 1 and 4094.
D	Delete a MAC address.	
		Press "D." The command prompt changes to "Enter the MAC Address (xx:xx:xx:xx:xx:xx)>." Enter the target MAC address.
M	Change the VLAN ID of the local user.	
		Press "M." The command prompt changes to "Enter the MAC Address (xx:xx:xx:xx:xx:xx)>." Enter the target MAC address. After the entry, the command prompt changes to "Enter VLAN ID >." Enter a VLAN ID after change with an integer between 1 and 4094.
I	Move to the Import MAC Address from FDB screen.	
Q	Return to the parent menu.	

4.7.7.f. Import MAC Address from FDB

On the Local MAC Database Configuration, pressing "I" opens the Import MAC Address from FDB screen, as shown in Fig. 4-7-25-6. On this screen, you can add all the MAC addresses learned in the FDB as MAC authentication local MAC addresses.

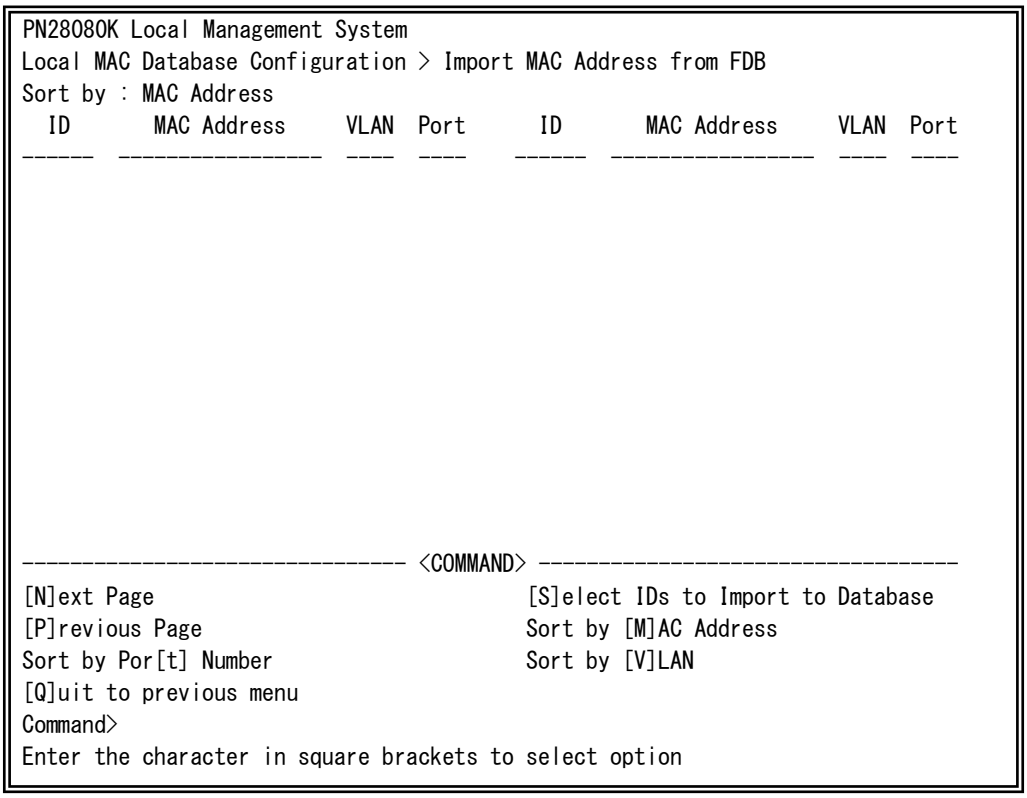


Fig. 4-7-25-6 Import MAC Address from FDB

Screen Description

Sort by	Displays the method of displaying the current MAC address.	
	MAC Address	Displays in ascending order of MAC address.
	Port xx	Displays in ascending order of MAC address on the specified port.
	VLAN xxxx	Displays in ascending order of MAC address on the specified VLAN.
ID	Displays the ID of the MAC address displayed for each page.	
MAC Address	Displays the MAC address learned in the FDB.	
VLAN	Displays the VLAN ID of the MAC address learned in the FDB.	
Port	Displays the port number of the MAC address learned in the FDB.	

Available commands are listed below.

N	Display the next page.	
		Press "N" to display the next page.
P	Display the previous page.	
		Press "P" to display to the previous page.
S	Import a specified ID to the local MAC database.	
		Press "S." The command prompt changes to "Enter the IDs >." Enter the ID to be imported. After the entry, the command prompt changes to "Enter VLAN ID >." Enter a VLAN ID to be assigned after authentication with an integer between 1 and 4094.
M	Display the table in ascending order of MAC address.	
T	Display the table in ascending order of MAC address for the specified port number.	
		Press "T." The command prompt changes to "Select port number >." Enter the target port number.
V	Change the VLAN ID of the local user.	
		Press "V." The command prompt changes to "Select VLAN ID >." Enter the target VLAN ID.
Q	Return to the parent menu.	

4.7.7.g. 802.1X Access Control Configuration

On the Authentication Configuration Menu, pressing "X" opens the 802.1X Access Control Configuration Menu screen, as shown in Fig. 4-7-25-7. On this screen, you can configure the IEEE 802.1X compatible access control function.
The supported authentication methods are EAP-MD5, TLS, and PEAP.

```
PN2808OK Local Management System
Authentication Configuration -> 802.1X Access Control Configuration Menu

802.1X [G]lobal Configuration
[P]erUser/MAC Based Access Control Configuration
[F]orce Authorized MAC Address Configuration
[S]tatistics
[E]AP-Request Configuration
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-7 802.1X Access Control Configuration

Screen Description

802.1X Global Configuration	Configures the IEEE802.1X access control global settings.
PerUser/MAC Based Access Control Configuration	Configures the IEEE802.1X access control function.
Force Authorized MAC Address Configuration	Sets the force authorized MAC address.
Statistics	Displays the IEEE802.1X statistics information.
EAP-Request Configuration	Configures the EAP-Request transmission settings.
Quit to previous menu	Returns to the access control configuration.

4.7.7.h. 802.1X Global Configuration Menu

On the 802.1x Access Control Configuration, pressing "G" opens the 802.1X Global Configuration Menu screen, as shown in Fig. 4-7-25-8. On this screen, you can configure the IEEE802.1X global settings.

```
PN28080K Local Management System
802.1X Access Control Configuration -> 802.1X Global Configuration Menu

Primary Database   : Local                Auth Fail Action     : Stop
Secondary Database : None

--------------------------------- <COMMAND> -----------------------------------
Set [P]rimary Database                    Set [S]econdary Database

[Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-8 802.1X Global Configuration Menu

Screen Description

Primary Database	Displays the reference for the first authentication.	
	RADIUS	The reference is the RADIUS server.
	Local	The reference is the local user database. (Factory default setting)
Secondary Database	Displays the reference for authentication that failed in the Primary Database.	
	Local	The reference is the local user database.
	None	The terminal is authorized without authentication. (Factory default setting)
Auth Fail Action	Displays the action when authentication fails in the Primary Database.	
	Stop (fixed)	Stops the authentication process without performing authentication in the Secondary Database. Only when the Primary Database is RADIUS and a RADIUS server timeout occurs, the process moves to the Secondary Database.

Available commands are listed below.

P	Set the Primary Database.	
		Press "P." The command prompt changes to "Select the primary database (R/L)>." Press "R" to use the RADIUS server or "L" to use the local user database.
S	Set the Secondary Database.	
		Press "S." The command prompt changes to "Select the secondary database (L/N)>." Press "L" to use the local user database or "N" to authorize the terminal.
Q	Return to the parent menu.	

4.7.7.i. IEEE802.1X Port Base Access Control Configuration

On the 802.1X Access Control Configuration Menu, pressing "p" opens the 802.1x Port Base Access Control Configuration screen, as shown in Fig. 4-7-25-9. On this screen, you can configure the IEEE 802.1X compatible port-based access control. The supported authentication methods are EAP-MD5, TLS, and PEAP.

```
PN28080K Local Management System
Advanced Switch Configuration -> Port Based Access Control Configuration Menu
NAS ID: Nas1             Port No: 1      Port Control : Force Authorized
Port Status : Authorized          Authorized MAC Address: --:--:--:--:--:--
Operational Control Direction   : Both
Administrative Control Direction: Both
Per Port Re-auth   : Disabled         Re-Auth Timer Mode      : RADIUS
Current PVID       : 1

Transmit Period    : 30    seconds    Max Request             : 2
Supplicant Timeout : 30    seconds    Quiet Period            : 60    seconds
Serv Timeout       : 30    seconds    Re-auth Period          : 3600  seconds
Guest VLAN ID      : ----             Default VLAN ID         : ----
-------------------------------- <COMMAND> ----------------------------------
[N]ext Page              [T]ransmission Period    R[e]-auth Period
Pre[v]ious Page          Q[u]iet Period           Re-[a]uth Status
[P]ort No                Ma[x]imum Request        [K]ind of Re-auth Timer Mode
Port Auth [M]ode         Server Time[o]ut         Initiali[z]e
Port [C]ontrol           Supp[l]icant Timeout     [R]e-auth Initialize
Port Ctrl [D]irection    De[f]ault VLAN ID        Delete Aut[h] MAC
Num[b]er of Supplicant   [G]uest VLAN ID          Force Auth MAC T[i]meout
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-9 IEEE802.1X Port Base Access Control Configuration

Screen Description

NAS ID	Displays the authentication ID (NAS Identifier).	
Port No	Displays the port number.	
Port Control	Displays the operation mode for authentication requests.	
	Auto	The access control function is enabled. The authentication process relay is performed between the client and authentication server.
	Force Unauthorized	The access control function is disabled. All authentication requests from the client are ignored.
	Force Authorized	The access control function is disabled. Communication of the port is possible without authorization. (Factory default setting)
Port Status	Displays the authentication status.	
	Unauthorized	Authentication is unauthorized.
	Authorized	Authentication is authorized.
Authorized MAC Address	Displays the MAC address of a terminal that succeeded in authentication or a terminal that uses Guest Access. Displays "--:--:--:--:--:--" when nothing is used.	
Operational Control Direction	Displays the operation status at the time of authentication request. (Reflects the settings by Administrative Control Direction below.)	
	Both	Without authentication, this switch does not transmit/receive packets from the applicable port.
	In	Without authentication, this switch does not receive packets from the applicable port.
Administrative Control Direction	Displays the operation method at the time of authentication request.	
	Both	Without authentication, this switch does not transmit/receive packets from the applicable port.
	In	Without authentication, this switch does not receive packets from the applicable port.
Per Port Re-auth	Displays whether periodic re-authentication is enabled or disabled.	
	Enabled	Periodic re-authentication is performed.
	Disabled	Periodic re-authentication is not performed. (Factory default setting)
Re-Auth Timer Mode	Displays whether or not to use this value when Session-Timeout Attribute is reported from the RADIUS server.	
	RADIUS	Preferably uses the Session-Timeout value. (Factory default setting)
	Local	Always uses the Re-auth Period value of this switch.
Current PVID	Displays the PVID currently applied.	
Transmit Period	The number of seconds to wait before requesting the client to reattempt authentication. The factory default setting is 30 seconds.	
Max Request	The maximum number of times of retransmitting an authentication request. The factory default setting is 2.	
Supplicant Timeout	Displays the timeout for the client. The factory default setting is 30 seconds.	
Quiet Period	The number of seconds to wait before reattempting a failed authentication. The factory default setting is 60 seconds.	
Serv Timeout	Displays the timeout for the authentication server. The factory default setting is 30 seconds.	
Re-auth Period	Displays the re-authentication time interval. The factory default setting is 3600 seconds.	
Guest VLAN ID	Displays the VLAN ID to be applied when the terminal is not authorized. Displays "----" when Guest Access is disabled.	

Default VLAN ID	The default VLAN ID is applied when VLAN information could not be obtained from the authentication server even though the dynamic VLAN was enabled and succeeded in authentication. Displays "----" when the Dynamic VLAN is disabled.

Available commands are listed below.

P	Set the port number.	
		Press "P." The command prompt changes to "Enter port number>." Enter the port number you wish to configure.
M	Set the IEEE802.1X access control type.	
		Press "M." The command prompt changes to "Select the Port based or MAC based auth mode (P/M)>." Press "P" for port-based access control or "M" for MAC-based access control.
C	Set the IEEE802.1X access control operation.	
		Press "C." The command prompt changes to "Select authenticator port control ?(A/U/F)>." Press "A" for Auto, "U" for Force Unauthorized, or "F" for Force Authorized.
D	Set the transmission/receiving direction of packets to be discarded when the terminal is not authorized.	
		Press "D." The command prompt changes to "Select Administrative Control Direction, Both or In? (B/I)>." Press "B" to control transmission/receiving or "I" to control receiving.
B	Enabled only in MAC-based access control.	
T	Set the number of seconds to wait before requesting to reattempt authentication.	
		Press "T." The command prompt changes to "Enter Transmission Period>." Enter an integer number between 1 and 65535 (seconds).
U	Set the period time to wait before reattempting a failed authentication.	
		Press "U." The command prompt changes to "Enter quiet period>." Enter an integer number between 1 and 65535 (seconds).
X	Set the maximum number of reattempts of authentication.	
		Press "M." The command prompt changes to "Enter maximum request count>." Enter the maximum number of reattempts with an integer between 1 and 10.
O	Set the timeout for the authentication server.	
		Press "O." The command prompt changes to "Enter server timeout>." Enter an integer number between 1 and 65535 (seconds).
L	Set the timeout for the client.	
		Press "L." The command prompt changes to "Enter supplicant timeout value>." Enter an integer number between 1 and 65535 (seconds).
F	Set the VLAN ID of the Default VLAN.	
		Press "F." The command prompt changes to "Enter default VLAN ID >." Enter the default VLAN ID of the assignment destination. To disable the function, enter 0.
G	Set the VLAN ID of the guest VLAN.	
		Press "G." The command prompt changes to "Enter guest VLAN ID >." Enter the guest VLAN ID of the assignment destination. To disable the function, enter 0.
E	Set the re-authentication time interval.	
		Press "E." The command prompt changes to "Enter re-authentication period>." Enter an integer number between 1 and 65535 (seconds).
A	Enable/disable re-authentication.	
		Press "A." The command prompt changes to "Enable or Disable re-authentication ?(E/D) >." Press "E" to enable re-authentication. Press "D" to disable it.
K	Set the re-authentication timer.	
		Press "K." The command prompt changes to "Select re-authentication timer, RADIUS or Local? (R/L)>." Press "R" to use the re-authentication time reported from the RADIUS. Press "L" to use Re-auth Period of this switch.
Z	Initialize the authentication status.	
		Press "Z." The command prompt changes to "Would you initialize authenticator?(Y/N) >." Press "Y" to initialize the authentication status. Otherwise, press "N."

R	Initialize the re-authentication status.	
		Press "R." The command prompt changes to "Initialize re-authentication?(Y/N) >." Press "Y" to initialize the re-authentication status. Otherwise, press "N."
H	Enabled only in MAC-based access control.	
I	Enabled only in MAC-based access control.	
Q	Return to the parent menu.	

4.7.7.j. MAC Based Access Control Configuration

On the 802.1X Access Control Configuration Menu, when Port Auth Mode is set to MAC-base access control, pressing "p" opens the MAC Based Access Control Configuration screen, as shown in Fig. 4-7-25-10. On this screen, you can configure the IEEE 802.1X compatible MAC-based access control.

```
PN28080K Local Management System
Advanced Switch Configuration -> MAC Based Access Control Configuration Menu
NAS ID: Nas1              Port No: 1     Number of Supplicant: 512
Operational Control Direction: Both   Administrative Control Direction: Both
Transmit Period: 30    sec  Max Request : 2      Supplicant Timeout : 30    sec
Quiet Period   : 60    sec  Serv Timeout: 30    sec  Re-auth Period : 3600  sec
Force Auth MAC Timeout: 3600  sec  Re-auth: Disabled Re-auth Timer Mode: RADIUS
Supplicant MAC Addr  Type      MAC Control     Auth Status  Re-auth
 ------------------ ------- ----------------- ------------ --------




-------------------------------- <COMMAND> -----------------------------------
[N]ext Page              [T]ransmission Period    R[e]-auth Period
Pre[v]ious Page          Q[u]iet Period           Re-[a]uth Status
[P]ort No                Ma[x]imum Request        [K]ind of Re-auth Timer Mode
Port Auth [M]ode         Server Time[o]ut         Initiali[z]e
Port [C]ontrol           Supp[l]icant Timeout     [R]e-auth Initialize
Port Ctrl [D]irection    De[f]ault VLAN ID        Delete Aut[h] MAC
Num[b]er of Supplicant   [G]uest VLAN ID          Force Auth MAC T[i]meout
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-10 MAC Based Access Control Configuration

Screen Description

NAS ID	Displays the authentication ID (NAS Identifier).	
Port No	Displays the port number.	
Number of Supplicant	Displays the number of supplicants that can be authenticated.	
Operational Control Direction	Displays the packet control status when the terminal is not authorized. (Reflects the settings by Administrative Control Direction below.)	
	Both	Without authentication, this switch does not transmit/receive packets from the applicable port.
	In	Without authentication, this switch does not receive packets from the applicable port.
Administrative Control Direction	Displays the packet control method when the terminal is not authorized.	
	Both	Without authentication, this switch does not transmit/receive packets from the applicable port.
	In	Without authentication, this switch does not receive packets from the applicable port.
Transmit Period	The number of seconds to wait before requesting the supplicant to reattempt authentication. The factory default setting is 30 seconds.	
Max Request	The maximum number of times of retransmitting an authentication request. The factory default setting is 2.	
Supplicant Timeout	Displays the timeout for the client. The factory default setting is 30 seconds.	
Quiet Period	The number of seconds to wait before reattempting a failed authentication. The factory default setting is 60 seconds.	
Serv Timeout	Displays the timeout for the authentication server. The factory default setting is 30 seconds.	
Re-auth Period	Displays the re-authentication time interval. The factory default setting is 3600 seconds.	
Force Auth MAC Timeout	Displays the re-authentication interval of the force authorized MAC address. The factory default setting is 3600 seconds.	
Re-auth Timer Mode	Displays the reference for the re-authentication time interval. The factory default setting is RADIUS.	
	RADIUS	Preferably uses the value reported from the RADIUS server.
	Local	Uses the Re-auth Period value.
Re-auth Timer Mode	Displays the reference for the re-authentication time interval. The factory default setting is RADIUS.	
	RADIUS	Preferably uses the value reported from the RADIUS server.
	Local	Uses the Re-auth Period value.
Supplicant MAC Addr	Displays the MAC address of the supplicant.	
Type	Displays the authentication type.	
	Dynamic	Indicates that the terminal was dynamically authorized by the RADIUS server.
	Static	Indicates that the terminal was statically authorized by the registered information.
MAC Control	Displays the authentication type.	
	Auto	The authentication type is the RADIUS server.
	Force Authorized	The authentication type is force authorized.
	Force Unauthorized	The authentication type is force unauthorized.
Auth Status	Displays the authentication status.	
	Authorized	Authentication is authorized.
	Unauthorized	Authentication is not authorized.
Re-auth	Displays the re-authentication status for each supplicant.	

	Enabled	Re-authentication is enabled.
	Disabled	Re-authentication is disabled.

Available commands are listed below.

P	Set the port number.	
		Press "P." The command prompt changes to "Enter port number>." Enter the port number you wish to configure.
M	Set the IEEE802.1X access control type.	
		Press "M." The command prompt changes to "Select the Port based or MAC based auth mode (P/M)>." Press "P" for port-based access control or "M" for MAC-based access control.
C	Enabled only in port-based access control.	
D	Set the transmission/receiving direction of packets to be discarded when the terminal is not authorized.	
		Press "D." The command prompt changes to "Select Administrative Control Direction, Both or In? (B/I)>." Press "B" to control transmission/receiving or "I" to control receiving.
B	Set the number of supplicants that can be authenticated.	
		Press "B." The command prompt changes to "Enter the number of supplicant >." Enter an integer number between 1 and 512.
T	Set the number of seconds to wait before requesting to reattempt authentication.	
		Press "T." The command prompt changes to "Enter Transmission Period>." Enter an integer number between 1 and 65535 (seconds).
U	Set the period time to wait before reattempting a failed authentication.	
		Press "U." The command prompt changes to "Enter quiet period>." Enter an integer number between 1 and 65535 (seconds).
X	Set the maximum number of reattempts of authentication.	
		Press "M." The command prompt changes to "Enter maximum request count>." Enter the maximum number of reattempts with an integer between 1 and 10.
O	Set the timeout for the authentication server.	
		Press "O." The command prompt changes to "Enter server timeout>." Enter an integer number between 1 and 65535 (seconds).
L	Set the timeout for the client.	
		Press "L." The command prompt changes to "Enter supplicant timeout value>." Enter an integer number between 1 and 65535 (seconds).
F	Enabled only in port-based access control.	
G	Enabled only in port-based access control.	
E	Set the re-authentication time interval.	
		Press "E." The command prompt changes to "Enter re-authentication period>." Enter an integer number between 1 and 65535 (seconds).
A	Enable/disable re-authentication.	
		Press "A." The command prompt changes to "Select Per port or MAC address (P/M) >." Press "P" to set per port. Press "M" to set per MAC address. Press "P." The command prompt changes to "Enable or Disable re-authentication ?(E/D) >." Press "E" to enable re-authentication. Press "D" to disable it. Press "M." The command prompt changes to "Enter supplicant MAC address >." Enter the MAC address to be configured. Then, the command prompt changes to "Enable or Disable re-authentication ?(E/D) >." Press "E" to enable re-authentication. Press "D" to disable it.
K	Set the reference for the re-authentication time interval.	
		Press "K." The command prompt changes to "Select re-authentication timer, RADIUS or Local? (R/L)>." Press "R" to use the re-authentication time reported from the RADIUS. Press "L" to use Re-auth Period of this switch.
Z	Initialize the authentication status.	
		Press "Z." The command prompt changes to "Would you initialize authenticator?(Y/N) >." To initialize the authentication status, press "Y." Otherwise, press "N."

R	Initialize the re-authentication status.	
		Press "R." The command prompt changes to "Initialize re-authentication?(Y/N) >." To initialize the re-authentication status, press "Y." Otherwise, press "N."
H	Delete an authorized MAC address and deauthorize it.	
		Press "H." The command prompt changes to "Enter supplicant MAC address >." Enter the MAC address to be deauthorized.
I	Set the re-authentication interval of the force authorized MAC address.	
		Press "I." The command prompt changes to "Enter Force auth MAC period >." Enter an integer number between 1 and 65535 (seconds). To disable re-authentication, enter 0.
Q	Return to the parent menu.	

4.7.7.k. Force Authorized MAC Configuration Menu

On the 802.1x Access Control Configuration, pressing "F" opens the Force Authorized MAC Configuration Menu screen, as shown in Fig. 4-7-25-11. On this screen, you can set the MAC address of a device to be authorized/unauthorized without IEEE802.1X access control.

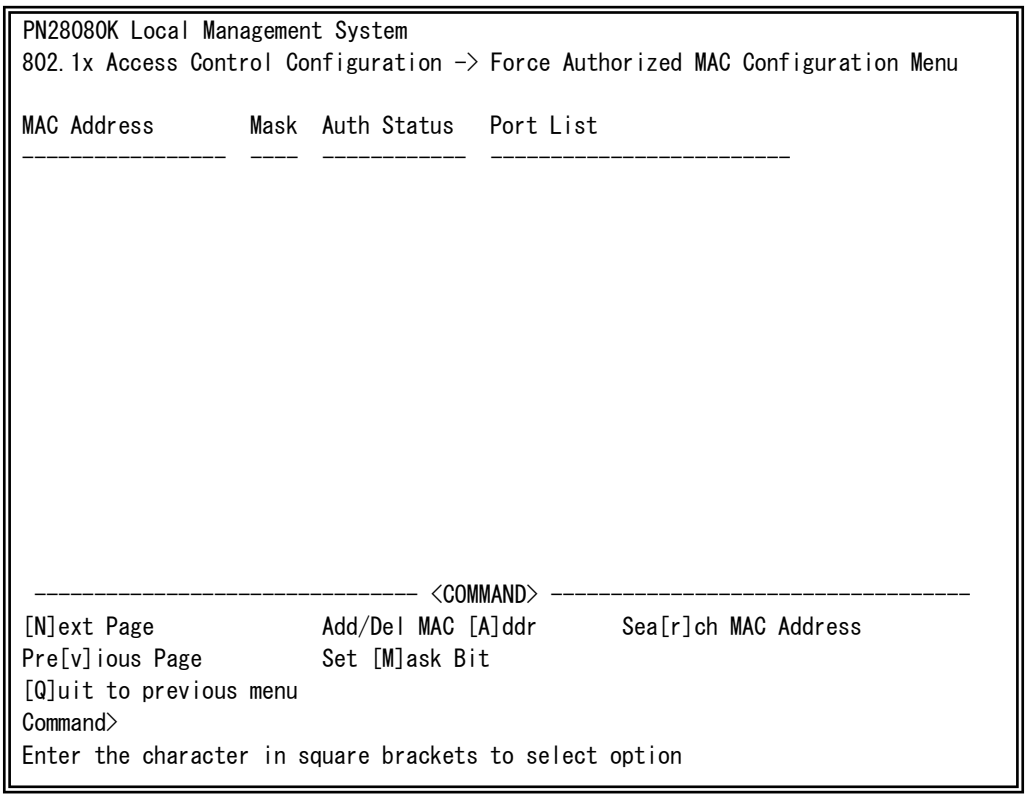


Fig. 4-7-25-11 Force Authorized MAC Configuration Menu

Screen Description

MAC Address	Displays the MAC address of the device to be forcibly authorized.	
Mask	Displays the mask length of the registered MAC address.	
Auth Status	Displays the force authorization type.	
	Authorized	The authentication type is force authorized.
	Unauthorized	The authentication type is force unauthorized.
Port List	Displays the target port list.	

Available commands are listed below.

N	Display the next page.	
		Press "N" to display the next page.
P	Display the previous page.	
		Press "P" to display the previous page.
A	Set the transmission/receiving direction of packets to be discarded when the terminal is not authorized.	
		Press "A." The command prompt changes to "Add or Delete MAC address (A/D)>." Press "A" to add a MAC address. Press "D" to delete it. Then, the command prompt changes to "Enter MAC Address(xx:xx:xx:xx:xx:xx)>." Enter the target MAC address. For adding, the command prompt changes to "Enter mask length>." Enter an integer number between 1 and 48. Then, the command prompt changes to "Select auth status (A/U) >." Press "A" for forced authorize. Press "U" for force unauthorized. Then, the command prompt changes to "Enter port number>." Enter the target port number.
M	Set the mask length of the MAC address.	
		Press "M." The command prompt changes to "Enter MAC Address(xx:xx:xx:xx:xx:xx)>." Enter the MAC address to be configured. Then, the command prompt changes to "Enter mask length>." Enter an integer number between 1 and 48.
R	Narrow down by MAC address.	
		Press "R." The command prompt changes to "Enter MAC Address(xx:xx:xx:xx:xx:xx)>." Enter the target MAC address.
Q	Return to the parent menu.	

4.7.7.1. IEEE802.1 Statistics Menu

On the 802.1x Access Control Configuration, pressing "s" opens the Statistics Menu screen, as shown in Fig. 4-7-25-12. On this screen, you can check the transmission/receiving status of EAPOL packets used in IEEE802.1X.

```
PN28080K Local Management System
802.1x Access Control Configuration -> Statistics Menu
Port: 1   Refresh: 300 Sec.      Elapsed Time Since System Up: 000:00:00:00
<Counter Name>          <Total>
TxReqId                   0
TxReq                     0
TxTotal                   0
RxStart                   0
RxLogoff                  0
RxRespId                  0
RxResp                    0
RxInvalid                 0
RxLenError                0
RxTotal                   0
RxVersion                 0
LastRxSrcMac              00:00:00:00:00:00
-------------------------------- <COMMAND> ----------------------------------
[N]ext  [P]revious  [S]elect Port  Re[f]resh Mode  Since [R]eset  [Q]uit




Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-12 IEEE802.1 Statistics Menu

Screen Description

Port	Displays the port number.
Refresh	Displays the refresh interval.
Elapsed Time Since System Up	Displays the time in which the current counter value has been accumulated. It is the time that has passed since booting or rebooting.
Counter Name	Displays each counter name.
Total	Displays the value accumulated in the counter.

Available commands are listed below.

S	Switch the port to display the values.	
		Press "S." The command prompt changes to "Select Port number>." Enter the port number for which you wish to display values.
N	Display the values of the next port.	
		Press "N." The screen displays the counter values of the next port.
P	Display the values of the previous port.	
		Press "P." The screen displays the counter values of the previous port.
R	Switch the displayed values to the ones after reset of the counter values.	
		Press "R." The values are switched immediately to the ones after reset of the counter values. The time indication at the upper right corner of the screen changes to "Elapsed Time Since System Reset."
F	Set the counter refresh mode.	
		Press "F." "1 for start to refresh,2 for set refresh rate" is displayed in the comment line. To stop refreshing, press "1." The refresh interval is displayed as "STOP" and the display is not refreshed. To change the refresh interval, press "2." The command prompt changes to "Input refresh time>." Enter an integer number between 5 and 600 (seconds).
Q	Return to the parent menu.	

On this screen, you can display two types of counter values: Values accumulated after booting or power-off of this switch (Fig. 4-7-25-12), and values accumulated after resetting the counters (Fig. 4-7-25-13).

```
PN28080K Local Management System
802.1x Access Control Configuration -> Statistics Menu
Port: 1   Refresh: 300 Sec.    Elapsed Time Since System Reset: 000:00:00:00
<Counter Name>          <Total>
TxReqId                   0
TxReq                     0
TxTotal                   0
RxStart                   0
RxLogoff                  0
RxRespId                  0
RxResp                    0
RxInvalid                 0
RxLenError                0
RxTotal                   0
RxVersion                 0
LastRxSrcMac              00:00:00:00:00:00
-------------------------------- <COMMAND> ----------------------------------
[N]ext  [P]revious  [S]elect Port  Re[f]resh Mode  Since [R]eset  [Q]uit




Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-13 Display of Values Accumulated after Resetting the Counters

Screen Description

Port	Displays the port number.
Refresh	Displays the refresh interval.
Elapsed Time Since Reset	Displays the time that has elapsed since resetting of the counters.
Counter Name	Displays each counter name.
Total	Displays the value accumulated in the counter.

Available commands are listed below.

S	Switch the port to display the values.	
		Press "S." The command prompt changes to "Select Port number>." Enter the port number for which you wish to display values.
N	Display the values of the next port.	
		Press "N." The screen displays the counter values of the next port.
P	Display the values of the previous port.	
		Press "P." The screen displays the counter values of the previous port.
U	Switch to the counter display from booting.	
		Press "U." The counter display changes to the one from the system start.
R	Switch to the counter display from resetting the counters.	
		Press "R." The counter display changes to the one from the counter reset.
F	Set the counter refresh mode.	
		Press "F." The command prompt changes to "1 for start to refresh,2 for set refresh rate." Press "1" to cancel the automatic refreshing. Press "2" to change the refresh interval. If you press "2," the command prompt changes to "Input refresh time>." Enter an integer number between 5 and 600 (seconds).
Q	Return to the parent menu.	

The counters are described below.

TxReqId	Displays the number of EAP Request Identity frames transferred from the switch.
TxReq	Displays the number of EAP Request frames transferred from the switch.
TxTotal	Displays the total number of all the types of EAP frames transferred from the switch.
RxStart	Displays the number of EAPOL Start frames received from the supplicant.
RxLogoff	Displays the number of EAPOL Logoff frames received from the supplicant.
RxRespId	Displays the number of EAP Response Identity frames received from the supplicant.
RxResp	Displays the number of EAP Response frames received from the supplicant.
RxInvalid	Displays the number of frames whose frame types cannot be recognized among EAPOL frames received from the supplicant.
RxLenError	Displays the number of frames whose fields indicating the length of the packet body are disabled among EAPOL frames received from the supplicant.
RxTotal	Displays the total number of frames among EAP frames received from the supplicant.
RxVersion	Displays the number of frames that were received in the form of IEEE802.1X version 1 among EAP frames received from the supplicant.
LastRxSrcMac	Displays the source MAC address of the last EAPOL frame received by this switch.

4.7.7.m. EAP-Request Configuration Menu

On the 802.1x Access Control Configuration, pressing "E" opens the EAP-Request Configuration screen, as shown in Fig. 4-7-25-14. On this screen, you can configure the EAP Request transmission settings used in the IEEE802.1X MAC-based access control mode.

```
PN28080K Local Management System
802.1x Access Control Configuration -> EAP-Request Configuration


[E]AP-Request Port Configuration
[U]nauthorized MAC Address Table
[Q]uit to previous menu

Notes: EAP-Request Function is supported for MAC Based Access Control only









Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-14 EAP-Request Configuration

4.7.7.m.1. EAP-Request Port Configuration Menu

On the EAP-Request Configuration, pressing "E" opens the EAP-Request Port Configuration screen, as shown in Fig. 4-7-25-15. On this screen, you can configure the EAP Request transmission settings used in the IEEE802.1X MAC-based access control mode.

```
PN28080K Local Management System
802.1x Access Control Configuration -> EAP-Request Port Configuration

EAP-Request Interval: 5 Sec.

Port    EAP-Request
-----   ------------
   1      Disabled
   2      Disabled
   3      Disabled
   4      Disabled
   5      Disabled
   6      Disabled
   7      Disabled
   8      Disabled

-------------------------------- <COMMAND> ----------------------------------
[N]ext Page              [E]AP-Request Interval
[P]revious Page          [S]et EAP-Request Mode
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-15 EAP-Request Port Configuration Menu

Screen Description

EAP-Request Interval	Display the interval (seconds) to transmit EAP-Requests to unauthorized supplicants. (Factory default setting: 5 seconds)	
Port	Displays the port number.	
EAP-Request	Displays the EAP Request transmission status.	
	Enabled	Transmits EAP Requests to the MAC addresses registered in the unauthorized MAC address table at the EAP-Request Interval.
	Disabled	Does not transmit EAP Requests. (Factory default setting)

Available commands are listed below.

N	Display the values of the next port.	
		Press "N" to display the next page.
P	Display the values of the previous port.	
		Press "P" to display the previous page.
E	Change the transmission interval of EAP Requests.	
		Press "E." The command prompt changes to "Enter new interval>." Enter an integer number between 1 and 3600 (seconds).
S	Change the EAP Request Mode status.	
		Press "S." The command prompt changes to "Enter port number>." Enter the port number to be specified. After the entry, the command prompt changes to "Enable or Disable EAP-Request ?(E/D)>." Press "E" to enable the EAP-Request. Press "D" to disable it.
Q	Return to the parent menu.	

4.7.7.m.2. Unauthorized MAC Address Table

On the EAP-Request Configuration, pressing "U" opens the Unauthorized MAC Address Table screen, as shown in Fig. 4-7-25-16. On this screen, you can view the list of unauthorized MAC addresses to which EAP Requests are to be transmitted.

```
PN28080K Local Management System
802.1x Access Control Configuration -> Unauthorized MAC Address Table

Age-Out Time: 300 Sec.  Display by:MAC      Selected Port:

MAC Address         Port
-----------------   ----









-------------------------------- <COMMAND> ----------------------------------
[N]ext Page                                 Display MAC Address by [M]AC
Pre[v]ious Page                             Display MAC Address by [P]ort
Set Age-Out [T]ime                          Add/Del Unauth MAC [A]ddress
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-16 Unauthorized MAC Address Table

Screen Description

Age-Out Time	Displays the age-out time of the registered MAC address.	
Display by	Displays the method of displaying the current unauthorized MAC address.	
	MAC	Displays in the order of MAC address.
	Port	Narrows down by arbitrary port number.
Selected Port	Displays the port number used when Display by is Port.	
MAC Address	Displays the unauthorized MAC address.	
Port	Displays the port number to which a supplicant with the unauthorized MAC address is connected.	

Available commands are listed below.

N	Display the values of the next port.	
		Press "N" to display the next page.
V	Display the values of the previous port.	
		Press "V" to display the previous page.
T	Change the age-out time.	
		Press "T." The command prompt changes to "Enter new age-out time>." Enter an integer number between 0 and 65535 (seconds).
M	Change to display in the order of MAC address.	
P	Change to narrow down by port number.	
		Press "P." The command prompt changes to "Enter port number>." Enter the target port number.
A	Add or delete a MAC address to/from the table.	
		Press "A." The command prompt changes to "Add or Delete MAC address (A/D)>." Press "A" to add a MAC address. Then, the command prompt changes to "Enter MAC Address(xx:xx:xx:xx:xx:xx)>." Enter a MAC address to be added. Then, the command prompt changes to "Enter port number>." Enter the IEEE802.1X MAC-based access control port number. To delete a MAC address, press "D" and enter a MAC address to be deleted.
Q	Return to the parent menu.	

4.7.7.n. MAC Authentication Configuration Menu

On the Authentication Configuration, pressing "M" opens the MAC Authentication Configuration Menu screen, as shown in Fig. 4-7-25-17. On this screen, you can configure the MAC authentication settings.

```
PN28080K Local Management System
Authentication Configuration -> MAC Authentication Configuration Menu

Primary Database       : Local            Auth Fail Action     : Stop
Secondary Database     : None             Auth Fail Block Time : 60    seconds

MAC Address Format for RADIUS Username
  Case                 : Upper
  Delimiter            : Hyphen
  Delimited Characters : 2

RADIUS Password Type   : MAC Address
Manual Password        :


-------------------------------- <COMMAND> ----------------------------------
Set [P]rimary Database                    Set [S]econdary Database
Set Auth [F]ail Action                    Set Auth Fail [B]lock Time
Set MAC Address [C]ase                    Set [D]elimiter
Set [N]umber of Delimited Characters      Set RADIUS Password [T]ype
Set Manual Pass[w]ord
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-17 MAC Authentication Configuration Menu

Screen Description

Primary Database		Displays the reference for the first authentication.	
		RADIUS	The reference is the RADIUS server.
		Local	The reference is the local user database. (Factory default setting)
Secondary Database		Displays the reference for authentication that failed in the Primary Database.	
		RADIUS	The reference is the RADIUS server.
		Local	The reference is the local user database.
		None	The terminal is authorized without authentication. (Factory default setting)
Auth Fail Action		Displays the action when authentication fails in the Primary Database.	
		Stop	Stops the authentication process without performing authentication in the Secondary Database. (Factory default setting) Only when the Primary Database is RADIUS and a RADIUS server timeout occurs, the process moves to the Secondary Database.
		Secondary DB	Performs authentication in the Secondary Database.
Auth Fail Block Time		Displays the time (seconds) before accepting the authentication process again after an authentication failure. (Factory default setting: 60)	
MAC Address Format for RADIUS Username		Displays the MAC address format of the user name transmitted to the RADIUS server when the RADIUS server is used for MAC authentication.	
	Case	Displays the uppercase/lowercase of the MAC address.	
		Upper	Transmits in uppercase. (Factory default setting)
		Lower	Transmits in lowercase.
	Delimiter	Displays the delimiter type of the MAC address.	
		Hyphen	Uses a hyphen (-). (Factory default setting)
		Colon	Uses a colon (:).
		Dot	Uses a dot (.).
		None	Uses no delimiter.
	Delimited Characters	Displays the number of delimited characters of the MAC address.	
		2	Delimits each two characters. (Factory default setting)
		4	Delimits each four characters.
		6	Delimits each six characters.
RADIUS Password Type		Displays the text type of the password transmitted to the RADIUS server when the RADIUS server is used for MAC authentication.	
		MAC Address	Uses the same MAC address format text as the user name. (Factory default setting)
		Manual	Uses arbitrary fixed text.
Manual Password		Displays the text of the password transmitted to the RADIUS server. This can be used only when RADIUS Password Type is set to Manual.	

Available commands are listed below.

P	Set the Primary Database.	
		Press "P." The command prompt changes to "Select the primary database (R/L)>." Press "R" to use the RADIUS server or "L" to use the local user database.
S	Set the Secondary Database.	
		Press "S." The command prompt changes to "Select the secondary database (R/L/N)>." Press "R" to use the RADIUS server, "L" to use the local user database, or "N" to authorize the terminal.
F	Set the Auth Fail Action.	
		Press "F." The command prompt changes to "Enter Auth Fail Action for Primary Database (D/P)>." To performing authentication in the Secondary Database, press "D." Otherwise, press "P."
B	Set the Auth Fail Block Time.	
		Press "B." The command prompt changes to "Enter auth fail block time >." Enter the waiting time before restarting authentication with an integer between 1 and 65535 (seconds).
C	Set the uppercase/lowercase of the MAC address used for the user name of the RADIUS account.	
		Press "C." The command prompt changes to "Select MAC address case (U/L)>." Press "U" for uppercase or "L" for lowercase.
D	Set the delimiter type of the MAC address used for the user name of the RADIUS account.	
		Press "D." The command prompt changes to "Select delimiter (H/C/D/N)>." Press "H" for hyphen, "L" for colon, "D" for dot, or "N" for no delimiter.
N	Set the number of delimited characters of the MAC address used for the user name of the RADIUS account.	
		Press "N." The command prompt changes to "Select number of delimited characters (2/4/6)>." Press "2" to delimit each two characters, "4" for each four, or "6" for each six.
T	Set the text type used for the password of the RADIUS account.	
		Press "T." The command prompt changes to "Select RADIUS password type (A/M)>." Press "A" to use the same text as the MAC address or "M" to use arbitrary fixed text.
W	Set the fixed text used for the password of the RADIUS account.	
		Press "W." The command prompt changes to "Enter manual password string >." Enter a user name in 32 alphanumeric characters or less.
Q	Return to the parent menu.	

4.7.7.o. WEB Authentication Configuration Menu

On the Authentication Configuration, pressing "W" opens the MAC Authentication Configuration Menu screen, as shown in Fig. 4-7-25-18. On this screen, you can configure the WEB authentication settings.

Connecting the host to the WEB authentication port and accessing a URL from the WEB browser automatically transfers it to the WEB authentication login screen.

```
PN28080K Local Management System
Authentication Configuration -> WEB Authentication Configuration Menu

Primary Database   : Local                Auth Fail Action     : Stop
Secondary Database : None                 Auth Fail Block Time : 60    seconds

Virtual IP Address : 0.0.0.0
HTTP Port Number   : 80
Redirect URL       :









-------------------------------- <COMMAND> ----------------------------------
Set [P]rimary Database                    Set [S]econdary Database
Set Auth [F]ail Action                    Set Auth Fail [B]lock Time
Set Virtual [I]P Address                  Set [H]TTP Port Number
Set Redirect [U]RL
[W]EB Page Contents Config                Temporary [D]HCP Server Config
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-18 WEB Authentication Configuration Menu

Screen Description

Primary Database	Displays the reference for the first authentication.	
	RADIUS	The reference is the RADIUS server.
	Local	The reference is the local user database. (Factory default setting)
Secondary Database	Displays the reference for authentication that failed in the Primary Database.	
	RADIUS	The reference is the RADIUS server.
	Local	The reference is the local user database.
	None	The terminal is authorized without authentication. (Factory default setting)
Auth Fail Action	Displays the action when authentication fails in the Primary Database.	
	Stop	Stops the authentication process without performing authentication in the Secondary Database. (Factory default setting) Only when the Primary Database is RADIUS and a RADIUS server timeout occurs, the process moves to the Secondary Database.
	Secondary DB	Performs authentication in the Secondary Database.
Auth Fail Block Time	Displays the time (seconds) before accepting the authentication process again after an authentication failure. (Factory default setting: 60)	
Virtual IP Address	Displays the Virtual IP Address used on the WEB authentication login screen.	
HTTP Port Number	Displays the TCP port number used on the WEB authentication login screen. (Factory default setting: 80)	
Redirect URL	Displays the URL to be redirected after WEB authentication succeeds.	

Note: The Virtual IP Address needs to be set for WEB authentication.

Note: Specify the IP address of a network different from the one actually connected, such as 1.1.1.1, for the Virtual IP Address.

Note: If a WEB authentication target host is using a fixed IP address, the host needs to be able to communicate with the default gateway before authentication. It is recommended that you normally use the DHCP client and also use the temporary DHCP server.

Note: If the HTTP Port Number is changed, the TCP port number on the WEB setting screen is also changed.

Available commands are listed below.

P	Set the Primary Database.	
		Press "P." The command prompt changes to "Select the primary database (R/L)>." Press "R" to use the RADIUS server or "L" to use the local user database.
S	Set the Secondary Database.	
		Press "S." The command prompt changes to "Select the secondary database (R/L/N)>." Press "R" to use the RADIUS server, "L" to use the local user database, or "N" to allow authentication.
F	Set the Auth Fail Action.	
		Press "F." The command prompt changes to "Enter Auth Fail Action for Primary Database (D/P)>." To performing authentication in the Secondary Database, press "D." Otherwise, press "P."
B	Set the Auth Fail Block Time.	
		Press "B." The command prompt changes to "Enter auth fail block time >." Enter the waiting time before restarting authentication with an integer between 1 and 65535 (seconds).
I	Set the Virtual IP Address on the WEB authentication login screen.	
		Press "I." The command prompt changes to "Enter Virtual IP address >." Enter an IP address.
H	Set the TCP port on the WEB authentication login screen.	
		Press "H." The command prompt changes to "Enter HTTP port number (1-65535)>." Enter the TCP port number on the WEB authentication login screen with an integer between 1 and 65535.
U	Set the redirect URL.	
		Press "U." The command prompt changes to "Enter redirect URL >." Enter the redirected URL after authentication starting with "http://."
W	Move to the WEB Page Contents Config.	
D	Move to the Temporary DHCP Server Config.	
Q	Return to the parent menu.	

4.7.7.o.1. WEB Page Contents Configuration Menu

On the WEB Authentication Configuration Menu, pressing "W" opens the WEB Page Contents Configuration Menu screen, as shown in Fig. 4-7-25-19. On this screen, you can configure the display contents on the WEB authentication login screen.

```
PN28080K Local Management System
WEB Authentication Configuration -> WEB Page Contents Configuration Menu

Page Title       :
Logo Data        : None
User Name String : User Name
Password String  : Password
Message     :




Description :




-------------------------------- <COMMAND> ---------------------------------
Set Page [T]itle          Set [U]ser Name String      Set [P]assword String
Set [M]essage             [S]et Description           [C]lear All Texts
Store [L]ogo Data         [D]elete Logo Data
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-19 WEB Page Contents Configuration Menu

Note: You can enter Japanese in Unicode on this screen. Use a terminal emulator supporting UTF-8 and set the kanji code to UTF-8.

Screen Description

Page Title	Displays the text of the WEB authentication login screen page title. You can use Japanese in Unicode.	
Logo Data	Displays whether logo data exists or not. You can transfer image data of up to 512 KB in JPG/PNG/GIF format via the TFTP server. The actual image can be checked on the WEB setting screen.	
	Existed	Logo data is saved.
	None	Logo data is not saved. (Factory default)
User Name String	Displays the text in the user name input field. (Factory default setting: User Name) You can use Japanese in Unicode.	
Password String	Displays the text in the password input field. (Factory default setting: Password) You can use Japanese in Unicode.	
Message	Displays the display text in the message field. You can use Japanese in Unicode and the following HTML tags. (Other HTML tags are disabled.) <a> <b> <i> <u> <right> <left> <font> <h1>-<h5> <p>	
Description	Displays the display text in the description field. You can use Japanese in Unicode and the following HTML tags. (Other HTML tags are disabled.) <a> <b> <i> <u> <right> <left> <font> <h1>-<h5> <p>	

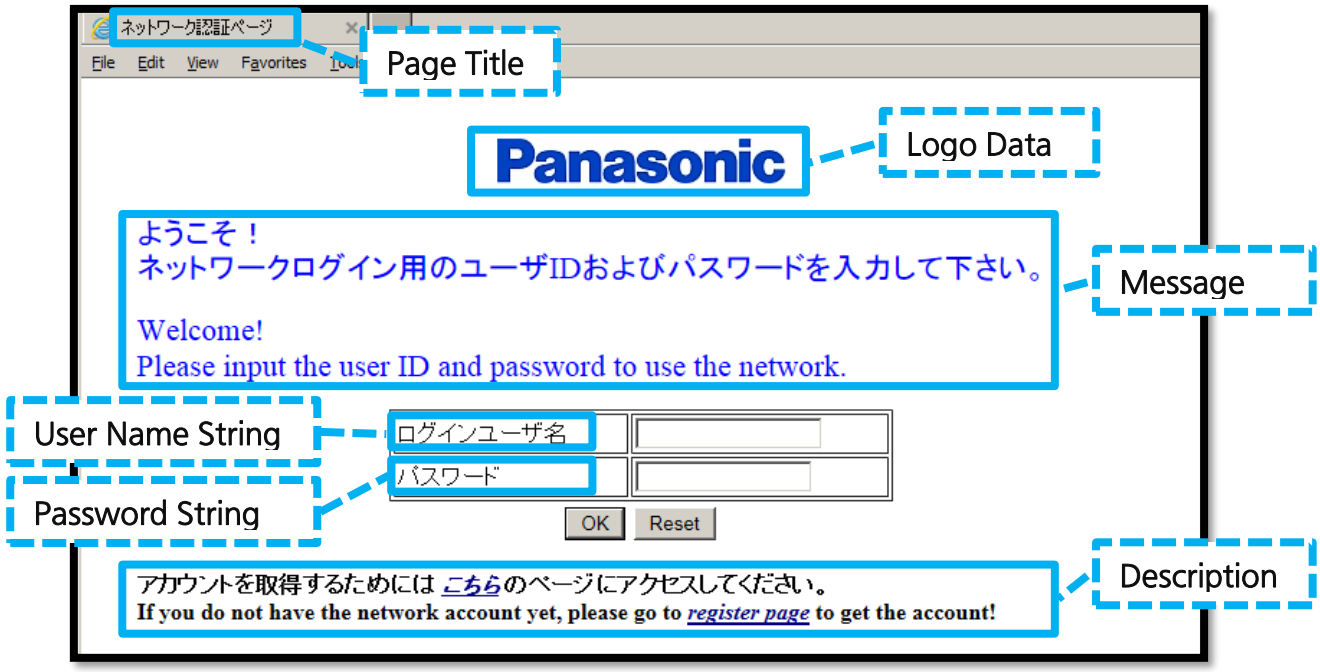


Fig. 4-7-25-20 Configurable Range and Display Example of the WEB Authentication Login Screen Page

Available commands are listed below.

T	Change the text of the WEB authentication login screen page title.	
		Press "T." The command prompt changes to "Enter page title >." Enter text in 64 characters or less. You can use Japanese in Unicode.
U	Change the text of the user name.	
		Press "U." The command prompt changes to "Enter user name string text >." Enter text in 32 characters or less. You can use Japanese in Unicode.
P	Change the text of the password.	
		Press "P." The command prompt changes to "Enter password text >." Enter text in 32 characters or less. You can use Japanese in Unicode.
M	Change the text in the message field.	
		Press "M." The command prompt changes to "Enter message text >." Enter text in 256 characters or less. You can use Japanese in Unicode and the following HTML tags. <a> <b> <i> <u> <right> <left> <font> <h1>-<h5> <p>
S	Change the text in the description field.	
		Press "S." The command prompt changes to "Enter description text >." Enter text in 256 characters or less. You can use Japanese in Unicode and the following HTML tags. <a> <b> <i> <u> <right> <left> <font> <h1>-<h5> <p>
C	Reset all the text settings to the factory settings.	
L	Save logo data to this switch via the TFTP server.	
		Press "L." The command prompt changes to "Enter TFTP server IP >." Enter the IP address of the transmission source TFTP server. After the entry, the command prompt changes to "Enter filename of logo data >." Enter a logo data file name in 39 characters or less.
D	Delete saved logo data.	
		Press "D." The command prompt changes to "Delete logo data? (Y/N)>." To delete the data, press "Y." Otherwise, press "N."
Q	Return to the parent menu.	

4.7.7.o.2. Temporary DHCP Server Configuration Menu

On the WEB Authentication Configuration Menu, pressing "D" opens the Temporary DHCP Server Configuration Menu screen, as shown in Fig. 4-7-25-21. On this screen, you can configure the temporary DHCP server settings to distribute IP addresses required for the WEB authentication port and the DHCP client in the guest VLAN to perform WEB authentication.

```
PN28080K Local Management System
WEB Authentication Configuration -> Temporary DHCP Server Configuration Menu

Temporary DHCP Server Status : Disabled

DHCP Lease Time              : 30 seconds
Start of Leased IP Address   : 0.0.0.0
Number of Leased IP Address  : 32
Default Router Address       :
DNS Server Address           :









-------------------------------- <COMMAND> ----------------------------------
Set Temporary DHCP Server [S]tatus        Set DHCP Lease [T]ime
Set Start of [L]eased IP Address          Set [N]umber of Leased IP Address
Set Default [R]outer Address              Set [D]NS Server Address
[Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-21 Temporary DHCP Server Configuration Menu

Screen Description

Temporary DHCP Server Status	Displays the temporary DHCP server status. IP addresses required for WEB authentication access are leased to the guest VLAN and a port with WEB authentication enabled. To use this function, set a guest VLAN with the management VLAN enabled to the target WEB authentication port.	
	Enabled	The temporary DHCP server is enabled.
	Disabled	The temporary DHCP server is disabled. (Factory default setting)
DHCP Lease Time	Displays the lease time (seconds) of the IP address. (Factory default setting: 30)	
Start of Leased IP Address	Displays the start address of the leased IP address. The subnet mask is fixed to 255.255.255.0.	
Number of Leased IP Address	Displays the number of leased IP addresses. (Factory default setting: 32)	
Default Router Address	Displays the default router address value to be reported using the DHCP. **Specify an IP address that exists in the guest VLAN.** **＊ It is recommended that you use the IP address of this switch.**	
DNS Server Address	Displays the DNS server address value to be reported using the DHCP.	

Note: An IP address lease target port is limited to a WEB authentication port that belongs to the guest VLAN set to the management VLAN.

Note: Specify an IP address that exists in the guest VLAN for Default Router Address.

Note: This function cannot be used as a general DHCP server because it is dedicated to WEB authentication.

Available commands are listed below.

S	Change the temporary DHCP server function status.	
		Press "S." The command prompt changes to "Enable or Disable temporary DHCP server status (E/D)>." Press "E" to enable the temporary DHCP server function or "D" to disable it.
T	Change the DHCP lease time.	
		Press "T." The command prompt changes to "Enter DHCP Lease Time (30-60) >." Enter an integer number between 30 and 60 (seconds).
L	Change the start address of the leased IP address.	
		Press "L." The command prompt changes to "Enter start of released IP address >." Enter the start address of the leased IP address.
N	Change the maximum number of leased IP addresses.	
		Press "N." The command prompt changes to "Enter number of leased IP address (1-64) >." Enter an integer number between 1 and 64 (seconds).
R	Change the default router address (default gateway) to be reported using the DHCP.	
		Press "R." The command prompt changes to "Enter default router address >." Enter the default router address.
D	Changed the DNS server address to be reported using the DHCP.	
		Press "D." The command prompt changes to "Enter DNS server address >." Enter the DNS server address.
Q	Return to the parent menu.	

4.7.7.p. Dynamic VLAN Configuration Menu

On the Authentication Configuration, pressing "V" opens the Dynamic VLAN Configuration Menu screen, as shown in Fig. 4-7-25-22. On this screen, you can configure the dynamic VLAN settings.

```
PN28080K Local Management System
Authentication Configuration -> Dynamic VLAN Configuration Menu

Accept RADIUS Attribute: Enabled

Port  Current PVID    Auth Status   Guest   Default
----  ------------    ------------  ------  -------
   1       1            Authorized   ----    ----
   2       1            Authorized   ----    ----
   3       1            Authorized   ----    ----
   4       1            Authorized   ----    ----
   5       1            Authorized   ----    ----
   6       1            Authorized   ----    ----
   7       1            Authorized   ----    ----
   8       1            Authorized   ----    ----


-------------------------------- <COMMAND> ----------------------------------

[N]ext Page              Set RADIUS [A]ttribute       Set [D]efault VLAN
[P]revious Page          Set [G]uest VLAN             [Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-7-25-22 Dynamic VLAN Configuration Menu

Screen Description

Accept RADIUS Attribute	Displays whether or not to use the Attribute reported from the RADIUS server. The target Attribute is as follows. - Tunnel-Private-Group-ID	
	Enabled	Uses the reported Attribute. (Factory default setting)
	Disabled	Uses the setting of this switch.
Port	Displays the port number.	
Current PVID	Displays the current PVID.	
Auth Status	Displays the current port authentication status.	
	Authorized	The authentication function is disabled, or the port is already authorized by IEEE802.1X port-based access control.
	Unauthorized	The port is on standby for IEEE802.1X MAC-based access control, MAC authentication, or WEB authentication.
Guest	Displays the VLAN ID of the guest VLAN. Specify a VLAN to be assigned while a client connected to the authorized port is not authorized.	
Default	Displays the VLAN ID of the default VLAN. Specify a VLAN to be assigned when Accept RADIUS Attribute is Enabled and Tunnel-Private-Group-ID is not reported from the RADIUS server.	

Available commands are listed below.

N	Display the next page.	
		Press "N" to display the next page.
P	Display the previous page.	
		Press "P" to display to the previous page.
A	Set whether or not to use the Attribute reported from the RADIUS server.	
		Press "A." The command prompt changes to "Enable or Disable to accept RADIUS attribute (E/D)>." Press "E" to use the Attribute from the RADIUS server or "D" to use the setting of this switch.
G	Set the guest VLAN.	
		Press "G." The command prompt changes to "Enter port number>." Enter the port number to be specified. After the entry, the command prompt changes to "Enter guest VLAN ID>." Enter an existing VLAN ID to be set as the guest VLAN. To disable the guest VLAN, enter 0.
D	Set the default VLAN.	
		Press "D." The command prompt changes to "Enter port number>." Enter the port number to be specified. After the entry, the command prompt changes to "Enter default VLAN ID>." Enter an existing VLAN ID to be set as the default VLAN. To disable the default VLAN, enter 0.
Q	Return to the parent menu.	

Note: If the guest VLAN is set, the PVID of the target port is changed to the guest VLAN ID.

4.7.8 Loop Detection Configuration Menu

On the Advanced Switch Configuration Menu, pressing "D" opens the Loop Detection Configuration Menu, as shown in Fig. 4-7-26. On this screen, you can set the loop detection and shut-off function.
For network configuration, also refer to "Appendix C. Example of Network Configuration using Loop Detection/Shut-off Function and Its Precautions" in this operation manual.

```
PN28080K Local Management System
Advanced Switch Configuration -> Loop Detection Configuration Menu
Global Loop Detection Status: Disabled
Port  Trunk  Link     State     Loop Detect    Mode    Recovery  Recovery Time
----  -----  ----  -----------  -----------  --------  --------  -------------
  1    ---   Down  Forwarding   Enabled      Block     Enabled       60
  2    ---   Down  Forwarding   Enabled      Block     Enabled       60
  3    ---   Down  Forwarding   Enabled      Block     Enabled       60
  4    ---   Down  Forwarding   Enabled      Block     Enabled       60
  5    ---   Down  Forwarding   Enabled      Block     Enabled       60
  6    ---   Down  Forwarding   Enabled      Block     Enabled       60
  7    ---   Down  Forwarding   Enabled      Block     Enabled       60
  8    ---   Down  Forwarding   Disabled     Block     Enabled       60
  9    ---   Down  Forwarding   Disabled     Block     Enabled       60



--------------------------------- <COMMAND> -----------------------------------
Set Port [L]oop Detect Status          Set Port Recovery [S]tatus
[E]nable/Disable Loop Detection        Set Port Recovery [T]imer
Loop History [I]nformation             [Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-7-26 Loop Detection Configuration Menu

Screen Description

Global Loop Detection Status	Shows the status of loop detection/shut-off function.	
	Enabled	The loop detection/shut-off function is enabled. (Factory default setting)
	Disabled	The loop detection/shut-off function is disabled.
Port	Shows the port number.	
Trunk	Shows the link aggregation group ID.	
Link	Shows the state of linkup.	
	Up	Link is up.
	Down	Link is down.
State	Shows the behavior of loop detection/shut-off function.	
	Forwarding	Packet is normally forwarded.
	Loop Detect	Loop is detected and the port is shut off.
Loop Detect	Shows the status of loop detection/shut-off function of each port.	
	Enabled	The loop detection/shut-off function is enabled. (Factory default setting: Port 1 to 7)
	Disabled	The loop detection/shut-off function is disabled. (Factory default setting: Port 8 to 9)
Mode	Shows the mode of Loop detection behavior.	
	Block	When the Switching Hub detects loop, the ports are blocked. (Factory default setting)
	Shutdown	When the Switching Hub detects loop, the ports are shut down.
Recovery	Shows the recovery mode for auto-recovery of the shutoff port.	
	Enabled	Automatically recovers from port shutoff after the recovery time elapses. (Factory default setting)
	Disabled	Does not recover from port shutoff until manually set.
Recovery Time	Shows the number of seconds for recovery time, which is standby time until the shutoff port is automatically recovered. (Factory default setting: 60)	

Available commands are listed below.

E	Set the status of loop detection/shut-off function.	
		Press "E." The command prompt changes to "Enable or Disable Loop Detection (E/D)>." Press "E" to enable the loop detection/shut-off function. Press "D" to disable it.
I	Press "I." The Loop History Information screen opens.	
L	Set the status of loop detection/shut-off function of each port.	
		Press "L." The command prompt changes to "Select port number to be changed>." Enter a target port number. Then, the command prompt changes to "Enable or Disable Loop Detection (E/D)>." Enter "E" to enable the loop detection/shut-off function of each port. Press "D" to disable it. Upon setting, the command prompt changes to " Select Loop Detection mode (B/S)>." Pless "B" to change to the block mode. Pless "S" to change to the shutdown mode. When entering multiple port numbers, delimit with comma with no space, or hyphenate the continuous numbers. Enter "0" to apply all ports.
S	Set the status of recovery mode for auto-recovery of the shutoff port.	
		Press "S." The command prompt changes to "Select port number to be changed>." Enter a target port number. Then, the command prompt changes to "Enable or Disable Recovery for port x (E/D)>." Press "E" to enable auto-recovery of the port. Press "D" to disable it. When entering multiple port numbers, delimit with comma with no space, or hyphenate the continuous numbers. Enter "0" to apply all ports.
T	Set the recovery time in seconds, which is the standby time until the shutoff port is automatically recovered.	
		Press "T." The command prompt changes to "Select port number to be changed>." Enter a target port number. Then, the command prompt changes to "Enter Recovery Timer>." Enter the recovery time in seconds from 60 to 86400.
Q	Return to the previous menu.	

Note: If the status of loop detection/shut-off function (Global Loop Detection Status) is changed, the configuration information is saved and all settings are stored in a built-in memory.

4.7.7.a. Loop History Information

On the Loop Detection Configuration Menu, pressing "I" opens the Loop History Information screen, as shown in Fig. 4-7-27. On this screen, the date and time of detecting loop and the event information are listed.

```
PN28080K Local Management System
Loop Detection Configuration Menu -> Loop History Information

Entry  Time(YYYY/MM/DD HH:MM:SS)                    Event
-----  --------------------------   ------------------------------------------

--------------------------------- <COMMAND> -----------------------------------
[N]ext Page
[P]revious Page
[C]lear Loop Detection history
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Fig. 4-7-27 Loop History Information

Screen Description

Entry	Shows the event number.	
Time	Shows the time when the event occurred. If the time is not set, the accumulated running time since boot is shown.	
Event	Shows the description of the event occurred to the Switching Hub.	
	The loop detected on portX.	Indicates that a loop was detected in a Switching Hub under port X, and the connection has been shut down.
	The loop detected between portX and portY.	Indicates that a loop was detected between port X and port Y, and the connection has been shut down.
	PortX auto recovery.	Indicates that the port X is automatically recovered from being shut down.

Available commands are listed below.

N	Show the next page.
	Press "N." The screen shows the next page.
P	Show the previous page.
	Press "P." The screen shows the previous page.
C	Delete the history information in the loop history function.
Q	Return to the previous menu.

4.7.9. Port Group Configuration Menu

On the Advanced Switch Configuration Menu, pressing "P" opens the Port Group Configuration Menu, as shown in Fig. 4-7-29. On this screen, you can configure port grouping. If a port grouping is configured, ports designated as members of the port group can communicate only among member ports in the same group. Multiple port groups can be assigned to each port. An example of configuration using port grouping is given in Fig. 4-7-28.

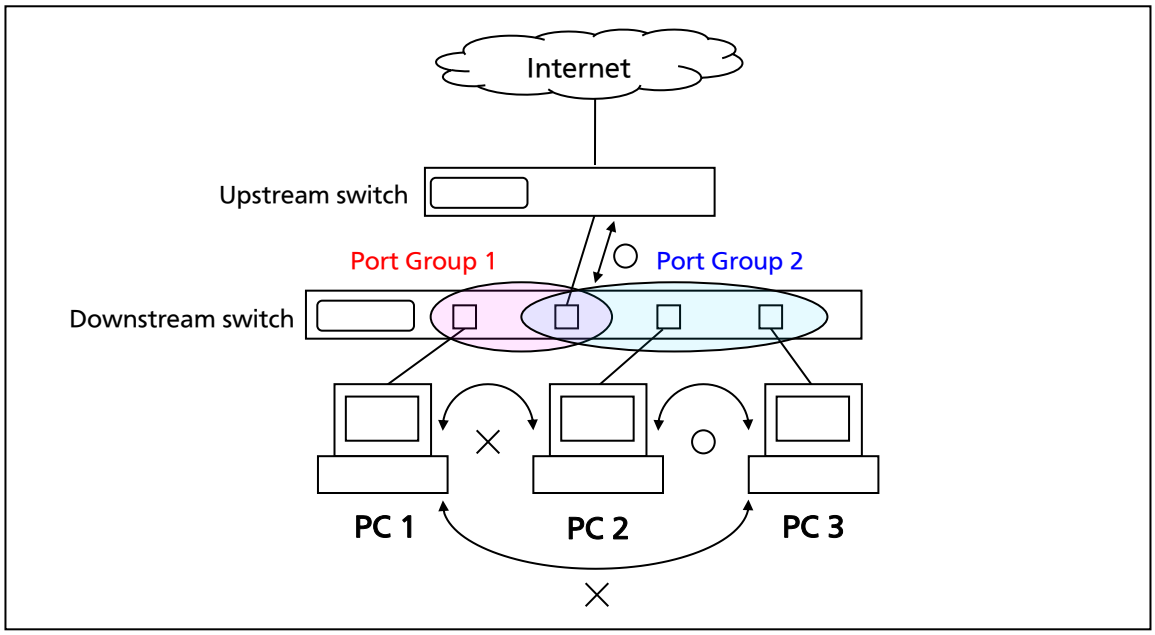


Fig. 4-7-28 Example of Configuration Using Port Grouping
(This configuration allows communications between PC1 and Internet, and among PC2, PC3, and Internet.)

Note: The loop detection/shut-off function detects a loop of a frame and shuts down the connection, even if the loop occurs between different port groups.
If some member ports of a link aggregation group are configured across two or more port groups, a frame may not be transferred normally.

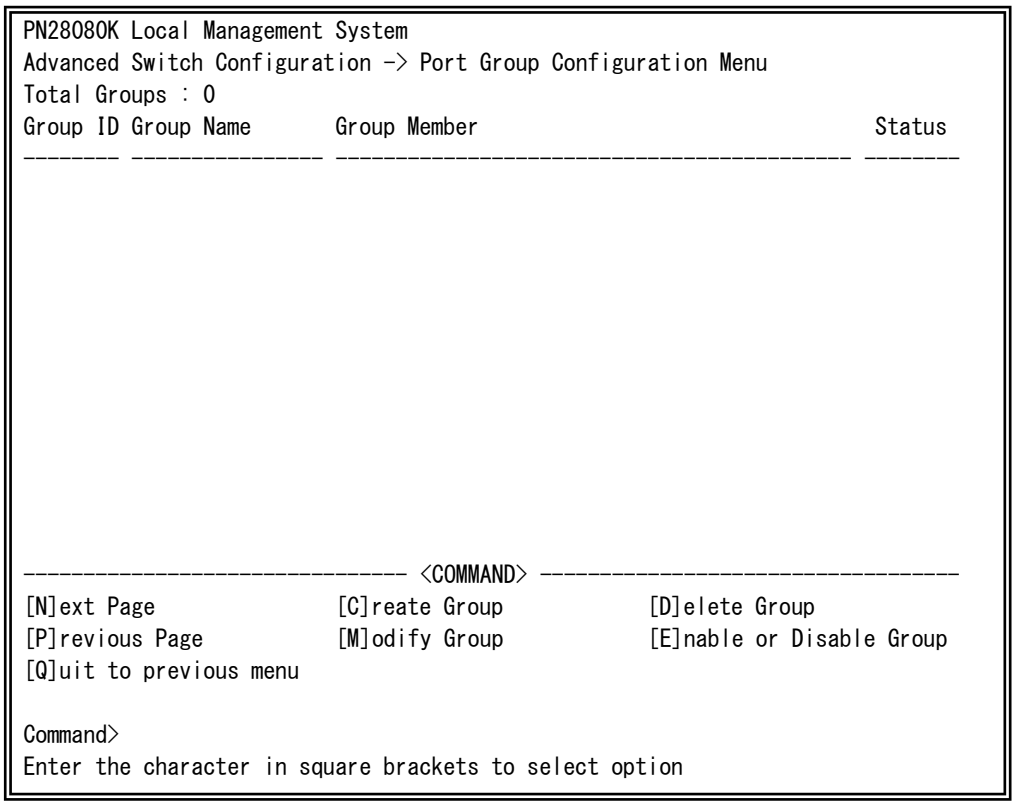


Fig. 4-7-29 Port Group Configuration Menu

Screen Description

Group ID	Shows the port group ID.
Group Name	Shows the port group name being configured.
Group Member	Shows member ports belonging to the port group.

Available commands are listed below.

N	Show the next page.
	Press "N." The screen shows the next page.
P	Show the previous page.
	Press "P." The screen shows the previous page.
C	Go to the screen for creating a port group.
	Press "C." The Port Group Create Menu opens. For details, refer to the next section **(4.7.9.a).**
D	Delete a port group.
	Press "D." The command prompt changes to "Enter Port Group ID>." Enter a port group ID you wish to delete with a value of 1 to 256.
M	Go to the screen for changing a port grouping setting.
	Press "M." The command prompt changes to "Enter Port Group ID>." Enter a port group ID you wish to configure with a value of 1 to 256. Then, the Port Group Modification Menu opens. For details, refer to the next section **(4.7.9.b).**
Q	Return to the previous menu.

4.7.8.a. Port Group Creation Menu

On the Port Group Management Menu, pressing "C" opens the Port Group Creation Menu, as shown in Fig. 4-7-30. On this screen, you can create a port group.

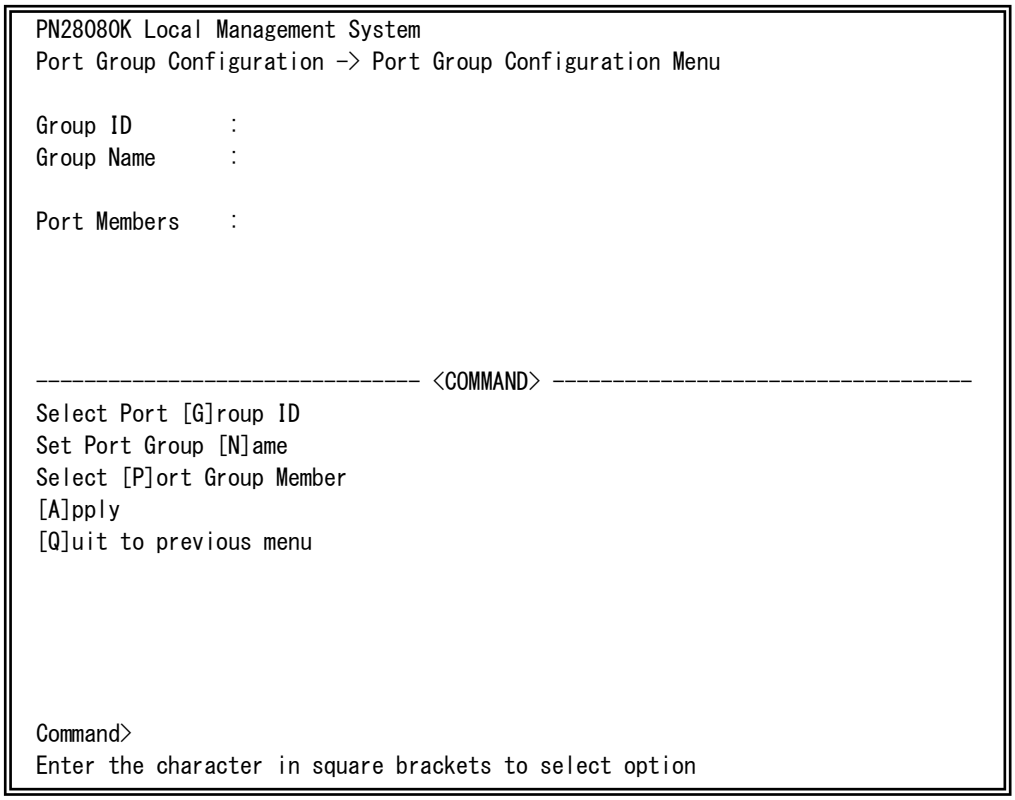


Fig. 4-7-30 Port Group Creation Menu

Screen Description

Group ID	Shows the port group ID.
Group Name	Shows the port group name being configured.
Port Members	Shows member ports belonging to the port group.

Available commands are listed below.

G	Set a port group ID.	
		Press "G." The command prompt changes to "Enter Port Group ID>." Enter a port group ID.
N	Set a port group name.	
		Press "N." The command prompt changes to "Enter Port Group name>." Enter a port group name in 16 one-byte characters or less.
P	Set a port group member.	
		Press "P." The command prompt changes to "Enter egress port number>." Enter a port number you wish to set. When entering multiple port numbers, delimit with comma with no space, or hyphenate the continuous numbers.
A	Create a port group.	
		Press "A" to apply the setting.
Q	Return to the previous menu.	

Note: After setting a port group, make sure to press "A" to apply the setting. If you press "Q" without pressing "A", the setting will be discarded and the port group will not be created.

4.7.8.b. Port Group Modification Menu

On the Port Group Management Menu, pressing "o" and then specifying a port group ID open the Port Group Modification Menu, as shown in Fig. 4-7-31. On this screen, you can modify the port group setting.

```
PN28080K Local Management System
Port Group Configuration -> Port Group Modification Menu

Group ID        : 1
Group Name      :

Port Members    : 1-8




-------------------------------- <COMMAND> ----------------------------------
Set Port Group [N]ame
Select [P]ort Group Member
[A]pply
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-7-31 Port Group Modification Menu

Screen Description

Group ID	Shows the port group ID.
Group Name	Shows the port group name being configured.
Port Members	Shows member ports belonging to the port group.

Available commands are listed below.

N	Set a port group name.	
		Press "N." The command prompt changes to "Enter Port Group name>." Enter a port group name in 16 one-byte characters or less.
P	Set a port group member.	
		Press "P." The command prompt changes to "Enter egress port number>." Enter a port number you wish to set. When entering multiple port numbers, delimit with comma with no space, or hyphenate the continuous numbers.
A	Apply modified setting of the port group.	
		Press "A" to apply the setting.
Q	Return to the previous menu.	

4.7.10. Digital Diagnostic Monitoring Menu

On the Advanced Switch Configuration Menu, pressing "G" opens the Digital Diagnostic Monitoring Menu, as shown in Fig. 4-7-32. On this screen, you can show the SFP status and set the alarm.

```
PN28080K Local Management System
Advanced Switch Configuration -> Digital Diagnostic Monitoring Menu

Limit Trap Status     : Disabled

SFP Port Number       :  9                Transceiver Type      :
Vender Name           :                   Vender Product Number :
Vender Serial Number  :

               RX Power     TX Power     Temp          Voltage    Bias Current
               (dBm)        (dBm)        (deg. C)      (V)        (mA)
               -----------  -----------  ------------  ---------  ------------
Status           0.0000       0.0000       0.0000      0.0000       0.0000
High Alarm     0.0000(A)    0.0000(A)    0.0000(A)   0.0000(A)    0.0000(A)
High Warning   0.0000(A)    0.0000(A)    0.0000(A)   0.0000(A)    0.0000(A)
Low  Alarm     0.0000(A)    0.0000(A)    0.0000(A)   0.0000(A)    0.0000(A)
Low  Warning   0.0000(A)    0.0000(A)    0.0000(A)   0.0000(A)    0.0000(A)
-------------------------------- <COMMAND> ------------------------------------
[N]ext SFP port           Set [R]X Power Limit       Set T[e]mp Limit
[P]revious SFP port       Set [T]X Power Limit       Set [B]ias Current Limit
Set Limit Trap [S]tatus   Set [V]oltage Limit        [Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Fig. 4-7-32 Digital Diagnostic Monitoring Menu

Screen Description

Limit Trap Status:	Shows the trap sending settings for detecting DDM alarm or warning.	
	Enabled:	The trap sending is enabled.
	Disabled:	The trap sending is disabled. (Factory default setting)
SFP Port Number	Shows the current SFP port.	
Tranceiver Type	Shows the kind of SFP.	
Vender Name	Shows the SFP vender name.	
Vender Product Number	Shows the SFP product number.	
Vender Serial Number	Shows the SFP serial number.	
Rx Power (dBm)	Shows the Rx power.	
Tx Power (dBm)	Shows the Tx power.	
Temp (deg. C)	Shows the Temparature.	
Voltage (V)	Shows the Voltage.	
Bias Current (mA)	Shows the bias current.	
Status	Shows the current value.	
High Alarm	Shows the high alarm value.	
High Warning	Shows the high warning value.	
Low Alarm	Shows the low alarm value.	

Low Warning	Shows the low warning value.

Available commands are listed below.

N	Show the next page.	
		Press "N." The screen shows the next port.
P	Show the previous page.	
		Press "P." The screen shows the previous port.
S	Enable/disable a sending SNMP trap.	
		Press "S." The command prompt changes to " Enable or Disable Limit trap(E/D)>." Press "E" to enable the sending SNMP trap. Press "D" to disable it.
R	Configure the Rx power threshold settings.	
		Press "R." The command prompt changes to " Auto or Manual (A/M)>." Press "A" to set the SFP default value. Press "M" to set the value manually. If "M" is selected, the command prompt changes to " High or Low(H/L)>." Press "H" to set the high alarm or warning value. Press "L" to set the low alarm or warning value. Upon setting, the command prompt changes to " Alarm or Warning(A/W)>." Select "A" for alarm. Select "W" for warning. Then, the command prompt changes to " Enter value>." Enter the threshold value.
T	Configure the Tx power threshold settings.	
		Press "T." The command prompt changes to " Auto or Manual (A/M)>." Press "A" to set the SFP default value. Press "M" to set the value manually. If "M" is selected, the command prompt changes to " High or Low(H/L)>." Press "H" to set the high alarm or warning value. Press "L" to set the low alarm or warning value. Upon setting, the command prompt changes to " Alarm or Warning(A/W)>." Select "A" for alarm. Select "W" for warning. Then, the command prompt changes to " Enter value>." Enter the threshold value.
V	Configure the Voltage threshold settings.	
		Press "V." The command prompt changes to " Auto or Manual (A/M)>." Press "A" to set the SFP default value. Press "M" to set the value manually. If "M" is selected, the command prompt changes to " High or Low(H/L)>." Press "H" to set the high alarm or warning value. Press "L" to set the low alarm or warning value. Upon setting, the command prompt changes to " Alarm or Warning(A/W)>." Select "A" for alarm. Select "W" for warning. Then, the command prompt changes to " Enter value>." Enter the threshold value.
E	Configure the Temparature threshold settings.	
		Press "E." The command prompt changes to " Auto or Manual (A/M)>." Press "A" to set the SFP default value. Press "M" to set the value manually. If "M" is selected, the command prompt changes to " High or Low(H/L)>." Press "H" to set the high alarm or warning value. Press "L" to set the low alarm or warning value. Upon setting, the command prompt changes to " Alarm or Warning(A/W)>." Select "A" for alarm. Select "W" for warning. Then, the command prompt changes to " Enter value>." Enter the threshold value.
B	Configure the bias current threshold settings.	
		Press "B." The command prompt changes to " Auto or Manual (A/M)>." Press "A" to set the SFP default value. Press "M" to set the value manually. If "M" is selected, the command prompt changes to " High or Low(H/L)>." Press "H" to set the high alarm or warning value. Press "L" to set the low alarm or warning value. Upon setting, the command prompt changes to " Alarm or Warning(A/W)>." Select "A" for alarm. Select "W" for warning. Then, the command prompt changes to " Enter value>." Enter the threshold value.
Q	Return to the previous menu.	

4.7.11. Static Multicast Address

On the Advanced Switch Configuration Menu, pressing "U" opens the Static Multicast Address Table Menu, as shown in Fig. 4-7-33. On this screen, you can set the forwarding multicast group to the specific port only.

```
PN28080K Local Management System
Advanced Switch Configuration -> Static Multicast Address Table Menu

VLAN ID  Group MAC Address  Group Members
-------  -----------------  ------------------------------------------------
     1   01:00:5E:00:00:00   1









-------------------------------- <COMMAND> -----------------------------------
[N]ext Page               [P]revious Page            [Q]uit to previous menu
[A]dd Static Member Port  [D]elete Static Member Port


Command>
Enter the character in square brackets to select option
```

Fig. 4-7-33 Digital Diagnostic Monitoring Menu

Screen Description

VLAN ID	Shows the VLAN ID of multicast group.
Group MAC Address	Shows the MAC address of multicast group.
Group Members	Shows the ports of multicast group.

Available commands are listed below.

N	Show the next page.
	Press "N." The screen shows the next page.
P	Show the previous page.
	Press "P." The screen shows the previous page.
A	Register an additional Multicast group address.
	Press "A." The command prompt changes to " Enter VLAN ID >." Enter a VLAN ID between 1 and 4094. Then, The command prompt changes to " Enter MAC address for multicast entry>." Enter a multicast group MAC address to be added. Then, the command prompt changes to " Select group member>." Enter a port.
D	Delete a Multicast group MAC address that has been registered.
	Press "D." The command prompt changes to " Enter VLAN ID >." Enter a VLAN ID between 1 and 4094. Then, The command prompt changes to " Enter MAC address for multicast entry>." Enter a multicast group MAC address to be delete. Then, the command prompt changes to " Select group member>." Enter a port.
Q	Return to the previous menu.

4.8. Statistics

On the Main Menu, pressing "S" opens the Statistics Menu, as shown in Fig. 4-8-1. On this screen, you can confirm the statistics information of packets and thereby grasp the network status.

```
PN28080K Local Management System
Main Menu -> Statistics Menu
Port:  1   Refresh: 300 Sec.   Elapsed Time Since System Reset: 000:00:00:00
<Counter Name>          <Total>                 <Avg./s>
Total RX Bytes          0                       0
Total RX Pkts           0                       0
Good Broadcast          0                       0
Good Multicast          0                       0
CRC/Align Errors        0                       0
Undersize Pkts          0                       0
Oversize Pkts           0                       0
Fragments               0                       0
Jabbers                 0                       0
Collisions              0                       0
64-Byte Pkts            0                       0
65-127 Pkts             0                       0
128-255 Pkts            0                       0
256-511 Pkts            0                       0
512-1023 Pkts           0                       0
1024-1518 Pkts          0                       0
-------------------------------- <COMMAND> ----------------------------------
[N]ext  [P]revious  [S]elect Port  Re[f]resh Mode  [R]eset  Since [U]p  [Q]uit
Command>
Enter the character in square brackets to select option
```

Fig. 4-8-1 Statistics: Values accumulated since booting

Screen Description

Port	Shows the port number.
Refresh	Shows the refresh interval of the screen. (Factory default setting: 300 seconds)
Elapsed Time Since System Up	Shows the time elapsed since booting of this Switching Hub.
Counter Name	Shows each counter name.
Total	Shows each counter value.
Avg./s	Shows the average per second of each counter.

Available commands are listed below.

N	Show the values of the next port.	
		Press "N." The screen shows the counter values of the next port. Disabled in Port 9.
P	Show the values of the previous port.	
		Press "P." The screen shows the counter values of the previous port. Disabled in Port 1.
S	Switch a target port.	
		Press "S." The command prompt changes to "Select Port number>." Enter the port number you wish to display.
F	Set the screen refresh mode.	
		Press "F." The command prompt changes to "1 for start to refresh, 2 for set refresh rate." Press "1" to stop auto-refresh. Press "2" to change the refresh interval. If you press "2," the command prompt changes to "Input refresh time>." Enter an integer between 5 and 600 (seconds).
R	Reset counter values.	
		Press "R" to reset counter values. The display is changed at the counter reset.
Q	Return to the previous menu.	

On this screen, you can display two types of values: Values accumulated since booting the Switching Hub (Fig. 4-8-1) and values accumulated since the counter reset (Fig. 4-8-2). An accumulated value since booting is retained even if the counter is reset.

```
PN28080K Local Management System
Main Menu -> Statistics Menu
Port:  1   Refresh: 300 Sec.   Elapsed Time Since System Reset: 000:00:00:00
<Counter Name>          <Total>                 <Avg./s>
Total RX Bytes          0                       0
Total RX Pkts           0                       0
Good Broadcast          0                       0
Good Multicast          0                       0
CRC/Align Errors        0                       0
Undersize Pkts          0                       0
Oversize Pkts           0                       0
Fragments               0                       0
Jabbers                 0                       0
Collisions              0                       0
64-Byte Pkts            0                       0
65-127 Pkts             0                       0
128-255 Pkts            0                       0
256-511 Pkts            0                       0
512-1023 Pkts           0                       0
1024-1518 Pkts          0                       0
-------------------------------- <COMMAND> ---------------------------------
[N]ext  [P]revious  [S]elect Port  Re[f]resh Mode  [R]eset  Since [U]p  [Q]uit
Command>
Enter the character in square brackets to select option
```

Fig. 4-8-2 Statistics: Values accumulated since resetting counters

Screen Description

Port	Shows the port number.
Refresh	Shows the refresh interval of the screen. (Factory default setting: 300 seconds)
Elapsed Time Since Reset	Shows the time elapsed since resetting counters.
Counter Name	Shows each counter name.
Total	Shows each counter value.
Avg./s	Shows the average per second of each counter.

Available commands are listed below.

N	Show the values of the next port.	
		Press "N." The screen shows the counter values of the next port. Disabled in Port 9.
P	Show the values of the previous port.	
		Press "P." The screen shows the counter values of the previous port. Disabled in Port 1.
S	Switch a target port.	
		Press "S." The command prompt changes to "Select Port number>." Enter the port number you wish to display.
F	Set the counter refresh mode.	
		Press "F." The command prompt changes to "1 for start to refresh, 2 for set refresh rate." Press "1" to stop auto-refresh. Press "2" to change the refresh interval. If you press "2," the command prompt changes to "Input refresh time>." Enter an integer between 5 and 600 (seconds).
R	Switch to display counter values since resetting counters.	
		Press "R" to reset the counter values. Elapsed Time Since System Reset becomes 0.
U	Set the screen refresh mode.	
		Press "U" to display counters since booting.
Q	Return to the previous menu.	

The counters are described below.

Total RX Bytes	Shows the number of bytes of all packets received.
Total RX Pkts	Shows the number of all packets received.
Good Broadcast	Shows the number of broadcast packets received.
Good Multicast	Shows the number of multicast packets received.
CRC/Align Errors	Shows the number of error packets that have a normal packet length (64 to 1518 bytes); however, have an error found by an error detection code (FCS). If the packet length is an integral multiple of one byte, the error is a CRC (FCS) error. If not, it is an alignment error.
Undersize Pkts	Shows the number of error packets that have a packet length less than 64 bytes; however, have no other errors.
Oversize Pkts	＜When the Jumbo status is disabled＞ Shows the number of packets having a packet length greater than 1518 bytes. ＜When the Jumbo status is enabled＞ Shows the number of packets having a packet length greater than 9216 bytes.
Fragments	Shows the number of error packets that have a packet length less than 64 bytes and have a CRC or alignment error.
Jabbers	Shows the number of error packets that have a packet length greater than 1518 bytes and have a CRC or alignment error.
Collisions	Shows the number of packet collisions.
64-Byte Pkts	Shows the total number of packets having a packet length of 64 bytes.
65-127 Pkts	Shows the total number of packets having a packet length of 65 to 127 bytes.
128-255 Pkts	Shows the total number of packets having a packet length of 128 to 255 bytes.
256-511 Pkts	Shows the total number of packets having a packet length of 256 to 511 bytes.
512-1023 Pkts	Shows the total number of packets having a packet length of 512 to 1023 bytes.
1024-1518 Pkts	Shows the total number of packets having a packet length of 1024 to 1518 bytes. ＊ This field is displayed when the Jumbo status is enabled.

4.9. Switch Tools Configuration

On the Main Menu, pressing "T" opens the Switch Tools Configuration screen, as shown in Fig. 4-9-1. On this screen, you can configure and use additional functions of the Switching Hub, including firmware upgrade, upload/download of configuration, system reboot, and log viewing.

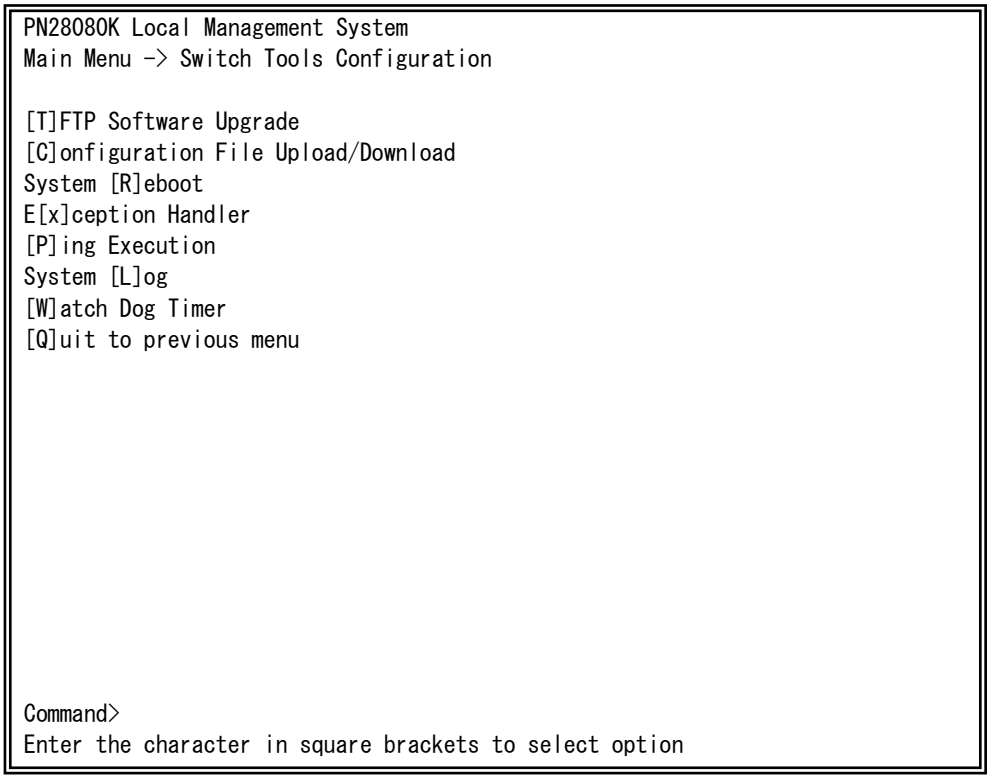


Fig. 4-9-1 Switch Tools Configuration

Screen Description

TFTP Software Upgrade	Configures and executes the firmware version upgrade of this Switching Hub.
Configuration File Upload/Download	Configures and executes the upload/download of the configuration of this Switching Hub.
System Reboot	Configures and executes the reboot of this Switching Hub.
Exception Handler	Configures the operation when exception occurs in this Switching Hub.
Ping Execution	Executes ping from this Switching Hub.
System Log	Shows the system log of this Switching Hub.
Watch Dog Timer	Configures the Watch Dog function.
Quit to previous menu	Quits the Switch Tools Configuration Menu and returns to the Main menu.

4.9.1. TFTP Software Upgrade

On the Switch Tools Configuration Menu, pressing "T" opens the TFTP Software Upgrade screen, as shown in Fig. 4-9-2. On this screen, you can upgrade the firmware version.

```
PN28080K Local Management System
Switch Tools Configuration -> TFTP Software Upgrade

Image Version:        1.0.0.xx
TFTP Server IP:       0.0.0.0
TFTP Server IPv6:     ::
Image File Name:
Reboot Timer:         0 seconds

-------------------------------- <COMMAND> ----------------------------------
Set TFTP [S]erver IP Address
Set TFTP Server [I]Pv6 Address
Set Image [F]ile Name
[U]pgrade Image
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-9-2 TFTP Software Upgrade

Screen Description

Image Version	Shows the current firmware version.
TFTP Server IP	Shows the IP address of the TFTP server providing the firmware to be used for update.
Image File Name	Shows the file name of the firmware to be upgraded.
Reboot Timer	Shows the time before rebooting after downloading the firmware. You can set the time in the System Reboot Menu.

Available commands are listed below.

S	Set the IP address of the TFTP server providing the firmware to be used for update.	
		Press "S." The command prompt changes to "Enter IP address of TFTP server>." Enter the IP address of the TFTP server.
F	Set the file name of the firmware to be upgraded.	
		Press "F." The command prompt changes to "Enter file name>." Specify the file name of the downloaded program within 30 one-byte characters.
U	Start upgrading.	
		Press "D." The command prompt changes to "Download file(Y/N)>." Confirm whether or not you wish to start the process. Confirm that all settings are correct. Press "Y" to start upgrading. If you find any incorrect setting, press "N" to reset the settings.
Q	Return to the previous menu.	

When the download starts, the screen shown in Fig. 4-9-3 opens, and the download status is displayed. (To cancel the TFTP transfer process, press Ctrl+C during transfer.) When download is completed, the firmware is rewritten. After waiting for the time set by the Reboot Timer, rebooting is automatically executed.

```
PN28080K Local Management System
Software Upgrade Menu -> Download Status
TFTP Server IP:       192.168.1.10
TFTP Server IPv6:     ::
Image File Name:      M8eG.rom
Protocol: TFTP

*******< Press CTRL-C to quit downloading >*******
         Data received (Bytes)
         ---------------------
```

Fig. 4-9-3 Download in Process

Note: Be sure not to turn off the power of the Switching Hub while upgrading the firmware version.

4.9.2. Configuration File Upload/Download

On the Switch Tools Configuration Menu, pressing "C" opens the Configuration File Upload/Download Menu, as shown in Fig. 4-9-4. On this screen, you can upload/download the configuration information of this Switching Hub to/from a PC as a file.

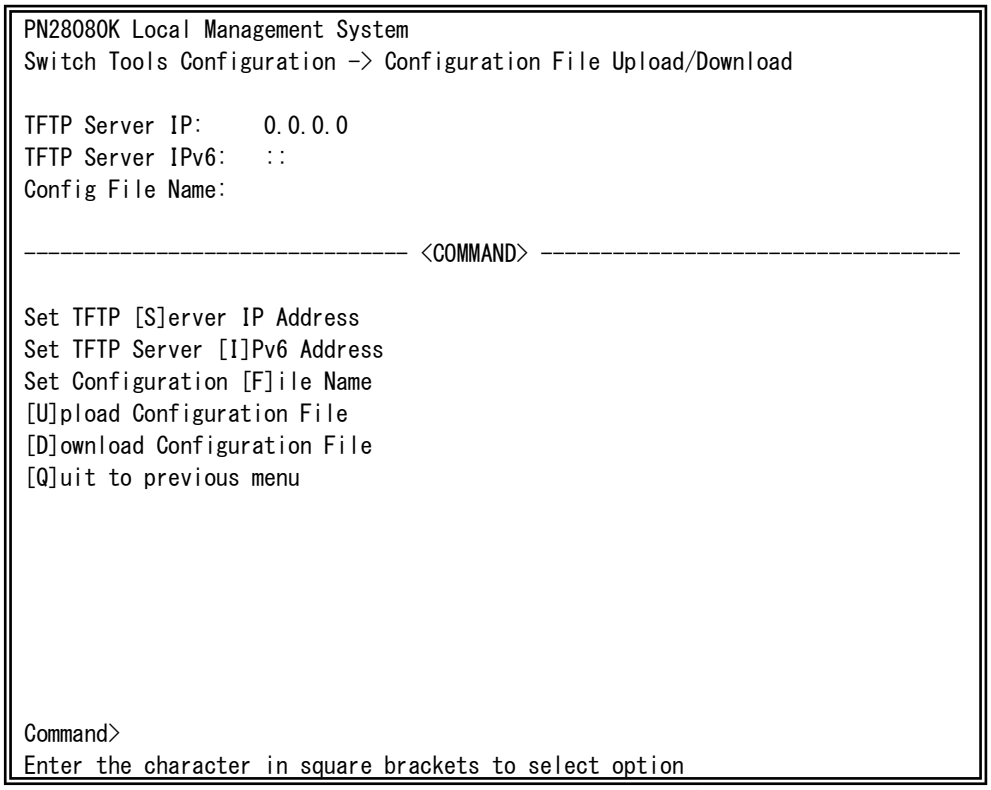


Fig. 4-9-4 Configuration File Upload/Download

Screen Description

TFTP Server IP	Shows the IP address of the TFTP server to upload/download the configuration.
Config File Name	Shows the configuration file name.

Available commands are listed below.

S	Set the IP address of the TFTP server to upload/download the configuration information.	
		Press "S." The command prompt changes to "Enter IP address of TFTP server>." Enter the IP address of the TFTP server.
F	Set the file name of the configuration information to be uploaded/downloaded.	
		Press "F." The command prompt changes to "Enter file name>." Specify the file name of the downloaded program within 30 one-byte characters.
U	Start uploading the configuration information.	
		Press "U." The command prompt changes to "Upload file(Y/N)>." Confirm whether or not you wish to start the process. Confirm that all settings are correct. Press "Y" to start uploading. If you find any incorrect setting, press "N" to reset the settings.
D	Start downloading the configuration information.	
		Press "D." The command prompt changes to "Download file(Y/N)>." Confirm whether or not you wish to start the process. Confirm that all settings are correct. Press "Y" to start downloading. If you find any incorrect setting, press "N" to reset the settings.
Q	Return to the previous menu.	

4.9.3. System Reboot

On the Switch Tools Configuration Menu, pressing "R" opens the System Reboot Menu, as shown in Fig. 4-9-5. On this screen, you can reboot this Switching Hub.

```
PN28080K Local Management System
Switch Tools Configuration -> System Reboot Menu

Reboot Status:        Stop
Reboot Type:          Normal
Reboot Timer:         0 seconds
Time Left:            N/A

-------------------------------- <COMMAND> ----------------------------------
Set Reboot [O]ption
Start [R]eboot Process
Set Reboot [T]imer
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-9-5 System Reboot

Screen Description

Reboot Status	Shows whether or not the reboot command is being executed.	
	Stop	Indicates that the reboot command is not being executed.
Reboot Type	Shows the reboot type. The factory default setting is "Normal."	
	Normal	Normal reboot is executed.
	Factory Default	All settings are reset to factory default.
	Factory Default Except IP	All settings except the IP address are reset to factory default.
Reboot Timer	Shows the time between execution of the reboot command and actual reboot. The factory default setting is 0 seconds.	
Time Left	Shows the time left before the system actually reboots after execution of the reboot command. A key entry refreshes the screen display, allowing you to check the elapsed time.	

Available commands are listed below.

O	Set the reboot type to normal reboot or factory default.	
		Press "O." The command prompt changes to "Select one option (N/F/I)>." Press "N" to set the type to normal reboot. Press "F" to return it to factory default. Press "I" to save only the IP address setting and return the other settings to factory default.
R	Execute the reboot.	
		Press "R." The command prompt changes to "Are you sure to reboot the system (Y/N)>." Press "Y" to execute it. Press "N" to cancel it.
T	Set the time before the system reboots.	
		Press "T." The command prompt changes to "Enter Reboot Timer>." Enter a value between 0 or 5 and 86400 seconds (24 hours).
Q	Return to the previous menu.	

4.9.4. Exception Handler

On the Switch Tools Configuration Menu, pressing "x" opens the Exception Handler screen, as shown in Fig. 4-9-6. On this screen, you can configure the exception handling operations.

```
PN28080K Local Management System
Switch Tools Configuration -> Exception Handler

Exception Handler:            Disabled
Exception Handler Mode:       Debug Message









--------------------------------- <COMMAND> -----------------------------------
Enable/Disable E[x]ception Handler
Set Exception Handler [M]ode
[Q]uit to previous menu



Command>
Enter the character in square brackets to select option
```

Fig. 4-9-6 Exception Handler

Screen Description

Exception Handler	Shows the status of exception handler. The factory default setting is "Disabled."	
	Enabled	Exception handler is enabled.
	Disabled	Exception handler is disabled.
Exception Handler Mode	Shows the method of exception handler.	
	Debug Message	When the Switching Hub detects exception handler, a debug message is displayed on the console screen.
	System Reboot	When the Switching Hub detects exception handler, the system automatically starts rebooting.

Available commands are listed below.

X	Enable/disable exception handler.	
		Press "X." The command prompt changes to "Enable or Disable Exception Handler (E/D)>." Press "E" to enable the function. Press "D" to disable it.
M	Set the method of exception handler.	
		Press "M." The command prompt changes to "Select Exception Handler Mode (M/R)>." Press "M" to display a debug message. Press "R" to reboot.
Q	Return to the previous menu.	

4.9.5. Ping Execution

On the Switch Tools Configuration Menu, pressing "P" opens the Ping Execution screen, as shown in Fig. 4-9-7. On this screen, you can select IPv4 or IPv6 ping command.

```
PN28080K Local Management System
Switch Tools Configuration -> Ping Execution


IPv[4] Ping Execution
IPv[6] Ping Execution
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Fig. 4-9-7 Ping Execution

4.9.5.a. IPv4 Ping Execution

On the Ping Execution Menu, pressing "4" opens the IPv4 Ping Execution screen, as shown in Fig. 4-9-8. On this screen, you can execute the IPv4 ping command from the Switching Hub to confirm communications with connected terminals and other devices.

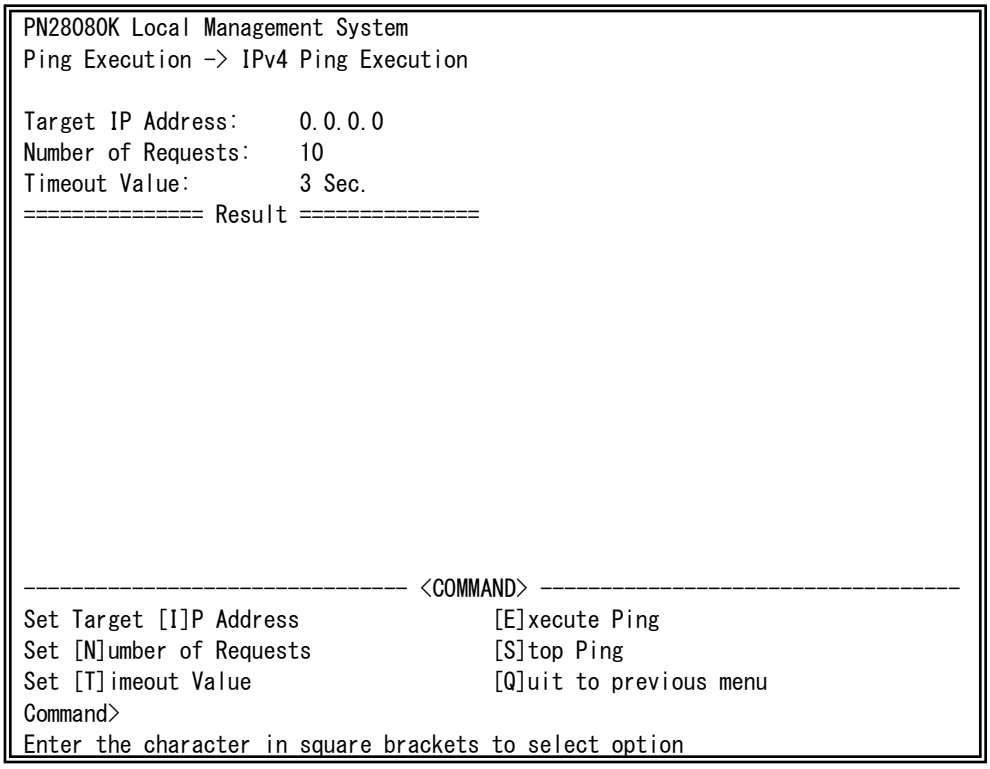


Fig. 4-9-8 IPv4 Ping Execution

Screen Description

Target IP Address:	Shows the IP address of the target of the ping. The factory default setting is 0.0.0.0.
Number of Request	Shows the number of times of ping. The factory default setting is 10 times.
Timeout Value	Shows the time before timeout occurs. The factory default setting is 3 seconds.
Result	Shows the ping result.

Available commands are listed below.

I	Set the IP address of the target of the ping.	
		Press "I." The command prompt changes to "Enter new Target IP Address >." Enter the IP address.
N	Set the number of times of ping.	
		Press "N." The command prompt changes to "Enter new Request Times>." Enter the number of times. Ping can be executed up to 10 times. Enter the number of times between 1 and 10.
T	Set the time before timeout occurs.	
		Press "T." The command prompt changes to "Enter new Timeout Value>." Set the time in seconds. Up to 5 seconds can be set. Enter the time between 1 to 5 seconds.
E	Execute the ping command. Or, clear the display.	
		Press "E." The command prompt changes to "Execute Ping or Clean before Ping Data (E/C)>." Press "E" to execute ping. Press "C" to only clear the display.
S	Cancel the ping command.	
		Press "S" or "Ctrl+C" during the ping execution to cancel it.
Q	Return to the previous menu.	

```
PN28080K Local Management System
Ping Execution -> IPv4 Ping Execution

Target IP Address:     192.168.0.100
Number of Requests:    10
Timeout Value:         3 Sec.
=============== Result ===============
     No. 1               < 10 ms
     No. 2               < 10 ms
     No. 3               < 10 ms
     No. 4               < 10 ms
     No. 5               < 10 ms
     Waiting for response...




-------------------------------- <COMMAND> ----------------------------------
Set Target [I]P Address              [E]xecute Ping
Set [N]umber of Requests             [S]top Ping
Set [T]imeout Value                  [Q]uit to previous menu
 >
S or Ctrl-C Stop ping function
```

Fig. 4-9-9 Display during IPv4 Ping Execution

4.9.5.b. IPv6 Ping Execution

On the Ping Execution Menu, pressing "6" opens the IPv6 Ping Execution screen, as shown in Fig. 4-9-10. On this screen, you can execute the IPv6 ping command from the Switching Hub to confirm communications with connected terminals and other devices.

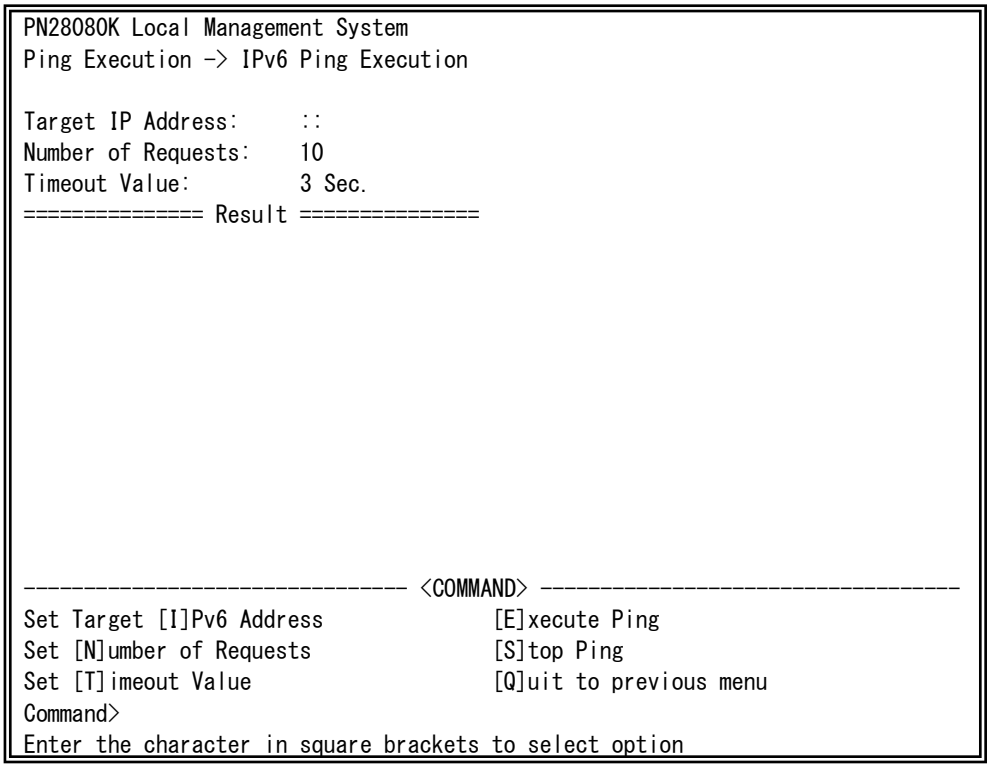


Fig. 4-9-10 Ping Execution

Screen Description

Target IP Address:	Shows the IPv6 address of the target of the ping. The factory default setting is ::.
Number of Request	Shows the number of times of ping. The factory default setting is 10 times.
Timeout Value	Shows the time before timeout occurs. The factory default setting is 3 seconds.
Result	Shows the ping result.

Available commands are listed below.

I	Set the IPv6 address of the target of the ping.	
		Press "I." The command prompt changes to " Enter new target IPv6 address>." Enter the IPv6 address.
N	Set the number of times of ping.	
		Press "N." The command prompt changes to "Enter new Request Times>." Enter the number of times. Ping can be executed up to 10 times. Enter the number of times between 1 and 10.
T	Set the time before timeout occurs.	
		Press "T." The command prompt changes to "Enter new Timeout Value>." Set the time in seconds. Up to 5 seconds can be set. Enter the time between 1 to 5 seconds.
E	Execute the ping command. Or, clear the display.	
		Press "E." The command prompt changes to "Execute Ping or Clean before Ping Data (E/C)>." Press "E" to execute ping. Press "C" to only clear the display.
S	Cancel the ping command.	
		Press "S" or "Ctrl+C" during the ping execution to cancel it.
Q	Return to the previous menu.	

```
PN28080K Local Management System
Ping Execution -> IPv6 Ping Execution

Target IP Address:     2001:1::1:201
Number of Requests:    10
Timeout Value:         3 Sec.
=============== Result ===============
     No. 1               < 10 ms
     No. 2               < 10 ms
     No. 3               < 10 ms
     No. 4               < 10 ms
     No. 5               < 10 ms
     No. 6               < 10 ms
     No. 7               < 10 ms
     Waiting for response...



-------------------------------- <COMMAND> ----------------------------------
Set Target [I]Pv6 Address              [E]xecute Ping
Set [N]umber of Requests               [S]top Ping
Set [T]imeout Value                    [Q]uit to previous menu
 >
S or Ctrl-C Stop ping function
```

Fig. 4-9-11 Display during Ping Execution

4.9.6. System Log

On the Switch Tools Configuration Menu, pressing "L" opens the System Log Menu, as shown in Fig. 4-9-12. This screen shows logs of events occurred to the Switching Hub. This allows you to grasp the events occurred to the Switching Hub and utilize them for network management.

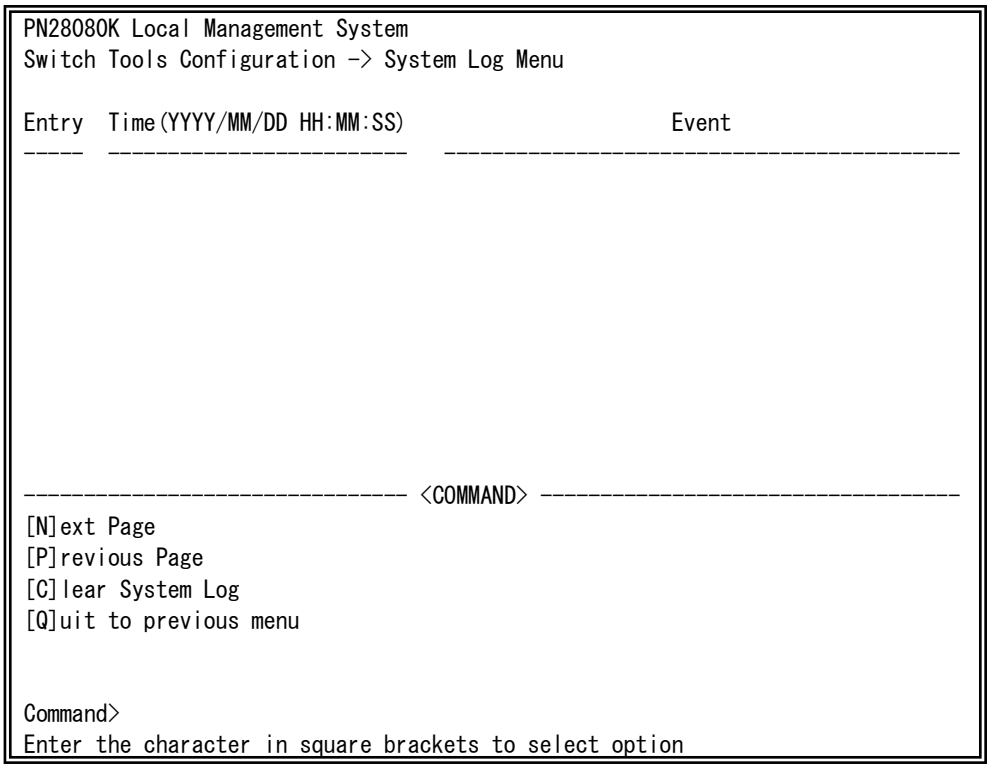


Fig. 4-9-12 System Log

Each event displayed on this screen links to an SNMP trap. An event for which a trap is set is displayed here. The relationships with traps are described below.

Screen Description

Entry	Shows the event number.
Time	Shows the time when the event occurred. If the time is not set, the accumulated running time since boot is shown.
Event	Shows the description of the event occurred to the Switching Hub.

Available commands are listed below.

N	Show the next page.
	Press "N." The screen shows the next page.
P	Show the previous page.
	Press "P." The screen shows the previous page.
C	Clear all logs.
	Press "C" to clear all logs.
Q	Return to the previous menu.

System logs are as follows.

Counter	
Error	Received error packets. (CRC/Align Errors)
	Indicates that receiving CRC/Align error packet.
	Received the error packets. (Undersize Pkts)
	Indicates that receiving the packet under 64 Bytes.
	Received the error packets. (Oversize Pkts)
	Indicates that receiving the packet over 1518 Bytes.
	Received the error packets. (Fragments)
	Indicates that receiving Fragment frame.
	Received the error packets. (Jabbers)
	Indicates that receiving Jabber frame.
	Received the error packets. (Collisions)
	Indicates the detecting Collision.
	Cannot send the packets. (Ping)
	Indicate that cannot send the packet.
	Cannot send the packets. (Telnet)
	Indicate that cannot send the packet.
	Cannot send the packets. (SNMP)
	Indicate that cannot send the packet.
	Cannot send the packets. (Syslog)
	Indicate that cannot send the packet.
	Cannot send the packets. (RADIUS)
	Indicate that cannot send the packet.
	Cannot send the packets. (SSH)
	Indicate that cannot send the packet.
	Cannot send the packets. (SNTP)
	Indicate that cannot send the packet.

	Cannot send the packets. (ARP)
	Indicate that cannot send the packet.
	Cannot send the packets. (EAP)
	Indicate that cannot send the packet.
	Cannot send the packets. (TFTP)
	Indicate that cannot send the packet.
Loop Detect	
Error	The loop detected between port xx and yy.
	Indicates that a loop was detected between Port A and Port B.
	The loop detected port xx
	Indicates that a loop was detected on Port X.
Info	Port xx aute recovery
	Indicates that Port X has auto-recovered from shutoff after loop detection.
Port Monitoring	
Info	Start monitoring function
	Indicates that the monitoring function started.
	Stop monitoring function
	Indicates that the monitoring function stopped.
RADIUS	
Info	Accept Login via RADIUS
	Indicates that the login operation was executed via RADIUS, and was successful.
Error	Reject Login via RADIUS
	Indicates that the login operation was executed via RADIUS, and was rejected.
	RADIUS Timeout
	Indicates that the login operation was executed via RADIUS, and was timeout.
SNTP	
Info	SNTP update to yyyy/mm/dd hh:mm:ss
	Indicates the time synchronized with SNTP server.
	SNTP first update to yyyy/mm/dd hh:mm:ss
	Indicates that communication has failed due to no transmission route to configured SNTP server.
	No response from SNTP server.
	Indicates that time-out occurred in time synchronized with SNTP server.
Storm	
Info	Detect the storm. (DLF)
	Indicates that storm occurred.
	Detect the storm. (Multicast)

	Indicates that multicast storm occurred.
	Detect the storm. (Broadcast)
	Indicates that broadcast storm occurred.
System	
Info	System Cold Start.
	Indicates that the power of the Switching Hub was turned on.
	Port-X Link-up.
	Indicates that Port-X was linked up.
	Port-X Link-down.
	Indicates that Port-X was linked down.
	Connect SFP module(Port-x).
	Indicates that SFP module was connected.
	Disconnect SFP module(Port-x).
	Indicates that SFP module was disconnected.
Error	Copied configuration 2 to 1
	Indicates that detected the configuration file 1 is broken, and was copied the configuration file 2 to 1.
	Copied configuration 1 to 2
	Indicates that detected the configuration file 2 is broken, and was copied the configuration file 1 to 2.
	Reset configuration 1 & 2 to default
	Indicates that detected the configuration file 1 and 2 is broken, and the configuration is initialized.
	Copy configuration 2 to 1 is failed
	Indicates that detected the configuration file 1 is broken, the copying the configuration file 2 to 1 is failed.
	Copy configuration 1 to 2 is failed
	Indicates that detected the configuration file 2 is broken, the copying the configuration file 1 to 2 is failed.
	Save of configuration 1 is failed
	Indicates that the saving to the configuration file 1 was failed.
	Save of configuration 2 is failed
	Indicates that the saving to the configuration file 2 was failed.
Info	Login from console.
	Indicates that the login operation was executed via console, and was successful.
	Login from telnet. (IP:xxx.xxx.xxx.xxx)
	Indicates a login from the host with IP address xxx.xxx.xxx.xxx via TELNET.
	Login from SSH (IP:xxx.xxx.xxx.xxx).

	Indicates a login from the host with IP address xxx.xxx.xxx.xxx via SSH.
Error	Login Failed from console.
	Indicates that the login operation was executed via console, and was failed.
	Login Failed from telnet(IP: xxx.xxx.xxx.xxx).
	Indicates that the login operation was executed via TELNET, and was failed.
	Login Failed from ssh(IP: xxx.xxx.xxx.xxx).
	Indicates that the login operation was executed via SSH, and was failed.
	Not authorized! (IP: xxx.xxx.xxx.xxx) .
	Indicates that the login operation was executed via TELNET or SSH, and was failed three times.
	Reject Telnet Access.
	Indicates that the loginf operation was executed via TELNET, and was rejected based on TELNET access limitation function.
	System authentication failure.
	Indicates that authentication from the SNMP manager failed.
Info	Set IP via ipsetup interface (IP:xxx.xxx.xxx.xxx)
	Indicates that IP address was set from the host with IP address xxx.xxx.xxx.xxx via IP setup interface function.
Error	Failed to set IP via ipsetup interface
	Indicates that IP address setting operation was executed via IP setup interface function, and was failed.
	IP setup interface timeout.
	Indicates that IP address setting operation was executed via IP setup interface function, and was failed. Because it takes over 20 minutes from booting.
Info	Console timeout.
	Indicates that console was time out.
	Telnet Timeout (IP: xxx.xxx.xxx.xxx).
	Indicates that telnet from the host with IP address xxx.xxx.xxx.xxx was timeout.
	SSH Timeout (IP: xxx.xxx.xxx.xxx).
	Indicates that SSH from the host with IP address xxx.xxx.xxx.xxx was timeout.
	Changed user name.
	Indicates that username was changed.
	Chagned password.
	Indicates that password was changed.
Error	CPU drop the packet. (xx Bytes)
	Indicates that the packet to CPU was dropped.

Info	Runtime code changes.
	Indicates that runtime code was changed.
	Configuration file download.
	Indicates that the receiving the configuration from TFTP server, and was applied to running-config.
	Configuration file upload.
	Indicates that the sending running-config to TFTP server.
	Configuration changed.
	Indicates that the configuration was saved.
	Reboot: Normal.
	Indicates that Switching Hub was rebooted.
	Reboot: Factory Default.
	Indicates that Switching Hub was rebooted in the mode to return all settings to the factory default.
	Reboot: Factory Default Except IP.
	Indicates that Switching Hub was rebooted in the mode to return settings other than IP address to the factory default.
	Start reboot timer (xxx sec)
	Indicates that started the reboot timer.
	Stop reboot timer
	Indicates that stopped the reboot timer.
	Cleared system log
	Indicates that System log was cleared.
Error	Watch dog timer is expired.
	Indicates that Watch dog timer was expired.
	Cannot write in Flash (addr: 0x0000000000)
	Indicates that cannot write in FLASH.
	Cannot read in Flash (addr: 0x0000000000)
	Indicates that cannot read in FLASH.
	Cannot access to temperature sensor.
	Indicates that cannot access to temperature sensor.
	System exception in thread:THREAD freeMem:FREE_MEM!
	System information indicating that exception handler is called in the Switching Hub. THREAD indicates the thread name, and FREE_MEM indicates the free memory capacity.
	Duplication of IP address: IP ADDRESS (MAC ADDRESS).
	Indicates that IP address of Switching Hub is already used and conflicting.
	Logout by user
	Indicates that connection via console was terminated by user.
	Logout by user(IP: IP ADDRESS).
	Indicates that connection via TELENT or SSH was terminated by user.

DDM		
Info	[DDM] {RX power|TX power|Temperature|Votage|Bias current} is {exceeded|recovered from} { High|Low} {Alarm|Warning} on Port-x.	
	Indicates that SFP module status was changed.	
	RX power	Indicates that SFP Rx power status was changed.
	TX power	Indicates that SFP Tx power status was changed..
	Temperature	Indicates that SFP temarature status was changed..
	Votage	Indicates that SFP voltage status was changed..
	Bias current	Indicates that SFP bias current status was changed..
	Exceeded	Indicates that SFP status exceeded the threshold.
	recovered from	Indicates that SFP status recovered from threshold.
	High	Indicates that upper limit.
	Low	Indicates that lower limit.
	Alarm	Indicates the alarm.
	Warning	Indicates the warning.

4.9.7. Watch Dog Timer Menu

On the Switch Tools Configuration Menu, pressing "W" opens the Watch Dog Timer Menu, as shown in Fig. 4-9-10. On this screen, you can enable/disable the Watch Dog Timer function.

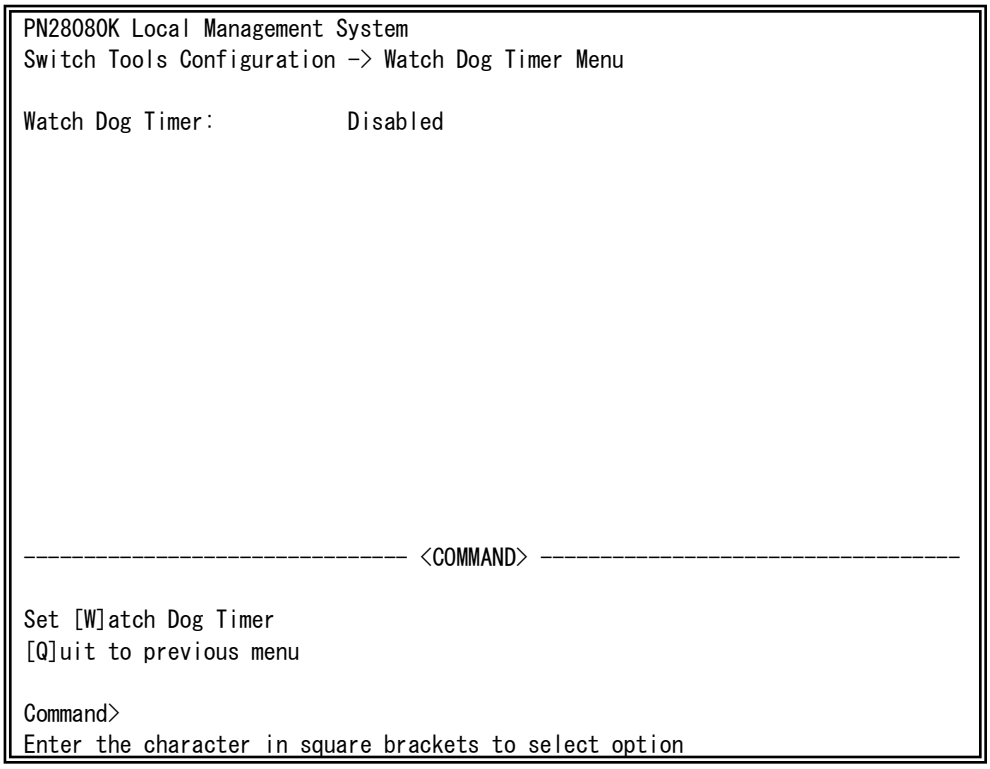


Fig. 4-9-10 Watch Dog Timer Menu

Screen Description

Watch Dog Timer	Shows the status of the Watch Dog Timer function. The factory default setting is "Disabled."	
	Enabled	The function is enabled.
	Disabled	The function is disabled.

Available commands are listed below.

W	Enable/disable the Watch Dog Timer function.	
		Press "W." The command prompt changes to "Enable or Disable Watch Dog Timer(E/D)>." Press "E" to enable the function. Press "D" to disable it.
Q	Return to the previous menu.	

4.10. Save Configuration to Flash

On the Main Menu, pressing "F" opens the Save Configuration to Flash screen, as shown in Fig. 4-10-1. Execute this command to save the Switching Hub configuration to the built-in memory. On this screen, the command prompt shows "Save current configuration?(Y/N)." Press "Y" to save the configuration. Press "N" to cancel it. If you don't save the configuration on this screen, it will be deleted when the system is rebooted or turned off.

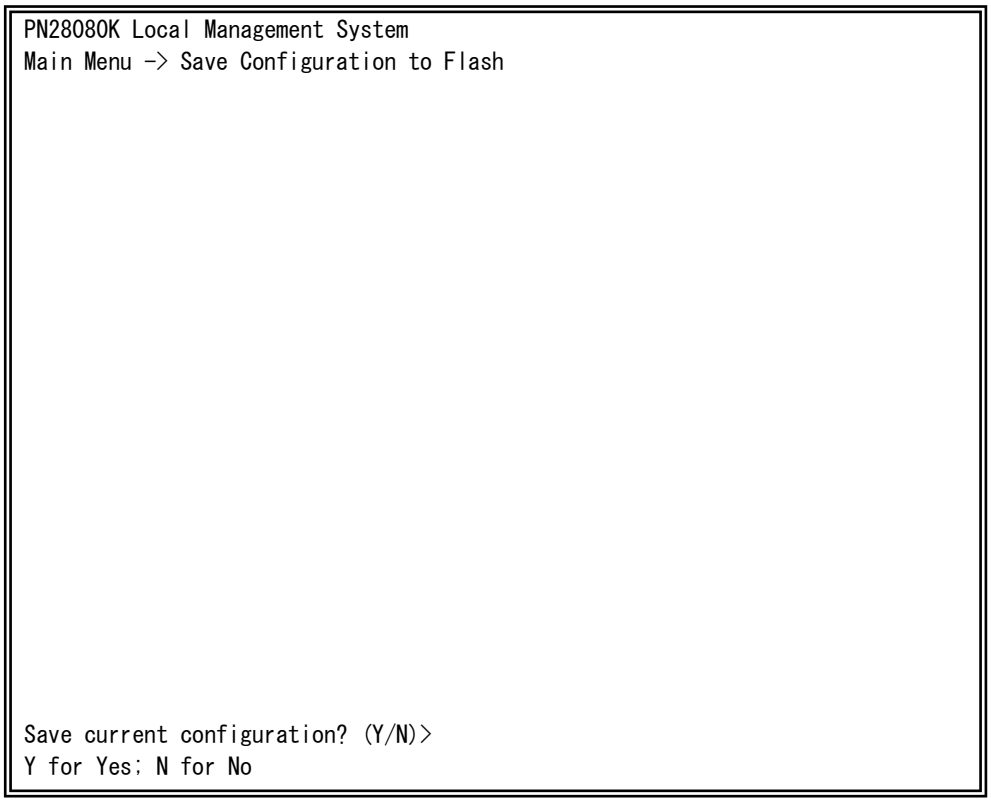


Fig. 4-10-1 Save Configuration to Flash screen: Confirmation to save

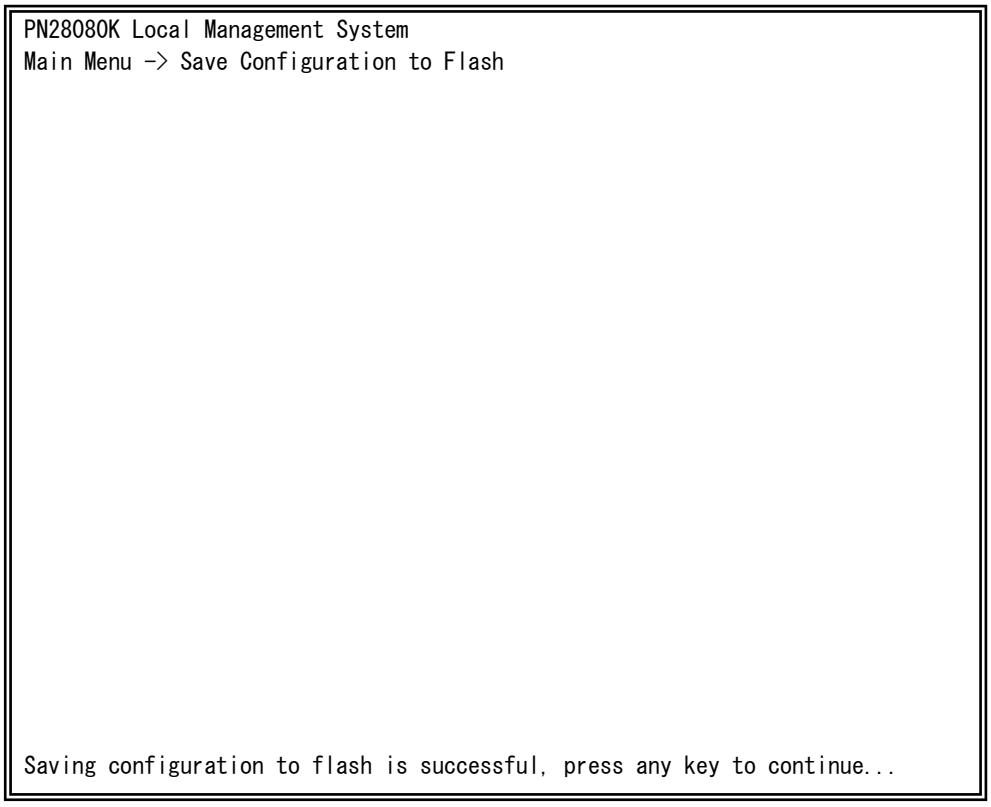


Fig. 4-10-2 Saving Configuration to Flash screen: Completion of save

4.11. Command Line Interface (CLI)

On the Main Menu, pressing "C" opens the screen shown in Fig. 4-11-1.
On this screen, you can use the command line for configuration instead of the menu screen. For configuration procedure, refer to the separate volume "Operation Manual (CLI)." Enter "logout" at the command prompt to return from CLI to menu screens.

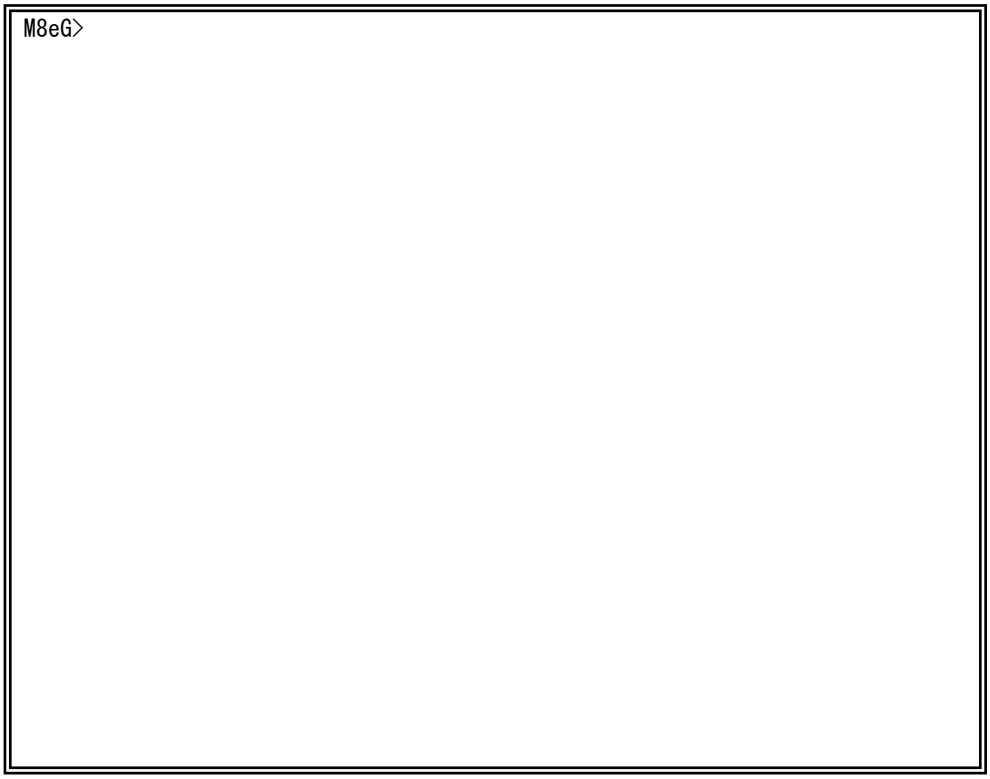


Fig. 4-11-1 Command Line Interface (CLI)

4.12. Logout

If you access from the console port, pressing "Q" on the Main Menu opens the login screen shown in Fig. 4-2-1. If you access using Telnet, pressing "Q" terminates the connection. To login again, follow the login procedures shown in the section 4.2. You are automatically logged out after a specified timeout period.

Appendix A. Specifications

○ Interface
- Twisted-pair port 1 - 8 (RJ45 connector)
  - ✧ Standards: IEEE 802.3 10BASE-T
    IEEE 802.3u 100BASE-TX
    IEEE 802.3ab 1000BASE-T

- SFP extension slot port 9 (*Select either of RF45 or SFP for use)
  - ✧ Standards: IEEE 802.3z
    1000BASE-SX/1000BASE-LX

- Console port x 1 (RJ45 connector)
  - ✧ RS-232C (ITU-TS V.24)

○ Switching functions
- Store and forward
- Forwarding rate: 10BASE-T: 14,880 pps
  100BASE-TX: 148,800 pps
  1000BASE-T/SFP: 1,488,000 pps
- MAC address table: 8K entries/unit
- Buffer memory: 512 KBytes
- Flow control: IEEE 802.3x (full duplex)
  Back pressure (half duplex)

○ Major functions
- IEEE 802.1Q: Tag VLAN (256 VLANS max.)
- IEEE 802.1p: QoS function(4 priority queues supported)
- IEEE 802.3x: Flow control
- Link aggregation: Configurable up to 8 ports and 4 groups
- Port monitoring: 1: n supported
- IEEE 802.1X: Port Based Access Control
  (EAP-MD5/TLS/PEAP)
- IEEE 802.3az: Energy Efficient Ethernet
  (Support LPI excluded 10BASE-Te)

○ Agent specifications
- SNMP v1 (RFC1157)
- SNMP v2c (RFC1901, RFC1908)
- SNMP v3 (RFC3411, RFC3414)
- TELNET (RFC854)
- TFTP (RFC783)
- SNTP v3 (RFC1769)
- SSH v2 (RFC4250, RFC4251, RFC4252, RFC4253, RFC4254)

○ Supported MIB
- MIB II (RFC1213)
  Not support “At”, “ipRouteTable”, “icmp”, “egp”.

- Bridge-MIB (RFC4188)
  Not support “dot1dStp”, “dot1dSr”, “dot1dStatic”.
- SNMPv2-MIB(RFC 1907)
- RMON-MIB(RFC 2819)
  Support etherStatsTable only.
- SNMP-FRAMEWORK-MIB(RFC 2571)
- SNMP-MPD-MIB(RFC 2572)
- SNMP-NOTIFICATION-MIB(RFC 2573N)
- SNMP-TARGET-MIB(RFC 2573T)
- SNMP-USER-BASED-SM-MIB(RFC 2574)
- SNMP-VIEW-BASED-ACM-MIB(RFC 2575)
- SNMP-COMMUNITY-MIB(RFC 2576)
- IP-MIB(RFC 4293)
- IF-MIB(RFC 2863)
- IEEE8021-PAE-MIB
  Not support dot1xPaeSupplicant.

○ Power supply specifications

- Power supply	AC 100-240 V, 50/60 Hz, 0.5 A
- Power consumption	Normally, max. 6.1 W, min. 2.6 W

○ Environment specifications

- Operating temperature	0 - 50°C
- Operating humidity	20 - 80% RH (no condensation)
- Storage temperature	-20 - 70°C
- Storage humidity	10 - 90% RH (no condensation)

○ External specifications

- Dimensions	44 mm (Height) × 210 mm (Width) × 130 mm (Depth)(Excluding the protruding sections)
- Mass (Weight)	1,100 g

Appendix B. Easy IP Address Setup Function

The following are points to note when using an easy IP address setup function.

[Known compatible software]
"ZEQUO assist" Ver.2.1.1.1

[User-settable items]
- *IP address, subnet mask and default gateway

[Restrictions]
- The time for accepting setting changes is limited to 20 minutes after power-on to ensure security.
  However, you can change settings regardless of the time limit if the IP address, subnet mask, default gateway, user name and password values are the factory defaults.
  * You can check the current settings because the list is displayed even after the time limit elapses.

Appendix C. Example of Network Configuration using Loop Detection Function and Its Precautions

Example of configuration using loop detection function

By using the loop detection function, you can prevent a loop failure that is likely to be caused in a downstream Switching Hub that the user directly uses.
In addition, if a downstream Switching Hub is connected with a device, such as a hub without loop detection function, and a loop failure occurs under the device, the downstream Switching Hub shuts down the corresponding port to prevent the failure from extending to the entire network.

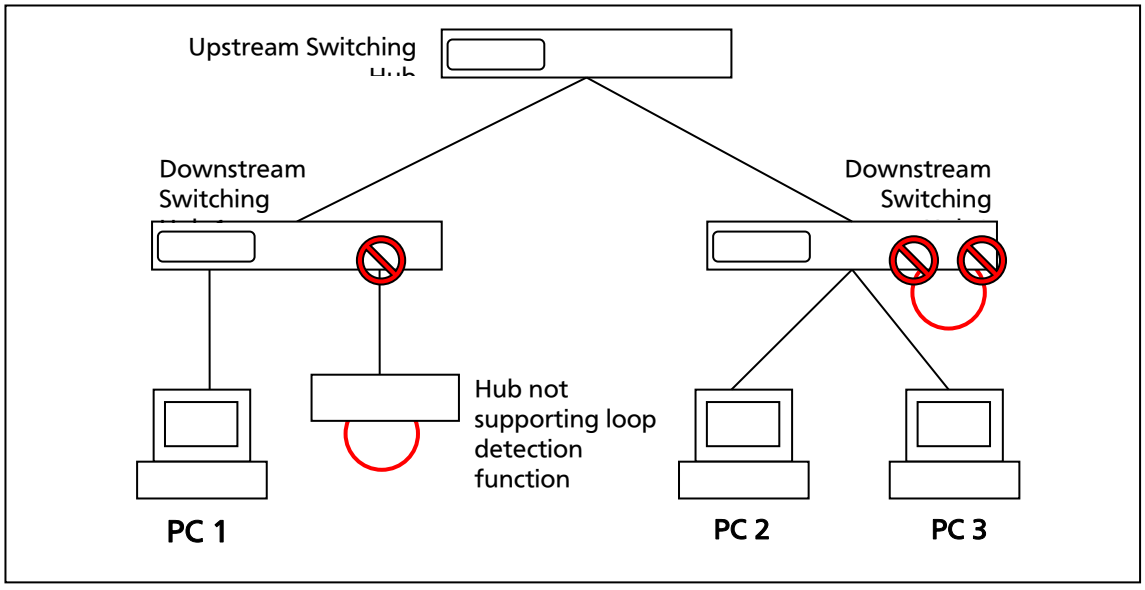
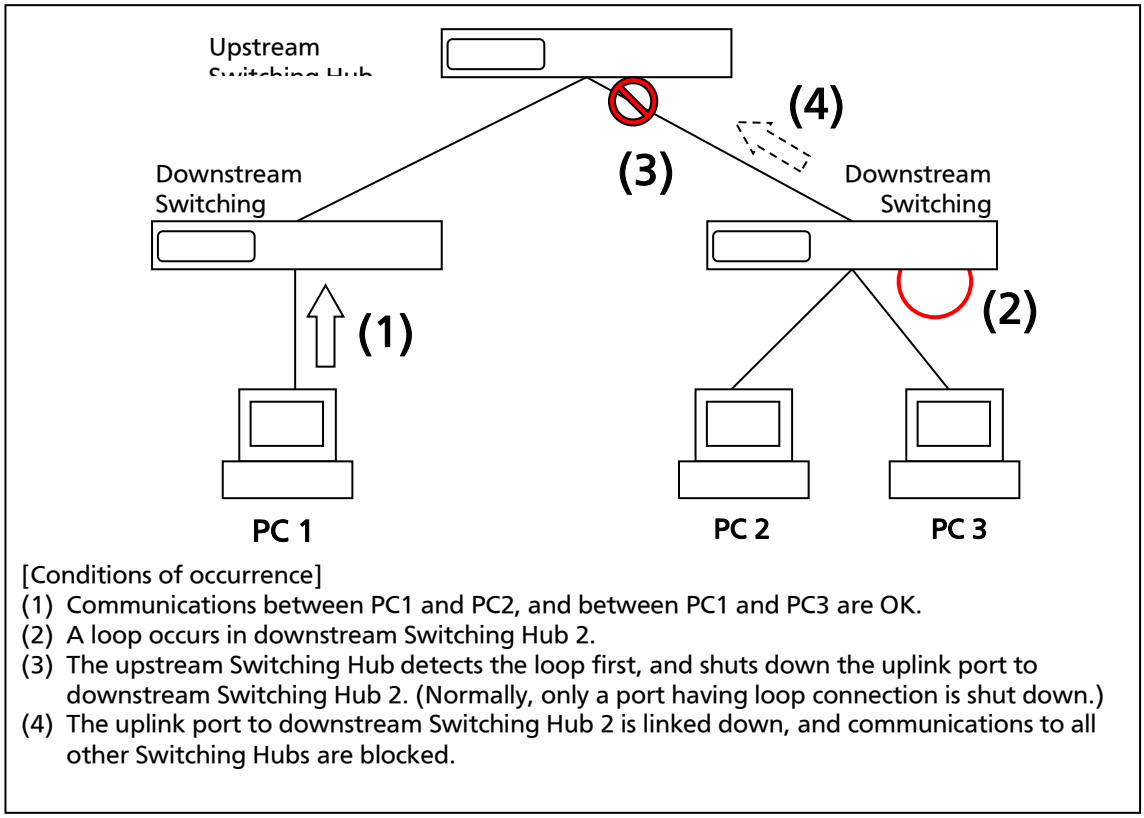


Fig. 1 Example of configuration using loop detection function

Precautions in using loop detection function
 - Disable loop detection at upstream port(s)

If a network is consisted of only Switching Hub equipped with loop detection function, an upstream Switching Hub may detect on ahead and block a loop occurred in a downstream Switching Hub. This may block all communications to the downstream Switching Hub. To minimize the communication failure by loop detection, disable the loop detection function of the upstream Switching Hub so that only a port of the Switching Hub causing loop will be blocked. You need to examine this type of network configuration and Switching Hub settings.



[Conditions of occurrence]
(1) Communications between PC1 and PC2, and between PC1 and PC3 are OK.
(2) A loop occurs in downstream Switching Hub 2.
(3) The upstream Switching Hub detects the loop first, and shuts down the uplink port to downstream Switching Hub 2. (Normally, only a port having loop connection is shut down.)
(4) The uplink port to downstream Switching Hub 2 is linked down, and communications to all other Switching Hubs are blocked.

Fig. 2 Precautions in using loop detection function

Appendix D. MIB List

The MIB list of this Switching Hub is as follows.

<port_num> is a port number.
<ip_address> is an IP address.
<ipv4IfIndex> is an ipv4InterfaceIfIndex.
<ipv6IfIndex> is an ipv6InterfaceIfIndex.
<ipSysVersion> is an ipSystemStatsIPVersion.
<etherIndex> is an etherStatsIndex.
<ipVersion> is an ipIfStatsIPVersion.
<ifIndex> is an ipIfStatsIfIndex.

1. SNMPv2 MIB (RFC1907) & MIB2 (RFC1213)

1.1.system

MIB object	Access	Identifier	Remarks
sysDescr	RO	sysDescr.0	
sysObjectID	RO	sysObjectID.0	
sysUpTime	RO	sysUpTimeInstance.0	
sysContact	R/W	sysContact.0	
sysName	R/W	sysName.0	
sysLocation	R/W	sysLocation.0	
sysServices	RO	sysServices.0	
sysORLastChange	RO	sysORLastChange.0	
sysORID	RO	sysORID.1	
sysORDescr	RO	sysORDescr.1	
sysORUpTime	RO	sysORUpTime.1	

1.2.TCP

MIB object	Access	Identifier	Remarks
tcpRtoAlgorithm	RO	tcpRtoAlgorithm.0	
tcpRtoMin	RO	tcpRtoMin.0	
tcpRtoMax	RO	tcpRtoMax.0	
tcpMaxConn	RO	tcpMaxConn.0	
tcpPassiveOpens	RO	tcpPassiveOpens.0	
tcpAttemptFails	RO	tcpAttemptFails.0	
tcpEstabResets	RO	tcpEstabResets.0	
tcpCurrEstab	RO	tcpCurrEstab.0	
tcpInSegs	RO	tcpInSegs.0	
tcpOutSegs	RO	tcpOutSegs.0	
tcpRetransSegs	RO	tcpRetransSegs.0	
tcpInErrs	RO	tcpInErrs.0	
tcpOutRsts	RO	tcpOutRsts.0	
tcpConnState	RO		
tcpConnLocalAddress	RO		
tcpConnLocalPort	RO		
tcpConnRemAddress	RO		
tcpConnRemPort	RO		

1.3.UDP

MIB object	Access	Identifier	Remarks
udpInDatagrams	RO	udpInDatagrams.0	
udpNoPorts	RO	udpNoPorts.0	
udpInErrors	RO	udpInErrors.0	
udpOutDatagrams	RO	udpOutDatagrams.0	
udpLocalAddress	RO		
udpLocalPort	RO		

1.4.SNMP

MIB object	Access	Identifier	Remarks
snmpInPkts	RO	snmpInPkts.0	
snmpOutPkts	RO	snmpOutPkts.0	
snmpInBadVersions	RO	snmpInBadVersions.0	
snmpInASNParseErrs	RO	snmpInASNParseErrs.0	
snmpInTotalReqVars	RO	snmpInTotalReqVars.0	
snmpInTotalSetVars	RO	snmpInTotalSetVars.0	
snmpInGetRequests	RO	snmpInGetRequests.0	
snmpInGetNexts	RO	snmpInGetNexts.0	
snmpInSetRequests	RO	snmpInSetRequests.0	
snmpInGetResponses	RO	snmpInGetResponses.0	
snmpInTraps	RO	snmpInTraps.0	
snmpOutGetResponses	RO	snmpOutGetResponses.0	
snmpOutTraps	RO	snmpOutTraps.0	
snmpEnableAuthenTraps	R/W	snmpEnableAuthenTraps.0	

2. IF MIB (RFC2863)

2.1.interfaces

MIB object	Access	Identifier	Remarks
ifNumber	RO	ifNumber.0	
ifIndex	RO	ifIndex.<port_num>	
ifDescr	RO	ifDescr.<port_num>	
ifType	RO	ifType.<port_num>	
ifMtu	RO	ifMtu.<port_num>	
ifSpeed	RO	ifSpeed.<port_num>	
ifPhysAddress	RO	ifPhysAddress.<port_num>	
ifAdminStatus	R/W	ifAdminStatus.<port_num>	
ifOperStatus	RO	ifOperStatus.<port_num>	
ifOLastChange	RO	ifOLastChange.<port_num>	
ifInOctets	RO	ifInOctets.<port_num>	
ifHCInOctets	RO	ifHCInOctets.<port_num>	
ifInUcastPkts	RO	ifInUcastPkts.<port_num>	
ifInNUcastPkts	RO	ifInNUcastPkts.<port_num>	
ifInDiscards	RO	ifInDiscards.<port_num>	
ifInErrors	RO	ifInErrors.<port_num>	
ifInUnknownProtos	RO	ifInUnknownProtos.<port_num>	
ifOutOctets	RO	ifOutOctets.<port_num>	
ifHCOutOctets	RO	ifHCOutOctets.<port_num>	

	ifOutUcastPkts	RO	ifOutUcastPkts.<port_num>	
	ifOutNUcastPkts	RO	ifOutNUcastPkts.<port_num>	
	ifOutDiscards	RO	ifOutDiscards.<port_num>	
	ifOutErrors	RO	ifOutErrors.<port_num>	
	ifOutQLen	RO	ifOutQLen.<port_num>	
	ifSpecific	RO	ifSpecific.<port_num>	

3. IP MIB (RFC4293)

3.1.IP				
	MIB object	**Access**	**Identifier**	**Remarks**
	ipForwarding	R/W	ipForwarding.0	
	ipDefaultTTL	R/W	ipDefaultTTL.0	
	ipInReceives	RO	ipInReceives.0	
	ipInHdrErrors	RO	ipInHdrErrors.0	
	ipInAddrErrors	RO	ipInAddrErrors.0	
	ipInUnknownProtos	RO	ipInUnknownProtos.0	
	ipInDiscards	RO	ipInDiscards.0	
	ipInDelivers	RO	ipInDelivers.0	
	ipOutRequests	RO	ipOutRequests.0	
	ipOutDiscards	RO	ipOutDiscards.0	
	ipOutNoRoutes	Ro	ipOutNoRoutes.0	
	ipReasmTomeout	RO	ipReasmTomeout	
	ipReasmReqds	RO	ipReasmReqds.0	
	ipReasmOKs	RO	ipReasmOKs.0	
	ipReasmFails	RO	ipReasmFails.0	
	ipFragOKs	RO	ipFragOKs.0	
	ipFragFails	RO	ipFragFails.0	
	ipFragCreates	RO	ipFragCreates.0	
3.2. ipAddrTable				
	MIB object	**Access**	**Identifier**	**Remarks**
	ipAdEntAddr	RO	ipAdEntAddr.<ip_address>	
	ipAdEntIfIndex	RO	ipAdEntIfIndex.<ip_address>	
	ipAdEntNetMask	RO	ipAdEntNetMask.<ip_address>	
	ipAdEntBcastAddr	RO	ipAdEntBcastAddr.<ip_address>	
	ipAdEntReasmMaxSize	RO	ipAdEntReasmMaxSize.<ip_address>	
3.3. ipNetToMediaTable				
	MIB object	**Access**	**Identifier**	**Remarks**
	ipNetToMediaIfIndex	RO	ipNetToMediaIfIndex.<ip_address>	
	ipNetToMediaPhysAddress	RO	ipNetToMediaPhysAddress.<ip_address>	
	ipNetToMediaNetAddress	RO	ipNetToMediaNetAddress.<ip_address>	
	ipNetToMediaType	RO	ipNetToMediaType.<ip_address>	
3.4.				
	MIB object	**Access**	**Identifier**	**Remarks**
	ipRoutingDiscards	RO	ipRoutingDiscards.0	
	ipv6IpForwarding	R/W	ipv6IpForwarding.0	
	ipv6IpDefaultHopLimit	R/W	ipv6IpDefaultHopLimit.0	

	ipv4InterfaceTableLastChange	RO	ipv4InterfaceTableLastChange.0	
3.5.ipv4InterfaceTable				
	MIB object	**Access**	**Identifier**	**Remarks**
	ipv4InterfaceReasmMaxSize	RO	ipv4InterfaceReasmMaxSize.<ipv4IfIndex>	
	ipv4InterfaceEnableStatus	R/W	ipv4InterfaceEnableStatus.<ipv4Index>	
	ipv4InterfaceRetransmitTime	RO	ipv4InterfaceRetransmitTime.<ipv4IfIndex>	
3.6.				
	MIB object	**Access**	**Identifier**	**Remarks**
	ipv6InterfaceTableLastChange	RO	ipv6InterfaceTableLastChange.0	
3.7.ipv6InterfaceTable				
	MIB object	**Access**	**Identifier**	**Remarks**
	ipv6InterfaceReasmMaxSize	RO	ipv6InterfaceReasmMaxSize.<ipv6IfIndex>	
	ipv6InterfaceIdentifier	RO	ipv6InterfaceIdentifier.<ipv6IfIndex>	
	ipv6InterfaceEnableStatus	R/W	ipv6InterfaceEnableStatus.<ipv6IfIndex>	
	ipv6InterfaceReachableTime	RO	ipv6InterfaceReachableTime.<ipv6IfIndex>	
	ipv6InterfaceRetransmitTime	RO	ipv6InterfaceRetransmitTime.<ipv6IfIndex>	
	ipv6InterfaceForwarding	R/W	ipv6InterfaceForwarding.<ipv6IfIndex>	
3.8.ipSystemStatsTable				
	MIB object	**Access**	**Identifier**	**Remarks**
	ipSystemStatsInReceives	RO	ipSystemStatsInReceives.< ipSysVersion>	
	ipSystemStatsHCInReceives	RO	ipSystemStatsHCInReceives.< ipSysVersion>	
	ipSystemStatsInOctets	RO	ipSystemStatsInOctets.< ipSysVersion>	
	ipSystemStatsHCInOctets	RO	ipSystemStatsHCInOctets.< ipSysVersion>	
	ipSystemStatsInHdrErrors	RO	ipSystemStatsInHdrErrors.< ipSysVersion>	
	ipSystemStatsInNoRoutes	RO	ipSystemStatsInNoRoutes.< ipSysVersion>	
	ipSystemStatsInAddrErrors	RO	ipSystemStatsInAddrErrors.< ipSysVersion>	
	ipSystemStatsInUnknownProtos	RO	ipSystemStatsInUnknownProtos.< ipSysVersion>	
	ipSystemStatsInTruncatedPkts	RO	ipSystemStatsInTruncatedPkts.< ipSysVersion>	
	ipSystemStatsInForwDatagrams	RO	ipSystemStatsInForwDatagrams.< ipSysVersion>	
	ipSystemStatsHCInForwDatagrams	RO	ipSystemStatsHCInForwDatagrams.< ipSysVersion>	
	ipSystemStatsReasmReqds	RO	ipSystemStatsReasmReqds.< ipSysVersion>	
	ipSystemStatsReasmOKs	RO	ipSystemStatsReasmOKs.< ipSysVersion>	
	ipSystemStatsReasmFails	RO	ipSystemStatsReasmFails.< ipSysVersion>	
	ipSystemStatsInDiscards	RO	ipSystemStatsInDiscards.< ipSysVersion>	
	ipSystemStatsInDelivers	RO	ipSystemStatsInDelivers.< ipSysVersion>	
	ipSystemStatsHCInDelivers	RO	ipSystemStatsHCInDelivers.< ipSysVersion>	
	ipSystemStatsOutRequests	RO	ipSystemStatsOutRequests.< ipSysVersion>	
	ipSystemStatsHCOutRequests	RO	ipSystemStatsHCOutRequests.< ipSysVersion>	
	ipSystemStatsOutNoRoutes	RO	ipSystemStatsOutNoRoutes.< ipSysVersion>	
	ipSystemStatsOutForwDatagrams	RO	ipSystemStatsOutForwDatagrams.< ipSysVersion>	
	ipSystemStatsHCOutForwDatagrams	RO	ipSystemStatsHCOutForwDatagrams.< ipSysVersion>	
	ipSystemStatsOutDiscards	RO	ipSystemStatsOutDiscards.< ipSysVersion>	

	ipSystemStatsOutFragReqds	RO	ipSystemStatsOutFragReqds.< ipSysVersion>	
	ipSystemStatsOutFragOKs	RO	ipSystemStatsOutFragOKs.< ipSysVersion>	
	ipSystemStatsOutFragFails	RO	ipSystemStatsOutFragFails.< ipSysVersion>	
	ipSystemStatsOutFragCreates	RO	ipSystemStatsOutFragCreates.< ipSysVersion>	
	ipSystemStatsOutTransmits	RO	ipSystemStatsOutTransmits.< ipSysVersion>	
	ipSystemStatsHCOutTransmits	RO	ipSystemStatsHCOutTransmits.< ipSysVersion>	
	ipSystemStatsOutOctets	RO	ipSystemStatsOutOctets.< ipSysVersion>	
	ipSystemStatsHCOutOctets	RO	ipSystemStatsHCOutOctets.< ipSysVersion>	
	ipSystemStatsInMcastPkts	RO	ipSystemStatsInMcastPkts.< ipSysVersion>	
	ipSystemStatsHCInMcastPkts	RO	ipSystemStatsHCInMcastPkts.< ipSysVersion>	
	ipSystemStatsInMcastOctets	RO	ipSystemStatsInMcastOctets.< ipSysVersion>	
	ipSystemStatsHCInMcastOctets	RO	ipSystemStatsHCInMcastOctets.< ipSysVersion>	
	ipSystemStatsOutMcastPkts	RO	ipSystemStatsOutMcastPkts.< ipSysVersion>	
	ipSystemStatsHCOutMcastPkts	RO	ipSystemStatsHCOutMcastPkts.< ipSysVersion>	
	ipSystemStatsOutMcastOctets	RO	ipSystemStatsOutMcastOctets.< ipSysVersion>	
	ipSystemStatsHCOutMcastOctets	RO	ipSystemStatsHCOutMcastOctets.< ipSysVersion>	
	ipSystemStatsInBcastPkts	RO	ipSystemStatsInBcastPkts.< ipSysVersion>	
	ipSystemStatsHCInBcastPkts	RO	ipSystemStatsHCInBcastPkts.< ipSysVersion>	
	ipSystemStatsOutBcastPkts	RO	ipSystemStatsOutBcastPkts.< ipSysVersion>	
	ipSystemStatsHCOutBcastPkts	RO	ipSystemStatsHCOutBcastPkts.< ipSysVersion>	
	ipSystemStatsDiscontinuityTime	RO	ipSystemStatsDiscontinuityTime.< ipSysVersion>	
	ipSystemStatsRefreshRate	RO	ipSystemStatsRefreshRate.< ipSysVersion>	
3.9.				
	MIB object	**Access**	**Identifier**	**Remarks**
	ipIfStatsTableLastChange	RO	ipIfStatsTableLastChange.0	
3.10. ipIfStatsTable				
	MIB object	**Access**	**Identifier**	**Remarks**
	ipIfStatsInReceives	RO	ipIfStatsInReceives.<ipVersion>.<IfIndex>	
	ipIfStatsHCInReceives	RO	ipIfStatsHCInReceives.<ipVersion>.<IfIndex>	
	ipIfStatsInOctets	RO	ipIfStatsInOctets.<ipVersion>.<IfIndex>	
	ipIfStatsHCInOctets	RO	ipIfStatsHCInOctets.<ipVersion>.<IfIndex>	
	ipIfStatsInHdrErrors	RO	ipIfStatsInHdrErrors.<ipVersion>.<IfIndex>	
	ipIfStatsInNoRoutes	RO	ipIfStatsInNoRoutes.<ipVersion>.<IfIndex>	
	ipIfStatsInAddrErrors	RO	ipIfStatsInAddrErrors.<ipVersion>.<IfIndex>	
	ipIfStatsInUnknownProtos	RO	ipIfStatsInUnknownProtos.<ipVersion>.<IfIndex>	
	ipIfStatsInTruncatedPkts	RO	ipIfStatsInTruncatedPkts.<ipVersion>.<IfIndex>	
	ipIfStatsInForwDatagrams	RO	ipIfStatsInForwDatagrams.<ipVersion>.<IfIndex>	
	ipIfStatsHCInForwDatagrams	RO	ipIfStatsHCInForwDatagrams.<ipVersion>.<IfIndex>	
	ipIfStatsReasmReqds	RO	ipIfStatsReasmReqds.<ipVersion>.<IfIndex>	
	ipIfStatsReasmOKs	RO	ipIfStatsReasmOKs.<ipVersion>.<IfIndex>	
	ipIfStatsReasmFails	RO	ipIfStatsReasmFails.<ipVersion>.<IfIndex>	
	ipIfStatsInDiscards	RO	ipIfStatsInDiscards.<ipVersion>.<IfIndex>	
	ipIfStatsInDelivers	RO	ipIfStatsInDelivers.<ipVersion>.<IfIndex>	
	ipIfStatsHCInDelivers	RO	ipIfStatsHCInDelivers.<ipVersion>.<IfIndex>	

	ipIfStatsOutRequests	RO	ipIfStatsOutRequests.<ipVersion>.<IfIndex>	
	ipIfStatsHCOutRequests	RO	ipIfStatsHCOutRequests.<ipVersion>.<IfIndex>	
	ipIfStatsOutForwDatagrams	RO	ipIfStatsOutForwDatagrams.<ipVersion>.<IfIndex>	
	ipIfStatsHCOutForwDatagrams	RO	ipIfStatsHCOutForwDatagrams.<ipVersion>.<IfIndex>	
	ipIfStatsOutDiscards	RO	ipIfStatsOutDiscards.<ipVersion>.<IfIndex>	
	ipIfStatsOutFragReqds	RO	ipIfStatsOutFragReqds.<ipVersion>.<IfIndex>	
	ipIfStatsOutFragOKs	RO	ipIfStatsOutFragOKs.<ipVersion>.<IfIndex>	
	ipIfStatsOutFragFails	RO	ipIfStatsOutFragFails.<ipVersion>.<IfIndex>	
	ipIfStatsOutFragCreates	RO	ipIfStatsOutFragCreates.<ipVersion>.<IfIndex>	
	ipIfStatsOutTransmits	RO	ipIfStatsOutTransmits.<ipVersion>.<IfIndex>	
	ipIfStatsHCOutTransmits	RO	ipIfStatsHCOutTransmits.<ipVersion>.<IfIndex>	
	ipIfStatsOutOctets	RO	ipIfStatsOutOctets.<ipVersion>.<IfIndex>	
	ipIfStatsHCOutOctets	RO	ipIfStatsHCOutOctets.<ipVersion>.<IfIndex>	
	ipIfStatsInMcastPkts	RO	ipIfStatsInMcastPkts.<ipVersion>.<IfIndex>	
	ipIfStatsHCInMcastPkts	RO	ipIfStatsHCInMcastPkts.<ipVersion>.<IfIndex>	
	ipIfStatsInMcastOctets	RO	ipIfStatsInMcastOctets.<ipVersion>.<IfIndex>	
	ipIfStatsHCInMcastOctets	RO	ipIfStatsHCInMcastOctets.<ipVersion>.<IfIndex>	
	ipIfStatsOutMcastPkts	RO	ipIfStatsOutMcastPkts.<ipVersion>.<IfIndex>	
	ipIfStatsHCOutMcastPkts	RO	ipIfStatsHCOutMcastPkts.<ipVersion>.<IfIndex>	
	ipIfStatsOutMcastOctets	RO	ipIfStatsOutMcastOctets.<ipVersion>.<IfIndex>	
	ipIfStatsHCOutMcastOctets	RO	ipIfStatsHCOutMcastOctets.<ipVersion>.<IfIndex>	
	ipIfStatsInBcastPkts	RO	ipIfStatsInBcastPkts.<ipVersion>.<IfIndex>	
	ipIfStatsHCInBcastPkts	RO	ipIfStatsHCInBcastPkts.<ipVersion>.<IfIndex>	
	ipIfStatsOutBcastPkts	RO	ipIfStatsOutBcastPkts.<ipVersion>.<IfIndex>	
	ipIfStatsHCOutBcastPkts	RO	ipIfStatsHCOutBcastPkts.<ipVersion>.<IfIndex>	
	ipIfStatsDiscontinuityTime	RO	ipIfStatsDiscontinuityTime.<ipVersion>.<IfIndex>	
	ipIfStatsRefreshRate	RO	ipIfStatsRefreshRate.<ipVersion>.<IfIndex>	

4. Bridge MIB (RFC4188)

4.1.dot1dBase

	MIB object	Access	Identifier	Remarks
	dot1dBaseBridgeAddress	RO	dot1dBaseBridgeAddress.0	
	dot1dBaseBridgeAddress	RO	dot1dBaseBridgeAddress.0	
	dot1dBaseNumPorts	RO	dot1dBaseNumPorts.0	
	dot1dBaseType	RO	dot1dBaseType.0	
	dot1dBasePort	RO	dot1dBasePort.<port_num>	
	dot1dBasePortIfIndex	RO	dot1dBasePortIfIndex.<port_num>	
	dot1dBasePortCircuit	RO	dot1dBasePortCircuit.<port_num>	
	dot1dBasePortDelayExceededDiscards	RO	dot1dBasePortDelayExceededDiscards.<port_num>	
	dot1dBasePortMtuExceeded Discards	RO	dot1dBasePortMtuExceededDiscards.<port_num>	

4.2.dot1dTp

	MIB object	Access	Identifier	Remarks
	dot1dTpLearnedEntryDiscards	RO	dot1dTpLearnedEntryDiscards.0	
	dot1dTpAgingTime	R/W	dot1dTpAgingTime.0	
	dot1dTpFdbAddress	RO		

	dot1dTpFdbPort	RO		
	dot1dTpFdbStatus	RO		
	dot1dTpPort	RO	dot1dTpPort.<port_num>	
	dot1dTpPortMaxInfo	RO	dot1dTpPortMaxInfo.<port_num>	
	dot1dTpPortInFrames	RO	dot1dTpPortInFrames.<port_num>	
	dot1dTpPortOutFrames	RO	dot1dTpPortOutFrames.<port_num>	
	dot1dTpPortInDiscards	RO	dot1dTpPortInDiscards.<port_num>	

5. IEEE8021PAE MIB

5.1.dot1xPaeSystem

	MIB object	Access	Identifier	Remarks
	dot1xPaeSystemAuthControl	R/W	dot1xPaeSystemAuthControl.0	

5.2.dot1xPaePortTable

	MIB object	Access	Identifier	Remarks
	dot1xPaePortProtocolVersion	RO	dot1xPaePortProtocolVersion.<port_num>	
	dot1xPaePortCapabilities	RO	dot1xPaePortCapabilities.<port_num>	
	dot1xPaePortInitialize	R/W	dot1xPaePortInitialize.<port_num>	
	dot1xPaePortReauthenticate	R/W	dot1xPaePortReauthenticate.<port_num>	

5.3.dot1xAuthConfigTable

	MIB object	Access	Identifier	Remarks
	dot1xAuthPaeState	RO	dot1xAuthPaeState.<port_num>	
	dot1xAuthBackendAuthState	RO	dot1xAuthBackendAuthState.<port_num>	
	dot1xAuthAdminControlledDirections	R/W	dot1xAuthAdminControlledDirections.<port_num>	
	dot1xAuthOperControlledDirections	RO	dot1xAuthOperControlledDirections.<port_num>	
	dot1xAuthAuthControlledPortStatus	RO	dot1xAuthAuthControlledPortStatus.<port_num>	
	dot1xAuthAuthControlledPortControl	R/W	dot1xAuthAuthControlledPortControl.<port_num>	
	dot1xAuthQuietPeriod	R/W	dot1xAuthQuietPeriod.<port_num>	
	dot1xAuthTxPeriod	R/W	dot1xAuthTxPeriod.<port_num>	
	dot1xAuthSuppTimeout	R/W	dot1xAuthSuppTimeout.<port_num>	
	dot1xAuthServerTimeout	R/W	dot1xAuthServerTimeout.<port_num>	
	dot1xAuthMaxReq	R/W	dot1xAuthMaxReq.<port_num>	
	dot1xAuthReAuthPeriod	R/W	dot1xAuthReAuthPeriod.<port_num>	
	dot1xAuthReAuthEnabled	R/W	dot1xAuthReAuthEnabled.<port_num>	
	dot1xAuthKeyTxEnabled	R/W	dot1xAuthKeyTxEnabled.<port_num>	

5.4.dot1xAuthStatsTable

	MIB object	Access	Identifier	Remarks
	dot1xAuthEapolFramesRx	RO	dot1xAuthEapolFramesRx.<port_num>	
	dot1xAuthEapolFramesTx	RO	dot1xAuthEapolFramesTx.<port_num>	
	dot1xAuthEapolStartFramesRx	RO	dot1xAuthEapolStartFramesRx.<port_num>	
	dot1xAuthEapolLogoffFramesRx	RO	dot1xAuthEapolLogoffFramesRx.<port_num>	
	dot1xAuthEapolRespIdFramesRx	RO	dot1xAuthEapolRespIdFramesRx.<port_num>	
	dot1xAuthEapolRespFramesRx	RO	dot1xAuthEapolRespFramesRx.<port_num>	
	dot1xAuthEapolReqIdFramesTx	RO	dot1xAuthEapolReqIdFramesTx.<port_num>	

	dot1xAuthEapolReqFramesTx	RO	dot1xAuthEapolReqFramesTx.<port_num>	
	dot1xAuthInvalidEapolFramesRx	RO	dot1xAuthInvalidEapolFramesRx.<port_num>	
	dot1xAuthEapLengthErrorFramesRx	RO	dot1xAuthEapLengthErrorFramesRx.<port_num>	
	dot1xAuthLastEapolFrameVersion	RO	dot1xAuthLastEapolFrameVersion.<port_num>	
	dot1xAuthLastEapolFrameSource	RO	dot1xAuthLastEapolFrameSource.<port_num>	

5.5.dot1xAuthDiagTable

	MIB object	Access	Identifier	Remarks
	dot1xAuthEntersConnecting	RO	dot1xAuthEntersConnecting.<port_num>	
	dot1xAuthEapLogoffsWhileConnecting	RO	dot1xAuthEapLogoffsWhileConnecting.<port_num>	
	dot1xAuthEntersAuthenticating	RO	dot1xAuthEntersAuthenticating.<port_num>	
	dot1xAuthAuthSuccessWhileAuthenticating	RO	dot1xAuthAuthSuccessWhileAuthenticating.<port_num>	
	dot1xAuthAuthTimeoutsWhileAuthenticating	RO	dot1xAuthAuthTimeoutsWhileAuthenticating.<port_num>	
	dot1xAuthAuthFailWhileAuthenticating	RO	dot1xAuthAuthFailWhileAuthenticating.<port_num>	
	dot1xAuthAuthReauthsWhileAuthenticating	RO	dot1xAuthAuthReauthsWhileAuthenticating.<port_num>	
	dot1xAuthAuthEapStartsWhileAuthenticating	RO	dot1xAuthAuthEapStartsWhileAuthenticating.<port_num>	
	dot1xAuthAuthEapLogoffWhileAuthenticating	RO	dot1xAuthAuthEapLogoffWhileAuthenticating.<port_num>	
	dot1xAuthAuthReauthsWhileAuthenticated	RO	dot1xAuthAuthReauthsWhileAuthenticated.<port_num>	
	dot1xAuthAuthEapStartsWhileAuthenticated	RO	dot1xAuthAuthEapStartsWhileAuthenticated.<port_num>	
	dot1xAuthAuthEapLogoffWhileAuthenticated	RO	dot1xAuthAuthEapLogoffWhileAuthenticated.<port_num>	
	dot1xAuthBackendResponses	RO	dot1xAuthBackendResponses.<port_num>	
	dot1xAuthBackendAccessChallenges	RO	dot1xAuthBackendAccessChallenges.<port_num>	
	dot1xAuthBackendOtherRequestsToSupplicant	RO	dot1xAuthBackendOtherRequestsToSupplicant.<port_num>	
	dot1xAuthBackendNonNakResponsesFromSupplicant	RO	dot1xAuthBackendNonNakResponsesFromSupplicant.<port_num>	
	dot1xAuthBackendAuthSuccesses	RO	dot1xAuthBackendAuthSuccesses.<port_num>	
	dot1xAuthBackendAuthFails	RO	dot1xAuthBackendAuthFails.<port_num>	

5.6.dot1xAuthSessionStatsTable

	MIB object	Access	Identifier	Remarks
	dot1xAuthSessionOctetsRx	RO	dot1xAuthSessionOctetsRx.<port_num>	
	dot1xAuthSessionOctetsTx	RO	dot1xAuthSessionOctetsTx.<port_num>	
	dot1xAuthSessionFramesRx	RO	dot1xAuthSessionFramesRx.<port_num>	
	dot1xAuthSessionFramesTx	RO	dot1xAuthSessionFramesTx.<port_num>	
	dot1xAuthSessionId	RO	dot1xAuthSessionId.<port_num>	
	dot1xAuthSessionAuthenticMethod	RO	dot1xAuthSessionAuthenticMethod.<port_num>	
	dot1xAuthSessionTime	RO	dot1xAuthSessionTime.<port_num>	

	dot1xAuthSessionTerminateCause	RO	dot1xAuthSessionTerminateCause.<port_num>	
	dot1xAuthSessionUserName	RO	dot1xAuthSessionUserName.<port_num>	

6. RMON framework MIB (RFC2819)

6.1.etherStatsTable				
	MIB object	**Access**	**Identifier**	**Remarks**
	etherStatsIndex	RO	etherStatsIndex.<etherIndex>	
	etherStatsDataSource	R/C	etherStatsDataSource.<etherIndex>	
	etherStatsDropEvents	RO	etherStatsDropEvents.<etherIndex>	
	etherStatsOctets	RO	etherStatsOctets.<etherIndex>	
	etherStatsPkts	RO	etherStatsPkts.<etherIndex>	
	etherStatsBroadcastPkts	RO	etherStatsBroadcastPkts.<etherIndex>	
	etherStatsMulticastPkts	RO	etherStatsMulticastPkts.etherIndex>	
	etherStatsCRCAlignErrors	RO	etherStatsCRCAlignErrors.<etherIndex>	
	etherStatsUndersizePkts	RO	etherStatsUndersizePkts.<etherIndex>	
	etherStatsOversizePkts	RO	etherStatsOversizePkts.<etherIndex>	
	etherStatsFragments	RO	etherStatsFragments.<etherIndex>	
	etherStatsJabbers	RO	etherStatsJabbers.<etherIndex>	
	etherStatsCollisions	RO	etherStatsCollisions.<etherIndex>	
	etherStatsPkts64Octets	RO	etherStatsPkts64Octets.<etherIndex>	
	etherStatsPkts65to127Octets	RO	etherStatsPkts65to127Octets.<etherIndex>	
	etherStatsPkts128to255Octets	RO	etherStatsPkts128to255Octets.<etherIndex>	
	etherStatsPkts256to511Octets	RO	etherStatsPkts256to511Octets.<etherIndex>	
	etherStatsPkts512to1023Octets	RO	etherStatsPkts512to1023Octets.<etherIndex>	
	etherStatsPkts1024to1518Octets	RO	etherStatsPkts1024to1518Octets.<etherIndex>	
	etherStatsOwner	R/C	etherStatsOwner.<etherIndex>	
	etherStatsStatus	R/C	etherStatsStatus.<etherIndex>	

7. SNMP framework MIB (RFC2571)

7.1.snmpFrameworkAdmin				
	MIB object	**Access**	**Identifier**	**Remarks**
	usmNoAuthProtocol	-	(ObjectID: 1.3.6.1.6.3.10.1.1.1)	
	usmHMACMD5AuthProtocol	-	(ObjectID: 1.3.6.1.6.3.10.1.1.2)	
	usmHMACSHAAuthProtocol	-	(ObjectID: 1.3.6.1.6.3.10.1.1.3)	
	usmNoPrivProtocol	-	(ObjectID: 1.3.6.1.6.3.10.1.2.1)	
	usmDESPrivProtocol	-	(ObjectID: 1.3.6.1.6.3.10.1.2.2)	
7.2.snmpEngine				
	MIB object	**Access**	**Identifier**	**Remarks**
	snmpEngineID	RO	snmpEngineID.0	
	snmpEngineBoots	RO	snmpEngineBoots.0	
	snmpEngineTime	RO	snmpEngineTime.0	
	snmpEngineMaxMessageSize	RO	snmpEngineMaxMessageSize.0	

8. SNMP MPD MIB (RFC2572)

8.1.

MIB object	Access	Identifier	Remarks
snmpUnknownSecurityModels	RO	snmpUnknownSecurityModels.0	
snmpInvalidMsgs	RO	snmpInvalidMsgs.0	
snmpUnknownPDUHandlers	RO	snmpUnknownPDUHandlers.0	

9. SNMP notification MIB (RFC2573n)

9.1.

MIB object	Access	Identifier	Remarks
snmpNotifyTag	R/C	snmpNotifyTag.notify	
snmpNotifyType	R/C	snmpNotifyType.notify	
snmpNotifyStorageType	R/C	snmpNotifyStorageType.notify	
snmpNotifyRowStatus	R/C	snmpNotifyRowStatus.notify	

10. SNMP target MIB (RFC2573t)

10.1.

MIB object	Access	Identifier	Remarks
snmpTargetSpinLock	R/W	snmpTargetSpinLock.0	
snmpTargetAddrTDomain	R/C	snmpTargetAddrTDomain.<snmp_host_name>	
snmpTargetAddrTAddress	R/C	snmpTargetAddrTAddress.<snmp_host_name>	
snmpTargetAddrTimeout	R/C	snmpTargetAddrTimeout.<snmp_host_name>	
snmpTargetAddrRetryCount	R/C	snmpTargetAddrRetryCount.<snmp_host_name>	
snmpTargetAddrTagList	R/C	snmpTargetAddrTagList.<snmp_host_name>	
snmpTargetAddrParams	R/C	snmpTargetAddrParams.<snmp_host_name>	
snmpTargetAddrStorageType	R/C	snmpTargetAddrStorageType.<snmp_host_name>	
snmpTargetAddrRowStatus	R/C	snmpTargetAddrRowStatus.<snmp_host_name>	
snmpTargetParamsMPModel	R/C	snmpTargetParamsMPModel.<snmp_host_name>	
snmpTargetParamsSecurityModel	R/C	snmpTargetParamsSecurityModel.<snmp_host_name>	
snmpTargetParamsSecurityName	R/C	snmpTargetParamsSecurityName.<snmp_host_name>	
snmpTargetParamsSecurityLevel	R/C	snmpTargetParamsSecurityLevel.<snmp_host_name>	
snmpTargetParamsStorageType	R/C	snmpTargetParamsStorageType.<snmp_host_name>	
snmpTargetParamsRowStatus	R/C	snmpTargetParamsRowStatus.<snmp_host_name>	
snmpUnavailableContexts	RO	snmpUnavailableContexts.0	
snmpUnknownContexts	RO	snmpUnknownContexts.0	

11. SNMP USM MIB (RFC2574)

11.1. usmStats

MIB object	Access	Identifier	Remarks
usmStatsUnsupportedSecLevels	RO	usmStatsUnsupportedSecLevels.0	
usmStatsNotInTimeWindows	RO	usmStatsNotInTimeWindows.0	
usmStatsUnknownUserNames	RO	usmStatsUnknownUserNames.0	
usmStatsUnknownEngineIDs	RO	usmStatsUnknownEngineIDs.0	
usmStatsWrongDigests	RO	usmStatsWrongDigests.0	
usmStatsDecryptionErrors	RO	smStatsDecryptionErrors.0	

11.2. usmUser

MIB object	Access	Identifier	Remarks
usmUserSpinLock	R/W	usmUserSpinLock.0	
usmUserSecurityName	RO	usmUserSecurityName.<snmp_user_name>	
usmUserCloneFrom	R/C	usmUserCloneFrom.<snmp_user_name>	
usmUserAuthProtocol	R/C	usmUserAuthProtocol.<snmp_user_name>	
usmUserAuthKeyChange	R/C	usmUserAuthKeyChange.<snmp_user_name>	
usmUserOwnAuthKeyChange	R/C	usmUserOwnAuthKeyChange.<snmp_user_name>	
usmUserPrivProtocol	R/C	usmUserPrivProtocol.<snmp_user_name>	
usmUserPrivKeyChange	R/C	usmUserPrivKeyChange.<snmp_user_name>	
usmUserOwnPrivKeyChange	R/C	usmUserOwnPrivKeyChange.<snmp_user_name>	
usmUserPublic	R/C	usmUserPublic.<snmp_user_name>	
usmUserStorageType	R/C	usmUserStorageType.<snmp_user_name>	
usmUserStatus	R/C	usmUserStatus.<snmp_user_name>	

12. SNMP VACM MIB (RFC2575)

12.1.

MIB object	Access	Identifier	Remarks
vacmContextName	RO	vacmContextName.<snmp_group_name>	
vacmGroupName	R/C	vacmGroupName.<snmp_group_name>	
vacmSecurityToGroupStorageType	R/C	vacmSecurityToGroupStorageType.<snmp_group_name>	
vacmSecurityToGroupStatus	R/C	vacmSecurityToGroupStatus.<snmp_group_name>	
vacmAccessContextMatch	R/C	vacmAccessContextMatch.<snmp_group_name>	
vacmAccessReadViewName	R/C	vacmAccessReadViewName.<snmp_group_name>	
vacmAccessWriteViewName	R/C	vacmAccessWriteViewName.<snmp_group_name>	
vacmAccessNotifyViewName	R/C	vacmAccessNotifyViewName.<snmp_group_name>	
vacmAccessStorageType	R/C	vacmAccessStorageType.<snmp_group_name>	
vacmAccessStatus	R/C	vacmAccessStatus.<snmp_group_name>	

12.2.vacmMIBViews

MIB object	Access	Identifier	Remarks
vacmViewSpinLock	R/W	vacmViewSpinLock.0	
vacmViewTreeFamilyMask	R/C	vacmViewTreeFamilyMask.<snmp_view_name>	
vacmViewTreeFamilyType	R/C	vacmViewTreeFamilyType.<snmp_view_name>	
vacmViewTreeFamilyStorageType	R/C	vacmViewTreeFamilyStorageType.<snmp_view_name>	
vacmViewTreeFamilyStatus	R/C	vacmViewTreeFamilyStatus.<snmp_view_name>	

13. SNMP community (RFC2576)

13.1.

MIB object	Access	Identifier	Remarks
snmpCommunityName	R/C	snmpCommunityName.<snmp_community_name>	
snmpCommunitySecurityName	R/C	snmpCommunitySecurityName.<snmp_community_name>	
snmpCommunityContextEngineID	R/C	snmpCommunityContextEngineID.<snmp_community_name>	
snmpCommunityContextName	R/C	snmpCommunityContextName.<snmp_community_name>	

	snmpCommunityTransportTag	R/C	snmpCommunityTransportTag .<snmp_community_name>	
	snmpCommunityStorageType	R/C	snmpCommunityStorageType .<snmp_community_name>	
	snmpCommunityStatus	R/C	snmpCommunityStatus. <snmp_community_name>	
	snmpTargetAddrTMask	R/C	snmpTargetAddrTMask. <snmp_community_name>	
	snmpTargetAddrMMS	R/C	snmpTargetAddrMMS. <snmp_community_name>	
	snmpTrapAddress	Accessible-for-notify	snmpTrapAddress.0	
	snmpTrapCommunity	Accessible-for-notify	snmpTrapCommunity.0	

14. Traps

14.1.				
	Trap description	**Access**	**Identifier**	**Remarks**
	Cold Start			
	Link up/Down			
	Login Failure			
	Authentication Failure			
	mnoBusAccessErrorNotification		ObjectID: 1.3.6.1.4.1.396.5.5.1.6	
	mnoLoopDetection		ObjectID: 1.3.6.1.4.1.396.5.5.2.1	
	mnoLoopRecovery		ObjectID: 1.3.6.1.4.1.396.5.5.2.2	
	mnoDdmAlarmTrap		ObjectID: 1.3.6.1.4.1.396.5.5.1.4.0.1	
	mnoDdmWarningTrap		ObjectID: 1.3.6.1.4.1.396.5.5.1.4.0.2	

Panasonic Electric Works Networks Co.,Ltd.

2-12-7, Higashi-Shimbashi, Minato-ku, Tokyo Japan, 105-0021

URL: https://panasonic.co.jp/ew/pewnw/english/

P0316-10042