MITSUBISHI ELECTRIC

Programmable Controller

CC-Link IE TSN Industrial Managed Ethernet Switch User's Manual

-NZ2MHG-TSNT8F2
-NZ2MHG-TSNT4

Powered by MOXA®

The managed switch was jointly developed and manufactured by Mitsubishi Electric and Moxa inc.

*Note that the warranty on this product differs from that on other programmable controller products.
(Refer to "WARRANTY" in this manual.)

COPYRIGHT

PRECAUTIONS REGARDING WARRANTY AND SPECIFICATIONS

The managed switch was jointly developed and manufactured by Mitsubishi Electric Corporation and Moxa Inc. Thus, warranty information is different from that of other MELSEC products. For inquiries and service, our response may take some time, depending on the contents or the time we have received the inquiries.

- Warranty

Item	Managed switch	Other programmable controller products (e.g. MELSEC iQ-R series)
Gratis warranty term	36 months after delivery or 60 months after produced, whichever is less.	36 months after delivery or 42 months after produced
Repair term after discontinuation of production	5 years	7 years
Service not covered by the warranty	Replacement with a new product (charged)	Repair (charged)

- Applicable standards

Item	Managed switch	Other programmable controller products (e.g. MELSEC iQ-R series)
EMC standard	EN 61000-6-2 EN 61000-6-4 EN 55032 EN 55035	EN 61131-2
Vibration resistance	IEC 60068-2-6	IEC 61131-2
Shock resistance	IEC 60068-2-27	IEC 61131-2

SAFETY PRECAUTIONS

(Read these precautions before using this product.)

Before using this product, please read this manual and the relevant manuals carefully and pay full attention to safety to handle the product correctly.

The precautions given in this manual are concerned with this product only. For the safety precautions of the programmable controller system, refer to the user's manual for the CPU module used.

In this manual, the safety precautions are classified into two levels: "⚠WARNING" and "⚠CAUTION".

⚠ WARNING	Indicates that incorrect handling may cause hazardous conditions, resulting in death or severe injury.
⚠ CAUTION	Indicates that incorrect handling may cause hazardous conditions, resulting in minor or moderate injury or property damage.

Under some circumstances, failure to observe the precautions given under "⚠CAUTION" may lead to serious consequences.

Observe the precautions of both levels because they are important for personal and system safety.

Make sure that the end users read this manual and then keep the manual in a safe place for future reference.

[Design Precautions]

⚠CAUTION

- The values of link speed at the transfer rate described in this manual (such as 1000Mbps) are the theoretical maximum values of the wired LAN standards. They are not the actual data transfer speed.
- Frame loss may occur depending on the connected external devices or installation environment.

[Security Precautions]

⚠WARNING

- To maintain the security (confidentiality, integrity, and availability) of the programmable controller and the system against unauthorized access, denial-of-service (DoS) attacks, computer viruses, and other cyberattacks from external devices via the network, take appropriate measures such as firewalls, virtual private networks (VPNs), and antivirus solutions.

[Installation Precautions]

⚠WARNING

- Shut off the external power supply (all phases) used in the system before installing or removing the module. Failure to do so may result in electric shock or cause the module to fail or malfunction.
- The module may become very hot during the setting and operation. Lock the control panel so that only qualified maintenance personnel can access the module. When installing/removing the module, take a measure to prevent a burn and be sure that the module is not very hot.

[Installation Precautions]

⚠CAUTION

- Use the module in an environment that meets Page 16 General Specifications in this manual. Failure to do so may result in electric shock, fire, malfunction, or damage to or deterioration of the product.
- Do not directly touch any conductive parts and electronic components of the module or connectors. Doing so can cause malfunction or failure of the module.
- Securely fix the module with a DIN rail or module mounting bracket.
- Securely connect the cable connectors. Poor contact may cause malfunction.
- MicroSD memory cards cannot be used. Do not insert it to the slot. Doing so may cause malfunction.
- Install the product according to the methods described in Page 25 INSTALLATION AND WIRING in this manual. Failure to do so may result in electric shock, fire, malfunction, or damage to or deterioration of the product.
- Tighten the screws within the specified torque range. Undertightening can cause drop of the component or wire, short circuit, or malfunction. Overtightening can damage the screw and/or module, resulting in drop, short circuit, or malfunction.
- Use a provided connector and console cable only. Failure to do so may result in electric shock, fire, malfunction, or damage to or deterioration of the product.
- Ground the power used to supply the power to the module. Failure to do so may result in electric shock or malfunction.
- Use a module mounting bracket that is allowed for the module fixing. If a bracket other than that is used, proper fixing of the module is not guaranteed.

[Wiring Precautions]

⚠WARNING

- Shut off the external power supply (all phases) used in the system before wiring. Failure to do so may result in electric shock or cause the module to fail or malfunction.
- To supply the power to the module, use the reinforced insulation power supply that is UL-certified, does not generate hazardous voltage of 60V or higher, and satisfies the following: the safety extra-low voltage (SELV) circuit requirements, the limited power source (LPS) requirements. Be sure that the power supply used satisfies the specifications required. Failure to do so may result in electric shock or cause the module to fail or malfunction.
- When an overcurrent caused by a failure of an external device or a module flows for a long time, it may cause smoke and fire. To prevent this, configure an external safety circuit, such as a fuse.

[Precautions for using the NZ2MHG-TSNT8F2]

- The optical transmitter and receiver of the SFP module, which is to be connected to the SFP ports, use laser diodes (class 1 in accordance with IEC 60825-1/JIS C6802). Do not look directly at a laser beam when using the SFP module. Doing so may harm your eyes.

[Wiring Precautions]

⚠CAUTION

- Individually ground the FG terminal of the programmable controller with a ground resistance of 100 ohms or less. Failure to do so may result in electric shock or malfunction.
- Before wiring to the module, check the rated voltage and terminal layout of the module, and connect the cables correctly. Connecting a power supply with a different voltage rating or incorrect wiring may cause a fire or failure.
- Tighten the terminal block screws within the specified torque range. Undertightening can cause short circuit, fire, or malfunction. Overtightening can damage the screw and/or module, resulting in drop, short circuit, fire, or malfunction.
- Place the cables in a duct or clamp them. If not, dangling cable may swing or inadvertently be pulled, resulting in damage to the module or cables or malfunction due to poor contact.
- Do not install the control lines or communication cables together with the main circuit lines or power cables. Keep a distance of 100mm or more between them. Failure to do so may result in malfunction due to noise.
- When disconnecting the cable from the module, do not pull the cable by the cable part. For the cable with connector, hold the connector part of the cable. Pulling the cable connected to the module may result in malfunction or damage to the module or cable.
- Prevent foreign matter such as dust or wire chips from entering the module. Such foreign matter can cause a fire, failure, or malfunction.
- Check the interface type and correctly connect the cable. Incorrect wiring (connecting the cable to an incorrect interface) may cause failure of the module and external device.
- The product must be installed in control panels. Wiring and replacement of a module must be performed by qualified maintenance personnel with knowledge of protection against electric shock. For wiring methods, refer to Page 25 INSTALLATION AND WIRING in this manual.
- For Ethernet cables to be used in the system, select the ones that meet the specifications in the user's manual for the module used. If not, normal data transmission is not guaranteed.
- Ground the power used to supply the power to the module. Failure to do so may result in electric shock or malfunction.

[Precautions for using the NZ2MHG-TSNT8F2]

- Attach a provided cover to unused SFP ports. Touching the port with bare hands may result in injury.
- When using the SFP ports, select an SFP module and an optical fiber cable that are connectable to the ports, and use them in the system. If an unconnectable product is used for wiring, normal data transmission is not guaranteed.

[Startup and Maintenance Precautions]

⚠WARNING

- Do not touch any terminal while power is on. Doing so will cause electric shock or malfunction.
- Shut off the external power supply (all phases) used in the system before cleaning the module, retightening the terminal block screws or connector screws. Failure to do so may cause the module to fail or malfunction.
- The module may become very hot. Lock the control panel so that only qualified maintenance personnel can access the module. When installing/removing the module, take a measure to prevent a burn and be sure that the module is not very hot.

[Startup and Maintenance Precautions]

⚠CAUTION

- Do not disassemble or modify the modules. Doing so may cause failure, malfunction, injury, or a fire.
- Shut off the external power supply (all phases) used in the system before installing or removing the module. Failure to do so may cause the module to fail or malfunction.
- Use any radio communication device such as a cellular phone or PHS (Personal Handy-phone System) more than 25cm away in all directions from the module. Failure to do so may cause malfunction.
- After the first use of the product, do not connect/remove the terminal block more than 50 times. Exceeding the limit may cause malfunction.
- Before handling the module or cables to the module, touch a conducting object such as a grounded metal to discharge the static electricity from the human body. Failure to do so may cause the module to fail or malfunction.
- Startup and maintenance of a control panel must be performed by qualified maintenance personnel with knowledge of protection against electric shock. In addition, lock the control panel so that only qualified maintenance personnel can operate it.
- Use a clean and dry cloth to wipe off dirt on the module.

[Disposal Precautions]

⚠CAUTION

- When disposing of this product, treat it as industrial waste.

[Transportation Precautions]

⚠CAUTION

- The halogens (such as fluorine, chlorine, bromine, and iodine), which are contained in a fumigant used for disinfection and pest control of wood packaging materials, may cause failure of the product. Prevent the entry of fumigant residues into the product or consider other methods (such as heat treatment) instead of fumigation. The disinfection and pest control measures must be applied to unprocessed raw wood.

CONDITIONS OF USE FOR THE PRODUCT

(1) MELSEC programmable controller ("the PRODUCT") shall be used in conditions;

i) where any problem, fault or failure occurring in the PRODUCT, if any, shall not lead to any major or serious accident; and

ii) where the backup and fail-safe function are systematically or automatically provided outside of the PRODUCT for the case of any problem, fault or failure occurring in the PRODUCT.

(2) The PRODUCT has been designed and manufactured for the purpose of being used in general industries.

MITSUBISHI ELECTRIC SHALL HAVE NO RESPONSIBILITY OR LIABILITY (INCLUDING, BUT NOT LIMITED TO ANY AND ALL RESPONSIBILITY OR LIABILITY BASED ON CONTRACT, WARRANTY, TORT, PRODUCT LIABILITY) FOR ANY INJURY OR DEATH TO PERSONS OR LOSS OR DAMAGE TO PROPERTY CAUSED BY the PRODUCT THAT ARE OPERATED OR USED IN APPLICATION NOT INTENDED OR EXCLUDED BY INSTRUCTIONS, PRECAUTIONS, OR WARNING CONTAINED IN MITSUBISHI ELECTRIC USER'S, INSTRUCTION AND/OR SAFETY MANUALS, TECHNICAL BULLETINS AND GUIDELINES FOR the PRODUCT.

("Prohibited Application")

Prohibited Applications include, but not limited to, the use of the PRODUCT in;

- Nuclear Power Plants and any other power plants operated by Power companies, and/or any other cases in which the public could be affected if any problem or fault occurs in the PRODUCT.
- Railway companies or Public service purposes, and/or any other cases in which establishment of a special quality assurance system is required by the Purchaser or End User.
- Aircraft or Aerospace, Medical applications, Train equipment, transport equipment such as Elevator and Escalator, Incineration and Fuel devices, Vehicles, Manned transportation, Equipment for Recreation and Amusement, and Safety devices, handling of Nuclear or Hazardous Materials or Chemicals, Mining and Drilling, and/or other applications where there is a significant risk of injury to the public or property.

Notwithstanding the above restrictions, Mitsubishi Electric may in its sole discretion, authorize use of the PRODUCT in one or more of the Prohibited Applications, provided that the usage of the PRODUCT is limited only for the specific applications agreed to by Mitsubishi Electric and provided further that no special quality assurance or fail-safe, redundant or other safety features which exceed the general specifications of the PRODUCTs are required. For details, please contact the Mitsubishi Electric representative in your region.

(3) Mitsubishi Electric shall have no responsibility or liability for any problems involving programmable controller trouble and system trouble caused by DoS attacks, unauthorized access, computer viruses, and other cyberattacks.

INTRODUCTION

Thank you for purchasing the CC-Link IE TSN industrial managed Ethernet switch (hereafter abbreviated as managed switch).

This manual describes the specifications, procedures before operation, system configuration, installation, wiring, parameter settings, functions, and troubleshooting of the managed switch.

Before using this product, please read this manual carefully and develop familiarity with the functions and performance of the managed switch to handle the product correctly.

Note that the menu names and operating procedures may differ depending on an operating system in use and its version.

When reading this manual, replace the names and procedures with the applicable ones as necessary.

Please make sure that the end users read this manual.

Relevant product

NZ2MHG-TSNT8F2, NZ2MHG-TSNT4

CONTENTS

CHAPTER 9 MAINTENANCE AND INSPECTION 254

CHAPTER 10 TROUBLESHOOTING 256

APPENDICES 263

INDEX 403

RELEVANT MANUALS

Manual name [manual number]	Description	Available form
CC-Link IE TSN Industrial Managed Ethernet Switch User's Manual [SH-082449ENG] (this manual)	Specifications, procedures before operation, system configuration, installation and wiring, parameter settings, functions, and troubleshooting of the managed switch	Print book e-Manual PDF

Point

e-Manual refers to the Mitsubishi Electric FA electronic book manuals that can be browsed using a dedicated tool.

e-Manual has the following features:

- Required information can be cross-searched in multiple manuals.
- Other manuals can be accessed from the links in the manual.
- The hardware specifications of each part can be found from the product figures.
- Pages that users often browse can be bookmarked.

TERMS

Unless otherwise specified, this manual uses the following terms.

Term	Description
CC-Link IE Field Network	A high-speed and large-capacity open field network that is based on Ethernet (1000BASE-T)
CC-Link IE TSN Class[*1]	A group of devices and switching hubs compatible with CC-Link IE TSN, classified according to the functions and performance by the CC-Link Partner Association. For the CC-Link IE TSN Class, refer to the CC-Link IE TSN Installation Manual (BAP-C3007ENG-001) published by the CC-Link Partner Association.
Engineering tool	A tool used for setting up programmable controllers, programming, debugging, and maintenance
Grandmaster	A source device or station to synchronize clocks in the time synchronization via PTP (Precision Time Protocol)

*1 The term has been changed for standardization among manuals and software applications related to CC-Link IE TSN. However, the term used in some CC-Link IE TSN related software windows may remain unchanged and may be different from the term used in this manual.
In case of inconsistency, refer to the following.

Term used in software window	Term after change
Authentication Class	CC-Link IE TSN Class

GENERIC TERMS AND ABBREVIATIONS

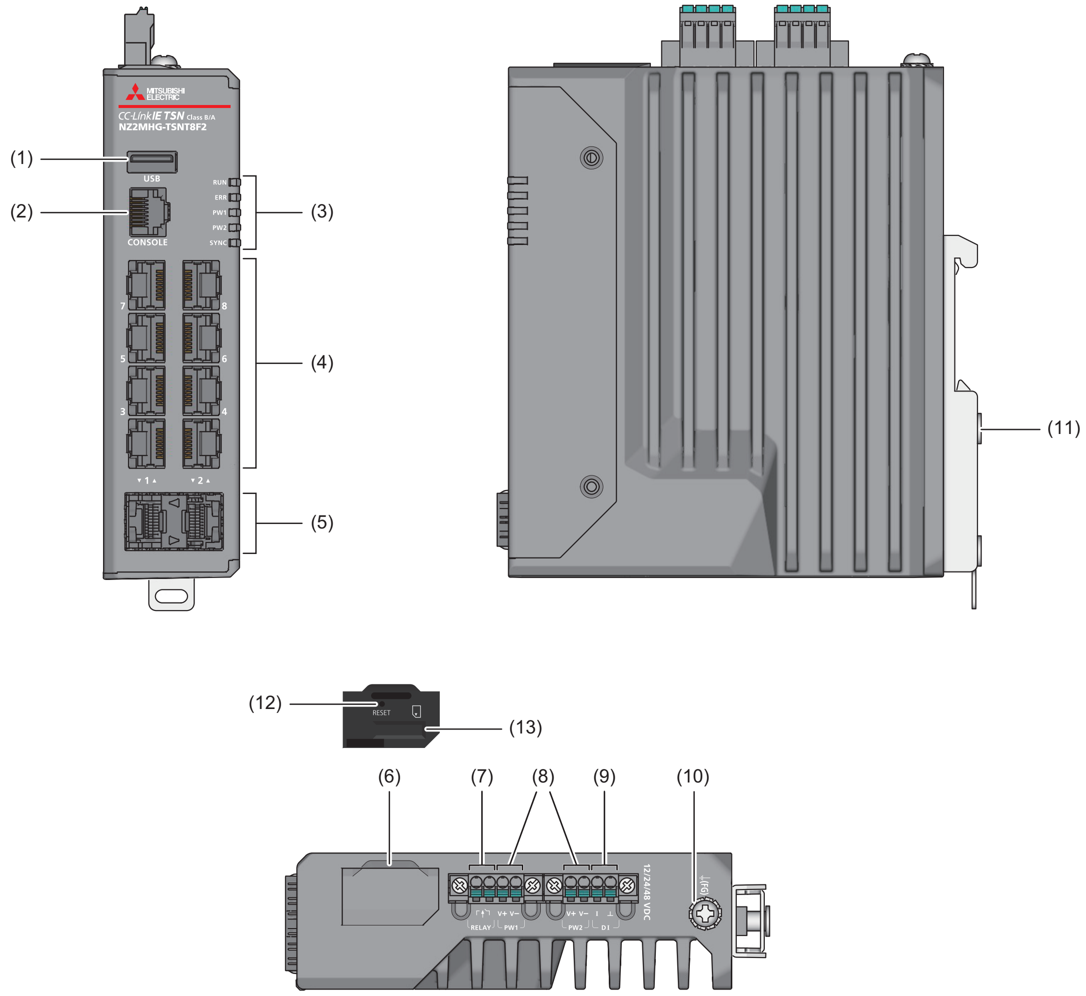
Unless otherwise specified, this manual uses the following generic terms and abbreviations.

Generic term and abbreviation	Description
CSR	An abbreviation for Certificate Signing Request. This signature request is required for issuing an SSL server certificate to a certificate authority.
DHCP	An abbreviation for Dynamic Host Configuration Protocol. This protocol is used to automatically allocate the IP address, subnet mask, and DNS server address in response to the request from the DHCP client.
FTP	An abbreviation for File Transfer Protocol. This predefined protocol is used to transfer data files over a network.
LLDP	An abbreviation for Link Layer Discovery Protocol. This protocol is used to detect and manage the connection of devices connected to a network. This protocol is standardized in IEEE 802.1ab.
MIB	An abbreviation for Management Information Base. A set of data that summarizes the settings and statuses of the device to be monitored, which is used when remotely monitoring and managing devices using a protocol such as SNMP. This data set is also a standard that defines the formats and reference methods.
NTP	An abbreviation for Network Time Protocol. This protocol is used to acquire clock data from a single server to precisely adjust the time of network devices.
OID	An abbreviation for Object Identifier. An identifier used to distinguish individual pieces of information (objects) stored in the MIB.
PCP	An abbreviation for Priority Code Point. The priority of frame relay defined in IEEE 802.1p.
PTP	An abbreviation for Precision Time Protocol. A predefined protocol for time synchronization between devices on a network.
RADIUS	An abbreviation for Remote Authentication Dial In User Service. This predefined protocol is used to authenticate a user, give authority, and record the status of use on a network.
RSTP	An abbreviation for Rapid Spanning Tree Protocol. This protocol is used to speed up the convergence time when changing topology from STP. This protocol is standardized in IEEE 802.1w.
SFD	An abbreviation for Start Frame Delimiter. This bit string is used to identify the start of a frame.
SNMP	An abbreviation for Simple Network Management Protocol. This protocol is used to monitor and control network devices on the IP network.
SNTP	An abbreviation for Simple Network Time Protocol. This protocol is used to acquire clock data from a single server to precisely adjust the time of network devices.
STP	An abbreviation for Spanning Tree Protocol. This predefined protocol for data link layer is used to prevent loop configurations on the LAN. This protocol is standardized in IEEE 802.1D.
SSH	An abbreviation for Secure Shell. This protocol (or virtual terminal software) is used on the TCP/IP network to safely log in to and operate a personal computer from a remote location by encryption.
SSL	An abbreviation for Secure Sockets Layer. This function is used for encrypting data communications between a web browser and a web server.
TACACS+	An abbreviation for Terminal Access Controller Access Control System Plus. This predefined protocol is used to authenticate a user, give authority, and record the status of use on a network.
TCP/IP	An abbreviation for Transmission Control Protocol/Internet Protocol. One of the predefined protocols.
Telnet	This protocol (or virtual terminal software) is used on the TCP/IP network to log in to and operate a personal computer from a remote location.
UDP/IP	An abbreviation for User Datagram Protocol/Internet Protocol. One of the predefined protocols.
UTC	An abbreviation for Coordinated Universal Time. A time standard to which a leap second is applied to keep the time close to GMT (Greenwich Mean Time).
VLAN	An abbreviation for Virtual Local Area Network. This virtual LAN is built by the managed switch in addition to the physical LAN.
VLAN ID	This ID number is added to each port for the VLAN function setting.
Managed switch	A generic term for CC-Link IE TSN Class B switching hubs authorized by the CC-Link Partner Association

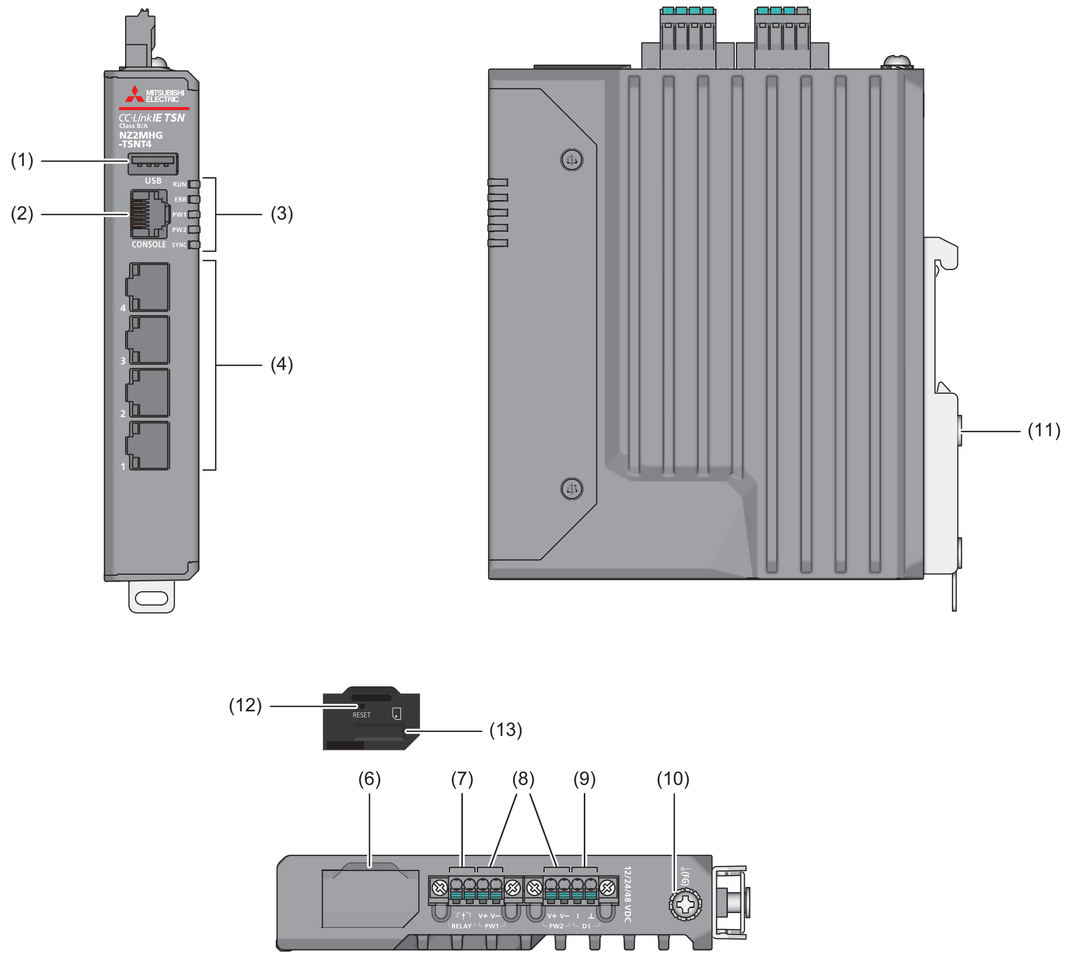
1 PART NAMES

This chapter describes the names of each part of the managed switch.

- NZ2MHG-TSNT8F2



- NZ2MHG-TSNT4



No.	Name	Description
(1)	USB port	A USB connector to connect a USB flash drive (connectable product)
(2)	Console port	An RJ45 connector for connecting with the personal computer with the console cable
(3)	RUN LED	Indicates the operating status of the managed switch. • On (green): Normal operation[*1] • Flashing (green) (500ms interval): The reset button is pressed and held. • Flashing (green) (250ms interval): Normally operating (with a USB flash drive connected) • Flashing (red): Initializing • Off: Power-off
	ERR LED	Indicates the module error status. • On (red): An initial error has occurred or access to the USB flash drive has failed. • Off: No error
	PW1 LED	Indicates the power supply status of power supply 1. • On: Power-on • Off: Power-off
	PW2 LED	Indicates the power supply status of power supply 2. • On: Power-on • Off: Power-off
	SYNC LED	Indicates the time synchronization status. • On (orange): Operating as the time synchronization master • On (green): Operating as the time synchronization slave • Flashing (orange): Initializing the time synchronization processing, or in the time synchronization unstable state[*2] • Off: The time synchronization function disabled

No.	Name		Description
(4)	Ethernet port	Ethernet ports 1 to 8[*3]	Connect an Ethernet cable. For wiring methods and wiring precautions, refer to the following. ☞ Page 33 Wiring to Ethernet ports
		1Gbps LINK LED (Upper)	Indicates the link status. • On (green): Link-up (1Gbps) • Flashing (green): Data being sent (1Gbps) • Off: Link-down
		100Mbps/10Mbps LINK LED (Lower)	Indicates the link status. • On (orange): Link-up (100Mbps/10Mbps) • Flashing (orange): Data being sent (100Mbps/10Mbps) • Off: Link-down
(5)[*4]	Optical fiber port	SFP ports 1, 2	Attach an SFP module, and connect an optical fiber cable. For wiring methods and wiring precautions, refer to the following. ☞ Page 35 Wiring to optical fiber ports
		1Gbps/100Mbps LINK LED	Indicates the link status and data sending status. • On (green): Link-up (1Gbps) • On (orange): Link-up (100Mbps) • Flashing (green): Data being sent (1Gbps) • Flashing (orange): Data being sent (100Mbps) • Off: Link-down
(6)	Rubber cover		A cover that protects the microSD card slot and reset button
(7)	Relay output terminal (RELAY)		A terminal for relay output Can be used as the external output for event notification.
(8)	Power input terminal (PW1/PW2)		A terminal for power supply connection
(9)	Digital input terminal (DI)		A terminal for digital input Can be used as a trigger for event notification.
(10)	FG connection screw		A screw for FG connection
(11)	DIN rail mounting kit		Metal fittings for mounting on the DIN rail
(12)	Reset button		A button to restart or initialize the configurations • To restart: Press the button and release it immediately. • To initialize the configurations: Press and hold the button for five seconds before release.
(13)	microSD memory card slot		The microSD memory card slot cannot be used. Do not insert a microSD memory card into the slot. Doing so may cause malfunction.

[*1] Since USB flash drive connection is supported in firmware versions "05" and later, those firmware versions take longer from power-on until the RUN LED turns on green compared firmware versions "04" or earlier. The time to enable the Ethernet port does not change.

[*2] The time correction amount from the grandmaster (Offset from Master) exceeds the Accuracy Alert.

[*3] For the NZ2MHG-TSNT4, Ethernet ports 1 to 4 are used.

[*4] For the NZ2MHG-TSNT4, no optical fiber port exists.

2 SPECIFICATIONS

This chapter describes the managed switch specifications.

2.1 General Specifications

This section describes the general specifications for the managed switch.

Item	Specifications
Operating ambient temperature	-10 to 60℃
Storage ambient temperature	-40 to 85℃
Operating ambient humidity	5 to 95%RH, non-condensing
Storage ambient humidity	5 to 95%RH, non-condensing
Vibration resistance	IEC 60068-2-6
Shock resistance	IEC 60068-2-27
Operating atmosphere	No corrosive gases, flammable gases, less conductive dust
Operating altitude	0 to 2000m[*1][*2]
Installation location	Inside a control panel
Pollution degree[*3]	2 or less
Equipment class	Class Ⅲ

[*1] The managed switch cannot be stored or used in an environment in which the level of pressure is equal to or higher than the atmospheric pressure that can occur near 0m elevation.

[*2] When the managed switch is used at altitude above 2000m, the withstand voltage performance and the upper limit of the operating ambient temperature decrease. Please consult your local Mitsubishi representative.

[*3] This index indicates the degree to which conductive material is generated in terms of the environment in which the equipment is used. In pollution degree 2, only non-conductive pollution occurs. A temporary conductivity caused by condensing must be expected occasionally.

2.2 Performance Specifications

This section describes the performance specifications for the managed switch.

Item		Specifications	
		NZ2MHG-TSNT8F2	NZ2MHG-TSNT4
Transmission speed (RJ45 port)	10BASE-T	10Mbps (Full-duplex/half-duplex)	
	100BASE-TX	100Mbps (Full-duplex/half-duplex)	
	1000BASE-T	1Gbps (Full-duplex)	
Transmission speed (SFP port)	1000BASE-SX[*1]	1Gbps (Full-duplex/half-duplex)	—
	100BASE-FX[*1]	100Mbps (Full-duplex/half-duplex)	—
Maximum segment length	10BASE-T	100m	
	100BASE-TX		
	1000BASE-T		
	1000BASE-SX[*1]	550m	—
	100BASE-FX[*1]	2km	—
Communication interface	RJ45 port[*2]	• 8 ports • Auto-negotiation function • Auto MDI/MDI-X function	• 4 ports • Auto-negotiation function • Auto MDI/MDI-X function
	SFP ports[*2]	2 ports	—
Number of MAC addresses to be learned		9216 maximum	
Aging time for the MAC address table		10 to 300s	
VLAN	VLAN ID range	1 to 4094	
	Number of VLANs to be set	256 maximum	
Packet buffer size		4Mbit	2Mbit
Compatible MIB		RFC1213, Ethernet-like MIB, IF MIB, LLDP MIB, Bridge MIB, QBRIDGE MIB, IEEE8021-PAE-MIB, IEEE8021-SPANNING-TREE-MIB, SNMPv2-MIB	
Compatible protocol	Management purpose	IPv4/IPv6, LLDP, SMTP, SNMP Inform, SNMPv1/v2c/v3, SNMP Trap, DHCP Server/Client, ARP, TFTP, SFTP, HTTP, HTTPS, SSH, Telnet, Private MIB, Syslog	
	Redundancy	STP/RSTP	
	Security	RADIUS, TACACS+	
	Time synchronization	IEEE 1588v2 (PTP), SNTP, NTP Server/Client	
TSN compatible standard		IEEE 802.1AS (gPTP), IEEE 802.1Qbv	
CC-Link IE TSN Class		CC-Link IE TSN Class B CC-Link IE TSN Class A	
Serial interface	Console port	RJ45 connector	
	USB port	USB Type-A connector	
Relay output	Number of ports	1	
	Maximum allowable voltage of contact	1A at 24VDC	
Digital input	Number of ports	1	
	Rated input voltage	• 13 to 30V: H input • -30 to 3V: L input	
	Rated input current	8mA	
Power supply specifications	Rated voltage	12/24/48VDC	
	Allowable voltage range	9.6 to 60VDC	
	Protection function	• Overcurrent protection function • Reverse connection protection function	
	Redundancy function	Multi-power supply compatible	
	Internal current consumption (12VDC)	1.72A	1.25A
	Internal current consumption (24VDC)	0.84A	0.62A
	Internal current consumption (48VDC)	0.43A	0.32A
Protection degree		IP40	
External dimensions	Height	135mm	135mm
	Width	36mm	25mm
	Depth	115mm	115mm
Weight		0.79kg	0.59kg

*1 The transmission speed and maximum segment length vary depending on the SFP module used. For details, check the SFP module used.

*2 The RJ45 ports and SFP ports exclusively use Port 1 and Port 2. When the ports are used as the SFP ports, Ethernet Port 1 and Port 2 with the same numbers cannot be used.

2.3 Function List

The following is the list of functions for the managed switch.

Item		Description	Reference
System management [System Management]	Device information setting [Information Setting]	Allows any device information to be set to the managed switch.	Page 69 Device information setting [Information Setting]
	Firmware upgrade function [Firmware Upgrade]	Allows the firmware version of the managed switch to be updated.	Page 71 Firmware upgrade function [Firmware Upgrade]
	Configuration backup and restoration [Configuration Backup and Restore]	Allows the parameters of the managed switch to be backed up/restored as the configuration file.	Page 76 Configuration backup and restoration [Configuration Backup and Restore]
	Event log output function [Event Log Backup]	The managed switch records various types of events that occur as logs.	Page 89 Event log output function [Event Log Backup]
Account management [Account Management]	User account setting function [User Account]	Allows the account required for login to the managed switch to be added, edited, or deleted.	Page 97 User account setting function [User Account]
	Password policy [Password Policy]	Allows the conditions to be set for the number of characters and for character combinations for the password.	Page 105 Password policy [Password Policy]
Network [Network]	IP configuration [IP Configuration]	Allows the IP address of the managed switch main unit to be set by the following two methods. • Manual (Manual): The IP address can be changed from the web interface. • Auto (DHCP): The IP address can be assigned via the DHCP server.	Page 106 IP configuration [IP Configuration]
	DHCP server [DHCP Server]	By operating the managed switch as the DHCP server, the IP address is automatically assigned to the connected devices.	Page 108 DHCP server function [DHCP Server]
Time [Time]	Time zone [Time Zone]	Controls the clock of the managed switch in synchronization with the time zone of the region where the switch is used.	Page 118 Time zone [Time Zone]
	System time setting [System Time]	Allows the system time to be changed.	Page 120 System time [System Time]
	Time synchronization function [Time Synchronization]	A function to synchronize the time with the time of the grandmaster in the network	Page 129 Time synchronization function [Time Synchronization]
Port interface [Port Interface]	Port setting [Port Setting]	Allows the following settings to be configured for each port. Also, the connection status can be checked for each port. • Disabling the port • Communication speed of the port • Changing the port interface	Page 141 Port setting [Port Setting]
Layer 2 switching function [Layer 2 Switching]	VLAN function [VLAN]	Allows a VLAN to be built in any location within the network where a single or multiple managed switches are present.	Page 144 VLAN function [VLAN]
	Priority management function [Priority Management]	Allows the priority of receive frames to be managed.	Page 157 Priority management function [Priority Management]
	MAC address [MAC]	Allows the MAC address registered in the MAC address table to be checked. Also, the aging time for the MAC address table can be set.	Page 166 MAC address [MAC]
	Multicast setting function [Static Multicast]	Allows the multicast MAC address to be manually registered to the MAC address table.	Page 170 Multicast setting function [Static Multicast]
	Time-sharing communications [Time-Aware Shaper]	The managed switch supports the time-sharing communication function by IEEE 802.1Qbv. Time-sharing communication is a function that applies time-sharing scheduling to a traffic that is input to the managed switch by priority before outputting in a desired time slot.	Page 173 Time-sharing communication [Time-Aware Shaper]
Layer 2 redundancy function [Layer 2 Redundancy]	Spanning tree function [Spanning Tree]	Builds a logical topology in which loop paths are eliminated on the network to create a redundant communication path between the managed switches.	Page 179 Spanning tree function

Item		Description	Reference
Network management [Network Management]	SNMP	On SNMP, the devices are monitored and controlled by the following operations. • MIB acquisition request [Get Request] • MIB modification request [Set Request]	Page 187 SNMP
	SNMP Trap/Inform	Notifies the SNMP manager at event occurrence.	Page 193 SNMP Trap/Inform
Device security function [Device Security]	Interface management function [Management Interface]	Allows the connection method for setting the parameters of the managed switch to be disabled.	Page 202 Interface management function [Management Interface]
	Login policy [Login Policy]	The login policy can be set to improve the security of the managed switch.	Page 205 Login policy [Login Policy]
	Access permitted function [Trusted Access]	Allows the IP address for which access to the managed switch is permitted to be set to prevent access from unauthorized IP addresses.	Page 207 Access permitted function [Trusted Access]
	SSH	Allows the key to be used for SSH encryption to be regenerated.	Page 212 SSH
	SSL	Allows CSR to be output, the SSL server certificate to be regenerated, and the SSL server certificate to be imported.	Page 213 SSL
Network security function [Network Security]	Traffic control function [Traffic Storm Control]	Discards the frame when reception of a specific traffic exceeds the threshold value.	Page 216 Traffic control function [Traffic Storm Control]
Authentication method [Authentication]	Login authentication method [Login Authentication]	Allows the login authentication method to be changed.	Page 219 Login authentication method [Login Authentication]
System status check [System Status]	System utilization [Utilization]	Graphically shows the information of the managed switch.	Page 226 System utilization [Utilization]
	Statistical information [Statistics]	Shows the statistical information of data communications for each port.	Page 229 Statistical information [Statistics]
Event notification [Event Notification]	Event notification function [Event Notification]	Notifies the external devices of events that have occurred in the system or each port.	Page 235 Event notification function [Event Notification]
	Relay alarm cut-off [Relay Alarm Cut-off]	Turns off the notifications by relay output.	Page 240 Relay alarm cut-off [Relay Alarm Cut-off]
	Email notification function [Email Notification]	Notifies events via email.	Page 241 Email notification function [Email Notification]
	Syslog function [Syslog]	Sends various types of event logs to the Syslog server.	Page 242 Syslog function [Syslog]
Diagnostic function [Diagnosis]	LLDP	Periodically sends the configuration information to the neighboring devices.	Page 244 LLDP
	Ping	Allows to check for any abnormality on the route between the personal computer and the network devices with which communication is established.	Page 248 Ping
	ARP table [ARP Table]	Shows the ARP table.	Page 249 ARP table
	Event log [Event Log]	Shows the event logs.	Page 250 Event log [Event Log]

3 PROCEDURES BEFORE OPERATION

The following describes the procedures before the operation.

1. Installation of the managed switch

Install a managed switch into the control panel by using a DIN rail or module mounting brackets. (☞ Page 25 Installation Environment and Installation Position)

2. Wiring

Connect the power supply cable and the communication cables. (☞ Page 29 Wiring)

3. Powering on the managed switch

Power on the managed switch.

The PW1 LED, PW2 LED, and RUN LED turn on.

4. Parameter settings

Set the parameters of the managed switch. (☞ Page 56 PARAMETER SETTINGS)

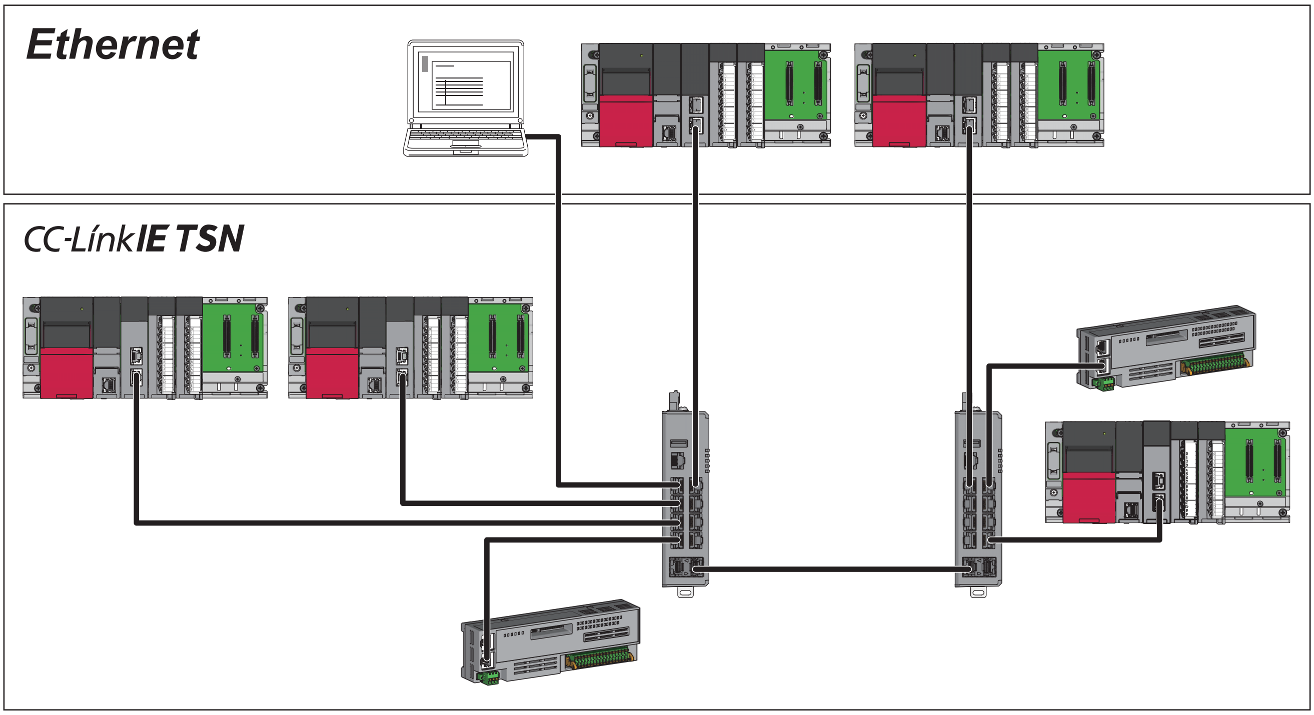
5. Powering on connected external devices

Power on connected external devices.

MEMO

4 SYSTEM CONFIGURATION

This chapter describes the system configuration in which the managed switch is used.



4.1 Concurrent Use Combination of Network Devices

The following table lists the combinations of network devices that can be concurrently connected to the managed switch.

For details on the settings, refer to the following.

☞ Page 38 How to Connect with CC-Link IE TSN Compatible Devices

◎: Setting is not required.

○: Setting is required.

△: The network needs to be separated using the VLAN function.

Compatible device	CC-Link IE TSN compatible device	CC-Link IE Field Network compatible device	Ethernet device
CC-Link IE TSN compatible device	◎[*1]	△	○
CC-Link IE Field Network compatible device	△	◎[*2]	△
Ethernet device	○	△	◎

[*1] Settings are required when a device other than the CC-Link IE TSN Class B device is connected, or when the SFP module (optical fiber cable) is used.

[*2] The network needs to be separated using the VLAN function when connecting CC-Link IE Field Network compatible devices whose network numbers differ from one another.

5 INSTALLATION AND WIRING

This chapter describes the installation and wiring of the managed switch.

5.1 Installation Environment and Installation Position

Install a managed switch into a control panel in either of the following ways:

- Mounting to a DIN rail (☞ Page 27 Mounting to a DIN Rail)
- Using module mounting brackets (installing directly on the wall surface)

Point

For how to install a managed switch directly on a wall surface, refer to the following.

📖 Applicable Products for CC-Link IE TSN Industrial Managed Switch (FA-A-0347)

Precautions

The module may become very hot during the setting and operation. When installing/removing the module, be sure that the module is not hot and avoid a burn.

⚠

Installation environment

Install a managed switch according to the installation environment shown in the general specifications. (☞ Page 16 General Specifications)

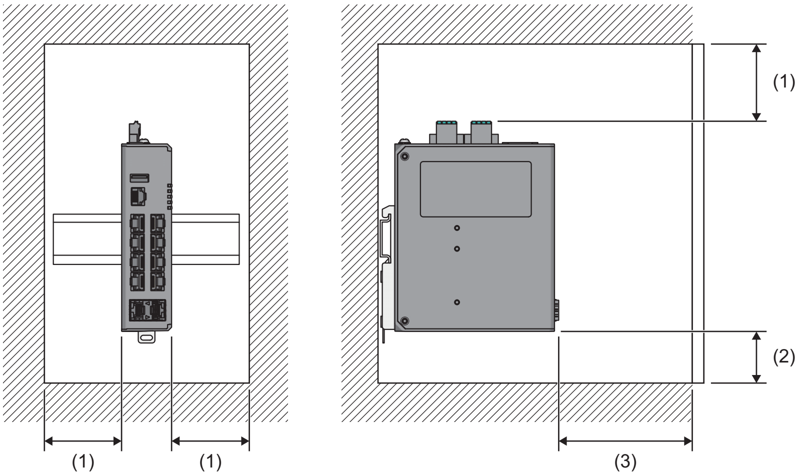
Do not install the switch in the following places.

- The operating ambient temperature is outside the range of -10 to 60℃.
- The operating ambient humidity is outside the range of 5 to 95%RH.
- Condensation occurs because of rapid temperature change.
- Corrosive gas or combustible gas exists.
- Conductive powder such as dust and iron powder, oil mist, salinity, or organic solvent is filled.
- The managed switch is exposed to direct sunlight.
- Strong electric field or strong magnetic field is generated.
- The managed switch is subject to direct vibration or shock.

Installation position

When installing the managed switch into a place such as the control panel, to improve the airflow and change a module easily, provide clearance between the managed switch and structures/parts as shown below.

Provide clearance in the same way also when two or more of this product are installed adjacent to each other.



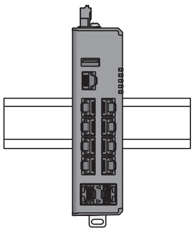
(1) 50mm or more

(2) 30mm or more

(3) 80mm or more

Installation orientation

For heat dissipation, install the managed switch in the following orientation (front installation) before use.



Do not use the managed switch in the following installation orientations.

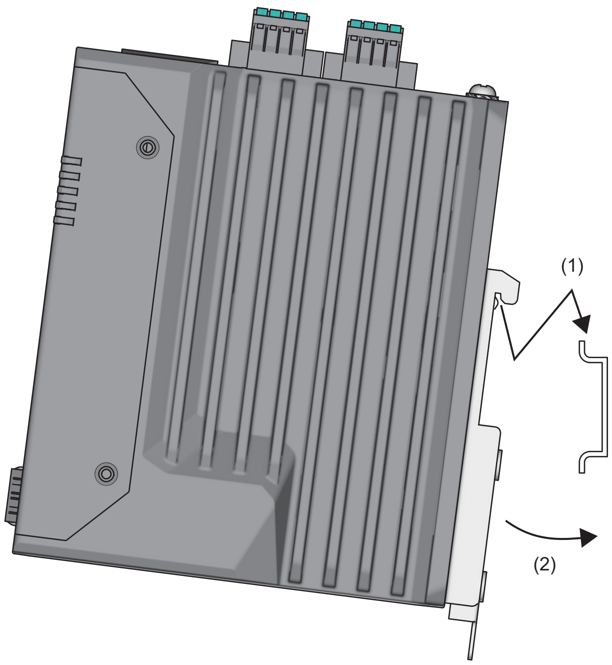
- Downward installation
- Vertical installation
- Upside-down installation
- Upward installation

5.2 Mounting to a DIN Rail

This section describes how to install a managed switch to a DIN rail. The following DIN rails are applicable (JIS C 2812, IEC 60715).

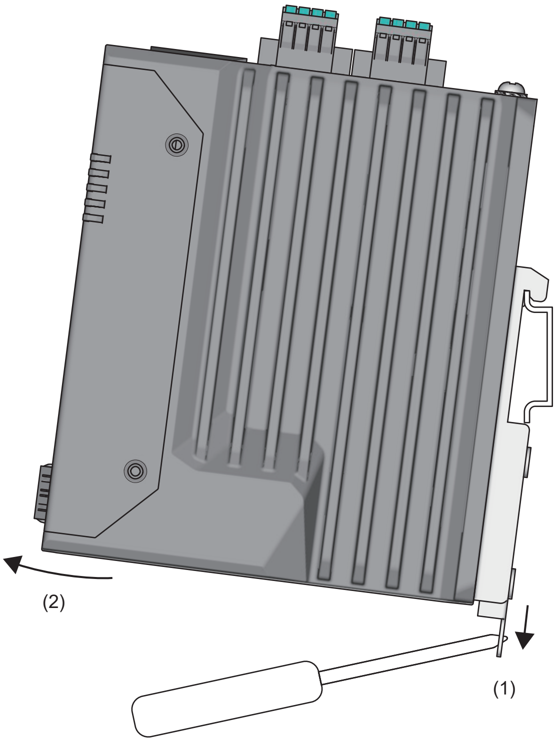
- TH35-7.5Fe
- TH35-7.5Al
- TH35-15Fe

Installation procedure



1. Hitch the upper part of the DIN rail mounting kit on the DIN rail.
2. Press the lower part of the managed switch all the way until it clicks.

Removal procedure



1. Press down the DIN rail mounting hook using a flathead screwdriver.
2. Pull the lower part of the managed switch to remove the managed switch from the DIN rail.

Precautions

If the DIN rail mounting kit was removed and needs to be reattached, apply the following tightening torque to each screw to securely fix the kit.

- Tightening torque: 0.4N·m

5.3 Wiring

Tightening torque

Tighten the terminal block mounting screws for the relay output terminal, power input terminal, and digital input terminal within the following torque range. Overtightening may damage the managed switch.

Screw	Tightening torque
Terminal block mounting screw (M2.5)	0.3N·m

Applicable wire

The following table lists the wire to be connected with the relay output terminal, power input terminal, and digital input terminal.

Wire diameter	Type	Material	Temperature rating
18 to 24 AWG	Stranded wire	Copper wire	105℃ or higher

Applicable solderless terminal

The following table lists the applicable solderless terminals.

Product	Terminal shape	Model	Applicable wire size	Bar solderless terminal tool	Manufacturer
Bar solderless terminal	Ferrule (with insulation sleeve)	AI0.5-10WH	0.5㎟	CRIMPFOX6	PHOENIX CONTACT GmbH & Co. KG
		AI0.75-10GY	0.75㎟		
	Ferrule (without insulation sleeve)	A0.5-10	0.5㎟		
		A0.75-10	0.75㎟		
		A1.0-10	1.0㎟		

Precautions

Use UL-certified solderless terminals. For processing, use a tool recommended by their manufacturer. For the usage methods and precautions of each tool, check with the solderless terminal manufacturer.

Installing/removing the terminal block

To remove a terminal block, loosen the terminal block mounting screws with a screwdriver.
To install a terminal block, tighten the terminal block mounting screws with a screwdriver.

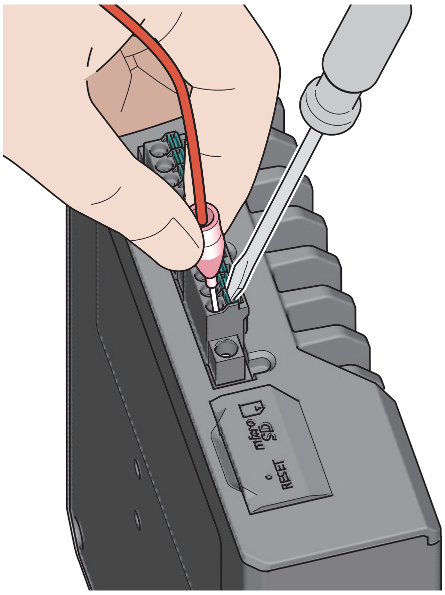
Connecting a cable

To connect a cable, push the open/close button with a flathead screwdriver.

While the open/close button is pushed in, insert a wire with a bar solderless terminal into the wire insertion opening and push the wire.

When the wire is completely pushed in, release the flathead screwdriver.

After inserting the wire, pull it lightly to check that it is securely clamped.



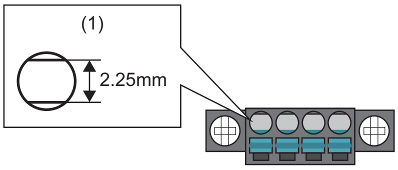
Disconnecting a cable

To disconnect a cable, push the open/close button with a flathead screwdriver.

While the open/close button is pushed in, pull out the wire attached to the bar solderless terminal.

Precautions

- For wiring to the terminal block, use bar solderless terminals. If a stripped wire is inserted to the wire insertion opening, the wire cannot be securely clamped.
- For how long the wire should be stripped, follow the specifications of the bar solderless terminal used. To attach a bar solderless terminal to a wire, use a crimping tool.
- Before inserting a bar solderless terminal to the wire insertion opening (1), check the shape of the opening and the shape of the terminal. Insert the terminal paying attention to the orientation. If a bar solderless terminal larger than the wire insertion opening (1) is inserted, the terminal block may be damaged.



- For use under severe noise environment conditions, attach a ferrite core whose damping characteristics are equivalent to those of the ZCAT3035-1330 (manufactured by TDK Corporation) between the external power supply and this product.

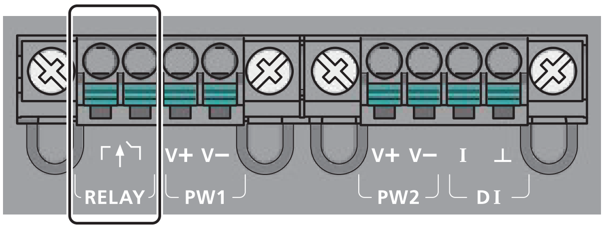
Wiring to the power input terminal

For the power supply to the module, connect the power supply that satisfies the following specifications.

- The reinforced insulation power supply is UL-certified, satisfies the safety extra-low voltage (SELV) circuit requirements, and does not generate hazardous voltage of 60V or higher.
- The DC output hold time at a momentary power failure is 10ms or more.
- The power supply is UL-certified and satisfies the limited power source (LPS) requirements.
- Rated voltage: 12V/24V/48VDC
- Minimum output current: 1.72A or higher (NZ2MHG-TSNT8F2), 1.25A or higher (NZ2MHG-TSNT4)
- Operating temperature: 60℃ or higher

Wiring to the relay output terminal

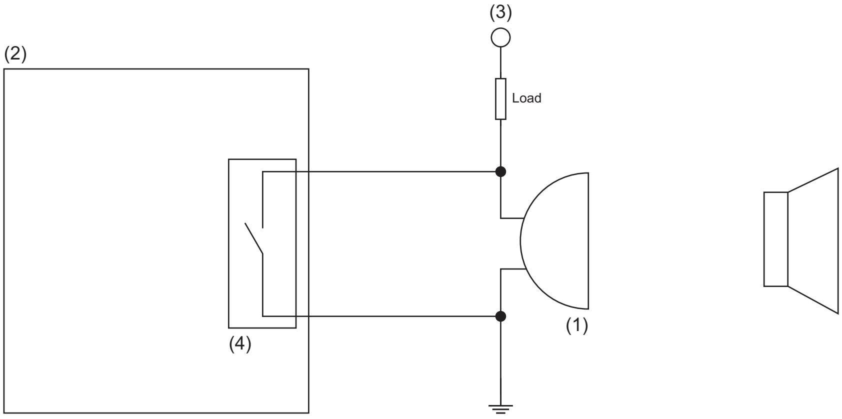
The relay of the managed switch is closed during normal operation. This relay opens when power is not being supplied to the managed switch or when a user-configured event has occurred. For connection, use the terminal block on the PW1 side.



The other specifications are described below.
Maximum allowable current of contact: 1A at 24VDC

Ex.

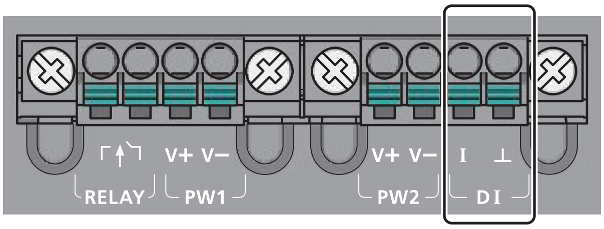
The following figure shows the connection example of a system that sounds a buzzer when the module power supply is interrupted or when a user-configured event has occurred.



(1) Buzzer
(2) Managed switch
(3) Power supply
(4) Relay connector

Wiring to the digital input terminal

For digital input connection, use the terminal block on the PW2 side.
Connect the positive (signal output) to the I terminal and the negative (GND) to the ⊥ terminal.



The other specifications are described below.

- Insulation digital input
- ON voltage: 13VDC or higher (30VDC maximum)
- OFF voltage: 3VDC or lower (-30VDC minimum)
- Maximum input current: 8mA

FG wiring

For the tightening torque of FG connection screws, follow the tightening torque listed below.

Screw	Tightening torque
FG line mounting screw (M4 screw)	0.49N·m

Use the thickest cable (maximum of 2mm²). Bring the grounding point close to this product as much as possible so that the ground cable can be shortened.

Wiring to Ethernet ports

This section describes the wiring to Ethernet ports.

Wiring method

The following describes connection and disconnection of the Ethernet cable.

■Connecting method

1. Push the Ethernet cable connector into the managed switch until it clicks. Pay attention to the orientation of the connector.
2. Lightly pull the cable to check that it is securely connected.
3. Check whether the 1Gbps LINK LED or the 100Mbps/10Mbps LINK LED of the port connected with the Ethernet cable is on. Also, check the on/off status to see whether the communication speed is correct.*1 (☞ Page 13 PART NAMES)

*1 The time between the cable connection and the 1Gbps LINK LED or 100Mbps/10Mbps LINK LED turning on may vary. The LED usually turn on in a few seconds. Note, however, that the time may be extended further if the link-up processing is repeated depending on the status of the device on the line. If the 1Gbps LINK LED or 100Mbps/10Mbps LINK LED does not turn on, check that there is no problem with the Ethernet cable.

■Disconnecting method

1. Press the latch down and unplug the Ethernet cable.

Precautions

- Place the Ethernet cable in a duct or clamp them. If not, dangling cable may swing or inadvertently be pulled, resulting in damage to the module or cables or malfunction due to poor contact.
- Do not touch the core of the Ethernet cable-side or module-side connector, and protect it from dirt or dust. If oil from your hand, dirt, or dust is attached to the core, it can increase transmission loss, causing a problem in data link.
- Check that the Ethernet cable is not disconnected/shorted or that there is no problem with the connector connection.
- Do not use Ethernet cables with broken latches. Doing so may cause disconnection of the cable or malfunction.
- Hold the connector part when connecting and disconnecting the Ethernet cable. Pulling the cable connected to the module may result in damage to the module or cable, or malfunction due to poor contact of the cable.
- The maximum segment length of the Ethernet cable is 100m. However, the length may become shorter depending on the operating environment of the cable. For details, contact the manufacturer of the cables used.
- The bending radius of the Ethernet cable is limited. For details, check the specifications of the Ethernet cable to be used.

Wiring products

■Ethernet cable

Use the following devices to configure network using Ethernet ports.

Application		Ethernet cable	Connector	Standard
Ethernet	1Gbps	Category 5e or higher, straight cable (shielded, STP)	RJ45 connector	IEEE 802.3 (1000BASE-T)
		Category 5e or higher, crossover cable (shielded, STP)		
	100Mbps	Category 5 or higher, straight cable (shielded, STP)		IEEE 802.3 (100BASE-TX)
		Category 5 or higher, crossover cable (shielded, STP)		
	10Mbps	Category 3 or higher, straight cable (shielded, STP)		IEEE 802.3 (10BASE-T)
		Category 3 or higher, crossover cable (shielded, STP)		
CC-Link IE TSN	1Gbps	📖 Refer to the user's manual for the master station used.		📖 Refer to the user's manual for the master station used.
	100Mbps			
CC-Link IE Field Network	1Gbps	📖 Refer to the user's manual for the master station used.		📖 Refer to the user's manual for the master station used.

Wiring to optical fiber ports

This section describes the wiring to optical fiber ports. (Only for the NZ2MHG-TSNT8F2)

Connectable devices

For devices that can be connected to the optical fiber port, refer to the following.

📖 Applicable Products for CC-Link IE TSN Industrial Managed Switch (FA-A-0347)

Wiring method

The following describes connection and disconnection of an optical fiber cable.

■Connecting method

1. Insert an SFP module to the optical fiber port. Pay attention to the orientation of the SFP module.
2. Insert the optical fiber cable connector to the SFP module until it clicks. Pay attention to the orientation of the connector.
3. Lightly pull the cable to check that it is securely connected.
4. Check that the 1Gbps/100Mbps LINK LED of the port to which the optical fiber cable is connected is on. Also, check the on/off status to see whether the communication speed is correct.[*1] (☞ Page 13 PART NAMES)

[*1] The time between the optical fiber cable connection and the 1Gbps/100Mbps LINK LED turning on may vary. The LED usually turn on in a few seconds. Note, however, that the time may be extended further if the link-up processing is repeated depending on the status of the device on the line. If the 1Gbps/100Mbps LINK LED does not turn on, check that there is no problem with the optical fiber cable.

■Disconnecting method

1. Press the connector hook down and unplug the optical fiber cable.
2. Remove the SFP module from the optical fiber port.

Precautions

- Place the optical fiber cable in a duct or clamp them. If not, dangling cable may swing or inadvertently be pulled, resulting in damage to the SFP module or cable or malfunction due to poor contact.
- Do not touch the optical fiber core of the optical fiber cable-side or SFP module-side connector, and protect it from dirt or dust. If any oil from your hand, or any dirt or dust sticks to the core, it can increase transmission loss, causing data link to fail.
- Check that the optical fiber cable is not disconnected or that there is no problem with the connector connection.
- Hold the connector part when connecting or disconnecting the optical fiber cable. Pulling the cable connected to the SFP module may result in damage to the SFP module or cable, or malfunction due to poor contact of the cable.
- For an unused optical fiber port, attach the provided connector cover to prevent foreign matter such as dust from entering the port. Touching the port with bare hands may result in injury.
- The maximum segment length of the optical fiber cable for 1000BASE-SX is 550m, and for 100BASE-FX is 2km. The allowable delay of the optical fiber cable at time synchronization is up to 10μs. Therefore, the length may become shorter depending on the cable to be connected. Also, the length may become shorter depending on the operating environment of the cable and the SFP module. For details, contact the manufacturers of the cable and the SFP module used.
- The bending radius of the optical fiber cable is limited. For details, check the specifications of the cable used.
- The laser class (JIS C 6802, IEC 60825-1) is Class 1. Do not look directly at a laser beam. Doing so may harm your eyes.

Wiring to the console port

This section describes the wiring to the console port.

Wiring method

The following describes connection and disconnection of the console cable.

■Connecting method

1. Push the cable console connector into the managed switch until it clicks. Pay attention to the orientation of the connector.
2. Lightly pull the cable to check that it is securely connected.

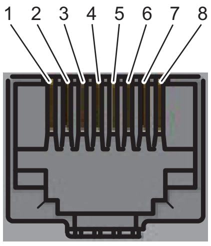
■Disconnecting method

1. Press the latch down and unplug the console cable.

Wiring products

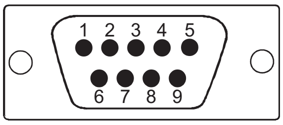
■Console port

The console port is an RJ45 connector whose shape is the same as that of the Ethernet port, but it has an RS-232 interface. The pin layout is described below.

Console port	Pin layout	
	No.	**Name**
	1	DSR
	2	RTS
	3	—
	4	TXD
	5	RXD
	6	GND
	7	CTS
	8	DTR

■Specifications for the RS-232 connector on the external device side

For connection on the external device side, check whether the external device is the RS-232 interface (D-sub 9 pin male) whose specifications are the same as those listed below and connect the device using the provided console cable (RJ45-D-sub 9 pin female).

RS-232 interface (D-sub 9 pin male)	Pin layout	
	No.	**Name**
	1	DCD
	2	RXD
	3	TXD
	4	DTR
	5	GND
	6	DSR
	7	RTS
	8	CTS
	9	RI

Connection to USB port

The automatic restoration function and event log automatic backup are available when a connectable USB flash drive is connected to the USB port.

Connectable devices

For devices that can be connected to the USB port, refer to the following.
📖 Applicable Products for CC-Link IE TSN Industrial Managed Switch (FA-A-0347)

Connection method

The following describes connection and disconnection of the USB flash drives.

■Connecting method

1. Insert the USB flash drive. Pay attention to the orientation of the connector.

■Disconnecting method

1. Confirm that the USB flash drive is not being accessed and automatic restoration is not in progress. When the USB flash drive is being accessed or automatic restoration is in progress, the LEDs indicate the status as follows: RUN LED (green) flashes → ERR LED flashes → SYNC LED (green) flashes → RUN LED (green) flashes.
2. Pull out the USB flash drive from the connector.

Notes on connection to USB port

■Notes on supported firmware versions

The USB port cannot be used with firmware version "04" or earlier. Do not connect any USB device.

■Notes on USB flash drives

- USB flash drives other than those that can be connected cannot be used. If a USB flash drive other than one of those that can be connected is connected, a malfunction may be caused.
- Check that the USB flash drive is not being accessed before powering on and off the managed switch, resetting it, or disconnecting the USB flash drive. If the managed switch is powered on and off, reset, or the USB flash drive is disconnected while the USB flash drive is being accessed, the data in the USB flash drive may be corrupted. When the USB flash drive is being accessed, the LEDs operate as follows: RUN LED (green) flashes → ERR LED flashes → SYNC LED (green) flashes → RUN LED (green) flashes.
- Multiple USB flash drives cannot be connected even via a USB hub.
- Format the USB flash drives in the FAT or FAT32 format.
- For the names of files and folders to be stored, use one-byte alphanumeric characters and one-byte special characters (excluding ¥, /, *, ?, <, >, |, :, and "). If any characters other than one-byte alphanumeric characters and one-byte special characters are used in the file names or folder names, the names may become garbled.

■Notes on the configuration automatic restoration function

By default, the configuration automatic restoration function is enabled. If the managed switch could not detect any restorable configuration file when the USB flash drive is connected, the switch skips the configuration restoration, turns on the ERR LED, and starts the operation. When the configuration automatic restoration function is not used, disable the function. (☞ Page 84 Automatic restoration function)

■Notes on event log automatic backup

By default, event log automatic backup is enabled. Event log automatic backup is not executed if the USB flash drive does not have sufficient free space. Also, the ERR LED turns on. When event log automatic backup is not used, disable the function. (☞ Page 95 USB flash drive (Event log backup))

6 CONNECTION METHOD

This chapter describes how to connect the managed switch.

6.1 How to Connect with CC-Link IE TSN Compatible Devices

To connect with CC-Link IE TSN compatible devices, the configuration of each device needs to be unified across the overall CC-Link IE TSN system. This section describes the setting details required for connecting the managed switch with the CC-Link IE TSN compatible devices.

- Time synchronization mode
- Communication cycle

Point

If the time synchronization mode of the master station is IEEE 802.1AS, the managed switch can establish data link with the default settings. However, communication may be unstable. Configure the settings as follows.

Time synchronization mode

■Setting items of the master station

Set the time synchronization mode of the master station according to the system configuration.

- IEEE 802.1AS (Default)
- IEEE 1588

Setting on the engineering tool

Setting item	Setting value	
	IEEE 802.1AS	IEEE 1588
CC-Link IE TSN Class Setting	CC-Link IE TSN Class B Only	Mixture of CC-Link IE TSN Class B/A or CC-Link IE TSN Class A Only

■Setting items of the managed switch

Set the items according to the time synchronization mode of the master station. All other setting items do not need to be changed from the default.

The following table lists the setting items that need to be changed.

Setting item	Setting value	
	IEEE 802.1AS	IEEE 1588
Profile	Default	IEEE 1588v2 DefaultProfile
Neighbor Propagation Delay Threshold	*1	—

*1 To connect the SFP module (optical fiber cable), change the default value to 10000. If the SFP module (optical fiber cable) is not connected, the default value of 3000 can be used.

Communication cycle

■Setting items of the master station

Set the communication cycle of the master station. (☞ Page 41 Setting items of the RJ71GN11-T2)

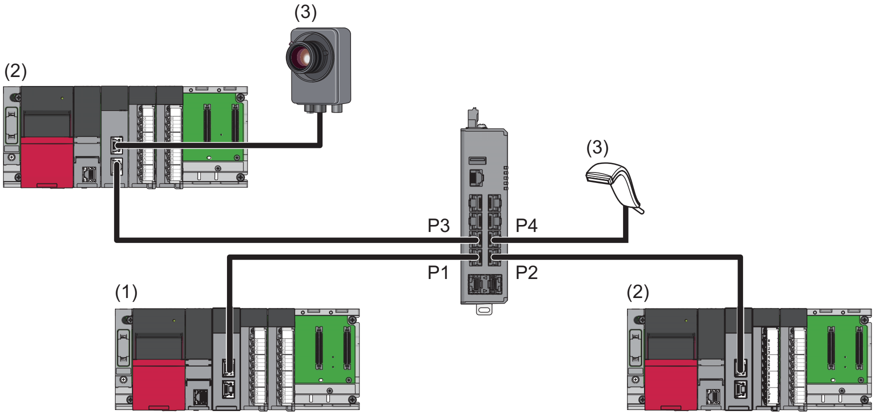
■Setting items of the managed switch

Set the communication cycle to the same value as that of the master station. (☞ Page 41 Setting items of the managed switch)

System configuration example

Connect the following devices to CC-Link IE TSN compatible devices and configure them on the CC-Link IE TSN Class B system. Connect all the devices using the CC-Link IE TSN compatible Ethernet cables, connect CC-Link IE TSN compatible devices to Ports 1 to 3 of the managed switch, and connect an Ethernet device to Port 4.

- Master station
- Slave station 1, Slave station 2
- Managed switch (NZ2MHG-TSNT8F2)



P1: Port 1
P2: Port 2
P3: Port 3
P4: Port 4
(1) Master station (RJ71GN11-T2)
(2) Slave stations (RJ71GN11-T2)
(3) Ethernet device

Setting example

When the devices are built as described in the system configuration example, configure the following settings.

- Time synchronization mode
- Communication cycle

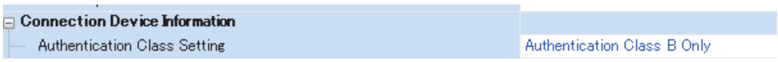
Time synchronization mode

■Setting items of the RJ71GN11-T2

Operating procedure

Select "CC-Link IE TSN Class B Only" in "CC-Link IE TSN Class Setting".

[Navigation window] ⇨ [Parameter] ⇨ [Module Information] ⇨ [RJ71GN11-T2] ⇨ [Basic Settings] ⇨ [Connection Device Information]



Connection Device Information	
Authentication Class Setting	Authentication Class B Only

In this manual, "Authentication Class" is described as "CC-Link IE TSN Class".

■Setting items of the managed switch

Set the items from the web interface. When the time synchronization mode of the RJ71GN11-T2 is set to "CC-Link IE TSN Class B Only", the default settings can be used except for the ports connected with the following device.

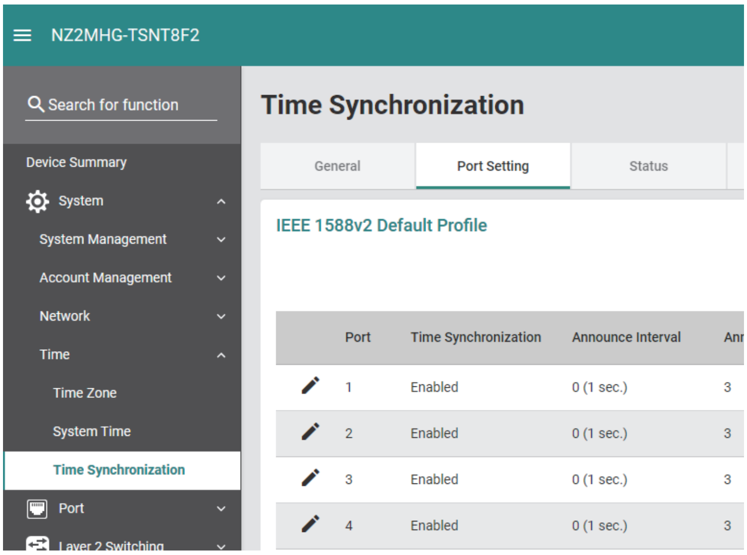
- Ports not connected with CC-Link IE TSN compatible devices (Port 4 (Ethernet device) in the system configuration example)

*1 Port 4 (Ethernet device) does not support time synchronization.

Operating procedure

1. Click the [Port Setting] tab.

[System] ⇨ [Time] ⇨ [Time Synchronization]

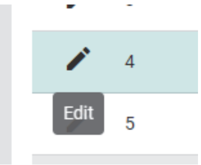


Time Synchronization

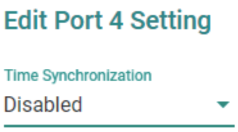
IEEE 1588v2 Default Profile

	Port	Time Synchronization	Announce Interval	Anr
✎	1	Enabled	0 (1 sec.)	3
✎	2	Enabled	0 (1 sec.)	3
✎	3	Enabled	0 (1 sec.)	3
✎	4	Enabled	0 (1 sec.)	3

2. Click the [Edit] icon for Port 4.



3. Change "Time Synchronization" to "Disabled".



Edit Port 4 Setting

Time Synchronization
Disabled

4. Click the [Apply] button.

Communication cycle

■Setting items of the RJ71GN11-T2

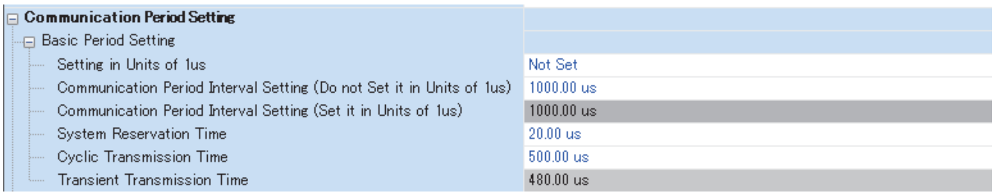
- Communication cycle setting, communication cycle division setting

Operating procedure

1. Set "Communication Period Interval Setting (Do Not Set it in Units of 1μs)" under "Communication Period Setting".

[Navigation window] ⇨ [Parameter] ⇨ [Module Information] ⇨ [RJ71GN11-T2] ⇨ [Basic Settings] ⇨ [Communication Period Setting]

2. Set "System Reservation Time" and "Cyclic Transmission Time" under "Communication Period Setting". The transient transmission time is automatically set.



⊟ Communication Period Setting	
⊟ Basic Period Setting	
Setting in Units of 1us	Not Set
Communication Period Interval Setting (Do not Set it in Units of 1us)	1000.00 us
Communication Period Interval Setting (Set it in Units of 1us)	1000.00 us
System Reservation Time	20.00 us
Cyclic Transmission Time	500.00 us
Transient Transmission Time	480.00 us

■Setting items of the managed switch

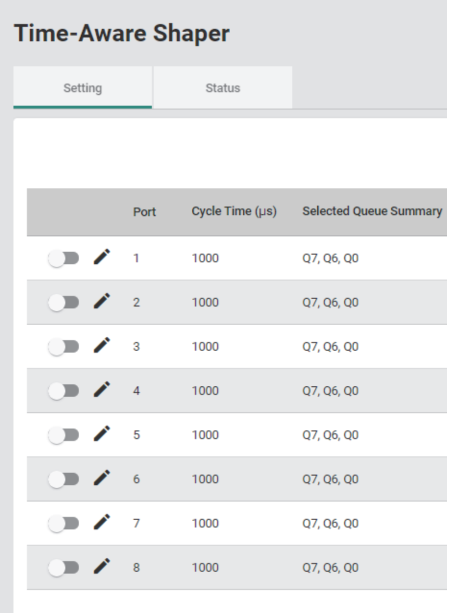
Set the items from the web interface. The communication cycle needs to be the same value as that of the RJ71GN11-T2.

Operating procedure

1. Click the [Setting] tab.

[Layer 2 Switching] ⇨ [Time-Aware Shaper]

2. Select the [Setting] tab.

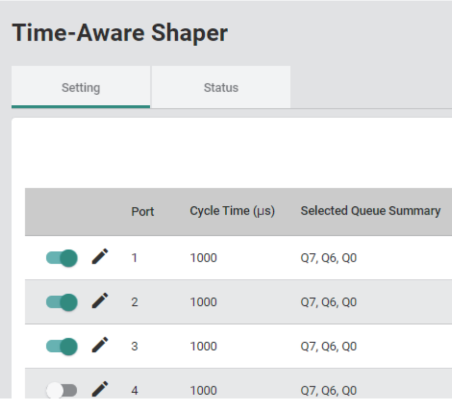


Time-Aware Shaper

	Port	Cycle Time (μs)	Selected Queue Summary
	1	1000	Q7, Q6, Q0
	2	1000	Q7, Q6, Q0
	3	1000	Q7, Q6, Q0
	4	1000	Q7, Q6, Q0
	5	1000	Q7, Q6, Q0
	6	1000	Q7, Q6, Q0
	7	1000	Q7, Q6, Q0
	8	1000	Q7, Q6, Q0

3. Enable the communication cycle of the ports.

Port 4 (Ethernet device), which is not connected with CC-Link IE TSN compatible devices, does not need to be set.



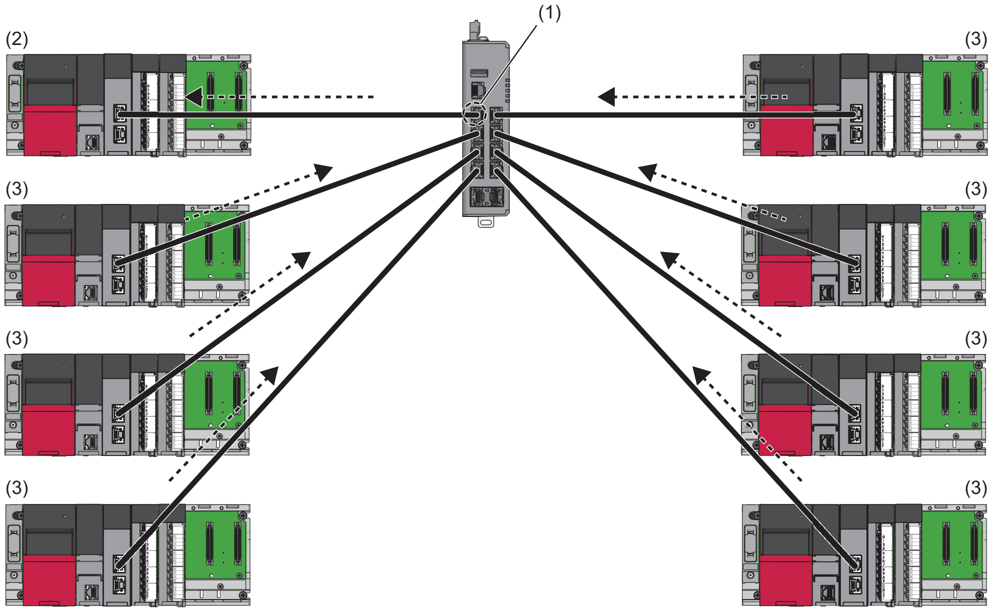
Time-Aware Shaper

	Port	Cycle Time (μs)	Selected Queue Summary
●	1	1000	Q7, Q6, Q0
●	2	1000	Q7, Q6, Q0
●	3	1000	Q7, Q6, Q0
○	4	1000	Q7, Q6, Q0

Precautions for system configuration

In some system configurations, if the line load is concentrated on one port, frame loss may occur due to an overflow of relay buffers in the managed switch. To prevent frame loss, refer to the restrictions. (☞ Page 45 Restrictions)

For unicast



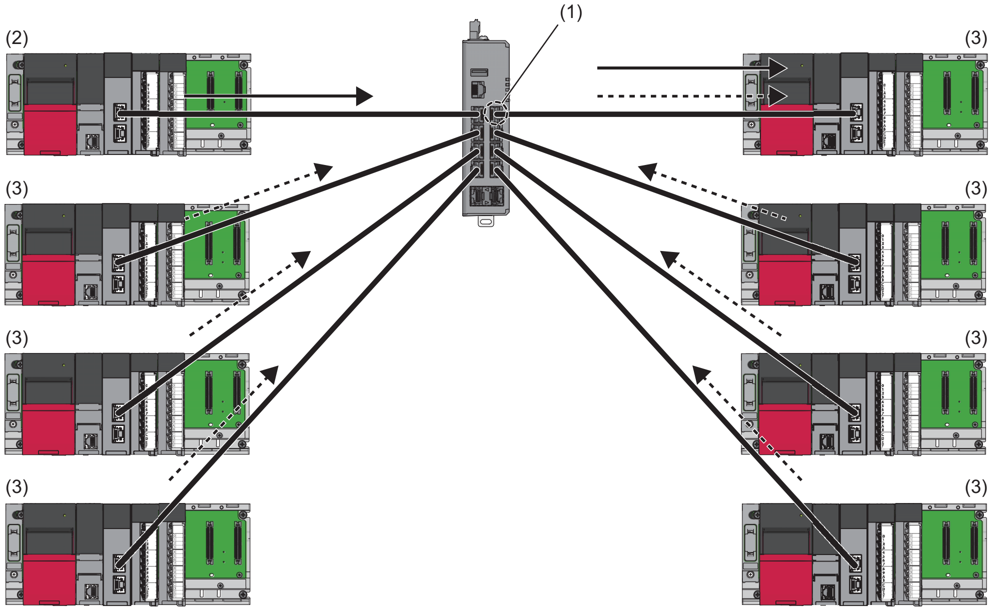
- - - - - - - - - ▸ Cyclic Ss frame

(1) Heavy line load

(2) Master station

(3) Slave station

For multicast



- - - - - - - - -▶ Cyclic Ss frame

——————▶ Cyclic Ms frame

(1) Heavy line load

(2) Master station

(3) Slave station

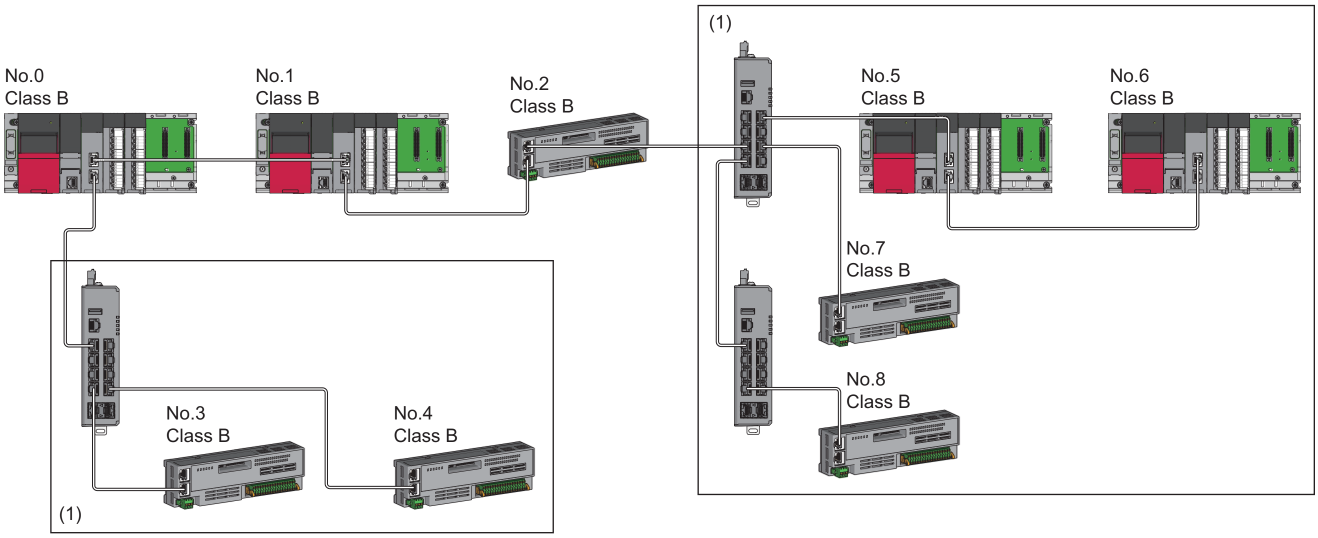
Restrictions

This section describes the restrictions for preventing frame loss.

CC-Link IE TSN Class B device only

Failing to observe the following restrictions may result in one of the slave stations being disconnected.

- Maintain 40 kilobytes or less for the total cyclic data size of all the slave stations on the slave station side, which serves as the boundary between the master station side and the slave station side of the managed switch.
- For the master station, set 4 times or more for "Disconnection Detection Setting" in "Slave Station Setting" of "Basic Setting".

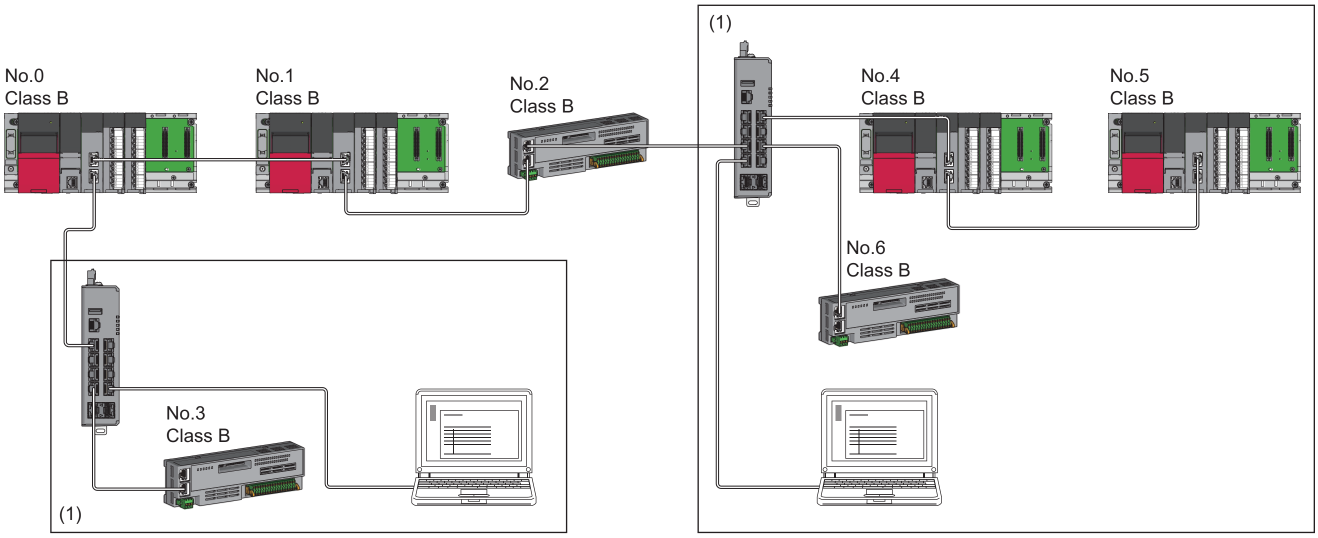


No.0: Master station
No.1, No.5, and No.6: Local station
No.2, No.3, No.4, No.7, No.8: Remote station
(1) Maintain 40 kilobytes or less for the total cyclic data size.

Connecting external devices directly to the managed switch

Failing to observe the following restrictions may result in one of the slave stations being disconnected.

- Maintain 8 kilobytes or less for the total cyclic data size of all the slave stations on the slave station side, which serves as the boundary between the master station side and the slave station side of the managed switch. However, if the data size of the external device per cycle can be identified, the combination of the total cyclic data size and the data size of the external device per cycle should be 40 kilobytes or less.
- For the master station, set 4 times or more for "Disconnection Detection Setting" in "Slave Station Setting" of "Basic Setting".



No.0: Master station

No.1, No.4, and No.5: Local station

No.2, No.3, and No.6: Remote station

(1) Maintain 8 kilobytes or less for the total cyclic data size.

Calculation of the total cyclic data size

For the formula used to calculate the total cyclic data size, refer to the following.

📖 User's manual for the master station used

Number of connectable slave stations

The following table lists an example of the number of slave stations that can be connected when the total cyclic data size is 40 kilobytes or less or 8 kilobytes or less.

Model	Number of points for each module				Total cyclic data size	
	RX	RWr	LB	LW	40 kilobytes or less	8 kilobytes or less
NZ2GN2B1-32DT	32	4	0	0	Up to 120 stations can be connected	Up to 77 stations can be connected
NZ2GN2B-60AD4	32	16	0	0	Up to 120 stations can be connected	Up to 76 stations can be connected
NZ2GN2B-60DA4	32	32	0	0	Up to 120 stations can be connected	Up to 76 stations can be connected

6.2 How to Connect with CC-Link IE Field Network Compatible Devices

The managed switch can be connected with CC-Link IE Field Network compatible devices. In addition, the VLAN function can be used to connect the mixture of network devices.

The following table lists the concurrent use combinations of CC-Link IE Field Network compatible devices and network devices.

◎: Setting is not required, △: Network separation by the VLAN function is required.

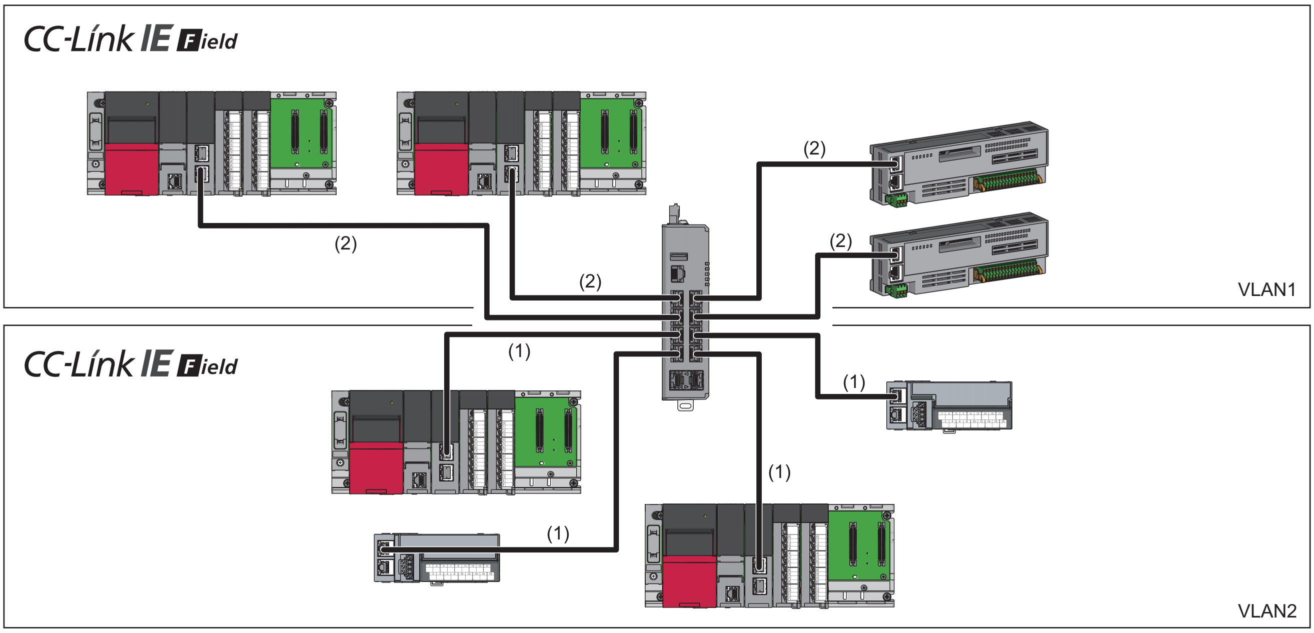
Compatible device	CC-Link IE Field Network compatible device	CC-Link IE TSN compatible device	Ethernet device
CC-Link IE Field Network compatible device	◎*1	△	△

*1 The network needs to be separated using the VLAN function when connecting CC-Link IE Field Network compatible devices whose network numbers differ from one another.

Connecting devices whose network numbers differ from one another

System configuration example

The following figure shows an example of a system configuration in which CC-Link IE Field Network compatible devices whose network numbers differ from one another are connected.



(1) Network No.1
(2) Network No.2

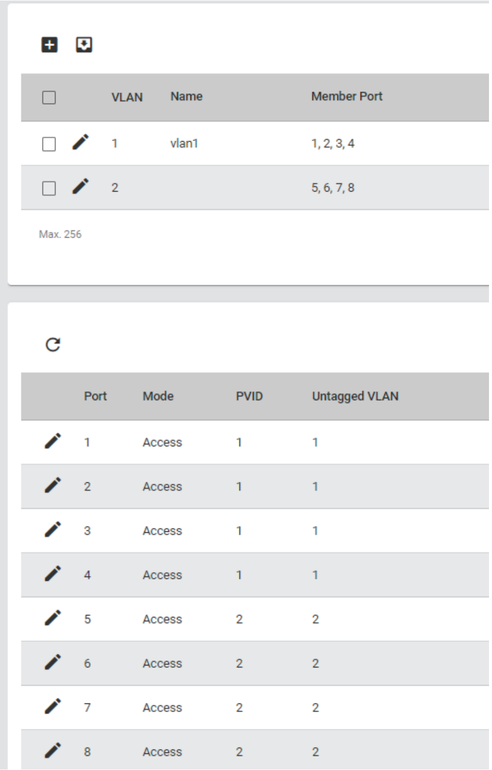
Setting example

The following procedure describes a setting example when connecting CC-Link IE Field Network compatible devices whose network numbers differ from one another.

Operating procedure

1. Set the VLAN as shown below.

For details, refer to VLAN function. (☞ Page 144 VLAN function [VLAN])



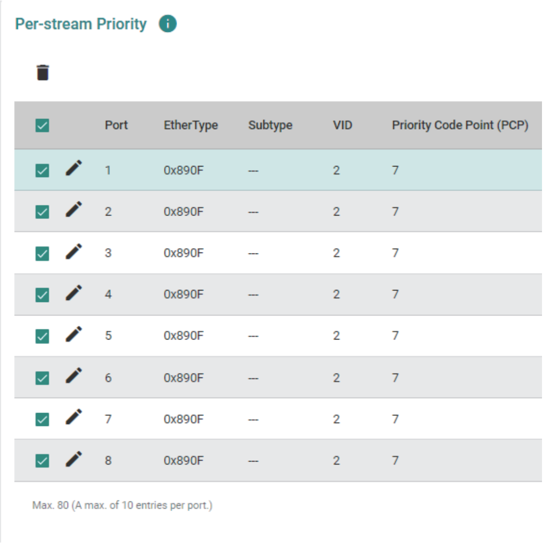
□		VLAN	Name	Member Port
□	✎	1	vlan1	1, 2, 3, 4
□	✎	2		5, 6, 7, 8

Max. 256

	Port	Mode	PVID	Untagged VLAN
✎	1	Access	1	1
✎	2	Access	1	1
✎	3	Access	1	1
✎	4	Access	1	1
✎	5	Access	2	2
✎	6	Access	2	2
✎	7	Access	2	2
✎	8	Access	2	2

Port number	Connected device	Port mode	PVID	Untagged VLAN	Tagged VLAN
P1 to P4	CC-Link IE Field Network compatible device (Network No.1)	Access	1	1	—
P5 to P8	CC-Link IE Field Network compatible device (Network No.2)	Access	2	2	—

2. Delete unnecessary per-stream priority settings. (☞ Page 157 Priority management function [Priority Management])



Per-stream Priority

☑		Port	EtherType	Subtype	VID	Priority Code Point (PCP)
☑	✎	1	0x890F	—	2	7
☑	✎	2	0x890F	—	2	7
☑	✎	3	0x890F	—	2	7
☑	✎	4	0x890F	—	2	7
☑	✎	5	0x890F	—	2	7
☑	✎	6	0x890F	—	2	7
☑	✎	7	0x890F	—	2	7
☑	✎	8	0x890F	—	2	7

Max. 80 (A max. of 10 entries per port.)

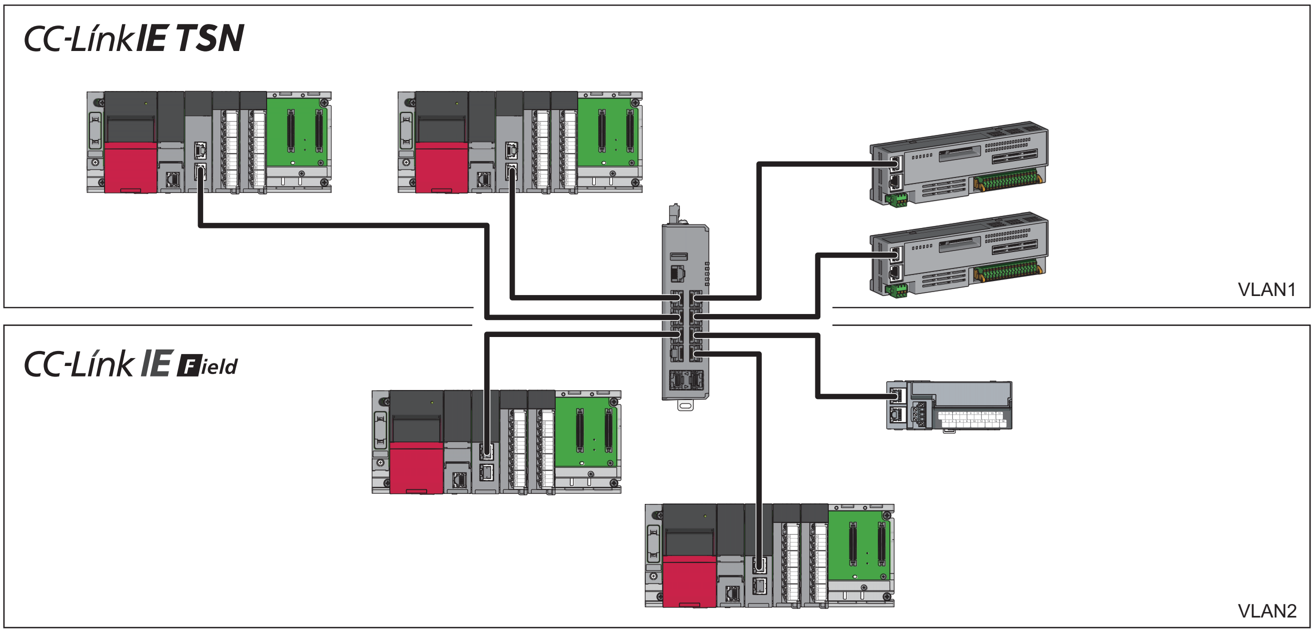
Precautions

To use the mixture of the CC-Link IE Field Network compatible devices whose network numbers differ from one another, do not share the wiring through the trunk port. Doing so may cause the disconnection of all stations.

Mixing CC-Link IE Field Network compatible devices and CC-Link IE TSN compatible devices

System configuration example

The following figure shows an example of a system configuration in which CC-Link IE Field Network compatible devices and CC-Link IE TSN compatible devices are mixed.



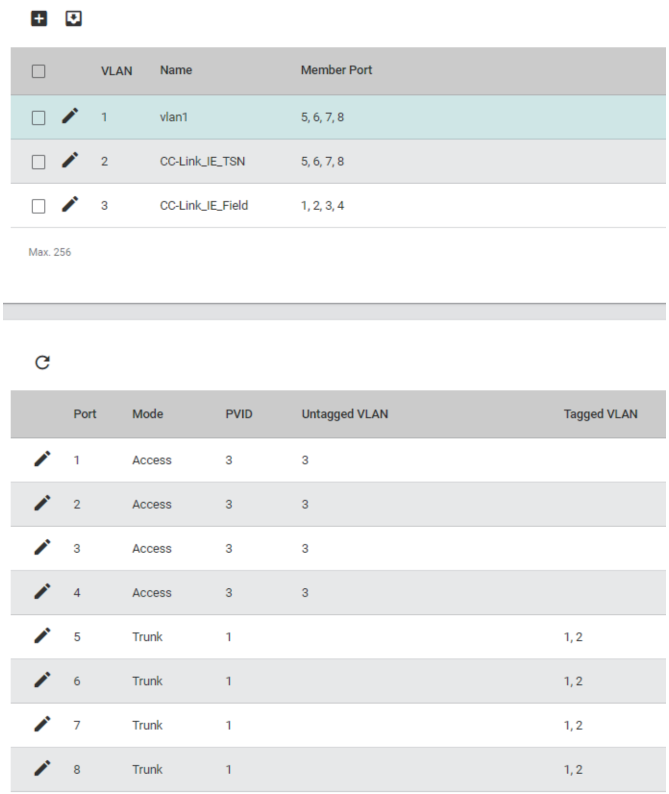
Setting example

The following procedure describes a setting example when mixing CC-Link IE Field Network compatible devices and CC-Link IE TSN compatible devices.

Operating procedure

1. Set the VLAN as shown below.

For details, refer to VLAN function. (☞ Page 144 VLAN function [VLAN])



□		VLAN	Name	Member Port
□	✎	1	vlan1	5, 6, 7, 8
□	✎	2	CC-Link_IE_TSN	5, 6, 7, 8
□	✎	3	CC-Link_IE_Field	1, 2, 3, 4

Max. 256

	Port	Mode	PVID	Untagged VLAN	Tagged VLAN
✎	1	Access	3	3	
✎	2	Access	3	3	
✎	3	Access	3	3	
✎	4	Access	3	3	
✎	5	Trunk	1		1, 2
✎	6	Trunk	1		1, 2
✎	7	Trunk	1		1, 2
✎	8	Trunk	1		1, 2

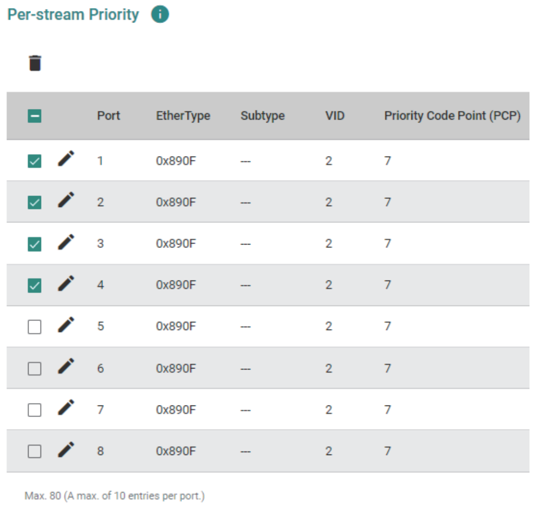
Port number	Connected device	Port mode	PVID	Untagged VLAN	Tagged VLAN
P1 to P4	CC-Link IE Field Network compatible device	Access	3	3	—
P5 to P8	CC-Link IE TSN compatible device (CC-Link IE TSN Class B)	Trunk	1	—	1, 2

2. Configure various settings for ports (P5 to P8) to be connected to the CC-Link IE TSN.

For the setting details, refer to the following.

☞ Page 38 How to Connect with CC-Link IE TSN Compatible Devices

3. For ports (P1 to P4) to be connected to the CC-Link IE Field Network compatible devices, delete unnecessary per-stream priority settings. (☞ Page 157 Priority management function [Priority Management])



Per-stream Priority

▬		Port	EtherType	Subtype	VID	Priority Code Point (PCP)
☑	✎	1	0x890F	--	2	7
☑	✎	2	0x890F	--	2	7
☑	✎	3	0x890F	--	2	7
☑	✎	4	0x890F	--	2	7
□	✎	5	0x890F	--	2	7
□	✎	6	0x890F	--	2	7
□	✎	7	0x890F	--	2	7
□	✎	8	0x890F	--	2	7

Max. 80 (A max. of 10 entries per port.)

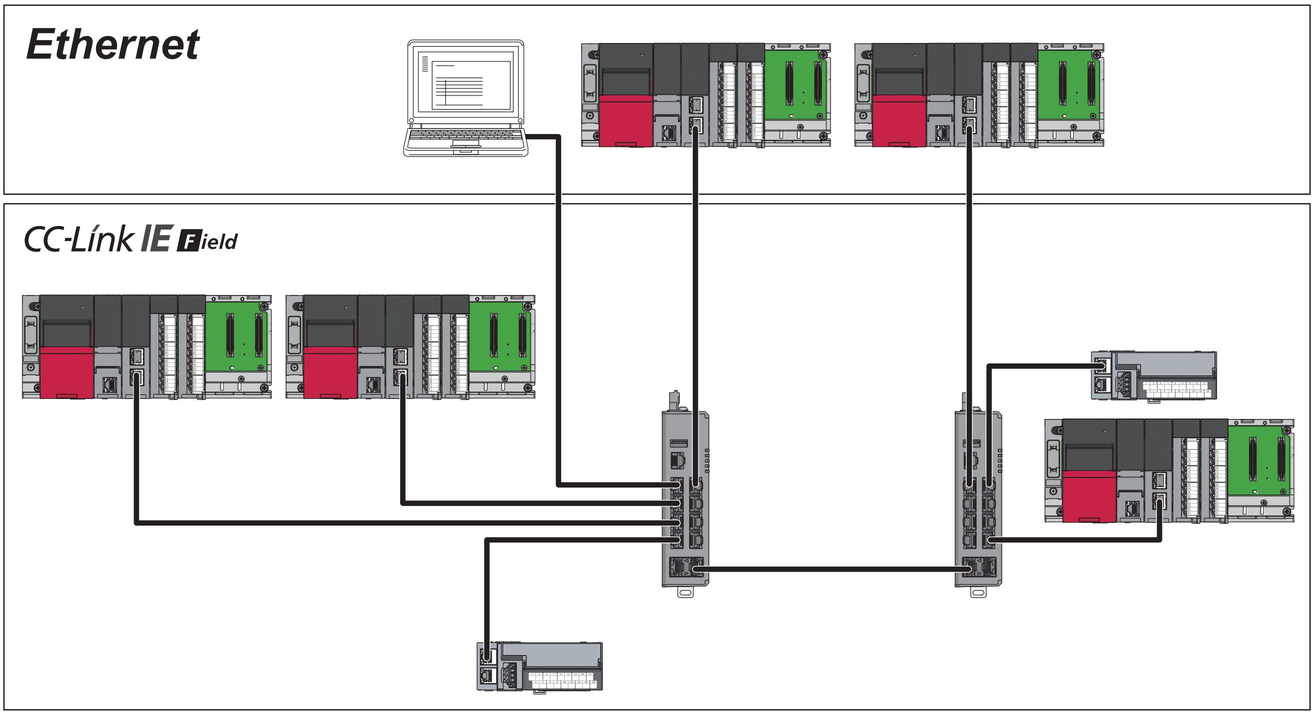
Precautions

To mix the CC-Link IE Field Network compatible devices and CC-Link IE TSN compatible devices in the network where multiple managed switches are present, do not share the wiring through the trunk port. Doing so may cause the disconnection of all stations.

Mixing CC-Link IE Field Network compatible devices and Ethernet devices

System configuration example

The following figure shows an example of a system configuration in which CC-Link IE Field Network compatible devices and Ethernet devices are mixed.



Setting example

Set the VLAN and delete unnecessary per-stream priority settings, in the same way when connecting CC-Link IE Field Network compatible devices whose network numbers differ from one another. (☞ Page 48 Connecting devices whose network numbers differ from one another)

Restrictions

The following lists the restrictions for connecting the CC-Link IE Field Network compatible devices.

- The CC-Link IE Field Network synchronous communication function is not supported.
- The fast link-up function is not supported.

7 PARAMETER SETTINGS

The following two methods are available to set parameters for the managed switch.

- Setting parameters from the web interface
- Setting parameters from the CLI

Precautions

Take the following measures to prevent theft, tampering, faulty operation, unauthorized execution resulting from unauthorized access by an outsider.

- Change the password from the default. Use alphanumeric characters (a to z, A to Z, and 0 to 9), and the password must be 11 characters or longer in length. (☞ Page 97 User account setting function [User Account], ☞ Page 280 Configure User Account Setting)
- Give administrator privileges to only the administrator account. (☞ Page 97 User account setting function [User Account], ☞ Page 280 Configure User Account Setting)
- After the operation, log out from the managed switch immediately. (☞ Page 384 Logout, ☞ Page 392 Logout)

7.1 Web Interface

This section describes how to set parameters from the web interface.

Google Chrome® is recommended for the web browser.

Connection to the web interface

The managed switch supports direct connection to a personal computer through an Ethernet cable and connection through a network. The following describes the procedure for login to the managed switch.

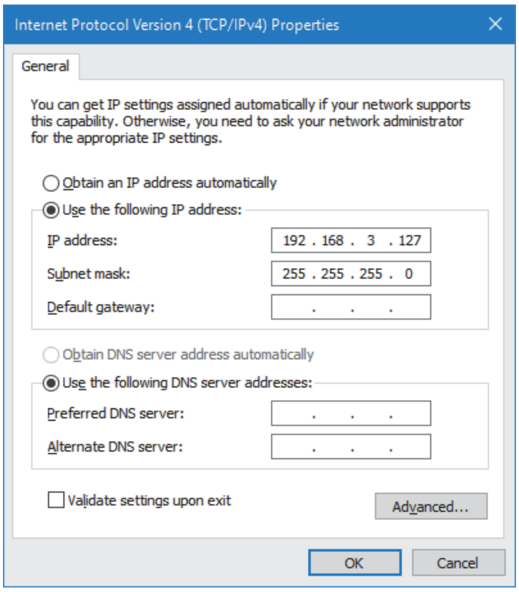
Operating procedure

1. Connect a personal computer to the managed switch with an Ethernet cable.

2. Set the IP address of the personal computer to the same network as the managed switch. (The window shown below is that on Windows 10.)

By default, the IP address of the managed switch is set as follows.

- IP address: 192.168.3.252
- Subnet mask: 255.255.255.0



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 3 . 127

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

3. Connect to the web interface.

For connection, input the IP address of the managed switch to the web browser on the personal computer.

- http:// followed by the set IP address

For connection through encrypted communications (SSL communications), input as follows.

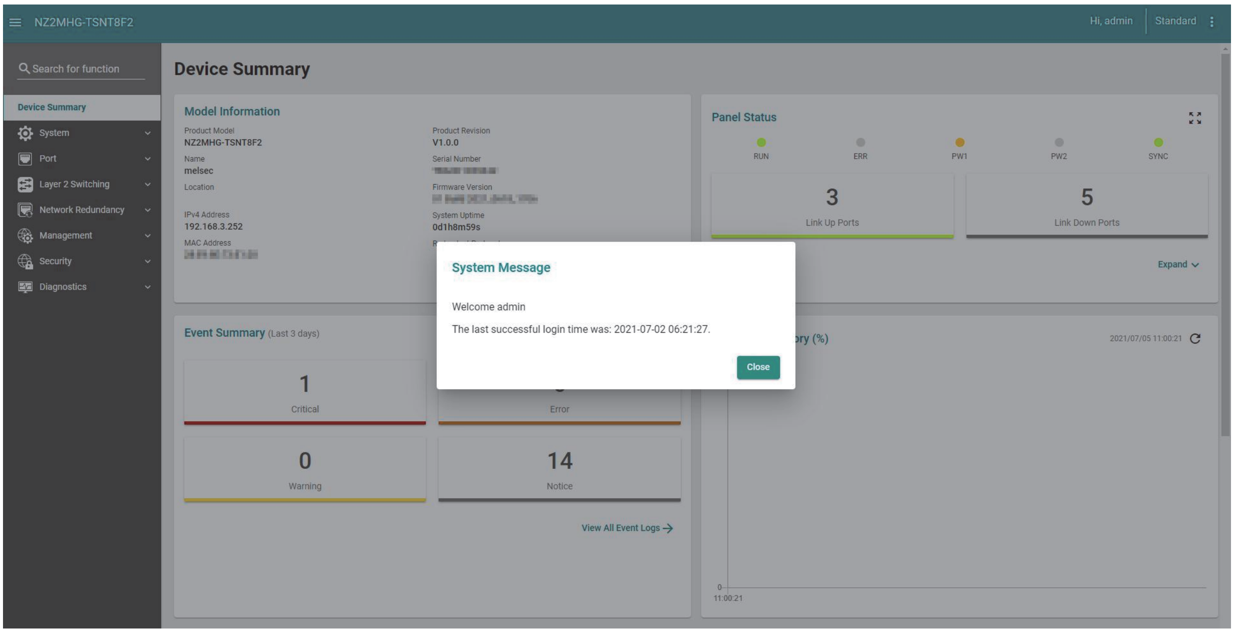
- https:// followed by the set IP address

4. Log in to the managed switch.

For login, input the account information. By default, the login information is set as follows.

- User name: admin
- Password: admin

5. If the login is successful, the dialog and the web interface window appear.



Device Summary

Model Information

Product Model: NZ2MHG-TSNT8F2

Product Revision: V1.0.0

Name: melsec

Serial Number: [redacted]

Location:

Firmware Version: [redacted]

IPv4 Address: 192.168.3.252

System Uptime: 0d1h8m59s

MAC Address: [redacted]

System Message

Welcome admin

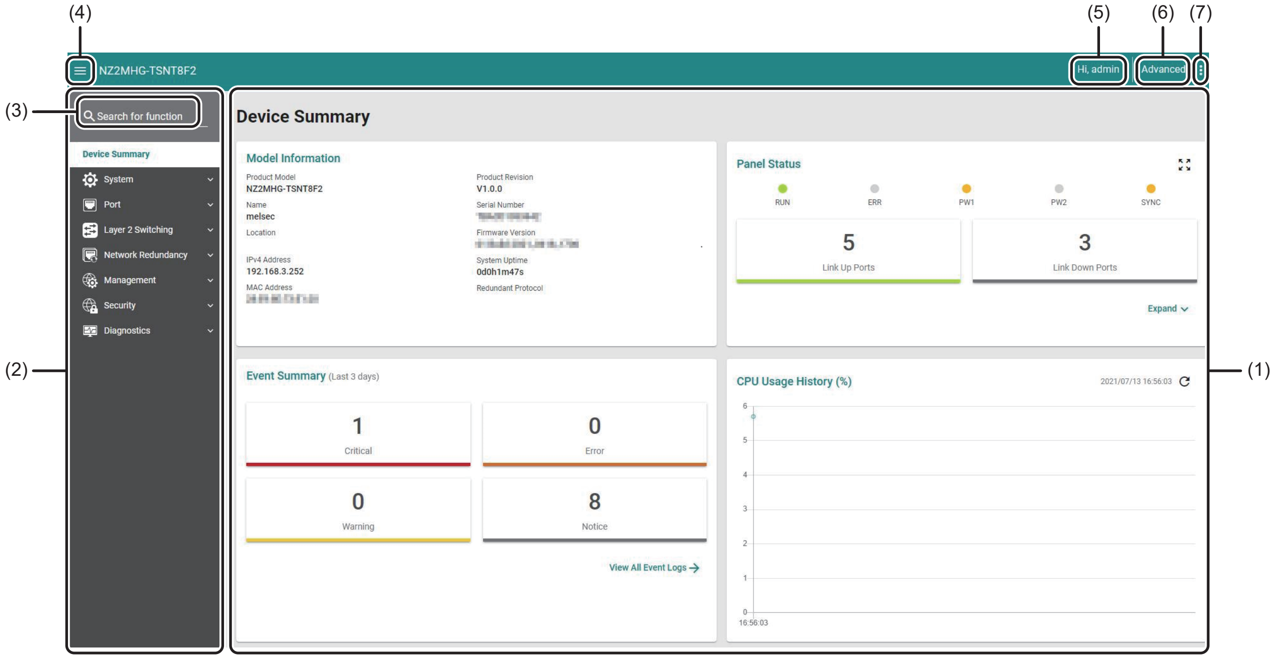
The last successful login time was: 2021-07-02 06:21:27.

Precautions

- When a proxy server is used, connection to the web interface may fail depending on the proxy server settings. If connection to the web interface fails, check and correct the proxy server settings.
- Connection to the web interface may fail depending on the firewall settings. If connection to the web interface fails, check and correct the firewall settings.
- When connecting to the web interface, enable JavaScript and cookies from the web browser setting.

Window structure

This section describes the window structure of the web interface.



Device Summary

Model Information

Product Model NZ2MHG-TSNT8F2

Name melsec

Location

IPv4 Address 192.168.3.252

MAC Address [redacted]

Product Revision V1.0.0

Serial Number [redacted]

Firmware Version [redacted]

System Uptime 0d0h1m47s

Redundant Protocol

Panel Status

5 Link Up Ports

3 Link Down Ports

Event Summary (Last 3 days)

1 Critical

0 Error

0 Warning

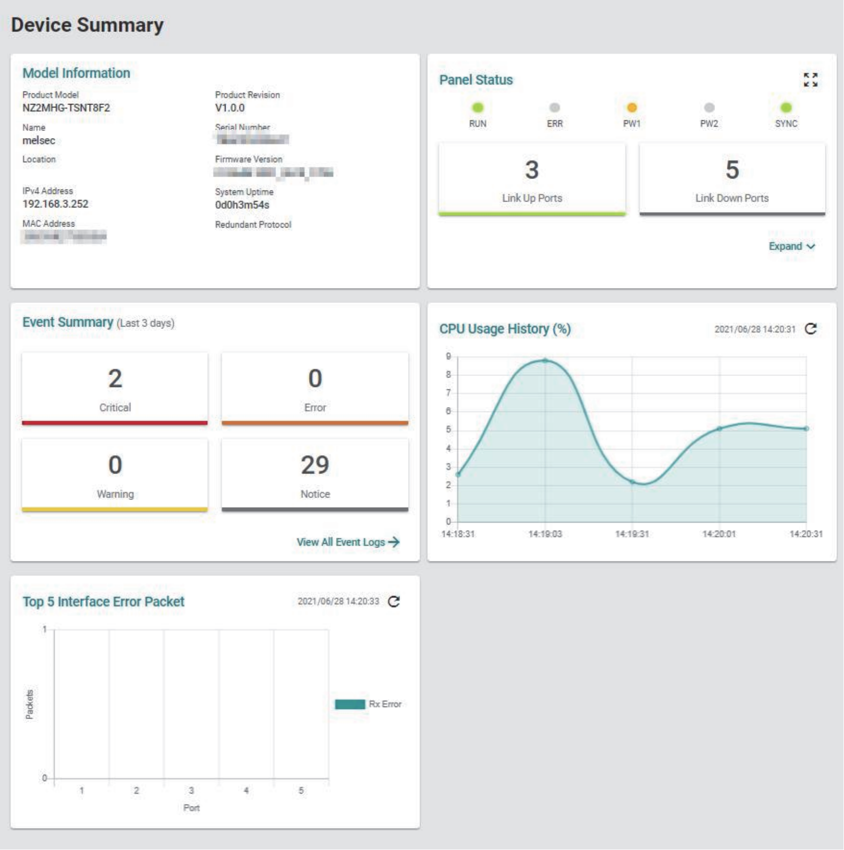
8 Notice

CPU Usage History (%) 2021/07/13 16:56:03

No.	Name	Description
(1)	Function area	Displays the window of each function.
(2)	Function menu	Displays all the managed switch functions in a tree format. Click the function name to display the window of the clicked function in the function area.
(3)	Search bar	Allows any function to be searched from the function menu.
(4)	Menu button	Click the menu button to show or hide the function menu and search bar.
(5)	Login name	Displays the login account name.
(6)	Setting mode	Displays the current setting mode. (☞ Page 385 Configuration mode change)
(7)	Menu icon button	Click the menu icon button to display Maintenance and Tool (Maintenance/Tool).

Device Summary

When the login is successful, the function area displays the "Device Summary" window. From "Device Summary", various types of information on the managed switch can be checked. The following image shows the window structure of "Device Summary".



Device Summary

Model Information

Product Model
NZ2MHG-TSNT8F2

Product Revision
V1.0.0

Name
melsec

Serial Number
[redacted]

Location

Firmware Version
[redacted]

IPv4 Address
192.168.3.252

System Uptime
0d0h3m54s

MAC Address
[redacted]

Redundant Protocol

Panel Status

● RUN ● ERR ● PW1 ● PW2 ● SYNC

3 Link Up Ports

5 Link Down Ports

Expand

Event Summary (Last 3 days)

2 Critical

0 Error

0 Warning

29 Notice

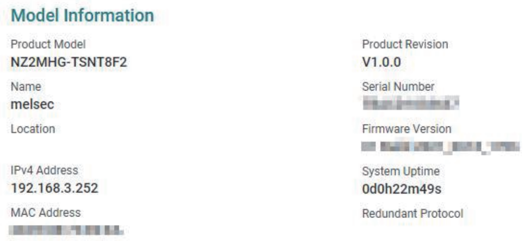
View All Event Logs →

CPU Usage History (%) 2021/06/28 14:20:31

Top 5 Interface Error Packet 2021/06/28 14:20:33

■Model Information

This area displays information related to the managed switch.



Model Information

Product Model
NZ2MHG-TSNT8F2

Name
melsec

Location

IPv4 Address
192.168.3.252

MAC Address
[redacted]

Product Revision
V1.0.0

Serial Number
[redacted]

Firmware Version
[redacted]

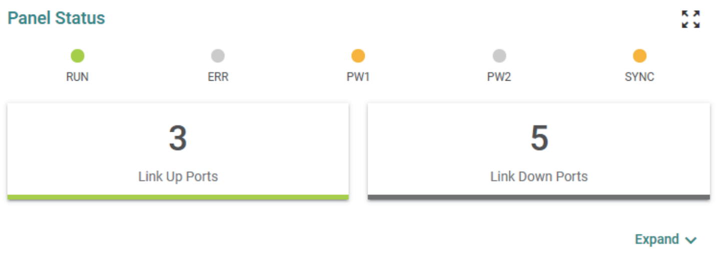
System Uptime
0d0h22m49s

Redundant Protocol

Item	Description
Product Model	Displays the product model name.
Name	Displays the device name.
Location	Displays the location where the managed switch is used.
IPv4 Address	Displays the IPv4 address of the managed switch.
MAC Address	Displays the MAC address of the managed switch.
Product Revision	Displays the product version.
Serial Number	Displays the serial number.
Firmware Version	Displays the firmware version.
System Uptime	Displays the time elapsed after system start-up.
Redundant Protocol	Displays the redundancy protocol in use.

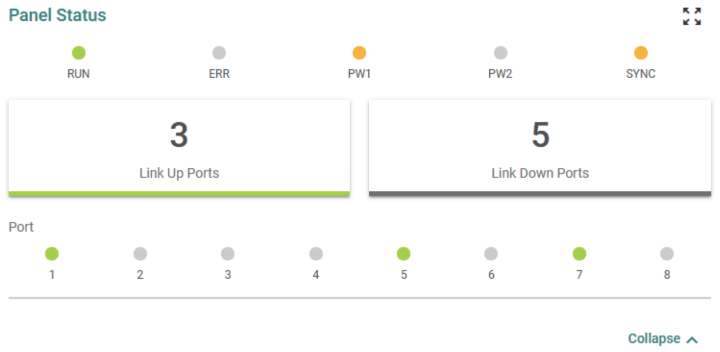
■Panel Status

The LED indication status of the managed switch and the port link status can be checked from the web interface.

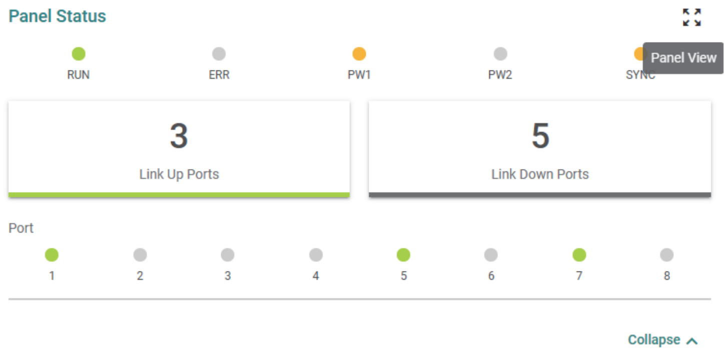


- Link Up Ports: Displays the number of link-up ports.
- Link Down Ports: Displays the number of link-down ports.

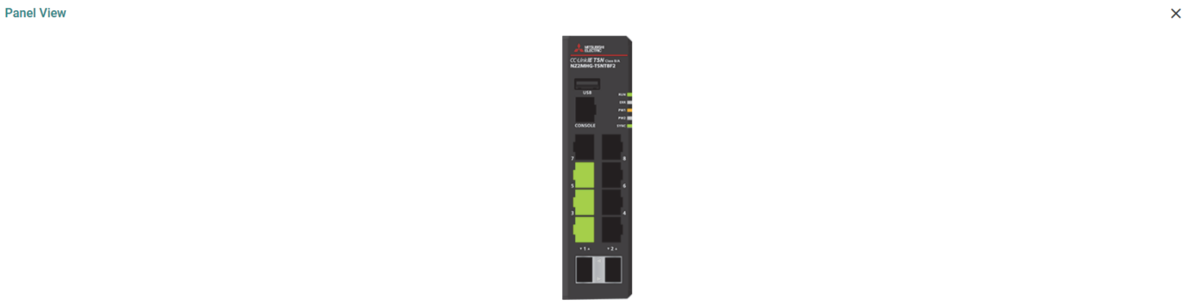
Click the [Expand] button at the lower right of the window to acquire the detailed port information.



Click the [Panel View] icon at the upper right of the window to check various types of statuses from the external view of the managed switch.



↓

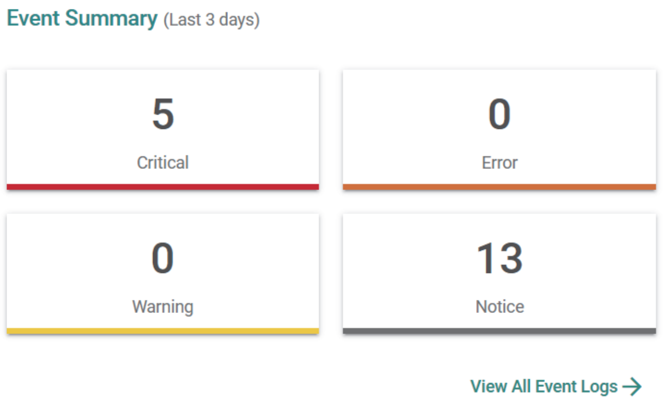


Precautions

- The Panel Status window is updated at an interval of approximately 30 seconds.
- This window does not support the LED indication that indicates the statuses where the USB flash drive is being accessed or automatic restoration is in progress.

■Event Summary

The total value of the events registered in the last three days is displayed. Click the [View All Event Logs] button to move to "Event Log". (☞ Page 250 Event log [Event Log])



Event Summary (Last 3 days)

5 Critical

0 Error

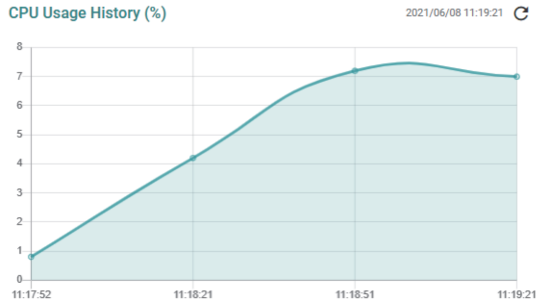
0 Warning

13 Notice

View All Event Logs →

■CPU Usage History

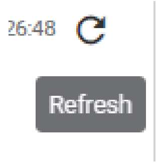
The CPU utilization of the managed switch is displayed in a graph. The current CPU utilization is reacquired at regular intervals to update the graph.



Vertical axis: CPU utilization
Horizontal axis: Web browser time at data acquisition

Point

The graph can also be updated by clicking the [Refresh] icon.



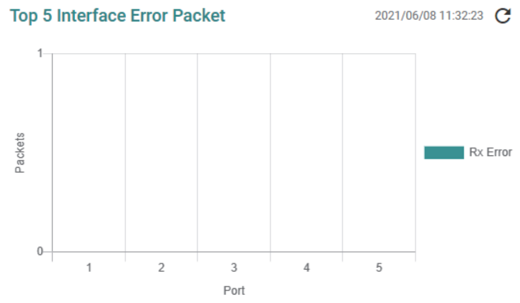
■Top 5 Interface Error Packet

The number of error packets in the managed switch is displayed in a graph in descending order. The current number of error packets is reacquired at regular intervals to update the graph.

The number of error packets is the total value of the following items. For details, refer to the following. (☞ Page 229 Statistical information [Statistics])

- CRC Align Error Packets
- Drop Packets
- Undersize
- Oversize Packets

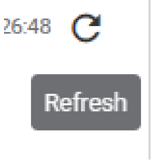
For the NZ2MHG-TSNT4, the number of error packets for Port 1 to 4 is displayed.



Vertical axis: Number of error packets
Horizontal axis: Port number

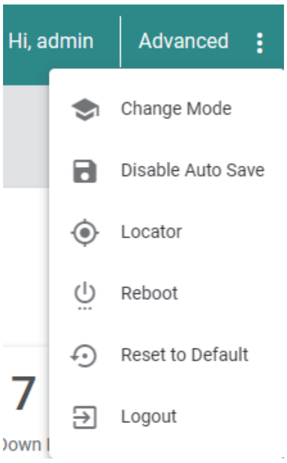
Point

The graph can also be updated by clicking the [Refresh] icon.



Maintenance and Tool

The following functions can be operated by clicking the [Menu icon] button at the upper right of the window. (☞ Page 385 Maintenance/Tool)



Parameters

This section describes how to set parameters from the web interface.

For details on how to set parameters for each function, refer to the following.

☞ Page 69 FUNCTIONS

Required parameters

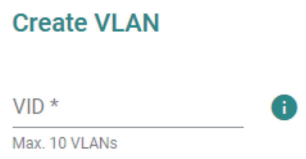
Parameters marked with an asterisk (*) are those that need to be input when each function is set.

The following buttons cannot be clicked if the required item is not input or if the setting value is out of range.

- [Create] button
- [Apply] button

Ex.

Create VLAN



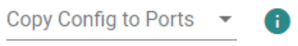
Create VLAN

VID *

Max. 10 VLANs

Copying the settings to multiple ports

The setting parameters of a port can be copied to other ports. From the drop-down menu, select the copy destination port. Multiple copy destination ports can be selected.



Copy Config to Ports

Applying the settings

Click the [Create] button or the [Apply] button.

Precautions

If any facility or device connected to the managed switch is operating, unexpected operations may occur. Before setting the parameters, stop the operation of the facility or device.

Enabling or disabling the settings

For some settings, the function can be enabled and disabled. The function can be enabled or disabled as needed without having to reconfigure the same setting.

Search function

Input a keyword in the Search bar to display only the related items.

Search

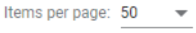
Output function

Click the [Export] icon to output the current setting status in CSV format (character code: UTF-8) or PDF format.

Number of display items

The number of items to be displayed per page can be set. The number of display items can be selected from the values listed below.

- 50
- 100
- 200
- 1000



Items per page: 50

7.2 CLI

This section describes how to set parameters with the CLI.

CLI connection through the RS-232

The following describes the procedure for login to the managed switch.

Operating procedure

1. Connect a personal computer to the managed switch with the provided console cable. (☞ Page 36 Wiring to the console port)

2. Set a terminal emulator.

Set the serial communication setting for the terminal emulator as shown below.

- Baud rate (BPS): 115200
- Data length: 8 bits
- Stop bit: 1 bit
- Parity: None

3. Connect to the managed switch from the terminal emulator.

4. Log in to the managed switch.

For login, input the account information. By default, the login information is set as follows.

- User name: admin
- Password: admin

5. When the login is successful, the command input is enabled. (☞ Page 263 Command Line Interface Commands)

CLI connection through Telnet

The managed switch supports direct connection to a personal computer through an Ethernet cable and connection through a network. The following describes the procedure for login to the managed switch.

Operating procedure

1. Connect a personal computer to the managed switch with an Ethernet cable.

2. Set the IP address of the personal computer to the same network as the managed switch.

By default, the IP address of the managed switch is set as follows.

- IP address: 192.168.3.252
- Subnet mask: 255.255.255.0

3. Start a Telnet client and input the following IP address and port number.

- IP address: 192.168.3.252
- Port number: 23 (Default)

For connection through SSH encrypted communications, use an SSH client.

4. Log in to the managed switch.

For login, input the account information. By default, the login information is set as follows.

- User name: admin
- Password: admin

5. When the login is successful, the command input is enabled. (☞ Page 263 Command Line Interface Commands)

Precautions

With the initial values, connection cannot be established from multiple Telnet clients to the same managed switch.

With the following parameter setting, up to five modules can be concurrently connected.

■Changing the maximum number of concurrent connections from the web interface

Interface management function (☞ Page 202 Interface management function [Management Interface])

■Command example for changing the maximum number of concurrent connections from the CLI

```
melsec# !
melsec# configure terminal
melsec(config)# ip terminal max-session <session-number (Number of Telnet clients to be concurrently connected)>
```

8 FUNCTIONS

8.1 System Management [System Management]

The following functions can be used from the system management [System Management] displayed on the function menu of the web interface.

- Device information setting [Information Setting]
- Firmware upgrade function [Firmware Upgrade]
- Configuration backup and restoration [Config Backup and Restore]
- Event log output function [Event Log Backup]

Device information setting [Information Setting]

Any device information can be set to the managed switch. Set the device information in advance to easily identify the managed switch when monitoring via a network. In addition, the contact information (such as email address and phone number) to be used when a problem occurs can also be set.

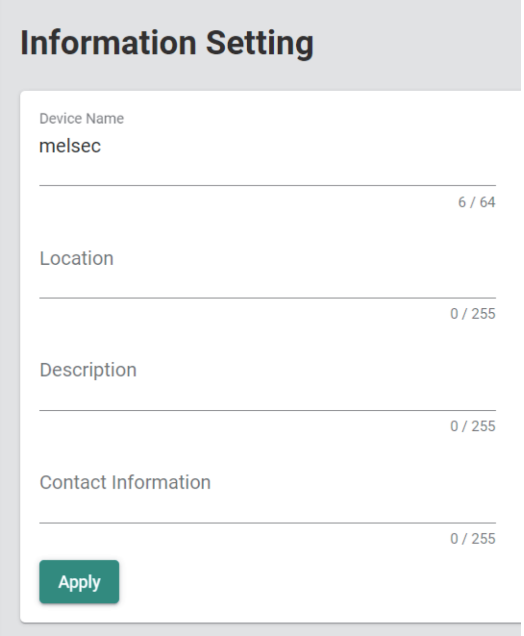
Setting method

Operating procedure

1. Start the operation from the "Information Setting" window.

[System] ⇨ [System Management] ⇨ [Information Setting]

2. Set the required items.



Information Setting

Device Name
melsec
6 / 64

Location
0 / 255

Description
0 / 255

Contact Information
0 / 255

Apply

Item	Description	Setting range
Device Name	Set the device name of the managed switch. The device name cannot be left empty.	1 to 64 characters (one-byte alphanumeric characters and symbols) (Default: melsec)
Location	Set the location where the managed switch is used.	0 to 255 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Description	Set the detailed description of the managed switch.	0 to 255 characters (one-byte alphanumeric characters and symbols) (Default: empty)

Item	Description	Setting range
Contact Information	Input the contact information such as email address and phone to be used when a problem occurs.	0 to 255 characters (one-byte alphanumeric characters and symbols) (Default: empty)

3. Click the [Apply] button.

Restriction

The following restrictions are applied for "Device Name".

- Lower-case alphabetic characters (a to z), numbers (0 to 9), and special character (hyphen "-") are to be used.
- The special character (hyphen "-") cannot be used as the first character or the last character.
- Input formats such as port-xyz cannot be used. (When a number (0 to 9) is set for all x, y, and z)
- Input formats such as port-xyz-abcde cannot be used. (When a number (0 to 9) is set for all x, y, z, a, b, c, d, and e)

Firmware upgrade function [Firmware Upgrade]

The firmware version of the managed switch can be updated. The firmware file (*.rom) can be downloaded from the Mitsubishi Electric FA website. Store the firmware file into a location in any of the following four types from which the file will be read.

- Local drive
- SFTP server
- TFTP server
- USB flash drive

Precautions

- Before updating the firmware, download the latest firmware file (*.rom) from the Mitsubishi Electric FA website.[*1]
- After the firmware update is complete, the managed switch automatically restarts. For devices connected with the managed switch, communication is interrupted until the managed switch is started up again. Before executing the firmware update, stop the operation of any connected facilities or devices that are running. Otherwise, unexpected operations may occur.
- After updating the firmware, check that the firmware version is updated. (☞ Page 59 Device Summary)

[*1] The file name is described below. (ff: Firmware version, yyyy_mmdd_hhmm: Build time)
For the NZ2MHG-TSNT8F2: NZ2MHG-TSNT8F2_ff_yyyy_mmdd_hhmm.rom
For the NZ2MHG-TSNT4: NZ2MHG-TSNT4_ff_yyyy_mmdd_hhmm.rom

Point

Various types of data such as parameters and event logs are inherited after the firmware is updated.

Local drive

Import the firmware file into a device such as a personal computer. Execute the update from a device such as a personal computer.

SFTP server or TFTP server

Import the firmware file into an SFTP server or TFTP server. From the web interface, specify the Server IP Address and execute the update.

USB flash drive

Import the firmware file into a device such as a personal computer. Write the firmware file from a device such as a personal computer into the USB flash drive, connect the USB flash drive to the USB port of the managed switch, and execute the update.

Setting method

■Local drive

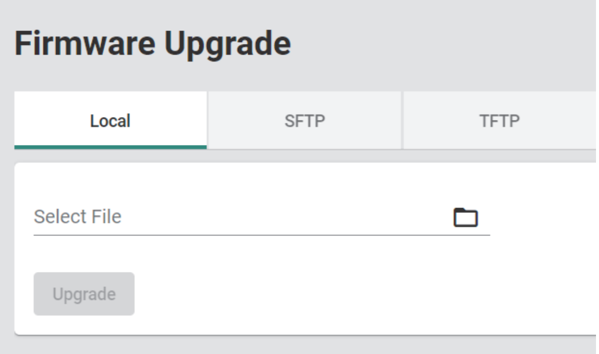
Operating procedure

1. Start the operation from the "Firmware Upgrade" window.

[System] ⇨ [System Management] ⇨ [Firmware Upgrade]

2. Select the [Local] tab.

3. Select the firmware file (* .rom).



4. Click the [Upgrade] button.

The firmware update is executed. After the firmware update is complete, the managed switch automatically restarts.

■SFTP server

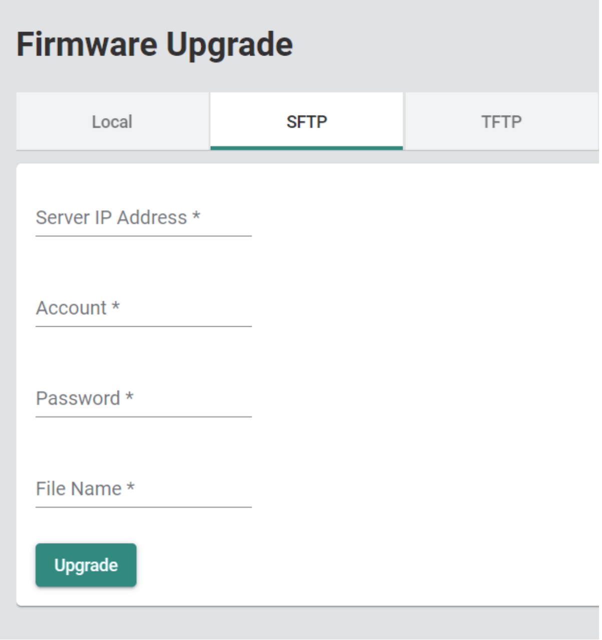
Operating procedure

1. Start the operation from the "Firmware Upgrade" window.

[System] ⇨ [System Management] ⇨ [Firmware Upgrade]

2. Select the [SFTP] tab.

3. Set the required items.



Firmware Upgrade

Item	Description	Setting range
Server IP Address	Input the IP address of the server where the firmware file is stored.	0.0.0.1 to 255.255.255.254 (Default: empty)
Account	Input the account name for server connection.	One-byte alphanumeric characters and symbols (Default: empty)
Password	Input the password of the account for server connection.	One-byte alphanumeric characters and symbols (Default: empty)
File Name	Input the file name of the firmware file.	One-byte alphanumeric characters and symbols (Default: empty)

4. Click the [Upgrade] button.

After the firmware update is complete, the managed switch automatically restarts.

■TFTP server

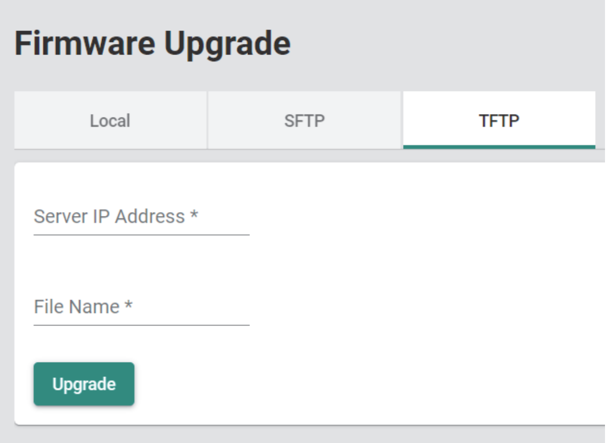
Operating procedure

1. Start the operation from the "Firmware Upgrade" window.

[System] ⇨ [System Management] ⇨ [Firmware Upgrade]

2. Select the [TFTP] tab.

3. Set the required items.



Firmware Upgrade

Item	Description	Setting range
Server IP Address	Input the IP address of the server where the firmware file is stored.	0.0.0.1 to 255.255.255.254 (Default: empty)
File Name	Input the file name of the firmware file.	One-byte alphanumeric characters and symbols (Default: empty)

4. Click the [Upgrade] button.

After the firmware update is complete, the managed switch automatically restarts.

■USB flash drive

Operating procedure

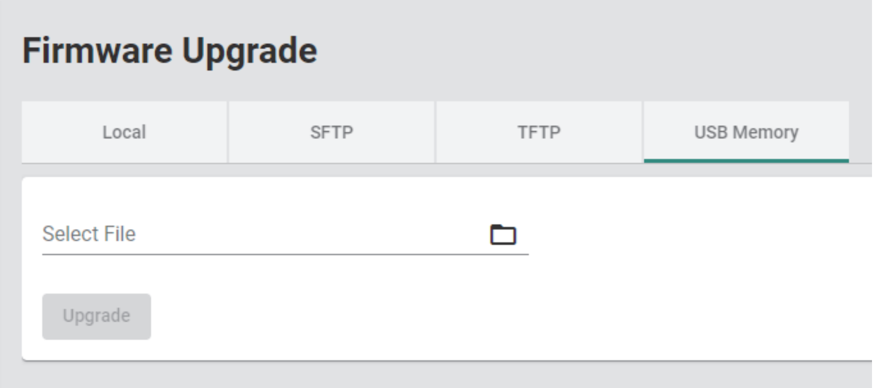
1. Create the \NZ2MHG-TSNT8F2 or \NZ2MHG-TSN4 folder in the USB flash drive using a device such as a personal computer and store the firmware file (.rom) into the created folder. Match the folder name with the model name of the managed switch to be updated.

2. Connect the USB flash drive to the USB port of the managed switch and check that the RUN LED flashes green.

3. Display the "Firmware Upgrade" window.

[System] ⇨ [System Management] ⇨ [Firmware Upgrade]

4. Select the [USB Memory] tab.



5. Click "Select File" to display the files in the USB flash drive in the dialog. Select the firmware file (*.rom) in the USB flash drive and click the [Select] button.

6. Click the [Upgrade] button.

After the firmware update is complete, the managed switch automatically restarts.

Configuration backup and restoration [Configuration Backup and Restore]

The parameters of the managed switch can be backed up or restored as the configuration file.

The configuration file can be copied when the managed switch is replaced or when the same parameters are reflected to multiple managed switches. Also, the configuration file can be encrypted.

The backup function and restoration function can be used in the following ways.

- Backup or restoration by web interface operations
- Automatic restoration using a USB flash drive

Backup or restoration by web interface operations

Operate the web interface and back up the configuration file to a desired save location. Also, restore the settings from the configuration file saved in a desired save location. The configuration file to be used can be encrypted.

The following four types can be selected for the save location of the configuration file to be used for backup or restoration.

- Local drive
- SFTP server
- TFTP server
- USB flash drive

■Local drive

Import the configuration file to a device such as a personal computer. Restore the configuration file from a device such as a personal computer.

■SFTP server or TFTP server

Import the configuration file to an SFTP server or TFTP server. On the web interface, specify the Server IP Address and restore the configuration file.

■USB flash drive

Import the configuration file into a USB flash drive. Restore the configuration file from the USB flash drive.

Precautions

- Restore the configuration file backed up for the product whose model name and firmware version are the same.
- The larger configuration file size increases the required restoration time.

Setting method

■Local drive (Backup)

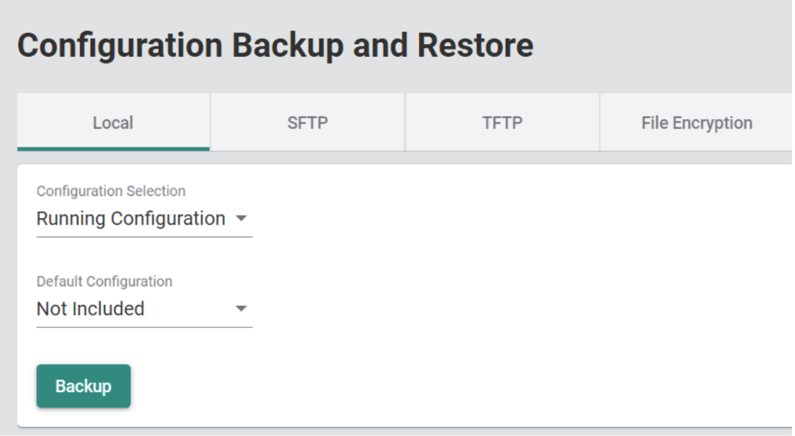
Operating procedure

1. Start the operation from the "Configuration Backup and Restore" window.

🖱 [System] ⇨ [System Management] ⇨ [Config Backup and Restore]

2. Select the [Local] tab.

3. Set the required items.



Configuration Backup and Restore

Configuration Selection: Running Configuration

Default Configuration: Not Included

Item	Description	Setting range
Configuration Selection	Select whether to back up the settings during operation or at startup. • Running Configuration: The settings during operation are backed up. • Startup Configuration: The settings at startup are backed up.	• Running Configuration • Startup Configuration (Default: Running Configuration)
Default Configuration	Set whether to include the default settings in the backup. • Not Included: The default settings are not included at backup. • Included: The default settings are included at backup.	• Not Included • Included (Default: Not Include)

4. Click the [Backup] button.

Precautions

To output the startup configuration file (Startup Configuration) of the managed switch, disable the auto save function before setting the parameters. If the auto save function is enabled, the parameters set after startup are reflected to the startup configuration file of the managed switch.

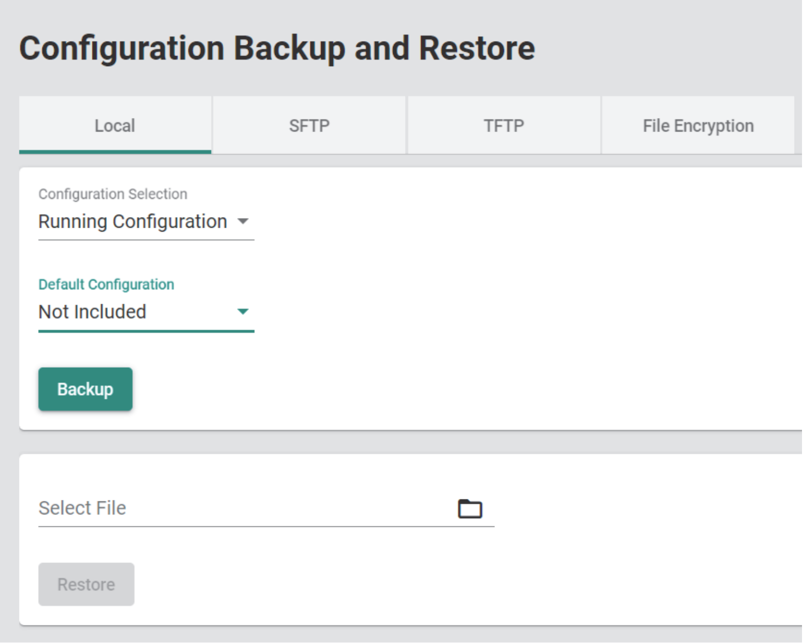
■Local drive (Restoration)

Operating procedure

1. Start the operation from the "Configuration Backup and Restore" window.

[System] ⇨ [System Management] ⇨ [Config Backup and Restore]

2. Select the [Local] tab.

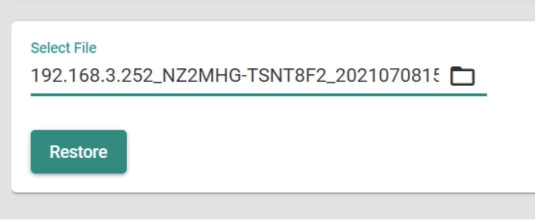


Configuration Backup and Restore

Configuration Selection: Running Configuration

Default Configuration: Not Included

3. Select the configuration file (*.ini).



Select File: 192.168.3.252_NZ2MHG-TSNT8F2_202107081

Item	Description	Setting range
Select File	Select the configuration file to be restored.	—

4. Click the [Restore] button.

■SFTP server (Backup)

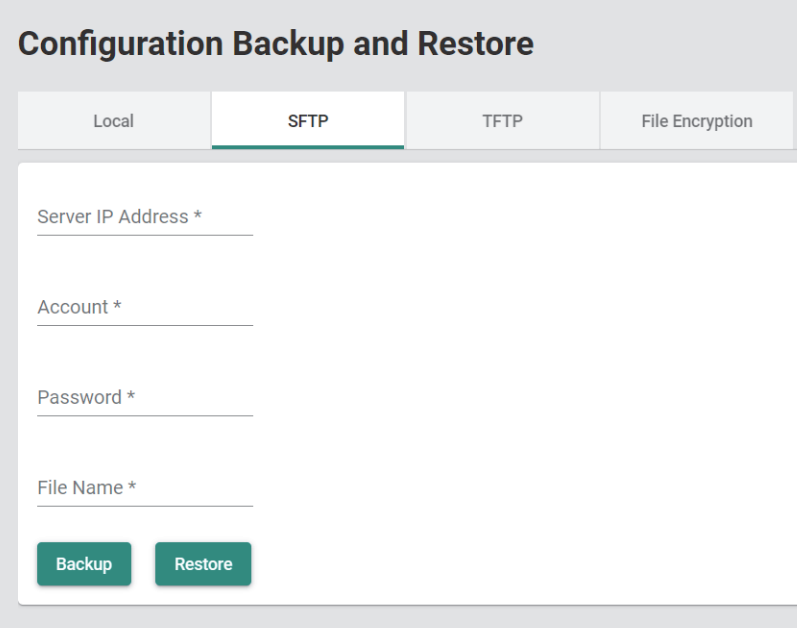
Operating procedure

1. Start the operation from the "Configuration Backup and Restore" window.

[System] ⇨ [System Management] ⇨ [Config Backup and Restore]

2. Select the [SFTP] tab.

3. Set the required items.



Configuration Backup and Restore

Item	Description	Setting range
Server IP Address	Input the IP address of the server where the configuration file is output.	0.0.0.1 to 255.255.255.254 (Default: empty)
Account	Input the account name for server connection.	One-byte alphanumeric characters and symbols (Default: empty)
Password	Input the password of the account for server connection.	One-byte alphanumeric characters and symbols (Default: empty)
File Name	Input the file name.	One-byte alphanumeric characters and symbols (Default: empty)

4. Click the [Backup] button.

Precautions

The startup configuration (excluding the default settings) of the managed switch is output to the configuration file. If the auto save function is enabled, the parameters set after startup are output to the configuration file.

■SFTP server (Restoration)

Operating procedure

1. Procedures 1 and 2 are the same as those for the operating procedure for backup.

For restoration, input the IP address of the server whose "Server IP Address" contains the configuration file.

2. Click the [Restore] button to restore the configuration file.

■TFTP server (Backup)

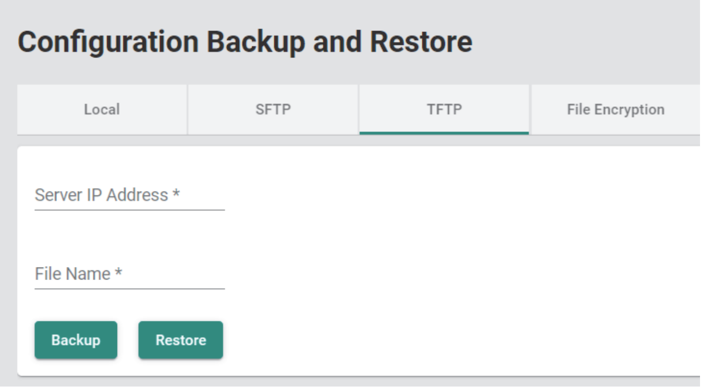
Operating procedure

1. Start the operation from the "Configuration Backup and Restore" window.

[System] ⇨ [System Management] ⇨ [Config Backup and Restore]

2. Select the [TFTP] tab.

3. Set the required items.



Configuration Backup and Restore

Server IP Address *

File Name *

Item	Description	Setting range
Server IP Address	Input the IP address of the server where the configuration file is output.	0.0.0.1 to 255.255.255.254 (Default: empty)
File Name	Input the file name.	One-byte alphanumeric characters and symbols (Default: empty)

4. Click the [Backup] button.

Precautions

The startup configuration (excluding the default settings) of the managed switch is output to the configuration file. If the auto save function is enabled, the parameters set after startup are output to the configuration file.

■TFTP server (Restoration)

Operating procedure

1. Follow backup procedures 1 to 3.

For restoration, input the IP address of the server whose "Server IP Address" contains the configuration file.

2. Click the [Restore] button.

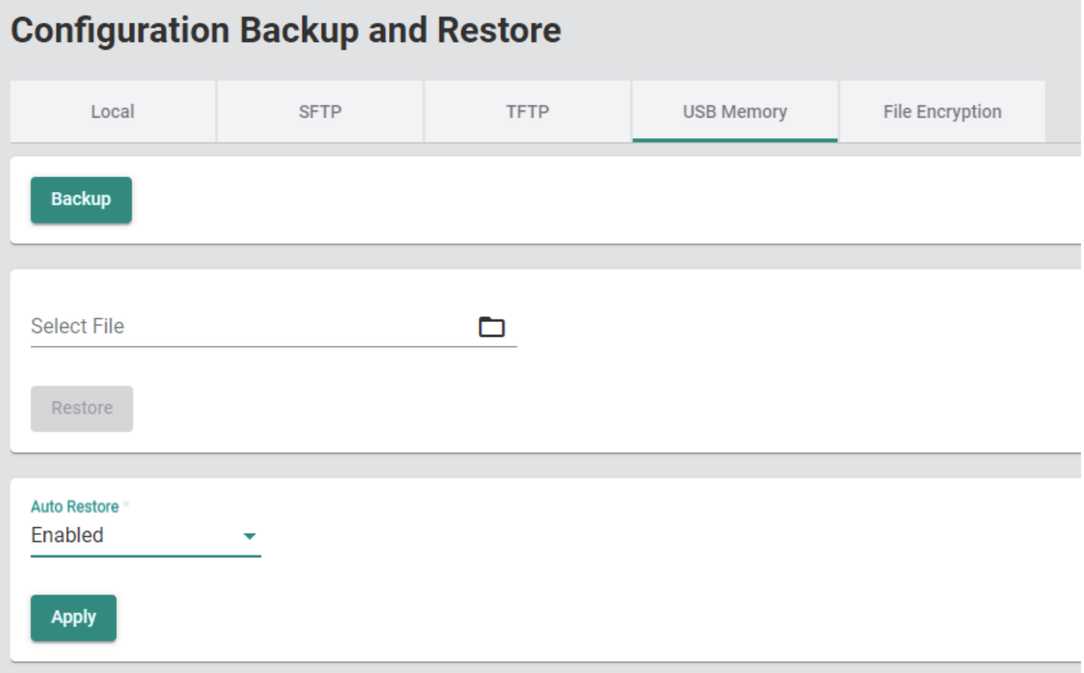
■USB flash drive (Backup)

Operating procedure

1. Connect the USB flash drive to the USB port of the managed switch and check that the RUN LED flashes green.
2. Display the "Configuration Backup and Restore" window.

[System] ⇨ [System Management] ⇨ [Config Backup and Restore]

3. Select the [USB Memory] tab.



Auto Restore: Enabled

4. Click the [Backup] button.
5. The following two configuration files are saved to \Model name\config in the USB flash drive. When any file already present in the save destination has the same name as the generated file, the file is overwritten. When the configuration files are saved, the save time and date of the file is added to the file name in the YYYYMMDDHHmm format. (Example: 192.168.3.252_NZ2MHG-TSNT8F2_202306301010.ini)

- Auto-backup_Model name.ini
- IP address_Model name_YYYYMMDDHHmm.ini

Precautions

In the configuration file, the settings for during operation are output and the default settings are not included.

Point

- When no save folder exists in the connected USB flash drive, the folder is automatically generated.
- The configuration file (Auto-backup_Model name.ini) can be used by the automatic restoration function without changing the file name.
- To restore the settings from the configuration file previously output by operating the web interface, use IP address_Model name_YYYYMMDDHHmm.ini as the configuration file.

■USB flash drive (Restoration)

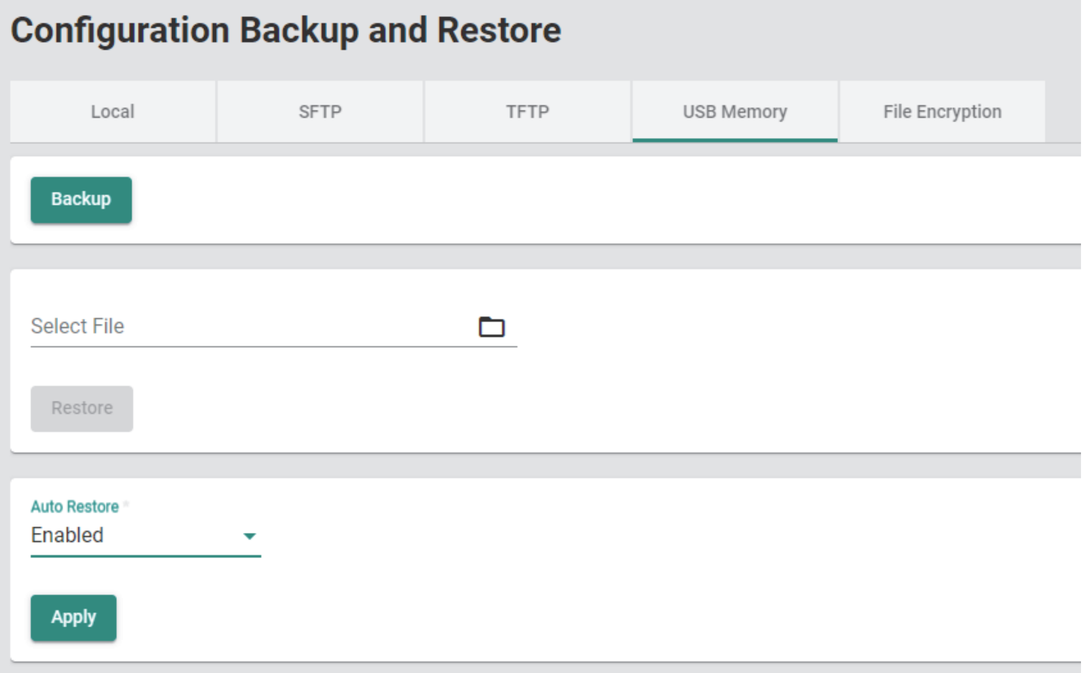
Operating procedure

1. Connect the USB flash drive to the USB port of the managed switch and check that the RUN LED flashes green.

2. Display the "Configuration Backup and Restore" window.

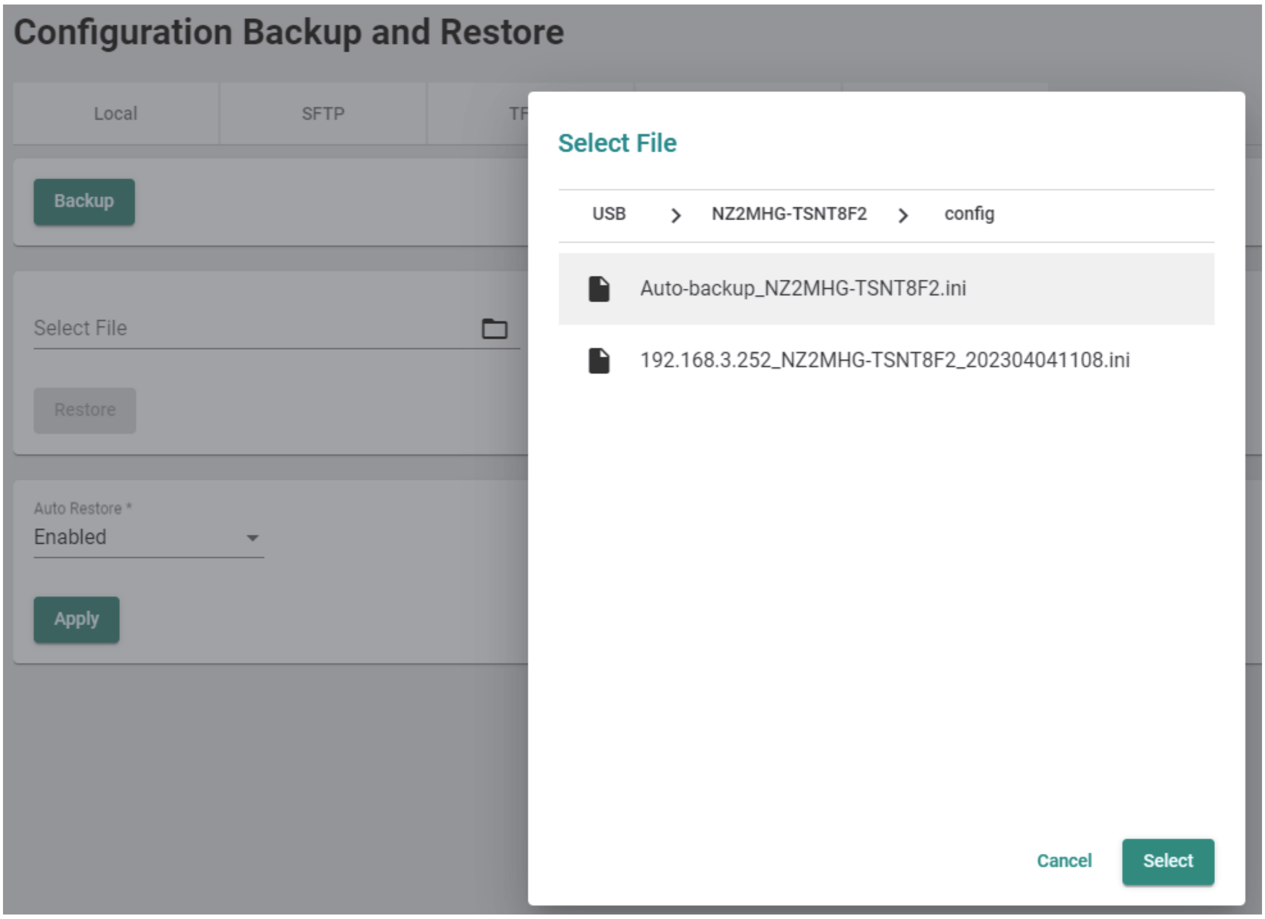
[System] ⇨ [System Management] ⇨ [Config Backup and Restore]

3. Select the [USB Memory] tab.



Auto Restore: Enabled

4. Click "Select File" to display the dialog. Select the configuration file (*.ini) saved in the USB flash drive and click the [Select] button.



Configuration Backup and Restore

Select File

USB > NZ2MHG-TSNT8F2 > config

Auto-backup_NZ2MHG-TSNT8F2.ini

192.168.3.252_NZ2MHG-TSNT8F2_202304041108.ini

Auto Restore *: Enabled

Item	Description	Setting range
Select File	Select the configuration file to be restored.	—

5. Click the [Restore] button.

Automatic restoration function

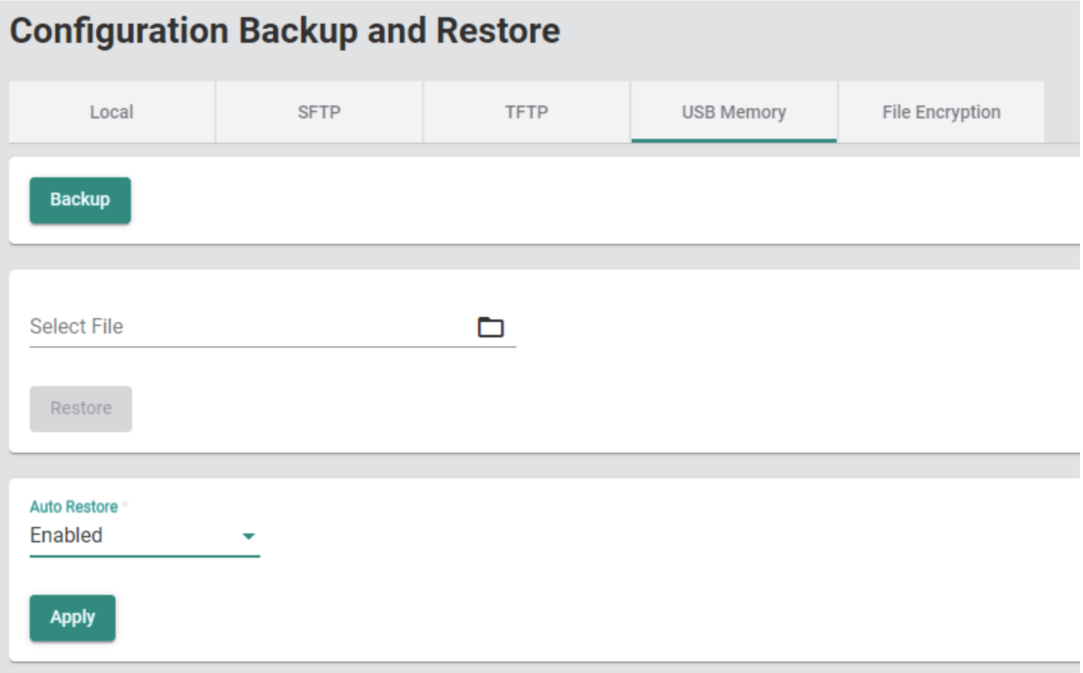
This function automatically restores the settings from the configuration file saved in the USB flash drive when the managed switch is powered-on or booted. By saving the configuration file into the USB flash drive in advance, the settings are restored without web interface operations. The configuration file to be used can be encrypted.

Operating procedure

1. Start the operation from the "Configuration Backup and Restore" window.

[System] ⇨ [System Management] ⇨ [Config Backup and Restore]

2. Select the [USB Memory] tab.



3. Set "Auto Restore" to "Enabled" and click the [Apply] button.

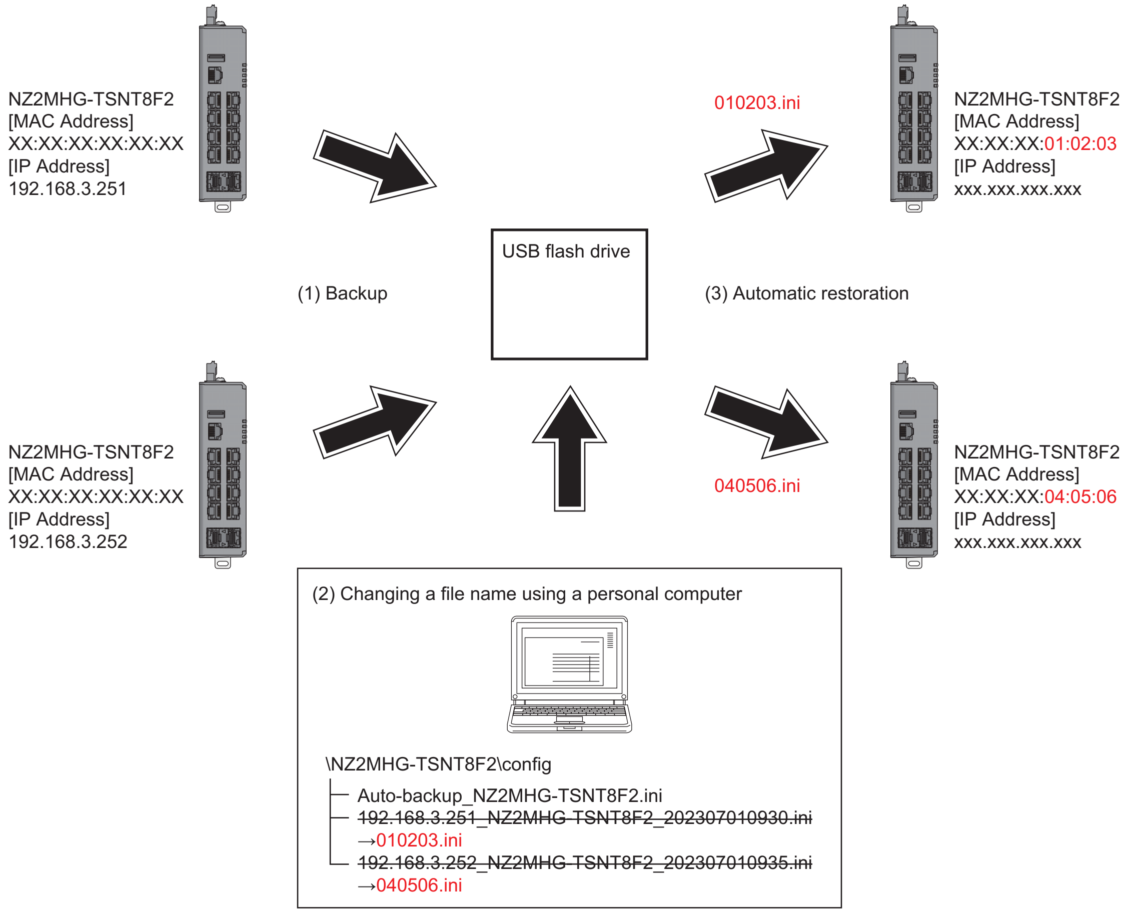
Item	Description	Setting range
Auto Restore	Select to enable or disable the configuration automatic restoration using the USB flash drive.	• Enabled • Disabled (Default: Enabled)

4. Store the configuration file into the \Model name\config folder in the USB flash drive. When the restoration is executed, the configuration file name is identified and the restoration is executed in accordance with the following priority order. Change the configuration file name as necessary.

Priority	File name	Description
High	MAC address information.ini	Change the file name to the MAC address (fourth octet to sixth octet) of the device to which the settings will be restored. (If the MAC address is 28:E9:8E:73:E0:12, change the file name to 73E012.ini.)
Low	Auto-backup_Model name.ini	This configuration file is generated when a configuration file is backed up in a USB flash drive. (If NZ2MHG-TSNT8F2 is used, the file name will be Auto-backup_NZ2MHG-TSNT8F2.ini.)

Point

By setting the configuration file name to a MAC address information.ini and executing automatic restoration, the same settings can be copied to a desired managed switch.



5. Connect a USB flash drive to the managed switch and power-on or reboot the switch. The settings are automatically restored. When automatic restoration is completed, the RUN LED flashes green (250ms interval).

Precautions

- Restore the configuration file backed up for the product whose model name and firmware version are the same.
- The larger configuration file size increases the required restoration time.
- The managed switch communicates using the pre-restoration settings until completion of automatic restoration. To prevent the communications using unintentional settings, check that automatic restoration is completed successfully before starting the main system operation. When it is completed successfully, the RUN LED flashes green (250ms interval) and the restoration log is recorded in the event log.
- The automatic restoration function will be executed even when there is no difference between the settings in the managed switch and those in the configuration file.
- To execute automatic restoration to a desired managed switch using MAC address information, check that the MAC address lower six digits of the managed switch to which automatic restoration is executed completely match the configuration file name. If no configuration file whose name matches the lower six digits can be detected, the configuration file whose name is an Auto-backup_Model name.ini will be automatically restored.
- If the managed switch could not detect any restorable configuration file, the switch skips the configuration automatic restoration, turns on the ERR LED, and starts the operation.
- When no USB flash drive is connected, no event logs related to normal/error completion of the automatic restoration function are registered. Also, the ERR LED does not turn on.

File encryption

■Backup

The following describes the procedure for encrypting the configuration file at backup.

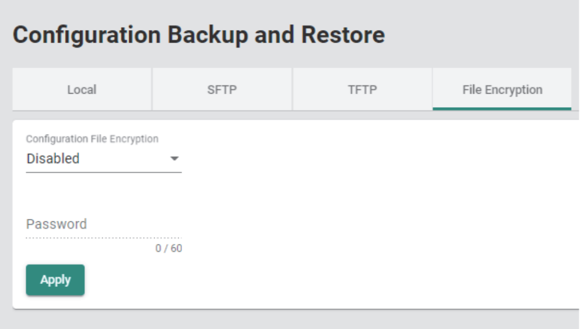
Operating procedure

1. Start the operation from the "Configuration Backup and Restore" window.

[System] ⇨ [System Management] ⇨ [Config Backup and Restore]

2. Select the [File Encryption] tab.

3. Set the required items.



Configuration Backup and Restore

Configuration File Encryption: Disabled

Password

Item	Description	Setting range
Configuration File Encryption	Enable or disable encryption of the configuration file. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)
Password	Input the password for encryption.	• When encryption is enabled: 1 to 60 characters (one-byte alphanumeric characters and symbols) • When encryption is disabled: Empty (Default: empty)

4. Click the [Apply] button.

5. The operating procedure for backup varies depending on the save location of the configuration file. For the operating procedure, refer to the following.

☞ Page 77 Setting method

Precautions

If "Configuration File Encryption" is "Disabled", "Password" cannot be set.

■Restoration

The following describes the procedure for restoring the encrypted configuration file.

Operating procedure

1. Start the operation from the "Configuration Backup and Restore" window.

🖱 [System] ⇨ [System Management] ⇨ [Config Backup and Restore]

2. Select the [File Encryption] tab.
3. In Password, input the password of the file that was encrypted at backup.
4. Click the [Apply] button.
5. The operating procedure for restoration varies depending on the save location of the configuration file. For the operating procedure, refer to the following.

☞ Page 77 Setting method

Precautions

- If "Configuration File Encryption" is "Disabled", "Password" cannot be set.
- If the password of the encrypted file is incorrect, the configuration file cannot be restored.
- After the restoration for settings is executed, the encryption setting will be the default (disabled).

Event log output function [Event Log Backup]

The managed switch records logs of various types of events that occur.

The recorded logs can be output as an event log file.

This event log file can be used to check events such as power-on/off and link-up/down that have occurred in the managed switch when a problem occurred.

The output destination of event log files can be selected from the following four types.

- Local drive
- SFTP server
- TFTP server
- USB flash drive

Precautions

The event log file is output for each managed switch.

Local drive

The recorded logs are output to a device such as a personal computer.

SFTP server or TFTP server

From the web interface, specify the Server IP Address and output the recorded logs to a location such as an SFTP server and TFTP server.

USB flash drive

The recorded logs are output to a USB flash drive. Event log automatic backup is available when a USB flash drive is connected.

■Event log automatic backup

This function automatically saves some of the registered event logs to a USB flash drive when the number of logs reaches the maximum number. When the number of managed switch event logs has reached the upper limit of the registration number (10000 logs), the function backs up 1000 event logs from the oldest one to the USB flash drive and deletes these logs from the managed switch event logs.

The automatically backed up event logs will be saved in \Model name\log in the USB flash drive. The file name at saving is IP address_Model name_YYYYMMDDHHmm.log. YYYYMMDDHHmm indicates the time and date of saving. When any file already present in the save destination has the same name as the generated file, the file is overwritten.

Point

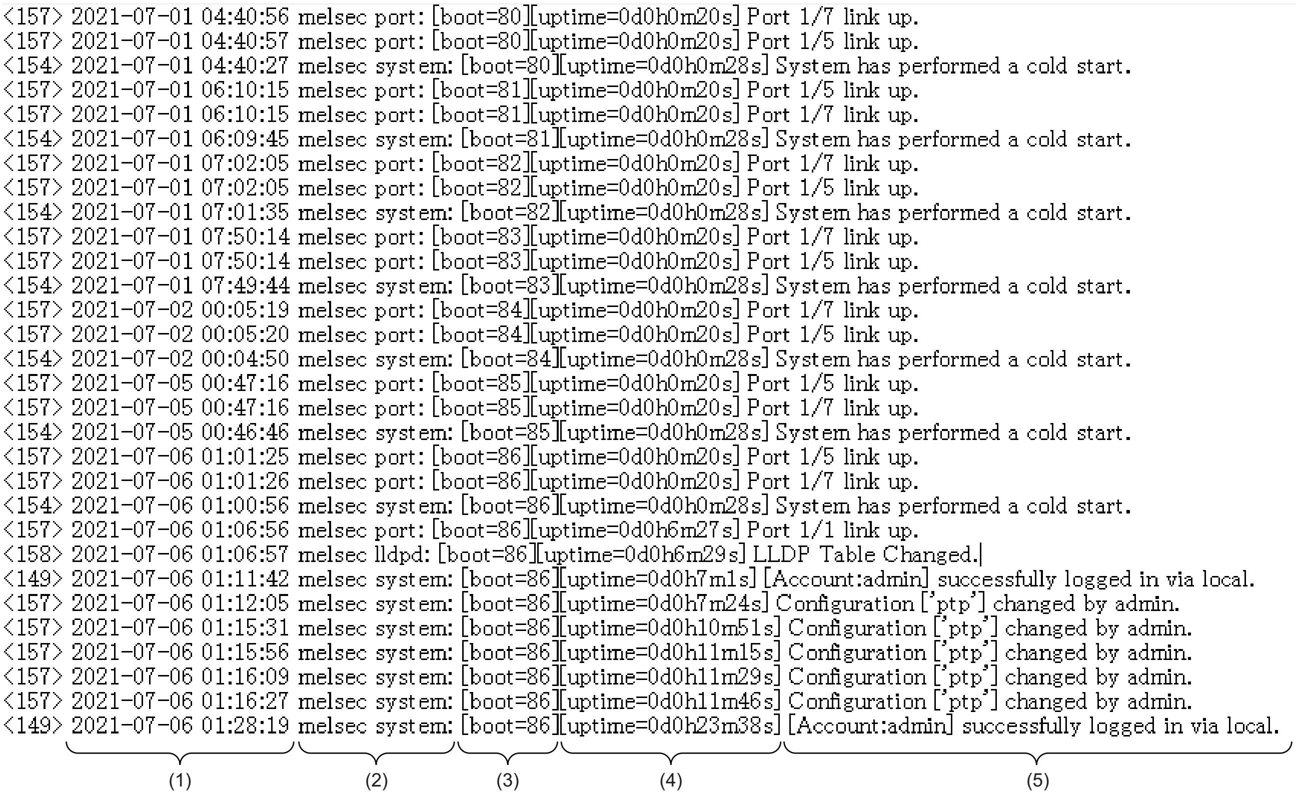
When no save folder exists in the connected USB flash drive, the folder is automatically generated.

Precautions

- Event log automatic backup is not executed if the USB flash drive does not have sufficient free space. Also, the ERR LED turns on.
- When no USB flash drive is connected, no event logs related to normal/error completion of event log automatic backup are registered. Also, the ERR LED does not turn on.
- Event log automatic backup applies also to logs to be used by the system side. For the logs to be used by the system side, <159> is added as the identifier to the beginning of the log. The logs to be used by the system side are information for investigation by the manufacturer.

Event log output file

The following is an example of an event log output file.



```
<157> 2021-07-01 04:40:56 melsec port: [boot=80][uptime=0d0h0m20s] Port 1/7 link up.
<157> 2021-07-01 04:40:57 melsec port: [boot=80][uptime=0d0h0m20s] Port 1/5 link up.
<154> 2021-07-01 04:40:27 melsec system: [boot=80][uptime=0d0h0m28s] System has performed a cold start.
<157> 2021-07-01 06:10:15 melsec port: [boot=81][uptime=0d0h0m20s] Port 1/5 link up.
<157> 2021-07-01 06:10:15 melsec port: [boot=81][uptime=0d0h0m20s] Port 1/7 link up.
<154> 2021-07-01 06:09:45 melsec system: [boot=81][uptime=0d0h0m28s] System has performed a cold start.
<157> 2021-07-01 07:02:05 melsec port: [boot=82][uptime=0d0h0m20s] Port 1/7 link up.
<157> 2021-07-01 07:02:05 melsec port: [boot=82][uptime=0d0h0m20s] Port 1/5 link up.
<154> 2021-07-01 07:01:35 melsec system: [boot=82][uptime=0d0h0m28s] System has performed a cold start.
<157> 2021-07-01 07:50:14 melsec port: [boot=83][uptime=0d0h0m20s] Port 1/7 link up.
<157> 2021-07-01 07:50:14 melsec port: [boot=83][uptime=0d0h0m20s] Port 1/5 link up.
<154> 2021-07-01 07:49:44 melsec system: [boot=83][uptime=0d0h0m28s] System has performed a cold start.
<157> 2021-07-02 00:05:19 melsec port: [boot=84][uptime=0d0h0m20s] Port 1/7 link up.
<157> 2021-07-02 00:05:20 melsec port: [boot=84][uptime=0d0h0m20s] Port 1/5 link up.
<154> 2021-07-02 00:04:50 melsec system: [boot=84][uptime=0d0h0m28s] System has performed a cold start.
<157> 2021-07-05 00:47:16 melsec port: [boot=85][uptime=0d0h0m20s] Port 1/5 link up.
<157> 2021-07-05 00:47:16 melsec port: [boot=85][uptime=0d0h0m20s] Port 1/7 link up.
<154> 2021-07-05 00:46:46 melsec system: [boot=85][uptime=0d0h0m28s] System has performed a cold start.
<157> 2021-07-06 01:01:25 melsec port: [boot=86][uptime=0d0h0m20s] Port 1/5 link up.
<157> 2021-07-06 01:01:26 melsec port: [boot=86][uptime=0d0h0m20s] Port 1/7 link up.
<154> 2021-07-06 01:00:56 melsec system: [boot=86][uptime=0d0h0m28s] System has performed a cold start.
<157> 2021-07-06 01:06:56 melsec port: [boot=86][uptime=0d0h6m27s] Port 1/1 link up.
<158> 2021-07-06 01:06:57 melsec lldpd: [boot=86][uptime=0d0h6m29s] LLDP Table Changed.
<149> 2021-07-06 01:11:42 melsec system: [boot=86][uptime=0d0h7m1s] [Account:admin] successfully logged in via local.
<157> 2021-07-06 01:12:05 melsec system: [boot=86][uptime=0d0h7m24s] Configuration ['ptp'] changed by admin.
<157> 2021-07-06 01:15:31 melsec system: [boot=86][uptime=0d0h10m51s] Configuration ['ptp'] changed by admin.
<157> 2021-07-06 01:15:56 melsec system: [boot=86][uptime=0d0h11m15s] Configuration ['ptp'] changed by admin.
<157> 2021-07-06 01:16:09 melsec system: [boot=86][uptime=0d0h11m29s] Configuration ['ptp'] changed by admin.
<157> 2021-07-06 01:16:27 melsec system: [boot=86][uptime=0d0h11m46s] Configuration ['ptp'] changed by admin.
<149> 2021-07-06 01:28:19 melsec system: [boot=86][uptime=0d0h23m38s] [Account:admin] successfully logged in via local.
```

No.	Description
1	Shows the time stamp at event registration. The system time is applied. (☞ Page 120 System time [System Time])
2	Shows Device Name and classification (system, port, lldpd).
3	Shows the number of restarts caused by operations such as power off and on and by the rebooting function. (boot=1 (1 time), boot=2 (2 times))
4	Shows the operating time from power-on to event registration.
5	Shows the event description.

Event description

The following table lists the event description to be recorded.

Event name	Event description	
Login success	[Account:{{user_name}}] successfully logged in via {{interface}}.	Login has succeeded.
Login fail	[Account:{{user_name}}] log in failed via {{interface}}.	Login has failed.
Login lockout	[Account:{{user_name}}] locked due to {{failed_times}} failed login attempts.	Lockout has occurred.
Account setting changed	• Account settings of [Account:{{user_name}}] has been updated. • Account settings of [Account:{{user_name}}] has been deleted. • Account settings of [Account:{{user_name}}] has been created.	The account settings have been changed.
SSL Certification changed	• SSL certificate has been changed. • SSL certificate has been regenerated.	The SSL certificate has been regenerated or imported.
Password changed	The password of [Account:{{user_name}}] has been changed.	The password has been changed.
Cold start	The system has performed a cold start.	The managed switch has been restarted by turning off and on the power.
Warm start	The system has performed a warm start.	• The managed switch has been restarted using the reset button. • The managed switch has been restarted using the rebooting function.
Configuration Changed	Configurations {{modules}} have been changed by[Account:{{user_name}}].	The configurations have been changed.
Configuration Imported	Configuration import {{succeeded/failed}} by {{user_name}} via {{interface}}	The configurations have been imported (restored).
Log capacity threshold	The threshold of event log entries {{numbers}} has been reached.	The event log capacity has reached the threshold value.
PWR On	Power {{index}} has turned on.	The power supply has been turned on.
PWR Off	Power {{index}} has turned off.	The power supply has been turned off.
DI On	Digital Input {{index}} has turned on.	The digital input has been turned on.
DI Off	Digital Input {{index}} has turned off.	The digital input has been turned off.
Port link up	Port {{number}} link up.	The port has linked up.
Port link down	Port {{number}} link down.	The port has linked down.
Topology Changed (RSTP)	Topology has been changed by RSTP.	The topology has been changed.
LLDP Table Changed	LLDP remote table changed.	The LLDP table has been changed.
Relay Override Message	Relay alarm is on due to {{Event Name}}.	The relay alarm notification has been issued.
SSH Key Generate	SSH key has been regenerated.	The SSH key has been generated.
Configuration Export	Configuration export {{successful /failed}} By {{user_name}} via {{interface}}.	The configurations have been exported (backed up).
FWR upgrade success	Firmware Successfully Upgraded.	The firmware has been successfully upgraded.
Relay Cut Off	{relay_name} relay alarm has been cut off.	The relay alarm has been blocked.
TACACS+ Auth. Success	[Account:{{user_name}}] successfully logged in via {{interface}}.	Login via TACACS+ has succeeded.
TACACS+ Auth. Fail	[Account:{{user_name}}] log in failed via {{interface}}.	Login via TACACS+ has failed.
RADIUS Auth. Success	[Account:{{user_name}}] successfully logged in via {{interface}}.	Login via RADIUS has succeeded.
RADIUS Auth. Fail	[Account:{{user_name}}] log in failed via {{interface}}.	Login via RADIUS has failed.
External storage	USB memory is {{inserted/unplugged}}	The USB flash drive has been connected or disconnected.
Event Log Export	Event log export {{succeeded/failed}} by{{user_name}} via {{interface}}	The event logs have been exported (backed up).

The content enclosed by {{ }} varies depending on the setting and status at event occurrence.

Content	Description
{{user_name}}	Login user name or system (system)
{{interface}}	Login authentication method (Local/TACACS+/RADIUS), or file save destination/acquisition source (local/sftp/tftp/usb)
{{failed_times}}	Number of failures (Example: Number of login attempt failures)
{{modules}}	Classification of parameters (☞ Page 92 Description of modules)
{{'successful'/'failed'}}	Success or failure
{{numbers}}	Numerical value (Example: Port numbers (Port1, Port2))
{{index}}	Index (Example: Power1, Power2)
{{Event Name}}	Event name
{{relay_name}}	Relay name (Relay)

■Description of modules

Content	Description
Info Setting	Device information setting (Example: Device name, location)
Configure File	Configuration backup/restoration (Example: Enabling/disabling encryption of the configuration file)
Account	• User account settings of the account management (Example: Adding/deleting/changing the account) • Password policy of the account management (Example: Setting the minimum number of characters for the password) • Login policy setting (Example: Enabling/disabling the lockout function) • Login authentication function (Example: Login authentication method)
Mgmt IP	IP address setting (Example: IP address)
DHCP Server	DHCP server (Example: Enabling/disabling the DHCP server function)
Time	Time setting (Example: System time, summer time)
ptp	Setting related to the time synchronization function (Example: Profile)
dot1as	Setting related to Profile: 802.1AS of the time synchronization function (Example: Timeout count of the Sync frame receptions)
1588Default	Setting related to Profile: 1588v2 Default Profile of the time synchronization function (Example: Delay mechanism)
Port Setting	Port setting (Example: Enabling/disabling the port)
VLAN	VLAN function (Example: Port mode (Access/Trunk))
QoS	Port priority setting (Example: Priority (PCP: Priority Code Point))
streamadapter	Per-stream priority setting (Example: Priority of VID to be assigned to a receive frame (PCP: Priority Code Point))
stddot1qbv	Time-sharing communication setting (Example: Time slot interval)
L2 Redundancy	Layer 2 redundancy function (Example: Enabling/disabling the spanning tree function, STP mode (STP/RSTP))
Spanning Tree	Spanning tree function (Example: Bridge priority, time setting up to topology change confirmation)
SNMP	SNMP (Example: SNMP version)
Mgmt Interface	Interface management function (Example: Enabling/disabling the Telnet connection)
Trusted Access	Access permitted function setting (Example: Enabling/disabling the access permission)
Storm Control	Traffic control function (Example: Enabling/disabling the send/receive limitation of broadcast frames)
Event Notify	• Event notification function (Example: Enabling/disabling the event notification) • Mail notification function (Example: Mail Server setting)
Syslog	Syslog function (Example: Enabling/disabling Syslog)
LLDP	LLDP (Example: Enabling/disabling LLDP)
Event Log	Event log (Example: Threshold value of event log capacity that triggers the warning)
Locator	Location check function (Example: Flashing duration)
Web	Web interface configuration (Example: Configuration mode (Standard Mode/Advanced Mode), display settings (settings for the statistical information to be displayed))

Setting method

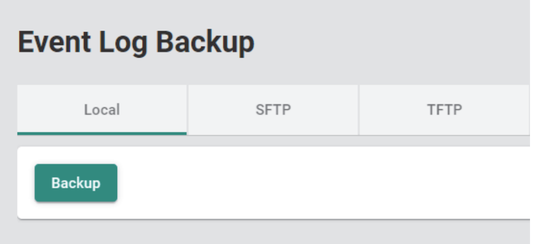
■Local drive

Operating procedure

1. Start the operation from the "Event Log Backup" window.

[System] ⇨ [System Management] ⇨ [Event Log Backup]

2. Select the [Local] tab.



3. Click the [Backup] button.

■SFTP server

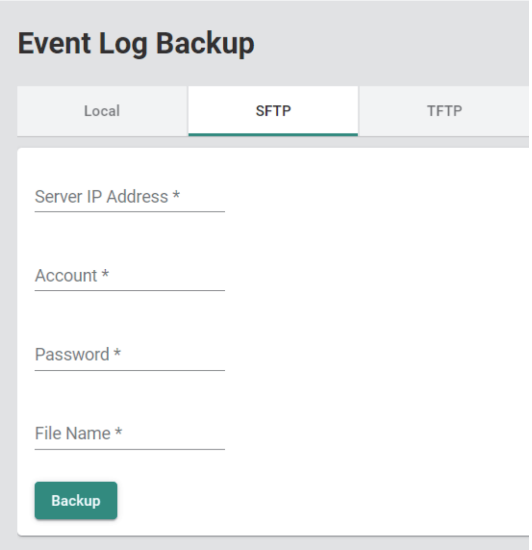
Operating procedure

1. Start the operation from the "Event Log Backup" window.

[System] ⇨ [System Management] ⇨ [Event Log Backup]

2. Select the [SFTP] tab.

3. Set the required items.



Item	Description	Setting range
Server IP Address	Input the IP address of the server.	0.0.0.1 to 255.255.255.254 (Default: empty)
Account	Input the account name for server connection.	One-byte alphanumeric characters and symbols (Default: empty)
Password	Input the password of the account for server connection.	One-byte alphanumeric characters and symbols (Default: empty)
File Name	Enter the name of the event log backup file.	One-byte alphanumeric characters and symbols (Default: empty)

4. Click the [Backup] button.

■TFTP server

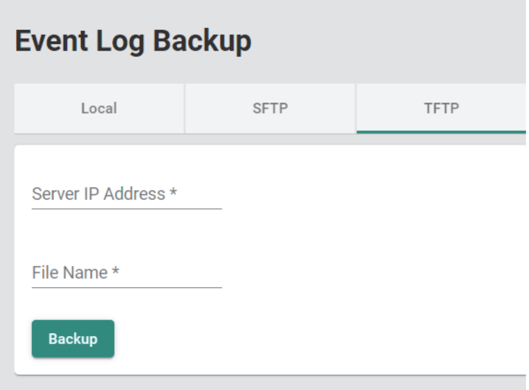
Operating procedure

1. Start the operation from the "Event Log Backup" window.

🖱 [System] ⇨ [System Management] ⇨ [Event Log Backup]

2. Select the [TFTP] tab.

3. Set the required items.



Item	Description	Setting range
Server IP Address	Input the IP address of the server.	0.0.0.1 to 255.255.255.254 (Default: empty)
File Name	Enter the name of the event log backup file.	One-byte alphanumeric characters and symbols (Default: empty)

4. Click the [Backup] button.

■USB flash drive (Event log backup)

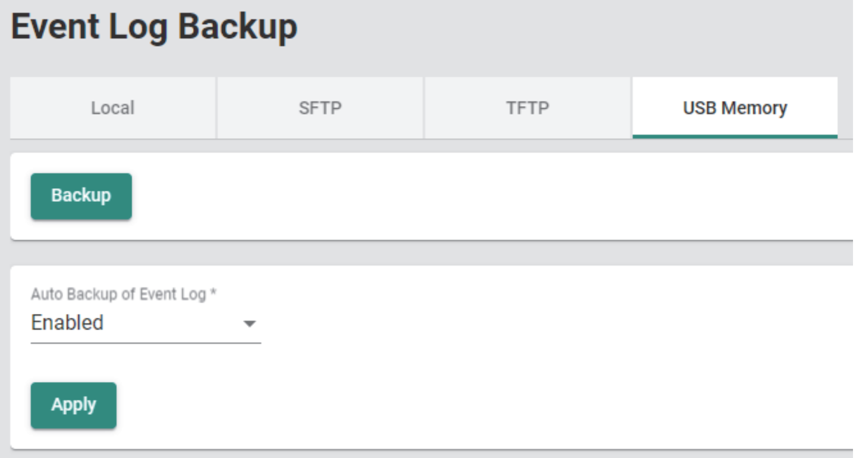
Operating procedure

1. Connect the USB flash drive to the managed switch and check that the RUN LED flashes green.

2. Start the operation from the "Event Log Backup" window.

[System] ⇨ [System Management] ⇨ [Event Log Backup]

3. Select the [USB Memory] tab.



Event Log Backup

Auto Backup of Event Log *: Enabled

4. Click the [Backup] button. The event logs are saved in the \Model name\log folder in the USB flash drive. The file name at saving is IP address_Model name_YYYYMMDDHHmm.log. YYYYMMDDHHmm indicates the time and date of saving. When any file already present in the save destination has the same name as the generated file, the file is overwritten.

Point

When no save folder exists in the connected USB flash drive, the folder is automatically generated.

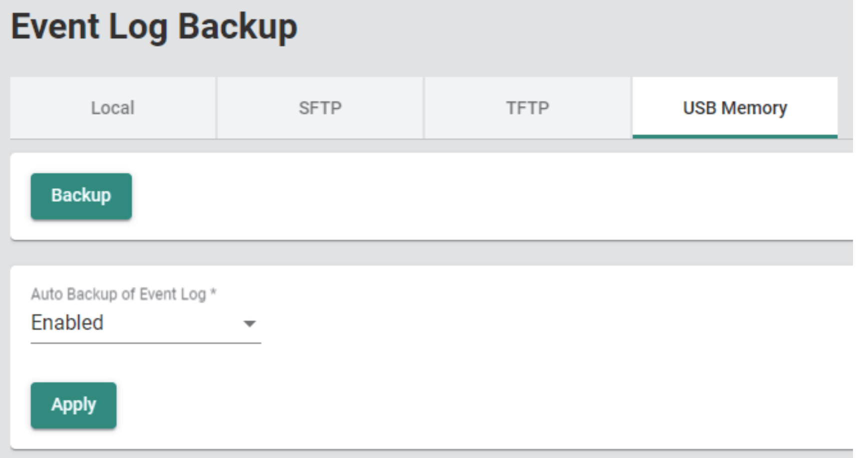
■USB flash drive (Event log automatic backup)

Operating procedure

1. Start the operation from the "Event Log Backup" window.

[System] ⇨ [System Management] ⇨ [Event Log Backup]

2. Select the [USB Memory] tab.



Event Log Backup

Auto Backup of Event Log *
Enabled

3. Set the following items.

Item	Description	Setting range
Auto Backup of Event Log	Select to enable or disable event log automatic backup using the USB flash drive. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)

4. Connect the USB flash drive to the managed switch and check that the RUN LED flashes green.

8.2 Account Management [Account Management]

The following functions can be used from the account management [Account Management] displayed on the function menu of the web interface.

- User account setting function [User Account]
- Password policy [Password Policy]

User account setting function [User Account]

The account required for login to the managed switch can be added, edited, or deleted.
Access rights can be set to limit the parameters that can be set for each account. The following three access rights are available for selection.

- Admin: All parameters can be read and written.
- Supervisor: Partial parameters can be read and written.
- User: Partial parameters can be read.

Point

The default account is as follows.

- User name: admin
- Password: admin
- Authority: Admin

Precautions

Take the following measures to prevent theft, tampering, faulty operation, unauthorized execution resulting from unauthorized access by an outsider.

- Change the password from the default. Use alphanumeric characters (a to z, A to Z, and 0 to 9), and the password must be 11 characters or longer in length. (☞ Page 280 Configure User Account Setting)
- Give administrator privileges to only the administrator account. (☞ Page 280 Configure User Account Setting)

Access right in the web interface

The following table lists access rights related to the web interface.

○: Can be executed, ×: Cannot be executed

Function item			Access right		
			Admin	Supervisor	User
System	System Management	Information Setting	Read, write	Read, write	Read
		Firmware Upgrade	○	×	×
		Config Backup and Restore	○	×	×
		Event Log Backup	○	○	○
	Account Management	User Account	Read, write	×	×
		Password Policy	Read, write	×	×
	Network	IP Configuration	Read, write	Read, write	Read
		DHCP Server	Read, write	Read, write	Read
	Time	Time Zone	Read, write	Read, write	Read
		System Time	Read, write	Read, write	Read
		Time Synchronization	Read, write	Read, write	Read
Port	Port Interface	Port Setting	Read, write	Read, write	Read
Layer 2 Switching	VLAN	IEEE 802.1Q	Read, write	Read, write	Read
	Priority Management		Read, write	Read, write	Read
	MAC	Static Unicast	Read, write	Read, write	Read
		MAC Address Table	Read, write	Read, write	Read
	Multicast	Static Multicast	Read, write	Read, write	Read
	Time-Aware-Shaper		Read, write	Read, write	Read
Network Redundancy	Layer 2 Redundancy	Spanning Tree	Read, write	Read, write	Read
Management	Network Management	SNMP	Read, write	×	×
		SNMP Trap/Inform	Read, write	×	×
Security	Device Security	Management Interface	Read, write	Read, write	Read
		Login Policy	Read, write	Read	Read
		Trusted Access	Read, write	Read	Read
		SSH&SSL	○	○	×
	Network Security	Traffic Storm Control	Read, write	Read, write	Read
	Authentication	Login Authentication	Read, write	×	×
		RADIUS	Read, write	×	×
		TACACS+	Read, write	×	×
Diagnostics	System Status	Utilization	Read	Read	Read
		Statistics	Read	Read	Read
	Event Notification	Event Notification	Read, write	Read, write	Read
		Relay Alarm Cut-off	Read, write	Read, write	Read
		Email Notification	Read, write	Read	Read
		Syslog	Read, write	Read	Read
	Diagnosis	LLDP	Read, write	Read, write	Read
		Ping	○	○	○
		ARP Table	Read	Read	Read
		Event Log	Read, write	Read, write	Read
Maintenance and Tool		Standard/Advanced Mode	○	○	○
		Disable Auto Save	Read, write	Read, write	Read
		Locator	Read, write	Read, write	○
		Reboot	○	○	×
		Reset to default	Read, write	×	×

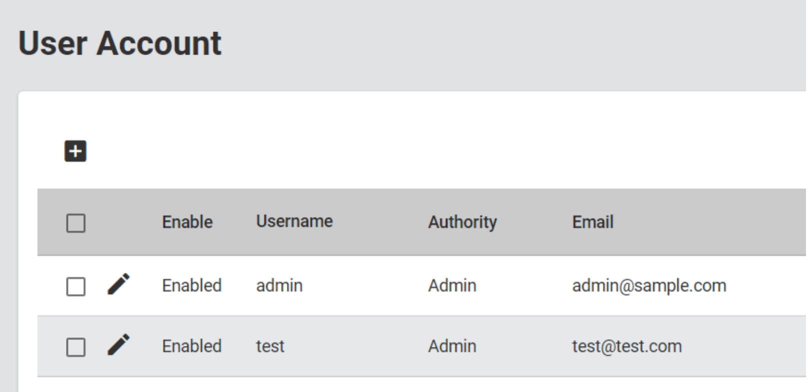
Setting method

■Editing an account

Operating procedure

1. Start the operation from the "User Account" window.

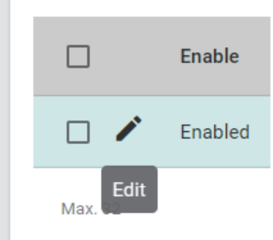
[System] ⇨ [Account Management] ⇨ [User Account]



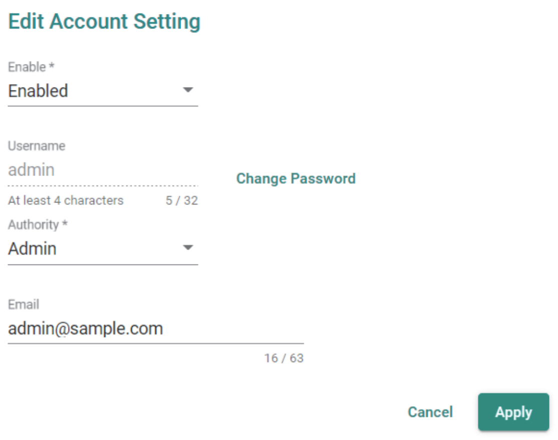
User Account

□		Enable	Username	Authority	Email
□	✎	Enabled	admin	Admin	admin@sample.com
□	✎	Enabled	test	Admin	test@test.com

2. Click the [Edit] icon of an account to be edited.



3. Set the required items.



Edit Account Setting

Enable *
Enabled

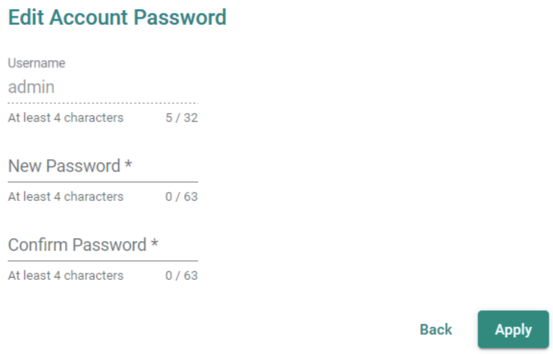
Username
admin
At least 4 characters 5 / 32

Authority *
Admin

Email
admin@sample.com
16 / 63

Item	Description	Setting range
Enable	Enable or disable the account. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Username	■For Edit Shows the user name. ■For Add Set the user name of a new account.	■For Edit — ■For Add 4 to 32 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Authority	Set the account right. • Admin: All parameters can be read and written. • Supervisor: Partial parameters can be read and written. • User: Partial parameters can be read.	■For Edit • Admin • Supervisor • User (Default: Admin) ■For Add • Admin • Supervisor • User (Default: empty)
Email	Set the email address of the account.	■For Edit 1 to 63 characters (one-byte alphanumeric characters and symbols) (Default: admin@sample.com) ■For Add 1 to 63 characters (one-byte alphanumeric characters and symbols) (Default: empty)

4. To change the password, click the [Change Password] button.



Edit Account Password

Username
admin
At least 4 characters 5 / 32

New Password *
At least 4 characters 0 / 63

Confirm Password *
At least 4 characters 0 / 63

Item	Description	Setting range
New Password	Input a new password. The necessary number of characters or available characters for the password depends on the password policy settings.	4 to 63 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Confirm Password	Input the password again for confirmation. The necessary number of characters or available characters for the password depends on the password policy settings.	4 to 63 characters (one-byte alphanumeric characters and symbols) (Default: empty)

5. Click the [Apply] button.

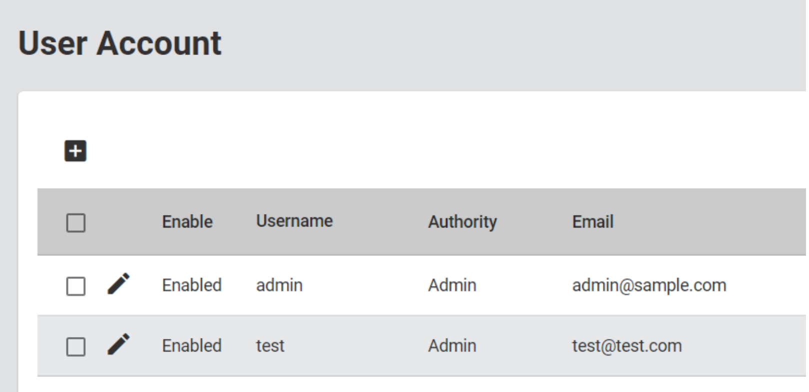
6. When the window returns to that of procedure 3, click the [Apply] button.

■Adding an account

Operating procedure

1. Start the operation from the "User Account" window.

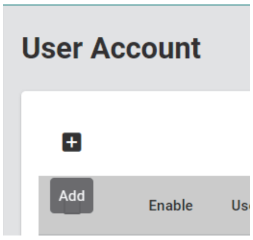
[System] ⇨ [Account Management] ⇨ [User Account]



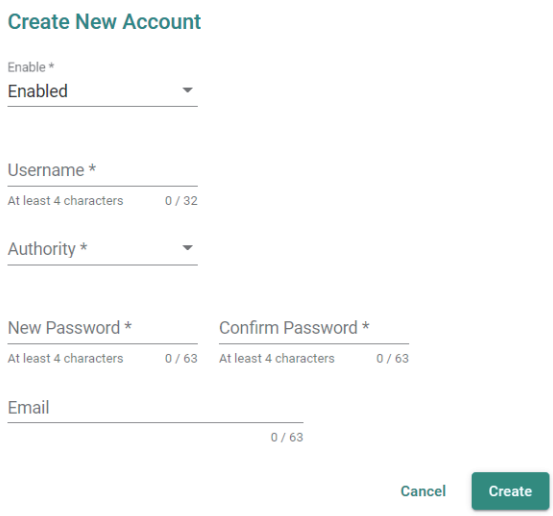
User Account

□		Enable	Username	Authority	Email
□	✎	Enabled	admin	Admin	admin@sample.com
□	✎	Enabled	test	Admin	test@test.com

2. Click the [Add] icon.



3. Set the required items.



Create New Account

Enable *: Enabled

Username * — At least 4 characters 0 / 32

Authority *

New Password * — At least 4 characters 0 / 63

Confirm Password * — At least 4 characters 0 / 63

Email — 0 / 63

Item	Description	Setting range
Enable	Enable or disable the account. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Username	Set the user name of a new account.	■For Edit — ■For Add 1 to 32 characters (one-byte alphanumeric characters and symbols) (Default: empty)

Item	Description	Setting range
Authority	Set the account right. • Admin: All parameters can be read and written. • Supervisor: Partial parameters can be read and written. • User: Partial parameters can be read.	■For Edit • Admin • Supervisor • User (Default: Admin) ■For Add • Admin • Supervisor • User (Default: empty)
New Password	Input a new password. The necessary number of characters or available characters for the password depends on the password policy settings.	4 to 63 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Confirm Password	Input the password again for confirmation. The necessary number of characters or available characters for the password depends on the password policy settings.	4 to 63 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Email	Set the email address of the account.	■For Edit 1 to 63 characters (one-byte alphanumeric characters and symbols) (Default: admin@sample.com) ■For Add 1 to 63 characters (one-byte alphanumeric characters and symbols) (Default: empty)

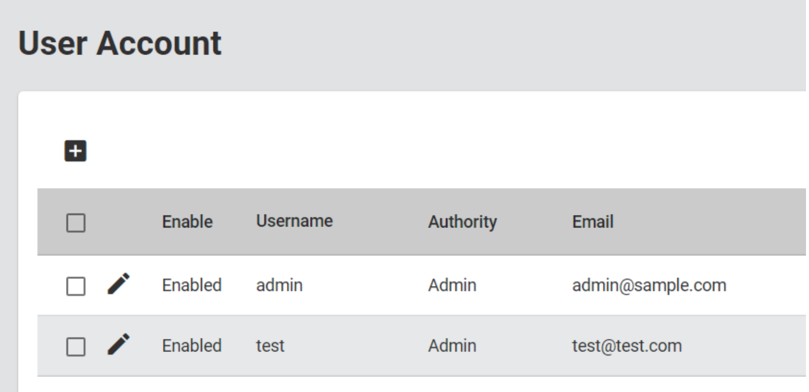
4. Click the [Create] button.

■Deleting an account

Operating procedure

1. Start the operation from the "User Account" window.

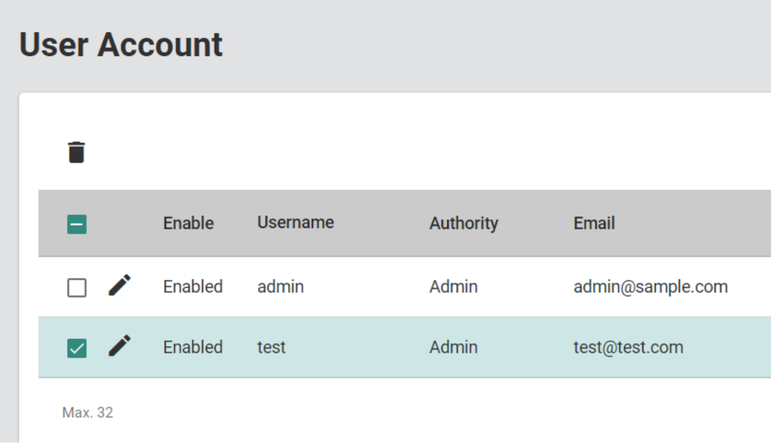
[System] ⇨ [Account Management] ⇨ [User Account]



User Account

		Enable	Username	Authority	Email
□	✎	Enabled	admin	Admin	admin@sample.com
□	✎	Enabled	test	Admin	test@test.com

2. Select the checkbox of one or more accounts to be deleted.

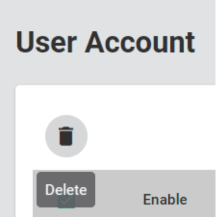


User Account

		Enable	Username	Authority	Email
□	✎	Enabled	admin	Admin	admin@sample.com
☑	✎	Enabled	test	Admin	test@test.com

Max. 32

3. Click the [Delete] icon.



User Account

4. The confirmation dialog appears. Click the [Delete] button to perform deletion.

Password policy [Password Policy]

Conditions can be set for the number of characters and character combinations to be used for the password. Also, the expiration date can be set for the password to encourage users to change their password at regular intervals.

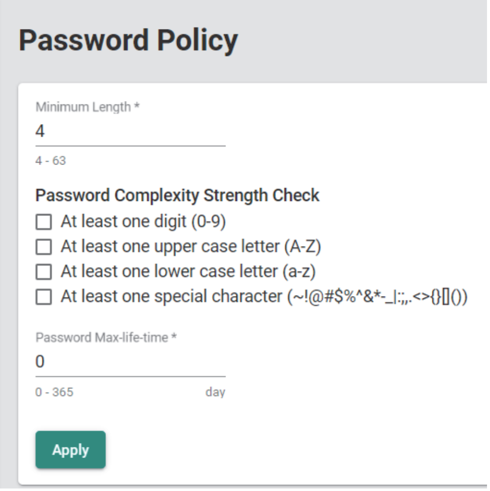
Setting method

Operating procedure

1. Start the operation from the "Password Policy" window.

[System] ⇨ [Account Management] ⇨ [Password Policy]

2. Set the required items.



Password Policy

Minimum Length *
4
4 - 63

Password Complexity Strength Check
□ At least one digit (0-9)
□ At least one upper case letter (A-Z)
□ At least one lower case letter (a-z)
□ At least one special character (~!@#$%^&*-_|:;,.<>{}[]())

Password Max-life-time *
0
0 - 365 day

Item	Description	Setting range
Minimum Length	Set the minimum number of characters for the password.	4 to 63 (Default: 4)
Password Complexity Strength Check	Set the password policy. Multiple items can be selected. • Clear • At least one digit: One or more digits of numbers (0 to 9) are to be included. • At least one upper case letter: One or more upper-case alphabetic characters (A to Z) are to be included. • At least one lower case letter: One or more lower-case alphabetic characters (a to z) are to be included. • At least one special character: One or more special characters (~!@#$%^&:-|:;,.<>{}[]()) are to be included.	• Clear • at least one digit • at least one upper case letter • at least one lower case letter • at least one special character (Default: empty)
Password Max life time	Set the expiration date for the password. If the expiration date has passed, a message will be displayed during login informing this. If this item is set to 0, the expiration date is not set.	0 to 365 days (Default: 0)

3. Click the [Apply] button.

Point

When logged in with an account whose password has exceeded the expiration date, a message will be displayed prompting that the password be changed. To prevent this message from being displayed, change the password. Login is possible even with an account whose password has expired.

8.3 Network [Network]

The following functions can be used from the network [Network] displayed on the function menu of the web interface.

- IP configuration [IP Configuration]
- DHCP server [DHCP Server]

IP configuration [IP Configuration]

The IP address of the managed switch main unit can be set by the following two methods.

- Manual (Manual): The IP address can be changed from the web interface.
- Auto (DHCP): The IP address can be assigned via the DHCP server.

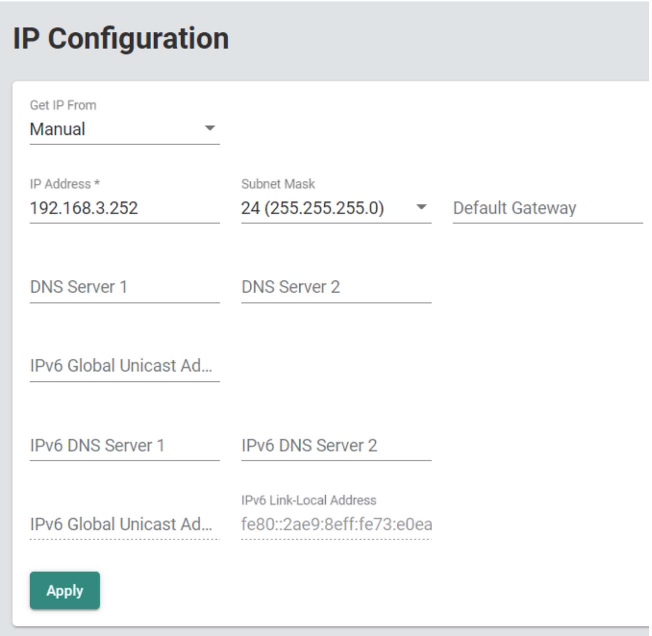
Setting method

Operating procedure

1. Start the operation from the "IP Configuration" window.

[System] ⇨ [Network] ⇨ [IP Configuration]

2. Set the required items.



IP Configuration

Get IP From: Manual

IP Address *: 192.168.3.252

Subnet Mask: 24 (255.255.255.0)

Default Gateway

DNS Server 1

DNS Server 2

IPv6 Global Unicast Ad...

IPv6 DNS Server 1

IPv6 DNS Server 2

IPv6 Global Unicast Ad...

IPv6 Link-Local Address: fe80::2ae9:8eff:fe73:e0ea

Item	Description	Setting range
Get IP From	Select an IP address setting method. • Manual: Manual setting • DHCP: Auto setting	• Manual • DHCP (Default: Manual)
IP Address	Input the IP address to be used.	0.0.0.1 to 255.255.255.254 (Default: 192.168.3.252)
Subnet Mask	Input the subnet mask to be used.	30 (255.255.255.252) to 1 (128.0.0.0) (Default: 24 (255.255.255.0))
Default Gateway	Input the default gateway to be connected to the LAN, WAN, and other networks.	• Empty • 0.0.0.0 to 255.255.255.255 (Default: empty)
DNS Server 1	Input the IPv4 address of DNS Server 1 to be used in the network. If the default gateway is not set, the setting needs to match the network part of the IPv4 address.	• Empty • 0.0.0.0 to 255.255.255.255 (Default: empty)
DNS Server 2	Input the IPv4 address of DNS Server 2 to be used in the network. If the default gateway is not set, the setting needs to match the network part of the IPv4 address. Use this server when DNS Server 1 cannot be used.	• Empty • 0.0.0.0 to 255.255.255.255 (Default: empty)

Item	Description	Setting range
IPv6 Global Unicast Address Prefix (Prefix Length: 64 bits) Default Gateway	Input a prefix value (64 bits) of the IPv6 address. Input the prefix value in the format defined by RFC2373.	Follow the format defined by RFC2373. (Default: empty)
IPv6 DNS Server 1	Specify the IPv6 address of DNS Server 1.	Follow the format defined by RFC2373. (Default: empty)
IPv6 DNS Server 2	Specify the IPv6 address of DNS Server 2. Use this server when IPv6 DNS Server 1 cannot be used.	Follow the format defined by RFC2373. (Default: empty)
IPv6 Global Unicast Address	This address is automatically set by setting the IPv6 Global Unicast Address Prefix (Prefix Length: 64 bits) Default Gateway. The IPv6 global unicast address is displayed. Use the prefix value of the IPv6 global unicast for the network part of the global unicast address, and use the EUI-64 interface ID for the host part. The EUI-64 interface ID is automatically generated from the MAC address.	—
IPv6 Link-Local Address	The IPv6 link local address is displayed.	—

3. Click the [Apply] button.

Point

For the setting method in Auto (DHCP), refer to the manual of the DHCP server to be used.

Precautions

- Items such as "IP Address" can be set only when "Get IP From" is set to "Manual".
- IPv6 can be set only in the Advanced Mode setting. (☞ Page 385 Configuration mode change)

DHCP server function [DHCP Server]

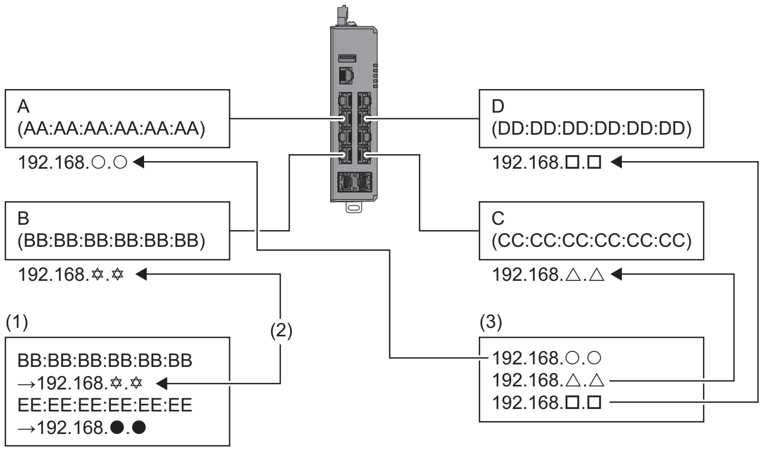
The IP address is automatically assigned to the connected devices by operating the managed switch as the DHCP server.

The following two methods can be used for assigning IP addresses to devices.

- DHCP server IP address pool: Set the IP address range to automatically assign an IP address.
- Allocation setting for each MAC address: Specify the MAC address and assign an IP address to a specific device.

In the allocation setting for each MAC address, the IP address is fixed by the MAC address so that the same IP address can be used in the device even if the device is disconnected and connected again. For other devices, the IP address is automatically reassigned from the DHCP server IP address pool.

Also, in devices for which the allocation setting for each MAC address is configured, the same IP address is assigned even if the connection location is changed.



A: Device A

B: Device B

C: Device C

(1) Allocation setting for each MAC address

(2) Specify a MAC address and assign an IP address to each device.

(3) DHCP server IP address pool

Point

- The IP address assignment using the DHCP server function is enabled only for devices that support the DHCP client function.
- When the allocation setting for MAC address is configured and the DHCP server IP address pool is set, the allocation setting for each MAC address is prioritized over the DHCP server IP address pool.

Setting method

■DHCP server IP address pool (Addition)

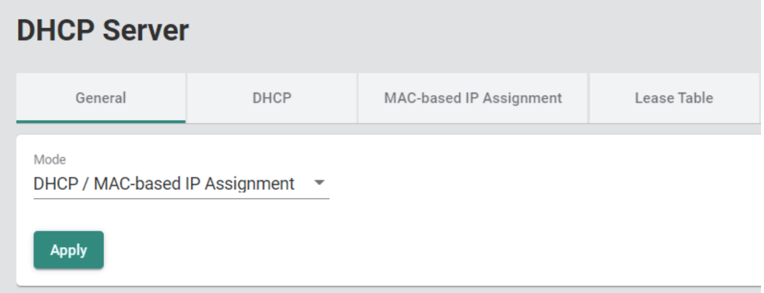
Operating procedure

1. Start the operation from the "DHCP Server" window.

[System] ⇨ [Network] ⇨ [DHCP Server]

2. Select the [General] tab.

3. Set "Mode" to "DHCP/MAC-based IP Assignment".



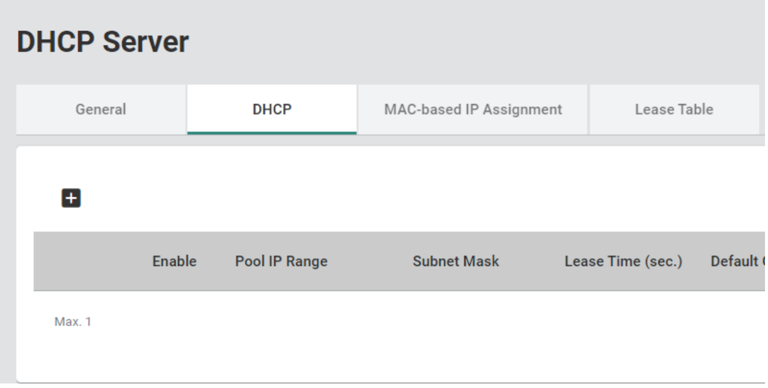
DHCP Server

General | DHCP | MAC-based IP Assignment | Lease Table

Mode: DHCP / MAC-based IP Assignment

4. Click the [Apply] button.

5. Select the [DHCP] tab.



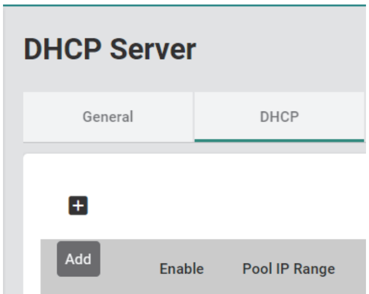
DHCP Server

General | DHCP | MAC-based IP Assignment | Lease Table

	Enable	Pool IP Range	Subnet Mask	Lease Time (sec.)	Default (

Max. 1

6. Click the [Add] icon.

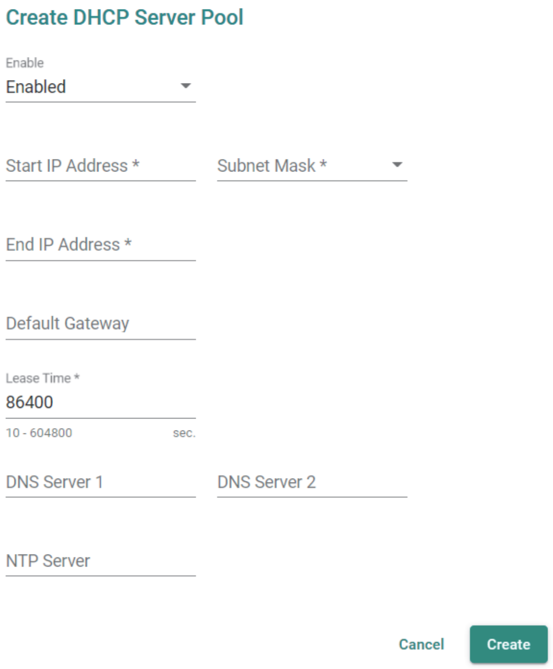


DHCP Server

General | DHCP

	Enable	Pool IP Range

7. Set the required items.



Create DHCP Server Pool

Enable: Enabled

Start IP Address *

Subnet Mask *

End IP Address *

Default Gateway

Lease Time *: 86400

10 - 604800 sec.

DNS Server 1

DNS Server 2

NTP Server

Item	Description	Setting range
Enable	Enable or disable the DHCP server IP address pool. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Start IP Address	Specify the first IP address of the DHCP server IP address pool.	0.0.0.1 to 255.255.255.254 (Default: empty)
Subnet Mask	Specify the subnet mask of the DHCP server IP address pool.	30 (255.255.255.252) to 8 (255.0.0.0) (Default: empty)
End IP Address	Specify the last IP address of the DHCP server IP address pool.	0.0.0.1 to 255.255.255.254 (Default: empty)
Default Gateway	Set the default gateway to be used by the client. The setting needs to match the network part of the IP address.	• Empty • 0.0.0.0 to 255.255.255.255 (Default: empty)
Lease Time	Input the lease time up to the IP address assignment of the DHCP server.	10 to 604800s (Default: 86400s)
DNS Server 1	Input the IP address of DNS Server 1 to be used by the client. If the default gateway is not set, the setting needs to match the network part of the IP address.	• Empty • 0.0.0.0 to 255.255.255.255 (Default: empty)
DNS Server 2	Input the IP address of DNS Server 2 to be used by the client. If the default gateway is not set, the setting needs to match the network part of the IP address.	• Empty • 0.0.0.0 to 255.255.255.255 (Default: empty)
NTP Server	Specify the NTP server to be used by the client.	• Empty • 0.0.0.1 to 255.255.255.254 (Default: empty)

8. Click the [Create] button.

Precautions

Only one IP address pool can be created.

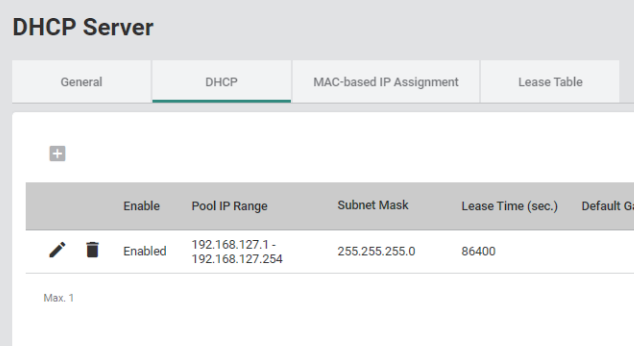
■DHCP server IP address pool (Editing)

Operating procedure

1. Start the operation from the "DHCP Server" window.

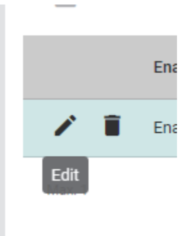
[System] ⇨ [Network] ⇨ [DHCP Server]

2. Select the [DHCP] tab.



	Enable	Pool IP Range	Subnet Mask	Lease Time (sec.)	Default G
	Enabled	192.168.127.1 - 192.168.127.254	255.255.255.0	86400	

3. Click the [Edit] icon.



4. Edit the required items.

The content of each item is the same as that for the add operation.

5. Click the [Apply] button.

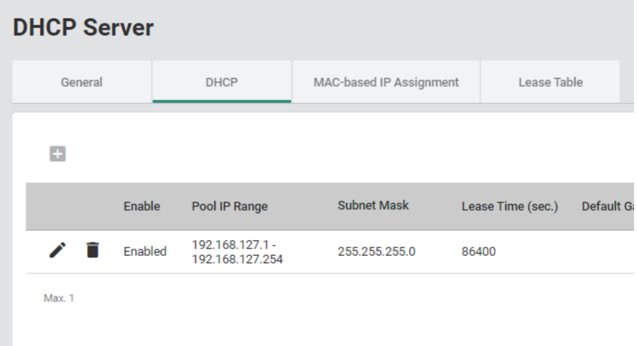
■DHCP server IP address pool (Deletion)

Operating procedure

1. Start the operation from the "DHCP Server" window.

[System] ⇨ [Network] ⇨ [DHCP Server]

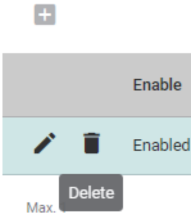
2. Select the [DHCP] tab.



	Enable	Pool IP Range	Subnet Mask	Lease Time (sec.)	Default G
	Enabled	192.168.127.1 - 192.168.127.254	255.255.255.0	86400	

Max. 1

3. Click the [Delete] icon.



4. The confirmation dialog appears. Click the [Delete] button to perform deletion.

■Allocation setting for each MAC address (Addition)

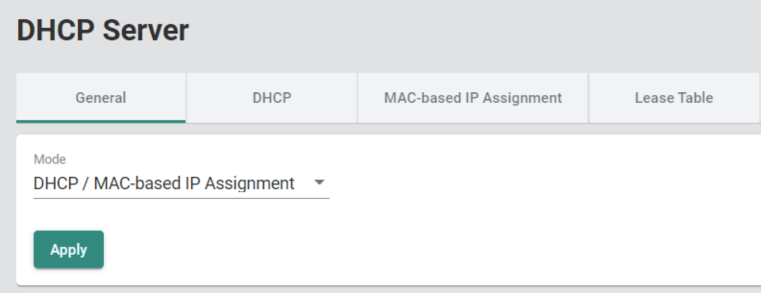
Operating procedure

1. Start the operation from the "DHCP Server" window.

[System] ⇨ [Network] ⇨ [DHCP Server]

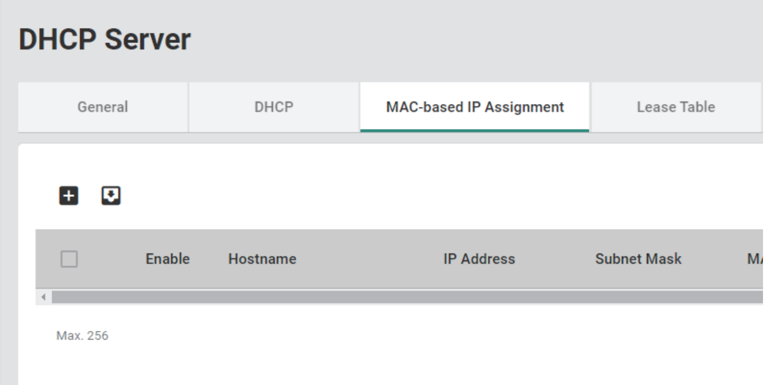
2. Select the [General] tab.

3. Set "Mode" to "DHCP/MAC-based IP Assignment".


DHCP Server

Mode: DHCP / MAC-based IP Assignment

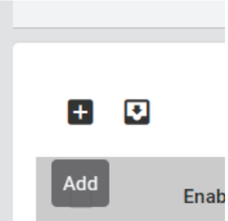
4. Select the [MAC-based IP Assignment] tab.


DHCP Server

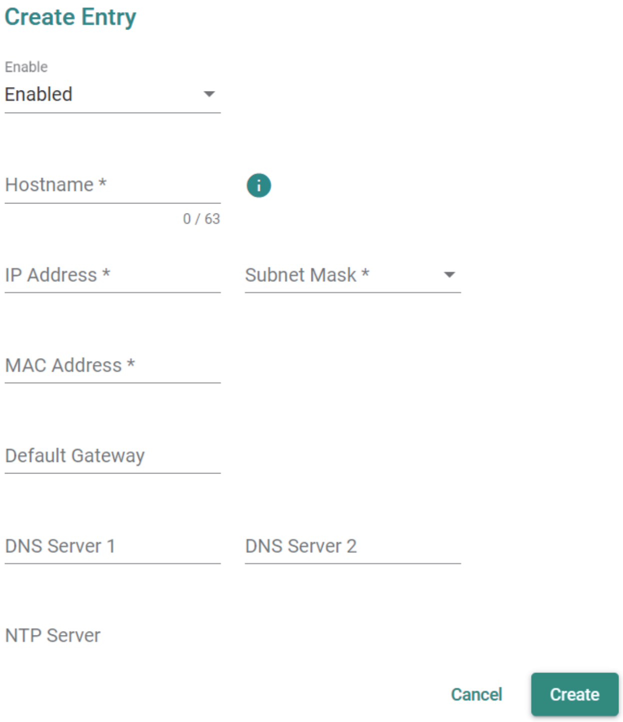
□	Enable	Hostname	IP Address	Subnet Mask	M

Max. 256

5. Click the [Add] icon.



6. Set the required items.



Create Entry

Enable: Enabled

Hostname * 0 / 63

IP Address *

Subnet Mask *

MAC Address *

Default Gateway

DNS Server 1

DNS Server 2

NTP Server

Item	Description	Setting range
Enabled	Enable or disable the IP address allocation setting for each MAC address. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Hostname	Specify the host name to be used for the DHCP client.	0 to 63 characters (one-byte alphanumeric characters and symbols) (Default: empty)
IP Address	Specify the IP address to be assigned to the client.	0.0.0.1 to 255.255.255.254 (Default: empty)
Subnet Mask	Specify the subnet mask to be used for the client.	30 (255.255.255.252) to 8 (255.0.0.0) (Default: empty)
MAC Address	Input the MAC address of the device to which the IP address is assigned.	□□:□□:□□:□□:□□:□□ (Default: empty)
Default Gateway	Input the IP address of the default gateway to be used by the client. The setting needs to match the network part of the IP address.	• Empty • 0.0.0.0 to 255.255.255.255 (Default: empty)
DNS Server 1	Input the IP address of DNS Server 1 to be used by the client. If the default gateway is not set, the setting needs to match the network part of the IP address.	• Empty • 0.0.0.0 to 255.255.255.255 (Default: empty)
DNS Server 2	Input the IP address of DNS Server 2 to be used by the client. If the default gateway is not set, the setting needs to match the network part of the IP address.	• Empty • 0.0.0.0 to 255.255.255.255 (Default: empty)
NTP Server	Specify the NTP server to be used by the client.	• Empty • 0.0.0.1 to 255.255.255.254 (Default: empty)

7. Click the [Create] button.

Point

Up to 256 MAC address-based IP assignments can be created.

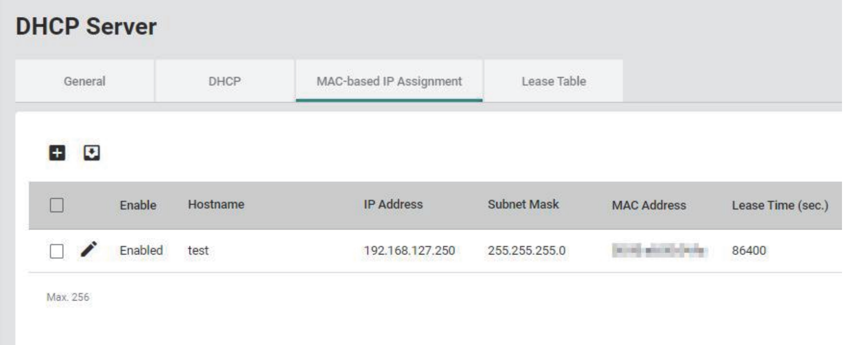
■Allocation setting for each MAC address (Editing)

Operating procedure

1. Start the operation from the "DHCP Server" window.

[System] ⇨ [Network] ⇨ [DHCP Server]

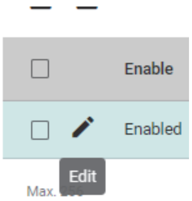
2. Select the [MAC-based IP Assignment] tab.



□		Enable	Hostname	IP Address	Subnet Mask	MAC Address	Lease Time (sec.)
□	✎	Enabled	test	192.168.127.250	255.255.255.0	[redacted]	86400

Max. 256

3. Click the [Edit] icon.



4. Edit the required items.

The content of each item is the same as that for the add operation.

5. Click the [Apply] button.

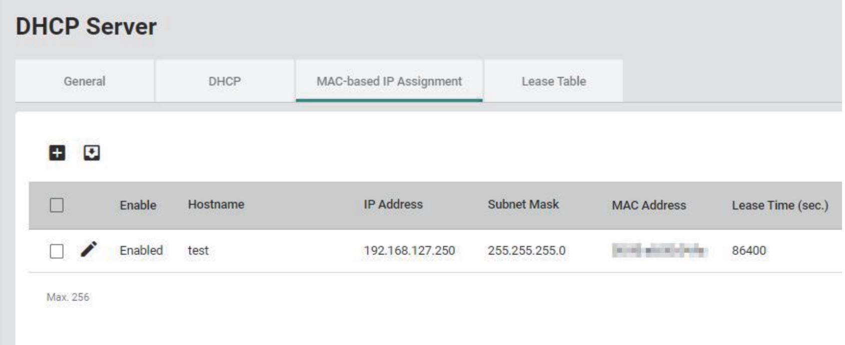
■Allocation setting for each MAC address (Deletion)

Operating procedure

1. Start the operation from the "DHCP Server" window.

[System] ⇨ [Network] ⇨ [DHCP Server]

2. Select the [MAC-based IP Assignment] tab.

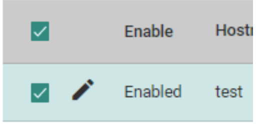


DHCP Server

□		Enable	Hostname	IP Address	Subnet Mask	MAC Address	Lease Time (sec.)
□	✎	Enabled	test	192.168.127.250	255.255.255.0	[redacted]	86400

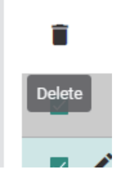
Max. 256

3. Select the checkbox of one or more items to be deleted.



☑		Enable	Host
☑	✎	Enabled	test

4. Click the [Delete] icon.



5. The confirmation dialog appears. Click the [Delete] button to perform deletion.

Lease table

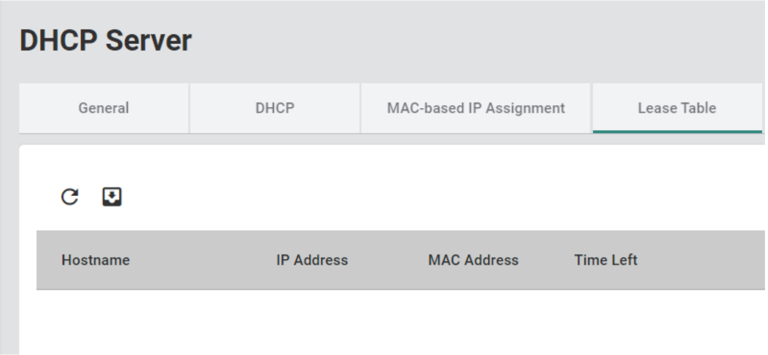
This table lists the lease time of IP addresses set to devices using the DHCP server function.

Operating procedure

1. Start the operation from the "DHCP Server" window.

[System] ⇨ [Network] ⇨ [DHCP Server]

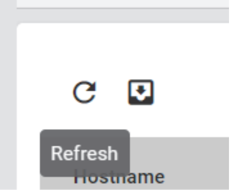
2. Select the [Lease Table] tab.



Item	Description
Hostname	Shows the host name on the client side.
IP Address	Shows the IP address on the client side.
MAC Address	Shows the MAC address on the client side.
Time Left	Shows the remaining lease time until the IP address assignment for the DHCP server. Shows (static) for MAC-based IP Assignment.

Point

Click the [Refresh] icon to update the display to the latest information.



8.4 Time [Time]

The following functions can be used from the time [Time] displayed on the function menu of the web interface.

- Time zone [Time Zone]
- System time [System Time]
- Time synchronization function [Time Synchronization]

Precautions

The managed switch can synchronize its time with the connected devices. However, the time lag may occur immediately after the managed switch is powered-on.

Time zone [Time Zone]

The clock of the managed switch can be adjusted to synchronize with the time zone of the region where the switch is used.

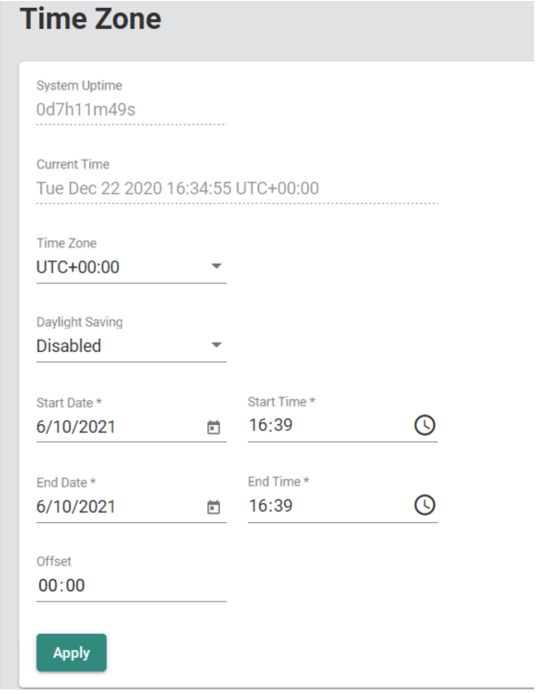
Setting method

Operating procedure

1. Start the operation from the "Time Zone" window.

[System] ⇨ [Time] ⇨ [Time Zone]

2. Set the required items.



Time Zone

System Uptime
0d7h11m49s

Current Time
Tue Dec 22 2020 16:34:55 UTC+00:00

Time Zone
UTC+00:00

Daylight Saving
Disabled

Start Date *
6/10/2021

Start Time *
16:39

End Date *
6/10/2021

End Time *
16:39

Offset
00:00

Item	Description	Setting range
Time Zone	Specify the time zone.	• UTC-12:00 to UTC+14:00 (Default: UTC+00:00)
Daylight Saving	Enable or disable the summer time. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)
Start Date	Specify the start date of the summer time.	2000/1/1 to 2037/12/31 (Default: Time acquired from the web browser)
Start time	Specify the start time of the summer time.	00:00 to 23:59 (Default: Time acquired from the web browser)
End Date	Specify the end date of the summer time.	2000/1/1 to 2037/12/31 (Default: Time acquired from the web browser)

Item	Description	Setting range
End Time	Specify the end time of the summer time.	00:00 to 23:59 (Default: Time acquired from the web browser)
Offset	Specify the offset to be applied during the summer time. Example: 02:00 for two hours, 24:00 for one day	00:00 to 24:00 (Default: 00:00)

3. Click the [Apply] button.

Precautions

- Incorrect dates cannot be set to the calendar. (Example: 2021/2/29, 2020/11/31)
- The summer time ends when the time zone is set close to the end time of the summer time.

Point

The calendar automatically makes the leap year adjustment.

System time [System Time]

The system time of the managed switch can be selected from the following four types.

- Local time: Manually set the system time.
- PTP (Precision Time Protocol): The time synchronizes with the grandmaster time in the network.
- SNTP (Simple Network Time Protocol): The time synchronizes by connecting to the time server.
- NTP (Network Time Protocol): The time synchronizes by connecting to the time server. (NTP authentication will be performed.)

This function can also operate as the time server (NTP server).

Setting method

■Local time

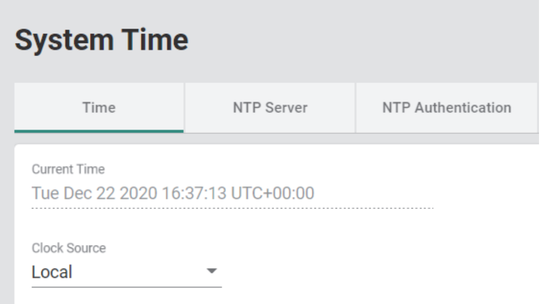
Operating procedure

1. Start the operation from the "System Time" window.

[System] ⇨ [Time] ⇨ [System Time]

2. Select the [Time] tab.

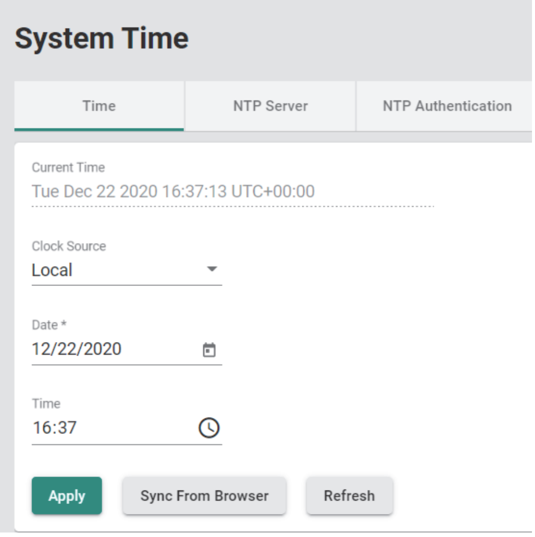
3. Set "Clock Source" to "Local".



Current Time
Tue Dec 22 2020 16:37:13 UTC+00:00

Clock Source
Local

4. Set the required items.



Current Time
Tue Dec 22 2020 16:37:13 UTC+00:00

Clock Source
Local

Date *
12/22/2020

Time
16:37

Item	Description	Setting range
Date	Set the date of the managed switch.	2000/1/1 to 2037/12/31 (Default: Date and time of the managed switch)
Time	Set the time of the managed switch.	00:00 to 23:59 (Default: Date and time of the managed switch)

5. Click the [Apply] button.

Precautions

Incorrect dates cannot be set to the calendar. (Example: 2021/2/29, 2020/11/31)

Point

- The calendar automatically makes the leap year adjustment.
- Click the [Sync From Browser] button to acquire Date and Time from the time used by the web browser.

■PTP

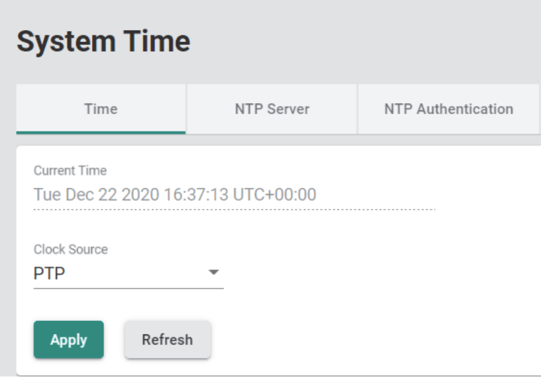
Operating procedure

1. Start the operation from the "System Time" window.

[System] ⇨ [Time] ⇨ [System Time]

2. Select the [Time] tab.

3. Set "Clock Source" to "PTP".



Current Time
Tue Dec 22 2020 16:37:13 UTC+00:00

Clock Source
PTP

4. Click the [Apply] button.

■SNTP

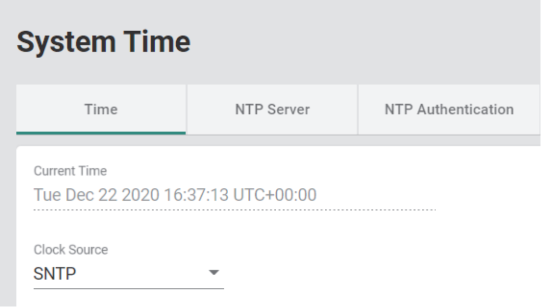
Operating procedure

1. Start the operation from the "System Time" window.

[System] ⇨ [Time] ⇨ [System Time]

2. Select the [Time] tab.

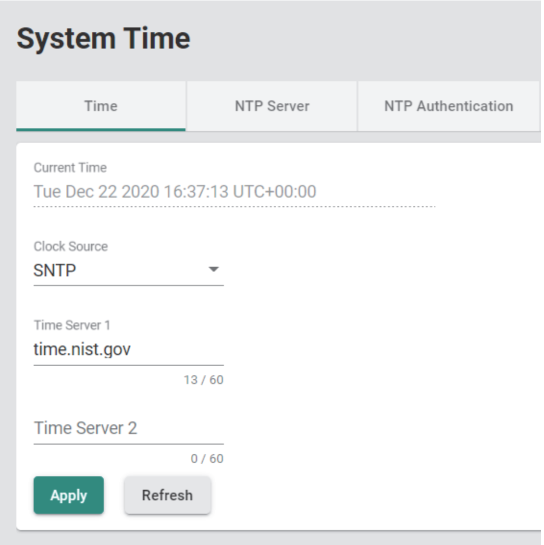
3. Set "Clock Source" to "SNTP".



Current Time
Tue Dec 22 2020 16:37:13 UTC+00:00

Clock Source
SNTP

4. Set the required items.



Current Time
Tue Dec 22 2020 16:37:13 UTC+00:00

Clock Source
SNTP

Time Server 1
time.nist.gov
13 / 60

Time Server 2
0 / 60

Item	Description	Setting range
Time Server 1	Specify the IP address or domain address of Server 1. Example: 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov	• Empty • 1 to 60 characters (one-byte alphanumeric characters and symbols) (Default: time.nist.gov)
Time Server 2	Specify the IP address or domain address of Server 2. Use this server when Server 1 cannot be connected.	• Empty • 1 to 60 characters (one-byte alphanumeric characters and symbols) (Default: empty)

5. Click the [Apply] button.

■Operating the system time as the NTP client

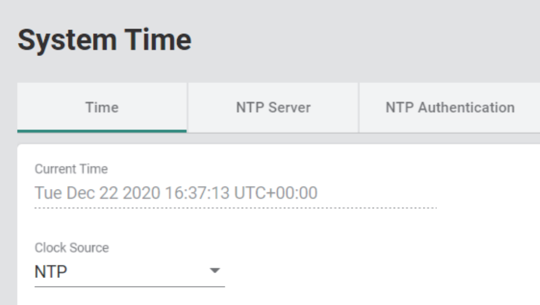
Operating procedure

1. Start the operation from the "System Time" window.

[System] ⇨ [Time] ⇨ [System Time]

2. Select the [Time] tab.

3. Set "Clock Source" to "NTP".

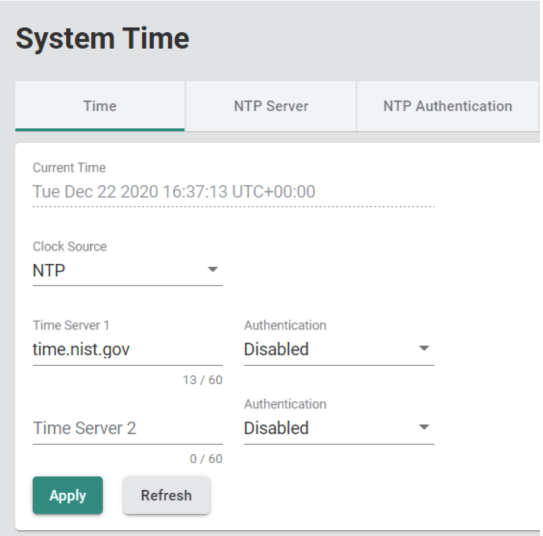


System Time

Current Time
Tue Dec 22 2020 16:37:13 UTC+00:00

Clock Source
NTP

4. Set the required items.



System Time

Current Time
Tue Dec 22 2020 16:37:13 UTC+00:00

Clock Source
NTP

Time Server 1
time.nist.gov
13 / 60

Authentication
Disabled

Time Server 2
0 / 60

Authentication
Disabled

Item	Description	Setting range
Time Server 1	Specify the IP address or domain address of Server 1. Example: 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov	• Empty • 1 to 60 characters (one-byte alphanumeric characters and symbols) (Default: time.nist.gov)
Authentication	Enable or disable NTP authentication. NTP authentication is enabled by specifying Key ID of the authentication information set in the [NTP Authentication] tab. (☞ Page 125 Adding NTP authentication information)	• Disabled • 1 to 65535 (Default: Disabled)
Time Server 2	Specify the IP address or domain address of Server 2. Use this server when Server 1 cannot be connected.	• Empty • 1 to 60 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Authentication	Enable or disable NTP authentication. NTP authentication is enabled by specifying Key ID of the authentication information set in the [NTP Authentication] tab. (☞ Page 125 Adding NTP authentication information)	• Disabled • 1 to 65535 (Default: Disabled)

5. Click the [Apply] button.

■Operating the system time as the NTP server

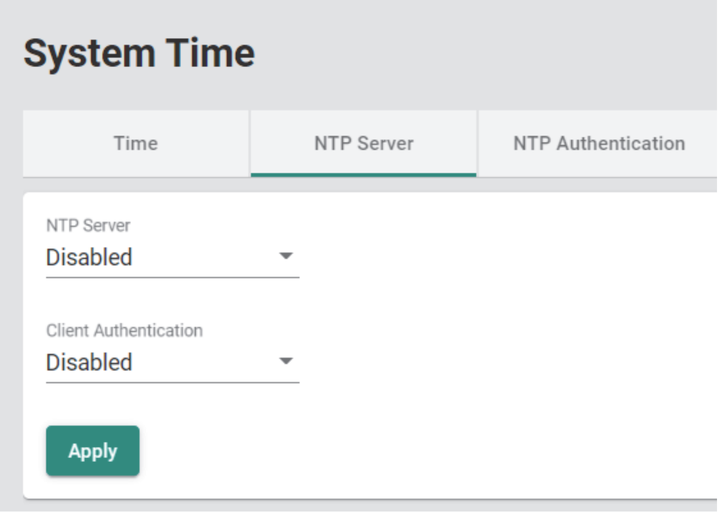
Operating procedure

1. Start the operation from the "System Time" window.

[System] ⇨ [Time] ⇨ [System Time]

2. Select the [NTP Server] tab.

3. Set the required items.



System Time

NTP Server: Disabled

Client Authentication: Disabled

Item	Description	Setting range
NTP Server	Enable or disable the NTP server. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)
Client Authentication	Enable or disable NTP authentication. Use the authentication information set in the [NTP Authentication] tab. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)

4. Click the [Apply] button.

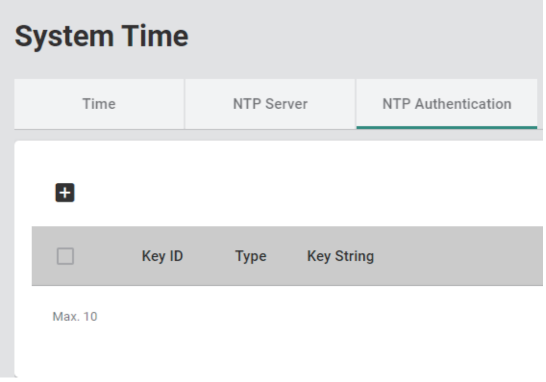
■Adding NTP authentication information

When NTP authentication is required to check that the time server is reliable, set the NTP key.

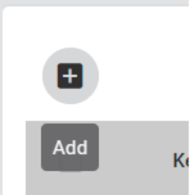
1. Start the operation from the "System Time" window.

[System] ⇨ [Time] ⇨ [System Time]

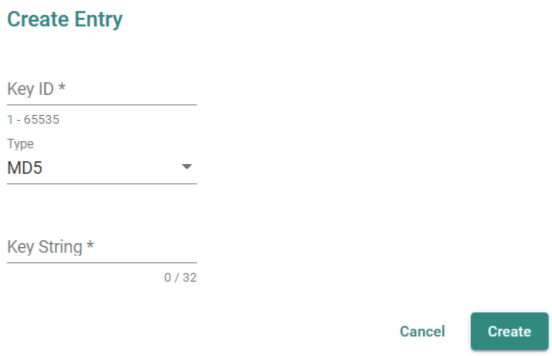
2. Select the [NTP Authentication] tab.



3. Click the [Add] icon.



4. Set the required items.



Item	Description	Setting range
Key ID	Input the ID key to be used for NTP authentication.	1 to 65535 one-byte alphanumeric characters (Default: empty)
Type	Input the authentication method.	MD5 (Fixed)
Key String	Input the password to be used for authentication.	1 to 32 characters (one-byte alphanumeric characters and symbols) (Default: empty)

5. Click the [Create] button.

Point

Up to 10 pieces of NTP authentication information can be created.

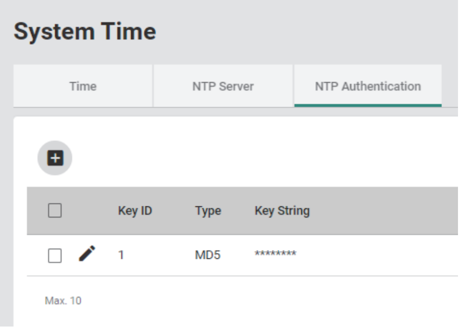
■Editing NTP authentication information

Operating procedure

1. Start the operation from the "System Time" window.

[System] ⇨ [Time] ⇨ [System Time]

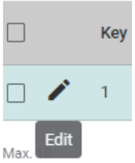
2. Select the [NTP Authentication] tab.



□		Key ID	Type	Key String
□	✎	1	MD5	********

Max. 10

3. Click the [Edit] icon.



4. Edit the required items.

The content of each item is the same as that for the add operation.

5. Click the [Apply] button.

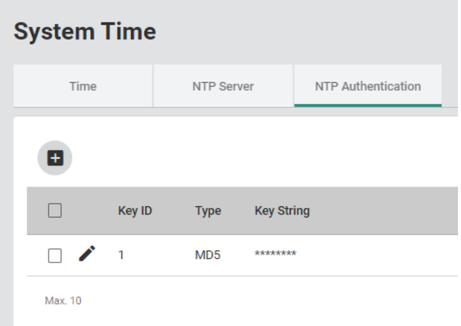
■Deleting NTP authentication information

Operating procedure

1. Start the operation from the "System Time" window.

[System] ⇨ [Time] ⇨ [System Time]

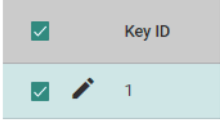
2. Select the [NTP Authentication] tab.



□		Key ID	Type	Key String
□	✎	1	MD5	********

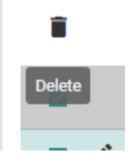
Max. 10

3. Select the checkbox of one or more pieces of NTP authentication information to be deleted.



☑		Key ID
☑	✎	1

4. Click the [Delete] icon.



5. The confirmation dialog appears. Click the [Delete] button to perform deletion.

Displaying of the system time

The current system time can be checked.

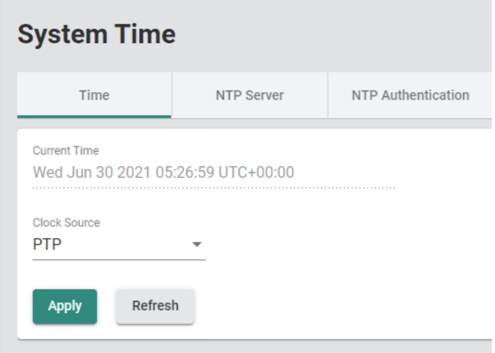
Operating procedure

1. Start the operation from the "System Time" window.

[System] ⇨ [Time] ⇨ [System Time]

2. Click the [Time] tab.

The current system time is displayed on "Current Time".



System Time

Current Time: Wed Jun 30 2021 05:26:59 UTC+00:00

Clock Source: PTP

Point

To display the latest current time, click the [Refresh] button.

Time synchronization function [Time Synchronization]

This function is used to synchronize the time with the time of the grandmaster in the network. Also, the managed switch can operate as the grandmaster.

Moreover, the current time synchronization mode and port status can be checked.

For the time synchronization mode, the following two types are available.

- IEEE 802.1AS
- IEEE 1588v2

Setting method

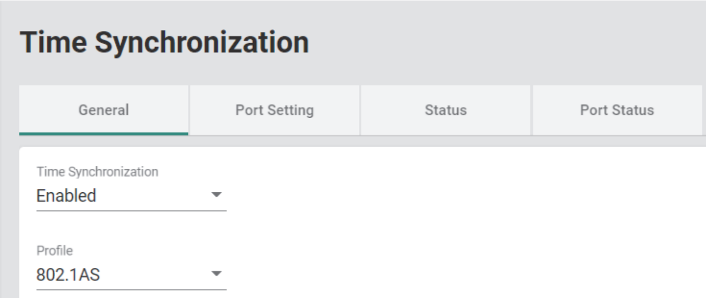
■IEEE 802.1AS

Operating procedure

1. Start the operation from the "Time Synchronization" window.

[System] ⇨ [Time] ⇨ [Time Synchronization]

2. Select the [General] tab.
3. Set "Time Synchronization" to "Enabled".
4. Set "Profile" to "802.1AS".

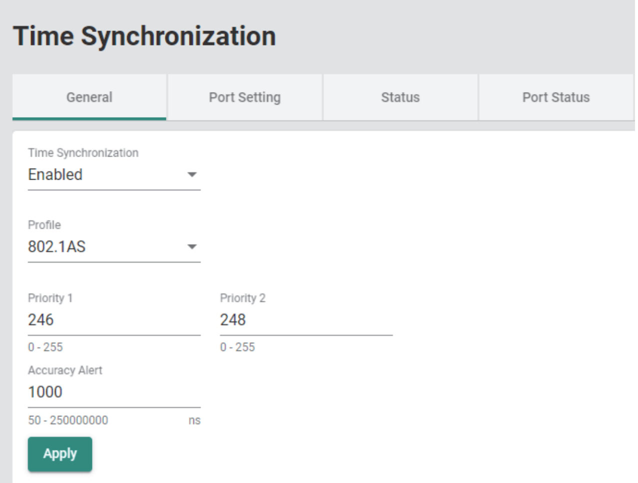


Time Synchronization

Time Synchronization: Enabled

Profile: 802.1AS

5. Set the required items.



Time Synchronization

Time Synchronization: Enabled

Profile: 802.1AS

Priority 1: 246 (0 - 255)

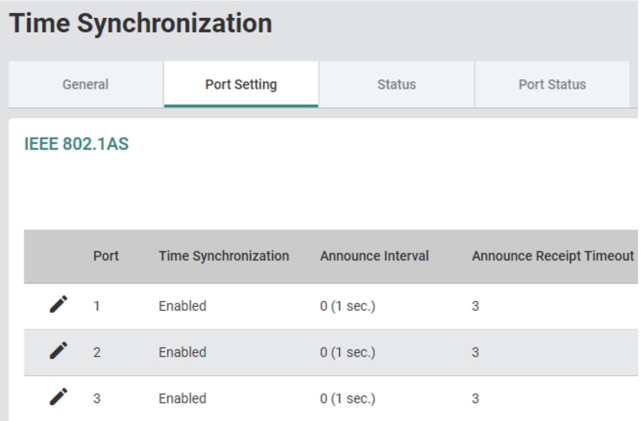
Priority 2: 248 (0 - 255)

Accuracy Alert: 1000 (50 - 250000000 ns)

Item	Description	Setting range
Priority 1	Specify the value of Priority 1.	0 to 255 (Default: 246)
Priority 2	Specify the value of Priority 2.	0 to 255 (Default: 248)
Accuracy Alert	Set the threshold value for the amount of time correction from the grandmaster, which issues a warning.	50 to 250000000ns (Default: 1000)

6. Click the [Apply] button.

7. Select the [Port Setting] tab.



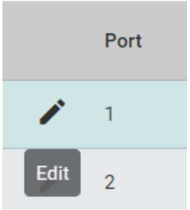
Time Synchronization

General | Port Setting | Status | Port Status

IEEE 802.1AS

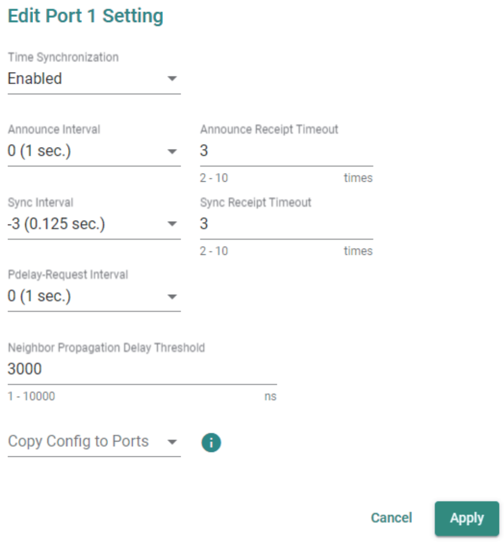
	Port	Time Synchronization	Announce Interval	Announce Receipt Timeout
✎	1	Enabled	0 (1 sec.)	3
✎	2	Enabled	0 (1 sec.)	3
✎	3	Enabled	0 (1 sec.)	3

8. Click the [Edit] icon of the port to be set.



	Port
✎	1
Edit	2

9. Set the required items.



Edit Port 1 Setting

Time Synchronization: Enabled

Announce Interval: 0 (1 sec.)

Announce Receipt Timeout: 3 (2 - 10 times)

Sync Interval: -3 (0.125 sec.)

Sync Receipt Timeout: 3 (2 - 10 times)

Pdelay-Request Interval: 0 (1 sec.)

Neighbor Propagation Delay Threshold: 3000 (1 - 10000 ns)

Copy Config to Ports

Cancel | Apply

Item	Description	Setting range
Time Synchronization	Enable or disable the time synchronization function. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Announce Interval	Set the transmission interval of the Announce frames.	0 (1 sec.) to 4 (16 sec.) (Default: 0 (1 sec.))
Announce Receipt Timeout	Set the timeout count of the Announce frame receptions.	2 to 10 (Default: 3)
Sync Interval	Set the transmission interval of the Sync frames.	-3 (0.125 sec.) to 5 (32 sec.) (Default: -3 (0.125 sec.))
Sync Receipt Timeout	Set the timeout count of the Sync frame receptions.	2 to 10 (Default: 3)
Pdelay-Request Interval	Set the transmission interval of the Pdelay_Req frames.	-3 (0.125 sec.) to 5 (32 sec.) (Default: 0 (1 sec.))
Neighbor Propagation Delay Threshold	Set the threshold value of the transmission delay time with the adjacent station. [ns]	1 to 10000 (Default: 3000)

Item	Description	Setting range
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Ports • 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: empty)

[*1] This item is not displayed for the NZ2MHG-TSNT4.

10. Click the [Apply] button.

■IEEE 1588

Operating procedure

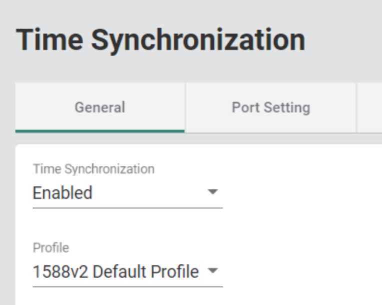
1. Start the operation from the "Time Synchronization" window.

[System] ⇨ [Time] ⇨ [Time Synchronization]

2. Select the [General] tab.

3. Set "Time Synchronization" to "Enabled".

4. Set "Profile" to "1588v2 Default Profile".

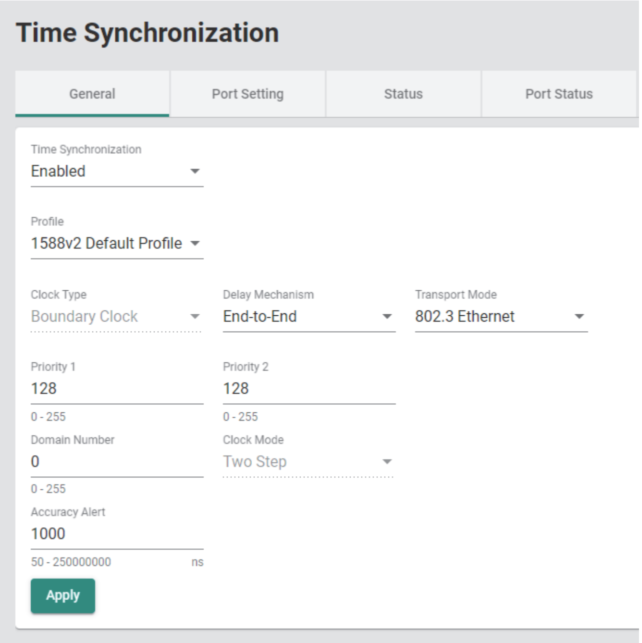


Time Synchronization

Time Synchronization: Enabled

Profile: 1588v2 Default Profile

5. Set the required items.



Time Synchronization

Time Synchronization: Enabled

Profile: 1588v2 Default Profile

Clock Type: Boundary Clock

Delay Mechanism: End-to-End

Transport Mode: 802.3 Ethernet

Priority 1: 128 (0 - 255)

Priority 2: 128 (0 - 255)

Domain Number: 0 (0 - 255)

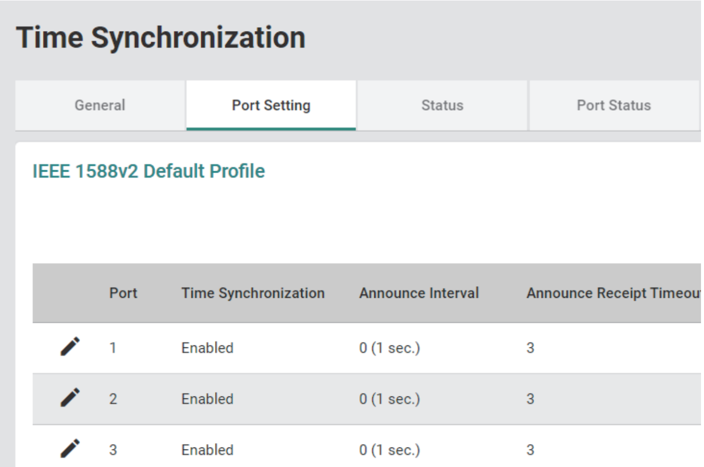
Clock Mode: Two Step

Accuracy Alert: 1000 (50 - 250000000 ns)

Item	Description	Setting range
Clock Type	Set the clock type.	Boundary Clock (Fixed)
Delay Mechanism	Set the delay mechanism.	• End-to-End • Peer-to-Peer (Default: End-to-End)
Transport Mode	Set the communication mode.	• 802.3 Ethernet • UDP IPv4 (Default: 802.3 Ethernet)
Priority 1	Specify the value of Priority 1.	0 to 255 (Default: 128)
Priority 2	Specify the value of Priority 2.	0 to 255 (Default: 128)
Domain Number	Specify the domain number.	0 to 255 (Default: 0)
Clock Mode	Set the clock mode.	Two Step (Fixed)
Accuracy Alert	Set the threshold value for the amount of time correction from the grandmaster, which issues a warning.	50 to 250000000ns (Default: 1000)

6. Click the [Apply] button.

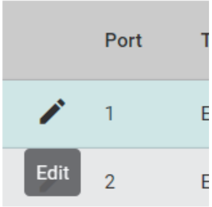
7. Click the [Port Setting] tab.



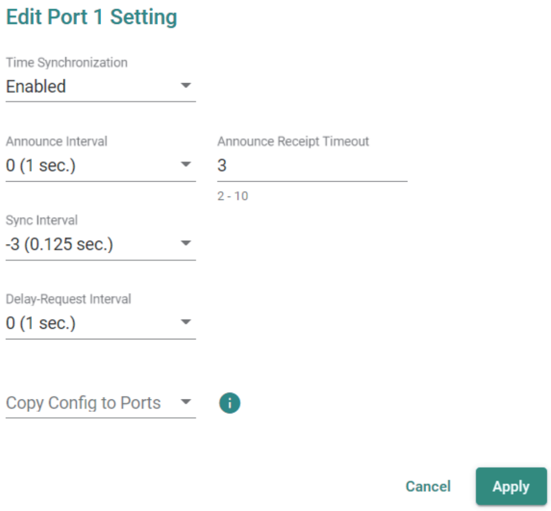
IEEE 1588v2 Default Profile

	Port	Time Synchronization	Announce Interval	Announce Receipt Timeou
✎	1	Enabled	0 (1 sec.)	3
✎	2	Enabled	0 (1 sec.)	3
✎	3	Enabled	0 (1 sec.)	3

8. Click the [Edit] icon of the port to be set.



9. Set the required items.



Edit Port 1 Setting

Time Synchronization: Enabled

Announce Interval: 0 (1 sec.)

Announce Receipt Timeout: 3

2 - 10

Sync Interval: -3 (0.125 sec.)

Delay-Request Interval: 0 (1 sec.)

Item	Description	Setting range
Time Synchronization	Enable or disable the time synchronization function. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Announce Interval	Set the transmission interval of the Announce frames.	0 (1 sec.) to 4 (16 sec.) (Default: 0 (1 sec.))
Announce Receipt Timeout	Set the timeout count of the Announce frame receptions.	2 to 10 (Default: 3)
Sync Interval	Set the transmission interval of the Sync frames.	-3 (0.125 sec.) to 5 (32 sec.) (Default: -3 (0.125 sec.))
Delay-Request Interval	Set the transmission interval of the Delay_Req frames.	-3 (0.125 sec.) to 5 (32 sec.) (Default: 0 (1 sec.))

Item	Description	Setting range
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Ports • 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: empty)

[*1] This item is not displayed for the NZ2MHG-TSNT4.

10. Click the [Apply] button.

Time synchronization status

The synchronization status of current time is indicated.

The amount of time correction with the grandmaster is indicated in a time series graph (PTP clock time).

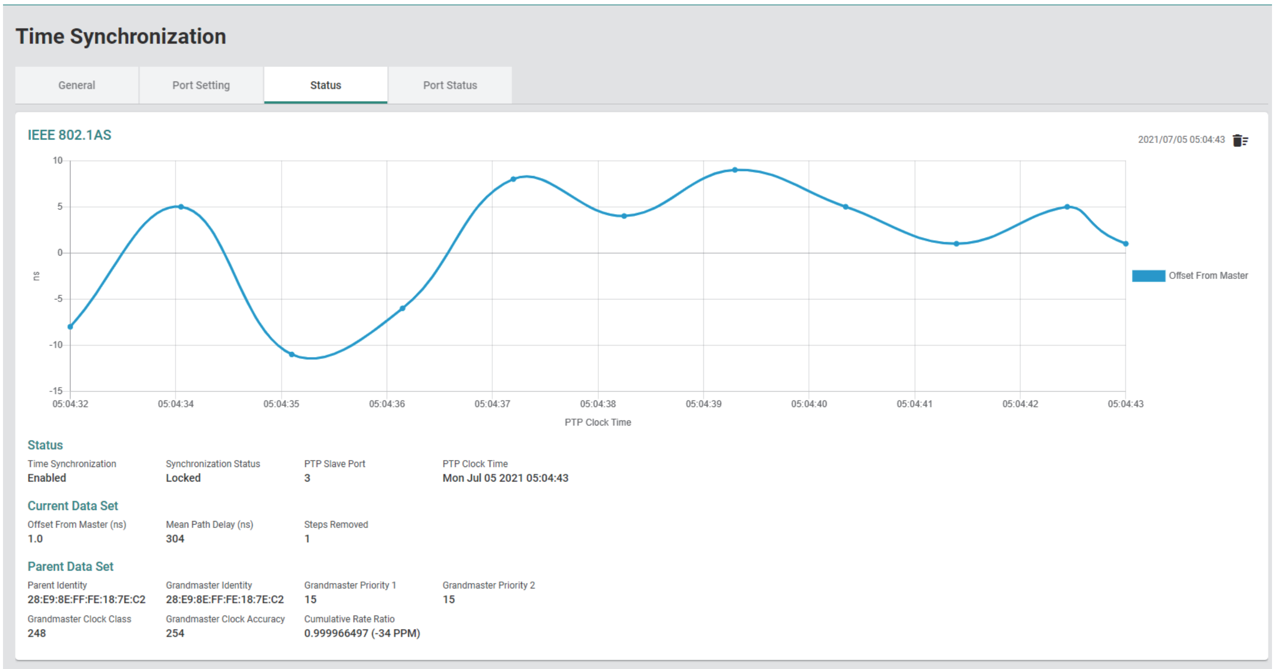
■IEEE 802.1AS

Operating procedure

1. Start the operation from the "Time Synchronization" window.

[System] ⇨ [Time] ⇨ [Time Synchronization]

2. Select the [Status] tab.



Status

Time Synchronization: Enabled

Synchronization Status: Locked

PTP Slave Port: 3

PTP Clock Time: Mon Jul 05 2021 05:04:43

Current Data Set

Offset From Master (ns): 1.0

Mean Path Delay (ns): 304

Steps Removed: 1

Parent Data Set

Parent Identity: 28:E9:8E:FF:FE:18:7E:C2

Grandmaster Identity: 28:E9:8E:FF:FE:18:7E:C2

Grandmaster Priority 1: 15

Grandmaster Priority 2: 15

Grandmaster Clock Class: 248

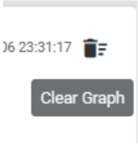
Grandmaster Clock Accuracy: 254

Cumulative Rate Ratio: 0.999966497 (-34 PPM)

Item		Description
Status	Time Synchronization	Shows the status of whether the time synchronization function is enabled (Enabled) or disabled (Disable).
	Synchronization Status	Shows the status of time synchronization with the grandmaster. • Locked: Time synchronization in progress • Unlocked: Time synchronization has not been performed, or the amount of time correction from the grandmaster (Offset from Master) has exceeded the Accuracy Alert. ■Precautions If the managed switch itself is the grandmaster, the status is displayed as Unlocked.
	PTP Slave Port	Shows the port operating as a SlavePort.
	PTP Clock Time	Shows the time synchronized with the grandmaster.
Current Data Set	Offset From Master (ns)	Shows the amount of time correction with the grandmaster.
	Mean Path Delay (ns)	Shows the propagation delay time with the adjacent station.
	Step Removed	Shows the number of hops from the grandmaster. This number is 0 if the managed switch is the grandmaster.
Parent Data Set	Parent Identity	Shows the information related to the grandmaster. Refer to the IEEE 802.1AS standards.
	Grandmaster Identity	
	Grandmaster Priority 1	
	Grandmaster Priority 2	
	Grandmaster Clock Class	
	Grandmaster Clock Accuracy	
	Cumulative Rate Ratio	

3. Click the [Clear Graph] icon.

The latest status is displayed.



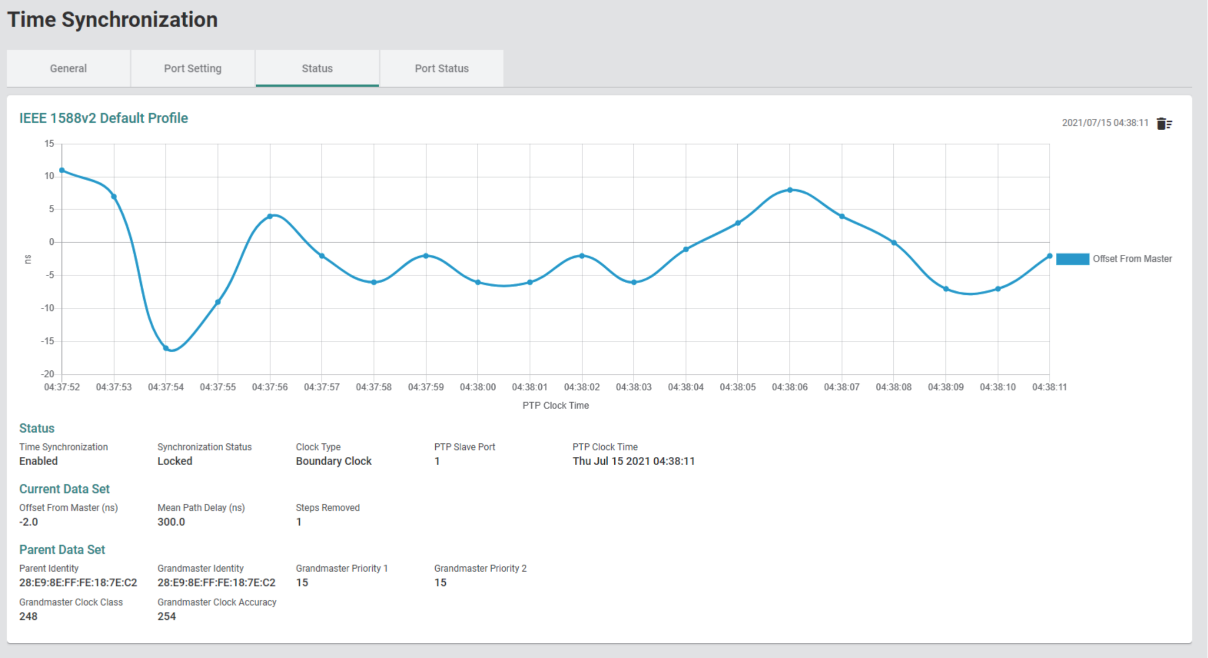
■IEEE 1588

Operating procedure

1. Start the operation from the "Time Synchronization" window.

[System] ⇨ [Time] ⇨ [Time Synchronization]

2. Select the [Status] tab.



Status

Time Synchronization	Synchronization Status	Clock Type	PTP Slave Port	PTP Clock Time
Enabled	Locked	Boundary Clock	1	Thu Jul 15 2021 04:38:11

Current Data Set

Offset From Master (ns)	Mean Path Delay (ns)	Steps Removed
-2.0	300.0	1

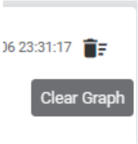
Parent Data Set

Parent Identity	Grandmaster Identity	Grandmaster Priority 1	Grandmaster Priority 2
28:E9:8E:FF:FE:18:7E:C2	28:E9:8E:FF:FE:18:7E:C2	15	15
Grandmaster Clock Class	Grandmaster Clock Accuracy		
248	254		

Item		Setting range
Status	Time Synchronization	Shows the status of whether the time synchronization function is enabled (Enabled) or disabled (Disable).
	Synchronization Status	Shows the status of time synchronization with the grandmaster. • Locked: Time synchronization in progress • Unlocked: Time synchronization has not been performed, or the amount of time correction from the grandmaster (Offset from Master) has exceeded the Accuracy Alert. ■Precautions If the managed switch itself is the grandmaster, the status is displayed as Unlocked.
	Clock Type	Shows the clock type.
	PTP Slave Port	Shows the port operating as a SlavePort.
	PTP Clock Time	Shows the time synchronized with the grandmaster.
Current Data Set	Offset From Master (ns)	Shows the amount of time correction with the grandmaster.
	Mean Path Delay (ns)	Shows the propagation delay time with the adjacent station.
	Step Removed	Shows the number of hops from the grandmaster. This number is 0 if the managed switch is the grandmaster.
Parent Data Set	Parent Identity	Shows the information related to the grandmaster. Refer to the IEEE 1588 standards.
	Grandmaster Identity	
	Grandmaster Priority 1	
	Grandmaster Priority 2	
	Grandmaster Clock Class	
	Grandmaster Clock Accuracy	

3. Click the [Clear Graph] icon.

The latest status is displayed.



Port status

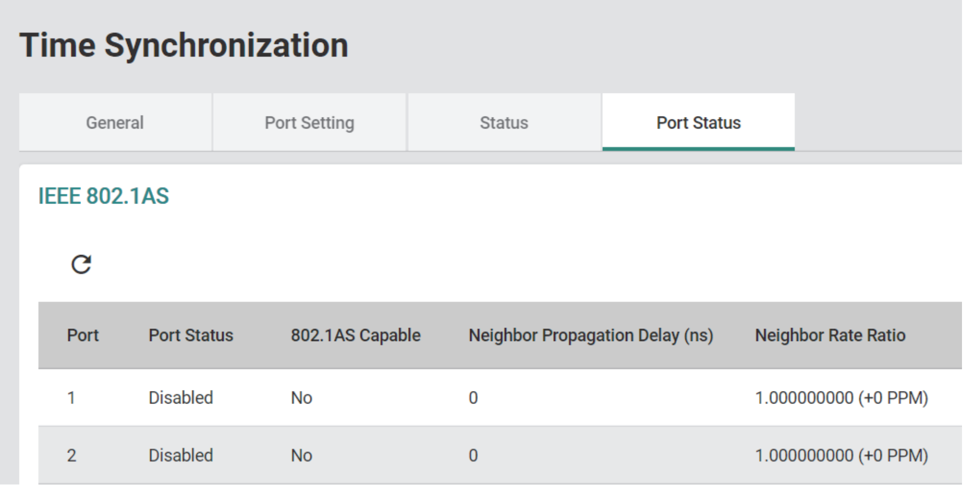
■IEEE 802.1AS

Operating procedure

1. Start the operation from the "Time Synchronization" window.

[System] ⇨ [Time] ⇨ [Time Synchronization]

2. Select the [Port Status] tab.

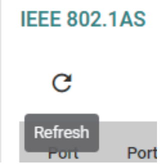


Port	Port Status	802.1AS Capable	Neighbor Propagation Delay (ns)	Neighbor Rate Ratio
1	Disabled	No	0	1.000000000 (+0 PPM)
2	Disabled	No	0	1.000000000 (+0 PPM)

Item	Setting range
Port	Shows the port number.
Port Status	Shows the port status.
802.1AS Capable	Shows the status of whether the IEEE 802.1AS protocol can be executed.
Neighbor Propagation Delay (ns)	Shows the propagation delay time with the adjacent station.
Neighbor Rate Ratio	Shows the clock ratio with the adjacent station.

Point

Click the [Refresh] icon to update the display to the latest information.



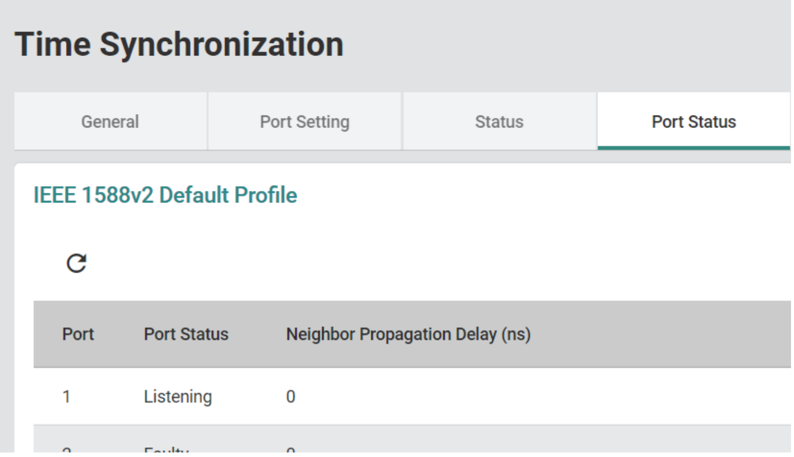
■IEEE 1588

Operating procedure

1. Start the operation from the "Time Synchronization" window.

[System] ⇨ [Time] ⇨ [Time Synchronization]

2. Select the [Port Status] tab.



Time Synchronization

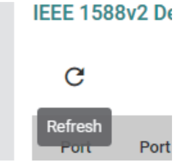
IEEE 1588v2 Default Profile

Port	Port Status	Neighbor Propagation Delay (ns)
1	Listening	0
2	Faulty	0

Item	Description
Port	Shows the port number.
Port Status	Shows the port status.
Neighbor Propagation Delay (ns)	Shows the propagation delay time with the adjacent station. This delay time is displayed when "Delay Mechanism" on the [General] tab is "Peer-to-Peer". 0 is displayed if "Delay Mechanism" is "End-to-End".

Point

Click the [Refresh] icon to update the display to the latest information.



8.5 Port Interface [Port Interface]

The following function can be used from the port interface [Port Interface] displayed on the function menu of the web interface.

- Port setting [Port Setting]

Port setting [Port Setting]

The following settings can be configured for each port. Also, the connection status can be checked for each port.

- Disabling the port
- Communication speed of the port
- Changing the port interface

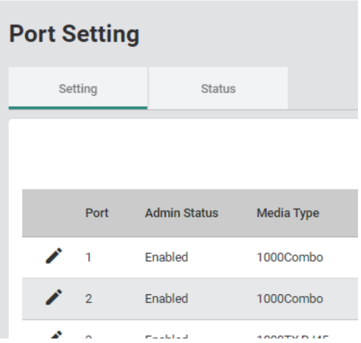
Setting method

Operating procedure

1. Start the operation from the "Port Setting" window.

[Port] ⇨ [Port Interface] ⇨ [Port Setting]

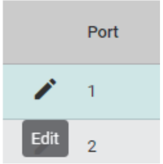
2. Select the [Setting] tab.



Port Setting

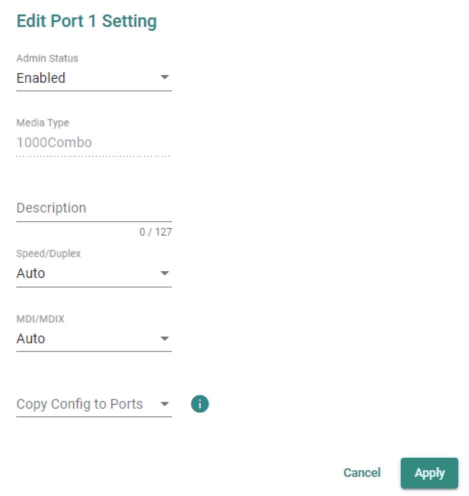
	Port	Admin Status	Media Type
✎	1	Enabled	1000Combo
✎	2	Enabled	1000Combo

3. Click the [Edit] icon of the port to be edited.



	Port
✎	1
Edit	2

4. Set the required items.



Edit Port 1 Setting

Admin Status: Enabled

Media Type: 1000Combo

Description: 0 / 127

Speed/Duplex: Auto

MDI/MDIX: Auto

Copy Config to Ports

Item	Description	Setting range
Admin Status	Permit or deny port data transfer. • Enabled: Permitted • Disabled: Denied	• Enabled • Disabled (Default: Enabled)
Media Type	Shows the media type of the port.	—
Description	Set the port alias (additional name). The initial character must be one-byte alphabetical characters.	0 to 127 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Speed/Duplex	Set the communication speed. If "Auto" (auto-negotiation) causes any problem, set a fixed speed for this item.	• Auto • 10M Half • 10M Full • 100M Half • 100M Full (Default: Auto)
MDI/MDIX	The port type of the Ethernet device is automatically detected and the port type is changed. If "Auto" (auto-detection) causes any problem, select "MDI" or "MDIX".	• Auto • MDI • MDIX (Default: Auto)
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Ports • 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: empty)

[*1] This item is not displayed for the NZ2MHG-TSNT4.

5. Click the [Apply] button.

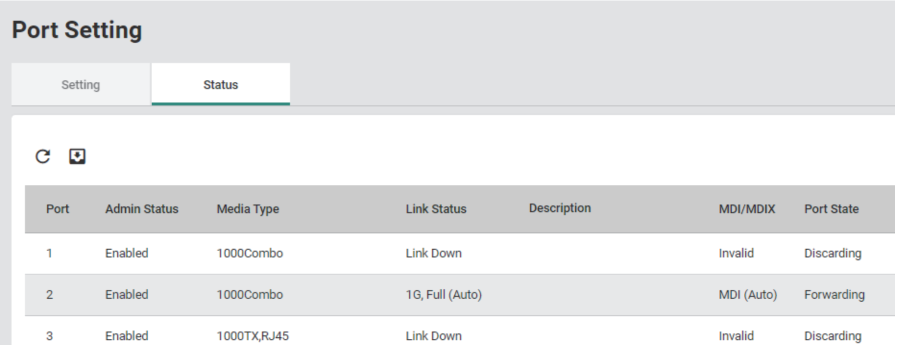
Status window

Operating procedure

1. Start the operation from the "Port Setting" window.

[Port] ⇨ [Port Interface] ⇨ [Port Setting]

2. Select the [Status] tab.



Port Setting

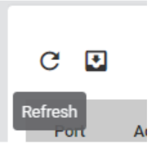
Setting | Status

Port	Admin Status	Media Type	Link Status	Description	MDI/MDIX	Port State
1	Enabled	1000Combo	Link Down		Invalid	Discarding
2	Enabled	1000Combo	1G, Full (Auto)		MDI (Auto)	Forwarding
3	Enabled	1000TX,RJ45	Link Down		Invalid	Discarding

Item	Description
Port	Shows the port number.
Admin Status	Shows the Admin Status set in "Port Setting". (☞ Page 141 Setting method)
Media Type	Shows the media type of the port.
Link Status	Shows the link status.
Description	Shows the description set in "Port Setting". (☞ Page 141 Setting method)
MDI/MDIX	Shows the port type of the Ethernet device. The type becomes Invalid when no port is connected.
Port State	Shows the port status.

Point

Click the [Refresh] icon to update the display to the latest information.



8.6 Layer 2 Switching Function [Layer 2 Switching]

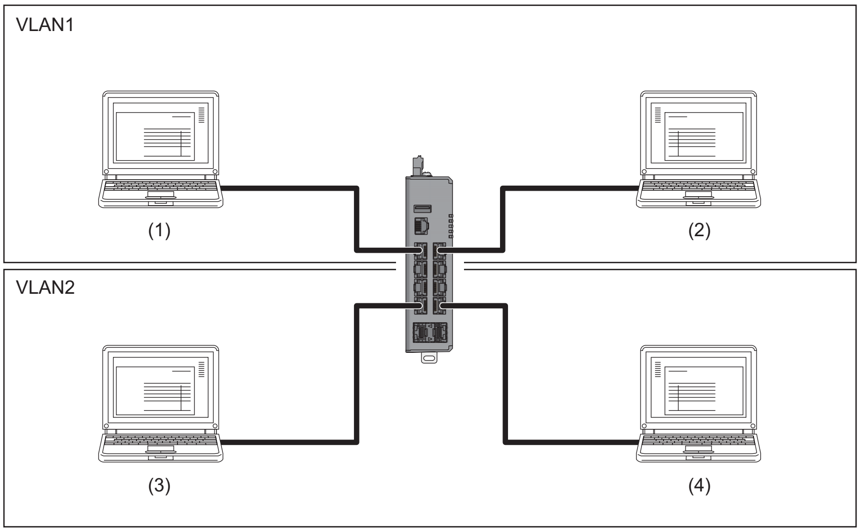
The following functions can be used from the layer 2 switching function [Layer 2 Switching] displayed on the function menu of the web interface.

- VLAN function [VLAN]
- Priority management setting [Priority Management]
- MAC address table [MAC]
- Multicast setting [Multicast]
- Time-sharing communication setting [Time-Aware Shaper]

VLAN function [VLAN]

The managed switch supports the VLAN function compliant with IEEE 802.1Q-2005. By using the VLAN function, networks can be virtually segmented without being limited by physical connections.

On the managed switch, a VLAN can be built at any location within the network where a single or multiple managed switches are present.



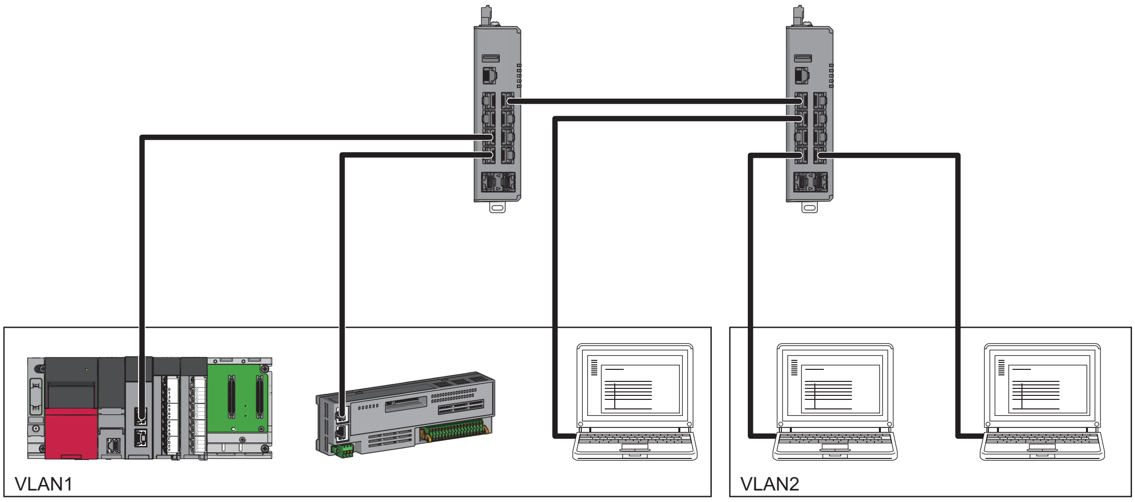
(1) Device No.1
(2) Device No.2
(3) Device No.3
(4) Device No.4

Using the VLAN function has the following three advantages.

- Ease of network management
- Bandwidth efficiency
- Enhanced security

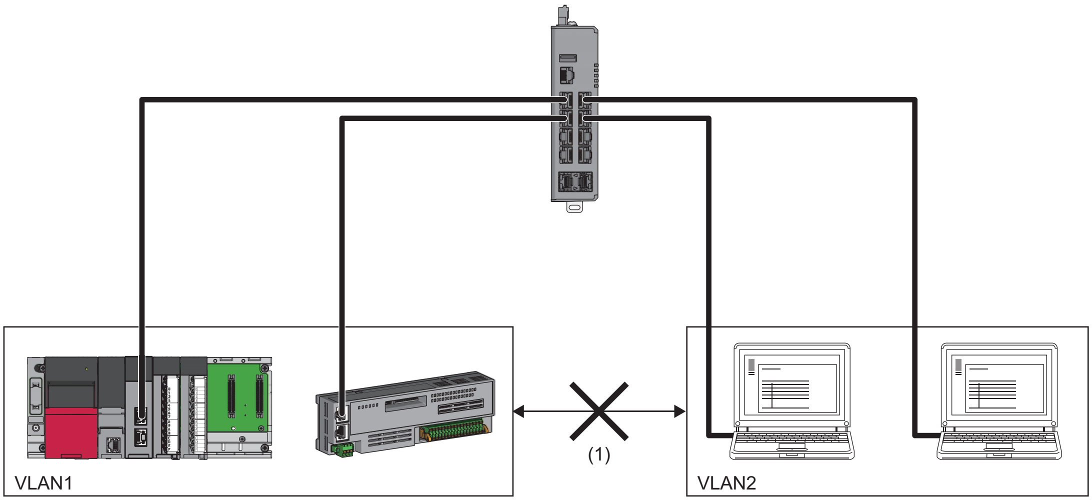
Ease of network management

The VLAN function allows a virtual network to be built at any location within a physical network where a single or multiple managed switches are present. Moreover, the network configuration can be changed by changing the managed switch settings. This eliminates the need for wiring and re-setting the parameters of the connected devices when changing the network configuration.



Bandwidth efficiency

In a large scale network, congestion may occur due to unnecessary traffic such as when broadcast frames are all transferred to network devices. By using the VLAN function to segment the devices that need to mutually communicate, network bandwidth can be effectively used.



(1) Even if physical connection is established, communication does not occur between VLANs.

Enhanced security

Virtually segmenting the network can minimize damage caused by unauthorized access, DoS attack, computer virus, and other types of cyber attack from Ethernet devices via the network.

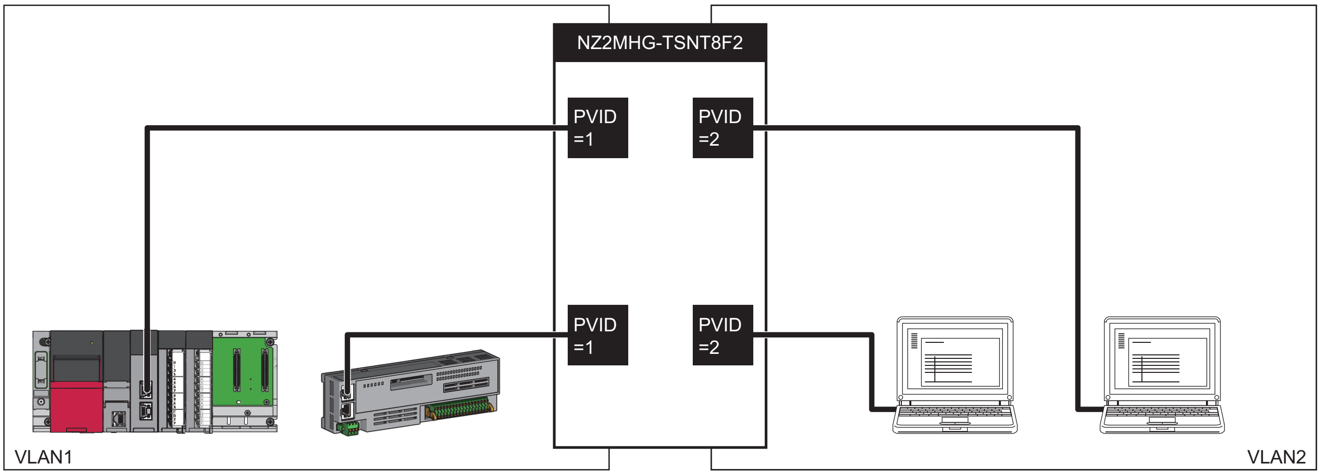
Port mode

The managed switch supports the following two VLAN port modes.

- Access port (Access Port)
- Trunk port (Trunk Port)

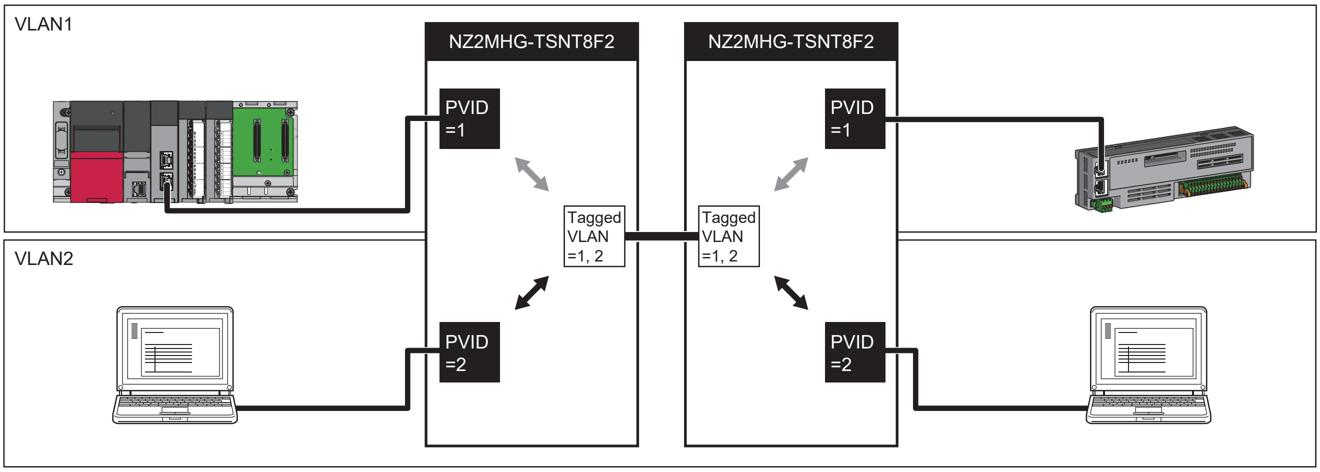
■Access port (Access Port)

A port to which devices (such as a personal computer) that are not assigned a VLAN tag are connected. This port belongs to a single VLAN and communicates with other ports assigned to the same VLAN.



■Trunk port (Trunk Port)

A trunk port is a port belonging to multiple VLANs. Ethernet frames to be sent and received via the trunk port are assigned a VLAN tag. VLAN tags can be used to identify which VLAN the frame belongs to, allowing communication to be sent and received to multiple VLANs with one cable.



(1) Access port

(2) Trunk port

(3) Two types of frames with different VLAN IDs are sent/received with one cable.

Management VLAN

The VID (VLAN ID) can be set for access to the web interface and CLI of the managed switch. Access is blocked if access is made from a VLAN that is not the management VLAN.

Point

By default, all ports can be used to access to the web interface or CLI of the managed switch.

Setting method

■Quick setting for management VLAN ports

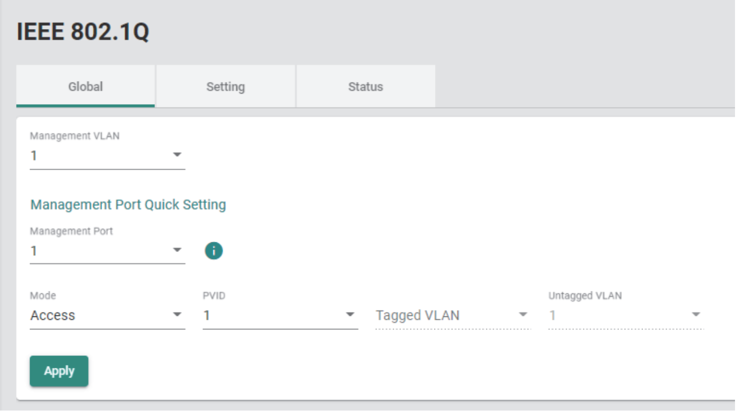
Operating procedure

1. Start the operation from the "IEEE 802.1Q" window.

[Layer 2 Switching] ⇨ [VLAN] ⇨ [IEEE802.1Q]

2. Select the [Global] tab.

3. Set the required items.



IEEE 802.1Q

Management VLAN: 1

Management Port Quick Setting

Management Port: 1

Mode: Access

PVID: 1

Tagged VLAN

Untagged VLAN: 1

Item	Description	Setting range
Management VLAN	Select a VID (VLAN ID) to be set to the management VLAN. (Select from those created in "VID" of the VLAN function (☞ Page 149 Adding a VLAN, Page 150 Editing a VLAN).)	1 to 4094 (Default: 1)
Management Port	Select a port number to be set.	NZ2MHG-TSNT8F2: 1 to 8 NZ2MHG-TSNT4: 1 to 4 (Default: 1)
Mode[*1]	Select the port mode. • Access: The port is set as the access port. • Trunk: The port is set as the trunk port.	• Access • Trunk (Default: empty)
PVID[*1]	Set a PVID (Port VLAN ID) of the port. (Select from those created in "VID" of the VLAN function (☞ Page 149 Adding a VLAN, Page 150 Editing a VLAN).)	1 to 4094 (Default: empty)
Tagged VLAN[*2]	Select the VLAN from which a tagged frame is to be sent. (Select from those created in "VID" of the VLAN function (☞ Page 149 Adding a VLAN, Page 150 Editing a VLAN).)	• All Member VIDs • 1 to 4094 (Default: empty)
Untagged VLAN[*3]	Shows the VLAN from which an untagged frame is to be sent.	—

*1 The setting is available after "Management Port" is set.

*2 Set this item when "Trunk" is selected for "Mode" of "Management Port".

*3 This item is displayed when "Access" is selected for "Mode" of "Management Port".

4. Click [Apply].

Point

To allocate a VLAN to which a device belongs, set the PVID (Port VLAN ID) for each port.

Precautions

If the management VLAN ID is changed, the connection with the managed switch is disconnected. Connect the personal computer to the port with the same VLAN ID as the new management VLAN ID, which can restore the connection.

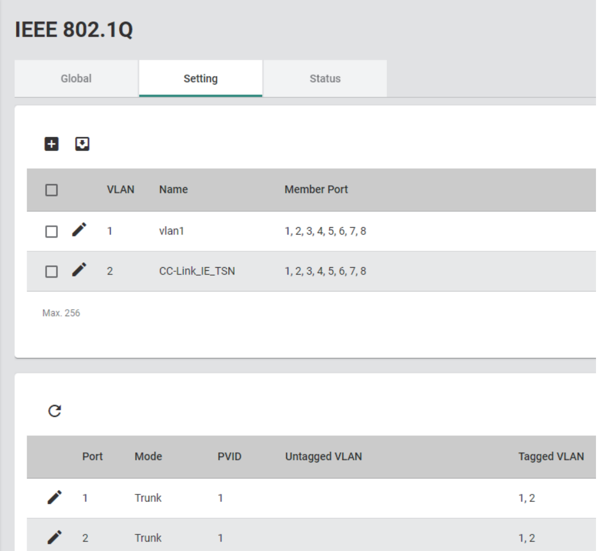
■Adding a VLAN

Operating procedure

1. Start the operation from the "IEEE 802.1Q" window.

[Layer 2 Switching] ⇨ [VLAN] ⇨ [IEEE802.1Q]

2. Select the [Setting] tab.



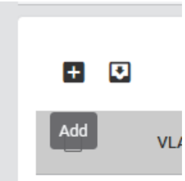
IEEE 802.1Q

□	VLAN	Name	Member Port
□	1	vlan1	1, 2, 3, 4, 5, 6, 7, 8
□	2	CC-Link_IE_TSN	1, 2, 3, 4, 5, 6, 7, 8

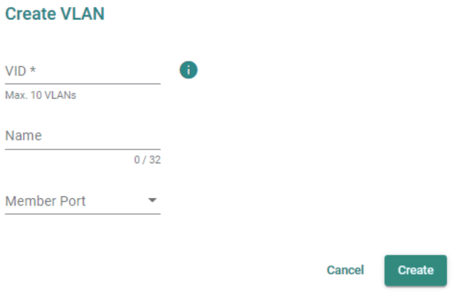
Max. 256

Port	Mode	PVID	Untagged VLAN	Tagged VLAN
1	Trunk	1		1, 2
2	Trunk	1		1, 2

3. Click the [Add] icon.



4. Input the required items.



Create VLAN

VID *

Max. 10 VLANs

Name

0 / 32

Member Port

Item	Description	Setting range
VID	■For Add Input a VLAN ID. Input as follows to create multiple VLAN IDs. Example: Input 3-12 to create 3 to 12 VLAN IDs. ■For Edit Shows the VLAN ID.	■For Add 1 to 4094 (Default: empty)
Name	Set the name of VLAN.	0 to 32 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Member Port[*1]	Select a port to belong to the VLAN.	NZ2MHG-TSNT8F2: 1 to 8 NZ2MHG-TSNT4: 1 to 4 (Default: empty)

[*1] The port can be selected only when the trunk port is set.

5. Click the [Create] button.

Point

Up to 256 items can be created.

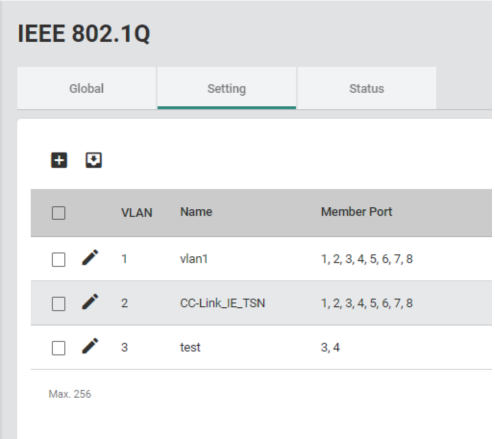
■Editing a VLAN

Operating procedure

1. Start the operation from the "IEEE 802.1Q" window.

[Layer 2 Switching] ⇨ [VLAN] ⇨ [IEEE802.1Q]

2. Select the [Setting] tab.

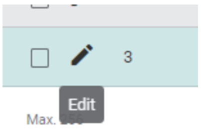


IEEE 802.1Q

□		VLAN	Name	Member Port
□	✎	1	vlan1	1, 2, 3, 4, 5, 6, 7, 8
□	✎	2	CC-Link_IE_TSN	1, 2, 3, 4, 5, 6, 7, 8
□	✎	3	test	3, 4

Max. 256

3. Click the [Edit] icon.



4. Input the required items.

The content of each item is the same as that for the add operation.

5. Click the [Apply] button.

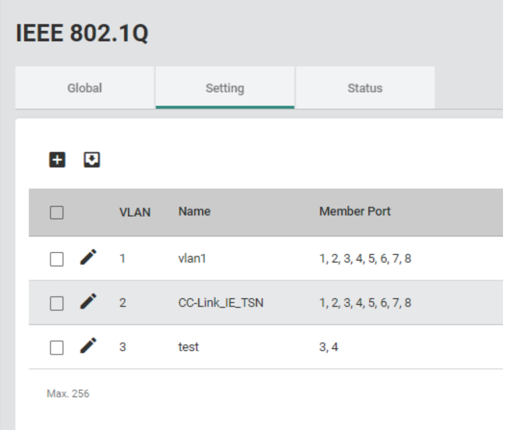
■Deleting a VLAN

Operating procedure

1. Start the operation from the "IEEE 802.1Q" window.

[Layer 2 Switching] ⇨ [VLAN] ⇨ [IEEE802.1Q]

2. Select the [Setting] tab.

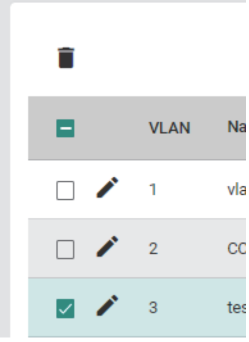


IEEE 802.1Q

☐		VLAN	Name	Member Port
☐	✎	1	vlan1	1, 2, 3, 4, 5, 6, 7, 8
☐	✎	2	CC-Link_IE_TSN	1, 2, 3, 4, 5, 6, 7, 8
☐	✎	3	test	3, 4

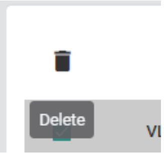
Max. 256

3. Select the checkbox of one or more VLANs to be deleted.



⊟		VLAN	Na
☐	✎	1	vla
☐	✎	2	CC
☑	✎	3	tes

4. Click the [Delete] icon.



5. The confirmation dialog appears. Click the [Delete] button to perform deletion.

Point

VLAN 1 and VLAN 2 cannot be deleted.

■VLAN setting for each port

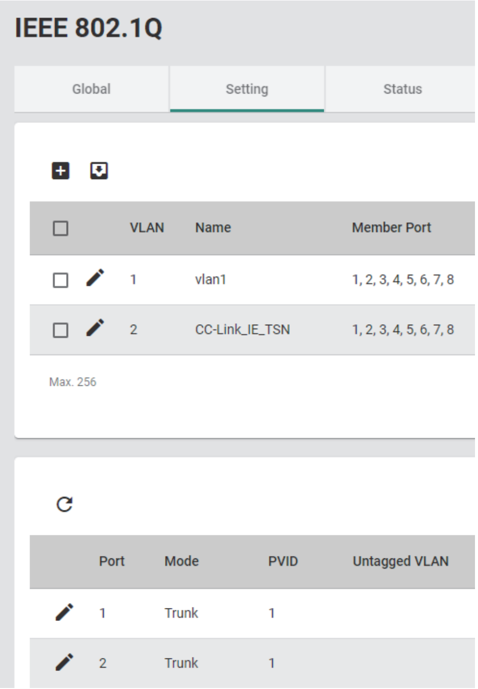
For each port, set the port mode and the VLAN to which the port belongs.

Operating procedure

1. Start the operation from the "IEEE 802.1Q" window.

[Layer 2 Switching] ⇨ [VLAN] ⇨ [IEEE802.1Q]

2. Select the [Setting] tab.

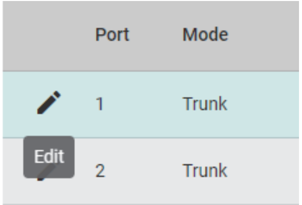


□		VLAN	Name	Member Port
□	✎	1	vlan1	1, 2, 3, 4, 5, 6, 7, 8
□	✎	2	CC-Link_IE_TSN	1, 2, 3, 4, 5, 6, 7, 8

Max. 256

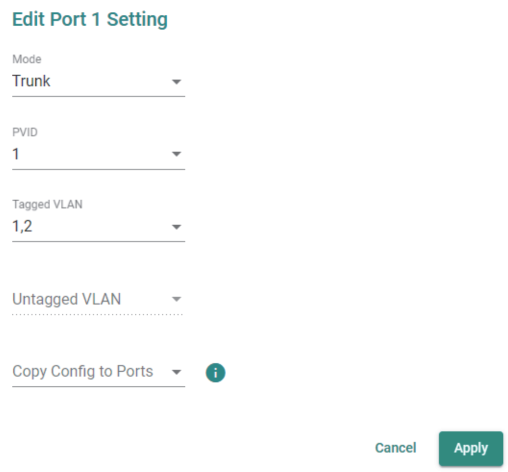
	Port	Mode	PVID	Untagged VLAN
✎	1	Trunk	1	
✎	2	Trunk	1	

3. From the port list at the lower part of the window, click the [Edit] icon of a port whose parameters are to be edited.



	Port	Mode
✎	1	Trunk
✎	2	Trunk

4. Set the required items.



Edit Port 1 Setting

Mode: Trunk

PVID: 1

Tagged VLAN: 1,2

Untagged VLAN

Copy Config to Ports

Item	Description	Setting range
Mode	Select the port mode. • Access: The port is set as the access port. • Trunk: The port is set as the trunk port.	• Access • Trunk (Default: Trunk)
PVID	Set a PVID (Port VLAN ID) of the port. (Select from those created in "VID" of the VLAN function (☞ Page 149 Adding a VLAN, Page 150 Editing a VLAN).)	1 to 4094 (Default: 1)
Tagged VLAN[*1]	Select the VLAN from which a tagged frame is to be sent. Multiple items can be selected. (Select from those created in "VID" of the VLAN function (☞ Page 149 Adding a VLAN, Page 150 Editing a VLAN).)	• All Member VIDs • 1 to 4094 (Default: 1, 2)
Untagged VLAN[*2]	Shows the VLAN from which an untagged frame is to be sent.	—
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Port • 1 • 2 • 3 • 4 • 5[*3] • 6[*3] • 7[*3] • 8[*3] (Default: empty)

[*1] This item is enabled only when "Mode" is set to "Trunk".

[*2] This item is enabled only when "Mode" is set to "Access".

[*3] This item is not displayed for the NZ2MHG-TSNT4.

5. Click the [Apply] button.

Precautions

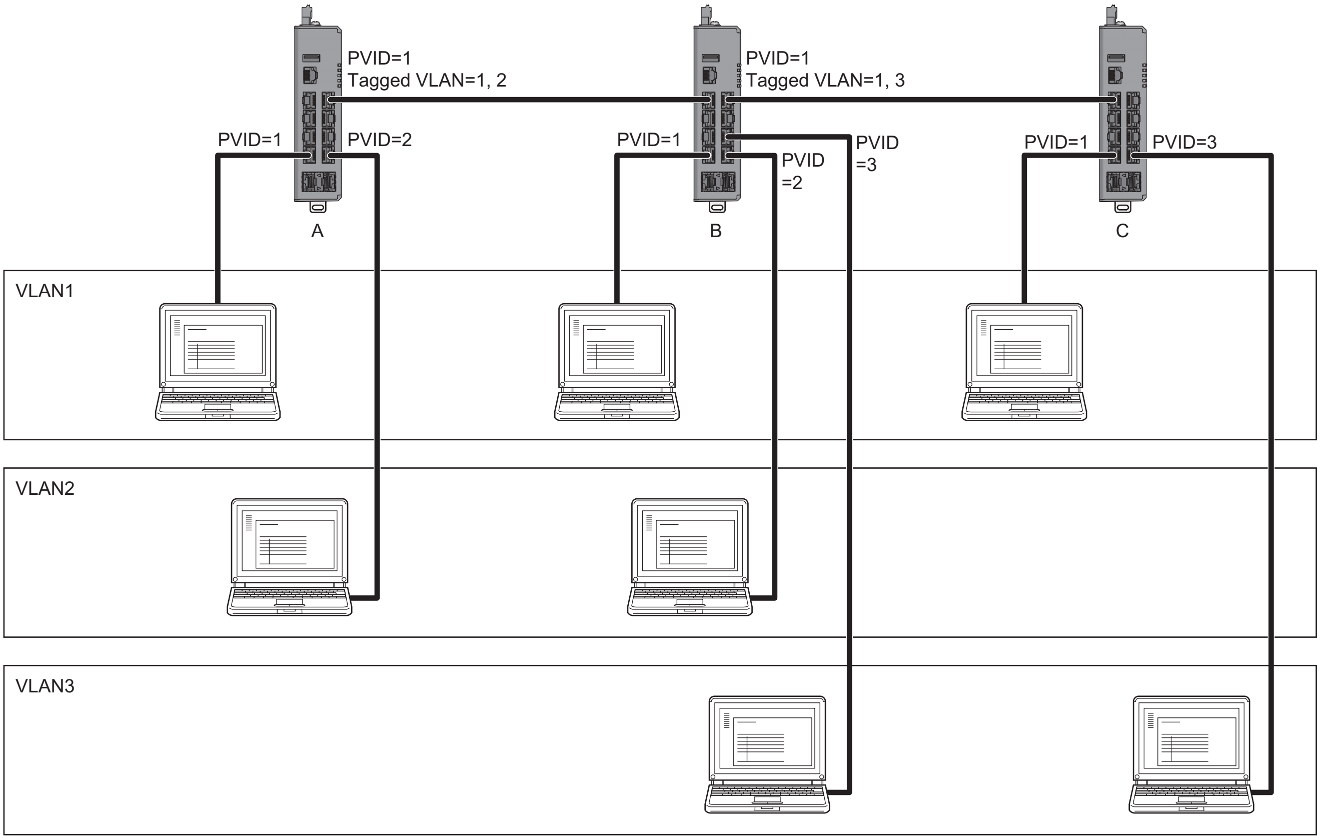
Only devices that support the VLAN function can communicate with the port set as the trunk port. If any device that does not support VLAN needs to be connected to the trunk port, configure the untagged output setting. (☞ Page 157 Priority management function [Priority Management])

Setting precautions

- Set the PVID (Port VLAN ID) of the access port so that the VIDs (VLAN IDs) match between devices that communicate with each other. Also, when communication is to be performed via the trunk port, set the VLAN so that the VLAN ID for communication to the Tagged VLAN of the trunk port is included.
- If the port belonging to the Member Port of the VLAN is not included, that VID (VLAN ID) cannot be used as the setting value.
- When frames input to the access port are output from the trunk port, the PVID (Port VLAN ID) of the input port is stored in the VLAN tag.
- When frames without a VLAN tag are input to the trunk port, the PVID (Port VLAN ID) of the input port is assigned to the frames.
- When different VIDs (VLAN IDs) are assigned by frame type in the per-stream priority setting and a device that does not support VLAN needs to communicate via multiple VLANs, set the port to be connected to the device that does not support VLAN to the trunk port.
- To share the cables, set the VLAN ID of the network from which communication is to be performed to the Tagged VLAN.

Setting example

The following figure shows the setting example of the VLAN function.



In the system configuration example shown above, multiple VLANs are used for communication between the managed switches A and B and the managed switches A and C. Therefore, the VLAN tagging setting is required for the port that are connected between the managed switches. The following table lists parameter settings for each port of each managed switch.

Managed switch	Port	Mode	PVID	Untagged VLAN[*2]	Tagged VLAN	Egress Untag[*3]
A	1	Access	1	1	—	Enabled
	2	Access	2	2	—	Enabled
	8	Trunk	1[*1]	—	1, 2	Disabled
B	1	Access	1	1	—	Enabled
	2	Access	2	2	—	Enabled
	4	Access	3	3	—	Enabled
	7	Trunk	1[*1]	—	1, 2	Disabled
	8	Trunk	1[*1]	—	1, 3	Disabled
C	1	Access	1	1	—	Enabled
	2	Access	3	3	—	Enabled
	7	Trunk	1[*1]	—	1, 3	Disabled

[*1] Since the trunk ports do not receive VLAN untagged frames, any PVID can be set.
[*2] The VLAN is automatically set according to the setting values of Mode and PVID.
[*3] For the setting of Egress Untag, refer to the following.
☞ Page 164 Untagged output

Precautions

The following are the precautions for using the VLAN function.

- The default VLAN 1 is set to the management VLAN with which parameters of the managed switches can be set. If the port belonging to the management VLAN is no longer present, the parameters cannot be set via the Ethernet.
- When communication is to be performed between devices assigned to different VLANs, install a router or layer 3 switching device to the port belonging to the respective VLANs.
- The time synchronization function and spanning tree function are unaffected by the VLAN function settings. The time synchronization function and spanning tree function cannot be used per VLAN.

Priority management function [Priority Management]

The priority of receive frames can be managed. By prioritizing receive frames, frames with a higher priority is transferred first when a conflict occurs in frame transfer. On the managed switch, receive frames can be prioritized by the following ways.

- Port priority: The priority (Priority Code Point (PCP)) of receive frames can be defined per port.
- Per-stream priority: By identifying the input port, EtherType value, and Subtype value of receive frames, the VID (VLAN ID) and priority (Priority Code Point (PCP)) can be defined by frame type.

Point

The per-stream priority takes precedence over the port priority.

Also, when frames are transferred, they can be output with the VLAN tags removed. This enables devices that do not support the VLAN function to be connected to the trunk port.

Setting method

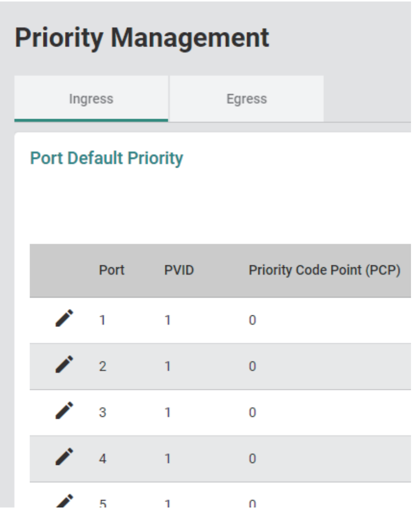
■Port priority

Operating procedure

1. Start the operation from the "Priority Management" window.

[Layer 2 Switching] ⇨ [Priority Management]

2. Select the [Ingress] tab.

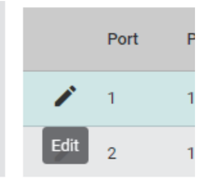


Priority Management

Port Default Priority

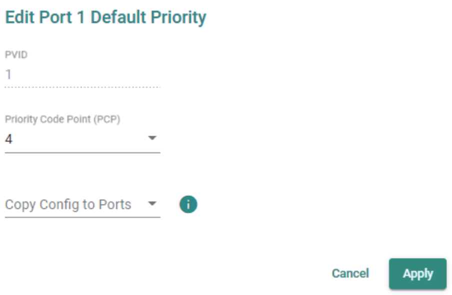
	Port	PVID	Priority Code Point (PCP)
✎	1	1	0
✎	2	1	0
✎	3	1	0
✎	4	1	0
✎	5	1	0

3. Click the [Edit] icon of the port to be edited.



	Port	P
✎	1	1
Edit	2	1

4. Set the required items.



Edit Port 1 Default Priority

PVID
1

Priority Code Point (PCP)
4

Copy Config to Ports

Item	Description	Setting range
PVID	Shows the PVID of the port.	—
Priority Code Point (PCP)	Set the priority.	0 to 7 (Default: 0)
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Port • 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: empty)

*1 This item is not displayed for the NZ2MHG-TSNT4.

5. Click the [Apply] button.

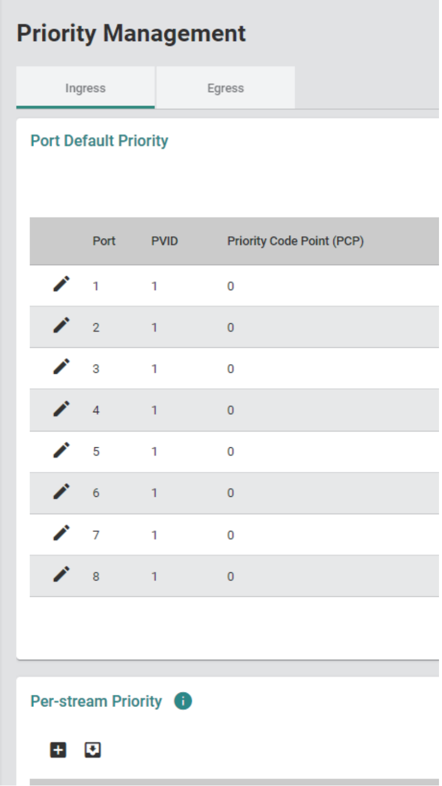
■Per-stream priority (Addition)

Operating procedure

1. Start the operation from the "Priority Management" window.

[Layer 2 Switching] ⇨ [Priority Management]

2. Select the [Ingress] tab.



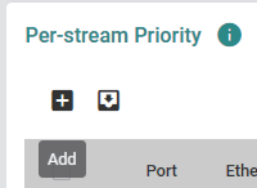
Priority Management

Port Default Priority

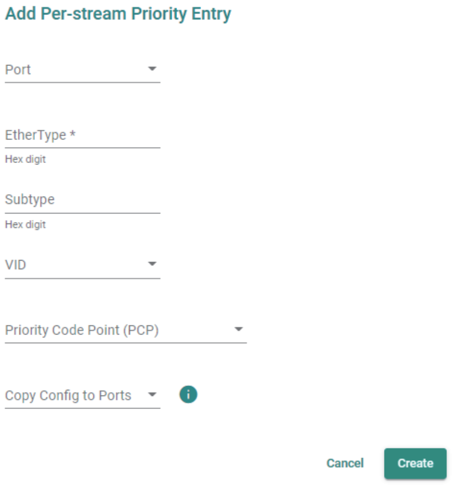
	Port	PVID	Priority Code Point (PCP)
✎	1	1	0
✎	2	1	0
✎	3	1	0
✎	4	1	0
✎	5	1	0
✎	6	1	0
✎	7	1	0
✎	8	1	0

Per-stream Priority

3. Click the [Add] icon of "Per-stream Priority" at the lower part of the window.



4. Set the required items.


Add Per-stream Priority Entry

Port

EtherType *
Hex digit

Subtype
Hex digit

VID

Priority Code Point (PCP)

Copy Config to Ports

Item	Description	Setting range
Port	Select the port to be set. This item cannot be changed when the per-stream priority is edited.	NZ2MHG-TSNT8F2: 1 to 8 NZ2MHG-TSNT4: 1 to 4 (Default: empty)
EtherType	Input the EtherType value for identifying the receive frames in hexadecimal.	One-byte alphanumeric characters and symbols (Default: empty)
Subtype	Input the Subtype value for identifying the receive frames in hexadecimal.	• Empty • One-byte alphanumeric characters and symbols (Default: empty)
VID	Select a VID (VLAN ID) to be assigned to the receive frames. (Select from those created in "VID" of the VLAN function (☞ Page 149 Adding a VLAN, Page 150 Editing a VLAN).)	1 to 4094 (Default: empty)
Priority Code Point (PCP)	Set the priority of the VID to be assigned to the receive frames.	0 to 7 (Default: empty)
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected. This item is not displayed when the per-stream priority is edited.	• All Port • 1 • 2 • 3 • 4 • 5*1 • 6*1 • 7*1 • 8*1 (Default: empty)

*1 This item is not displayed for the NZ2MHG-TSNT4.

5. Click the [Create] button.

Point

- Up to 80 priorities (10 priorities per port) can be added.
- If the Subtype value is not set, the Subtype of the receive frames is ignored.

Precautions

The receive frames are processed in the order in which they were added to the setting. The result of the VID (VLAN ID) and Priority Code Point (PCP) defined by the receive frames may change depending on the order in which the receive frames were added to the setting. (If a receive frame matches more than one setting, the first setting that matches is used for processing.)

Ex.

When the result changes by the added order

Receive frame: EtherType: 890FH + Subtype: 00C0H

Setting example 1			
EtherType	**Subtype**	**VID**	**PCP**
890FH	00C0H	1	0
890FH	—	1	7

Result 1: VID: 1 + PCP: 0

Setting example 2			
EtherType	**Subtype**	**VID**	**PCP**
890FH	—	1	7
890FH	00C0H	1	0

Result 2: VID: 1 + PCP: 7

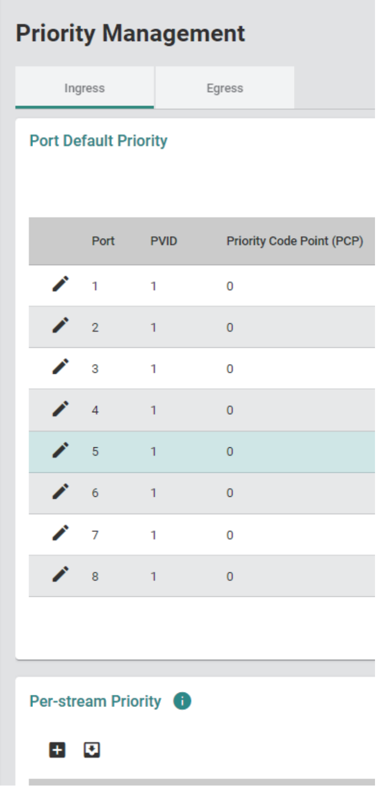
■Per-stream priority (Editing)

Operating procedure

1. Start the operation from the "Priority Management" window.

[Layer 2 Switching] ⇨ [Priority Management]

2. Select the [Ingress] tab.



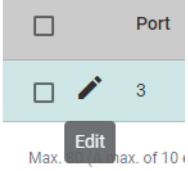
Priority Management

Port Default Priority

	Port	PVID	Priority Code Point (PCP)
✎	1	1	0
✎	2	1	0
✎	3	1	0
✎	4	1	0
✎	5	1	0
✎	6	1	0
✎	7	1	0
✎	8	1	0

Per-stream Priority

3. Click the [Edit] icon of "Per-stream Priority" at the lower part of the window.



□		Port
□	✎	3

Max. 80 (A max. of 10

4. Edit the required items.

- The parameter in "Port" cannot be edited.
- "Copy Config to Ports" is not displayed.

5. Click the [Apply] button.

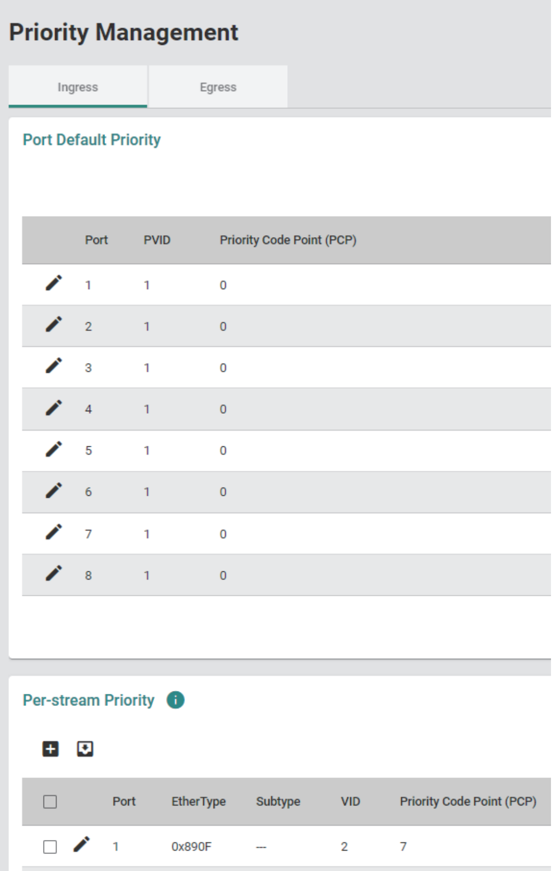
■Per-stream priority (Deletion)

Operating procedure

1. Start the operation from the "Priority Management" window.

[Layer 2 Switching] ⇨ [Priority Management]

2. Click the [Ingress] tab.



Priority Management

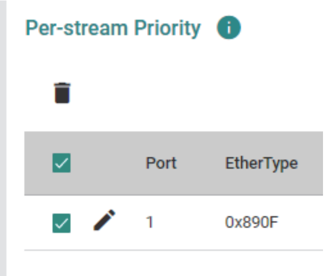
Port Default Priority

	Port	PVID	Priority Code Point (PCP)
✎	1	1	0
✎	2	1	0
✎	3	1	0
✎	4	1	0
✎	5	1	0
✎	6	1	0
✎	7	1	0
✎	8	1	0

Per-stream Priority

□		Port	EtherType	Subtype	VID	Priority Code Point (PCP)
□	✎	1	0x890F	--	2	7

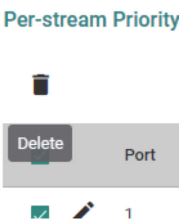
3. Select the checkbox of one or more priority settings to be deleted.



Per-stream Priority

☑		Port	EtherType
☑	✎	1	0x890F

4. Click the [Delete] icon.



Per-stream Priority

		Port
☑	✎	1

5. The confirmation dialog appears. Click the [Delete] button to perform deletion.

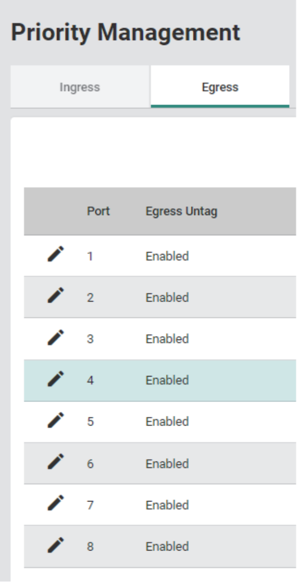
■Untagged output

Operating procedure

1. Start the operation from the "Priority Management" window.

[Layer 2 Switching] ⇨ [Priority Management]

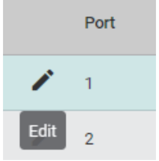
2. Select the [Egress] tab.



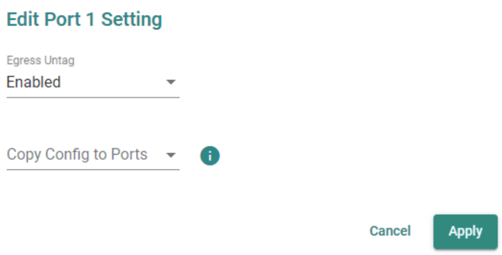
Priority Management

Port	Egress Untag
1	Enabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
6	Enabled
7	Enabled
8	Enabled

3. Click the [Edit] icon of the port to be edited.



4. Set the required items.



Edit Port 1 Setting

Egress Untag: Enabled

Copy Config to Ports

Item	Description	Setting range
Egress Untag	Enable or disable the untagged output. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Port • 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: empty)

*1 This item is not displayed for the NZ2MHG-TSNT4.

5. Click the [Apply] button.

Point

- If any device that does not support VLAN is to be connected to the trunk port, enable the untagged output.
- If the VLAN wiring is to be shared through the trunk port, disable the untagged output.

MAC address [MAC]

For the learning method of MAC addresses, the managed switch uses the Independent VLAN Learning mode.

In the Independent VLAN Learning mode, the MAC address information of a connected device is stored in the MAC address table that is created on each VLAN.

The MAC addresses are stored in association with VIDs (VLAN IDs). Therefore, the same MAC address may be associated with different VIDs (VLAN IDs) before being stored in the table.

The following two methods are available for registering MAC addresses in the MAC address table.

- Auto (Independent VLAN Learning mode)
- Manual (Static unicast address registration)

The following describes the static unicast address registration and MAC address table settings.

Static unicast address registration

Unicast MAC addresses can be manually registered in the MAC address table.

If the destination MAC address of the receive frames is absent in the MAC address table, the frames are sent to all the ports except the receive port belonging to the same VLAN.

Registering a MAC address to the MAC address table in advance can prevent unnecessary traffic.

MAC address table

MAC addresses registered in the MAC address table can be checked. Also, the aging time for the MAC address table can be set.

The aging time for the MAC address is the time in which the learned MAC address is held in the MAC address table.

When the set aging time for the MAC address has been reached, the learned MAC address is deleted from the MAC address table.

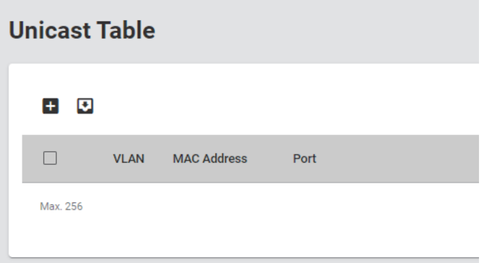
Setting method

■Static unicast (Addition)

Operating procedure

1. Start the operation from the "Unicast Table" window.

[Layer 2 Switching] ⇨ [MAC] ⇨ [Static Unicast]

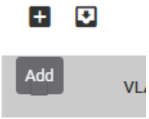


Unicast Table

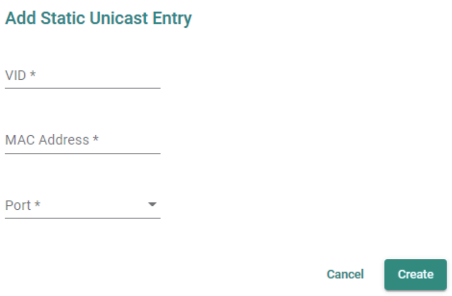
□	VLAN	MAC Address	Port

Max. 256

2. Click the [Add] icon.



3. Set the required items.



Item	Description	Setting range
VID	Input the VLAN ID to be associated. (Select from those created in "VID" of the VLAN function (☞ Page 149 Adding a VLAN, Page 150 Editing a VLAN).)	1 to 4094 (Default: empty)
MAC Address	Input a unicast MAC address.	□□:□□:□□:□□:□□:□□ (Default: empty)
Port	Specify a port for transmission.	• 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: empty)

[*1] This item is not displayed for the NZ2MHG-TSNT4.

4. Click the [Create] button and add the setting.

Point

Up to 256 unicast MAC addresses can be registered.

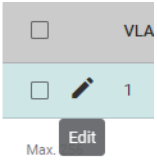
■Static unicast (Editing)

Operating procedure

1. Start the operation from the "Unicast Table" window.

[Layer 2 Switching] ⇨ [MAC] ⇨ [Static Unicast]

2. Click the [Edit] icon of the static unicast to be edited.



3. Edit the required items.

The content of each item is the same as that for the add operation.

4. Click the [Apply] button.

Point

When the static unicast has been edited, the edited content is reflected to the MAC address table after the power is turned off and on again.

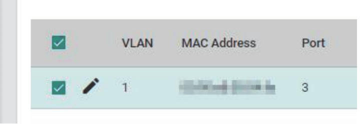
■Static unicast (Deletion)

Operating procedure

1. Start the operation from the "Unicast Table" window.

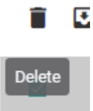
[Layer 2 Switching] ⇨ [MAC] ⇨ [Static Unicast]

2. Select the checkbox of one or more lists to be deleted.



☑	VLAN	MAC Address	Port
☑ ✎	1	[redacted]	3

3. Click the [Delete] icon.



4. The confirmation dialog appears. Click the [Delete] button to perform deletion.

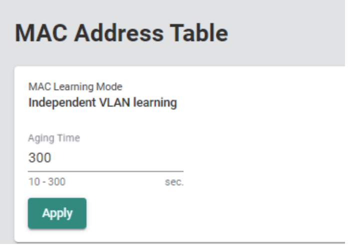
■MAC address table

Operating procedure

1. Start the operation from the "MAC Address Table" window.

[Layer 2 Switching] ⇨ [MAC] ⇨ [MAC Address Table]

2. Set the MAC address aging time.



MAC Address Table

MAC Learning Mode
Independent VLAN learning

Aging Time
300
10 - 300 sec.

Item	Description	Setting range
MAC Learning Mode	Shows the MAC address learning mode.	Independent VLAN learning (Fixed)
Aging Time	Set the MAC address aging time.	10 to 300 (Default: 300)

3. Click the [Apply] button.

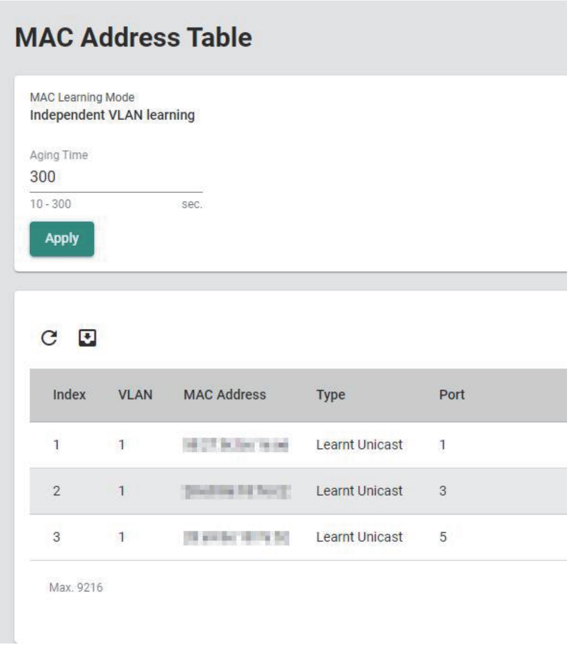
Checking the MAC address table

MAC addresses registered in the MAC address table can be checked.

Operating procedure

1. Start the operation from the "MAC Address Table" window.

[Layer 2 Switching] ⇨ [MAC] ⇨ [MAC Address Table]



MAC Address Table

MAC Learning Mode
Independent VLAN learning

Aging Time
300
10 - 300 sec.

Apply

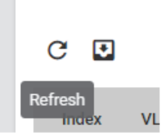
Index	VLAN	MAC Address	Type	Port
1	1	[redacted]	Learnt Unicast	1
2	1	[redacted]	Learnt Unicast	3
3	1	[redacted]	Learnt Unicast	5

Max. 9216

Item	Description
Index	Shows the MAC address registration number.
VLAN	Shows the VLAN number.
MAC Address	Shows the MAC address of a device.
Type	Shows the type. • Learnt Unicast: Learned unicast MAC address • Learnt Multicast: Learned multicast MAC address • Static Unicast: Static unicast MAC address • Static Multicast: Static multicast MAC address
Port	Shows the transfer port of the MAC address.

Point

Click the [Refresh] icon to update the display to the latest information.



Multicast setting function [Static Multicast]

The multicast MAC address can be manually registered to the MAC address table. Setting the transfer destination port in advance can reduce the network load.

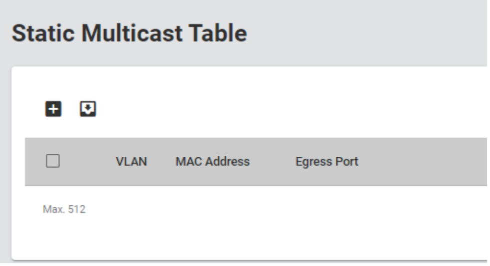
Setting method

■Adding

Operating procedure

1. Start the operation from the "Static Multicast Table" window.

[Layer 2 Switching] ⇨ [Multicast] ⇨ [Static Multicast]

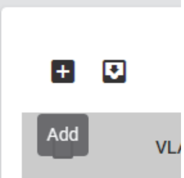


Static Multicast Table

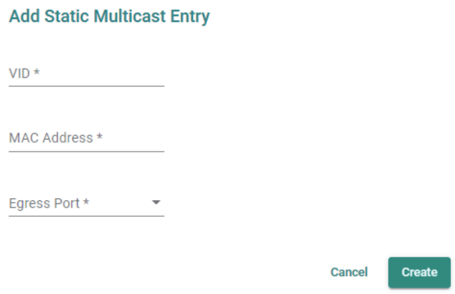
□	VLAN	MAC Address	Egress Port

Max. 512

2. Click the [Add] icon.



3. Set the required items.



Add Static Multicast Entry

VID *

MAC Address *

Egress Port *

Item	Description	Setting range
VID	Input a VLAN ID to be associated with the multicast group. (Select from those created in "VID" of the VLAN function (☞ Page 149 Adding a VLAN, Page 150 Editing a VLAN).)	1 to 4094 (Default: empty)
MAC Address	Input a multicast MAC address.	□□:□□:□□:□□:□□:□□ (Default: empty)
Egress Port	Specify the output port of the multicast. Multiple items can be selected.	• 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: empty)

*1 This item is not displayed for the NZ2MHG-TSNT4.

4. Click the [Create] button.

Point

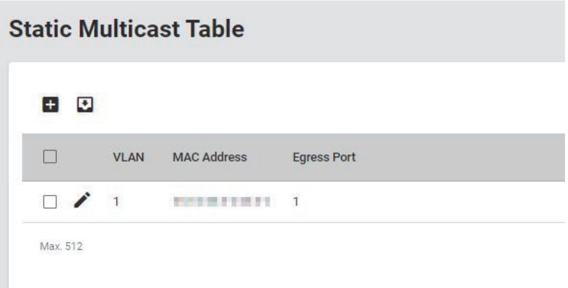
Up to 512 multicast MAC addresses can be registered.

■For editing

Operating procedure

1. Start the operation from the "Static Multicast" window.

[Layer 2 Switching] ⇨ [Multicast] ⇨ [Static Multicast]

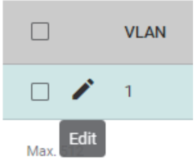


Static Multicast Table

□		VLAN	MAC Address	Egress Port
□	✎	1	[redacted]	1

Max. 512

2. Click the [Edit] icon.



3. Set the required items.

The content of each item is the same as that for the add operation.

4. Click the [Apply] button.

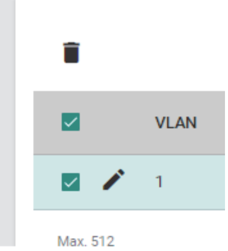
■Deleting

Operating procedure

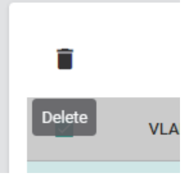
1. Start the operation from the "Static Multicast" window.

[Layer 2 Switching] ⇨ [Multicast] ⇨ [Static Multicast]

2. Select the checkbox of one or more lists to be deleted.



3. Click the [Delete] icon.

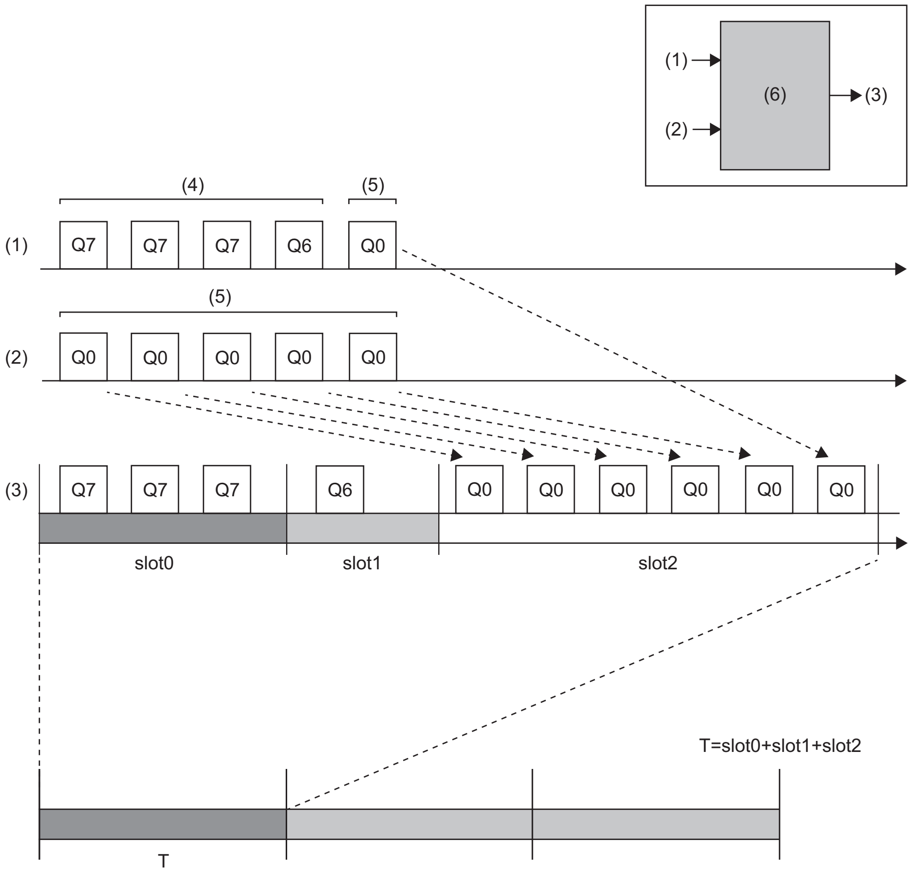


4. The confirmation dialog appears. Click the [Delete] button to perform deletion.

Time-sharing communication [Time-Aware Shaper]

The managed switch supports the time-sharing communication function by IEEE 802.1Qbv. Time-sharing communication is a function that applies the time-sharing scheduling to the traffic that was input to the managed switch by priority before outputting the traffic in a desired time slot.

The real time traffic and non-real time traffic can be mixed by applying time-sharing communication to the time synchronized networks. Also, the traffic can be guaranteed against the periodic transmission delay.



T: Communication cycle

(1) Input 1 (high priority + low priority)

(2) Input 2 (low priority)

(3) Output

(4) High priority

(5) Low priority

(6) Managed switch

Precautions

When time-sharing communication is used, the time slot and queue in the network need to be appropriately set so that the communication cycles match. If the communication cycles do not match, communication may become unstable.

Setting method

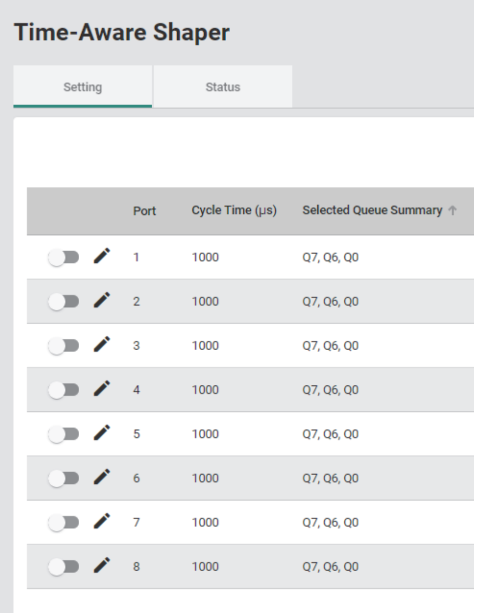
■Adding/editing time slots

Operating procedure

1. Start the operation from the "Time-Aware Shaper" window.

[Layer 2 Switching] ⇨ [Time-Aware Shaper]

2. Select the [Setting] tab.

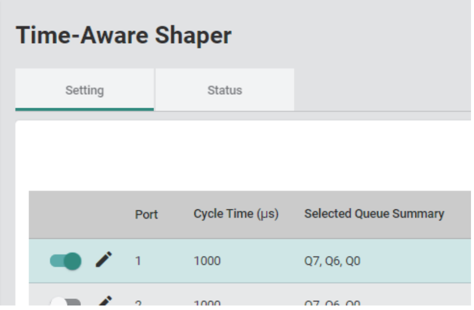


Time-Aware Shaper

	Port	Cycle Time (µs)	Selected Queue Summary ↑
	1	1000	Q7, Q6, Q0
	2	1000	Q7, Q6, Q0
	3	1000	Q7, Q6, Q0
	4	1000	Q7, Q6, Q0
	5	1000	Q7, Q6, Q0
	6	1000	Q7, Q6, Q0
	7	1000	Q7, Q6, Q0
	8	1000	Q7, Q6, Q0

3. Enable the setting of the port through which time-sharing communication is to be performed.

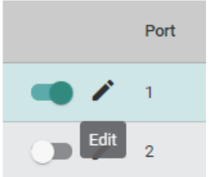
Time-sharing communication is enabled if the toggle button is green.



Time-Aware Shaper

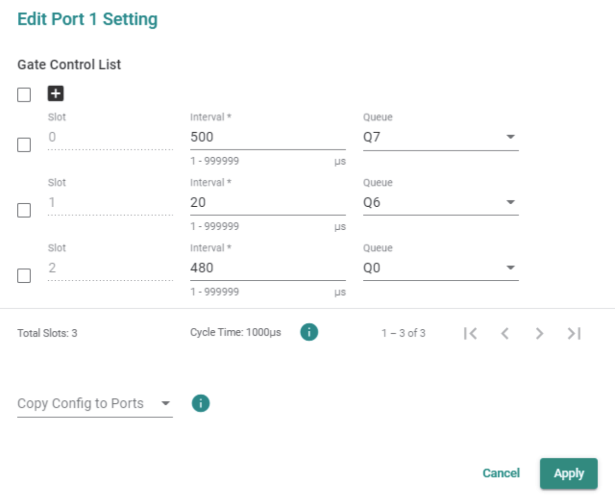
	Port	Cycle Time (µs)	Selected Queue Summary
	1	1000	Q7, Q6, Q0
	2	1000	Q7, Q6, Q0

4. Click the [Edit] icon.



	Port
	1
	2

5. The setting window is displayed.



Edit Port 1 Setting

Gate Control List

□ ⊞

	Slot	Interval *	Queue
□	0	500 1 - 999999 μs	Q7
□	1	20 1 - 999999 μs	Q6
□	2	480 1 - 999999 μs	Q0

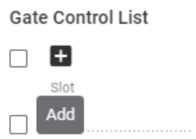
Total Slots: 3   Cycle Time: 1000μs   1 – 3 of 3

Point

To connect with CC-Link IE TSN compatible devices, the time slots are added to all ports by default. When connecting with CC-Link IE TSN compatible devices, change a value of "Interval" according to the communication period setting of the master station, and enable time-sharing communication. (☞ Page 38 How to Connect with CC-Link IE TSN Compatible Devices)

6. Click the [Add] icon.

Add time slots as needed.



Gate Control List

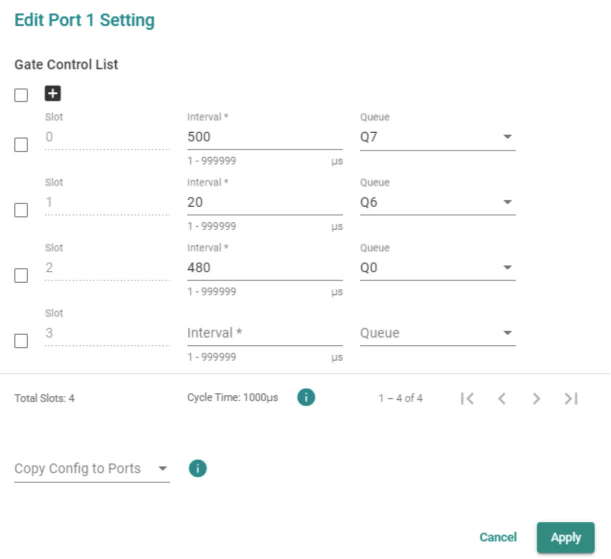
□ ⊞

Slot

□

8

7. Set the required items.



Edit Port 1 Setting

Gate Control List

□ ⊞

	Slot	Interval *	Queue
□	0	500 1 - 999999 µs	Q7
□	1	20 1 - 999999 µs	Q6
□	2	480 1 - 999999 µs	Q0
□	3	Interval * 1 - 999999 µs	Queue

Total Slots: 4   Cycle Time: 1000µs   1 – 4 of 4

Item	Description	Setting range
Interval	Set the time slot interval.	1.000 to 999999.000µs (Default: empty)
Queue	Set the queue. Multiple items can be selected.	• Q0 • Q2 • Q3 • Q4 • Q5 • Q6 • Q7 (Default: empty)
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Port • 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: empty)

[*1] This item is not displayed for the NZ2MHG-TSNT4.

8. Click the [Apply] button.

Point

- The communication data to be assigned to the queue corresponds to the PCP value. (☞ Page 157 Priority management function [Priority Management])
- If the communication cycle (Cycle Time) exceeds 999999µs, the setting cannot be saved.

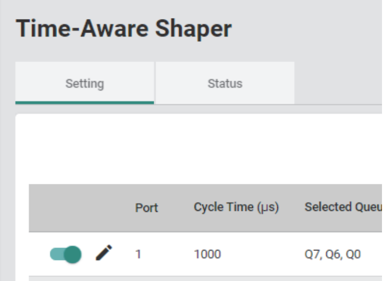
■Deleting time slots

Operating procedure

1. Start the operation from the "Time-Aware Shaper" window.

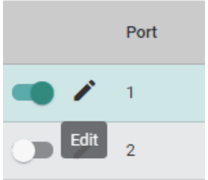
[Layer 2 Switching] ⇨ [Time-Aware Shaper]

2. Select the [Setting] tab.

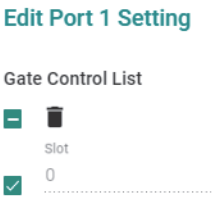


	Port	Cycle Time (μs)	Selected Queu
	1	1000	Q7, Q6, Q0

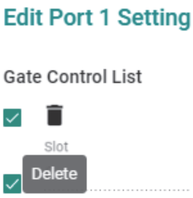
3. Click the [Edit] icon of the port to be deleted.



4. Select the checkbox of one or more lists to be deleted.



5. Click the [Delete] icon.



6. The setting is deleted.

7. Click the [Apply] button.

Displaying the status

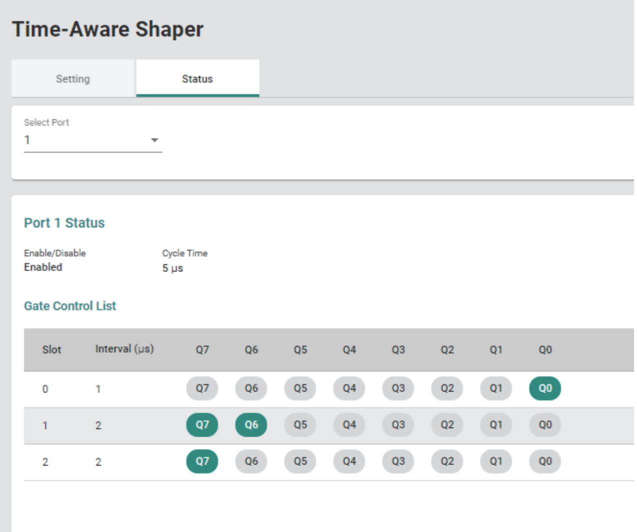
Operating procedure

1. Start the operation from the "Time-Aware Shaper" window.

[Port] ⇨ [Time-Aware Shaper]

2. Select the [Status] tab.

To check the setting status of time-sharing communication per port, specify a port number to be displayed in "Select Port".



Time-Aware Shaper

Setting | Status

Select Port
1

Port 1 Status

Enable/Disable
Enabled

Cycle Time
5 μs

Gate Control List

Slot	Interval (μs)	Q7	Q6	Q5	Q4	Q3	Q2	Q1	Q0
0	1	Q7	Q6	Q5	Q4	Q3	Q2	Q1	**Q0**
1	2	**Q7**	**Q6**	Q5	Q4	Q3	Q2	Q1	Q0
2	2	**Q7**	Q6	Q5	Q4	Q3	Q2	Q1	Q0

8.7 Layer 2 Redundancy Function

The following function can be used from the layer 2 redundancy function [Layer 2 Redundancy] displayed on the function menu of the web interface.

- Spanning tree function [Spanning Tree]

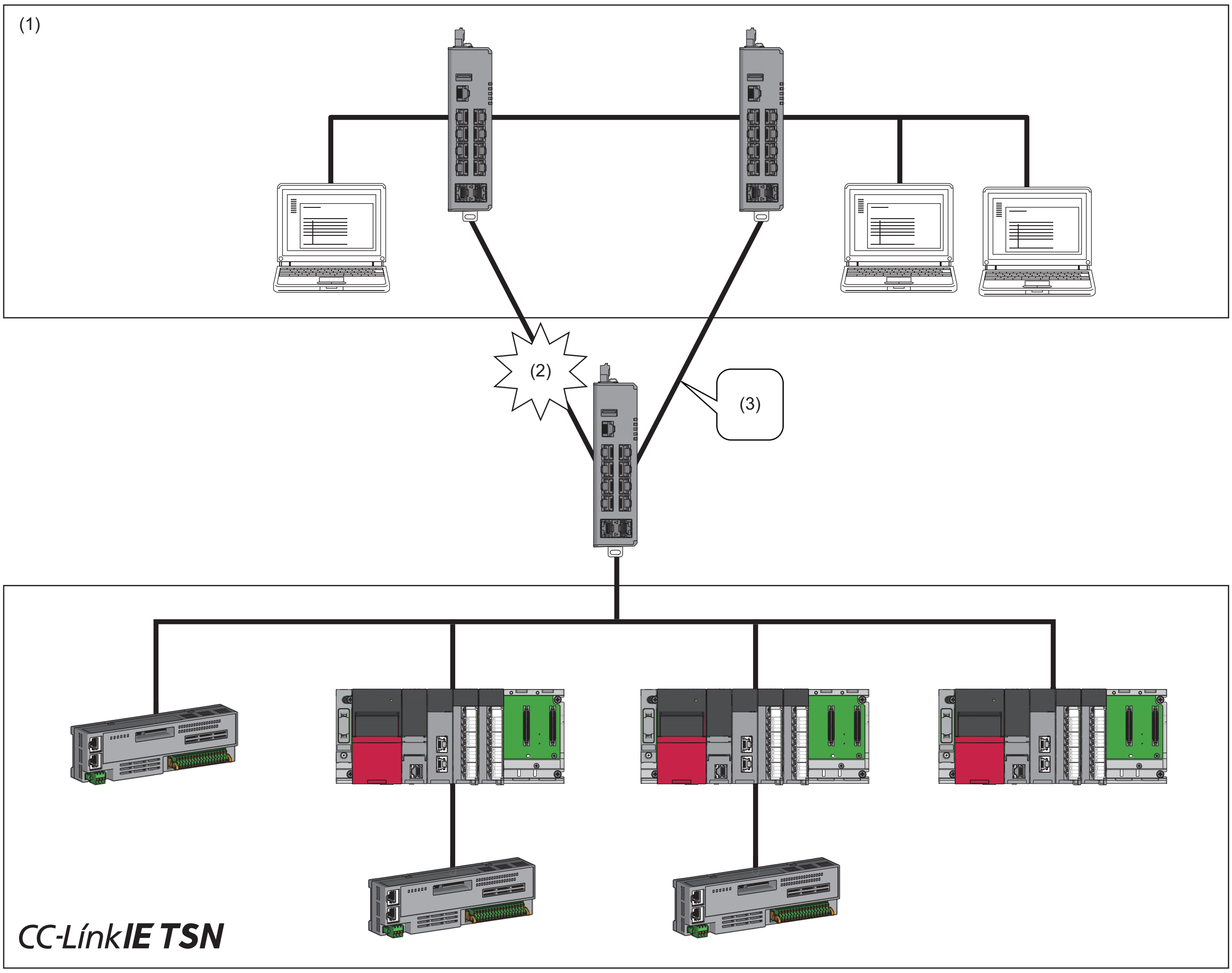
Spanning tree function

The spanning tree function builds the logical topology in which the loop paths have been eliminated on the network to make the communication route between the managed switches redundant.

If any failure such as cable disconnection occurs, the function automatically switches the communication route so that the system can recover in a short time. This function also prevents network failures caused by unintended loop formation.

The spanning tree function uses a control frame called the BPDU frame to perform the following processes.

- Find and disable low-efficiency paths (such as paths with low bandwidth).
- Enable one of the low-efficiency paths if a high-efficiency path fails.



(1) Information-system network
(2) Failure occurrence
(3) The system recovers automatically with a backup route.

Point

- By default, the spanning tree function is disabled.
- To make the communication route redundant, the spanning tree function needs to be enabled for all the managed switches included in the path that will become a loop.
- Switching the communication route takes time ranging from a few seconds to a few tens of seconds depending on the system configuration or the setting values of the parameters. Therefore, be aware that the stations in data link may be disconnected.

Difference between the STP and RSTP

In the RSTP (Rapid Spanning Tree Protocol), a port connected one-to-one (Point to Point) can switch the connection route quicker than that in the STP (Spanning Tree Protocol) by exchanging information between the adjacent managed switches.

Precautions

If any device such as a switching hub exists in the communication route between the managed switches, because it is not connected one-to-one (Point to Point), RSTP cannot be used for communication.

BPDU filter

The BPDU filter is a function to disable the transmission/reception of BPDUs (Bridge Protocol Data Units) per port. The BPDU is a frame to be used for communication route calculation in STP. The BPDU filter is used by a device connected to a port for blocking the transmission/reception of BPDUs.

Setting method

■Enabling the spanning tree

Operating procedure

1. Start the operation from the "Spanning Tree" window.

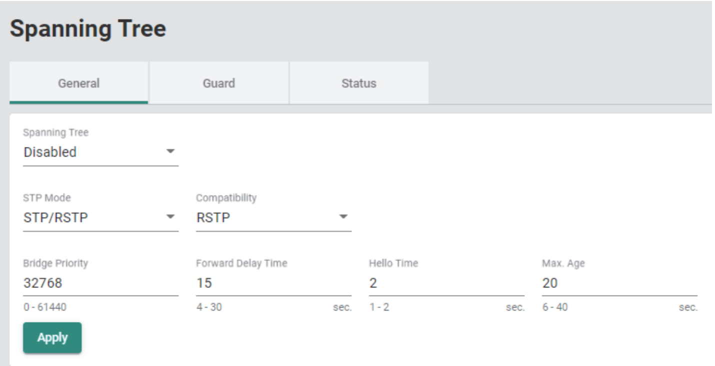
[Network Redundancy] ⇨ [Layer 2 Redundancy] ⇨ [Spanning Tree]

2. Click the [General] tab.

3. Set the required items.

Time required for switching the communication route varies depending on the setting values of the following parameters.

- Forward Delay Time
- Hello Time
- Max. Age



Spanning Tree

Spanning Tree: Disabled

STP Mode: STP/RSTP

Compatibility: RSTP

Bridge Priority: 32768 (0 - 61440)

Forward Delay Time: 15 (4 - 30 sec.)

Hello Time: 2 (1 - 2 sec.)

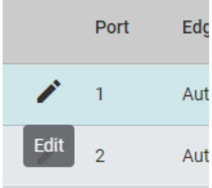
Max. Age: 20 (6 - 40 sec.)

Item	Description	Setting range
Spanning Tree	Enable or disable the spanning tree function. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)
STP Mode	The STP/RSTP mode is used for the spanning tree protocol.	STP/RSTP (Fixed)
Compatibility	Select the compatibility. • STP: Operates only in STP. • RSTP: Operates in STP and RSTP.	• STP • RSTP (Default: RSTP)
Bridge Priority	Set the bridge priority. The lower the setting value, the higher the bridge priority. Devices with high bridge priority are often selected as the route bridge of the spanning tree topology.	Multiple of 4096, which is from 0 to 61440 (Default: 32768)
Forward Delay Time	Set the time up to topology change confirmation.	4 to 30s (Default: 15s)
Hello Time	Set the transmission interval of the Hello messages. In the spanning tree protocol, the Hello messages are periodically sent to other devices on the network to check if the topology is normal.	1s, 2s (Default: 2s)

Item	Description	Setting range
Max. Age	If a device other than the route bridge could not receive the Hello messages sent from the route bridge by the time set in "Max. Age", the device sets itself as the route bridge. When two or more route bridges are recognized on the network, the respective devices rebuild the spanning tree topology.	6 to 40s (Default: 20s)

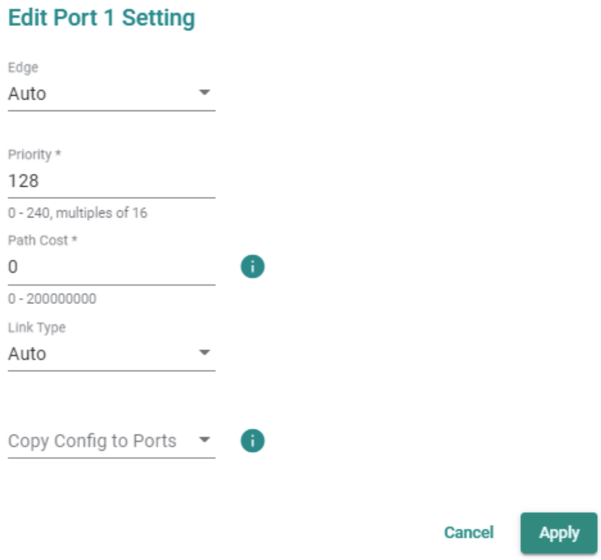
4. Click [Apply].

5. Click the [Edit] icon of the port to be edited.



	Port	Edg
✎	1	Aut
Edit	2	Aut

6. Set the required items.



Edit Port 1 Setting

Edge
Auto

Priority *
128
0 - 240, multiples of 16

Path Cost *
0
0 - 200000000

Link Type
Auto

Copy Config to Ports

Item	Description	Setting range
Edge	Configure the port setting. • Auto: The port is automatically set. • Yes: The port is set as the edge port. • No: The port is set as the non-edge port.	• Auto • Yes • No (Default: Auto)
Priority	Set the port priority. The smaller the value, the higher the port priority. Ports with high priority are often assigned to the route port. Set this item to a multiple of 16.	Multiple of 16, which is from 0 to 240 (Default: 128)
Path Cost	Set the path cost. If the value is set to 0, the path cost is automatically assigned according to the communication speed. ■For 1Gbps 20000 ■For 100Mbps 200000 ■For 10Mbps 2000000	0 to 200000000 (Default: 0)
Link Type[*1]	Configure the port mode setting. • Point-to-Point: Full-duplex mode. The port needs to be connected to a device that performs full-duplex communication. • Shared: Half-duplex mode. The port needs to be connected to a device that performs half-duplex communication. • Auto: The Point-to-Point mode or Shared mode is automatically selected.	• Point-to-Point • Shared • Auto (Default: Auto)

Item	Description	Setting range
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Ports • 1 • 2 • 3 • 4 • 5[*2] • 6[*2] • 7[*2] • 8[*2] (Default: empty)

*1 This item is displayed only when Advanced Mode is set.

*2 This item is not displayed for the NZ2MHG-TSNT4.

7. Click the [Apply] button.

Precautions

Do not set the port in which the managed switches are connected to each other as the edge port. Otherwise, an unintended loop may form.

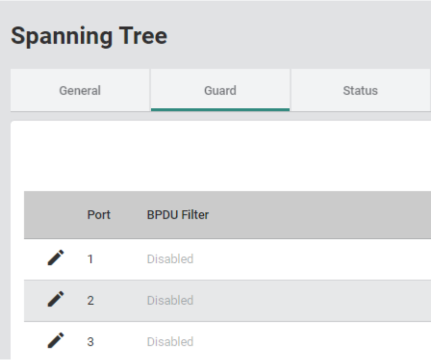
■BPDU filter

Operating procedure

1. Start the operation from the "Spanning Tree" window.

[Network Redundancy] ⇨ [Layer 2 Redundancy] ⇨ [Spanning Tree]

2. Select the [Guard] tab.

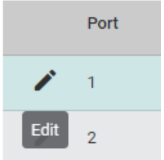


Spanning Tree

General | Guard | Status

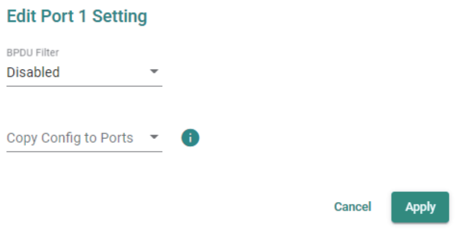
	Port	BPDU Filter
✎	1	Disabled
✎	2	Disabled
✎	3	Disabled

3. Click the [Edit] icon of the port to be set.



	Port
✎	1
Edit	2

4. Set the required items.



Edit Port 1 Setting

BPDU Filter: Disabled

Item	Description	Setting range
BPDU Filter	Enable or disable the BPDU filter. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Ports • 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: empty)

[*1] This item is not displayed for the NZ2MHG-TSNT4.

5. Click the [Apply] button.

Precautions

Disable the BPDU filter for the port where the loop occurs. If the BPDU filter is enabled for the port where the loop occurs, the communication route may not be properly redundant.

Status window

The following information can be checked from the status window.

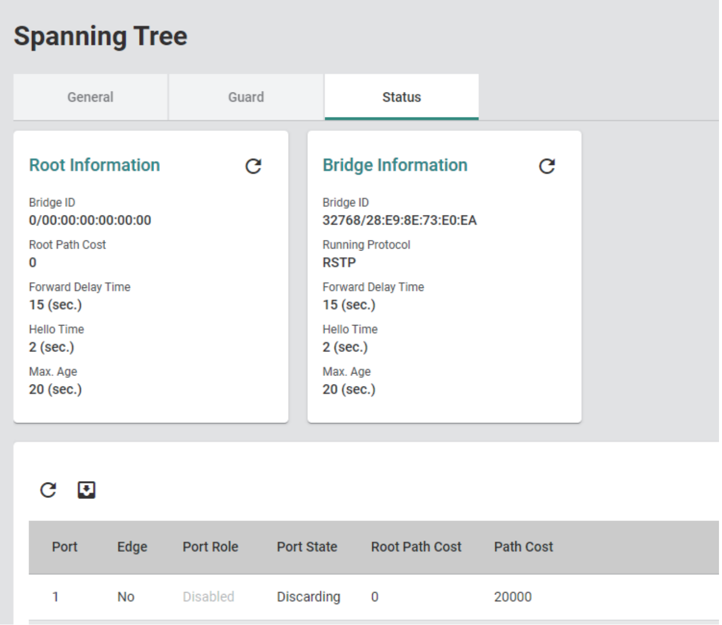
- Route information
- Bridge information
- Port status

Operating procedure

1. Start the operation from the "Spanning Tree" window.

[Network Redundancy] ⇨ [Layer 2 Redundancy] ⇨ [Spanning Tree]

2. Click the [Status] tab.



Spanning Tree

General | Guard | Status

Root Information

Bridge ID
0/00:00:00:00:00:00

Root Path Cost
0

Forward Delay Time
15 (sec.)

Hello Time
2 (sec.)

Max. Age
20 (sec.)

Bridge Information

Bridge ID
32768/28:E9:8E:73:E0:EA

Running Protocol
RSTP

Forward Delay Time
15 (sec.)

Hello Time
2 (sec.)

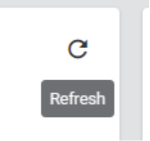
Max. Age
20 (sec.)

Port	Edge	Port Role	Port State	Root Path Cost	Path Cost
1	No	Disabled	Discarding	0	20000

Item		Description
Root Information	Bridge ID	Shows the Bridge Priority and MAC address of the route bridge.
	Root Path Cost	Shows the path cost up to the route bridge.
	Forward Delay Time	Shows the Forward Delay Time of the route bridge.
	Hello Time	Shows the Hello Time of the route bridge.
	Max. Age	Shows the Max. Age of the route bridge.
Bridge Information	Bridge ID	Shows the Bridge Priority and MAC address.
	Running Protocol	Shows the running protocol.
	Forward Delay Time	Shows the Forward Delay Time that is set.
	Hello Time	Shows the Hello Time that is set.
	Max. Age	Shows the Max. Age that is set.
Port		Shows the port number.
Edge		Shows the port.
Port Role		• Root: The port is directly or indirectly connected to the route bridge. • Designated: The port is specified if the port can send the optimum BPDU on the segment to which it is connected. • Alternate: The alternate [Alternate] port is a port that receives a more useful BPDU from another bridge before blocking communication. • Backup: The backup [Backup] port is a port that receives a more useful BPDU from the same bridge before blocking communication. • Disabled: The spanning tree function is disabled.
Port State		• Forwarding: Communication can be performed. • Discarding: Communication is blocked. • Disabled: The spanning tree function is disabled.
Root Path Cost		Shows the total path cost to the route bridge.
Path Cost		Shows the path cost of the port.

Point

Click the [Refresh] icon to update the display to the latest information.



8.8 Network Management

The following functions can be used from the network management [Network Management] displayed on the function menu of the web interface.

- SNMP
- SNMP Trap/Inform

SNMP

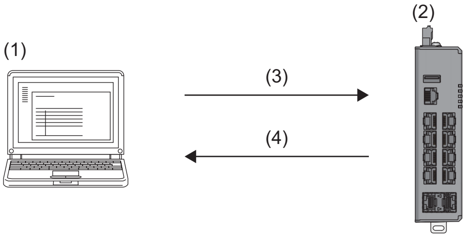
On the SNMP, the devices are monitored and controlled by the following operations.

- MIB acquisition request [Get Request]
- MIB modification request [Set Request]

MIB acquisition request

The MIB value can be acquired.

- SNMP manager: Specify the OID and request the information to be obtained from the SNMP agent.
- SNMP agent: Insert a value and reply to the OID requested from the SNMP manager.

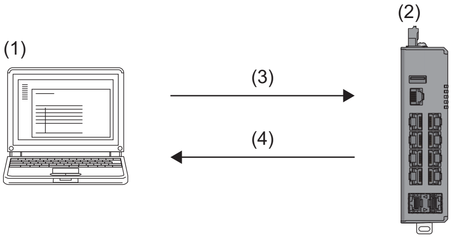


(1) Monitoring server (SNMP manager)
(2) Monitoring target device (SMP agent)
(3) Request for value (Get Request)
(4) Response (Get Response)

MIB modification request

The MIB value can be modified.

- SNMP manager: To modify the SNMP agent settings, specify the OID and request for modification.
- SNMP agent: Insert a value and reply to the OID requested from the SNMP manager.



(1) Monitoring server (SNMP manager)
(2) Monitoring target device (SMP agent)
(3) Request for value modification (Get Request)
(4) Response (Get Response)

Device management

To manage devices using SNMP, authentication needs to be set between the SNMP manager and the SNMP agent. (The SNMP agent allows access from the SNMP manager and allows information to be exchanged.)

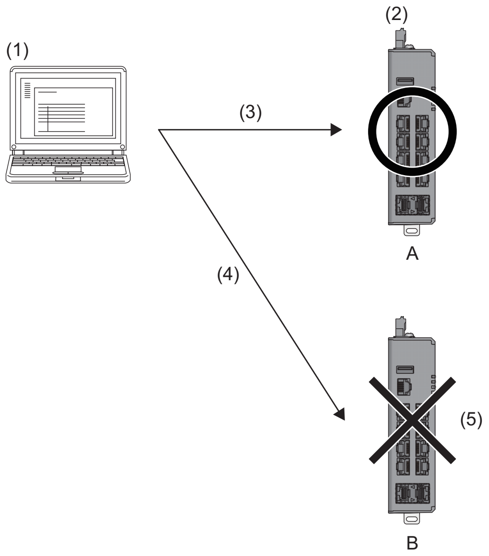
The managed switch supports SNMPv1, SNMPv2c, and SNMPv3. The following table lists the difference between the SNMP versions.

Version	Description
SNMPv1	Plain text authentication using the SNMP community string[*1]
SNMPv2c	
SNMPv3	Encrypted password authentication per user (MD5/SHA)

*1 The community string is a string used like a password for access from the manager to the agent.

Ex.

Plain text authentication using the SNMP community string



(1) Monitoring server (SNMP manager)
(2) Monitoring target device (SMP agent)
(3) SNMP (Community: public)
(4) SNMP (Community: test)
(5) Access cannot be made due to the community string being different.

Managed switch setting		
Item		**Setting value**
A, B	Read Community	public
	Read/Write Community	private

Setting method

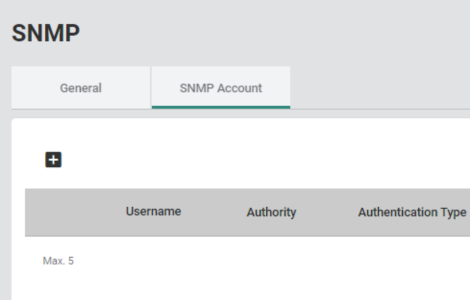
■SNMP account (Addition)

Operating procedure

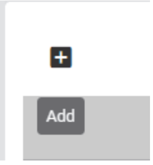
1. Start the operation from the "SNMP" window.

[Management] ⇨ [Network Management] ⇨ [SNMP]

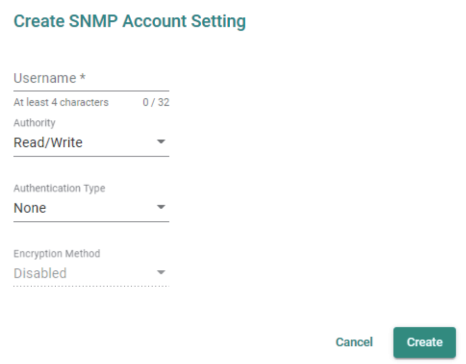
2. Select the [SNMP Account] tab.



3. Click the [Add] icon.



4. Set the required items.



Create SNMP Account Setting

Username *

At least 4 characters 0 / 32

Authority: Read/Write

Authentication Type: None

Encryption Method: Disabled

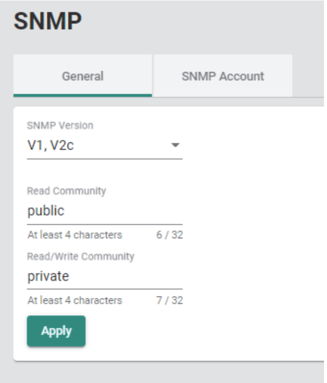
Item	Description	Setting range
Username	Input the user name.	4 to 32 characters (One-byte alphanumeric characters) (Default: empty)
Authority	Set the privilege. • Read/Write: The user has the read/write privilege. • Read Only: The user has only the read privilege.	• Read/Write • Read Only (Default: Read/Write)
Authentication Type	Set the authentication method. • None: The authentication method is disabled. • MD5: The authentication method is set to MD5. • SHA: The authentication method is set to SHA-1.	• None • MD5 • SHA (Default: None)
Authentication Password[*1]	Input the authentication password.	8 to 64 characters (One-byte alphanumeric characters) (Default: empty)
Encryption Method[*2]	Set the encryption method. • Disable: The encryption method is disabled. • DES: The DES encryption method is enabled. • AES: The AES encryption method is enabled.	• Disable • DES • AES (Default: Disable)
Encryption Key[*3]	Set the data encryption key.	8 to 64 characters (One-byte alphanumeric characters) (Default: empty)

*1 When "Authentication Type" is set to "None", this item is not displayed.
*2 When "Authentication Type" is set to "None", this item is fixed to Disable.
*3 When "Encryption Method" is set to "Disable", this item is not displayed.

5. Click the [Create] button.

6. Click the [General] tab.

7. Set the required items.



SNMP Version
V1, V2c

Read Community
public
At least 4 characters 6 / 32

Read/Write Community
private
At least 4 characters 7 / 32

Item	Description	Setting range
SNMP Version	Set the SNMP version. • V1, V2c, V3: The SNMP version is set to V1, V2c, and V3. • V1, V2c: The SNMP version is set to V1 and V2c. • V3 only: The SNMP version is set to V3.	• V1, V2c, V3 • V1, V2c • V3 only (Default: V1, V2c)
Read Community[*1]	Set the community string to allow the SNMP agent information to be read. The SNMP manager uses the community string for access.	4 to 32 characters (One-byte alphanumeric characters) (Default: public)
Read/Write Community[*1]	Set the community string to allow the SNMP agent information to be read/written. The SNMP manager uses the community string for access.	4 to 32 characters (One-byte alphanumeric characters) (Default: private)

*1 When "SNMP Version" is set to "V3 only", this item is not displayed.

8. Click the [Apply] button.

Precautions

- When "SNMP Version" is set to "V1, V2c, V3" or "V3 only", the SNMP Account needs to be set in advance.
- Up to five accounts can be created.

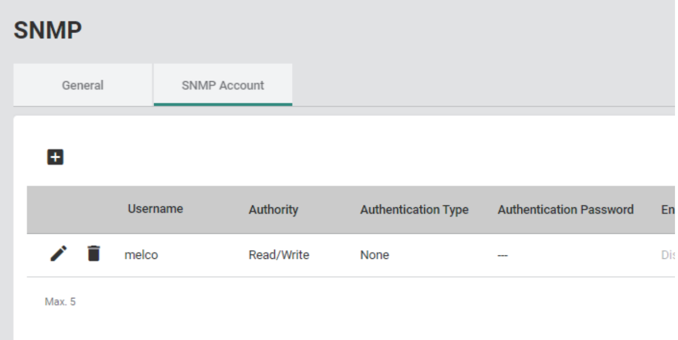
■SNMP account (Editing)

Operating procedure

1. Start the operation from the "SNMP" window.

[Management] ⇨ [Network Management] ⇨ [SNMP]

2. Select the [SNMP Account] tab.

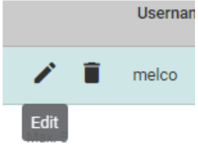


SNMP

	Username	Authority	Authentication Type	Authentication Password	En
	melco	Read/Write	None	---	Dis

Max. 5

3. Click the [Edit] icon of the item to be edited.



4. Edit the required items.

The content of each item is the same as that for the add operation.

5. Click the [Apply] button.

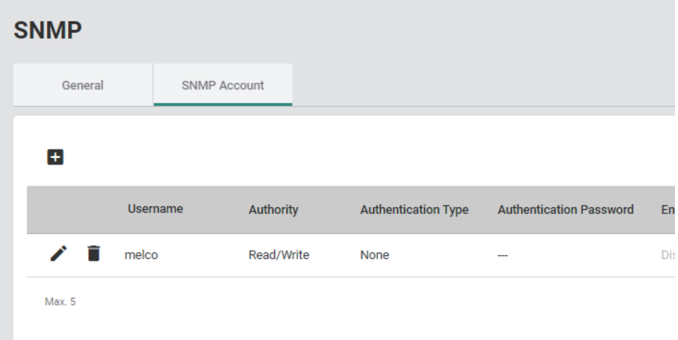
■SNMP account (Deletion)

Operating procedure

1. Start the operation from the "SNMP" window.

[Management] ⇨ [Network Management] ⇨ [SNMP]

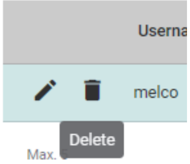
2. Select the [SNMP Account] tab.



	Username	Authority	Authentication Type	Authentication Password	En
	melco	Read/Write	None	---	Di

Max. 5

3. Click the [Delete] icon of the item to be deleted.



4. The confirmation dialog appears. Click the [Delete] button to perform deletion.

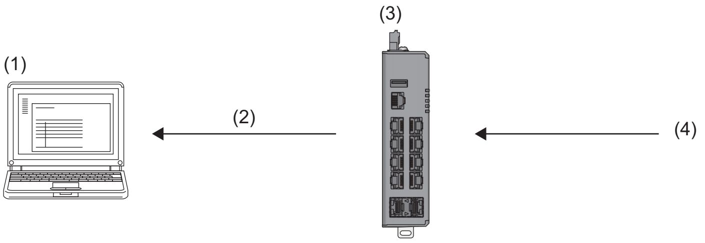
SNMP Trap/Inform

The SNMP agent has the following functions to notify the SNMP manager of event occurrence. The SNMP manager can receive notifications to keep track of changes in the system.

- Trap
- Inform

Trap

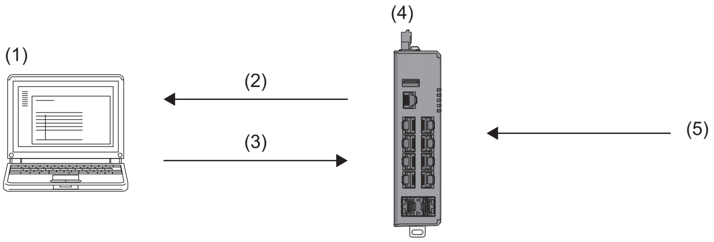
The SNMP agent does not request a response from the SNMP manager. Therefore, there is no way to check whether the notification has reached the SNMP manager.



(1) Monitoring server (SNMP manager)
(2) An event has occurred. (Event occurrence)
(3) Monitoring target (SNMP agent)
(4) Event occurrence

Inform

The SNMP agent requests a response from the SNMP manager. Therefore, it is possible to check whether the notification has reached the SNMP agent.



(1) Monitoring server (SNMP manager)
(2) An event has occurred. (Event occurrence)
(3) The notification has reached. (Response)
(4) Monitoring target (SNMP agent)
(5) Event occurrence

SNMP version

Version	Description
SNMP v1	• Trap function available • Inform function not available • Plain text authentication using the SNMP community string
SNMP v2c	• Trap function available • Inform function available • Plain text authentication using the SNMP community string
SNMP v3	• Trap function available • Inform function available • Encrypted password authentication per user (MD5/SHA)

Point

When SNMP Trap/Inform is used, "Registered Action" of the event notification function needs to include "Trap". (☞ Page 235 Event Notification [Event Notification])

Setting method

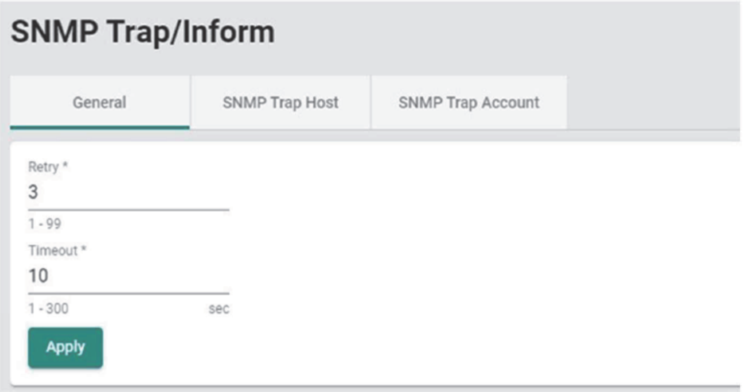
Operating procedure

1. Start the operation from the "SNMP Trap/Inform" window.

[Management] ⇨ [Network Management] ⇨ [SNMP Trap/Inform]

2. Select the [General] tab.

3. Set the required items.



Retry *
3
1 - 99
Timeout *
10
1 - 300 sec

Item	Description	Setting range
Retry	Input the retry count.	1 to 99 (Default: 3)
Timeout	Set the time up to the timeout.	1 to 300sec. (Default: 10)

4. Click the [Apply] button.

■SNMP Trap Host setting (Addition)

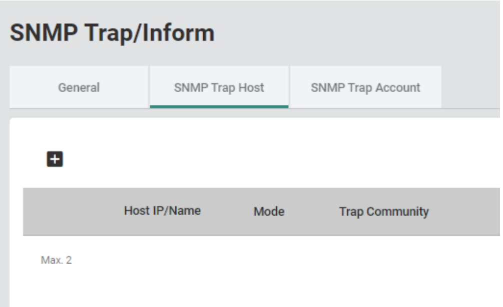
SNMP Trap Hosts are set from the SNMP manager.

Operating procedure

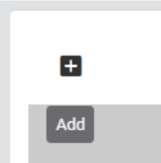
1. Start the operation from the "SNMP Trap/Inform" window.

[Management] ⇨ [Network Management] ⇨ [SNMP Trap/Inform]

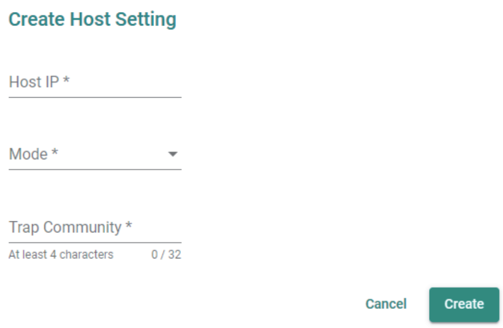
2. Select the [SNMP Trap Host] tab.



3. Click the [Add] icon.



4. Set the required items.



Item	Description	Setting range
Host IP	Input the IP address of the Trap server.	1 to 32 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Mode	Set the SNMP version. • Trap V1: The Trap function is enabled and the version SNMP v1 is used. • Trap V2c: The Trap function is enabled and the version SNMP v2c is used. • Inform V2c: The Inform function is enabled and the version SNMP v2c is used. • Trap V3: The Trap function is enabled and the version SNMP v3 is used. • Inform V3: The Inform function is enabled and the version SNMP v3 is used.	• Trap V1 • Trap V2c • Inform V2c • Trap V3 • Inform V3 (Default: empty)
Trap Community[*1]	Set the community string.	4 to 32 characters (One-byte alphanumeric characters) (Default: empty)

*1 When "Mode" is set to "Trap V3" or "Inform V3", this item is not displayed.

5. Click the [Create] button.

Precautions

- Up to two SNMP Trap Hosts can be created.
- When Mode is set to Trap V3 or Inform V3, the SNMP Trap Account needs to be set in advance.
- Some modes cannot be selected depending on the SNMP Version setting.

○: SNMP Trap Host can be created, ×: SNMP Trap Host cannot be created

Mode	SNMP Version		
	V1, V2c, V3	V1, V2c	V3 only
Trap V1	○	○	○
Trap V2c	○	○	○
Inform V2c	○	○	○
Trap V3	○	×	○
Inform V3	○	×	○

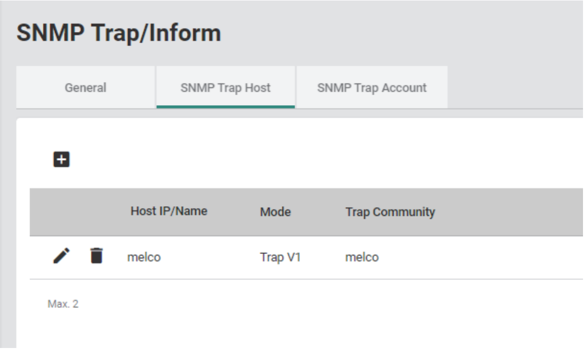
■SNMP Trap Host setting (Editing)

Operating procedure

1. Start the operation from the "SNMP Trap/Inform" window.

[Management] ⇨ [Network Management] ⇨ [SNMP Trap/Inform]

2. Select the [SNMP Trap Host] tab.

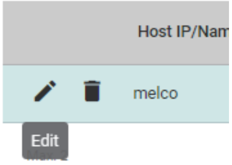


SNMP Trap/Inform

Host IP/Name	Mode	Trap Community
melco	Trap V1	melco

Max. 2

3. Click the [Edit] icon of the item to be edited.



4. Edit the required items.

The content of each item is the same as that for the add operation.

5. Click the [Apply] button.

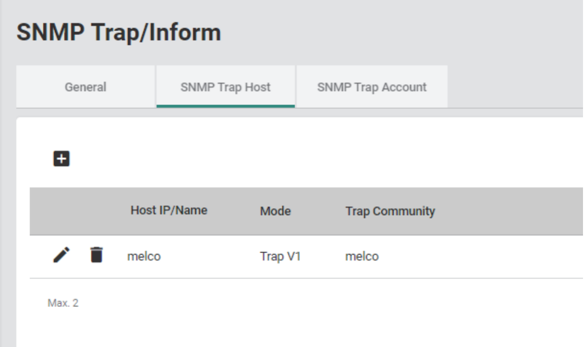
■SNMP Trap Host setting (Deletion)

Operating procedure

1. Start the operation from the "SNMP Trap/Inform" window.

[Management] ⇨ [Network Management] ⇨ [SNMP Trap/Inform]

2. Select the [SNMP Trap Host] tab.

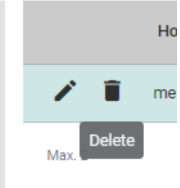


SNMP Trap/Inform

Host IP/Name	Mode	Trap Community
melco	Trap V1	melco

Max. 2

3. Click the [Delete] icon of the item to be deleted.



4. The confirmation dialog appears. Click the [Delete] button to perform deletion.

■SNMP Trap Account setting (Addition)

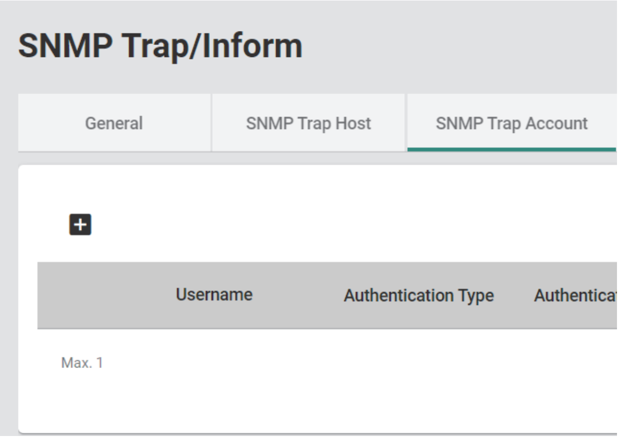
SNMP Trap Accounts are set from the SNMP agent.

Operating procedure

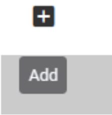
1. Start the operation from the "SNMP Trap/Inform" window.

[Management] ⇨ [Network Management] ⇨ [SNMP Trap/Inform]

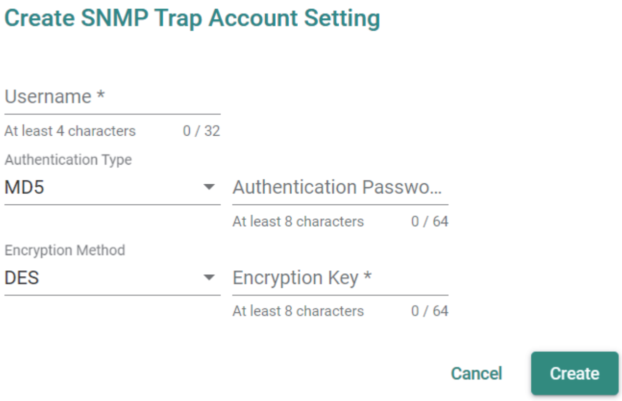
2. Select the [SNMP Trap Account] tab.


SNMP Trap/Inform

3. Click the [Add] icon.



4. Set the required items.



Create SNMP Trap Account Setting

Username *
At least 4 characters 0 / 32

Authentication Type
MD5

Authentication Passwo...
At least 8 characters 0 / 64

Encryption Method
DES

Encryption Key *
At least 8 characters 0 / 64

Item	Description	Setting range
Username	Input the user name.	4 to 32 characters (One-byte alphanumeric characters) (Default: empty)
Authentication Type	Select the authentication. • None: The authentication method is disabled. • MD5: The authentication method is set to MD5. • SHA: The authentication method is set to SHA-1.	• None • MD5 • SHA (Default: None)
Authentication Password[*1]	Input the authentication password.	8 to 64 characters (One-byte alphanumeric characters) (Default: empty)
Encryption Method[*2]	Set the encryption method. • Disable: The encryption method is disabled. • DES: The DES encryption method is enabled. • AES: The AES encryption method is enabled.	• Disable • DES • AES (Default: Disable)
Encryption Key[*3]	Set the data encryption key.	8 to 64 characters (One-byte alphanumeric characters) (Default: empty)

*1 When "Authentication Type" is set to "None", this item is not displayed.

*2 When "Authentication Type" is set to "None", this item is fixed to "Disable".

*3 When "Encryption Method" is set to "Disable", this item is not displayed.

5. Click the [Create] button.

Precautions

Only one SNMP Trap Account can be created.

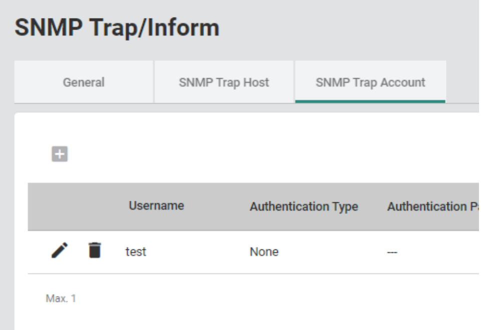
■SNMP Trap Account setting (Editing)

Operating procedure

1. Start the operation from the "SNMP Trap/Inform" window.

[Management] ⇨ [Network Management] ⇨ [SNMP Trap/Inform]

2. Select the [SNMP Trap Account] tab.

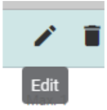


SNMP Trap/Inform

	Username	Authentication Type	Authentication P
	test	None	---

Max. 1

3. Click the [Edit] icon of the item to be edited.



4. Edit the required items.

The content of each item is the same as that for the add operation.

5. Click the [Apply] button.

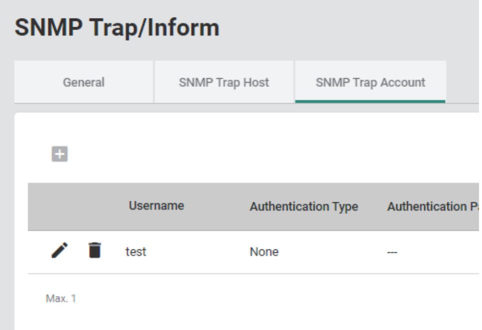
■SNMP Trap Account setting (Deletion)

Operating procedure

1. Start the operation from the "SNMP Trap/Inform" window.

[Management] ⇨ [Network Management] ⇨ [SNMP Trap/Inform]

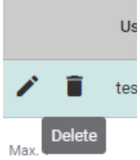
2. Select the [SNMP Trap Account] tab.



	Username	Authentication Type	Authentication P
	test	None	—

Max. 1

3. Click the [Delete] icon of the item to be deleted.



4. The confirmation dialog appears. Click the [Delete] button to perform deletion.

8.9 Device Security Function [Device Security]

The following functions can be used from the device security function [Device Security] displayed on the function menu of the web interface.

- Interface management function [Management Interface]
- Login policy [Login Policy]
- Access permitted function [Trusted Access]
- SSH
- SSL

Interface management function [Management Interface]

The interface management function can disable the following connection methods used to set the parameters of the managed switch. In addition, the TCP/UDP port number can be set according to the connected device. The number of concurrently connected modules to the managed switch can be limited.

- HTTP
- HTTPS
- Telnet
- SSH
- SNMP
- USB port

Point

For the connection methods, refer to the following.

- HTTP or HTTPS connection (☞ Page 56 Connection to the web interface)
- Telnet or SSH connection (☞ Page 67 CLI connection through the RS-232, Page 67 CLI connection through Telnet)

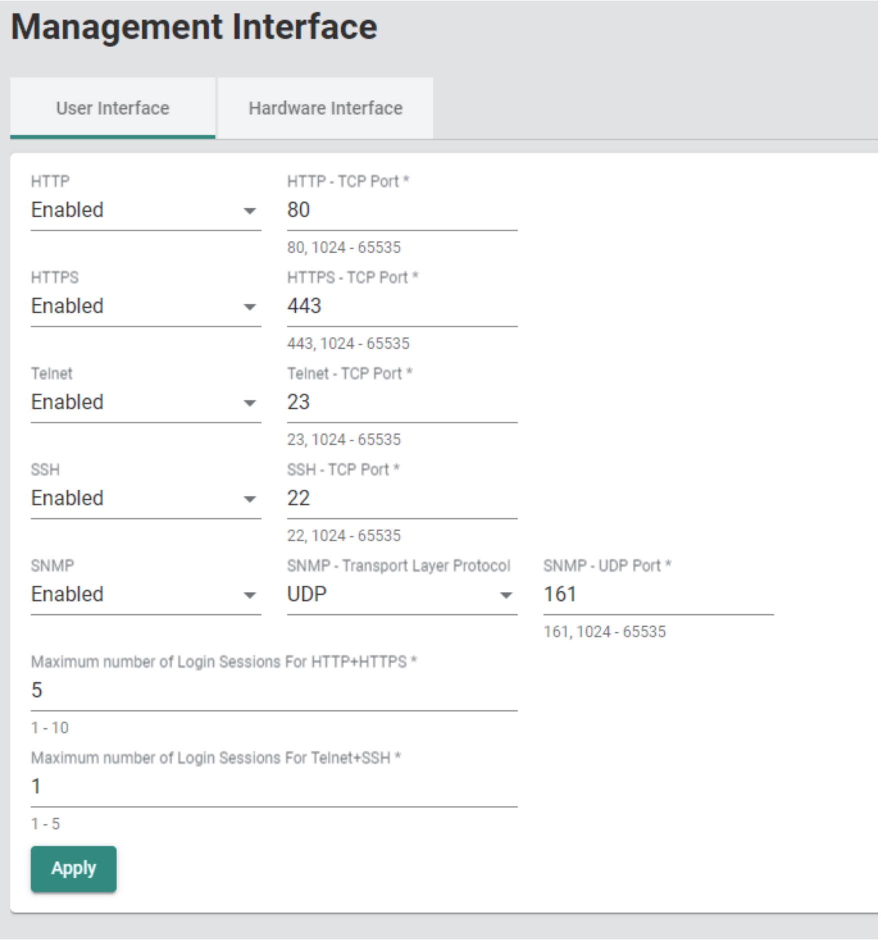
Setting method

Operating procedure

1. Start the operation from the "Management Interface" window.

[Security] ⇨ [Device Security] ⇨ [Management Interface]

2. Select the respective tabs and set the required items.



Management Interface

HTTP: Enabled

HTTP - TCP Port *: 80

80, 1024 - 65535

HTTPS: Enabled

HTTPS - TCP Port *: 443

443, 1024 - 65535

Telnet: Enabled

Telnet - TCP Port *: 23

23, 1024 - 65535

SSH: Enabled

SSH - TCP Port *: 22

22, 1024 - 65535

SNMP: Enabled

SNMP - Transport Layer Protocol: UDP

SNMP - UDP Port *: 161

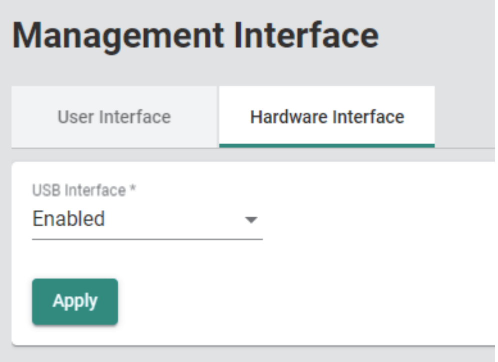
161, 1024 - 65535

Maximum number of Login Sessions For HTTP+HTTPS *: 5

1 - 10

Maximum number of Login Sessions For Telnet+SSH *: 1

1 - 5



USB Interface *
Enabled

Tab	Item	Description	Setting range
User Interface	HTTP	Enable or disable the HTTP connection. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
	HTTP-TCP Port	Set the HTTP connection port number.	• 80 • 1024 to 65535 (Default: 80)
	HTTPS	Enable or disable the HTTPS connection. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
	HTTPS-TCP-Port	Set the HTTPS connection port number.	• 443 • 1024 to 65535 (Default: 443)
	Telnet	Enable or disable the Telnet connection. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
	Telnet-TCP Port	Set the Telnet connection port number.	• 23 • 1024 to 65535 (Default: 23)
	SSH	Enable or disable the SSH connection. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
	SSH-TCP Port	Set the SSH connection port number.	• 22 • 1024 to 65535 (Default: 22)
	SNMP	Set the SNMP connection. • Enabled: Enable • Disabled: Disable • Read Only: Read only	• Enabled • Disabled • Read Only (Default: Enabled)
	SNMP-Transport Layer Protocol	Set the transmission protocol. • UDP: UDP is used as the transmission protocol. • TCP: TCP is used as the transmission protocol.	• UDP • TCP (Default: UDP)
	SNMP-UDP Port	Set the SNMP connection port number.	• 161 • 1024 to 65535 (Default: 161)
	Maximum number of Login Sessions For HTTP+HTTPS	Set the maximum number of sessions that can be logged in concurrently to the web interface with HTTP or HTTPS.	1 to 10 (Default: 5)
	Maximum number of Login Sessions For Telnet+SSH	Set the maximum number of sessions that can be logged in concurrently to CLI with Telnet or SSH.	1 to 5 (Default: 1)
Hardware Interface	USB Interface	Enables or disables the USB port. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)

3. Click the [Apply] button.

Precautions

Duplicated port numbers cannot be set.

Login policy [Login Policy]

The following settings can be configured for the login policy to improve the security of the managed switch.

- Login message
- Lockout
- Auto-logout time

Login message

A message to be displayed on the login window and a login-failure message can be set.

Lockout

If the password authentication fails a certain number of times, the password authentication is denied (locked out) for a certain period of time. This prevents brute force attacks by unauthorized users.

Auto-logout time

The time from the last web browser operation to auto-logout can be set.

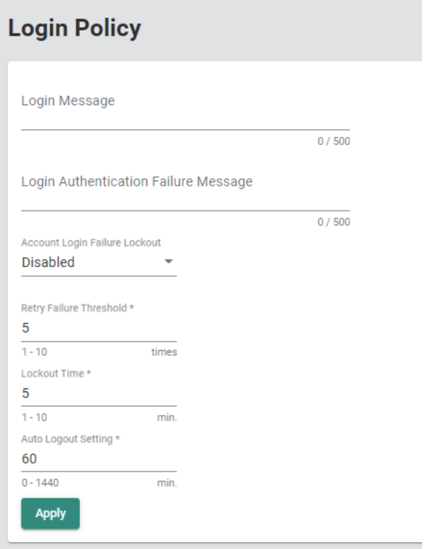
Setting method

Operating procedure

1. Start the operation from the "Login Policy" window.

[Security] ⇨ [Device Security] ⇨ [Login Policy]

2. Set the required items.



Login Policy

Login Message

0 / 500

Login Authentication Failure Message

0 / 500

Account Login Failure Lockout: Disabled

Retry Failure Threshold *: 5 (1 - 10 times)

Lockout Time *: 5 (1 - 10 min.)

Auto Logout Setting *: 60 (0 - 1440 min.)

Item	Description	Setting range
Login Message	Set the message to be displayed at login.	0 to 500 (characters) (Default: empty)
Login Authentication Failure Message	Set the message to be displayed at login-failure.	0 to 500 (characters) (Default: empty)
Account Login Failure Lockout	Enable or disable the lockout function at login-failure. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)
Retry Failure Threshold	Set the maximum value of the retry count.	1 to 10 (Default: 5)
Lockout Time	Set the time to be locked out before login can be attempted again.	1 to 10 (Default: 5)
Auto Logout Setting	Set the time until auto-logout. If this item is set to 0, auto-logout is disabled.	0 to 1440 (Default: 5)

3. Click the [Apply] button.

Access permitted function [Trusted Access]

The IP address for which access to the managed switch is permitted can be set to prevent access from unauthorized IP addresses.

Point

When access to the managed switch is denied due to the access permitted setting, follow any of the following methods.

- Access using the console cable
- Initialization of the managed switch (Press and hold the reset button for five seconds.)

Setting method

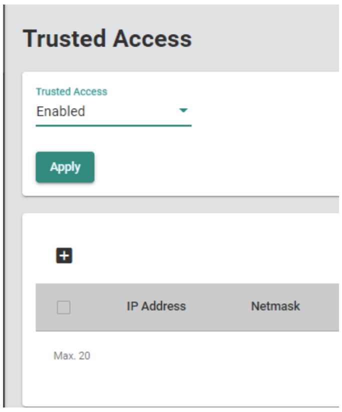
■Setting an IP address

Operating procedure

1. Start the operation from the "Trusted Access" window.

[Security] ⇨ [Device Security] ⇨ [Trusted Access]

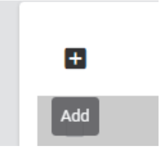
2. Set "Trusted Access" to "Enabled".



Trusted Access

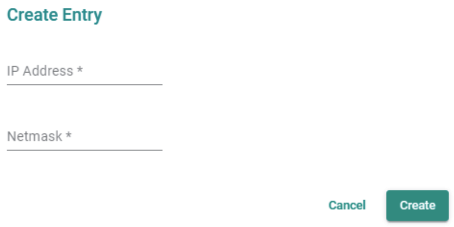
Trusted Access: Enabled

3. Click the [Add] icon.



4. Set the required items.

Before clicking the [Create] button, the IP address for which connection is to be permitted needs to be set.



Item	Description	Setting range
IP Address	Set the IP address for which connection to the managed switch is to be permitted.	0.0.0.0 to 255.255.255.254 (Default: empty)
Netmask	Set the netmask for which connection to the managed switch is to be permitted.	0.0.0.0 to 255.255.255.255 (Default: empty)

5. Click the [Create] button.

Point

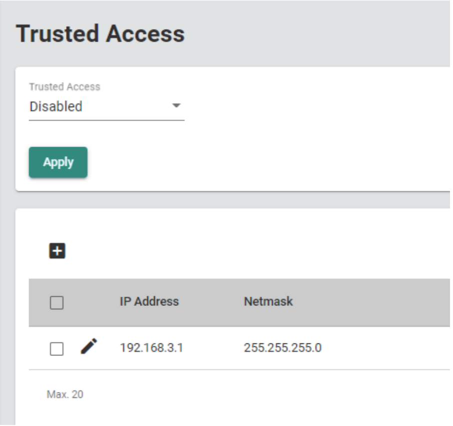
Up to 20 addresses can be set.

■Editing an IP address

Operating procedure

1. Start the operation from the "Trusted Access" window.

[Security] ⇨ [Device Security] ⇨ [Trusted Access]

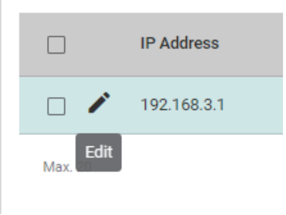

Trusted Access

Trusted Access: Disabled

□	IP Address	Netmask
□	192.168.3.1	255.255.255.0

Max. 20

2. Click the [Edit] icon of the IP address to be edited.



3. Edit the required items.

The content of each item is the same as that for the add operation.

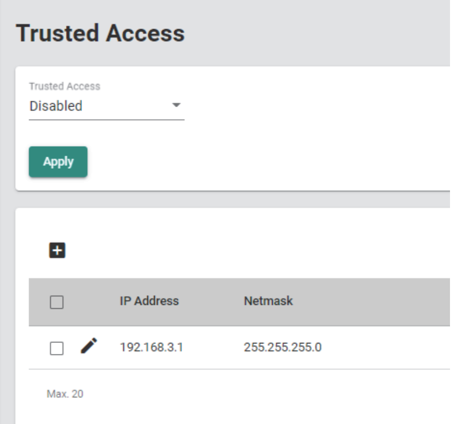
4. Click the [Apply] button.

■Deleting

Operating procedure

1. Start the operation from the "Trusted Access" window.

[Security] ⇨ [Device Security] ⇨ [Trusted Access]



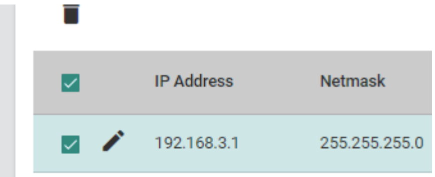
Trusted Access

Trusted Access: Disabled

□	IP Address	Netmask
□	192.168.3.1	255.255.255.0

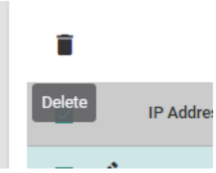
Max. 20

2. Select the checkbox of one or more lists to be deleted.



☑	IP Address	Netmask
☑	192.168.3.1	255.255.255.0

3. Click the [Delete] icon.

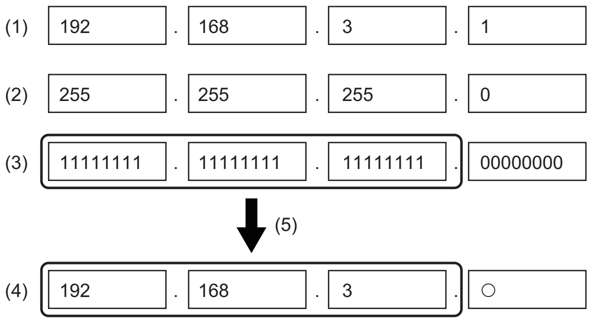


4. The confirmation dialog appears. Click the [Delete] button to perform deletion.

Setting example

Ex.

When 192.168.3.0 to 192.168.3.255 are set as the permission range of IP addresses



(1)	192	168	3	1
(2)	255	255	255	0
(3)	11111111	11111111	11111111	00000000
(4)	192	168	3	○

○: 0 to 255

(1) IP address

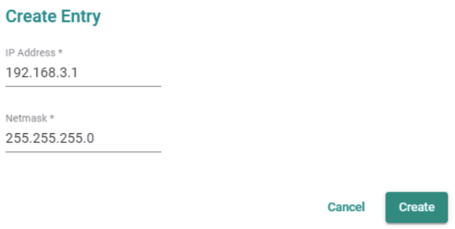
(2) Netmask

(3) Netmask (expressed in bits)

(4) IP address to be permitted

(5) The portion in the netmask where the bit is 1 indicates the fixed value of the IP address to be permitted.

The IP addresses are set as follows.



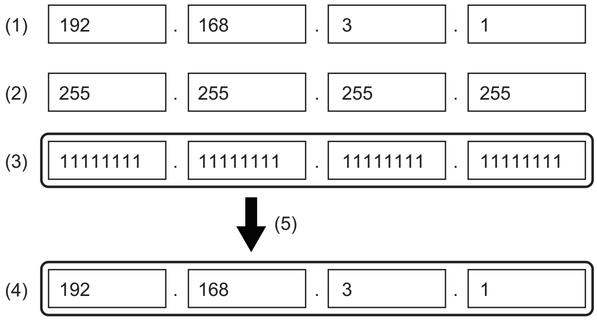
Create Entry

IP Address * 192.168.3.1

Netmask * 255.255.255.0

Ex.

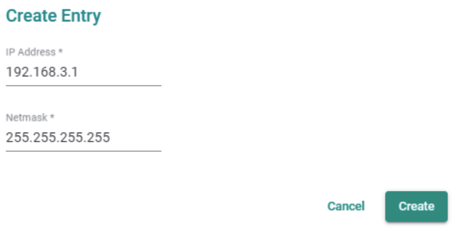
When only 192.168.3.1 is set as the permission range of IP addresses



(1)	192	168	3	1
(2)	255	255	255	255
(3)	11111111	11111111	11111111	11111111
(4)	192	168	3	1

(1) IP address
(2) Netmask
(3) Netmask (expressed in bits)
(4) IP address to be permitted
(5) The portion in the netmask where the bit is 1 indicates the fixed value of the IP address to be permitted.

The IP addresses are set as follows.



Create Entry

IP Address *
192.168.3.1

Netmask *
255.255.255.255

SSH

The managed switch supports connection to CLI via SSH encrypted communication. Also, the key to be used for SSH encryption can be regenerated.

CLI connection procedure via SSH

Connection to CLI can be performed in the same way as Telnet. (☞ Page 67 CLI connection through Telnet)

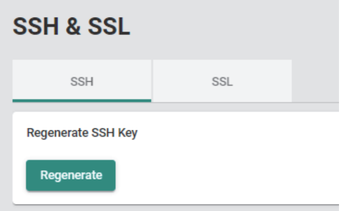
Key regeneration

Operating procedure

1. Start the operation from the "SSH&SSL" window.

🖱 [Security] ⇨ [Device Security] ⇨ [SSH&SSL]

2. Select the [SSH] tab.



3. Click the [Regenerate] button.

SSL

The managed switch supports SSL communication (encrypted communication) and can connect to the web interface using HTTPS. The managed switch can also output the CSR, regenerate the SSL server certificate, and import the SSL server certificate.

Connection to the web interface using HTTPS

Connection to the web interface can be performed in the same way as HTTP. (☞ Page 56 Connection to the web interface)

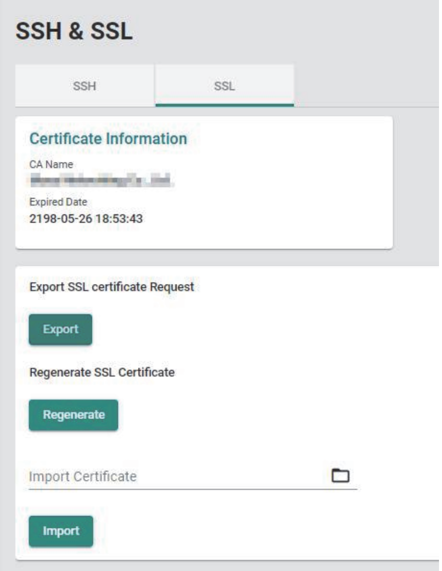
Outputting the CSR

Operating procedure

1. Start the operation from the "SSH&SSL" window.

[Security] ⇨ [Device Security] ⇨ [SSH&SSL]

2. Select the [SSL] tab.



SSH & SSL

Certificate Information

CA Name
[redacted]

Expired Date
2198-05-26 18:53:43

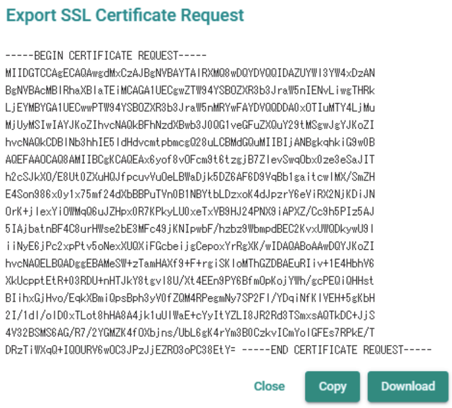
Export SSL certificate Request

Regenerate SSL Certificate

Import Certificate

3. Click the [Export] button.

4. To copy the CSR to the clipboard, click the [Copy] button. To output as the CSR file (*.csr), click the [Download] button.



Export SSL Certificate Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDGTCCAgECAQAwgdMxCzAJBgNVBAYTAlRXMQ8wDQYDVQQIDAZUYWl3YW4xDzAN
BgNVBAcMBlRhaXBlaTEiMCAGA1UECgwZTW94YSBOZXR3b3JraW5nIENvLiwgTHRk
LjEYMBYGA1UECwwPTW94YSBOZXR3b3JraW5nMRYwFAYDVQQDDA0xOTIuMTY4LjMu
MjUyMSIwIAYJKoZIhvcNAQkBFhNzdXBwb3J0QG1veGFuZXQuY29tMSgwJgYJKoZI
hvcNAQkCDBlNb3hhIE5ldHdvcmtpbmcgQ28uLCBMdGQuMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAx6yof8vOFcm9t6tzgjB7ZlevSwqObx0ze3eSaJIT
h2cSJkXO/E8Ut0ZXuHQJfpcuvVu0eLBWaDjk5DZ6AF6D9VqBb1gaitcwlMX/SmZH
E4Son986x0y1x75mf24dXbBBPuTVn0B1NBYtbLDzxoK4dJpzrY6eViRX2NjKDiJN
OrK+jlexYiOWMqQ6uJZHpx0R7KPkyLU0xeTxVB9HJ24PNX9iAPXZ/Cc9h5PIz5AJ
5IAjbatnBF4C8urHWse2bE3MFc49jKNIpwbF/hzbz9WbmpdBEC2KvxUWQDkywU9l
iiNyE6jPc2xpPtv5oNexXUQXiFGcbeijgCepoxYrRgXK/wIDAQABoAAwDQYJKoZI
hvcNAQELBQADggEBAMeSW+zTamHAXf9+F+rgiSKloMThGZDBAEuRIiv+1E4HbhV6
XkUcpptEtR+03RDU+nHTJkY8tgvl8U/Xt4EEn9PY6BfmOpKojYWh/gcPEQiQHHst
BIihxGjHvo/EqkXBmiQpsBph3yV0fZQM4RPegmNy7SP2Fl/YDqiNfKlVEH+5gKbH
2I/1dl/olD0xTLot8hHA8A4jk1uUlWaE+cYyItYZLI8JR2Rd3TSmxsAQTkDC+JjS
4V32BSMS6AG/R7/2YGMZK4fOXbjns/UbL6gK4rYm3B0CzkvICmYolGFEs7RPkE/T
DRzTiWXqQ+IQOURV6wOC3JPzJjEZRO3oPC38EtY= -----END CERTIFICATE REQUEST-----
```

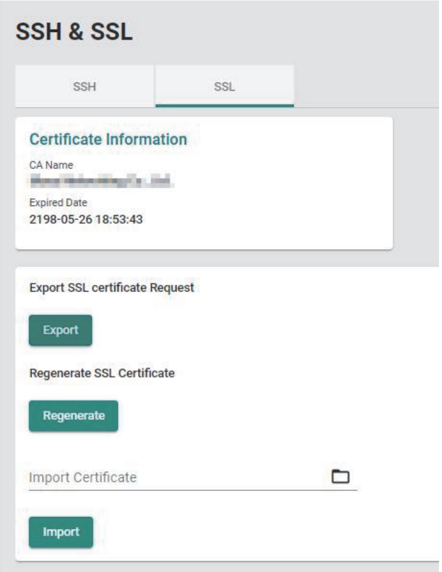
Regenerating the SSL server certificate

Operating procedure

1. Start the operation from the "SSH&SSL" window.

[Security] ⇨ [Device Security] ⇨ [SSH&SSL]

2. Select the [SSL] tab.



Certificate Information

CA Name
[redacted]

Expired Date
2198-05-26 18:53:43

Export SSL certificate Request

Regenerate SSL Certificate

Import Certificate

3. Click the [Regenerate] button.

Precautions

When the SSL server certificate is regenerated, the CSRs that have been output before cannot be used.

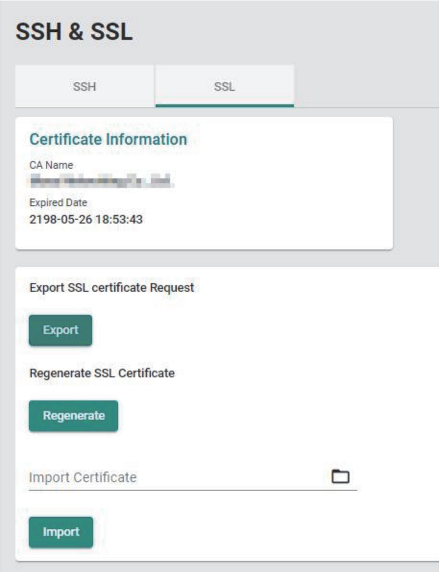
Importing the SSL server certificate

Operating procedure

1. Start the operation from the "SSH&SSL" window.

[Security] ⇨ [Device Security] ⇨ [SSH&SSL]

2. Select the [SSL] tab.



SSH & SSL

Certificate Information

CA Name

[redacted]

Expired Date

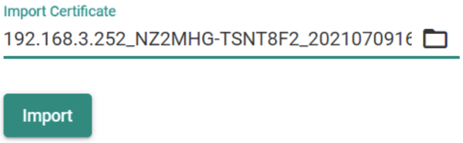
2198-05-26 18:53:43

Export SSL certificate Request

Regenerate SSL Certificate

Import Certificate

3. Set the SSL server certificate to be imported to "Import Certificate".



Import Certificate

192.168.3.252_NZ2MHG-TSNT8F2_2021070916

4. Click the [Import] button.

Precautions

Create the SSL server certificate to be imported to the managed switch by affixing a signature by the superior certificate to a CSR output from the managed switch.

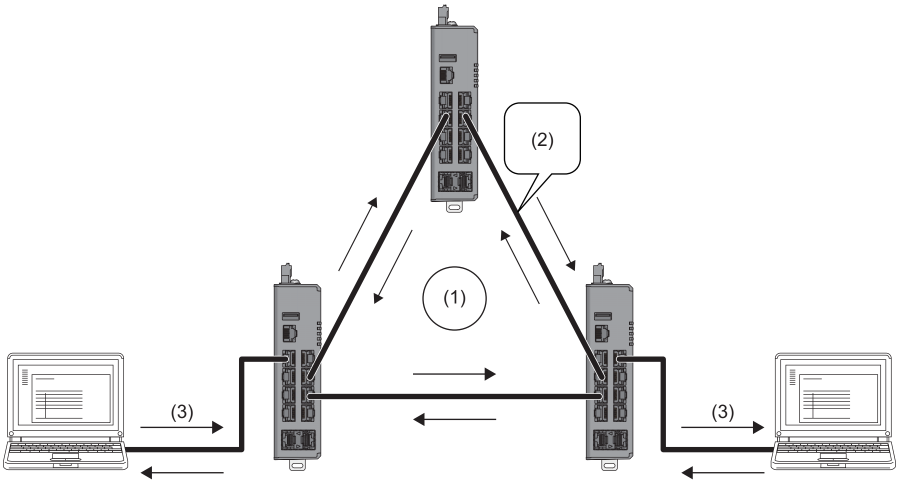
8.10 Network Security Function [Network Security]

The following function can be used from the network security function [Network Security] displayed on the function menu of the web interface.

- Traffic control function [Traffic Storm Control]

Traffic control function [Traffic Storm Control]

Frames are discarded when specific traffic to be received exceeds the threshold value. When a redundant protocol connects invalid devices to each other, an unintended loop may be formed and the network may become overloaded. In such a case, the traffic control function limits the reception of broadcast frames and multicast frames that cause the problem to reduce the network load.



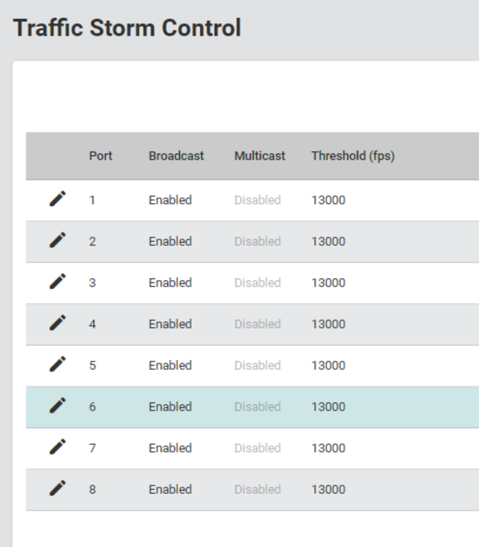
(1) Network failure (broadcast storm) occurrence
(2) Loop formation
(3) Data transmission

Setting method

Operating procedure

1. Start the operation from the "Traffic Storm Control" window.

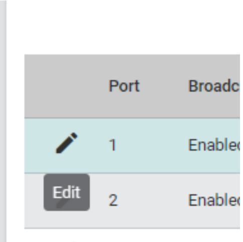
[Security] ⇨ [Network Security] ⇨ [Traffic Storm Control]



Traffic Storm Control

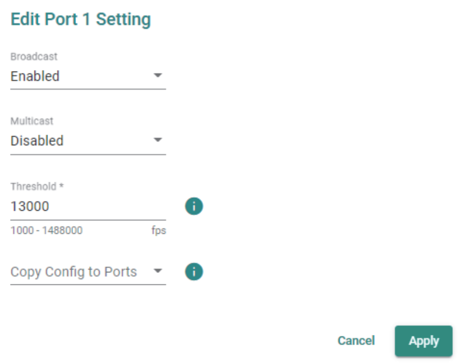
	Port	Broadcast	Multicast	Threshold (fps)
✎	1	Enabled	Disabled	13000
✎	2	Enabled	Disabled	13000
✎	3	Enabled	Disabled	13000
✎	4	Enabled	Disabled	13000
✎	5	Enabled	Disabled	13000
✎	6	Enabled	Disabled	13000
✎	7	Enabled	Disabled	13000
✎	8	Enabled	Disabled	13000

2. Click the [Edit] icon of the port to be edited.



	Port	Broadc
✎	1	Enable
Edit	2	Enable

3. Set the required items.



Edit Port 1 Setting

Broadcast: Enabled

Multicast: Disabled

Threshold *: 13000 (1000 - 1488000 fps)

Copy Config to Ports

Item	Description	Setting range
Broadcast	Enable or disable the send/receive limitation of broadcast frames. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Multicast	Enable or disable the send/receive limitation of multicast frames. • Enabled: Enable • Disabled: Disable	• Enabled: • Disabled (Default: Disabled)
Threshold	Set the threshold value by which to limit traffic. The frames to be received are limited to the set threshold value or less.	1000 to 1488000 (Default: 13000)

Item	Description	Setting range
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Ports • 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: empty)

*1 This item is not displayed for the NZ2MHG-TSNT4.

4. Click the [Apply] button.

Point

- For the port by which communication is to be performed at the communication speed of 100Mbps, set "Threshold" to 1300.
- When the multicast mode is to be used for communication via the CC-Link IE TSN connection, set "Multicast" to "Disabled".

8.11 Authentication Method [Authentication]

The following functions can be used from the authentication method [Authentication] displayed on the function menu of the web interface.

- Login authentication method [Login Authentication]
- RADIUS
- TACACS+

Login authentication method [Login Authentication]

The managed switch adopts user login authentication that uses the local database, RADIUS (Remote Authentication Dial In User Service), or TACACS+ (Terminal Access Controller Access-Control System Plus).

- Local database: Login authentication is performed with the user name and password registered in the user account settings. (☞ Page 97 Account Management [Account Management])
- RADIUS: Login authentication between the authentication client (managed switch) and the server is performed with the connection destination IP address and key. (☞ Page 220 RADIUS)
- TACACS+: The same as RADIUS (☞ Page 223 TACACS+)

RADIUS and TACACS+ centrally manage the "AAA" (Authentication, Authorization, and Accounting) system for connecting to network services. The account can be effectively and safely managed by using RADIUS or TACACS+.

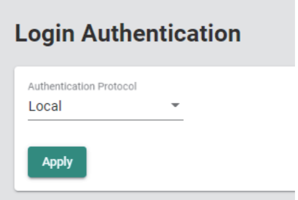
Setting procedure

Operating procedure

1. Start the operation from the "Login Authentication" window.

[Security] ⇨ [Authentication] ⇨ [Login Authentication]

2. Set the Authentication Protocol.


Login Authentication

Authentication Protocol: Local

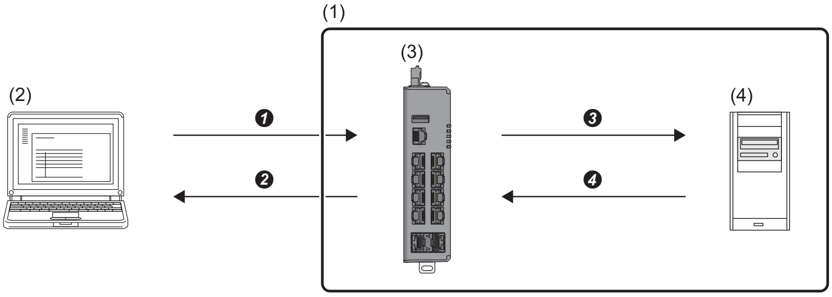
Item	Description	Setting range
Authentication Protocol	Select the login authentication method. ■Local Only the local database is checked. ■RADIUS Only RADIUS is checked. ■TACACS+ Only TACACS+ is checked. ■RADIUS, Local • When the RADIUS server is running and the managed switch can be connected to the RADIUS server, RADIUS is checked. • When the RADIUS server is disabled and the managed switch cannot be connected to the RADIUS server, the local database is checked. ■TACACS+, Local • When the TACACS server is running and the managed switch can be connected to the TACACS server, TACACS+ is checked. • When the TACACS server is disabled and the managed switch cannot be connected to the TACACS server, the local database is checked.	• Local • RADIUS • TACACS+ • RADIUS, Local • TACACS+, Local (Default: Local)

3. Click the [Apply] button.

RADIUS

RADIUS (Remote Authentication Dial In User Service) authentication can prevent unauthorized access by setting the connection destination IP address and key in advance between the authentication client and the server. Also, the following three authentication types are supported.

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)
- MSCHAP v1



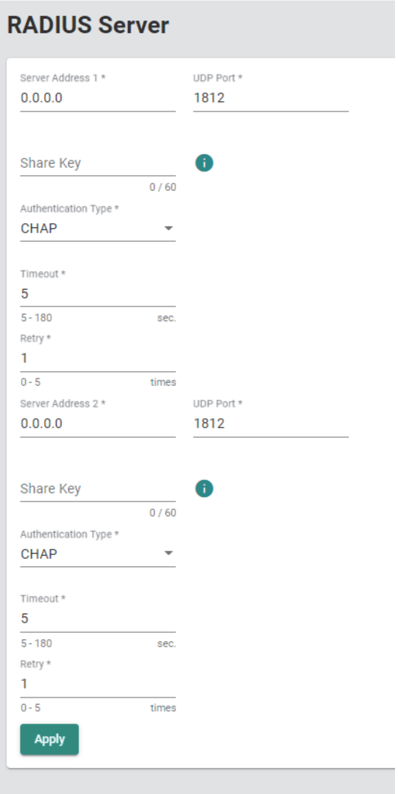
❶ Connection request
❷ Authentication or certification request
❸ Notification of result
❹ Execution of process
(1) RADIUS authentication
(2) Connection requesting device
(3) Client: 10.1.1.100, IP address of the authentication server: 10.1.1.253, Share key: ****
(4) Server: 10.1.1.253, IP address of the authentication client: 10.1.1.100, Share key: ****

Setting procedure

Operating procedure

1. Start the operation from the "RADIUS Server" window.

[Security] ⇨ [Authentication] ⇨ [RADIUS]



RADIUS Server

Server Address 1 * 0.0.0.0

UDP Port * 1812

Share Key 0 / 60

Authentication Type * CHAP

Timeout * 5 (5 - 180 sec.)

Retry * 1 (0 - 5 times)

Server Address 2 * 0.0.0.0

UDP Port * 1812

Share Key 0 / 60

Authentication Type * CHAP

Timeout * 5 (5 - 180 sec.)

Retry * 1 (0 - 5 times)

Item	Description	Setting range
Server Address1	Input the IP address of authentication server 1.	0.0.0.0 to 255.255.255.254 (Default: 0.0.0.0)
UDP Port	Specify the UDP port number of server 1.	1 to 65535 (Default: 1812)
Share Key	Input the shared key for server 1 authentication.	0 to 60 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Authentication Type	Select the authentication type for server 1.	• PAP • CHAP • MSCHAP v1 (Default: CHAP)
Timeout	Input the time to wait for the response from server 1.	5 to 180 (Default: 5)
Retry	Input the retry count for reconnecting to server 1.	0 to 5 (Default: 1)
Server Address2	Input the IP address of authentication server 2.	0.0.0.0 to 255.255.255.254 (Default: 0.0.0.0)
UDP Port	Specify the UDP port number of server 2.	1 to 65535 (Default: 1812)
Share Key	Input the shared key for server 2 authentication.	0 to 60 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Authentication Type	Select the authentication type for server 2.	• PAP • CHAP • MSCHAP v1 (Default: CHAP)
Timeout	Input the time to wait for the response from server 2.	5 to 180 (Default: 5)

Item	Description	Setting range
Retry	Input the retry count for reconnecting to server 2.	0 to 5 (Default: 1)

2. Click the [Apply] button.

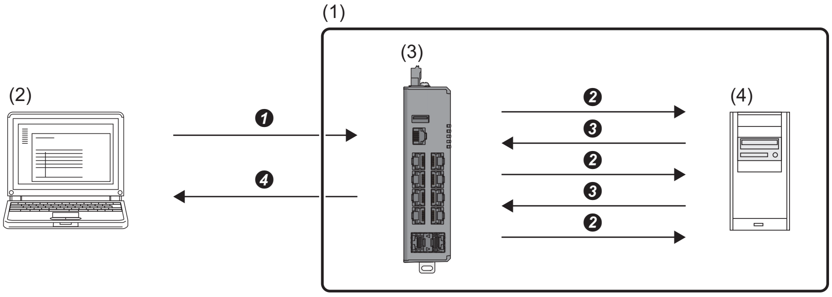
Point

In RADIUS, authentication is executed for server 1 first, and if this fails, authentication is executed for server 2.

TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) is characterized by the fact that the authentication service and the certification service are separated. Conversely, they are integrated in RADIUS. This allows authentication and certification to be used separately. Also, the following three authentication types are supported.

- ASCII
- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)



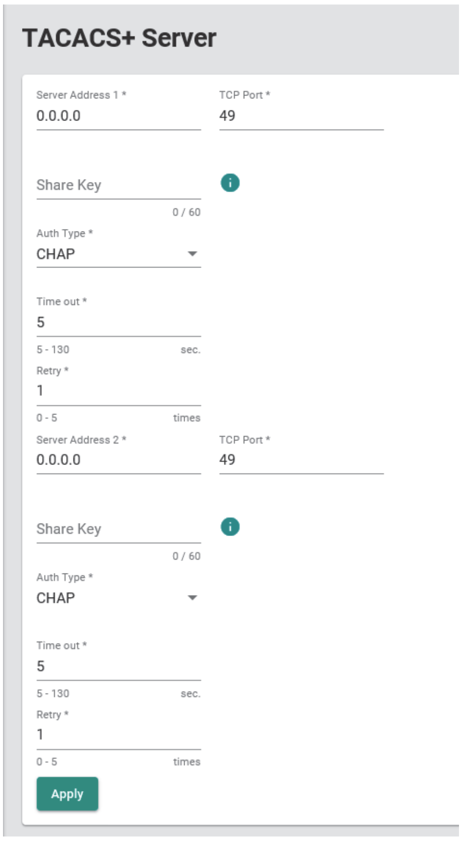
❶ Connection request
❷ Authentication, certification, or accounting
❸ Notification of result
❹ Execution of process
(1) TACACS+ authentication
(2) Connection requesting device
(3) Client: 10.1.1.100, IP address of the authentication server: 10.1.1.253, Share key: ****
(4) Server: 10.1.1.253, IP address of the authentication client: 10.1.1.100, Share key: ****

Setting procedure

Operating procedure

1. Start the operation from the "TACACS+ Server" window.

[Security] ⇨ [Authentication] ⇨ [TACACS+]



TACACS+ Server

Server Address 1 *: 0.0.0.0

TCP Port *: 49

Share Key: 0 / 60

Auth Type *: CHAP

Time out *: 5 (5 - 130 sec.)

Retry *: 1 (0 - 5 times)

Server Address 2 *: 0.0.0.0

TCP Port *: 49

Share Key: 0 / 60

Auth Type *: CHAP

Time out *: 5 (5 - 130 sec.)

Retry *: 1 (0 - 5 times)

Item	Description	Setting range
Server Address1	Input the IP address of authentication server 1.	0.0.0.0 to 255.255.255.254 (Default: 0.0.0.0)
TCP Port	Specify the TCP port number of server 1.	1 to 65535 (Default: 49)
Share Key	Input the shared key for server 1 authentication. When the parameter setting window is closed or updated, the shared key is automatically cleared to enhance security.	0 to 60 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Auth Type	Select the authentication type for server 1.	• ASCII • PAP • CHAP (Default: CHAP)
Timeout	Input the time to wait for the response from server 1.	5 to 130 (Default: 5)
Retry	Input the retry count for reconnecting to server 1.	0 to 5 (Default: 1)
Server Address2	Input the IP address of authentication server 2.	0.0.0.0 to 255.255.255.254 (Default: 0.0.0.0)
TCP Port	Specify the TCP port number of server 2.	1 to 65535 (Default: 49)
Share Key	Input the shared key for server 2 authentication. When the parameter setting window is closed or updated, the shared key is automatically cleared to enhance security.	0 to 60 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Auth Type	Select the authentication type for server 2.	• ASCII • PAP • CHAP (Default: CHAP)

Item	Description	Setting range
Timeout	Input the time to wait for the response from server 2.	5 to 130 (Default: 5)
Retry	Input the retry count for reconnecting to server 2.	0 to 5 (Default: 1)

2. Click the [Apply] button.

Point

In TACACS+, authentication is executed for server 1 first, and if this fails, authentication is executed for server 2.

8.12 System Status Check [System Status]

The following functions can be used from the system status check [System Status] displayed on the function menu of the web interface.

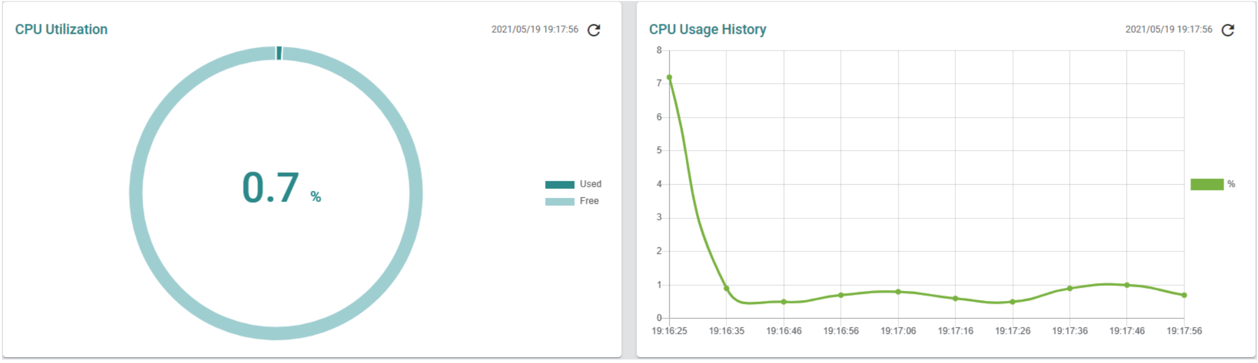
- System utilization [Utilization]
- Statistical information [Statistics]

System utilization [Utilization]

The following system information of the managed switch is displayed graphically.

- CPU utilization
- Memory usage
- Power consumption history

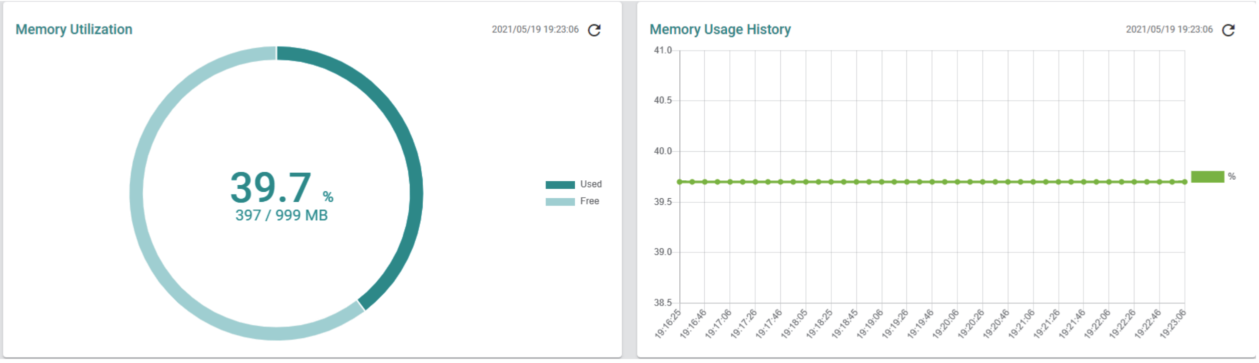
CPU utilization



Vertical axis: CPU utilization [%]

Horizontal axis: Web browser time at information acquisition

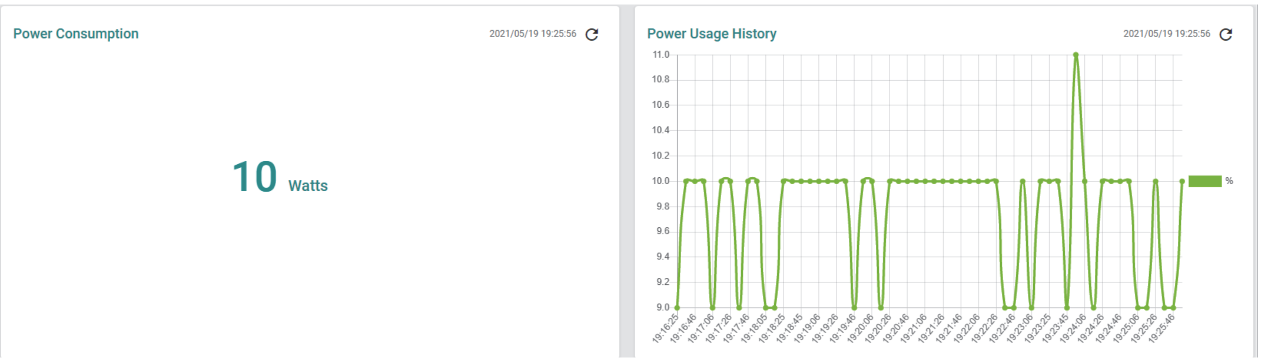
Memory usage



Vertical axis: Memory utilization [%]

Horizontal axis: Web browser time at information acquisition

Power consumption history



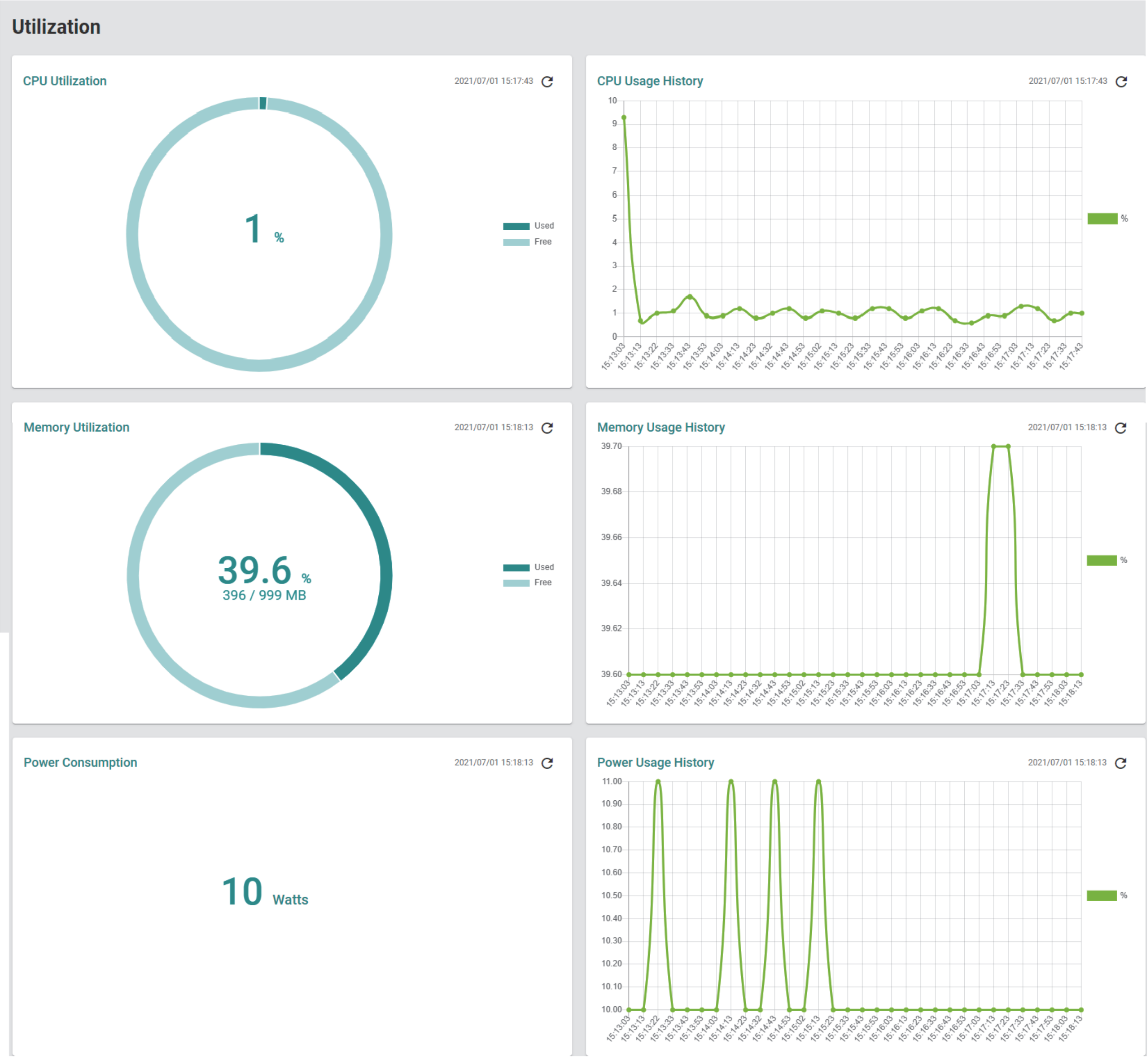
Vertical axis: Power consumption [W]
Horizontal axis: Web browser time at data acquisition

Display method

Operating procedure

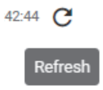
1. Start the operation from the "Utilization" window.

[Diagnostics] ⇨ [System Status] ⇨ [Utilization]



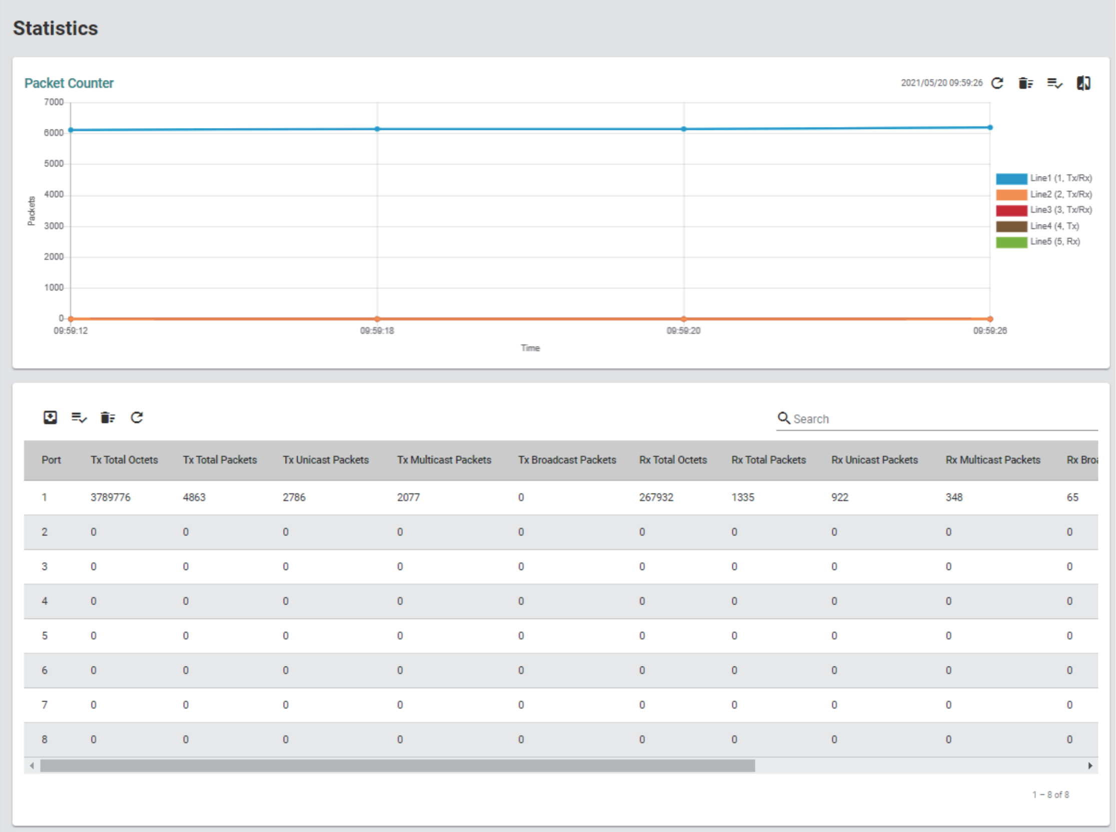
Point

Click the [Refresh] icon to update the display to the latest information.



Statistical information [Statistics]

The statistical information of data communication can be displayed per port. The statistical information is displayed in graph format (at the upper part of the window) and in table format (at the lower part of the window). Also, the statistical information of the respective ports can be compared.



Port	Tx Total Octets	Tx Total Packets	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Rx Total Octets	Rx Total Packets	Rx Unicast Packets	Rx Multicast Packets	Rx Bro
1	3789776	4863	2786	2077	0	267932	1335	922	348	65
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0

Graph area

In the graph area, the packet transmission information of the selected port is displayed graphically. The information is displayed in the following display modes.

- Packet counter
- Band utilization

The status of each port is displayed in a different color. Up to five pieces of port information can be displayed.

Point

- Data collection starts after the statistical information is displayed on the window.
- In the graph area, data is collected at intervals of approximately 10 seconds before being reflected on the window. In addition, when the display window is switched, the accumulated data is discarded.

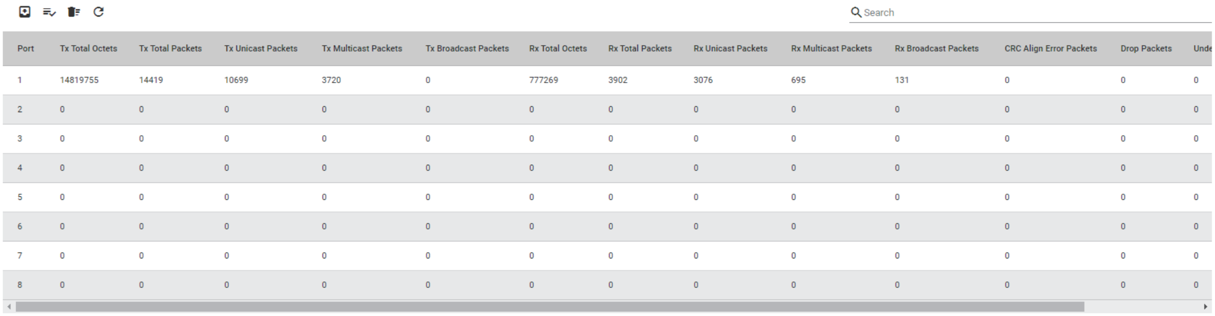
■Graph area icon

Item	Name	Description
↻	Update [Refresh]	Acquires the latest information and updates the graph area.
🗑	Graph reset [Reset]	Clears the accumulated data and updates the graph area.*1
≡✓	Display setting [Display Setting]	Set the statistical information to be displayed.
◧	Data comparison [Data Comparison]	Select the data to be compared.*1

*1 When the display mode is set to show band utilization, this item is not displayed.

Table area

In the table area, the detailed packet transmission information is displayed for each port.



Search

Port	Tx Total Octets	Tx Total Packets	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Rx Total Octets	Rx Total Packets	Rx Unicast Packets	Rx Multicast Packets	Rx Broadcast Packets	CRC Align Error Packets	Drop Packets	Unde
1	14819755	14419	10699	3720	0	777269	3902	3076	695	131	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0

Item	Description
Port	Port number
Tx Total Octets	Shows the total number of octets for transmission data.[*1] Preamble and SFD are not included.
Tx Total Packets	Shows the number of packets sent.
Tx Unicast Packets	Shows the number of unicast packets sent.
Tx Multicast Packet	Shows the number of multicast packets sent.
Tx Broadcast Packets	Shows the number of broadcast packets that were normally sent. Multicast packets are not included.
Rx Total Octets	Shows the total number of octets for receive data.[*1] Preamble and SFD are not included.
Rx Total Packets	Shows the number of packets received.
Rx Unicast Packets	Shows the number of unicast packets received.
Rx Multicast Packets	Shows the number of multicast packets received.
Rx Broadcast Packets	Shows the number of broadcast packets that were normally received. Multicast packets are not included.
CRC Align Error Packets	Shows the number of CRC errors and align errors occurred.
Drop Packets	Shows the number of packets dropped.
Undersize	Shows the number of packets whose receive size is less than 64 octets.
Oversize Packets	Shows the number of packets whose receive size is 1518 octets or more.

[*1] Bad packets and FCS are included.

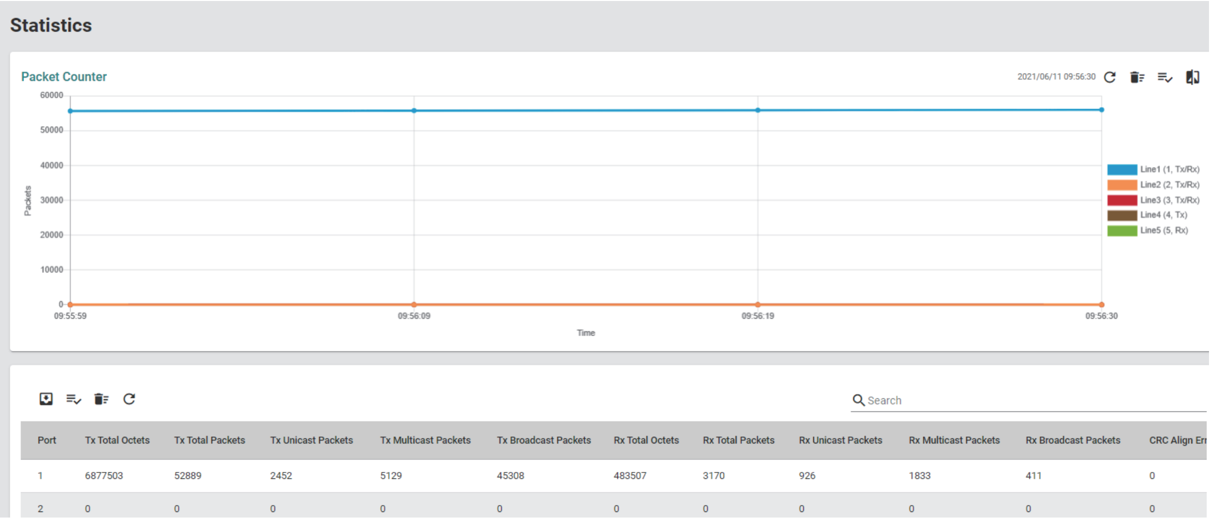
Setting method

■Display setting

Operating procedure

1. Start the operation from the "Statistics" window.

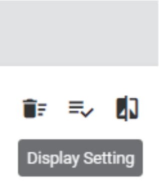
[Diagnostics] ⇨ [System Status] ⇨ [Statistics]



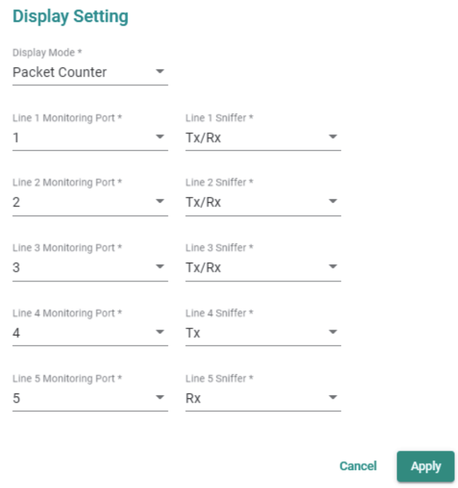
Statistics

Port	Tx Total Octets	Tx Total Packets	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Rx Total Octets	Rx Total Packets	Rx Unicast Packets	Rx Multicast Packets	Rx Broadcast Packets	CRC Align Err
1	6877503	52889	2452	5129	45308	483507	3170	926	1833	411	0
2	0	0	0	0	0	0	0	0	0	0	0

2. Click the [Display Setting] icon in the graph area.



3. Set the required items.



Display Setting

Display Mode *: Packet Counter

Line 1 Monitoring Port *: 1
Line 1 Sniffer *: Tx/Rx

Line 2 Monitoring Port *: 2
Line 2 Sniffer *: Tx/Rx

Line 3 Monitoring Port *: 3
Line 3 Sniffer *: Tx/Rx

Line 4 Monitoring Port *: 4
Line 4 Sniffer *: Tx

Line 5 Monitoring Port *: 5
Line 5 Sniffer *: Rx

Item	Description	Setting range
Display Mode	Select the graph display format. • Packet Counter: Packet counter • Bandwidth Utilization: Band utilization	• Packet Counter • Bandwidth Utilization (Default: Packet Counter)

Item	Description	Setting range
Line 1 Monitoring Port	Select the port to be displayed on line 1.	• None • 1 • 2 • 3 • 4 • 5[*2] • 6[*2] • 7[*2] • 8[*2] (Default: 1)
Line 2 Monitoring Port	Select the port to be displayed on line 2.	• None • 1 • 2 • 3 • 4 • 5[*2] • 6[*2] • 7[*2] • 8[*2] (Default: 2)
Line 3 Monitoring Port	Select the port to be displayed on line 3.	• None • 1 • 2 • 3 • 4 • 5[*2] • 6[*2] • 7[*2] • 8[*2] (Default: 3)
Line 4 Monitoring Port	Select the port to be displayed on line 4.	• None • 1 • 2 • 3 • 4 • 5[*2] • 6[*2] • 7[*2] • 8[*2] (Default: 4)
Line 5 Monitoring Port[*2]	Select the port to be displayed on line 5.	• None • 1 • 2 • 3 • 4 • 5 • 6 • 7 • 8 (Default: 5)
Line 1 Sniffer[*1]	Select whether to display receive, send, or both, on line 1. • Tx/Rx: Shows send and receive. • Tx: Shows send only. • Rx: Shows receive only.	• Tx/Rx • Tx • Rx (Default: Tx/Rx)
Line 2 Sniffer[*1]	Select whether to display receive, send, or both, on line 2. • Tx/Rx: Shows send and receive. • Tx: Shows send only. • Rx: Shows receive only.	• Tx/Rx • Tx • Rx (Default: Tx/Rx)
Line 3 Sniffer[*1]	Select whether to display receive, send, or both, on line 3. • Tx/Rx: Shows send and receive. • Tx: Shows send only. • Rx: Shows receive only.	• Tx/Rx • Tx • Rx (Default (NZ2MHG-TSNT8F2): Tx/Rx) (Default (NZ2MHG-TSNT4): Tx)
Line 4 Sniffer[*1]	Select whether to display receive, send, or both, on line 4. • Tx/Rx: Shows send and receive. • Tx: Shows send only. • Rx: Shows receive only.	• Tx/Rx • Tx • Rx (Default (NZ2MHG-TSNT8F2): Tx) (Default (NZ2MHG-TSNT4): Rx)

Item	Description	Setting range
Line 5 Sniffer[*1][*2]	Select whether to display receive, send, or both, on line 5. • Tx/Rx: Shows send and receive. • Tx: Shows send only. • Rx: Shows receive only.	• Tx/Rx • Tx • Rx (Default: Rx)

[*1] When "Display Mode" is set to "Bandwidth Utilization", this item is not displayed.

[*2] This item is not displayed for the NZ2MHG-TSNT4.

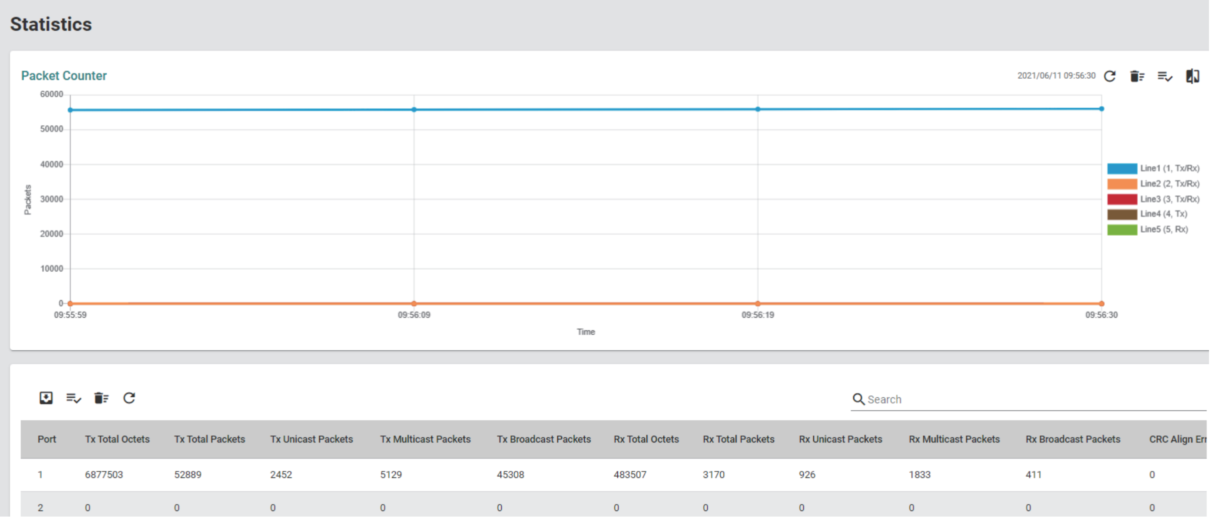
4. Click the [Apply] button.

■Data comparison

Operating procedure

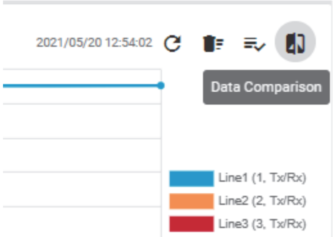
1. Start the operation from the "Statistics" window.

[Diagnostics] ⇨ [System Status] ⇨ [Statistics]

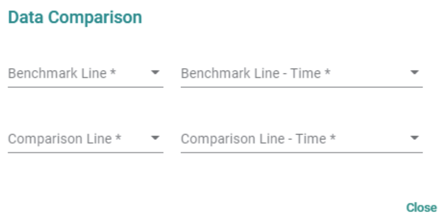


Port	Tx Total Octets	Tx Total Packets	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Rx Total Octets	Rx Total Packets	Rx Unicast Packets	Rx Multicast Packets	Rx Broadcast Packets	CRC Align Err
1	6877503	52889	2452	5129	45308	483507	3170	926	1833	411	0
2	0	0	0	0	0	0	0	0	0	0	0

2. Click the [Data Comparison] icon in the graph area.



3. Set the required items.



Data Comparison

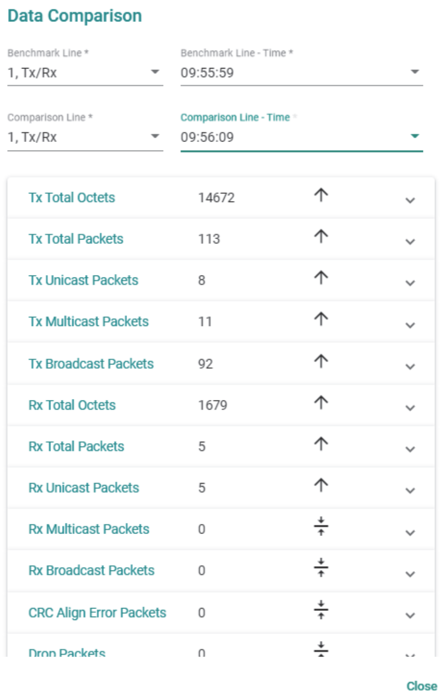
Benchmark Line * | Benchmark Line - Time *

Comparison Line * | Comparison Line - Time *

Item	Description	Setting range
Benchmark Line	Select the data to be used as the benchmark.	• None • 1 • 2 • 3 • 4 • 5*1 (Default: empty)
Benchmark Line - Time	Select the time of data to be used as the benchmark.	• None • Time (Default: empty)
Comparison Line	Select the data to be compared.	• None • 1 • 2 • 3 • 4 • 5*1 (Default: empty)
Comparison Line - Time	Select the time of the data to be compared.	• None • Time (Default: empty)

*1 This item is not displayed for the NZ2MHG-TSNT4.

4. The comparison result is displayed.



Data Comparison

Benchmark Line *: 1, Tx/Rx

Benchmark Line - Time *: 09:55:59

Comparison Line *: 1, Tx/Rx

Comparison Line - Time: 09:56:09

Tx Total Octets	14672	↑
Tx Total Packets	113	↑
Tx Unicast Packets	8	↑
Tx Multicast Packets	11	↑
Tx Broadcast Packets	92	↑
Rx Total Octets	1679	↑
Rx Total Packets	5	↑
Rx Unicast Packets	5	↑
Rx Multicast Packets	0	÷
Rx Broadcast Packets	0	÷
CRC Align Error Packets	0	÷
Drop Packets	0	÷

Point

- Data comparison can be used when "Packet Counter" is selected for "Display Mode".
- Items displayed for data comparison are the same as items displayed in the table area. (☞ Page 230 Table area)

8.13 Event Notification [Event Notification]

The following functions can be used from the event notification [Event Notification] displayed on the function menu of the web interface.

- Event notification function [Event Notification]
- Relay alarm cut-off [Relay Alarm Cut-off]
- Email notification function [Email Notification]
- Syslog function [Syslog]

Event notification function [Event Notification]

The managed switch can notify event occurrence in the system and ports. The system status and port status can be monitored by receiving notifications on a device such as a personal computer.

Event notification

The following two types of event notification are available.

- Notifications related to the system and functions
- Port status notifications

Event notification method

The following three types of event notification methods are available.

- Trap: Events are notified to the SMNP manager.
- Email: Events are notified via email.
- Relay: The relay output terminal of the managed switch turns on.

Event list

The following table lists events that can be notified. For details on the events, refer to the following.

☞ Page 91 Event description

■List of notifications related to the system and functions

Event name	Classification
Cold start	Critical
Warm start	Notice
Configuration changed	Notice
Login success	Notice
Login fail	Warning
Login lockout	Warning
Account setting changed	Notice
Configuration imported	Notice
SSL certification changed	Notice
Log capacity threshold	Warning
Password changed	Notice
PWR Off->On	Notice
PWR On->Off	Notice
DI On	Notice
DI Off	Notice
RSTP topology changed	Warning
LLDP table changed	Information

■List of port status notifications

Event name	Classification
Port On	Critical
Port Off	Notice

Setting method

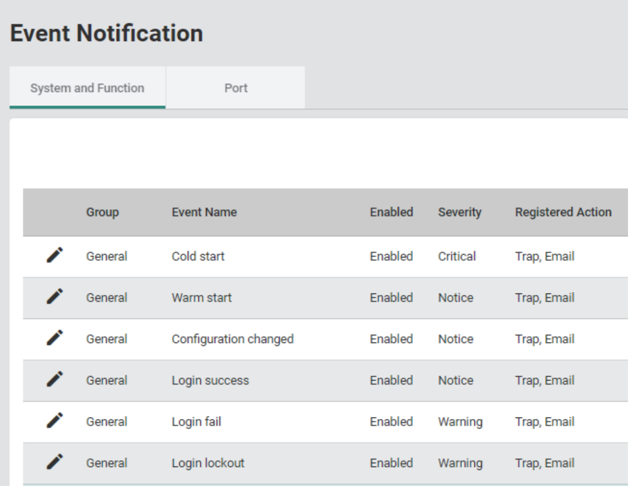
■Notifications related to the system and functions

Operating procedure

1. Start the operation from the "Event Notification" window.

[Diagnostics] ⇨ [Event Notification] ⇨ [Event Notification]

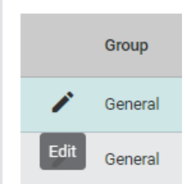
2. Select the [System and Function] tab.



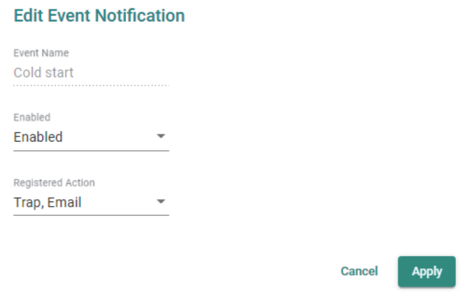
Event Notification

	Group	Event Name	Enabled	Severity	Registered Action
✎	General	Cold start	Enabled	Critical	Trap, Email
✎	General	Warm start	Enabled	Notice	Trap, Email
✎	General	Configuration changed	Enabled	Notice	Trap, Email
✎	General	Login success	Enabled	Notice	Trap, Email
✎	General	Login fail	Enabled	Warning	Trap, Email
✎	General	Login lockout	Enabled	Warning	Trap, Email

3. Click the [Edit] icon of the event for which notifications are to be set.



4. Set the required items.



Edit Event Notification

Event Name: Cold start

Enabled: Enabled

Registered Action: Trap, Email

Item	Description	Setting range
Enabled	Enable or disable the event notification. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Registered Action	Set the event notification method. Multiple methods can be selected. • Trap: Events are notified to the SMNP manager. • Email: Events are notified via email. • Relay: The relay output terminal of the managed switch turns on.	• Trap • Email • Relay (Default: Trap, Email)

5. Click the [Apply] button.

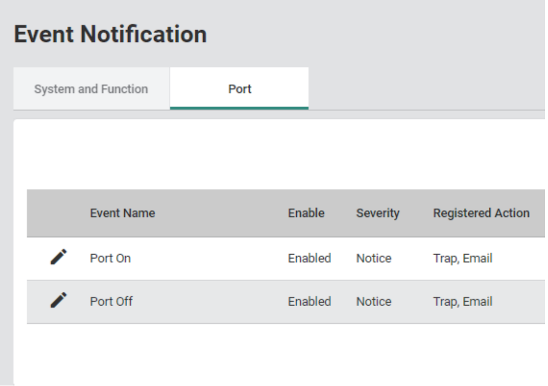
■Port status notifications

Operating procedure

1. Start the operation from the "Event Notification" window.

[Diagnostics] ⇨ [Event Notification] ⇨ [Event Notification]

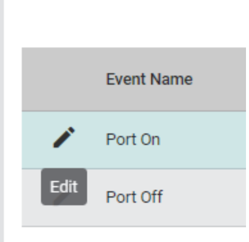
2. Select the [Port] tab.



Event Notification

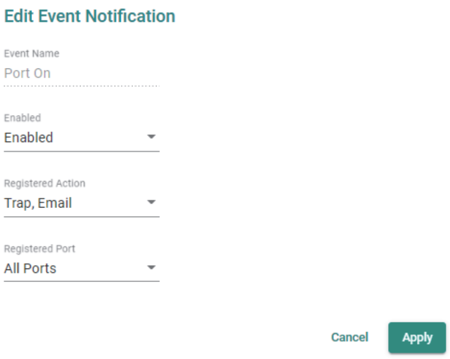
	Event Name	Enable	Severity	Registered Action
✎	Port On	Enabled	Notice	Trap, Email
✎	Port Off	Enabled	Notice	Trap, Email

3. Click the [Edit] icon of the event for which notifications are to be set.



	Event Name
✎	Port On
Edit	Port Off

4. Set the required items.



Edit Event Notification

Event Name: Port On

Enabled: Enabled

Registered Action: Trap, Email

Registered Port: All Ports

Item	Description	Setting range
Enabled	Enable or disable the event notification. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Registered Action	Set the event notification method. Multiple methods can be selected. • Trap: Events are notified to the SMNP manager. • Email: Events are notified via email. • Relay: The relay output terminal of the managed switch turns on.	• Trap • Email • Relay (Default: Trap, Email)

Item	Description	Setting range
Registered Port	Select the port to be set.	• All Ports • 1 • 2 • 3 • 4 • 5[*1] • 6[*1] • 7[*1] • 8[*1] (Default: All Ports)

*1 This item is not displayed for the NZ2MHG-TSNT4.

5. Click the [Apply] button.

Relay alarm cut-off [Relay Alarm Cut-off]

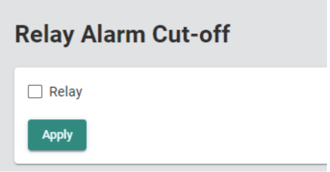
Notification by the relay output is turned off.

Setting method

Operating procedure

1. Start the operation from the "Relay Alarm Cut-off" window.

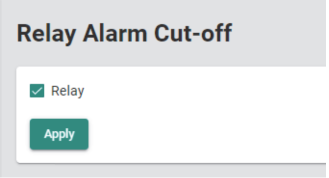
🖱 [Diagnostics] ⇨ [Event Notification] ⇨ [Relay Alarm Cut-off]



Relay Alarm Cut-off

□ Relay

2. Select the checkbox.



Relay Alarm Cut-off

☑ Relay

3. Click the [Apply] button.

Email notification function [Email Notification]

Events are notified via email. The managed switch supports email transmission using SMTP. To notify events via email, set the information such as the send source email address and send destination email address. Notification can be issued to up to five email addresses.

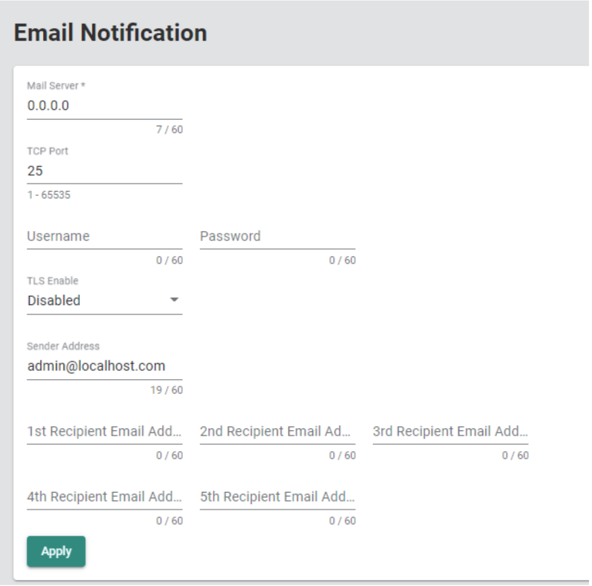
Setting method

Operating procedure

1. Start the operation from the "Email Notification" window.

[Diagnostics] ⇨ [Event Notification] ⇨ [Email Notification]

2. Set the required items.



Email Notification

Mail Server * 0.0.0.0

TCP Port 25

TLS Enable Disabled

Sender Address admin@localhost.com

7 / 60
1 - 65535
Username
0 / 60
Password
0 / 60
19 / 60
1st Recipient Email Add...
0 / 60
2nd Recipient Email Ad...
0 / 60
3rd Recipient Email Add...
0 / 60
4th Recipient Email Add...
0 / 60
5th Recipient Email Add...
0 / 60
Apply

Item	Description	Setting range
Mail Server	Set the IP address of the SMTP server.	0 to 60 characters (one-byte alphanumeric characters and symbols) (Default: 0.0.0.0)
TCP Port	Set the TCP port number for access to the SMTP server.	1 to 65535 (Default: 25)
Username	Set the user name of the email account.	0 to 60 characters (one-byte alphanumeric characters and symbols) (Default: empty)
Password	Set the password of the email account.	0 to 60 characters (one-byte alphanumeric characters and symbols) (Default: empty)
TLS Enable	Enable or disable TLS. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled: (Default: Disabled)
Sender Address	Set the email address of the managed switch.	0 to 60 characters (one-byte alphanumeric characters and symbols) (Default: admin@localhost.com)
1st Recipient Email Address	Set up to five email addresses to receive event notifications from the managed switch.	0 to 60 characters (one-byte alphanumeric characters and symbols) (Default: empty)
2nd Recipient Email Address		
3rd Recipient Email Address		
4th Recipient Email Address		
5th Recipient Email Address		

3. Click the [Apply] button.

Syslog function [Syslog]

Various types of event logs are sent to the Syslog server. The managed switch uses UDP to send Syslog messages.

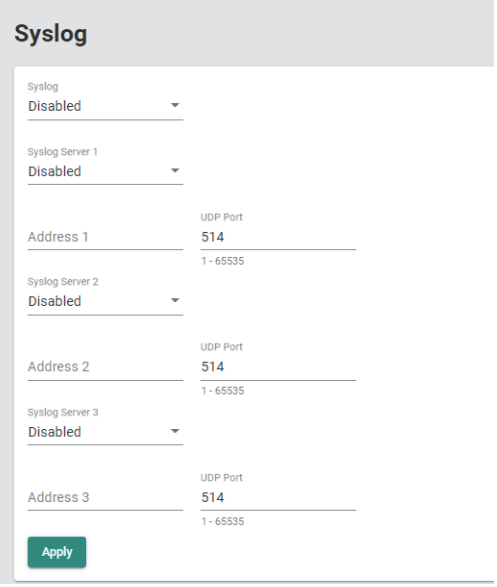
Setting method

Operating procedure

1. Start the operation from the "Syslog" window.

[Diagnostics] ⇨ [Event Notification] ⇨ [Syslog]

2. Set the required items.



Syslog

Syslog: Disabled

Syslog Server 1: Disabled

Address 1

UDP Port: 514 (1 - 65535)

Syslog Server 2: Disabled

Address 2

UDP Port: 514 (1 - 65535)

Syslog Server 3: Disabled

Address 3

UDP Port: 514 (1 - 65535)

Item	Description	Setting range
Syslog	Enable or disable Syslog. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)
Syslog Server 1	Enable or disable transmission to the first Syslog server. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)
Address 1	Input the IP address of the first Syslog server to which event logs are to be saved.	• Empty • One-byte alphanumeric characters and symbols (Default: empty)
UDP Port	Specify the UDP port number.	1 to 65535 (Default: 514)
Syslog Server 2	Enable or disable transmission to the second Syslog server. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)
Address 2	Input the IP address of the second Syslog server to which event logs are to be saved.	• Empty • One-byte alphanumeric characters and symbols (Default: empty)
UDP Port	Specify the UDP port number.	1 to 65535 (Default: 514)
Syslog Server 3	Enable or disable transmission to the third Syslog server. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Disabled)
Address 3	Input the IP address of the third Syslog server to which event logs are to be saved.	• Empty • One-byte alphanumeric characters and symbols (Default: empty)
UDP Port	Specify the UDP port number.	1 to 65535 (Default: 514)

Point

Syslog messages are sent to all the Syslog servers for which this function is set as "Enabled".

3. Click the [Apply] button.

8.14 Diagnostic Function [Diagnosis]

The following functions can be used from the diagnostic function [Diagnosis] displayed on the function menu of the web interface.

- LLDP
- Ping
- ARP table [ARP Table]
- Event log [Event Log]

LLDP

LLDP is a protocol that can send configuration information to adjacent devices. Therefore, LLDP devices can always keep track of the status and configuration of counterpart devices. For example, devices connected with the managed switch can be checked from a remote location.

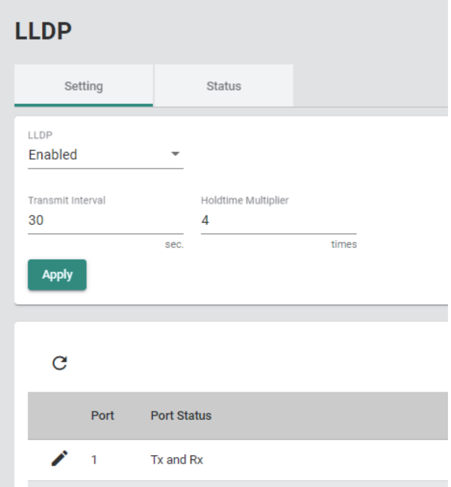
Operating procedure

1. Start the operation from the "LLDP" window.

[Diagnostics] ⇨ [Diagnosis] ⇨ [LLDP]

2. Select the [Setting] tab.

3. Set the required items.



LLDP

Setting | Status

LLDP: Enabled

Transmit Interval: 30 sec.

Holdtime Multiplier: 4 times

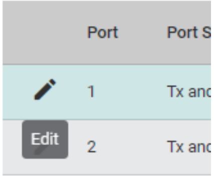
Apply

	Port	Port Status
✎	1	Tx and Rx

Item	Description	Setting range
LLDP	Enable or disable LLDP. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Transmit Interval	Specify the transmission interval of the LLDP messages.	5 to 32768s (Default: 30s)
Holdtime Multiplier	A multiplier for determining the TTL. (Time to Live: Information holdtime at the adjacent devices) Example: TTL = 30 (Transmit Interval) × 4 (Holdtime Multiplier)	2 to 10 (Default: 4)

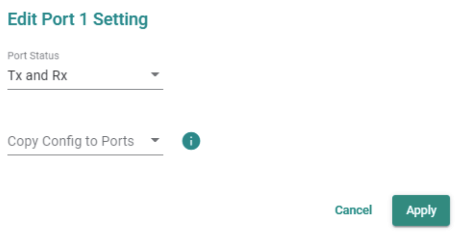
4. Click the [Apply] button.

5. Click the [Edit] icon of the port to be set.



	Port	Port S
✎	1	Tx anc
Edit	2	Tx anc

6. Set the required items.



Edit Port 1 Setting

Port Status: Tx and Rx

Item	Description	Setting range
Port Status	Configure the send/receive settings for the LLDP messages. • Tx Only: Only sends LLDP messages. • Rx Only: Only receives LLDP messages. • Tx and Rx: Sends and receives LLDP messages. • Disabled: Stops sending and receiving LLDP messages.	• Tx Only • Rx Only • Tx and Rx • Disabled (Default: Tx and Rx)
Copy Config to Ports	The settings are copied to other ports. Multiple items can be selected.	• All Ports • 1 • 2 • 3 • 4 • 5*1 • 6*1 • 7*1 • 8*1 (Default: empty)

*1 This item is not displayed for the NZ2MHG-TSNT4.

7. Click the [Apply] button.

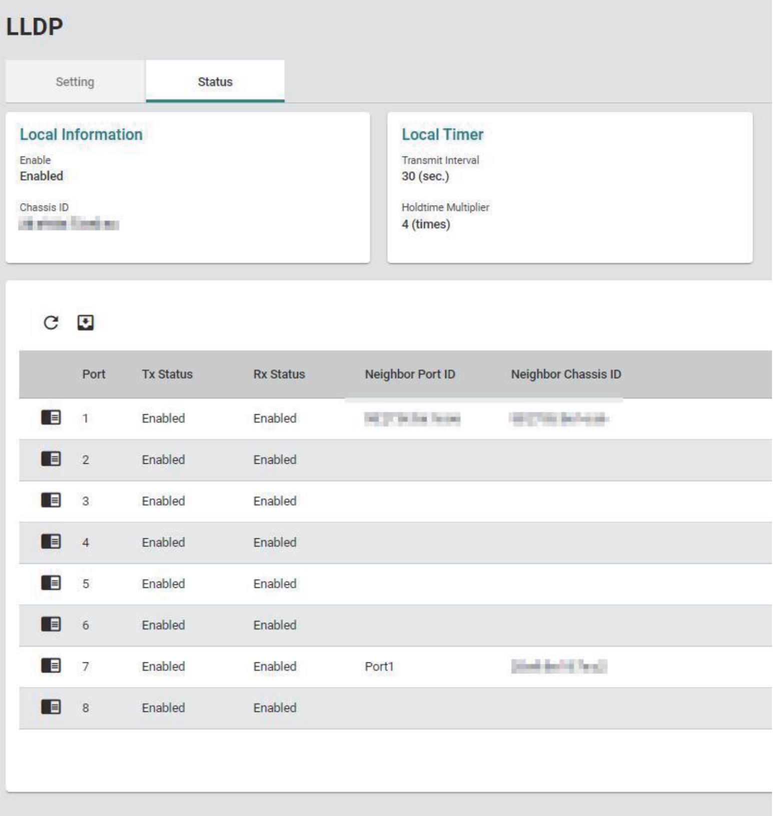
LLDP status

Operating procedure

1. Start the operation from the "LLDP" window.

[Diagnostics] ⇨ [Diagnosis] ⇨ [LLDP]

2. Select the [Status] tab.



Local Information

Enable
Enabled

Chassis ID
[redacted]

Local Timer

Transmit Interval
30 (sec.)

Holdtime Multiplier
4 (times)

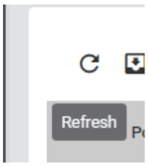
Port	Tx Status	Rx Status	Neighbor Port ID	Neighbor Chassis ID
1	Enabled	Enabled	[redacted]	[redacted]
2	Enabled	Enabled		
3	Enabled	Enabled		
4	Enabled	Enabled		
5	Enabled	Enabled		
6	Enabled	Enabled		
7	Enabled	Enabled	Port1	[redacted]
8	Enabled	Enabled		

Item		Description
Local Information	Enable	Shows whether LLDP is enabled or disabled.
	Chassis ID	Shows the information of the managed switch. (Such as MAC address)
Local Timer	Transmit Interval (sec.)	Shows the set value.
	Holdtime Multiplier[*1]	Shows the set value.
Port	Port	Shows the port number.
	Tx Status	Shows whether LLDP messages can be sent.
	Rx Status	Shows whether LLDP messages can be received.
	Neighbor Port ID	Shows the port ID of the adjacent device.
	NeighborChassis ID	Shows the information of the equipment of the adjacent device. (Such as MAC address)

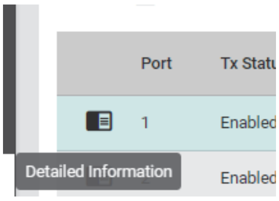
*1 This item is displayed only when Advanced Mode is set.

Point

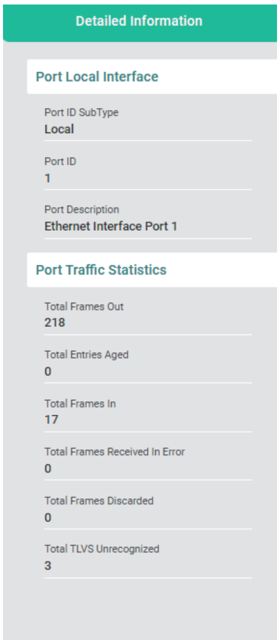
Click the [Refresh] icon. The display is updated to the latest information.



3. Click the [Detailed Information] icon of each port.



4. The detailed information is displayed.


Detailed Information

Port Local Interface

Port ID SubType
Local

Port ID
1

Port Description
Ethernet Interface Port 1

Port Traffic Statistics

Total Frames Out
218

Total Entries Aged
0

Total Frames In
17

Total Frames Received In Error
0

Total Frames Discarded
0

Total TLVS Unrecognized
3

Item		Description
Port Local Interface	Port Type SubType	Shows the subtype of Port ID TLV notified from the adjacent device.
	Port ID	Shows the Port ID information notified from the adjacent device via Port ID TLV.
	Port Description	Shows the port description notified from the adjacent device Shows Port Description TLV.
Port Traffic Statistics	Total Frames Out	Shows the total number of LLDP packets sent.
	Total Entries Aged	Shows the total number of timeout devices.
	Total Frames In	Shows the total number of LLDP packets received.
	Total Frames Received Error	Shows the total number of LLDP packets received in error.
	Total Frames Discarded	Shows the total number of LLDP packets discarded.
	Total TLVS Unrecognized	Shows the total number of unrecognizable data.

Ping

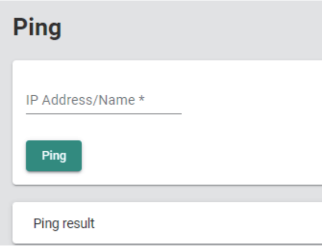
The route between the personal computer and the network devices to which communication is being made can be checked for any abnormality.

Setting method

Operating procedure

1. Start the operation from the "Ping" window.

🖱 [Diagnostics] ⇨ [Diagnosis] ⇨ [Ping]



Item	Description	Setting range
IP Address/Name	Input the IP address or host name from which to send a ping.	One-byte alphanumeric characters and symbols (Default: empty)

2. Click the [Ping] button.

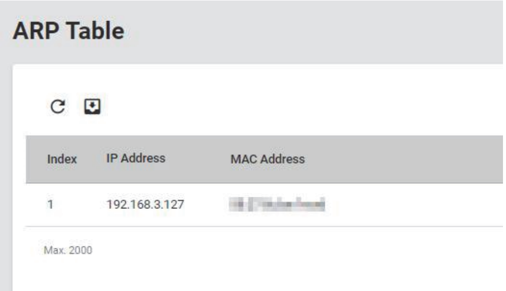
ARP table

ARP is a protocol to be used to obtain the MAC address from an IP address. The ARP table saves the information of the IP address and MAC address of a device to which communication was made. If 127 or more pieces of information are registered in the ARP table, the information that has been registered for a certain period of time will be deleted.

Operating procedure

1. Start the operation from the "ARP Table" window.

[Diagnostics] ⇨ [Diagnosis] ⇨ [ARP Table]



ARP Table

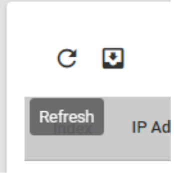
Index	IP Address	MAC Address
1	192.168.3.127	[redacted]

Max. 2000

Item	Description
Index	Shows the index.
IP Address	Shows the IP address of the device.
MAC Address	Shows the MAC address of the device.

Point

- Up to 2000 ARP tables are displayed.
- Click the [Refresh] icon to update the display to the latest information.



Event log [Event Log]

Events that have occurred are recorded in the event log. The recorded event logs can be displayed on the web interface window. Data analysis can be performed by logging events such as power-on/off and port link-up/link-down. Up to 10000 events can be recorded. (The maximum number of events may be reduced depending on the log used on the system side.)

Precautions

Event logs are collected for each managed switch.

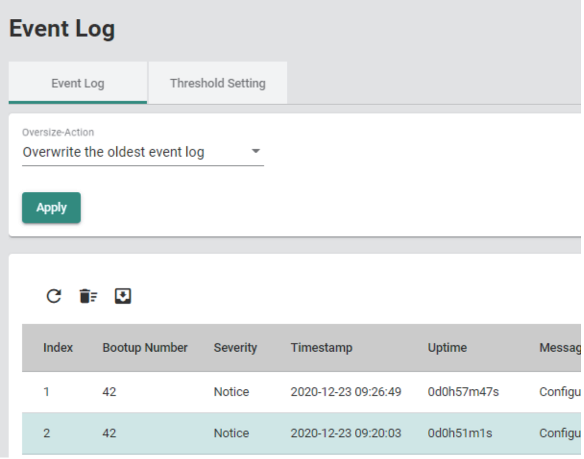
Setting method

Operating procedure

1. Start the operation from the "Event Log" window.

[Diagnostics] ⇨ [Diagnosis] ⇨ [Event Log]

2. Select the [Event Log] tab.



Event Log

Oversize-Action: Overwrite the oldest event log

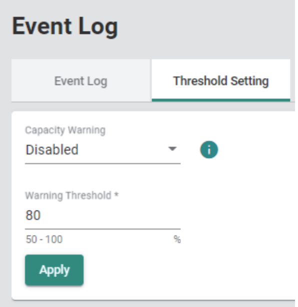
Index	Bootup Number	Severity	Timestamp	Uptime	Messag
1	42	Notice	2020-12-23 09:26:49	0d0h57m47s	Configu
2	42	Notice	2020-12-23 09:20:03	0d0h51m1s	Configu

Item	Description	Setting range
Oversize-Action	Set the processing to be applied when the log file cannot be saved (when the maximum number of logs is exceeded). • Overwrite the oldest event log: Event logs are overwritten from the oldest log. • Stop recording event log: Event log saving is stopped.	• Overwrite the oldest event log • Stop recording event log (Default: Overwrite the oldest event log)

3. Click the [Apply] button.

4. Select the [Threshold Setting] tab.

5. Set the required items.



Event Log

Capacity Warning: Disabled

Warning Threshold *: 80

50 - 100 %

Item	Description	Setting range
Capacity Warning	Enable or disable the event log save capacity warning. • Enabled: Enable • Disabled: Disable	• Enabled • Disabled (Default: Enabled)
Warning Threshold	Set the threshold value of save capacity by which to trigger the warning.	50 to 100 (Default: 80)

6. Click the [Apply] button.

Point

Warnings can be checked with the event log output function and the event notification function. (☞ Page 89 Event log output function [Event Log Backup], Page 235 Event notification function [Event Notification])

Displaying event logs

All the saved events can be checked from the event log page.

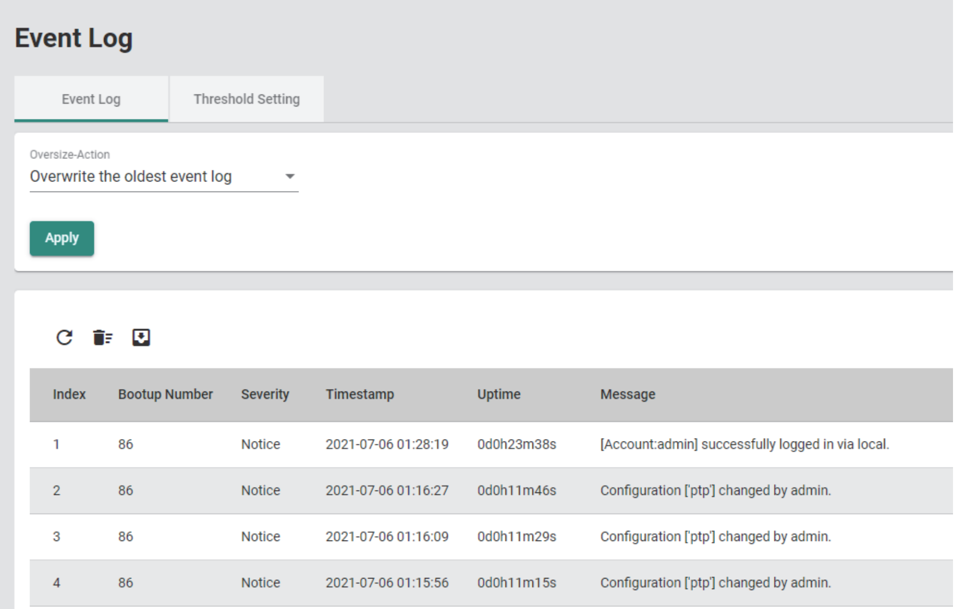
■Updating event logs

Operating procedure

1. Start the operation from the "Event Log" window.

[Diagnostics] ⇨ [Diagnosis] ⇨ [Event Log]

2. Select the [Event Log] tab.



Event Log

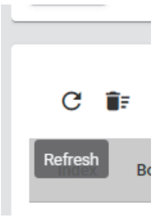
Oversize-Action: Overwrite the oldest event log

Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	86	Notice	2021-07-06 01:28:19	0d0h23m38s	[Account:admin] successfully logged in via local.
2	86	Notice	2021-07-06 01:16:27	0d0h11m46s	Configuration ['ptp'] changed by admin.
3	86	Notice	2021-07-06 01:16:09	0d0h11m29s	Configuration ['ptp'] changed by admin.
4	86	Notice	2021-07-06 01:15:56	0d0h11m15s	Configuration ['ptp'] changed by admin.

Item	Description
Index	Shows the index.
Bootup Number	Shows the number of restarts caused by operations such as power off and on and by the rebooting function.
Severity	Shows the classification (Notice, Critical, Info, Warning).
Timestamp	Shows the time stamp at event registration.
Uptime	Shows the operating time from power-on to event registration.
Message	Shows the event description. (☞ Page 91 Event description)

Point

Click the [Refresh] icon to update the event logs to the latest information.



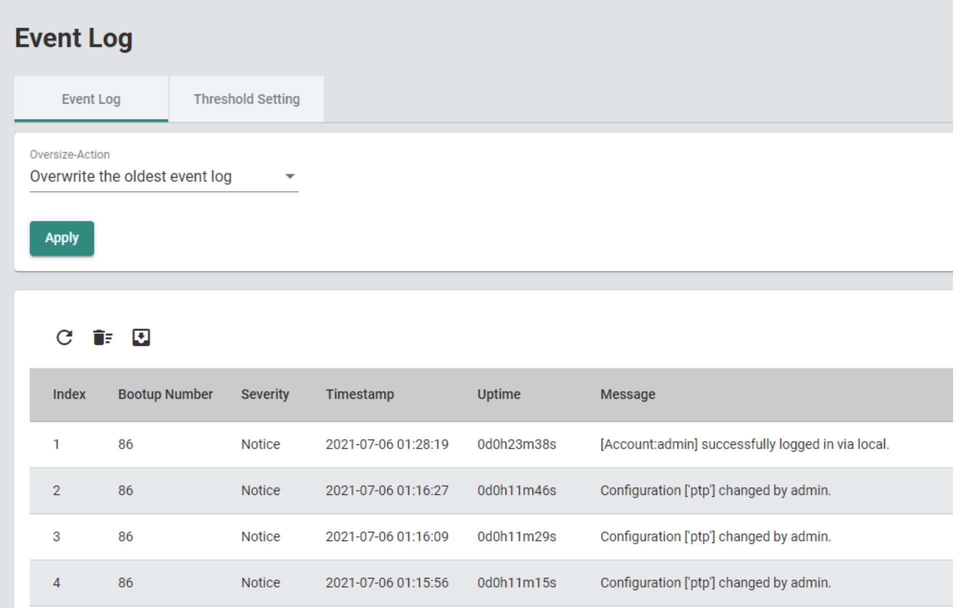
■Deleting event logs

Operating procedure

1. Start the operation from the "Event Log" window.

[Diagnostics] ⇨ [Diagnosis] ⇨ [Event Log]

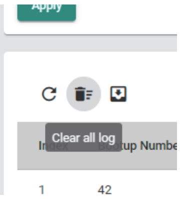
2. Select the [Event Log] tab.



Oversize-Action: Overwrite the oldest event log

Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	86	Notice	2021-07-06 01:28:19	0d0h23m38s	[Account:admin] successfully logged in via local.
2	86	Notice	2021-07-06 01:16:27	0d0h11m46s	Configuration ['ptp'] changed by admin.
3	86	Notice	2021-07-06 01:16:09	0d0h11m29s	Configuration ['ptp'] changed by admin.
4	86	Notice	2021-07-06 01:15:56	0d0h11m15s	Configuration ['ptp'] changed by admin.

3. Click the [Clear all log] icon.



4. The confirmation dialog appears. Click the [Clear] button to perform deletion.

9 MAINTENANCE AND INSPECTION

This chapter describes items that must be maintained or inspected daily or periodically to properly use a managed switch in optimal condition at all times.

9.1 Daily Inspection

The following table lists items that must be inspected daily.

Item	Inspection item	Inspection method	Criterion	Corrective action
1	Installation status	Check the FG line mounting screws and DIN rail mounting kit for looseness.	The screws and kit must be fixed securely.	Retighten the screws.
2	Connection status	Check the terminal block mounting screws for looseness.	The terminal block mounting screws must not be loose.	Retighten the terminal block mounting screws.
3		Check the cable connector for looseness.	The cable connector must not be loose.	Connect the connector securely.
4	RUN LED status	Check that the LED is on.	On (green)	When the criterion is not satisfied, refer to the following and take the corrective action. ☞ Page 256 Troubleshooting with LED Indicators
5	PW1, PW2 LED status	Check that the LED is on.	On (orange)	

9.2 Periodic Inspection

The following table lists items that must be inspected one or two times every six months to one year.

Item	Inspection item	Inspection method	Criterion	Corrective action
1	Ambient temperature	Measure the temperature by using a thermometer.	-10 to 60℃	Create the environment that satisfies the criterion.
2	Ambient humidity	Measure the humidity by using a hygrometer.	5 to 95%RH	
3	Atmosphere	Measure corrosive gases.	No corrosive gases	
4	Power supply voltage check	• PW1: Measure the voltage between the V+ and V- terminals. • PW2: Measure the voltage between the V+ and V- terminals.	9.6 to 60.0VDC	When the power supply does not satisfy the criterion range, change the power supply.
5	Looseness and rattling	Touch the managed switch to check for looseness and rattling.	The switch must be mounted securely.	Retighten the screws.
6	Attachment of dirt and foreign matter	Check visually.	Dirt and foreign matter must not be attached.	Remove them. Clean the managed switch. When cleaning the managed switch, use a dry cloth.
7	Installation status	Check the FG line mounting screws and DIN rail mounting kit for looseness.	The screws and kit must be fixed securely.	Retighten the screws.
8	Connection status	Check the terminal block mounting screws for looseness.	The terminal block mounting screws must not be loose.	Retighten the terminal block mounting screws.
9		Check the cable connector for looseness.	The cable connector must not be loose.	Connect the connector securely.

MEMO

10 TROUBLESHOOTING

This chapter describes troubleshooting for the managed switch.

10.1 Troubleshooting with LED Indicators

This section describes how to troubleshoot the managed switch with the LEDs.

When the PW1 LED and PW2 LED turn off

When the PW1 LED and PW2 LED turn off, check the following.

Cause	Corrective action
The power cable is not connected.	Connect the power cable.
No power is supplied or the power supply is out of the specified range.	• Input the power supply. • Use the specified power supply.
The power cable is disconnected.	Replace the power cable.
A hardware failure has occurred.	• Power off and on to restart the managed switch. • Initialize the parameters. Press and hold the reset button for five seconds to reset all the settings to default.

If the problem is not solved even after taking the actions above, please consult your local Mitsubishi representative.

When the RUN LED turns off

When the RUN LED turns off, check the following..

Cause	Corrective action
A hardware failure has occurred.	• Power off and on to restart the managed switch. • Initialize the parameters. Press and hold the reset button for five seconds to reset all the settings to default.

If the problem is not solved even after taking the actions above, please consult your local Mitsubishi representative.

When the ERR LED turns on red

When the ERR LED turns on red, check the following.

Cause	Corrective action
A software failure has occurred. (System initialization has failed.)	• Power off and on to restart the managed switch. • Initialize the parameters. Press and hold the reset button for five seconds to reset all the settings to default.
Configuration automatic restoration has failed. (In the event log, the automatic restoration failure log (Configuration import failed by system via usb) has been registered.) This event occurs only when a USB flash drive is connected. Prepare the necessary file in the specified folder in the USB flash drive.	• Prepare the necessary file in the specified folder in the USB flash drive. • Use a USB flash drive that is formatted in the FAT or FAT32 format. • Check for any USB flash drive errors. If any error is found, replace the USB flash drive. • When the configuration automatic restoration function is not used, disable the function.
Event log automatic backup has failed. This event occurs only when a USB flash drive is connected.	• Secure sufficient free space in the USB flash drive. • Use a USB flash drive that is formatted in the FAT or FAT32 format. • Check for any USB flash drive errors. If any error is found, replace the USB flash drive. • When the event log automatic backup function is not used, disable the function.

If the problem is not solved even after taking the actions above, please consult your local Mitsubishi representative.

When the SYNC LED turns off

When the SYNC LED turns off, check the following.

Cause	Corrective action
Time synchronization has not been performed. (The parameter is incorrectly set.)	Set "Time Synchronization" to "Enabled". (☞ Page 129 Setting method)

If the problem is not solved even after taking the actions above, please consult your local Mitsubishi representative.

Point

If the time synchronization function is disabled, the SYNC LED turns off. (The off state is normal.)

When the 1Gbps LINK LED and 100Mbps/10Mbps LINK LED turn off

When the 1Gbps LINK LED and 100Mbps/10Mbps LINK LED turn off, check the following.

Cause	Corrective action
The Ethernet cable is not connected.	Connect the Ethernet cable.
The Ethernet cable is disconnected.	Replace the Ethernet cable.
The parameters are incorrectly set.	• Set "Admin Status" to "Enabled". (☞ Page 141 Setting method) • Set the parameters such that they correspond to the communication speed and port type of the connected device.
A hardware failure has occurred.	• Power off and on to restart the managed switch. • Initialize the parameters. Press and hold the reset button for five seconds to reset all the settings to default.

If the problem is not solved even after taking the actions above, please consult your local Mitsubishi representative.

When the 1Gbps/100Mbps LINK LED turns off

When the 1Gbps/100Mbps LINK LED turns off, check the following.

Cause	Corrective action
The SFP module and optical fiber cable are not connected.	Connect the SFP module and optical fiber cable.
The optical fiber cable is disconnected.	Replace the optical fiber cable.
The SFP module in use is not connectable.	Use a connectable SFP module. (📖 Applicable Products for CC-Link IE TSN Industrial Managed Switch (FA-A-0347))
An SFP module error has occurred.	Check the SFP module. If the module is faulty, replace it.
The parameters are incorrectly set.	• Set "Admin Status" to "Enabled". (☞ Page 141 Setting method) • Set the parameters such that they correspond to the communication speed and port type of the connected device.
A hardware failure has occurred.	• Power off and on to restart the managed switch. • Initialize the parameters. Press and hold the reset button for five seconds to reset all the settings to default.

If the problem is not solved even after taking the actions above, please consult your local Mitsubishi representative.

10.2 Troubleshooting by Symptom

This section describes troubleshooting methods for various symptoms.

Communications fail between external devices

■When an Ethernet cable is used

Cause	Corrective action
The Ethernet cable is not connected.	Connect the Ethernet cable.
The Ethernet cable is disconnected.	Replace the Ethernet cable.
The parameters are incorrectly set.	• Set "Admin Status" to "Enabled". (☞ Page 141 Setting method) • Set the parameters such that they correspond to the communication speed and port type of the connected device. • When the VLAN function is used, set the parameters so that the same VLAN ID is assigned to external devices that communicate. (☞ Page 144 VLAN function [VLAN])
The IP address is overlapped.	Configure the devices so that their IP addresses are not overlapped on the network.

■When an optical fiber cable is used

Cause	Corrective action
The SFP module and optical fiber cable are not connected.	Connect the SFP module and optical fiber cable.
The optical fiber cable is disconnected.	Replace the optical fiber cable.
The SFP module in use is not connectable.	Use a connectable SFP module. (📖 Applicable Products for CC-Link IE TSN Industrial Managed Switch (FA-A-0347))
An SFP module error has occurred.	Check the SFP module. If the module is faulty, replace it.
The parameters are incorrectly set.	• Set "Admin Status" to "Enabled". (☞ Page 141 Setting method) • When the VLAN function is used, set the parameters so that the same VLAN ID is assigned to external devices that communicate. (☞ Page 144 VLAN function [VLAN])
The IP address is overlapped.	Configure the devices so that their IP addresses are not overlapped on the network.

Communications become unstable

Cause	Corrective action
A frame loss has occurred.	Use the statistical information to check whether any frame loss (Drop Packets) has occurred. If any frame loss has occurred, check and correct the communication load of the connected devices. (☞ Page 229 Statistical information [Statistics])
A loop has occurred.	Check and correct the connection to eliminate the loop. To include a loop in the network, perform the following. • Enable the spanning tree function. • Set the port in which the managed switches are connected to each other to a port other than the edge port.

Connection to the web interface fails

Cause	Corrective action
The Ethernet cable is not connected.	Connect the Ethernet cable.
The Ethernet cable is disconnected.	Replace the Ethernet cable.
The SFP module and optical fiber cable are not connected.	Connect the SFP module and optical fiber cable.
The optical fiber cable is disconnected.	Replace the optical fiber cable.
The SFP module in use is not connectable.	Use a connectable SFP module. (📖 Applicable Products for CC-Link IE TSN Industrial Managed Switch (FA-A-0347))
An SFP module error has occurred.	Check the SFP module. If the module is faulty, replace it.
The parameters are incorrectly set.	Connect to the CLI using a console cable and perform the following settings. • Set "Admin Status" to "Enabled". (☞ Page 141 Setting method) • Set the parameters such that they correspond to the communication speed and port type of the connected device.
The IP address of the connection destination is incorrect.	Check the IP address of the managed switch and retry the connection. All the settings can be reset to default by pressing and holding the reset button for five seconds. The default IP address and subnet mask are as follows. • IP address: 192.168.3.252 • Subnet mask: 255.255.255.0
The IP address of the personal computer to be connected is incorrect.	Set the IP address so that it is in the same class and subnet address.
The IP address is overlapped.	Configure the devices so that their IP addresses are not overlapped on the network.
The firewall and proxy server settings are enabled in the personal computer to be connected.	Check and correct the firewall and proxy server settings for the personal computer to be connected.
JavaScript and cookies are disabled in the web browser settings.	Enable JavaScript and cookies in the web browser settings.
The port for which the management VLAN ID is set is not connected.	Connect the personal computer to the port that is assigned to the management VLAN ID.
The number of concurrent connections has exceeded the maximum number.	Connect the devices so that the number of them does not exceed the maximum number of concurrent connections. (☞ Page 202 Interface management function [Management Interface])

Parameters cannot be set

■Web interface

Cause	Corrective action
The required items are not filled.	Input all the required items (items whose parameter name is marked with an asterisk (*)).
The parameter setting value is out of the setting range.	Set the parameter setting value within the setting range. If an error message is displayed, follow the description.
The login account does not have administrator privileges.	Some parameter settings are restricted if logged in with an account without administrator privileges. Configure the settings after logging in with the account that has administrator privileges.

■CLI command

Cause	Corrective action
The "% Ambiguous Command" message is displayed.	This message indicates that the input command is ambiguous. Input the command again. Input a question mark (?) at the end of the command during input to display a list of commands that can be input.
The "% Incomplete command" message is displayed.	This message indicates that the input command or setting value is incomplete. Input the command again. Input a space followed by a question mark (?) at the end of the command during input to display a list of commands that can be entered next and also a list of setting ranges that can be input.
The "% Invalid input detected at '^' marker" message is displayed.	This message indicates that the input command or setting value is invalid. (The invalid input part is indicated with a caret (^).) Input the command again. Input a space followed by a question mark (?) at the end of the command during input to display a list of commands that can be entered next and also a list of setting ranges that can be input.
The login account does not have administrator privileges.	Some parameter settings are restricted if logged in with an account without administrator privileges. Configure the settings after logging in with the account that has administrator privileges.

Connection to the CLI fails

■Telnet connection or SSH connection

Cause	Corrective action
The Ethernet cable is not connected.	Connect the Ethernet cable.
The Ethernet cable is disconnected.	Replace the Ethernet cable.
The SFP module and optical fiber cable are not connected.	Connect the SFP module and optical fiber cable.
The optical fiber cable is disconnected.	Replace the optical fiber cable.
The SFP module in use is not connectable.	Use a connectable SFP module. (📖 Applicable Products for CC-Link IE TSN Industrial Managed Switch (FA-A-0347))
An SFP module error has occurred.	Check the SFP module. If the module is faulty, replace it.
The parameters are incorrectly set.	Connect to the CLI using a console cable and perform the following settings. • Set "Admin Status" to "Enabled". (☞ Page 141 Setting method) • Set the parameters such that they correspond to the communication speed and port type of the connected device.
The IP address of the connection destination is incorrect.	Set the IP address of the managed switch. All the settings can be reset to default by pressing and holding the reset button for five seconds. The default IP address and subnet mask are as follows. • IP address: 192.168.3.252 • Subnet mask: 255.255.255.0
The IP address of the personal computer to be connected is incorrect.	Set the IP address so that it is in the same class and subnet address.
The IP address is overlapped.	Configure the devices so that their IP addresses are not overlapped on the network.
The firewall and proxy server settings are enabled in the personal computer to be connected.	Check and correct the firewall and proxy server settings for the personal computer to be connected.
The port for which the management VLAN ID is set is not connected.	Connect the personal computer to the port that is assigned to the management VLAN ID.
The number of concurrent connections has exceeded the maximum number.	Connect the devices so that the number of them does not exceed the maximum number of concurrent connections. (☞ Page 202 Interface management function [Management Interface])

■RS-232 connection

Cause	Corrective action
The console cable is not connected.	Connect the console cable.
The console cable is disconnected.	Replace the console cable.
The serial communication settings do not match.	Set the serial communication settings for the terminal emulator as follows. • Baud rate (BPS): 115200 • Data length: 8 bits • Stop bit: 1 bit • Parity: None

Logging in to the web interface or CLI fails

Cause	Corrective action
The account name or password is incorrect.	Check the account name and password set in the managed switch and retry logging in. If the login fails, log in with the account that has administrator privileges and reconfigure the account settings. If the login fails even with the account that has administrator privileges, press and hold the reset button for five seconds to reset the settings to default.

Time stamp does not match with peripherals

Cause	Corrective action
The time zone is incorrectly specified.	Check and correct the time zone setting so that it matches the time zone setting of the peripherals.

USB flash drive is not recognized

Cause	Corrective action
The USB flash drive is not a connectable type.	Use a connectable USB flash drive.
A USB flash drive error has occurred.	Check the USB flash drive and replace it.
The USB port is disabled.	Enable the USB port.
The firmware version of the managed switch is "04" or earlier.	Update the firmware version of the managed switch to "05" or later.

Configuration automatic restoration fails

Cause	Corrective action
No restorable configuration file can be detected.	Use the configuration file backed up with the same model name and firmware version. Check that the configuration file with a restorable file name is saved in the specified folder in the USB flash drive.
The USB flash drive has been formatted for an unsupported file system.	Use a USB flash drive that is formatted in the FAT or FAT32 format.

Backup of files to USB flash drive fails

Cause	Corrective action
The USB flash drive does not have sufficient free space.	Secure sufficient free space in the USB flash drive.
The USB flash drive has been formatted for an unsupported file system.	Use a USB flash drive that is formatted in the FAT or FAT32 format.

10.3 Error Message List

The following table lists error messages displayed on the web interface.

Window	Indication content	Corrective action
IP Configuration	Invalid: Invalid IPv4 Management Address {ipAddress}/{netmask}	Do not set the IP address out of the setting range or any special IP address.
	Invalid: DNS Server {dnsServer} is not reachable.	If the default gateway is not set, set the IP address such that the network part of the managed switch matches the network part of the DNS server.
	Invalid: Gateway {gateway'} is not reachable.	Set the IP address such that the network part of the managed switch matches the network part of the gateway.
	Invalid: Invalid global unicast address prefix {prefix}/{prefix length}	Set the following parameter in the format defined in the RFC 2373. • IPv6 Global Unicast Address Prefix (Prefix Length: 64 bits) Default Gateway
IEEE 802.1Q	Invalid: Default VLAN 1 cannot be deleted.	VLAN 1 cannot be deleted.
	Invalid: The interface should be the member of VLAN ID in static unicast MAC address entry.	Set the port and VLAN ID such that the integrity with the static unicast registration can be secured. (☞ Page 166 Setting method)
	Invalid: The interface should be the member of VLAN ID in static multicast MAC address entry.	Set the port and VLAN ID such that the integrity with the multicast can be secured. (☞ Page 170 Setting method)
Time-Aware Shaper	Invalid: cycle time cannot over 999,999,999 nsec	Set the total interval time of each slot such that it does not exceed 999999999 nanoseconds.
Priority Management	Invalid: IEEE Std. 802.1AS messages (EtherType = 0x88F7) use default traffic	Setting is not allowed because the PCP is fixed to 6 for IEEE Std. 802.1AS messages (EtherType = 0x88F7).

If an error message other than above is displayed, take corrective actions according to the error message.

APPENDICES

Appendix 1 Command Line Interface Commands

This section lists the Command Line Interface commands.

List of commands

The following table lists the list of commands.

System management [System Management]

Function	Command name	Description	Reference
Device information setting [Information Setting]	Configure Device Hostname	Sets the device name of the managed switch.	Page 274 Configure Device Hostname
	Configure Device Description	Sets the detailed description of the managed switch.	Page 274 Configure Device Description
	Configure Contact Information	Sets the contact information of the managed switch.	Page 275 Configure Contact Information
	Configure Location Information	Sets the location where the managed switch is used.	Page 275 Configure Location Information
	Show System Information	Shows the device information of the managed switch.	Page 276 Show System Information
Firmware upgrade function [Firmware Upgrade]	Upgrade the Firmware	Updates the firmware version of the managed switch.	Page 276 Upgrade the Firmware
Configuration backup and restoration [Config Backup and Restore]	Copy Running Configuration	Backs up or restores the running configuration.	Page 277 Copy Running Configuration
	Copy Startup Configuration	Backs up or restores the startup configuration.	Page 278 Copy Startup Configuration
	Configure Auto Restore Configuration[*1]	Enables or disables configuration automatic restoration.	Page 278 Configure Auto Restore Configuration
	Show External Storage Information[*1]	Shows the backup and restoration function settings that use a USB flash drive.	Page 279 Show External Storage Information

[*1] This command can be used with firmware version "05" or later.

Account management [Account Management]

Function	Command name	Description	Reference
User account setting function [User Account]	Configure User Account Setting	Sets the user account.	Page 280 Configure User Account Setting
	Show User Information	Shows the user account information registered in the managed switch.	Page 281 Show User Information
Password policy [Password Policy]	Configure Password Maximum Lifetime	Sets the expiration date for the password.	Page 281 Configure Password Maximum Lifetime
	Configure Password Validation Rules	Sets the input rules for the password.	Page 282 Configure Password Validation Rules
	Configure Password Minimum Length	Sets the minimum number of characters for the password.	Page 282 Configure Password Minimum Length
	Show Password Minimum Length	Shows the minimum number of characters for the password.	Page 283 Show Password Minimum Length
	Show Password Validation Rules	Shows the input rules for the password.	Page 283 Show Password Validation Rules

Network [Network]

Function	Command name	Description	Reference
IP configuration [IP Configuration]	Configure IP Management Address	Sets the IP address and other items of the managed switch.	Page 284 Configure IP Management Address
DHCP server [DHCP Server]	Show IP DHCP	Shows the DHCP settings.	Page 284 Show IP DHCP
	Configure/Disable DHCP Server Mode	Enables or disables DHCP.	Page 285 Configure/Disable DHCP Server Mode
	Enable/Disable IP DHCP Pool	Enables or disables the IP address pool of DHCP.	Page 285 Enable/Disable IP DHCP Pool
	Remove IP DHCP Pool	Removes the IP address pool of DHCP.	Page 286 Remove IP DHCP Pool
	Enable/Disable IP DHCP Static Pool	Enables or disables the allocation setting for each MAC address.	Page 286 Enable/Disable IP DHCP Static Pool
	Remove IP DHCP Static Pool	Removes the allocation setting for each MAC address.	Page 287 Remove IP DHCP Static Pool
	Configure DHCP Server Pool*1	Sets the IP address pool of DHCP.	Page 287 Configure DHCP Server Pool
	Configure DHCP Server Host IP Address*2	Sets the IP address for allocation of each MAC address.	Page 288 Configure DHCP Server Host IP Address
	Configure DHCP Server Host MAC Address*2	Sets the MAC address for allocation of each MAC address.	Page 288 Configure DHCP Server Host MAC Address
	Configure Lease Time*1	Sets the lease time of the IP address.	Page 288 Configure Lease Time
	Reset Lease time*1	Resets the lease time of the IP address.	Page 289 Reset Lease time
	Configure Default Router IP Address*1*2	Sets the IP address of the default gateway to be used by the client.	Page 289 Configure Default Router IP Address
	Remove Default Router IP Address*1*2	Removes the IP address of the default gateway to be used by the client.	Page 289 Remove Default Router IP Address
	Configure DNS Server IP Address*1*2	Sets the IP address of the DNS server to be used by the client.	Page 290 Configure DNS Server IP Address
	Remove DNS Server IP Address*1*2	Removes the IP address of the DNS server to be used by the client.	Page 290 Remove DNS Server IP Address
	Configure NTP Server IP Address*1*2	Sets the IP address of the NTP server to be used by the client.	Page 290 Configure NTP Server IP Address
	Remove NTP Server IP Address*1*2	Removes the IP address of the NTP server to be used by the client.	Page 291 Remove NTP Server IP Address

*1 Available when the Enable/Disable IP DHCP Pool command is used.

*2 Available when the Enable/Disable IP DHCP Static Pool command is used.

Time [Time]

Function	Command name	Description	Reference
Time zone [Time Zone]	Configure Clock Time Zone	Sets the time zone of the managed switch.	Page 292 Configure Clock Time Zone
System time setting [System Time]	Configure Clock Source	Sets the time acquisition method for the managed switch.	Page 293 Configure Clock Source
	Configure Clock Setting	Sets the local time setting.	Page 293 Configure Clock Setting
	Enable Clock Summer Time	Enables the summer time.	Page 294 Enable Clock Summer Time
	Disable Clock Summer Time	Disables the summer time.	Page 294 Disable Clock Summer Time
	Configure Clock Summertime Start Date	Sets the start time of the summer time.	Page 295 Configure Clock Summertime Start Date
	Configure Clock Summertime End Date	Sets the end time of the summer time.	Page 295 Configure Clock Summertime End Date
	Configure Clock Summertime Offset	Sets the offset to be applied during the summer time.	Page 296 Configure Clock Summertime Offset
	Configure NTP Authentication Key	Sets the NTP authentication key.	Page 296 Configure NTP Authentication Key
	Configure NTP Remote Server	Sets the IP address and authentication key to be used for connection to the NTP server.	Page 297 Configure NTP Remote Server
	Configure SNTP Remote Server	Sets the IP address to be used for connection to the SNTP server.	Page 297 Configure SNTP Remote Server
	Enable NTP Server	Enables the NTP server function.	Page 298 Enable NTP Server
	Disable NTP Server	Disables the NTP server function.	Page 298 Disable NTP Server
	Configure NTP Server Authentication	Sets the authentication key for the NTP server function.	Page 298 Configure NTP Server Authentication
	Disable NTP Server Authentication	Disables the authentication of the NTP server function.	Page 299 Disable NTP Server Authentication
	Show Clock Information	Shows the clock data of the managed switch.	Page 299 Show Clock Information

Function	Command name	Description	Reference
Time synchronization function [Time Synchronization]	Show Time Synchronization Global Information	Shows the time synchronization information of IEEE 802.1AS.	Page 299 Show Time Synchronization Global Information
	Show 802.1AS gPTP Clock Information	Shows the detailed time synchronization information of IEEE 802.1AS.	Page 300 Show 802.1AS gPTP Clock Information
	Show 802.1AS gPTP Profile and Parent Property	Shows the time synchronization information related to the grandmaster of IEEE 802.1AS.	Page 300 Show 802.1AS gPTP Profile and Parent Property
	Show gPTP Port Profile	Shows the time synchronization information of IEEE 802.1AS for each port.	Page 300 Show gPTP Port Profile
	Enable/disable Time Synchronization Function	Enables or disables the time synchronization function.	Page 301 Enable/disable Time Synchronization Function
	Configure 802.1AS gPTP Priority 1 and Priority 2	Sets the priority of IEEE 802.1AS.	Page 302 Configure 802.1AS gPTP Priority 1 and Priority 2
	Configure 802.1AS gPTP Profile Default	Enables IEEE 802.1AS.	Page 303 Configure 802.1AS gPTP Profile Default
	Configure 802.1AS gPTP Message Interval	Sets the IEEE 802.1AS communication interval for each port.	Page 303 Configure 802.1AS gPTP Message Interval
	Configure 802.1AS gPTP Timeout	Sets the timeout count of IEEE 802.1AS for each port.	Page 304 Configure 802.1AS gPTP Timeout
	Configure 802.1AS gPTP Neighbor Propagation Delay Threshold	Sets the threshold value of the IEEE 802.1AS neighbor propagation delay for each port.	Page 304 Configure 802.1AS gPTP Neighbor Propagation Delay Threshold
	Show IEEE1588 PTP Profile Default Clock	Shows the detailed time synchronization information of IEEE 1588.	Page 305 Show IEEE1588 PTP Profile Default Clock
	Show IEEE1588 PTP Profile Default Parent Information	Shows the time synchronization information related to the grandmaster of IEEE 1588.	Page 305 Show IEEE1588 PTP Profile Default Parent Information
	Show IEEE1588 PTP Profile Default Port	Shows the time synchronization information of IEEE 1588 for each port.	Page 306 Show IEEE1588 PTP Profile Default Port
	Configure IEEE1588 PTP Profile Default Mode	Sets the clock type of IEEE 1588.	Page 306 Configure IEEE1588 PTP Profile Default Mode
	Configure IEEE1588 PTP Profile Default Priority1	Sets priority 1 of IEEE 1588.	Page 307 Configure IEEE1588 PTP Profile Default Priority1
	Configure IEEE1588 PTP Profile Default Priority2	Sets priority 2 of IEEE 1588.	Page 307 Configure IEEE1588 PTP Profile Default Priority2
	Configure IEEE1588 PTP Profile Default Domain	Sets the domain of IEEE 1588.	Page 308 Configure IEEE1588 PTP Profile Default Domain
	Configure IEEE1588 PTP Profile Default Network-Transport	Sets the communication mode of IEEE 1588.	Page 308 Configure IEEE1588 PTP Profile Default Network-Transport
	Configure IEEE1588 PTP Profile Default	Enables IEEE 1588.	Page 309 Configure IEEE1588 PTP Profile Default
	Configure IEEE1588 PTP Profile Default Announcement Interval	Sets the transmission interval of the IEEE 1588 Announce frame for each port.	Page 309 Configure IEEE1588 PTP Profile Default Announcement Interval
	Configure IEEE1588 PTP Profile Default Synchronization Interval	Sets the Sync interval of IEEE 1588 for each port.	Page 310 Configure IEEE1588 PTP Profile Default Synchronization Interval
	Configure IEEE1588 PTP Profile Default Delay Request Interval	Sets the Delay-Req interval of IEEE 1588 for each port.	Page 310 Configure IEEE1588 PTP Profile Default Delay Request Interval
	Configure IEEE1588 PTP Profile Default Pdelay Request Interval	Sets the PDelay-Req interval of IEEE 1588 for each port.	Page 311 Configure IEEE1588 PTP Profile Default Pdelay Request Interval

Port interface [Port Interface]

Function	Command name	Description	Reference
Port setting [Port Setting]	Show Interface Status	Shows the port status.	Page 312 Show Interface Status
	Show Interface Type and ID	Shows the detailed port information for each port.	Page 312 Show Interface Type and ID
	Show Interface Description	Shows the remarks of the port.	Page 313 Show Interface Description
	Configure Shutdown Settings	Sets the port to the shutdown state.	Page 313 Configure Shutdown Settings
	Configure Description Settings	Sets the remarks of the port.	Page 313 Configure Description Settings
	Configure Duplex Settings	Sets the port to full-duplex or half-duplex.	Page 314 Configure Duplex Settings
	Configure Speed Settings	Sets the communication speed of the port.	Page 314 Configure Speed Settings
	Configure mdix Setting	Sets the port type.	Page 315 Configure mdix Setting
	Configure Auto-Negotiation Setting	Sets the auto-negotiation of the port.	Page 315 Configure Auto-Negotiation Setting

Layer 2 switching function [Layer 2 Switching]

Function	Command name	Description	Reference
VLAN function [VLAN]	Show VLAN Interface Status	Shows the VLAN information of the port.	Page 316 Show VLAN Interface Status
	Show VLAN Port Configuration	Shows the VLAN setting for the port.	Page 316 Show VLAN Port Configuration
	Show VLAN Management	Shows the management VLAN.	Page 317 Show VLAN Management
	Create/Delete a VLAN	Creates or deletes a VLAN.	Page 317 Create/Delete a VLAN
	Configure VLAN Name[*1]	Sets the name to the VLAN.	Page 318 Configure VLAN Name
	Configure VLAN Mode Member Ports[*1]	Sets the port that is assigned to the VLAN.	Page 318 Configure VLAN Mode Member Ports
	Configure PVID on a Specified Port	Sets PVID.	Page 319 Configure PVID on a Specified Port
	Configure Switch Port Operation Mode	Sets the VLAN port mode.	Page 320 Configure Switch Port Operation Mode
	Set VLAN Access Port	Sets the port as the access port.	Page 321 Set VLAN Access Port
	Configure VLAN Management	Sets the management VLAN.	Page 321 Configure VLAN Management
Priority management function [Priority Management]	Show Stream Adapter Information	Shows the priority per stream.	Page 322 Show Stream Adapter Information
	Configure Stream Adapter Rules	Sets the priority per stream.	Page 322 Configure Stream Adapter Rules
	Remove Stream Adapter Rules	Removes the priority per stream.	Page 323 Remove Stream Adapter Rules
	Enable Stream Adapter Egress Untag	Enables the untagged output.	Page 323 Enable Stream Adapter Egress Untag
	Disable Stream Adapter Egress Untag	Disables the untagged output.	Page 323 Disable Stream Adapter Egress Untag
MAC address table [MAC Address Table]	Configure a Static Unicast MAC Address in the Forwarding Database	Registers a static unicast MAC address to the MAC address table.	Page 324 Configure a Static Unicast MAC Address in the Forwarding Database
	Configure MAC Address Table Aging Time	Sets the MAC address table aging time.	Page 324 Configure MAC Address Table Aging Time
	Show MAC Address Table Information	Shows the information related to the MAC address table.	Page 325 Show MAC Address Table Information
Multicast setting function [Multicast]	Show MAC Address Table for Static Multicast	Shows the static multicast MAC address.	Page 326 Show MAC Address Table for Static Multicast
	Configure MAC Address Table for Static Multicast	Sets a static multicast MAC address.	Page 326 Configure MAC Address Table for Static Multicast

Function	Command name	Description	Reference
Time-sharing communications [Time-aware Shaper]	Show 802.1Qbv Information	Shows the information related to IEEE 802.1Qbv.	Page 327 Show 802.1Qbv Information
	Show 802.1Qbv Operative Information	Shows the IEEE 802.1Qbv operational information.	Page 327 Show 802.1Qbv Operative Information
	Enable/Disable 802.1Qbv Function	Enables or disables IEEE 802.1Qbv.	Page 328 Enable/Disable 802.1Qbv Function
	Configure 802.1Qbv Config-change Operation	Reflects the IEEE 802.1Qbv setting to the operation.	Page 328 Configure 802.1Qbv Config-change Operation
	Append 802.1Qbv Control List	Appends the IEEE 802.1Qbv control list.	Page 329 Append 802.1Qbv Control List
	Remove 802.1Qbv Control List	Removes the IEEE 802.1Qbv control list.	Page 329 Remove 802.1Qbv Control List
	Set 802.1Qbv Control List	Edits the IEEE 802.1Qbv control list.	Page 330 Set 802.1Qbv Control List
	Configure 802.1Qbv Cycle Time	Sets the IEEE 802.1Qbv communication cycle.	Page 330 Configure 802.1Qbv Cycle Time

*1 Available when the Create/Delete a VLAN command is used.

Layer 2 redundancy function [Layer 2 Redundancy]

Function	Command name	Description	Reference
Spanning tree function [Spanning Tree]	Configure Spanning Tree Compatibility	Sets the compatibility of STP.	Page 331 Configure Spanning Tree Compatibility
	Configure Spanning Tree Priority	Sets the priority of STP.	Page 331 Configure Spanning Tree Priority
	Configure Spanning Tree Forward Time	Sets the Forward Time of STP.	Page 332 Configure Spanning Tree Forward Time
	Configure Spanning Tree Hello Time	Sets the Hello Time of STP.	Page 332 Configure Spanning Tree Hello Time
	Configure Spanning Tree Maximum Age	Sets the Maximum Age of STP.	Page 333 Configure Spanning Tree Maximum Age
	Configure Spanning Tree Auto-edge	Automatically sets the port type.	Page 333 Configure Spanning Tree Auto-edge
	Configure Spanning Tree Cost	Sets the port cost.	Page 334 Configure Spanning Tree Cost
	Configure Spanning Tree Link Type	Sets the port link type.	Page 334 Configure Spanning Tree Link Type
	Configure Spanning Tree Portfast	Manually sets the port type.	Page 335 Configure Spanning Tree Portfast
	Configure Spanning Tree Port Priority	Sets the priority of the port.	Page 335 Configure Spanning Tree Port Priority
	Show Spanning Tree Bridge Information	Shows the information of the managed switch.	Page 336 Show Spanning Tree Bridge Information
	Show Spanning Tree Root Information	Shows the information of the root bridge.	Page 336 Show Spanning Tree Root Information
	Show Spanning Tree Interface Information	Shows the information of each port of the managed switch.	Page 337 Show Spanning Tree Interface Information
	Show Spanning Tree Details	Shows the detailed STP information.	Page 338 Show Spanning Tree Details

Network management [Network Management]

Function	Command name	Description	Reference
SNMP[SNMP]	Show SNMP Server Information	Shows the SNMP server information.	Page 338 Show SNMP Server Information
	Show SNMP Server User Account Information	Shows the SNMP user account information.	Page 338 Show SNMP Server User Account Information
	Configure SNMP Server Access Mode	Sets the access mode to the SNMP agent.	Page 339 Configure SNMP Server Access Mode
	Configure SNMP Server Read-Only Community Settings	Sets the community string for read-only access.	Page 339 Configure SNMP Server Read-Only Community Settings
	Configure SNMP Server Read-Only Community to Default Value	Resets the community string for read-only access to default.	Page 340 Configure SNMP Server Read-Only Community to Default Value
	Configure SNMP Server Read-Write Community Settings	Sets the community string for read/write access.	Page 340 Configure SNMP Server Read-Write Community Settings
	Configure SNMP Server Read-Write Community to Default Value	Resets the community string for read/write access to default.	Page 341 Configure SNMP Server Read-Write Community to Default Value
	Configure SNMP Server Version	Sets the SNMP version.	Page 341 Configure SNMP Server Version
	Configure SNMP Server Version to Default Value	Resets the SNMP version to default.	Page 342 Configure SNMP Server Version to Default Value
	Configure SNMP Server User Account Settings	Sets the user account with which to access the SNMP agent.	Page 343 Configure SNMP Server User Account Settings
	Delete SNMP Server User Account	Deletes the user account with which to the SNMP agent.	Page 344 Delete SNMP Server User Account
	Show SNMP Trap Information	Shows the SNMP Trap information.	Page 344 Show SNMP Trap Information
	Show SNMP Trap User Account Information	Shows the SNMP Trap user account information.	Page 345 Show SNMP Trap User Account Information
	Show SNMP Trap Host Information	Shows the host setting for SNMP Trap.	Page 345 Show SNMP Trap Host Information
	Configure SNMP Trap Host Settings	Sets the host of SNMP Trap.	Page 346 Configure SNMP Trap Host Settings
	Delete SNMP Trap Host Entry	Deletes the host setting for SNMP Trap.	Page 347 Delete SNMP Trap Host Entry
	Configure SNMP Trap Inform Retry Setting	Sets the retry count for SNMP Trap/Inform.	Page 347 Configure SNMP Trap Inform Retry Setting
	Reset SNMP Trap Inform Retry to Default Value	Resets the retry count of SNMP Trap/Inform to default.	Page 348 Reset SNMP Trap Inform Retry to Default Value
	Configure SNMP Trap Inform Timeout Setting	Sets the timeout count of SNMP Trap/Inform.	Page 348 Configure SNMP Trap Inform Timeout Setting
	Reset SNMP Trap Inform Timeout to Default Value	Resets the timeout count of SNMP Trap/Inform to default.	Page 348 Reset SNMP Trap Inform Timeout to Default Value
	Configure SNMP Trap User Account Settings	Sets the SNMP Trap user account.	Page 349 Configure SNMP Trap User Account Settings
	Delete SNMP Trap User Account	Deletes the SNMP Trap user account.	Page 350 Delete SNMP Trap User Account

Device security function [Device Security]

Function	Command name	Description	Reference
Interface management function [Management Interface]	Enable Network Server	Enables the managed switch interface.	Page 350 Enable Network Server
	Disable Network Server	Disables the managed switch interface.	Page 351 Disable Network Server
	Configure Network Port Numbers	Sets the port number of the interface.	Page 352 Configure Network Port Numbers
	Configure SNMP Server Port Number	Sets the port number to be used in SNMP.	Page 352 Configure SNMP Server Port Number
	Configure SNMP Server Transport Protocol Mode	Sets the predefined protocol to be used in SNMP.	Page 353 Configure SNMP Server Transport Protocol Mode
	Configure Network Maximum Session Numbers	Sets the maximum number of concurrent connections to the web interface.	Page 353 Configure Network Maximum Session Numbers
	Configure Network Terminal Maximum Session Numbers	Sets the maximum number of concurrent connections to the CLI.	Page 354 Configure Network Terminal Maximum Session Numbers
	Show Network Service Information	Shows the interface information.	Page 354 Show Network Service Information
	Configure Hardware Interface[*1]	Enables or disables the USB port.	Page 355 Configure Hardware Interface
	Show Hardware Interface Information[*1]	Shows the USB port settings.	Page 355 Show Hardware Interface Information
Login policy [Login Policy]	Configure Login Lockout Settings	Sets the items related to lockout.	Page 356 Configure Login Lockout Settings
	Configure Login Banner	Sets the login message.	Page 356 Configure Login Banner
	Configure Login Failure Message	Sets the login failure message.	Page 357 Configure Login Failure Message
	Configure Timeout Value for a Session End	Sets the items related to auto-logout.	Page 357 Configure Timeout Value for a Session End
	Show Session Timeout Information	Shows the auto-logout setting.	Page 358 Show Session Timeout Information
	Show Login Failure Message	Shows the login failure message.	Page 358 Show Login Failure Message
	Show Login Banner	Shows the login message.	Page 358 Show Login Banner
Access permitted function [Trusted Access]	Configure Trusted Access Settings	Sets the IP address to which access is permitted.	Page 359 Configure Trusted Access Settings
	Enable/Disable IP Trusted Access List	Enables or disables the access permitted function.	Page 359 Enable/Disable IP Trusted Access List
	Show Trusted Access IP List	Shows the IP address to which access is permitted.	Page 360 Show Trusted Access IP List
SSH[SSH]	Re-generate New SSH Key	Regenerates the key to be used for encryption.	Page 360 Re-generate New SSH Key
SSL[SSL]	Re-generate New Web SSL Certificate	Regenerates the SSL certificate.	Page 360 Re-generate New Web SSL Certificate
	Import New Web SSL Certificate via TFTP or SFTP	Imports the SSL certificate.	Page 361 Import New Web SSL Certificate via TFTP or SFTP
	Export Web SSL Certificate Signing Request via TFTP/SFTP	Outputs the CSR file.	Page 361 Export Web SSL Certificate Signing Request via TFTP/SFTP

[*1] This command can be used with firmware version "05" or later.

Network security function [Network Security]

Function	Command name	Description	Reference
Traffic control function [Traffic Storm Control]	Enable/Disable Storm Control	Sets the send/receive control.	Page 362 Enable/Disable Storm Control
	Show Storm Control Status	Shows the send/receive control setting.	Page 363 Show Storm Control Status

Authentication method [Authentication]

Function	Command name	Description	Reference
Login authentication method [Login Authentication]	Show Login Authentication	Shows the login authentication method.	Page 363 Show Login Authentication
	Configure Login Authentication Settings	Sets the login authentication method.	Page 364 Configure Login Authentication Settings
RADIUS[RADIUS]	Configure RADIUS Server Host Settings	Sets the RADIUS server to be connected.	Page 365 Configure RADIUS Server Host Settings
	Show RADIUS Server Information	Shows the RADIUS server to be connected.	Page 365 Show RADIUS Server Information
TACACS+[TACACS+]	Configure TACACS+ Server Host Settings	Sets the TACACS+ server to be connected.	Page 366 Configure TACACS+ Server Host Settings
	Show TACACS+ Server Information	Shows the TACACS+ server to be connected.	Page 366 Show TACACS+ Server Information

System status check [System Status]

Function	Command name	Description	Reference
System utilization [Utilization]	Show Device Current Information	Shows the current system utilization of the managed switch.	Page 367 Show Device Current Information
Statistical information [Statistics]	Show Traffic Statistics	Shows the statistical information.	Page 367 Show Traffic Statistics
	Clear Traffic Statistics	Clears the statistical information.	Page 368 Clear Traffic Statistics

Event notification [Event Notification]

Function	Command name	Description	Reference
Event notification function [Event Notification]	Show Event Notification	Shows the event notification settings.	Page 368 Show Event Notification
	Configure Event Notification Settings	Sets the events related to the system that provides notifications.	Page 369 Configure Event Notification Settings
	Configure Notification for Switching Event Settings	Sets the events related to the relay that provides notifications.	Page 370 Configure Notification for Switching Event Settings
Relay alarm cut-off [Relay Alarm Cut-off]	Configure Relay Alarm Cut-off Settings	Cuts off the relay alarm.	Page 371 Configure Relay Alarm Cut-off Settings
Email notification function [Email Notification]	Configure Email Notification Server	Sets the SMTP server to be used for email notifications.	Page 371 Configure Email Notification Server
	Configure Email Notification Sender	Sets the email address of the managed switch.	Page 372 Configure Email Notification Sender
	Configure Email Notification Server TLS Mode Setting	Enables or disables TLS at email transmission.	Page 372 Configure Email Notification Server TLS Mode Setting
	Configure Email Notification Receiver	Sets the email address at which email notifications are to be received.	Page 373 Configure Email Notification Receiver
	Show Email Notification Server	Shows the SMTP server to be used for email notifications.	Page 373 Show Email Notification Server
Syslog function [Syslog]	Configure Logging Server	Sets the Syslog server of the save destination.	Page 374 Configure Logging Server
	Delete Logging Server	Deletes the Syslog server of the save destination.	Page 374 Delete Logging Server
	Enable/Disable Logging Syslog Server	Enables or disables log saving to the Syslog server.	Page 375 Enable/Disable Logging Syslog Server
	Show Syslog Server Configuration	Shows the Syslog server of the save destination.	Page 375 Show Syslog Server Configuration

Diagnostic function [Diagnosis]

Function	Command name	Description	Reference
LLDP[LLDP]	Show LLDP Information	Shows the LLDP information.	Page 375 Show LLDP Information
	Show LLDP Neighbors	Shows the information related to neighboring devices.	Page 376 Show LLDP Neighbors
	Show LLDP Traffic	Shows the statistical information of LLDP communications.	Page 376 Show LLDP Traffic
	Enable/Disable LLDP Function	Enables or disables LLDP.	Page 377 Enable/Disable LLDP Function
	Configure Global LLDP Transmission Timer Interval	Sets the transmission interval of the LLDP messages.	Page 377 Configure Global LLDP Transmission Timer Interval
	Configure LLDP Holdtime Multiplier	Sets the information hold time at the neighboring devices.	Page 378 Configure LLDP Holdtime Multiplier
Ping[Ping]	Ping the Host	Executes a ping test.	Page 378 Ping the Host
ARP table [ARP Table]	Show IP ARP Table	Shows the ARP table.	Page 379 Show IP ARP Table
Event log [Event Log]	Show Logging Event Log	Shows the event logs.	Page 379 Show Logging Event Log
	Show Logging Log Capacity	Shows the threshold value by which to perform event notification.	Page 379 Show Logging Log Capacity
	Clear Logging Event Log	Clears all the event logs.	Page 380 Clear Logging Event Log
	Export Event Log File	Outputs the event logs.	Page 380 Export Event Log File
	Configure Event Log Capacity Settings	Sets the threshold value by which to perform event notification.	Page 381 Configure Event Log Capacity Settings
	Delete Logging Log Capacity Threshold	Deletes the threshold value by which to perform event notification.	Page 381 Delete Logging Log Capacity Threshold
	Configure Oversized Log Action Setting	Sets the event to be notified when the threshold value is exceeded.	Page 382 Configure Oversized Log Action Setting
	Configure Auto Backup Event Log[*1]	Enables or disables event log automatic backup.	Page 382 Configure Auto Backup Event Log

[*1] This command can be used with firmware version "05" or later.

Maintenance and tool [Maintenance and Tool]

Function	Command name	Description	Reference
Location check function [Locator]	Show the Locator	Flashes the LEDs of the managed switch.	Page 383 Show the Locator
Reboot function [Reboot]	Reboot the Switch	Restarts the managed switch.	Page 383 Reboot the Switch
Configuration initializing function [Reset to default]	Reset to Default	Resets the managed switch settings to default.	Page 384 Reset to Default
Logout [Logout]	Logout	Logs out the user from the managed switch.	Page 384 Logout

Commands

Command mode

The managed switch has multiple command modes. The following table lists the overview of the command modes and their switching methods.

Command mode	Description	Mode switching	Mode checking method
User EXEC	Allows the status of the managed switch to be checked.	Log in with the account that has user privileges.	melsec>
Privileged EXEC	Allows some commands to be executed.	Log in with the account that has administrator privileges.	melsec#
Global configuration	Allows parameters to be set.	While the command mode is "Privileged EXEC", input "!" or "configure".	melsec (config)#
Interface configuration	Allows parameters to be set for each port.	While the command mode is "Global configuration", input "interface ethernet 1/<port number>".	melsec (config-if)#

Input the "exit" command to move to the previous command mode. (When the command mode is User EXEC or Privileged EXEC, the "exit" command logs out the user from the managed switch.)

How to save the configuration

To save the running configuration as the startup configuration, use the following command.
"copy running-config startup-config"

Help command

Input the help command ("?") to display the list of commands that can be input. If the help command is input in the middle of command input, a list of commands that can be entered from the middle of input will be displayed.

Precautions

Among the displayed command names, the commands not described in this manual are not supported.

Details of commands

This section describes the details of the commands for the managed switch.

Configure Device Hostname

This command sets the device name of the managed switch.

■Command

- hostname <device-name(64)>
- no hostname

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	hostname	Configure the device hostname parameters
	device-name	The hostname of the device consisting of lower case letters, numbers, and hyphens
Defaults	hostname: melsec	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# hostname device-name device-name(config)# no hostname melsec(config)#	
Error Messages	—	
Related Commands	—	

Configure Device Description

This command sets the detailed description of the managed switch.

■Command

- description <text(255)>
- no description

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	description	Configure the device description parameters
	text	The description of the device
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# description "description data" melsec(config)# no description	
Error Messages	—	
Related Commands	—	

Configure Contact Information

This command sets the contact information of the managed switch.

■Command

- contact <text(255)>
- no contact

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	contact	Configure device contact information
	text	The contact information of the device
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# contact "contact info" melsec(config)# no contact	
Error Messages	—	
Related Commands	—	

Configure Location Information

This command sets the location where the managed switch is used.

■Command

- location <text(255)>
- no location

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	location	Configure the device location information
	text	The location information of the device
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# location "location info" melsec(config)# no location	
Error Messages	—	
Related Commands	—	

Show System Information

This command shows the device information of the managed switch.

■Command

show system information

Item	Description	
Syntax Description	show	Display configuration/status information
	system	Display system information
	information	Display system information
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show system information	
Error Messages	—	
Related Commands	—	

Upgrade the Firmware

This command updates the firmware version of the managed switch.

■Command

copy { <tftp_url> | <sftp_url> | <usb:filename>} device-firmware

Item	Description	
Syntax Description	copy	Copy the target file or input
	device-firmware	The system firmware
	tftp_url	The address of the remote TFTP server in the format "tftp://server/filename"
	sftp_url	The address of the remote SFTP server in the format "sftp://username:password@server/filename"
	usb:filename[*1]	File in USB Memory
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	copy tftp://192.168.127.2/FWR_TSN-G5000_v0.1_2019_0904_1452.rom device firmware copy usb:NZ2MHG-TSNT8F2/NZ2MHG-TSNT8F2_05_2022_1223_1008.rom devicefirmware	
Error Messages	Invalid: Firmware verify failed Invalid: File expects [0-9], [a-z], [A-Z], and -. _() Invalid: USB function is disable	
Related Commands	—	

[*1] This command can be used with firmware version "05" or later.

Copy Running Configuration

This command backs up or restores the running configuration.

■Command

- copy running-config { <tftp_url> | <sftp_url > | usb } [included-default] [password <string (60)>]
- copy { <tftp_url> | <sftp_url> | <usb:filename>} running-config [password <string 60>}]

Item	Description	
Syntax Description	copy	Copy the target file or input
	running-config	The running configuration to be copied
	tftp_url	The location of the file to be copied on the remote TFTP server
	sftp_url	The location of the file to be copied on the remote SFTP server
	included-default	Include default configurations in the configuration file
	password	The password for configuration file encryption
	<string (60)>	The length of the password (max. 60 characters)
	usb[*1]	Copy running-config to USB Memory
	usb:filename[*1]	File in USB Memory to be copied
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	copy running-config tftp://192.168.127.2/config.ini included-default password 12345 copy tftp://192.168.127.2 running-config password 12345 copy running-config usb copy usb:NZ2MHG-TSNT8F2/config/Auto-backup_NZ2MHG-TSNT8F2.ini running-config	
Error Messages	Invalid: Not support USB. Invalid: USB function is disable Invalid: USB configuration import failed	
Related Commands	—	

[*1] This command can be used with firmware version "05" or later.

Copy Startup Configuration

This command backs up or restores the startup configuration.

■Command

- copy startup-config { <tftp_url> | <sftp_url> | usb }[included-default] [password <string (60)>]
- copy running-config startup-config

Item	Description	
Syntax Description	copy	Copy the target file or input
	startup-config	The startup configuration to be copied
	running-config	The running configuration to be copied
	tftp_url	The location of the file to be copied on the remote TFTP server
	sftp_url	The location of the file to be copied on the remote SFTP server
	included-default	Include default configurations in the configuration file
	password	The password for configuration file encryption
	<string (60)>	The length of the password (max. 60 characters)
	usb*1	Copy startup-config to USB Memory
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	copy startup-config tftp://192.168.127.2/config.ini included-default password 12345 copy startup-config usb copy running-config usb	
Error Messages	Invalid: Not support USB. Invalid: USB function is disable Invalid: USB configuration import failed	
Related Commands	—	

*1 This command can be used with firmware version "05" or later.

Point

When restoring a configuration from the setting file where the configuration is backed up, restore the configuration by Copy Running Configuration, then execute the copy running-config startup-config command.

Configure Auto Restore Configuration

Enables or disables configuration automatic restoration.

■Command

- auto-restore config {enable | disable}

Item	Description	
Syntax Description	Auto-restore	Auto restore file from external storage
	Config	Configuration file
	enable	Enable setting
	disable	Disable setting
Defaults	enable	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# auto-restore config enable melsec(config)# auto-restore config disable	
Error Messages	—	
Related Commands	—	

Show External Storage Information

Shows the backup and restoration function settings that use a USB flash drive.

■Command

- show external-storage info

Item	Description	
Syntax Description	show	Display configuration information
	external-storage info	Display external storage information
Defaults	—	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec(config)# show external-storage info External Storage info ----------------------------------- Auto-backup event log Enable : YES Auto-restore configuration Enable : YES	
Error Messages	—	
Related Commands	—	

Configure User Account Setting

This command sets the user account.

■Command

- username <username> password <passwd> group { admin | user | supervisor } status { enable | disable } email <email>
- no username username

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	username	Configures username parameters
	username	The username to be used for login
	password	Configures password parameters
	password	The password to be entered by the user
	group	Configures the user privilege level
	group	Valid values are "admin", "supervisor", and "user" "admin" for admin group, "supervisor" for supervisor, and "user" for normal user group
	status	Configures user status parameters
	enable	Enable the user
	disable	Disable the user
	email	Configures the user email
	email	The user's email address
Defaults	username: admin password: admin group: Admin	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	(config)# username testuser password test123 group admin status enable email test@test.com	
Error Messages	% Max User Account Amount Reached % Invalid Username Format % Password doesn't comply with password rules. % Invalid Email Format % Invalid Password Format % User does not exist % At least one admin should be active. % User status cannot be updated by self. % User Deletion Failed % User cannot be disabled by self % User cannot be modified group by self % User cannot be deleted by self	
Related Commands	Show user	

Show User Information

This command shows the user account information registered in the managed switch.

■Command

show user

Item	Description	
Syntax Description	show	Display running information for the function
	user	Display user parameters
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	# show user	
Error Messages	—	
Related Commands	username	

Configure Password Maximum Lifetime

This command sets the expiration date for the password.

■Command

password max-life-time [<days (0-365)>]

Item	Description	
Syntax Description	password	Configure password parameters
	max-life-time	Configure the maximum lifetime of the password
	days	Maximum lifetime in days; a 0 or "no" value means it does not expire
Defaults	0	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec# config melsec(config)# password max-life-time 30 melsec(config)# password max-life-time	
Error Messages	—	
Related Commands	—	

Configure Password Validation Rules

This command sets the input rules for the password.

■Command

password validate-rules [lowercase] [uppercase] [numbers] [symbols]

Item	Description	
Syntax Description	password	Configure password parameters
	validate-rules	Configure validation rules
	lowercase	Configure at least 1 lowercase flag for password validation
	uppercase	Configure at least 1 uppercase flag for password validation
	numbers	Configure at least 1 numbers flag for password validation
	symbols	Configure at least 1 symbols flag for password validation
Defaults	There are no validation rules configured by default	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec# config melsec(config)# password validate-rules lowercase numbers melsec(config)# password validate-rules	
Error Messages	—	
Related Commands	show password validate-rules	

Configure Password Minimum Length

This command sets the minimum number of characters for the password.

■Command

password minimum-length <minimum-len (4-63)>

Item	Description	
Syntax Description	password	Configure password parameters
	minimum-length	Configure the minimum password length
	minimum-len	The minimum password length
Defaults	4	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec# config melsec(config)# password minimum-length 8	
Error Messages	—	
Related Commands	show password minimum-length	

Show Password Minimum Length

This command shows the minimum number of characters for the password.

■Command

show password minimum-length

Item	Description	
Syntax Description	show	Display running information for the function
	password	Display password parameters
	minimum-length	Display the minimum length of the password
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show password minimum-length	
Error Messages	—	
Related Commands	password minimum-length	

Show Password Validation Rules

This command shows the input rules for the password.

■Command

show password validate-rules

Item	Description	
Syntax Description	show	Display running information for the function
	password	Display password parameters
	validate-rules	Display the password validation rules
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show password validate-rules	
Error Messages	—	
Related Commands	password validate-rules	

Configure IP Management Address

This command sets the IP address and other items of the managed switch.

■Command

ip management address { dhcp | ipv4-address ipv4-netmask [ipv4-gateway] }

Item	Description	
Syntax Description	ip	Configure IP parameters
	management	Configure IPv4 management address parameters
	address	Configure the IPv4 management address of the device
	dhcp	Assign the IPv4 address by DHCP
	ipv4-address	The IPv4 address
	ipv4-netmask	The IPv4 subnet mask
	ipv4-gateway	The IPv4 gateway
Defaults	ipv4-address: 192.168.3.252 ipv4-netmask: 255.255.255.0 ipv4-gateway: —	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ip management address dhcp melsec(config)# ip management address 10.1.1.1 255.255.255.0 10.1.1.254	
Error Messages	Invalid: Invalid IPv4 Management Address ipv4-address/ipv4-netmask. Invalid: Gateway ipv4-gateway is not reachable.	
Related Commands	—	

Show IP DHCP

This command shows the DHCP settings.

■Command

show ip dhcp [{ binding | static }]

Item	Description	
Syntax Description	show	Display configuration/status information
	ip	Display IP information
	dhcp	Display DHCP server information
	binding	Display binding information
	static	Display MAC-based IP assignment information
Defaults	—	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show ip dhcp melsec# show ip dhcp binding melsec# show ip dhcp static melsec# show ip dhcp binding	
Error Messages	—	
Related Commands	—	

Configure/Disable DHCP Server Mode

This command enables or disables DHCP.

■Command

- dhcp-server mode disable
- dhcp-server mode dhcp-and-mac-based-ip-assignment

Item	Description	
Syntax Description	dhcp-server	Configure DHCP server parameters
	mode	Configure DHCP server mode parameters
	disable	Disable the DHCP server
	dhcp-and-mac-based-ipassignment	Standard DHCP server and MAC-based DHCP
Defaults	Disable	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# dhcp-server mode disable	
Error Messages	—	
Related Commands	—	

Enable/Disable IP DHCP Pool

This command enables or disables the IP address pool of DHCP.

■Command

ip dhcp pool <integer(1)> [{ enable | disable }]

Item	Description	
Syntax Description	ip	Configure IP parameters
	dhcp	Configure DHCP server parameters
	pool	Configure address pool parameters
	<integer>	Pool number
	enable	Enable the address pool
	disable	Disable the address pool
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# ip dhcp pool 1 enable melsec(dhcp-config)#	
Error Messages	—	
Related Commands	—	

Remove IP DHCP Pool

This command removes the IP address pool of DHCP.

■Command

no ip dhcp pool <integer(1)>

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	ip	Configure IP parameters
	dhcp	Configure DHCP server parameters
	pool	Configure address pool parameters
	<integer>	The address pool number
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# no ip dhcp pool 1	
Error Messages	—	
Related Commands	—	

Enable/Disable IP DHCP Static Pool

This command enables or disables the allocation setting for each MAC address.

■Command

ip dhcp static pool <string (63)> [{ enable | disable }]

Item	Description	
Syntax Description	ip	Configure IP parameters
	dhcp	Configure DHCP server parameters
	static	Configure MAC-based IP assignment parameters
	pool	Configure address pool parameters
	<string (63)>	The client host name (DHCP option 12)
	enable	Enable the address pool
	disable	Enable the address pool
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# ip dhcp static pool host1 enable melsec(dhcp-config)#	
Error Messages	—	
Related Commands	—	

Remove IP DHCP Static Pool

This command removes the allocation setting for each MAC address.

■Command

no ip dhcp static pool <string (63)>

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	ip	Configure IP parameters
	dhcp	Configure DHCP server parameters
	static	Configure MAC-based IP assignment parameters
	pool	Configure address pool parameters
	string (63)	The client host name (DHCP option 12)
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# no ip dhcp static pool host1	
Error Messages	—	
Related Commands	—	

Configure DHCP Server Pool

This command sets the IP address pool of DHCP.

■Command

network <ucast_addr> <ucast_addr> <ip_mask>

Item	Description	
Syntax Description	network	Configure network parameters
	<ucast_addr>	The address pool starting IP address
	<ucast_addr>	The address pool ending IP address
	<ip_mask>	The subnet mask
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# network 192.168.127.10 192.168.127.20 255.255.255.0	
Error Messages	—	
Related Commands	—	

Configure DHCP Server Host IP Address

This command sets the IP address for allocation of each MAC address.

■Command

host <ucast_addr> <ip_mask>

Item	Description	
Syntax Description	host	Configure host parameters
	<ucast_addr>	The unicast IP address
	<ip_mask>	The subnet mask
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# host 192.168.127.100 255.255.255.0	
Error Messages	—	
Related Commands	—	

Configure DHCP Server Host MAC Address

This command sets the MAC address for allocation of each MAC address.

■Command

hardware-address <ucast_mac>

Item	Description	
Syntax Description	hardware-address	Configure the MAC address
	<ucast_mac>	The MAC address
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# hardware-address □□:□□:□□:□□:□□:□□	
Error Messages	—	
Related Commands	—	

Configure Lease Time

This command sets the lease time of the IP address.

■Command

lease <integer (10-604800)>

Item	Description	
Syntax Description	lease	Configure the IP lease duration
	<integer (10-604800)>	The IP lease duration in seconds
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# lease 3600	
Error Messages	—	
Related Commands	—	

Reset Lease time

This command resets the lease time of the IP address.

■Command

no lease

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	lease	Configure the IP lease duration
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# no lease	
Error Messages	—	
Related Commands	—	

Configure Default Router IP Address

This command sets the IP address of the default gateway to be used by the client.

■Command

default-router <ucast_addr>

Item	Description	
Syntax Description	default-router	Configure the default router
	<ucast_addr>	The unicast IP address
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# default-router 192.168.127.254	
Error Messages	—	
Related Commands	—	

Remove Default Router IP Address

This command removes the IP address of the default gateway to be used by the client.

■Command

no default-router

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	default-router	Configure the default router
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# no default-router	
Error Messages	—	
Related Commands	—	

Configure DNS Server IP Address

This command sets the IP address of the DNS server to be used by the client.

■Command

dns-server <ucast_addr> [<ucast_addr>]

Item	Description	
Syntax Description	dns-server	Configure the DNS server
	<ucast_addr>	The unicast IP address
	<ucast_addr>	The unicast IP address
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# dns-server 192.168.127.254 melsec(dhcp-config)# dns-server 192.168.127.251 192.168.127.252	
Error Messages	—	
Related Commands	—	

Remove DNS Server IP Address

This command removes the IP address of the DNS server to be used by the client.

■Command

no dns-server

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	dns-server	Configure the DNS server
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# no dns-server	
Error Messages	—	
Related Commands	—	

Configure NTP Server IP Address

This command sets the IP address of the NTP server to be used by the client.

■Command

ntp-server <ucast_addr>

Item	Description	
Syntax Description	ntp-server	Configure the NTP server
	Configure the NTP server	The unicast IP address
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# ntp-server 192.168.127.254	
Error Messages	—	
Related Commands	—	

Remove NTP Server IP Address

This command removes the IP address of the NTP server to be used by the client.

■Command

no ntp-server

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	ntp-server	Configure the NTP server
Defaults	—	
Command Modes	DHCP Configuration	
Usage Guidelines	—	
Examples	melsec(dhcp-config)# no ntp-server	
Error Messages	—	
Related Commands	—	

Configure Clock Time Zone

This command sets the time zone of the managed switch.

■Command

clock timezone { "-12" | "-11" | "-10" | "-9:30" | "-9" | "-8" | "-7" | "-6" | "-5" | "-4" | "-3:30" | "-3" | "-2" | "-1" | "0" | "1" | "2" | "3" | "3:30" | "4" | "4:30" | "5" | "5:30" | "5:45" | "6" | "6:30" | "7" | "8" | "8:30" | "8:45" | "9" | "9:30" | "10" | "10:30" | "11" | "12" | "12:45" | "13" | "14" }

Item	Description	
Syntax Description	clock	Configure system clock parameters
	timezone	Configure the timezone
	"-12"	UTC-12:00
	"-11"	UTC-11:00
	"-10"	UTC-10:00
	"-9:30"	UTC-09:30
	"-9"	UTC-09:00
	"-8"	UTC-08:00
	"-7"	UTC-07:00
	"-6"	UTC-06:00
	"-5"	UTC-05:00
	"-4"	UTC-04:00
	"-3:30"	UTC-03:30
	"-3"	UTC-03:00
	"-2"	UTC-02:00
	"-1"	UTC-01:00
	"0"	UTC+00:00
	"1"	UTC+01:00
	"2"	UTC+02:00
	"3"	UTC+03:00
	"3:30"	UTC+03:30
	"4"	UTC+04:00
	"4:30"	UTC+04:30
	"5"	UTC+05:00
	"5:30"	UTC+05:30
	"5:45"	UTC+05:45
	"6"	UTC+06:00
	"6:30"	UTC+06:30
	"7"	UTC+07:00
	"8"	UTC+08:00
	"8:30"	UTC+08:30
	"8:45"	UTC+08:45
	"9"	UTC+09:00
	"9:30"	UTC+09:30
	"10"	UTC+10:00
	"10:30"	UTC+10:30
	"11"	UTC+11:00
	"12"	UTC+12:00
	"12:45"	UTC+12:45
	"13"	UTC+13:00
	"14"	UTC+14:00
Defaults	"0"	
Command Modes	Global Configuration	
Usage Guidelines	—	

Item	Description
Examples	melsec# configure terminal melsec(config)# clock timezone "8"
Error Messages	—
Related Commands	—

Configure Clock Source

This command sets the time acquisition method for the managed switch.

■Command

clock source { local | ntp | sntp | ptp}

Item	Description	
Syntax Description	clock	Configure system clock parameters
	source	Configure the source of the system clock
	local	Use the local clock
	ntp	Use Network Time Protocol (NTP)
	sntp	Use Simple Network Time Protocol (SNTP)
	ptp	Use Precision Time Protocol (PTP)
Defaults	clock source: ptp	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# clock source local	
Error Messages	—	
Related Commands	—	

Configure Clock Setting

This command sets the local time setting.

■Command

clock set hh:mm:ss [<month(1-12)>] [<day(1-31)>] [<year(2000-2037)>]

Item	Description	
Syntax Description	clock	Configure system clock parameters
	set	Configure the system time
	hh:mm:ss	The system time in the format hh:mm:ss
	month	The month, January (1) to December (12)
	day	The day of the month (1 to 31)
	year	The year (2000 to 2037)
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# clock set 11:11:11 12 31 2019	
Error Messages	—	
Related Commands	—	

Enable Clock Summer Time

This command enables the summer time.

■Command

clock summer-time enable

Item	Description	
Syntax Description	clock	Configure system clock parameters
	summer-time	Configure Daylight Savings Time parameters
	enable	Enable Daylight Savings Time
Defaults	Daylight saving time is disabled by default	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# clock summer-time enable	
Error Messages	Invalid: The start date plus offset should before the end date.	
Related Commands	—	

Disable Clock Summer Time

This command disables the summer time.

■Command

clock summer-time disable

Item	Description	
Syntax Description	clock	Configure system clock parameters
	summer-time	Configure Daylight Savings Time parameters
	disable	Disable Daylight Savings Time
Defaults	Daylight saving time is disabled by default	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# clock summer-time disable	
Error Messages	—	
Related Commands	—	

Configure Clock Summertime Start Date

This command sets the start time of the summer time.

■Command

clock summer-time start-date <month(1-12)> <day(1-31)> <year(2000-2037)> <hour(0-23)> [<minute(0-59)>]

Item	Description	
Syntax Description	clock	Configure system clock parameters
	summer-time	Configure Daylight Savings Time parameters
	start-date	Configure the start date of Daylight Saving Time
	month	The month, January (1) to December (12)
	day	The day of the month (1 to 31)
	year	The year (2000 to 2037)
	hour	The hour (0 to 23)
	minute	The minutes (0 to 59)
Defaults	The daylight saving time start date is set to Jan 01 2000 00:00	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# clock summer-time start-date 1 1 2019 23 30	
Error Messages	Invalid: Start date is invalid. Invalid: The start date plus offset should before the end date.	
Related Commands	—	

Configure Clock Summertime End Date

This command sets the end time of the summer time.

■Command

clock summer-time end-date <month(1-12)> <day(1-31)> <year(2000-2037)> <hour(0-23)> [<minute(0-59)>]

Item	Description	
Syntax Description	clock	Configure system clock parameters
	summer-time	Configure Daylight Savings Time parameters
	end-date	Configure the end date of Daylight Savings Time
	month	The month, January (1) to December (12)
	day	The day of the month (1 to 31)
	year	The year (2000 to 2037)
	hour	The hour (0 to 23)
	minute	The minutes (0 to 59)
Defaults	The daylight saving time end date is set to Dec 31 2000 23:00	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# clock summer-time end-date 7 31 2019 23 30	
Error Messages	Invalid: End date is invalid Invalid: The start date plus offset should before the end date.	
Related Commands	—	

Configure Clock Summertime Offset

This command sets the offset to be applied during the summer time.

■Command

clock summer-time offset <offset-hour(0-24)> [<offset-minute(0-59)>]

Item	Description	
Syntax Description	clock	Configure system clock parameters
	summer-time	Configure Daylight Savings Time parameters
	offset	Configure the offset of Daylight Saving Time
	offset-hour	The time offset hours
	offset-minute	The time offset minutes
Defaults	daylight saving time offset: 0 Hour 0 Minutes	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# clock summer-time offset 1 30	
Error Messages	Invalid: The start date plus offset should before the end date.	
Related Commands	—	

Configure NTP Authentication Key

This command sets the NTP authentication key.

■Command

- ntp authentication-key key-index key-id md5 key-string
- no ntp authentication-key key-index

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	ntp	Configure NTP/SNTP parameters
	authentication-key	Configure the NTP authentication key
	key-index	The index of the key, ranging from 1 to 10
	key-id	The key ID, ranging from 1 to 65535
	md5	Use MD5 authentication
	key-string	The authentication key with a maximum length of 32 characters for plain text
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ntp authentication-key 1 1 md5 1a2b3c4d melsec(config)# no ntp authentication-key 1	
Error Messages	Invalid: Authentication key ID key-id is duplicated.	
Related Commands	—	

Configure NTP Remote Server

This command sets the IP address and authentication key to be used for connection to the NTP server.

■Command

ntp remote-server ntp server-index server-address [authentication key key-id]

Item	Description	
Syntax Description	ntp	Configure NTP/SNTP parameters
	remote-server	Configure remote time server parameters
	ntp	Configure NTP server parameters
	server-index	The index of the server, ranging from 1 to 2
	server-address	The NTP server address
	authentication	Configure NTP authentication parameters
	key	Use key authentication
	key-id	The ID of the authentication key
Defaults	NTP time server: time.nist.gov	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ntp remote-server ntp 1 1.1.1.1 melsec(config)# ntp remote-server ntp 2 2.2.2.2 authentication key 1	
Error Messages	Invalid: Authentication key ID key-id of NTP client server-index does not exist.	
Related Commands	—	

Configure SNTP Remote Server

This command sets the IP address to be used for connection to the SNTP server.

■Command

ntp remote-server sntp server-index server-address

Item	Description	
Syntax Description	ntp	Configure NTP/SNTP parameters
	remote-server	Configure remote time server parameters
	sntp	Configure SNTP server parameters
	server-index	The index of the server, ranging from 1 to 2
	server-address	The SNTP server address
Defaults	The default SNTP time server is set to time.nist.gov	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ntp remote-server sntp 1 1.1.1.1	
Error Messages	—	
Related Commands	—	

Enable NTP Server

This command enables the NTP server function.

■Command

ntp server enable

Item	Description	
Syntax Description	ntp	Configure NTP/SNTP parameters
	server	Configure NTP server parameters
	enable	Enable the NTP server
Defaults	NTP server: disable	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ntp server enable	
Error Messages	—	
Related Commands	—	

Disable NTP Server

This command disables the NTP server function.

■Command

ntp server disable

Item	Description	
Syntax Description	ntp	Configure NTP/SNTP parameters
	server	Configure NTP server parameters
	disable	Disable the NTP server
Defaults	The NTP server is disabled by default	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ntp server disable	
Error Messages	—	
Related Commands	—	

Configure NTP Server Authentication

This command sets the authentication key for the NTP server function.

■Command

ntp server authentication

Item	Description	
Syntax Description	ntp	Configure NTP/SNTP parameters
	server	Configure NTP server parameters
	authentication	Enable authentication
Defaults	NTP server authentication is disabled by default	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ntp server authentication	
Error Messages	—	
Related Commands	—	

Disable NTP Server Authentication

This command disables the authentication of the NTP server function.

■Command

no ntp server authentication

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	ntp	Configure NTP/SNTP parameters
	server	Configure NTP server parameters
	authentication	NTP authentication
Defaults	NTP server authentication is disabled by default	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# no ntp server authentication	
Error Messages	—	
Related Commands	—	

Show Clock Information

This command shows the clock data of the managed switch.

■Command

show clock

Item	Description	
Syntax Description	show	Display the configuration/status information.
	clock	Display the system clock information.
Defaults	—	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show clock	
Error Messages	—	
Related Commands	—	

Show Time Synchronization Global Information

This command shows the time synchronization information of IEEE 802.1AS.

■Command

show ptp

Item	Description	
Syntax Description	ptp	Display PTP status and information
	profile	PTP profile selection
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show ptp	
Error Messages	—	
Related Commands	—	

Show 802.1AS gPTP Clock Information

This command shows the detailed time synchronization information of IEEE 802.1AS.

■Command

show ptp profile dot1as clock

Item	Description	
Syntax Description	ptp	Display PTP status and information
	profile	PTP profile selection
	dot1as	802.1AS profile
	clock	PTP clock information
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show ptp profile dot1as clock	
Error Messages	—	
Related Commands	show ptp profile dot1as parent	

Show 802.1AS gPTP Profile and Parent Property

This command shows the time synchronization information related to the grandmaster of IEEE 802.1AS.

■Command

show ptp profile dot1as parent

Item	Description	
Syntax Description	ptp	Display PTP status and information
	profile	PTP profile selection
	dot1as	802.1AS profile
	parent	PTP parent properties
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show ptp profile dot1as parent	
Error Messages	—	
Related Commands	—	

Show gPTP Port Profile

This command shows the time synchronization information of IEEE 802.1AS for each port.

■Command

show ptp profile dot1as port [<interface-type> <interface-id>]

Item	Description	
Syntax Description	ptp	Display PTP status and information
	profile	PTP profile selection
	dot1as	802.1AS profile
	port	PTP port properties
	<interface-type>	Ethernet (interface-type)
	<interface-id>	Interface-id: <1-X>/<1-Y> Slot Number/Port Number
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show ptp profile dot1as port Ethernet 1/1	
Error Messages	—	
Related Commands	—	

Enable/disable Time Synchronization Function

This command enables or disables the time synchronization function.

■Command

- ptp enable
- ptp disable

Item	Description	
Syntax Description	ptp	Configure the PTP parameters.
	enable	Enable the PTP operation.
	disable	Disable the PTP operation.
Defaults	Enable	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec (config)# ptp enable melsec (config)# ptp disable	
Error Messages	—	
Related Commands	—	

Configure 802.1AS gPTP Priority 1 and Priority 2

This command sets the priority of IEEE 802.1AS.

■Command

- ptp profile dot1as priority1 <value>
- no ptp profile dot1as priority1

Item	Description	
Syntax Description	ptp/no ptp	Configure PTP parameters / Reset to default value
	profile	PTP profile selection
	dot1as	802.1AS profile
	priority1	Priority 1 value used by the BMC algorithm
	<value>	0 to 255
Defaults	246	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# ptp profile dot1as priority1 246 melsec(config)# no ptp profile dot1as priority1	
Error Messages	—	
Related Commands	—	

■Command

- ptp profile dot1as priority2 <value>
- no ptp profile dot1as priority2

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	ptp	Configure PTP parameters
	profile	PTP profile selection
	dot1as	802.1AS profile
	priority2	Priority2 value used by the BMC algorithm
	<value>	0 to 255
Defaults	248	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# ptp profile dot1as priority2 248 melsec(config)# no ptp profile dot1as priority2	
Error Messages	—	
Related Commands	—	

Configure 802.1AS gPTP Profile Default

This command enables IEEE 802.1AS.

■Command

- ptp profile dot1as
- no ptp profile dot1as

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	dot1as	802.1AS profile
Defaults	The port is set to 802.1AS profile by default	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config)# interface Ethernet 1/1 melsec(config-if)# ptp profile dot1as melsec(config-if)# no ptp profile dot1as	
Error Messages	—	
Related Commands	—	

Configure 802.1AS gPTP Message Interval

This command sets the IEEE 802.1AS communication interval for each port.

■Command

- ptp profile dot1as <message> interval <value>
- no ptp profile dot1as <message> interval

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	ptp	Configure PTP parameters
	profile	PTP profile selection
	dot1as	802.1AS profile
	<message>	announce/sync/pdelay-req
	interval	Logarithmic message interval
	<value>	• Announce: 0 to 4 • Sync: -3 to 5 • Pdelay-req: -3 to 5
Defaults	Announce: 0 Sync: -3 Pdelay-req: 0	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config)# interface Ethernet 1/1 melsec(config-if)# ptp profile dot1as announce interval 0 melsec(config-if)# no ptp profile dot1as announce interval melsec(config-if)# ptp profile dot1as sync interval -3 melsec(config-if)# no ptp profile dot1as sync interval melsec(config-if)# ptp profile dot1as pdelay-req interval 0 melsec(config-if)# no ptp profile dot1as pdelay-req interval	
Error Messages	—	
Related Commands	—	

Configure 802.1AS gPTP Timeout

This command sets the timeout count of IEEE 802.1AS for each port.

■Command

- ptp profile dot1as <message> timeout <value>
- no ptp profile dot1as <message> timeout

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	ptp	Configure PTP parameters
	profile	PTP profile selection
	dot1as	802.1AS profile
	<message>	announce/sync
	timeout	Number of intervals without receiving corresponding message.
	<value>	• Announce: 2 to 10 • Sync: 2 to 10
Defaults	Announce: 3 Sync: 3	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	• melsec(config)# interface Ethernet 1/1 • melsec(config-if)# ptp profile dot1as announce timeout 3 • melsec(config-if)# no ptp profile dot1as announce timeout • melsec(config-if)# ptp profile dot1as sync timeout 3 • melsec(config-if)# no ptp profile dot1as sync timeout	
Error Messages	—	
Related Commands	—	

Configure 802.1AS gPTP Neighbor Propagation Delay Threshold

This command sets the threshold value of the IEEE 802.1AS neighbor propagation delay for each port.

■Command

- ptp profile dot1as neighbor-prop-delay-threshold <value(1-10000)>
- no ptp profile dot1as neighbor-prop-delay-threshold

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	ptp	Configure PTP parameters
	profile	PTP profile selection
	dot1as	802.1AS profile
	neighbor-propdelay-threshold	Neighbor propagation delay threshold
	<value>	nanoseconds
Defaults	neighbor-prop-delay-threshold: 3000	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config)# interface Ethernet 1/1 melsec(config-if)# ptp profile dot1as neighbor-prop-delay-threshold 800 melsec(config-if)# no ptp profile dot1as neighbor-prop-delay-threshold	
Error Messages	—	
Related Commands	—	

Show IEEE1588 PTP Profile Default Clock

This command shows the detailed time synchronization information of IEEE 1588.

■Command

show ptp profile default clock

Item	Description	
Syntax Description	ptp	Display PTP status and information
	profile	PTP profile selection
	default	Default profile
	clock	PTP clock information
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show ptp profile default clock	
Error Messages	—	
Related Commands	show ptp profile default parent	

Show IEEE1588 PTP Profile Default Parent Information

This command shows the time synchronization information related to the grandmaster of IEEE 1588.

■Command

show ptp profile default parent

Item	Description	
Syntax Description	ptp	Display PTP status and information
	profile	PTP profile selection
	default	Default profile
	parent	PTP parent properties
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show ptp profile default parent	
Error Messages	—	
Related Commands	—	

Show IEEE1588 PTP Profile Default Port

This command shows the time synchronization information of IEEE 1588 for each port.

■Command

show ptp profile default port [<interface-type> <interface-id>]

Item	Description	
Syntax Description	ptp	Display the PTP status and information.
	profile	The PTP profile selection.
	default	The Default profile.
	port	The PTP port properties.
	<interface-type>	Ethernet (interface-type)
	<interface-id>	Interface-id : <1-X>/<1-Y> Slot Number/Port Number
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show ptp profile default port Ethernet 1/1	
Error Messages	—	
Related Commands	—	

Configure IEEE1588 PTP Profile Default Mode

This command sets the clock type of IEEE 1588.

■Command

ptp profile default mode {boundary} delay-mechanism {e2e | p2p}

Item	Description	
Syntax Description	ptp	Configure PTP parameters
	profile	PTP profile selection
	default	Default profile
	mode	PTP clock mode
	boundary	Boundary clock
	delay-mechanism	Path delay mechanism
	e2e	End-to-End
	p2p	Peer-to-Peer
Defaults	End-to-End boundary clock	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# ptp profile default mode boundary delay-mechanism e2e	
Error Messages	—	
Related Commands	—	

Configure IEEE1588 PTP Profile Default Priority1

This command sets priority 1 of IEEE 1588.

■Command

- ptp profile default priority1 <value>
- no ptp profile default priority1

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	default	The Default profile.
	priority1	Priority 1 value used by the BMC algorithm
	<value>	0 to 255
Defaults	128	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# ptp profile default priority1 128 melsec(config)# no ptp profile default priority1	
Error Messages	—	
Related Commands	—	

Configure IEEE1588 PTP Profile Default Priority2

This command sets priority 2 of IEEE 1588.

■Command

- ptp profile default priority2 <value>
- no ptp profile default priority2

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp/no ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	default	The Default profile.
	priority2	Priority2 value used by the BMC algorithm
	<value>	0 to 255
Defaults	128	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# ptp profile default priority2 128 melsec(config)# no ptp profile default priority2	
Error Messages	—	
Related Commands	—	

Configure IEEE1588 PTP Profile Default Domain

This command sets the domain of IEEE 1588.

■Command

- ptp profile default domain <domain-number>
- no ptp profile default domain

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	default	The Default profile.
	domain	The PTP Domain related configuration.
	<domain-number>	0 to 255
Defaults	0	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# ptp profile default domain 0	
Error Messages	—	
Related Commands	—	

Configure IEEE1588 PTP Profile Default Network-Transport

This command sets the communication mode of IEEE 1588.

■Command

ptp profile default network-transport { ethernet | ipv4 }

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	default	The Default profile.
	network-transport	PTP network transport type related configuration
	ethernet	Layer 2 Transmission
	ipv4	UDP Internet Protocol version4
Defaults	ethernet	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# ptp profile default network-transport ethernet	
Error Messages	—	
Related Commands	—	

Configure IEEE1588 PTP Profile Default

This command enables IEEE 1588.

■Command

- ptp profile default
- no ptp profile default

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	default	The Default profile.
Defaults	The port is set to 802.1AS profile by default	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config)# interface Ethernet 1/1 /* Enable port ptp */ melsec(config-if)# ptp profile default /* Disable port ptp */ melsec(config-if)# no ptp profile default	
Error Messages	—	
Related Commands	—	

Configure IEEE1588 PTP Profile Default Announcement Interval

This command sets the transmission interval of the IEEE 1588 Announce frame for each port.

■Command

- ptp profile default announce interval <value>
- no ptp profile default announce interval

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	default	The Default profile.
	announce	Announce message related configuration
	interval	Logarithmic message interval
	<value>	Announce: 0 to 4
Defaults	Announce: 0	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec (config)# interface Ethernet 1/1 melsec (config-if)# ptp profile default announce interval 0 melsec (config-if)# no ptp profile default announce interval	
Error Messages	—	

Configure IEEE1588 PTP Profile Default Synchronization Interval

This command sets the Sync interval of IEEE 1588 for each port.

■Command

- ptp profile default sync interval <value>
- no ptp profile default sync interval

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	default	Default profile.
	sync	Sync message related configuration.
	interval	Logarithmic message interval.
	<value>	Sync: -3 to 5
Defaults	Sync: -3	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config)# interface Ethernet 1/1 melsec(config-if)# ptp profile default sync interval -3 melsec(config-if)# no ptp profile default sync interval	
Error Messages	—	
Related Commands	—	

Configure IEEE1588 PTP Profile Default Delay Request Interval

This command sets the Delay-Req interval of IEEE 1588 for each port.

■Command

- ptp profile default delay-req interval <value>
- no ptp profile default delay-req interval

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	default	The Default profile.
	delay-req	Delay request related configuration
	interval	Logarithmic message interval
	<value>	Delay-req: 0 to 5
Defaults	Delay-req: 0	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config)# interface Ethernet 1/1 melsec(config-if)# ptp profile default delay-req interval 0 melsec(config-if)# no ptp profile default delay-req interval	
Error Messages	—	
Related Commands	—	

Configure IEEE1588 PTP Profile Default Pdelay Request Interval

This command sets the PDelay-Req interval of IEEE 1588 for each port.

■Command

- ptp profile default pdelay-req interval <value>
- no ptp profile default pdelay-req interval

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	default	The Default profile.
	pdelay-req	Pdelay request related configuration
	interval	Logarithmic message interval
	<value>	Pdelay-req: 0 to 5.
Defaults	Pdelay-req: 0	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config)# interface Ethernet 1/1 melsec(config-if)# ptp profile default pdelay-req interval 0 melsec(config-if)# no ptp profile default pdelay-req interval	
Error Messages	—	
Related Commands	—	

Configure IEEE1588 PTP Profile Default Announcement Timeout

Sets the Announce frame reception timeout count of IEEE 1588 for each port.

■Command

- ptp profile default announce timeout <value>
- no ptp profile default announce timeout

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	ptp	Configure the PTP parameters.
	profile	The PTP profile selection.
	default	The Default profile.
	announce	announce
	timeout	Number of intervals without receiving corresponding message.
	<value>	Announce: 2 to 10
Defaults	Announce: 3	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config)# interface Ethernet 1/1 melsec(config-if)# ptp profile default announce timeout 3 melsec(config-if)# no ptp profile default announce timeout	
Error Messages	—	
Related Commands	—	

Show Interface Status

This command shows the port status.

■Command

show interface status

Item	Description	
Syntax Description	show	Show running system information
	interface	Display interface information
	status	The status of the interface
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show interface status	
Error Messages	—	
Related Commands	—	

Show Interface Type and ID

This command shows the detailed port information for each port.

■Command

- show interfaces [<interface-type> <interface-id>]
- show interfaces [{ [<interface-type> <interface-id>] [{ description | status }] }]

Item	Description	
Syntax Description	show	Display configuration/statistics/general
	interfaces	Display interface information
	interface-type	The Ethernet type
	interface-id	The slot number/port number
	description	Description about the interface
	status	The status of the interface
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show interfaces ethernet 1/1	
Error Messages	—	
Related Commands	—	

Show Interface Description

This command shows the remarks of the port.

■Command

show interface description

Item	Description	
Syntax Description	show	Display configuration/statistics/general information
	interface	Display interface information
	description	Description about the interface
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show interface description	
Error Messages	—	
Related Commands	—	

Configure Shutdown Settings

This command sets the port to the shutdown state.

■Command

- shutdown
- no shutdown

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	shutdown	Configure shutdown parameters
Defaults	Physical ports are enabled by default	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# shutdown	
Error Messages	—	
Related Commands	—	

Configure Description Settings

This command sets the remarks of the port.

■Command

- description <description of this interface(127)>
- no description

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	description	Configure description parameters
	description of this interface	The description of the interface
Defaults	Empty string	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# description melsec	
Error Messages	% Port Setting: Invalid: data.portTable[0].description must be shorter than or equal to 127 characters	
Related Commands	—	

Configure Duplex Settings

This command sets the port to full-duplex or half-duplex.

■Command

duplex { full | half }

Item	Description	
Syntax Description	duplex	Configure duplex parameters
	full	Set the port to full-duplex mode
	half	Set the port to half-duplex mode
Defaults	The port is full-duplex without auto-negotiation by default	
Command Modes	Interface Configuration	
Usage Guidelines	If the port is a combo port, the port duplex configuration is only effective on the copper interface.	
Examples	melsec(config-if)# no auto-negotiation melsec(config-if)# duplex full	
Error Messages	% Port Setting: Invalid: Fiber port can only be configured to full duplex/auto-mdix. % Port Setting: Invalid: Speed, Duplex and MDI/MDIX can only be configured when the port exists.	
Related Commands	speed { 10 | 100 }	

Configure Speed Settings

This command sets the communication speed of the port.

■Command

speed { 10 | 100 }

Item	Description	
Syntax Description	speed	Configure port speed parameters
	10	Set the port to run at 10 Mbps
	100	Set the port to run at 100 Mbps
Defaults	The port is set to 100 Mbps by default if auto-negotiation is disabled on the port	
Command Modes	Interface Configuration	
Usage Guidelines	If the port is a combo port, the speed configuration is only effective on the copper interface.	
Examples	melsec(config-if)# no auto-negotiation melsec(config-if)# speed 100	
Error Messages	% Port Setting: Invalid: Speed cannot configure a speed which is over the ability of the port. % Port Setting: Invalid: If a speed is equal to or faster than 10G, the port cannot configure autoNego/ duplex/speed. % Port Setting: Invalid: Speed, Duplex and MDI/MDIX can only be configured when the port exists.	
Related Commands	duplex { full | half }	

Configure mdix Setting

This command sets the port type.

■Command

mdix { auto | mdi | mdix }

Item	Description	
Syntax Description	mdix	Configure MDI/MDIX parameters
	auto	Set the port as an auto-crossover port
	mdi	Set the port as an MDI port
	mdix	Set the port as an MDIX port
Defaults	Auto-crossover is enabled by default	
Command Modes	Interface Configuration	
Usage Guidelines	If the port is a combo port, the mdix configuration is only effective on the copper interface.	
Examples	melsec(config-if)# mdix auto	
Error Messages	% Port Setting: Invalid: Fiber port can only be configured to full duplex/auto-mdix. % Port Setting: Invalid: Speed, Duplex and MDI/MDIX can only be configured when the port exists.	
Related Commands	—	

Configure Auto-Negotiation Setting

This command sets the auto-negotiation of the port.

■Command

- auto-negotiation
- no auto-negotiation

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	auto-negotiation	Configure auto-negotiation parameters
Defaults	Auto-negotiation is enabled by default	
Command Modes	Interface Configuration	
Usage Guidelines	If the port is a combo port, the auto-negotiation configuration is only effective on the copper interface.	
Examples	melsec(config-if)# auto-negotiation	
Error Messages	—	

Related Commands	speed { 10 | 100 }
	duplex { full | half }	

Show VLAN Interface Status

This command shows the VLAN information of the port.

■Command

show vlan

Item	Description	
Syntax Description	show	Display configuration/statistics/general information
	vlan	Display the VLAN interface status
Defaults	—	
Command Modes	Privileged EXEC User EXEC	
Usage Guidelines	—	
Examples	melsec# show vlan	
Error Messages	—	
Related Commands	vlan <vlan-id> vlan name	

Show VLAN Port Configuration

This command shows the VLAN setting for the port.

■Command

show vlan port config port [{ < interface-type > < interface-id> }]

Item	Description	
Syntax Description	show	Display configuration/statistics/general information
	vlan	Display VLAN interface status
	port	The port interface
	config	The port's configuration
	port	The port interface
	interface-type	The Ethernet type
	interface-id integer	The interface ID: slot number/port number
Defaults	—	
Command Modes	Privileged EXEC User EXEC	
Usage Guidelines	—	
Examples	melsec# show vlan port config port eth 1/1	
Error Messages	—	
Related Commands	Switchport pvid Switchport mode	

Show VLAN Management

This command shows the management VLAN.

■Command

show management vlan

Item	Description	
Syntax Description	show	Display configuration/statistics/general information
	management	Display Management VLAN information
	vlan	The VLAN interface
Defaults	—	
Command Modes	Privileged EXEC User EXEC	
Usage Guidelines	—	
Examples	melsec# show management vlan	
Error Messages	—	
Related Commands	Management vlan No management vlan	

Create/Delete a VLAN

This command creates or deletes a VLAN.

■Command

- vlan <vlan-id(1-4094)>
- no vlan <vlan-id>

Item	Description	
Syntax Description	vlan/no vlan	Create/delete a VLAN
	vlan-id	The VLAN identifier
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	To create a VLAN, a port must be added.	
Examples	melsec(config)# vlan 100 melsec(config)# no vlan 100 melsec(config)#	
Error Messages	—	
Related Commands	show vlan	

Configure VLAN Name

This command sets the name to the VLAN.

■Command

vlan name <vlan name string>

Item	Description	
Syntax Description	vlan name	Configure VLAN name
	vlan name string	Configure VLAN name string, 32 characters max.
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec# con melsec(config)# vlan 1 melsec(config-vlan)# vlan name test	
Error Messages	—	
Related Commands	—	

Configure VLAN Mode Member Ports

This command sets the port that is assigned to the VLAN.

■Command

- ports add {member ([<iftype> <iface_list>]) | untagged ([<iftype> <iface_list>]}
- ports set member ([<iftype> <iface_list>])
- ports set member ([<iftype> <iface_list>]) [untagged ([<iftype> <iface_list>]
- ports add {member | untagged} [<interface-type> <slot/port-port,slot/port,...>]
- no ports { [<interface-type> <slot/port-port,slot/port,...>] | [untagged ([<interface-type> <slot/port-port, slot/port,...>]) }

Item	Description	
Syntax Description	Ports/no ports	Set/delete member/untagged
	add	Add member/untag
	set	Overwrite member/untagged
	slot/port-port	The slot number/port number
	interface-type	The Ethernet type
	member	Configure the ports to be set as a member of the VLAN
	untagged	Configure the ports that will be used by the VLAN to transmit egress traffic as untagged packets.
Defaults	—	
Command Modes	Config VLAN mode	
Usage Guidelines	This command can only be executed from within VLAN configuration mode. From Configuration mode, enter vlan <vlan-id> to enter VLAN config mode.	
Examples	melsec(config)# vlan 10 melsec(config-vlan)#ports add member ethernet 1/3 melsec(config-vlan)#ports set member ethernet 1/3	
Error Messages	—	
Related Commands	switchport mode show vlan show mac-address-table count	

Configure PVID on a Specified Port

This command sets PVID.

■Command

- switchport pvid <vlan-id>
- no switchport pvid

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	pvid	Configure port-based VLAN parameters
	vlan-id	The VLAN ID, ranging from 1 to 4094.
Defaults	1	
Command Modes	Configuration	
Usage Guidelines	If a PVID does not exist for this system, it will be created automatically after configuration. If the port is configured to be in Access Mode, the actions below will be applied automatically. 1. Remove this port from member port list if it is bound to another VID which is different from PVID 2. Modify this port into an untagged member of this PVID If the port is configured to be in Trunk Mode, the port will automatically be modified into a tagged member of this PVID.	
Examples	melsec(config-if)# switchport pvid 1	
Error Messages	—	
Related Commands	switchport	

Configure Switch Port Operation Mode

This command sets the VLAN port mode.

■Command

switchport mode {access | trunk}

Item	Description	
Syntax Description	switchport	Configure the switch port
	mode	Configure switch port mode parameters
	access	Configure the port as an access port that accepts and sends only untagged packets. This kind of port is added as a member to a specific VLAN and only carries traffic for the VLAN to which the port is assigned. The port can only be set as an access port if the following 3 conditions are met: 1. The acceptable frame type is set as "Admit untagged and pri-tagged". 2. The port is not a tagged member of any VLAN. 3. The PVID is the same as the only untagged VLAN it joined.
	trunk	Configures the port as trunk port that accepts and sends only tagged frames. This kind of port is added as members of several existing VLANs, and carries traffic for all of them. The port can only be set as a trunk port. if the following 2 conditions are met: 1. The acceptable frame type is set as "Admit tagged only" 2. The port is not an untagged member of any VLAN.
Defaults	The default port operation mode is set to Trunk	
Command Modes	Interface Configuration	
Usage Guidelines	When changing from trunk to access mode, the following changes will be automatically applied: Forces the port to become an untagged member of the PVID domain If the port exists in another VLAN, it will be removed Forces the accept frame type to be set to "Admit untagged and pri-tagged" When changing from access to trunk mode, the following changes will be automatically applied: Forces the port to become a tagged member of the PVID domain If the port was an untagged member in another VLAN, it will changed into a tagged member. Forces the accept frame type to be set to "Admit tagged only"	
Examples	melsec (config-if)# switchport mode access	
Error Messages	—	
Related Commands	switchport vlan ports show vlan port config	

Set VLAN Access Port

This command sets the port as the access port.

■Command

switchport access vlan <vlan-id>

Item	Description	
Syntax Description	switchport access	Configure the port as an access port
	vlan <vlan-id>	The specified VLAN ID for which this access port will carry traffic, ranging from 1 to 4094.
Defaults	The port mode is set to trunk port by default	
Command Modes	Interface Configuration	
Usage Guidelines	Discarding the current operation mode of the port, this command will change the port to access mode and the following changes will automatically apply: Forces the acceptable frame type to be set to "untagged AND priority tagged" Sets PVID to specified a VLAN Changes the port into an untagged member of a specified VLAN and removes this port from any other VLANs. Sets the port mode to access mode	
Examples	melsec(config-if)# switchport access vlan 10	
Error Messages	—	
Related Commands	show vlan port config show vlan	

Configure VLAN Management

This command sets the management VLAN.

■Command

- management vlan <vlan-id>
- no management vlan <vlan>

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	management	Configure management
	vlan	Configure the management VLAN
	vlan-id	The management VLAN ID
Defaults	The default management VLAN ID is set to 1	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# management vlan 1	
Error Messages	—	
Related Commands	—	

Show Stream Adapter Information

This command shows the priority per stream.

■Command

show stream-adapter [interface <iftype> <ifnum>]

Item	Description	
Syntax Description	stream-adapter	Display stream adapter all information
	interface	Port interface
	iftype	Ethernet (interface-type)
	ifnum	Interface-id: <1-X>/<1-Y> Slot Number/Port Number; Note: X, Y are project dependent value. X means the numbers of max slot. Y means the number of max module port
Defaults	—	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec# show stream-adapter interface ethernet 1/1	
Error Messages	—	
Related Commands	—	

Configure Stream Adapter Rules

This command sets the priority per stream.

By default, the following command is executed to each port.

■Command

stream-adapter index <integer (0-9)> ethertype <integer (0-65535)> {subtype (integer (0-255))} vid <integer (1-4094)> pcp <integer (0-7)>

Item	Description	
Syntax Description	Stream-adapter	Configure the Stream Adapter rule parameters
	index	Configure a specific gate rule of the stream adapter
	<integer(0-9)>	Configure the index of the stream adapter
	ethertype	Configure the stream adapter ethertype parameter
	<integer(0-65535)>	Configure the ethertype
	subtype	Configure the stream adapter subtype parameter
	(integer (0-255))	Configure the subtype
	vid	Configure the stream adapter vlan id parameter
	<integer(1-4094)>	Configure the vlan id
	pcp	Configure the stream adapter pcp parameter
	<integer(0-7)>	Configure the pcp priority
Defaults	melsec(config-if)# stream-adapter index 0 ethertype 35087 vid 2 pcp 7	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# stream-adapter index 1 ethertype 5555 subtype 15 vid 3 pcp 7	
Error Messages	—	
Related Commands	—	

Remove Stream Adapter Rules

This command removes the priority per stream.

■Command

no stream-adapter index <integer (0-9)>

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	stream-adapter	Configure Stream Adapter rule parameters
	index	Configure a specific gate rule of stream adapter
	<integer (0-9)>	Configure the index of the stream adapter
Defaults	—	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# no stream-adapter index 1	
Error Messages	—	
Related Commands	—	

Enable Stream Adapter Egress Untag

This command enables the untagged output.

■Command

stream-adapter egress-untag

Item	Description	
Syntax Description	Stream-adapter	Configure Stream Adapter rule parameters
	egress-untag	remove the VLAN tag for all frame
Defaults	The egress untag is enabled by default	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# stream-adapter egress-untag	
Error Messages	—	
Related Commands	—	

Disable Stream Adapter Egress Untag

This command disables the untagged output.

■Command

no stream-adapter egress-untag

Item	Description	
Syntax Description	Stream-adapter	Configure Stream Adapter rule parameters
	egress-untag	not remove the VLAN tag
Defaults	The egress untag is enabled by default	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# no stream-adapter egress-untag	
Error Messages	—	
Related Commands	—	

Configure a Static Unicast MAC Address in the Forwarding Database

This command registers a static unicast MAC address to the MAC address table.

■Command

- mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id> set [interface ([<interface-type> <slot/port-port,slot/port,...>] [<interface-type> <slot/port-port,slot/port,...>]
- no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id>

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	mac-address-table	Configure MAC address table parameters
	static	Statically configured MAC address
	unicast	The unicast MAC address
	set	Overwrite port
	interface-id	The slot number/port number
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# mac-address-table static unicast □□:□□:□□:□□:□□:□□ vlan 168 set interface ethernet 2/4	
Error Messages	—	
Related Commands	mac-address-table static multicast vlan vlan ports add show mac-address-table static unicast	

Configure MAC Address Table Aging Time

This command sets the MAC address table aging time.

■Command

- mac-address-table aging-time <seconds (10-300)>
- no mac-address-table aging-time

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	mac-address-table	Configure the MAC-address-table
	aging-time	Maximum age of an entry in the MAC address table to its default value.
	second	The aging time ranging from 10 to 300 seconds
Defaults	300s	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# mac-address-table aging-time 100	
Error Messages	—	
Related Commands	show mac-address-table aging-time	

Show MAC Address Table Information

This command shows the information related to the MAC address table.

■Command

- show mac-address-table [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]
- show mac-address-table aging-time
- show mac-address-table count [vlan <vlan-id>]
- show mac-address-table dynamic unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] <interface-type> <interface-id> }]
- show mac-address-table static multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] <interface-type> <interface-id> }]
- show mac-address-table static unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] <interface-type> <interface-id> }]

Item	Description	
Syntax Description	mac-address-table	Display MAC address information
	address	The MAC address entry
	aging-time	The maximum age of a MAC address table entry
	count	The number of MAC addresses present on all VLANs or on a specified VLAN
	dynamic	Dynamically learned MAC address
	static	Statically configured MAC address
	multicast	The multicast MAC address
	unicast	The unicast MAC address
	vlan	The VLAN interface
	vlan-range	The VLAN ID range for which the details will be displayed. This value ranges from 1 to 4094. For example, 4000-4010 will show information for those VLAN IDs.
	interface-id	The slot number/port number
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show mac-address-table	
Error Messages	—	
Related Commands	mac-address-table	

Show MAC Address Table for Static Multicast

This command shows the static multicast MAC address.

■Command

show mac-address-table static multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] | <interface-type> <interface-id>]

Item	Description	
Syntax Description	mac-address-table	Display the MAC address table information
	static multicast	Display static multicast address information
	vlan <vlan-range>	Display all entries in the FDB table for the specified VLANs
	address <aa:aa:aa:aa:aa:aa>	Display the specified multicast MAC address in the FDB table
Defaults	—	
Command Modes	Privileged EXEC User EXEC	
Usage Guidelines	Display static multicast address table	
Examples	melsec# show mac-address-table static multicast	
Error Messages	—	
Related Commands	mac-address-table static multicast	

Configure MAC Address Table for Static Multicast

This command sets a static multicast MAC address.

■Command

mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id> {add | set} interface [<interface-type> <slot/port-port,slot/port,...>]

Item	Description	
Syntax Description	mac-address-table	Configure the MAC address table
	static multicast	Configure the static multicast address
	aa:aa:aa:aa:aa:aa	The multicast destination MAC address
	vlan <vlan-id>	The VLAN ID of the VLAN the multicast destination MAC address belongs to
	add	Add the new interface port
	Set	Overwrite the new interface port
	interface	Configure member ports details.
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	Configure the static multicast address	
Examples	melsec(config)# mac-address-table static multicast □□:□□:□□:□□:□□:□□ vlan 1 add interface ethernet 1/1-2	
Error Messages	"Invalid: Duplicate MAC Address." "Invalid: Configuration fail." "Invalid: The port is not included in VLAN egress ports." "Invalid: The MAC+VID entry must be removed from Port Security first." "Invalid: The port must remove from port security." "Invalid: Reserved multicast address (01:80:C2) is not allowed to set static multicast."	
Related Commands	show mac-address-table static multicast	

Show 802.1Qbv Information

This command shows the information related to IEEE 802.1Qbv.

■Command

show dot1qbv [interface <iftype> <ifnum>] administrative

Item	Description	
Syntax Description	dot1qbv	Display all information for the 802.1Qbv administrative.
	interface	The Port interface.
	iftype	Ethernet (interface-type)
	ifnum	Interface-id : <1-X>/<1-Y> Slot Number/Port Number ; Note: X, Y are project dependent value. X means the numbers of max slot. Y means the number of max module port
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show dot1qbv interface ethernet 1/1 administrative	
Error Messages	—	
Related Commands	—	

Show 802.1Qbv Operative Information

This command shows the IEEE 802.1Qbv operational information.

■Command

show dot1qbv [interface <iftype> <ifnum>] operative

Item	Description	
Syntax Description	dot1qbv	Display all information for the 802.1Qbv operative.
	interface	The Port interface.
	iftype	Ethernet (interface-type)
	ifnum	Interface-id: <1-X>/<1-Y> Slot Number/Port Number Note: X, Y is a project dependent value. X means the numbers of max slot. Y means the number of max module port.
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show dot1qbv interface ethernet 1/1 operative	
Error Messages	—	
Related Commands	—	

Enable/Disable 802.1Qbv Function

This command enables or disables IEEE 802.1Qbv.

■Command

- dot1qbv
- no dot1qbv

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value.
	dot1qbv	Enable the 802.1Qbv function.
Defaults	Disable	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# dot1qbv melsec(config-if)# no dot1qbv	
Error Messages	—	
Related Commands	—	

Configure 802.1Qbv Config-change Operation

This command reflects the IEEE 802.1Qbv setting to the operation.

■Command

dot1qbv config-change operation { true | false }

Item	Description	
Syntax Description	dot1qbv	Configure the 802.1Qbv parameters.
	config-change	Configure the config-change parameters.
	operation	Configure the config-change operations.
	true	Configure when the config-change operations start.
	false	Configure when the config-change operations stop.
Defaults	False	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# dot1qbv config-change operation true melsec(config-if)# dot1qbv config-change operation false	
Error Messages	—	
Related Commands	—	

Append 802.1Qbv Control List

This command appends the IEEE 802.1Qbv control list.

By default, the following command is executed to each port.

■Command

dot1qbv control-list append oper-name { sgs } gate-states <integer(0-255)> time <integer(0-999999999)>

Item	Description	
Syntax Description	dot1qbv	Configure the 802.1Qbv parameters.
	control-list	Configure the control-list parameters.
	append	Configure the control-list append operations.
	oper-name	Configure the control-list operation name.
	sgs	Configure the operation name to set-gate-states.
	gate-states	Configure the control-list gate-states parameter.
	(0-255)	Configure the gate-states.
	time	Configure the time interval.
	(0-999999999)	Configure the time interval.
Defaults	melsec(config-if)# dot1qbv control-list set index 0 oper-name sgs gate-states 128 time 500000 melsec(config-if)# dot1qbv control-list set index 1 oper-name sgs gate-states 64 time 20000 melsec(config-if)# dot1qbv control-list set index 2 oper-name sgs gate-states 1 time 480000 melsec(config-if)# dot1qbv cycle-time numerator 1 denominator 1000	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# dot1qbv control-list append oper-name sgs gate-states 100 time 12345	
Error Messages	—	
Related Commands	—	

Remove 802.1Qbv Control List

This command removes the IEEE 802.1Qbv control list.

By default, the following command is executed to each port.

■Command

dot1qbv control-list remove { index <integer(0-1023)> | all }

Item	Description	
Syntax Description	dot1qbv	Configure the 802.1Qbv parameters.
	control-list	Configure the control-list parameters.
	remove	Configure the control-list remove operation.
	index	Configure a specific gate rule of control-list.
	(0-1023)	Configure the index of the control-list.
	all	Configure all of the control-list.
Defaults	melsec(config-if)# dot1qbv control-list set index 0 oper-name sgs gate-states 128 time 500000 melsec(config-if)# dot1qbv control-list set index 1 oper-name sgs gate-states 64 time 20000 melsec(config-if)# dot1qbv control-list set index 2 oper-name sgs gate-states 1 time 480000 melsec(config-if)# dot1qbv cycle-time numerator 1 denominator 1000	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# dot1qbv control-list remove index 10 melsec(config-if)# dot1qbv control-list remove all	
Error Messages	Invalid index:10	
Related Commands	—	

Set 802.1Qbv Control List

This command edits the IEEE 802.1Qbv control list.

By default, the following command is executed to each port.

■Command

```
dot1qbv control-list set index <integer(0-1023)> oper-name { sgs } gate-states <integer(0-255)> time <integer(0-999999999)>
```

Item	Description	
Syntax Description	dot1qbv	Configure the 802.1Qbv parameters.
	control-list	Configure the control-list parameters.
	set	Configure control-list set operation.
	index	Configure a specific gate rule of control-list.
	(0-1023)	Configure the index of the control-list.
	oper-name	Configure control-list operation name.
	sgs	The operation name to set-gate-states.
	gate-states	Configure control-list gate-states parameter.
	(0-255)	Configure the gate-states.
	time	Configure the time interval.
	(0-999999999)	Configure the time interval.
Defaults	melsec(config-if)# dot1qbv control-list set index 0 oper-name sgs gate-states 128 time 500000 melsec(config-if)# dot1qbv control-list set index 1 oper-name sgs gate-states 64 time 20000 melsec(config-if)# dot1qbv control-list set index 2 oper-name sgs gate-states 1 time 480000 melsec(config-if)# dot1qbv cycle-time numerator 1 denominator 1000	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# dot1qbv control-list set index 11 oper-name sgs gate 100 time 10000	
Error Messages	Set index :11 failure	
Related Commands	—	

Configure 802.1Qbv Cycle Time

This command sets the IEEE 802.1Qbv communication cycle.

By default, the following command is executed to each port.

■Command

```
dot1qbv cycle-time numerator <integer(0-4294967295)> denominator <integer(0-4294967295)>
```

Item	Description	
Syntax Description	dot1qbv	Configure the 802.1Qbv parameters.
	cycle-time	Configure the cycle-time parameters.
	numerator	Configure the numerator of the cycle time.
	(0-4294967295)	Configure the value of the cycle time numerator.
	denominator	Configure the value of the cycle time denominator.
	(0-4294967295)	Configure the value of the cycle time denominator.
Defaults	melsec(config-if)# dot1qbv control-list set index 0 oper-name sgs gate-states 128 time 500000 melsec(config-if)# dot1qbv control-list set index 1 oper-name sgs gate-states 64 time 20000 melsec(config-if)# dot1qbv control-list set index 2 oper-name sgs gate-states 1 time 480000 melsec(config-if)# dot1qbv cycle-time numerator 1 denominator 1000	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec(config-if)# dot1qbv cycle-time numerator 1 denominator 100	
Error Messages	—	
Related Commands	—	

Configure Spanning Tree Compatibility

This command sets the compatibility of STP.

■Command

- spanning-tree compatibility { stp | rstp }
- no spanning-tree compatibility

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/resets to default value
	spanning-tree	Configure Spanning Tree Protocol parameters
	compatibility	The Spanning Tree compatibility version
	stp	Spanning Tree Protocol configuration
	rstp	Rapid Spanning Tree configuration
Defaults	Spanning Tree Protocol compatibility is set to rstp by default.	
Command Modes	Global Configuration	
Usage Guidelines	The "no spanning-tree compatibility" command will restore the default value	
Examples	melsec# configure terminal melsec(config)# spanning-tree compatibility stp melsec(config)# spanning-tree compatibility rstp melsec(config)# no spanning-tree compatibility	
Error Messages	—	
Related Commands	show spanning-tree show spanning-tree detail	

Configure Spanning Tree Priority

This command sets the priority of STP.

■Command

- spanning-tree priority <value (0-61440)>
- no spanning-tree priority

Item	Description	
Syntax Description	no	Disable the configuration / deletes the entry / resets to default value
	spanning-tree	Configure Spanning Tree Protocol parameters
	priority	Configure switch priority for Spanning Tree instances
	value	The switch priority value ranging from 0 to 61440
Defaults	The default priority is set to 32768	
Command Modes	Global Configuration	
Usage Guidelines	The "no spanning-tree priority" command will restore the default value	
Examples	melsec# configure terminal melsec(config)# spanning-tree priority 61440 melsec(config)# no spanning-tree priority	
Error Messages	—	
Related Commands	show spanning-tree show spanning-tree detail	

Configure Spanning Tree Forward Time

This command sets the Forward Time of STP.

■Command

- spanning-tree forward-time <seconds (4-30)>
- no spanning-tree forward-time

Item	Description	
Syntax Description	no	Disable the configuration/deletes the entry/resets to default value
	spanning-tree	Configure Spanning Tree Protocol parameters
	forward-time	The interval (in seconds) in which a port stays in its current state before moving to next state
	seconds	The forwarding time ranging from 4 to 30 seconds
Defaults	The default forwarding time is 15 seconds	
Command Modes	Global Configuration	
Usage Guidelines	Command "no spanning-tree forward-time" will reset to default value 2*(ForwardDelay -1)>=MaxAge >= 2*(Hello Time + 1)	
Examples	melsec# configure terminal melsec(config)# spanning-tree forward-time 16 melsec(config)# no spanning-tree forward-time	
Error Messages	% RSTP: 2*(Forward time -1)>=Max age time >= 2*(Hello time + 1)	
Related Commands	show spanning-tree show spanning-tree detail	

Configure Spanning Tree Hello Time

This command sets the Hello Time of STP.

■Command

- spanning-tree hello-time <seconds (1-2)>
- no spanning-tree hello-time

Item	Description	
Syntax Description	no	Disable the configuration/deletes the entry/resets to default value
	spanning-tree	Configure Spanning Tree Protocol parameters
	hello-time	The interval (in seconds) between the transmission of configuration BPDUs
	seconds	The hello time interval ranging from 1 to 2 seconds
Defaults	The default hello time is set to 2 seconds	
Command Modes	Global Configuration	
Usage Guidelines	The "no spanning-tree hello-time" command will restore the default value 2*(ForwardDelay -1)>=MaxAge >= 2*(Hello Time + 1)	
Examples	melsec# configure terminal melsec(config)# spanning-tree hello-time 1 melsec(config)# no spanning-tree hello-time	
Error Messages	% RSTP: 2*(Forward time -1)>=Max age time >= 2*(Hello time + 1)	
Related Commands	show spanning-tree show spanning-tree detail	

Configure Spanning Tree Maximum Age

This command sets the Maximum Age of STP.

■Command

- spanning-tree max-age <seconds (6-40)>
- no spanning-tree max-age

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	spanning-tree	Configure Spanning Tree Protocol parameters
	max-age	The maximum age (in seconds) before learnt STP information is discarded
	seconds	The maximum age ranging from 6 to 40 seconds
Defaults	The STP maximum age is set to 20 seconds by default	
Command Modes	Global Configuration	
Usage Guidelines	The "no spanning-tree max-age" command will restore the default value 2*(ForwardDelay -1)>=MaxAge >= 2*(Hello Time + 1)	
Examples	melsec# configure terminal melsec(config)# spanning-tree max-age 21 melsec(config)# no spanning-tree max-age	
Error Messages	% RSTP: 2*(Forward time -1)>=Max age time >= 2*(Hello time + 1)	
Related Commands	show spanning-tree show spanning-tree detail	

Configure Spanning Tree Auto-edge

This command automatically sets the port type.

■Command

- spanning-tree auto-edge
- no spanning-tree auto-edge

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	spanning-tree	Configure Spanning Tree Protocol
	auto-edge	Configure the automatic detection of bridges attached to an interface
Defaults	Spanning Tree auto-edge is enabled by default	
Command Modes	Interface Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# interface ethernet 1/1 melsec(config-if)# spanning-tree auto-edge melsec(config-if)# no spanning-tree auto-edge	
Error Messages	—	
Related Commands	show spanning-tree detail show spanning-tree interface ethernet 1/1 detail	

Configure Spanning Tree Cost

This command sets the port cost.

■Command

- spanning-tree cost <value (0-200000000)>
- no spanning-tree cost

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	spanning-tree	Configure Spanning Tree Protocol
	cost	Configure the path cost
	value	The Spanning Tree cost ranging from 0 to 200000000
Defaults	The default path cost is set to 0	
Command Modes	Interface Configuration	
Usage Guidelines	The "spanning-tree cost 0" command will auto-detect the cost based on port speed The "no spanning-tree cost" command will restore the default value	
Examples	melsec# configure terminal melsec(config)# interface ethernet 1/1 melsec(config-if)# spanning-tree cost 20000 melsec(config-if)# no spanning-tree cost	
Error Messages	—	
Related Commands	show spanning-tree detail show spanning-tree interface ethernet 1/1 show spanning-tree interface ethernet 1/1 detail	

Configure Spanning Tree Link Type

This command sets the port link type.

■Command

- spanning-tree link-type { point-to-point | shared }
- no spanning-tree link-type

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	spanning-tree	Configure Spanning Tree Protocol parameters
	link-type	Configure the link type as a point-to-point link or as a shared LAN segment on which another bridge is present
	point-to-point	Set the link to a point-to-point link
	shared	Set the link as a shared link
Defaults	The default Spanning Tree link-type is set to auto-detect	
Command Modes	Interface Configuration	
Usage Guidelines	The "no spanning-tree link-type" command will auto-detect the interface link type based on the port duplex mode	
Examples	melsec# configure terminal melsec(config)# interface ethernet 1/1 melsec(config-if)# spanning-tree link-type point-to-point melsec(config-if)# spanning-tree link-type shared melsec(config-if)# no spanning-tree link-type	
Error Messages	—	
Related Commands	show spanning-tree detail show spanning-tree interface ethernet 1/1 show spanning-tree interface ethernet 1/1 detail	

Configure Spanning Tree Portfast

This command manually sets the port type.

■Command

- spanning-tree portfast
- no spanning-tree portfast

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	spanning-tree	Configure Spanning Tree Protocol parameters
	portfast	Specify ports that have only hosts connected to enable immediate transition to a forwarding state
Defaults	Spanning Tree Portfast is disabled by default	
Command Modes	Interface Configuration	
Usage Guidelines	Shut down the interface before enabling the Portfast function The Portfast function cannot be enabled on a port that has loop guard enabled	
Examples	melsec# configure terminal melsec(config)# interface ethernet 1/1 melsec(config-if)# spanning-tree portfast melsec(config-if)# no spanning-tree portfast	
Error Messages	—	
Related Commands	show spanning-tree detail show spanning-tree interface ethernet 1/1 show spanning-tree interface ethernet 1/1 detail	

Configure Spanning Tree Port Priority

This command sets the priority of the port.

- spanning-tree port-priority <value (0-240)>
- no spanning-tree port-priority

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	spanning-tree	Configure Spanning Tree Protocol parameters
	port-priority	Configure the port priority value
	value	The Spanning Tree port priority ranging from 0 to 240
Defaults	The default Spanning Tree port priority is set to 128	
Command Modes	Interface Configuration	
Usage Guidelines	The "no spanning-tree port-priority" command will restore the default value	
Examples	melsec# configure terminal melsec(config)# interface ethernet 1/1 melsec(config-if)# spanning-tree port-priority 16 melsec(config-if)# no spanning-tree port-priority	
Error Messages	—	
Related Commands	show spanning-tree detail show spanning-tree interface ethernet 1/1 show spanning-tree interface ethernet 1/1 detail	

Show Spanning Tree Bridge Information

This command shows the information of the managed switch.

■Command

show spanning-tree bridge

Item	Description	
Syntax Description	show	Display the Configuration/statistics/general information
	spanning-tree	Spanning Tree-related information
	bridge	Spanning Tree bridge information
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show spanning-tree bridge	
Error Messages	—	
Related Commands	—	

Show Spanning Tree Root Information

This command shows the information of the root bridge.

■Command

show spanning-tree root

Item	Description	
Syntax Description	show	Display the configuration/statistics/general information
	spanning-tree	Spanning Tree-related information
	root	Spanning Tree root information
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show spanning-tree root	
Error Messages	—	
Related Commands	—	

Show Spanning Tree Interface Information

This command shows the information of each port of the managed switch.

■Command

- show spanning-tree interface { ethernet <slot/port> }
- show spanning-tree interface { ethernet <slot/port> } detail

Item	Description	
Syntax Description	show	Display the configuration/statistics/general information
	spanning-tree	Spanning Tree-related information
	interface	Spanning Tree interface information
	ethernet <slot/port>	The Ethernet slot or port number
	detail	Detailed information about the port and bridge
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show spanning-tree interface ethernet 1/2 melsec# show span in eth 1/1	
Error Messages	—	
Related Commands	—	

Show Spanning Tree Details

This command shows the detailed STP information.

■Command

show spanning-tree [detail]

Item	Description	
Syntax Description	show	Display the configuration/statistics/general information
	spanning-tree	Spanning Tree related information
	detail	Detailed Spanning Tree information
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show spanning-tree	
Error Messages	—	
Related Commands	—	

Show SNMP Server Information

This command shows the SNMP server information.

■Command

show snmp-server information

Item	Description	
Syntax Description	show	Display the configuration/statistics/general information
	snmp-server	Display SNMP server information
	information	Display general SNMP server information
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show snmp-server information	
Error Messages	% Can't get snmp-server information % Can't get snmp-server community information	
Related Commands	snmp-server	

Show SNMP Server User Account Information

This command shows the SNMP user account information.

■Command

show snmp-server user

Item	Description	
Syntax Description	show	Displays the configuration/statistics/general information
	snmp-server	Displays SNMP server information
	user	Displays SNMP server user accounts
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show snmp-server user	
Error Messages	% Can't get snmp-server user-account information % Can't get snmp-server user-account table	
Related Commands	snmp-server	

Configure SNMP Server Access Mode

This command sets the access mode to the SNMP agent.

■Command

snmp-server access { enable | disable | read-only }

Item	Description	
Syntax Description	snmp-server	Configure SNMP server parameters
	access	Configure the SNMP server access mode
	enable	Enable SNMP server access
	disable	Disable SNMP server access
	read-only	Set SNMP server access to read-only mode
Defaults	SNMP server access is enabled by default	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# snmp-server access enable melsec(config)# snmp-server access disable melsec(config)# snmp-server access read-only	
Error Messages	—	
Related Commands	snmp-server show snmp-server	

Configure SNMP Server Read-Only Community Settings

This command sets the community string for read-only access.

■Command

snmp-server community read-only <community-name(32)>

Item	Description	
Syntax Description	snmp-server	Configure snmp-server related parameters
	community	Configure the SNMP server community
	read-only	Configure the SNMP server community for read-only
	community-name (32)	The SNMP server read-only community name
Defaults	The default read-only community name is set to public	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# snmp-server community read-only public	
Error Messages	—	
Related Commands	snmp-server show snmp-server	

Configure SNMP Server Read-Only Community to Default Value

This command resets the community string for read-only access to default.

■Command

no snmp-server community read-only

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	snmp-server	Configure SNMP server parameters
	community	Configure the SNMP server community
	read-only	Configure the SNMP server community for read-only
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# no snmp-server community read-only	
Error Messages	—	
Related Commands	snmp-server show snmp-server	

Configure SNMP Server Read-Write Community Settings

This command sets the community string for read/write access.

■Command

snmp-server community read-write <community-name(32)>

Item	Description	
Syntax Description	snmp-server	Configure SNMP server parameters
	community	Configure the SNMP server community
	read-write	Configure the SNMP server community for read-write
	community-name (32)	The SNMP server read-write community name
Defaults	The default read-write community name is set to private	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# snmp-server community read-write private	
Error Messages	—	
Related Commands	snmp-server show snmp-server	

Configure SNMP Server Read-Write Community to Default Value

This command resets the community string for read/write access to default.

■Command

no snmp-server community read-write

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry /reset to default value
	snmp-server	Configures SNMP server parameters
	community	Configure the SNMP server community
	read-write	Configure the SNMP server community for read-write
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# no snmp-server community read-write	
Error Messages	—	
Related Commands	snmp-server show snmp-server	

Configure SNMP Server Version

This command sets the SNMP version.

■Command

snmp-server version { v1-v2c-v3 | v1-v2c | v3 }

Item	Description	
Syntax Description	snmp-server	Configure SNMP server parameters
	version	Configure the SNMP server version compatibility
	v1-v2c-v3	Set the SNMP server version to v1-v2c-v3
	v1-v2c	Set the SNMP server version to v1-v2c
	v3	Set the SNMP server version to v3-only
Defaults	The default SNMP server version is set to v1-v2c	
Command Modes	Global configuration	
Usage Guidelines	Set up at least one SNMP server user account before enabling v1-v2c-v3 or v3	
Examples	melsec(config)# snmp-server version v1-v2c-v3 melsec(config)# snmp-server version v1-v2c melsec(config)# snmp-server version v3	
Error Messages	% Atleast setup one valid user before enable snmp-server version v1-v2c-v3 or v3	
Related Commands	snmp-server show snmp-server	

Configure SNMP Server Version to Default Value

This command resets the SNMP version to default.

■Command

no snmp-server version

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	snmp-server	Configure SNMP server parameters
	version	Configure the SNMP server version compatibility
Defaults	The default SNMP server version is set to v1-v2c	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# no snmp-server version	
Error Messages	—	
Related Commands	snmp-server show snmp-server	

Configure SNMP Server User Account Settings

This command sets the user account with which to access the SNMP agent.

■Command

snmp-server user <user-name(32)> authority { read-only | read-write } auth-type { none | md5 | sha }
[auth-passwd <authentication-password(64)>] encryption { disable| des| aes }
[encryption-key <encryption-key(64)>]

Item	Description	
Syntax Description	snmp-server	Configure SNMP server parameters
	user	Configure SNMP server user accounts
	user-name (32)	The user name of the SNMP server user account
	authority	Configure the access right for the user account
	read-only	Give read-only access to the user
	read-write	Give read-write access to the user
	auth-type	Configure the authentication protocol for the SNMP server user account
	none	Do not use any authentication protocol
	md5	Use MD5 authentication
	sha	Use SHA authentication
	auth-passwd	Configure the authentication password for the SNMP server user account
	authentication-password (64)	The authentication password
	encryption	Configure the data encryption protocol for the SNMP server user account
	disable	Disable data encryption
	des	Use DES data encryption
	aes	Use AES data encryption
	encryption-key	Configure the data encryption key for the SNMP server user account
	encryption-key (64)	The data encryption key
Defaults	There is no user account table by default	
Command Modes	Global configuration	
Usage Guidelines	If the authentication type is set to none, data encryption should be disabled. If the authentication type is not none, an authentication password must be set up. If data encryption is not disabled, a data encryption key must be set up.	
Examples	melsec(config)# snmp-server user testNoAuthNoPriv authority read-write auth-type none encryption disable melsec(config)# melsec(config)# melsec(config)# snmp-server user testAuthNoPriv authority read-write auth-type md5 auth-passwd 1111111111 encryption disable melsec(config)# melsec(config)# melsec(config)# snmp-server user testAuthPriv authority read-write auth-type md5 auth-passwd 1111111111 encryption des encryption-key 2222222222 melsec(config)# melsec(config)#	
Error Messages	% If authentication-type is none, data-encryption method should be disabled % must setup authentication password % must setup data encryption key % Can't get snmp-server user-account information % Can't get snmp-server user-account table % Can't get snmp-server user-account table index ('%d') % Can't get user-name from snmp-server user-account table('%d') % Can't create user account % Can't modify user account	
Related Commands	snmp-server show snmp-server	

Delete SNMP Server User Account

This command deletes the user account with which to the SNMP agent.

■Command

no snmp-server user <user-name (32)>

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	snmp-server	Configure SNMP server parameters
	user	Configure SNMP server user accounts
	user-name (32)	The user name of the SNMP server user account
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# no snmp-server user testNoAuthNoPriv melsec(config)# no snmp-server user testAuthNoPriv melsec(config)# no snmp-server user testAuthPriv	
Error Messages	% Can't get snmp-server user-account information % Can't get snmp-server user-account table % Can't get snmp-server user-account table index ('%d') % Can't get user-name from snmp-server user-account % Can't delete user account	
Related Commands	snmp-server show snmp-server	

Show SNMP Trap Information

This command shows the SNMP Trap information.

■Command

show snmp-trap information

Item	Description	
Syntax Description	show	Display the configuration/statistics/general information
	snmp-trap	Display SNMP trap information
	information	Display general SNMP trap information
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show snmp-trap information	
Error Messages	% Can't get snmp-trap information % Can't get snmp-trap jason object	
Related Commands	snmp-trap	

Show SNMP Trap User Account Information

This command shows the SNMP Trap user account information.

■Command

show snmp-trap user

Item	Description	
Syntax Description	show	Display the configuration/statistics/general information
	snmp-trap	Display SNMP trap information
	user	Display SNMP trap user accounts
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show snmp-trap user	
Error Messages	% Can't get snmp-trap user-account information % Can't get snmp-trap user-account table % Can't get snmp-trap user-account table index ('%d')	
Related Commands	snmp-trap	

Show SNMP Trap Host Information

This command shows the host setting for SNMP Trap.

■Command

show snmp-trap host

Item	Description	
Syntax Description	show	Display the configuration/statistics/general information
	snmp-trap	Display SNMP trap information
	host	Display SNMP trap host information
Defaults	—	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	—	
Examples	melsec# show snmp-trap host	
Error Messages	% Can't get snmp-trap host information % Can't get snmp-trap host table % Can't get snmp-trap host table index('%d')	
Related Commands	snmp-trap	

Configure SNMP Trap Host Settings

This command sets the host of SNMP Trap.

■Command

snmp-trap host <host-address(32)> mode { trap-v1 | trap-v2c | inform-v2c | trap-v3 | inform-v3 } [community <community-name(32)>]

Item	Description	
Syntax Description	snmp-trap	Configure SNMP trap parameters
	host	Configure the SNMP trap host address
	host-address (32)	The SNMP trap host address
	mode	Configure the SNMP trap mode
	trap-v1	Use trap-v1 mode
	trap-v2c	Use trap-v2c mode
	inform-v2c	Use inform-v2c mode
	trap-v3	Use trap-v3 mode
	inform-v3	Use inform-v3 mode
	community	Configure the community for the SNMP trap host
	community-name (32)	The community name for the SNMP trap host
Defaults	There is no SNMP trap host entry by default	
Command Modes	Global configuration	
Usage Guidelines	A community name must be set when using trap-v1, trap-v2c, or infom-v2c mode. SNMP v3 must be enabled when SNMP trap-v3 mode is enabled. At least one valid user must be set up before setting the SNMP trap host to trap-v3 mode.	
Examples	melsec(config)# snmp-trap host 192.168.127.254 mode trap-v1 community public melsec(config)# snmp-trap host 192.168.127.253 mode inform-v3	
Error Messages	% Can't get snmp-trap host information % Can't get host name from snmp-trap host table % Can't get snmp-trap host table index('%d') % Can't get host-name from snmp-trap host table('%d') % Can't create host entry % Can't modify host entry % must set community name when mode is trap-v1, trap-v2c or infom-v2c % must enable v3 in snmp-server when snmp-trap host <host-address> trap-v3 mode is enable % Atleast setup one valid user before enable snmp-trap host to trap-v3 mode	
Related Commands	snmp-trap show snmp-trap	

Delete SNMP Trap Host Entry

This command deletes the host setting for SNMP Trap.

■Command

no snmp-trap host <host-address(32)>

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	snmp-trap	Configure SNMP trap parameters
	host	Configure the SNMP trap host address
	host-address (32)	The SNMP trap host address
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# no snmp-trap host 192.168.127.254 melsec(config)# no snmp-trap host 192.168.127.253	
Error Messages	% Can't get snmp-trap host information % Can't get host name from snmp-trap host table % Can't get snmp-trap host table index('%d') % Can't get host-name from snmp-trap host table('%d') % Can't delete host entry	
Related Commands	snmp-trap show snmp-trap	

Configure SNMP Trap Inform Retry Setting

This command sets the retry count for SNMP Trap/Inform.

■Command

snmp-trap inform-retries <inform-retries-number(1-99)>

Item	Description	
Syntax Description	snmp-trap	Configure SNMP trap parameters
	inform-retries	Configure SNMP trap inform retries
	inform-retries-number (1-99)	The amount of SNMP trap inform retries
Defaults	The default number of SNMP trap inform retries is set to 3	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# snmp-trap inform-retries 3	
Error Messages	—	
Related Commands	snmp-trap show snmp-trap	

Reset SNMP Trap Inform Retry to Default Value

This command resets the retry count of SNMP Trap/Inform to default.

■Command

no snmp-trap inform-retries

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	snmp-trap	Configure SNMP trap parameters
	inform-retries	Configure SNMP trap inform retries
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# no snmp-trap inform-retries	
Error Messages	—	
Related Commands	snmp-trap show snmp-trap	

Configure SNMP Trap Inform Timeout Setting

This command sets the timeout count of SNMP Trap/Inform.

■Command

snmp-trap inform-timeout <inform-timeout-number(1-300)>

Item	Description	
Syntax Description	snmp-trap	Configure SNMP trap parameters
	inform-timeout	Configure the SNMP trap inform timeout
	inform-timeout-number (1-300)	The SNMP trap inform timeout in seconds
Defaults	The default SNMP trap inform timeout is set to 10 seconds	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# snmp-trap inform-timeout 10	
Error Messages	—	
Related Commands	snmp-trap show snmp-trap	

Reset SNMP Trap Inform Timeout to Default Value

This command resets the timeout count of SNMP Trap/Inform to default.

■Command

no snmp-trap inform-timeout

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	snmp-trap	Configure SNMP trap parameters
	inform-timeout	Configure the SNMP trap inform timeout
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# no snmp-trap inform-timeout	
Error Messages	—	
Related Commands	snmp-trap show snmp-trap	

Configure SNMP Trap User Account Settings

This command sets the SNMP Trap user account.

■Command

snmp-trap user <user-name(32)> auth-type { none | md5 | sha } [auth-passwd <authentication-password(64)>] encryption { disable| des | aes } [encryption-key <encryption-key(64)>]

Item	Description	
Syntax Description	snmp-trap	Configures SNMP trap parameters
	user	Configure SNMP trap user accounts
	user-name(32)	The user name of the SNMP trap user account
	auth-type	Configure the authentication protocol for the SNMP trap user account
	none	Do not use any authentication protocol
	md5	Use MD5 authentication
	sha	Use SHA authentication
	auth-passwd	Configure the authentication password for the SNMP trap user account
	authentication-password (64)	The authentication password
	encryption	Configure the data encryption protocol for the SNMP trap user account
	disable	Disable data encryption
	des	Use DES data encryption
	aes	Use AES data encryption
	encryption-key	Configure the data encryption key for the SNMP trap user account
	encryption-key (64)	The data encryption key
Defaults	There is no user account table by default	
Command Modes	Global configuration	
Usage Guidelines	If the authentication type is set to none, data encryption should be disabled. If the authentication type is not none, an authentication password must be set up. If data encryption is not disabled, a data encryption key must be set up.	
Examples	melsec# con t melsec(config)# snmp-trap user test auth-type none encryption disable melsec(config)# snmp-trap user test auth-type md5 auth-passwd 1111111111 encryption disable melsec(config)# snmp-trap user test auth-type md5 auth-passwd 1111111111 encryption des encryption-key 2222222222	
Error Messages	% If authentication-type is none, data-encryption method should be disabled % must setup authentication password % must setup data encryption key % Can't get snmp-trap user-account information % Can't get snmp-trap user-account table % Can't get snmp-trap user-account table index ('%d') % Can't get user-name from snmp-trap user-account table('%d') % Can't create user account % Can't modify user account	
Related Commands	snmp-trap show snmp-trap	

Delete SNMP Trap User Account

This command deletes the SNMP Trap user account.

■Command

no snmp-trap user <user-name (32)>

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	snmp-trap	Configures SNMP trap parameters
	user	Configure SNMP trap user accounts
	user-name (32)	The user name of the SNMP trap user account
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# no snmp-trap user test	
Error Messages	% Can't get snmp-trap user-account information % Can't get snmp-trap user-account table % Can't get snmp-trap user-account table index ('%d') % Can't get user-name from snmp-trap user-account % Can't delete user account	
Related Commands	snmp-trap show snmp-trap	

Enable Network Server

This command enables the managed switch interface.

■Command

ip { http | https | telnet | ssh | melsec-command } server enable

Item	Description	
Syntax Description	ip	Configure IP parameters
	http	Configure HTTP management UI service parameters
	https	Configure HTTPS management UI service parameters
	telnet	Configure Telnet management UI service parameters
	ssh	Configure SSH management UI service parameters
	melsec-command	Configure melsec Command management UI service parameters
	server	Configure management UI service server parameters
	enable	Enable the management UI service
Defaults	http: enabled https: enabled telnet: enabled ssh: enabled melsec-command: enabled	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ip https server enable	
Error Messages	—	
Related Commands	—	

Disable Network Server

This command disables the managed switch interface.

■Command

ip { http | https | telnet | ssh | melsec-command } server disable

Item	Description	
Syntax Description	ip	Configure IP parameters
	http	Configure HTTP management UI service parameters
	https	Configure HTTPS management UI service parameters
	telnet	Configure Telnet management UI service parameters
	ssh	Configure SSH management UI service parameters
	melsec-command	Configure melsec Command management UI service parameters
	server	Configure management UI service server parameters
	disable	Disable the management UI service
Defaults	http: enabled https: enabled telnet: enabled ssh: enabled melsec-command: enabled	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ip telnet server disable	
Error Messages	—	
Related Commands	—	

Configure Network Port Numbers

This command sets the port number of the interface.

■Command

ip { http | https | telnet | ssh } port <port-number(1-65535)>

Item	Description	
Syntax Description	ip	Configure IP parameters
	http	Configure HTTP management UI service parameters
	https	Configure HTTPS management UI service parameters
	telnet	Configure Telnet management UI service parameters
	ssh	Configure SSH management UI service parameters
	port	Configure the service port of the management UI service
	port-number	The service port number
Defaults	http server port: 80 https server port: 443 telnet server port: 23 ssh server port: 22	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ip http port 8080	
Error Messages	Invalid: UI service management port port-number is duplicated.	
Related Commands	—	

Configure SNMP Server Port Number

This command sets the port number to be used in SNMP.

■Command

snmp-server port <port-number(1-65535)>

Item	Description	
Syntax Description	snmp-server	Configure SNMP server parameters
	port	Configure the service port of the SNMP server
	port-number	The service port number
Defaults	The default SNMP server port is set to 161	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# snmp-server port 1661	
Error Messages	—	
Related Commands	—	

Configure SNMP Server Transport Protocol Mode

This command sets the predefined protocol to be used in SNMP.

■Command

snmp-server transport-protocol { udp | tcp }

Item	Description	
Syntax Description	snmp-server	Configure SNMP server parameters
	transport-protocol	transport-protocol Transport layer protocol
	udp	udp User datagram protocol
	tcp	tcp Transmission control protocol
Defaults	udp	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# snmp-server transport-protocol udp melsec(config)# snmp-server transport-protocol tcp	
Error Messages	—	
Related Commands	snmp-server show snmp-server	

Configure Network Maximum Session Numbers

This command sets the maximum number of concurrent connections to the web interface.

■Command

ip http max-session <session-number(1-10)>

Item	Description	
Syntax Description	ip	Configure IP parameters
	http	Configure HTTP/HTTPS management UI service parameters
	max-session	Configure the maximum number of concurrent login sessions through HTTP and HTTPS
	session-number	The maximum number of login sessions
Defaults	The maximum number of concurrent HTTP sessions is set to 5 by default	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ip http max-session 3	
Error Messages	—	
Related Commands	—	

Configure Network Terminal Maximum Session Numbers

This command sets the maximum number of concurrent connections to the CLI.

■Command

```
ip terminal max-session <session-number(1-5)>
```

Item	Description	
Syntax Description	ip	Configure IP parameters
	terminal	Configure Telnet and SSH terminal parameters
	max-session	Configure the maximum number of concurrent login sessions through Telnet and SSH terminal
	session-number	Maximum number of login sessions
Defaults	max terminal session: 1	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec# configure terminal melsec(config)# ip terminal max-session 3	
Error Messages	—	
Related Commands	—	

Show Network Service Information

This command shows the interface information.

■Command

```
show ip service information
```

Item	Description	
Syntax Description	show	Display configuration/status information
	ip	Display IP information
	service	Display management UI service information
	information	Display the information for management UI services
Defaults	—	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show ip service information	
Error Messages	—	
Related Commands	—	

Configure Hardware Interface

Enables or disables the USB port.

■Command

hardware-interface usb {enable | disable}

Item	Description	
Syntax Description	hardware-interface	Configure hardware interface parameters
	usb	USB in device
	enable	Enable setting
	disable	disable setting
Defaults	enable	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# hardware-interface usb enable melsec(config)# hardware-interface usb disable	
Error Messages	—	
Related Commands	—	

Show Hardware Interface Information

Shows the USB port settings.

■Command

show hardware-interface

Item	Description	
Syntax Description	show	Display configuration information
	hardware-interface	Display hardware interface information
Defaults	—	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show hardware-interface USB: Enabled	
Error Messages	—	
Related Commands	—	

Configure Login Lockout Settings

This command sets the items related to lockout.

■Command

- login lockout <enable|disable>
- login lockout <minute(1-10)> attempts <tries(1-10)>

Item	Description	
Syntax Description	login	Configure login parameters
	lockout	Configure the maximum number of failed login attempts and the lockout time to block the user from logging in
	enable	Enable login lockout
	disable	Disable login lockout
	minute	Configure the lockout time ranging from 1 to 10 minutes
	attempts	Configure the maximum number of login attempts
	tries	The number of tries ranging from 1 to 10
Defaults	The login lockout is disabled by default lockout time: 5 minutes number of tries: 5	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	(config)# login lockout 10 attempts 5 (config)# login lockout enable (config)# login lockout disable	
Error Messages	—	
Related Commands	—	

Configure Login Banner

This command sets the login message.

■Command

- login banner <string (500)>
- no login banner

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	login	Configure login parameters
	banner	Configure a login banner
	string	The login banner content up to 500 characters
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	(config)# login banner "this is a banner" (config)# no login banner	
Error Messages	—	
Related Commands	—	

Configure Login Failure Message

This command sets the login failure message.

■Command

- login fail-message <string (500)>
- no login fail-message

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	login	Configure login parameters
	fail-message	Configure a login failure message
	string	The login failure message up to 500 characters
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	(config)# login fail-message "this is a failure message" (config)# no login fail-message	
Error Messages	—	
Related Commands	—	

Configure Timeout Value for a Session End

This command sets the items related to auto-logout.

■Command

session timeout <integer (0-1440)>

Item	Description	
Syntax Description	session	Configure session parameters
	timeout	Configure the session timeout value
	integer	The timeout value ranging from 1 to 1440 minutes. When timeout value is set to 0, session timeout is disabled.
Defaults	5	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	(config)# session timeout 100	
Error Messages	—	
Related Commands	—	

Show Session Timeout Information

This command shows the auto-logout setting.

■Command

show session timeout

Item	Description	
Syntax Description	show	Display running information
	session	Display session information
	timeout	Display session timeout information
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show session timeout	
Error Messages	—	
Related Commands	—	

Show Login Failure Message

This command shows the login failure message.

■Command

show login fail-message

Item	Description	
Syntax Description	show	Display running information
	login	Display login information
	fail-message	Display the login failure message
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show log fail-message	
Error Messages	—	
Related Commands	—	

Show Login Banner

This command shows the login message.

■Command

show login banner

Item	Description	
Syntax Description	show	Display running information
	login	Display login information
	banner	Display the login banner
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show log banner	
Error Messages	—	
Related Commands	—	

Configure Trusted Access Settings

This command sets the IP address to which access is permitted.

■Command

- trusted-access ip-source <ucast_addr> [{ <ip_mask> | "/" <short(0-32)> }]
- no trusted-access <ucast_addr> [{ <ip_mask> | "/" <short(0-32)> }]

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	trusted-access	Configure IP trusted access parameters
	ip-source	Configure the IP source
	ucast_addr	Configure the network or host IP address
	ip_mask	Configure the subnet mask of the IP address
	"/"	Configure the CIDR notation
	short (0-32)	Configure the prefix length
Defaults	Trusted access is disabled by default	
Command Modes	Global configuration	
Usage Guidelines	Trusted access will take effect when the "trusted-access enable" command is executed.	
Examples	melsec(config)# trusted-access ip-source 10.10.10.10 255.255.255.0 melsec(config)# trusted-access ip-source 20.10.10.10 / 24 melsec(config)# trusted-access ip-source 30.10.10.10 melsec(config)# no trusted-access ip-source 10.10.10.10 255.255.255.0 melsec(config)# no trusted-access ip-source 20.10.10.10 / 24 melsec(config)# no trusted-access ip-source 30.10.10.10	
Error Messages	—	
Related Commands	show trusted-access trusted-access enable	

Enable/Disable IP Trusted Access List

This command enables or disables the access permitted function.

■Command

- trusted-access <enable>
- trusted-access <disable>

Item	Description	
Syntax Description	trusted-access	Configure IP trusted access parameters
	enable	Enable the IP trusted access list
	disable	Disable the IP trusted access list
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# trusted-access enable melsec(config)# trusted-access disable	
Error Messages	—	
Related Commands	trusted-access disable	

Show Trusted Access IP List

This command shows the IP address to which access is permitted.

■Command

show trusted-access

Item	Description	
Syntax Description	show	Display configuration/status information
	trusted-access	Display IP trusted access information
Defaults	—	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show trusted-access	
Error Messages	% No such manager found % Manager is not configured	
Related Commands	trusted-access	

Re-generate New SSH Key

This command regenerates the key to be used for encryption.

■Command

ssh key generate

Item	Description	
Syntax Description	ssh	Configure SSH parameters
	key	Configure the SSH server key
	generate	Generate the SSH key
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# ssh key generate	
Error Messages	—	
Related Commands	—	

Re-generate New Web SSL Certificate

This command regenerates the SSL certificate.

■Command

web certificate generate

Item	Description	
Syntax Description	web	Configure web parameters
	certificate	Configure the web server certificate
	generate	Generate a self-signed certificate
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# web certificate generate	
Error Messages	—	
Related Commands	—	

Import New Web SSL Certificate via TFTP or SFTP

This command imports the SSL certificate.

■Command

web certificate import {<tftp_url> | <sftp_url>}

Item	Description	
Syntax Description	web	Configure web parameters
	certificate	Configure the web server certificate
	import	Import the certificate from a remote server
	tftp_url	The file on the remote TFTP server to be copied
	sftp_url	The file on the remote SFTP server to be copied
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# web certificate import tftp://192.168.1.1/server.crt	
Error Messages	Format or Password Error Server not Connected	
Related Commands	—	

Export Web SSL Certificate Signing Request via TFTP/SFTP

This command outputs the CSR file.

■Command

web signing-request export {<tftp_url> | <sftp_url>}

Item	Description	
Syntax Description	web	Configure Web related parameters
	signing-request	Configure the web server certificate signing request
	export	Export the certificate
	tftp_url	The file on the remote TFTP server to be copied
	sftp_url	The file on the remote SFTP server to be copied
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# web signing-request export tftp://192.168.1.1/server.csr	
Error Messages	Server not Connected	
Related Commands	—	

Enable/Disable Storm Control

This command sets the send/receive control.

■Command

- storm-control { bc | mc | bc_mc } level <rate-value(1000-1488000)>
- no storm-control {bc | mc | bc_mc }

Item	Description	
Syntax Description	no	Remove configuration delete entry/reset to default value
	storm-control	Configure storm control parameters
	bc	Configure broadcast packet storm control parameters
	mc	Configure multicast packet storm control parameters
	bc_mc	Configure broadcast and multicast packet storm control parameters
	level	Configure the control suppression level
	rate-value 1000-1488000	The storm control rate value
Defaults	Broadcast: enable Multicast: disable rate-value: 13000	
Command Modes	Interface configuration	
Usage Guidelines	—	
Examples	melsec# configure melsec(config)# interface ethernet 1/1 melsec(config-if)# storm-control bc level 1000 melsec# configure melsec(config)# interface ethernet 1/1 melsec(config-if)# storm-control bc_mc level 2000 melsec# configure melsec(config)# interface ethernet 1/1 melsec(config-if)# no storm-control bc	
Error Messages	'Invalid: The value of traffic storm control should be less than ingress rate limit threshold.' 'Invalid: Your configure value {}'.format(cfg_val) + ' exists too large bias because of limitation of hardware.' + ' We suggest configure the value {} again.'.format(suggest_cfg_val)	
Related Commands	—	

Show Storm Control Status

This command shows the send/receive control setting.

■Command

Show storm control interface [<ifXtype> <ifnum>]

Item	Description	
Syntax Description	show	Display configuration/status information
	interface	Display interface information
	ifXtype	The interface type
	ifnum	The interface number
	storm-control	Display the broadcast, multicast storm control suppression levels of the interface
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show storm-control interface ethernet 1/1	
Error Messages	—	
Related Commands	melsec (config-if)# storm-control {bc | mc | bc_mc } level <rate-value(1000-1488100)> melsec (config-if)# no storm-control {bc | mc | bc_mc }	

Show Login Authentication

This command shows the login authentication method.

■Command

show login authentication

Item	Description	
Syntax Description	show	Display running information
	login	Display login information
	authentication	Display authentication information
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show login authentication	
Error Messages	—	
Related Commands	—	

Configure Login Authentication Settings

This command sets the login authentication method.

■Command

login authentication [{ radius | tacacs }] [local]

Item	Description	
Syntax Description	login	Configure login parameters
	authentication	Configure authentication parameters
	radius	Configure RADIUS authentication servers
	tacacs	Configure a TACACS authentication system
	local	Configure a local authentication database
Defaults	Local	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# login authentication radius melsec(config)# login authentication tacacs melsec(config)# login authentication local melsec(config)# login authentication radius local melsec(config)# login authentication tacacs local	
Error Messages	—	
Related Commands	—	

Configure RADIUS Server Host Settings

This command sets the RADIUS server to be connected.

■Command

- radius-server host { <ucast_addr> } [auth-port {<integer(1-65535)>}] [timeout {<short(5-180)>}] [retransmit {<short(0-5)>}] key {<string(60)>} authtype { pap | chap | mschap } { primary | secondary }
- no radius-server { primary | secondary }

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	radius-server	Configure RADIUS server parameters
	host	Configure the RADIUS host
	auth-port	Configures the UDP destination port for authentication requests
	timeout	Configure time period (in seconds) until which a client waits for a response from the server before re-transmitting the request
	retransmit	Configure the maximum number of attempts the client undertakes to contact the server
	key	Configure the RADIUS server encryption key
	authtype	Configure the authentication type of the RADIUS server
	primary	Set as the primary server
	secondary	Set as the secondary server
Defaults	host: 0.0.0.0 auth-port: 1812 timeout: 5 retransmit: 1 key: — authtype: chap	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec(config)# radius-server host 1.1.1.1 auth-port 2222 timeout 5 retransmit 5 key test authtype pap primary melsec(config)# no radius-server primary	
Error Messages	—	
Related Commands	—	

Show RADIUS Server Information

This command shows the RADIUS server to be connected.

■Command

show radius-server

Item	Description	
Syntax Description	show	Display running information
	radius- server	Display the RADIUS server parameters
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show radius-server	
Error Messages	—	
Related Commands	—	

Configure TACACS+ Server Host Settings

This command sets the TACACS+ server to be connected.

■Command

- tacacs-server host { <ucast_addr> } [auth-port {<integer(1-65535)>}] [timeout {<short(5-130)>}] [retransmit {<short(0-5)>}] key {<string(60)>} authtype { pap | chap | ascii } { primary | secondary }
- no tacacs-server { primary | secondary }

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	tacacs -server	Configure TACACS server parameters
	host	Configure TACACS host parameters
	auth-port	Configure authentication port parameters
	timeout	Configure timeout parameters
	retransmit	Configure the maximum number of attempts the client undertakes to contact the server
	key	Configure the per-server encryption key
	authtype	Configure the authentication type of the TACACS server
	primary	Set as the primary server
	secondary	Set as the secondary server
Defaults	host: 0.0.0.0 auth-port: 49 timeout: 5 retransmit: 1 key: — authtype: chap	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	(config)# tacacs-server host 1.1.1.1 auth-port 2222 timeout 5 retransmit 5 key test authtype pap primary (config)# no tacacs-server primary	
Error Messages	—	
Related Commands	—	

Show TACACS+ Server Information

This command shows the TACACS+ server to be connected.

■Command

show tacacs-server

Item	Description	
Syntax Description	show	Displays running information
	tacacs-server	Displays the TACACS server parameters
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show tacacs-server	
Error Messages	—	
Related Commands	—	

Show Device Current Information

This command shows the current system utilization of the managed switch.

■Command

show env {all | power | RAM | CPU }

Item	Description	
Syntax Description	show	Display the statistics information
	env	Display switch information
	all	Show the current information for all resources such as CPU, RAM, and power
	power	Show the current power input information
	RAM	Show the current RAM information
	CPU	Show the current CPU information
Defaults	—	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	—	
Examples	# show env all # show env power # show env RAM # show env CPU	
Error Messages	—	
Related Commands	—	

Show Traffic Statistics

This command shows the statistical information.

■Command

show statistics [interface <interface-type> <interface-id>]

Item	Description	
Syntax Description	show	Display configuration/status information
	statistics	Display the interface statistics table
	interface-type	Display interface information
	interface-id	Display the specific interface information
Defaults	—	
Command Modes	Privileged EXEC Mode.	
Usage Guidelines	—	
Examples	melsec# show statistics interface ethernet 1/1	
Error Messages	—	
Related Commands	clear statistics	

Clear Traffic Statistics

This command clears the statistical information.

■Command

clear statistics [interface < interface-type> <interface-id>]

Item	Description	
Syntax Description	clear	Clear input
	statistics	Clear statistics
	interface-type	The interface type
	interface-id	The interface ID
Defaults	—	
Command Modes	Privileged EXEC Mode.	
Usage Guidelines	—	
Examples	melsec# clear statistics interface ethernet 1/1	
Error Messages	—	
Related Commands	show statistics	

Show Event Notification

This command shows the event notification settings.

■Command

show event-notification {general-event | port-event | switching-event}

Item	Description	
Syntax Description	show	Displays running information for the feature
	event-notification	Display event-notification configuration
	general-event	general event config
	port-event	port event config
	switching-event	switching event config
Defaults	—	
Command Modes	Privileged EXEC /User EXEC	
Usage Guidelines	—	
Examples	melsec# show event-notification port-event	
Error Messages	—	
Related Commands	event-notification general-event event-notification switching-event	

Configure Event Notification Settings

This command sets the events related to the system that provides notifications.

■Command

- event-notification general-event { all | cold-start | warm-start | config-change | login-success | login-fail | login-lockout | account-setting-changed | password-changed | config-import | ssl-certificated-changed | log-capacity | power-on | power-off | di-on |di-off}
- event-notification general-event { all | cold-start | warm-start | config-change | login-success | login-fail | login-lockout | account-setting-changed | password-changed | config-import | ssl-certificated-changed | log-capacity | power-on | power-off | di-on |di-off} action [{ trap | email | relay }]
- no event-notification general-event { all | cold-start | warm-start | config-change | login-success | login-fail | login-lockout | account-setting-changed | password-changed | config-import | ssl-certificated-changed | log-capacity | power-on | power-off | di-on |di-off}

Item	Description	
Syntax Description	no	Disable the configuration/deletes the entry/reset to default value
	event-notification	Configure event notifications
	general-event	Configure notifications for general events
	all	Notify for all general events
	cold-start	Notify when the system performs a cold start
	warm-start	Notify when the system performs a warm start
	config-change	Notify when the system configuration changes
	login-success	Notify when a user successfully logs in
	login-fail	Notify when a user failed to log in
	login-lockout	Notify when a user is locked out due to the login policy
	account-setting-changed	Notify when the user account information changes, including create account, remove account, and change of username, permission
	password-changed	Notify when the user account password changes
	config-import	Notify when the system configuration is imported
	ssl-certificated-changed	Notify when system certification changes
	log-capacity	Notify when the system log reaches the capacity threshold
	power-on	Notify when the power supply is on
	power-off	Notify when the power supply is off
	di-on	Notify when the digital input is on
	di-off	Notify when the digital input is off
	action	Set action for event notification
	trap	Set trap action for notification
	email	Set email action for notification
	relay	Set relay action for notification
Defaults	All configuration, trap, email event notifications are enabled by default	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec# config melsec(config)# event-notification general-event all action trap email relay melsec(config)# no event-notification general-event all action trap email relay	
Error Messages	—	
Related Commands	show event-notification event-notification switching-event	

Configure Notification for Switching Event Settings

This command sets the events related to the relay that provides notifications.

■Command

- event-notification switching-event { all | rstp-topology-changed | lldp-table-changed }
- event-notification switching-event { all | rstp-topology-changed | lldp-table-changed } action [{ trap | email | relay }]
- no event-notification switching-event { all | rstp-topology-changed | lldp-table-changed }

Item	Description	
Syntax Description	no	Disable the configuration/deletes the entry/resets to default value
	event-notification	Configure event notifications
	switching-event	Configure notifications for switching events
	all	Notify for all switching events
	rstp-topology-changed	Notify when the RSTP network topology changes
	lldp-table-changed	Notify when the LLDP remote table changes
	action	Set action for event notification
	trap	Set trap action for notification
	email	Set email action for notification
	relay	Set relay action for notification
Defaults	All configuration, trap, email event notifications are enabled by default	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	melsec# config melsec(config)# event-notification switching-event all action trap melsec(config)# no event-notification switching-event all action trap email	
Error Messages	—	
Related Commands	show event-notification event-notification general-event	

Configure Relay Alarm Cut-off Settings

This command cuts off the relay alarm.

■Command

relay alarm cut-off relay

Item	Description	
Syntax Description	relay	Configure relay parameters
	alarm	Configure the relay alarm
	cut-off	Configure the relay alarm cut-off
	relay	Cut off the relay alarm
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# relay alarm cut-off relay	
Error Messages	—	
Related Commands	—	

Configure Email Notification Server

This command sets the SMTP server to be used for email notifications.

■Command

email-notification server server-address <ucast_addr> [server-port <integer(1-65535)>] username <string(60)> password <string(60)>

Item	Description	
Syntax Description	email-notification	Configure email notification parameters
	server	Configure server parameters
	server-address	Configure the email notification server IP address
	server-port	Configure the email-notification server port
	username	Configure the email notification server username
	password	Configure the email notification server password
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	(config)# email-notification server-address 1.2.3.4 username aaa password bbb	
Error Messages	—	
Related Commands	—	

Configure Email Notification Sender

This command sets the email address of the managed switch.

■Command

email-notification sender <string (60)>

Item	Description	
Syntax Description	email-notification	Configure email notification parameters
	sender	Configure the email notification sender's email address
	string (60)	The sender's email address up to 60 characters
Defaults	Sender Address: admin@localhost.com	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	(config)# email-notification sender testuser@test.com	
Error Messages	Invalid Email Format	
Related Commands	—	

Configure Email Notification Server TLS Mode Setting

This command enables or disables TLS at email transmission.

■Command

email-notification server tls {enable | disable}

Item	Description	
Syntax Description	email-notification	Configure email notification parameters
	server	Configure server parameters
	tls	Configure the email notification server TLS mode
	enable	Enable the TLS mode
	disable	Disable the TLS mode
Defaults	Disable	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	(config)# email-notification server tls enable (config)# email-notification server tls disable	
Error Messages	—	
Related Commands	—	

Configure Email Notification Receiver

This command sets the email address at which email notifications are to be received.

■Command

- email-notification receiver <string (60)> index <integer (1-5)>
- no email-notification receiver index <integer (1-5)>

Item	Description	
Syntax Description	no	Disable the configuration/delete the entry/reset to default value
	email-notification	Configure email notification parameters
	receiver	Configure the email notification receiver
	index	Configure the index of the receiver
	string (60)	The receiver's name up to 60 characters
	integer (1-5)	The number index of the receiver ranging from 1 to 5
Defaults	—	
Command Modes	Global configuration	
Usage Guidelines	—	
Examples	(config)# email-notification receiver testuser@test.com index 1 (config)# no email-notification receiver index 1	
Error Messages	Invalid Email Format	
Related Commands	—	

Show Email Notification Server

This command shows the SMTP server to be used for email notifications.

■Command

show email-notification server

Item	Description	
Syntax Description	show	Display the configuration/statistics/general information
	email-notification	Display email notification parameters
	server	Display server parameters
Defaults	—	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	—	
Examples	# show email-notification server	
Error Messages	—	
Related Commands	—	

Configure Logging Server

This command sets the Syslog server of the save destination.

■Command

logging-server <short(1-3)> { ipv4 <ucast_addr> | <dns_host_name> } [port <integer(1-65535)>

Item	Description	
Syntax Description	logging-server	Configure logging server parameters
	short (1-3)	The index of the syslog server
	ipv4	Configure IPv4 parameters
	ucast_addr	The IP address
	dns_host_name	The host domain name
	port	Configure port parameters
	integer (1-65535)	The port number
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# logging-server 1 ipv4 10.128.1.8 port 514	
Error Messages	'Invalid: The server addresses are duplicated.' 'Invalid: The syslog server address cannot be empty if it is enabled.'	
Related Commands	no logging-server <short(1-3)> show logging syslog-server	

Delete Logging Server

This command deletes the Syslog server of the save destination.

■Command

no logging-server <short(1-3)> [enable]

Item	Description	
Syntax Description	no	Remove configuration / delete entry / reset to default value
	logging-server	Configure logging server parameters
	short (1-3)	The index of the syslog server
	enable	Disable this server entry
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# no logging-server 1	
Error Messages	—	
Related Commands	logging-server <short(1-3)> {ipv4 <ucast_addr> | <dns_host_name>} [port <integer(1-65535)>] show logging syslog-server	

Enable/Disable Logging Syslog Server

This command enables or disables log saving to the Syslog server.

■Command

logging syslog-server { enable | disable }

Item	Description	
Syntax Description	logging	Configure logging parameters
	syslog-server	Configure the syslog server
	enable	Enable the syslog server
	disable	Disable the syslog server
Defaults	—	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# logging syslog-server enable	
Error Messages	—	
Related Commands	show logging syslog-server	

Show Syslog Server Configuration

This command shows the Syslog server of the save destination.

■Command

show logging syslog-server

Item	Description	
Syntax Description	show	Display configuration/status information
	logging	Display logging information
	syslog-server	Display syslog server information
Defaults	—	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	Display the Syslog logging server table	
Examples	melsec# show logging syslog-server	
Error Messages	—	
Related Commands	logging syslog-server enable logging-server <short(1-3)> {ipv4 <ucast_addr> | <dns_host_name>} [port <integer(1-65535)>]	

Show LLDP Information

This command shows the LLDP information.

■Command

show lldp

Item	Description	
Syntax Description	show	Display configuration/statistics/general information
	lldp	Display global LLDP information
Defaults	—	
Command Modes	Privileged EXEC User EXEC	
Usage Guidelines	Display the global LLDP settings	
Examples	melsec# show lldp	
Error Messages	—	
Related Commands	lldp {enable | disable} lldp holdtime-multiplier <2-10> lldp transmit-interval <seconds(5-32768)>	

Show LLDP Neighbors

This command shows the information related to neighboring devices.

■Command

show lldp neighbors

Item	Description	
Syntax Description	show	Display configuration/statistics/general information
	lldp	Display the LLDP interface status
	neighbors	Display the LLDP remote interface database
Defaults	—	
Command Modes	Privileged EXEC User EXEC	
Usage Guidelines	Display LLDP neighbor interface information	
Examples	melsec# show lldp neighbors	
Error Messages	—	

Show LLDP Traffic

This command shows the statistical information of LLDP communications.

■Command

show lldp traffic

Item	Description	
Syntax Description	show	Display configuration/statistics/general information
	lldp	Display the LLDP interface status
	traffic	Display the LLDP local traffic
Defaults	—	
Command Modes	Privileged EXEC User EXEC	
Usage Guidelines	Display LLDP traffic for the local counter	
Examples	melsec# show lldp traffic	
Error Messages	—	
Related Commands	show lldp	

Enable/Disable LLDP Function

This command enables or disables LLDP.

■Command

- lldp enable
- lldp disable

Item	Description	
Syntax Description	lldp	Configure LLDP parameters
	enable	Enable LLDP
	disable	Disable LLDP
Defaults	Enable	
Command Modes	Global Configuration	
Usage Guidelines	Enable or disable global LLDP	
Examples	melsec (config)# lldp enable melsec (config)# lldp disable	
Error Messages	—	
Related Commands	show lldp show lldp neighbors show lldp traffic	

Configure Global LLDP Transmission Timer Interval

This command sets the transmission interval of the LLDP messages.

■Command

- lldp transmit-interval <seconds (5-32768)>
- no lldp transmit-interval

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	lldp	Configure LLDP parameters
	transmit-interval	Configure the transmit interval
	seconds	The interval time ranging from 5 to 32768 seconds
Defaults	The interval between successive transmit cycles is set to 30 seconds by default	
Command Modes	Global Configuration	
Usage Guidelines	Configure the global LLDP transmit interval time	
Examples	melsec(config)# lldp transmit-interval 30 melsec(config)# no lldp transmit-interval	
Error Messages	—	
Related Commands	show lldp lldp enable	

Configure LLDP Holdtime Multiplier

This command sets the information hold time at the neighboring devices.

■Command

- lldp holdtime-multiplier <value (2-10)>
- no lldp holdtime-multiplier

Item	Description	
Syntax Description	no	Remove configuration/delete entry/reset to default value
	lldp	Configure LLDP parameters
	holdtime-multiplier	A multiplier on the transmit-interval used to compute the TTL value of txTTL.
	value	The multiplier value ranging from 2 to 10
Defaults	The default holdtime multiplier is set to 4	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# lldp holdtime-multiplier 4 melsec(config)# no lldp holdtime-multiplier	
Error Messages	—	
Related Commands	show lldp lldp enable	

Ping the Host

This command executes a ping test.

■Command

ping <host> [repeat <repeat-count(1-10)>] [size <payload-size(36-2080)>] [timeout <request-timeout(1-100)>]

Item	Description	
Syntax Description	ping	Ping a target to check its status
	host	The IP address or domain name of the node to be pinged
	repeat	The number of ping packets that are sent to the destination address
	repeat-count	The repeat value
	size	The size of the ping packet
	payload-size	The length of the ping packet value
	timeout	The time in seconds after which the entity waiting for the ping response times out
	request-timeout	The timeout value
Defaults	—	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# ping 192.168.127.254 repeat 5	
Error Messages	—	
Related Commands	—	

Show IP ARP Table

This command shows the ARP table.

■Command

show ip arp

Item	Description	
Syntax Description	show	Display configuration/status information
	ip	Display IP information
	arp	Display the ARP table
Defaults	—	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# show ip arp	
Error Messages	—	
Related Commands	—	

Show Logging Event Log

This command shows the event logs.

■Command

show logging event-log

Item	Description	
Syntax Description	show	Display configuration/status information
	logging	Display logging information
	event-log	Display event log entries
Defaults	—	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	Display the log entries information	
Examples	melsec# show logging event-log	
Error Messages	—	
Related Commands	clear logging event-log	

Show Logging Log Capacity

This command shows the threshold value by which to perform event notification.

■Command

show logging log-capacity

Item	Description	
Syntax Description	show	Display configuration/status information
	logging	Display logging information
	log-capacity	Display log capacity information
Defaults	—	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	—	
Examples	melsec# show logging log-capacity	
Error Messages	—	
Related Commands	—	

Clear Logging Event Log

This command clears all the event logs.

■Command

clear logging event-log

Item	Description	
Syntax Description	clear	Clear the event
	logging	Display logging information
	event-log	The local event log entries to be cleared
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# clear logging event-log	
Error Messages	—	
Related Commands	show logging event-log	

Export Event Log File

This command outputs the event logs.

■Command

copy event-log {tftp://server/filename | sftp://<user-name>:<pass-word>@server/filename | usb}

Item	Description	
Syntax Description	copy	Copy the target file or input
	event-log	The system event log
	tftp://server/filename	The address of the remote TFTP server in the format "tftp://server/filename"
	sftp://<username>:<password>@server/filename	The address of the remote SFTP server in the format "sftp://username:password@server/filename"
	usb[*1]	Copy event-log to USB Memory
Defaults	—	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# copy event-log tftp://192.168.127.11/test1.log melsec# copy event-log usb	
Error Messages	Invalid: Not support USB. Invalid: USB function is disable	
Related Commands	show logging event-log	

[*1] This command can be used with firmware version "05" or later.

Configure Event Log Capacity Settings

This command sets the threshold value by which to perform event notification.

■Command

logging log-capacity threshold <short (50-100)>

Item	Description	
Syntax Description	logging	Configure logging parameters
	log-capacity	Configure the log capacity
	threshold	Configure the log capacity threshold
	short (50-100)	The log capacity threshold in percentage
Defaults	The default log threshold is set to 80 entries	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# logging log-capacity threshold 80	
Error Messages	—	
Related Commands	—	

Delete Logging Log Capacity Threshold

This command deletes the threshold value by which to perform event notification.

■Command

no logging log-capacity threshold

Item	Description	
Syntax Description	no	Remove configuration / delete entry / reset to default value
	logging	Configure logging parameters
	log-capacity	Configure the log capacity
	threshold	Configure the log capacity threshold
Defaults	The default log threshold is set to 80 entries	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# no logging log-capacity threshold	
Error Messages	—	
Related Commands	logging log-capacity threshold	

Configure Oversized Log Action Setting

This command sets the event to be notified when the threshold value is exceeded.

■Command

logging oversize-action { overwrite-oldest | stop-recording }

Item	Description	
Syntax Description	logging	Configure logging parameters
	oversize-action	Configure the action when exceeding the log threshold
	overwrite-oldest	Overwrite the oldest entry
	stop-recording	Stop recording events
Defaults	overwrite-oldest	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# logging oversize-action overwrite-oldest melsec(config)# logging oversize-action stop-recording	
Error Messages	—	
Related Commands	—	

Configure Auto Backup Event Log

Enables or disables event log automatic backup.

■Command

auto-backup log { enable | disable }

Item	Description	
Syntax Description	auto-backup	Auto backup file to external storage
	log	log file
	enable	Enable setting
	disable	Disable setting
Defaults	enable	
Command Modes	Global Configuration	
Usage Guidelines	—	
Examples	melsec(config)# auto-backup log enable melsec(config)# auto-backup log disable	
Error Messages	—	
Related Commands	—	

Show the Locator

This command flashes the LEDs of the managed switch.

■Command

locator [<duration (30-300)>]

Item	Description	
Syntax Description	locator	Activate the device locator so that the LED on the device blinks
	duration	The duration of locator activation in seconds
Defaults	The locator duration is set to 60 seconds by default	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# locator 100	
Error Messages	—	
Related Commands	—	

Reboot the Switch

This command restarts the managed switch.

■Command

reload

Item	Description	
Syntax Description	reload	Perform a warm restart
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# reload	
Error Messages	—	
Related Commands	—	

Reset to Default

This command resets the managed switch settings to default.

■Command

reload factory-default

Item	Description	
Syntax Description	reload	Perform a warm restart
	factory-default	Perform a warm restart and restore the factory default settings
Defaults	—	
Command Modes	Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# reload factory-default	
Error Messages	—	
Related Commands	—	

Logout

This command logs out the user from the managed switch.

■Command

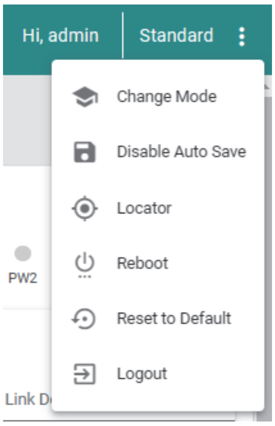
logout

Item	Description	
Syntax Description	logout	Log out from the device
Defaults	—	
Command Modes	User EXEC Privileged EXEC	
Usage Guidelines	—	
Examples	melsec# logout	
Error Messages	—	
Related Commands	—	

Appendix 2 Maintenance/Tool

The following operations can be performed by clicking the [Menu icon] button at the upper right of the web interface window.

- Configuration mode change
- Autosave
- Position check
- Reboot
- Setting initialization
- Logout



Configuration mode change

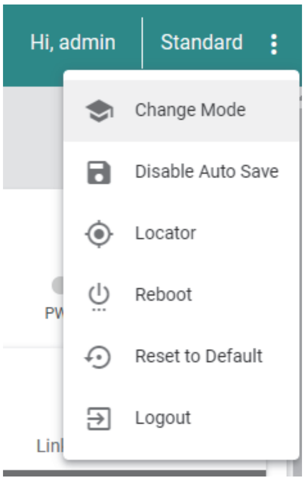
This operation allows the configuration mode of the managed switch to be switched.

Mode name	Description
Standard Mode (Default)	The standard configuration mode
Advanced Mode	The following functions can be set. • IPv6 address setting (☞ Page 106 IP configuration [IP Configuration]) • Link Type setting for the spanning tree function (☞ Page 179 Spanning tree function)

Setting method

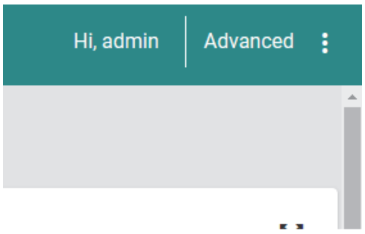
Operating procedure

1. Click the [Change Mode] button.



2. Click the [Change] button.

3. The configuration mode is changed.



Point

To change from Advanced Mode to Standard Mode, follow the same procedure.

Autosave

This operation enables or disables autosave, a function by which the configurations are automatically saved when applied.

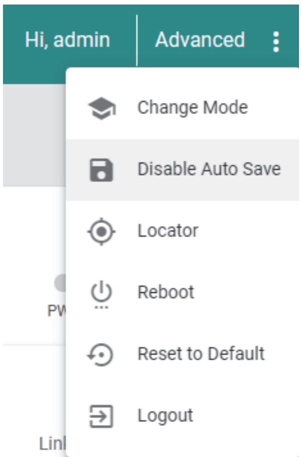
Autosave	Description
Enable (Default)	The configurations are saved when the [Apply] button, [Create] button, or [Delete] button is clicked.
Disable	The configurations are saved when the [Save Disk] button is clicked.

Setting method

■Changing from enable to disable

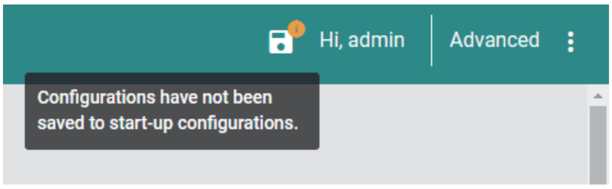
Operating procedure

1. Click the [Disable Auto Save] button.



2. A confirmation dialog appears. Click the [Disable] button.

3. Autosave is disabled and the [Save Disk] button is displayed.

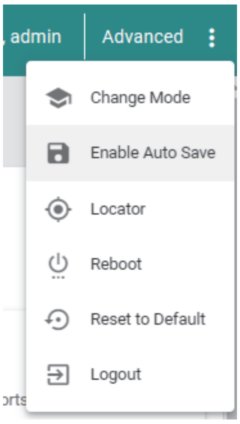


Configurations have not been saved to start-up configurations.

■Changing from disable to enable

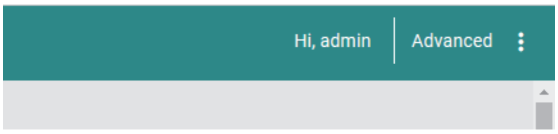
Operating procedure

1. Click the [Enable Auto Save] button.



2. A confirmation dialog appears. Click the [Enable] button to enable autosave.

3. Autosave is enabled and the [Save Disk] button is hidden.



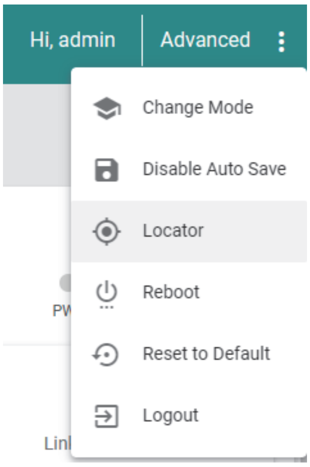
Position check

This operation allows the installation location of the managed switch to be checked. The RUN LED, ERR LED, and SYNC LED of the managed switch alternately flash.

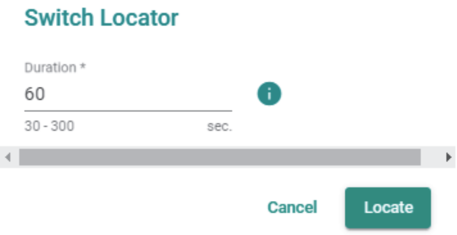
Setting method

Operating procedure

1. Click the [Locator] button.



2. Set the flashing duration.



Item	Description	Setting range
Duration	Set the LED flashing duration. (Unit: Second)	30 to 300 (Default: 60)

3. Click the [Locate] button.

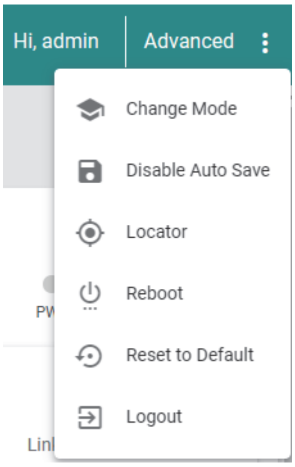
Reboot

This operation restarts the managed switch from the web interface.
Before executing this operation, stop any connected facilities or devices that are running. Otherwise, unexpected operations may occur.

Setting method

Operating procedure

1. Click the [Reboot] button.



2. A confirmation dialog appears. Click the [Restart] button to restart the managed switch.
3. The managed switch is restarted.

Setting initialization

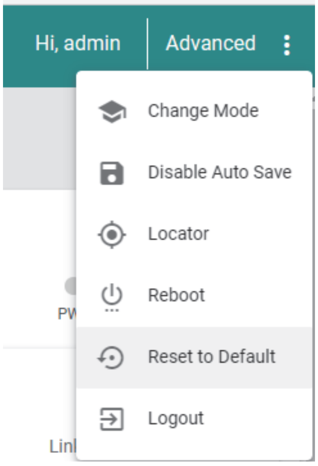
This operation resets all the configurations of the managed switch to default from the web interface.

When the configurations are initialized, the managed switch automatically restarts. Before executing this operation, stop any connected facilities or devices that are running. Otherwise, unexpected operations may occur.

Setting method

Operating procedure

1. Click the [Reset to Default] button.



2. A confirmation dialog appears. Click the [Reset] button to initialize the configurations.

3. The managed switch restarts and all the configurations are reset to default.

A

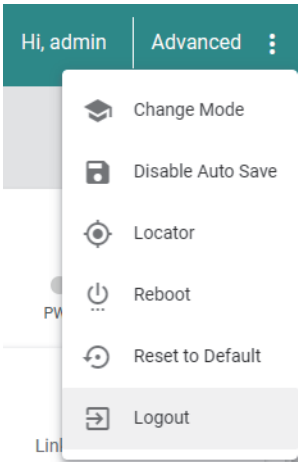
Logout

This operation is for logging out from the web interface.

Setting method

Operating procedure

1. Click the [Logout] button.



2. A confirmation dialog appears. Click the [Logout] button to log out.
3. The managed switch logs out.

Appendix 3 EMC and Low Voltage Directives

In each country, laws and regulations concerning electromagnetic compatibility (EMC) and electrical safety are enacted.
For the products sold in the European countries, compliance with the EU's EMC Directive has been a legal obligation as EMC regulation since 1996, as well as the EU's Low Voltage Directive as electrical safety regulation since 1997.
Manufacturers who recognize their products are compliant with the EMC and Low Voltage Directives are required to attach a "CE marking" on their products in European countries.
In some other countries and regions, manufacturers are required to make their products compliant with applicable laws or regulations and attach a certification mark on the products as well (such as UK Conformity Assessed (UKCA) marking in the UK, and Korea Certification (KC) marking in South Korea).
Each country works to make their regulatory requirements consistent across countries based on international standards.
When the requirements are consistent, measures to comply with the EMC and electrical safety regulations become common across countries.
The UK and South Korea have enacted EMC regulations whose requirements are consistent with those of the EMC Directive.
The UK has also enacted electrical safety regulations whose requirements are consistent with those of the Low Voltage Directive. In this section, the requirements of the EMC and Low Voltage Directives are described as examples of those of the EMC and electrical safety regulations.

Measures to comply with the EMC Directive

The EMC Directive sets requirements for emission (conducted and radiated electromagnetic interference emitted by a product) and immunity (the ability of a product not to be influenced by externally generated electromagnetic interference).
This section describes the precautions for machinery constructed with the module to comply with the EMC Directive.
These precautions are based on the requirements of the EMC Directive and the harmonized standards. However, they do not guarantee that the entire machinery constructed according to the descriptions complies with the EMC Directive.
The manufacturer of the machinery must determine the testing method for compliance and declare conformity to the EMC Directive.

EMC Directive related standards

■Emission requirements

Specifications: EN IEC 61000-6-4: 2019 Class A, EN55032: 2015+A11: 2020, Class A

Test item	Test description	Value of standard
Radiated emission EN IEC 61000-6-4:2019 EN55032: 2015+AC: 2016 CISPR32: Ed. 2.0	Radio waves from the product are measured.	• 30 to 230MHzQP: 40dBuV/m (measured at 10m distance) • 230 to 1000MHzQP: 47dBuV/m (measured at 10m distance) • 1 to 3GHzQP: 76dBuV/m (measured at 3m distance) • 3 to 6GHzQP: 80dBuV/m (measured at 3m distance)
Conducted emission (Power supply terminal) EN IEC 61000-6-4:2019 EN55032: 2015+AC: 2016 CISPR32: Ed. 2.0	Noise from the product to the power supply line is measured.	• 0.15 to 0.5MHzQP: 79dB, Mean: 66dB • 0.5 to 30MHzQP: 73dB, Mean: 60dB
Conducted emission (Communication port) EN IEC 61000-6-4:2019 EN55032: 2015+AC: 2016 CISPR32: Ed. 2.0		• 0.15 to 0.5MHzQP: 97 to 87dB, Mean: 84 to 74dB • 0.5 to 30MHzQP: 87dB, Mean: 74dB

■Immunity requirements

Specifications: EN IEC 61000-6-2: 2019, EN55035: 2017+A11: 2020

Test item	Test description	Value of standard
Electrostatic discharge immunity IEC 61000-4-2 Ed.2.0:2008	Immunity test in which static electricity is applied to the cabinet of the equipment	• 8kV: Air discharge • 4kV: Contact discharge
Radiated, radio-frequency electromagnetic field immunity IEC 61000-4-3 Ed.4.0:2020	Immunity test in which electric fields are irradiated to the product	80% AM modulation @1kHz • 80 to 1000MHz: 10V/m • 1.4 to 6.0GHz: 3V/m
Fast transient burst immunity IEC 61000-4-4 Ed.3.0:2012	Immunity test in which burst noise is applied to the power supply line and signal line	• DC power supply: 2kV • I/O and communication cable: 1kV
Surge immunity IEC 61000-4-5 Ed.3.1:2014 +A1:2017	Immunity test in which lightning surge is applied to the power supply line and signal line	• DC power supply: 1kV CM, 0.5kV DM • I/O and communication: 1kV CM
Conducted RF immunity IEC 61000-4-6 Ed.4.0:2013	Immunity test in which high frequency noise is applied to the power supply line and signal line	0.15 to 80MHz, 80% AM modulation @1kHz, 10Vrms
Power-frequency magnetic field immunity IEC 61000-4-8 Ed.2.0:2009	Immunity test in which the product is installed in the magnetic field of an induction coil	50/60Hz, 30A/m

Installation

For FG connection, use the thickest cable (maximum of 2㎟). Also, bring the FG grounding point to the module as much as possible so that the wire is shortened and the resistance value is 0.02Ω or less. For other instructions, refer to the following.

☞ Page 25 INSTALLATION AND WIRING

To make the programmable controller system in use comply with the EMC Directive, refer to the user's manual for the CPU module used.

Requirements for Low Voltage Directive compliance

The module operates at the rated voltage of 12VDC, 24VDC, and 48VDC. However, the modules which operate at less than 50VAC/75VDC rated input voltage are not targeted for the Low Voltage Directive compliance.

To make the programmable controller system in use comply with the EMC Directive, refer to the user's manual for the CPU module used.

Appendix 4 Indications Based on Radio Interference Regulations of Each Country/Region

Federal Communications Commission (FCC) Statement

It's herewith confirmed this device compiles with Part15 of the FCC Rules. Operation is subject to the following two conditions.

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

It is understood that each unit marketed is identical to the device as tested, and any changes to the device that could adversely affect the emission characteristics will require retest.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

VCCI Class A precautions

This equipment is the Class A information technology equipment. If this equipment is used in home environment, radio interference may occur. In such case, the user may be requested to take appropriate measures. VCCI-A

KC Statement

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다 .(Translation: This equipment has KC approval to be used for industrial environments and therefore it has possibility of interferences with household equipment.)

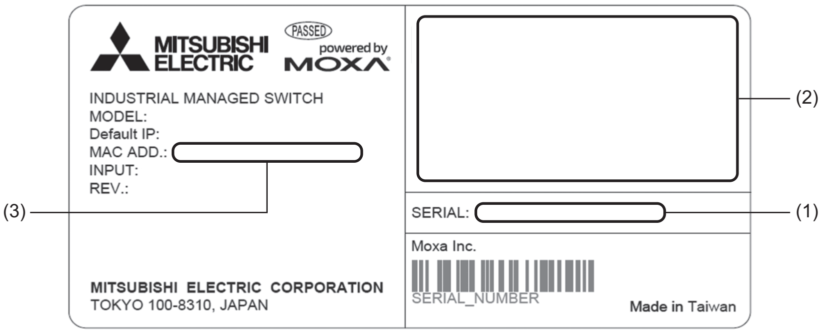
Appendix 4 Indications Based on Radio Interference Regulations of Each Country/Region

Appendix 5 Checking Production Information and Firmware Version

This section describes how to check the production information and firmware version of the managed switch.

Checking with the rating plate

The rating plate is located on the side of the managed switch.



(1) Production information

(2) Relevant standard symbol

(3) MAC address

Checking with the web interface

The information can be checked from Device Summary on the web interface. (☞ Page 60 Model Information)

Appendix 6 Open Source Software

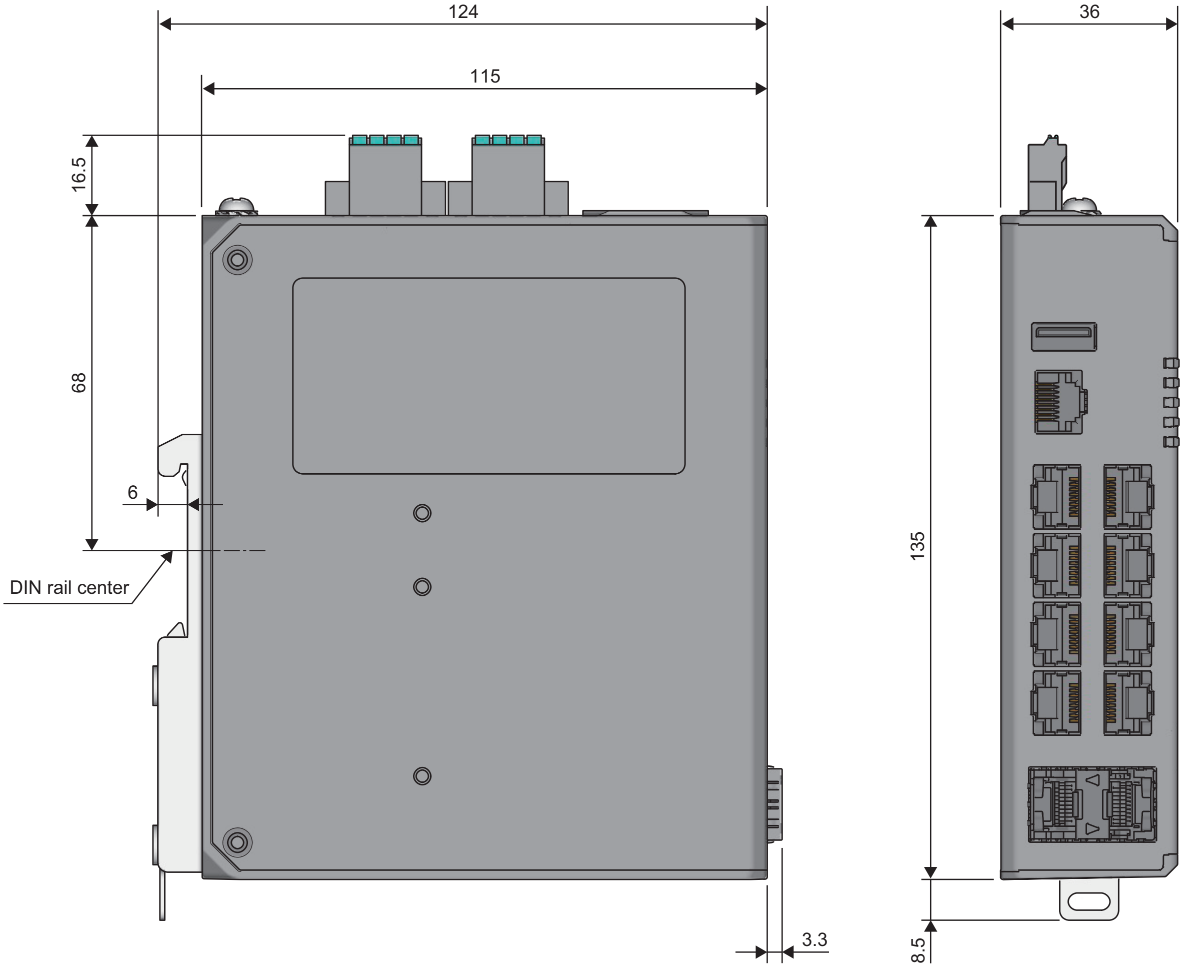
This product uses open source software.

For details, please consult your local Mitsubishi Electric representative.

Appendix 7 External Dimensions

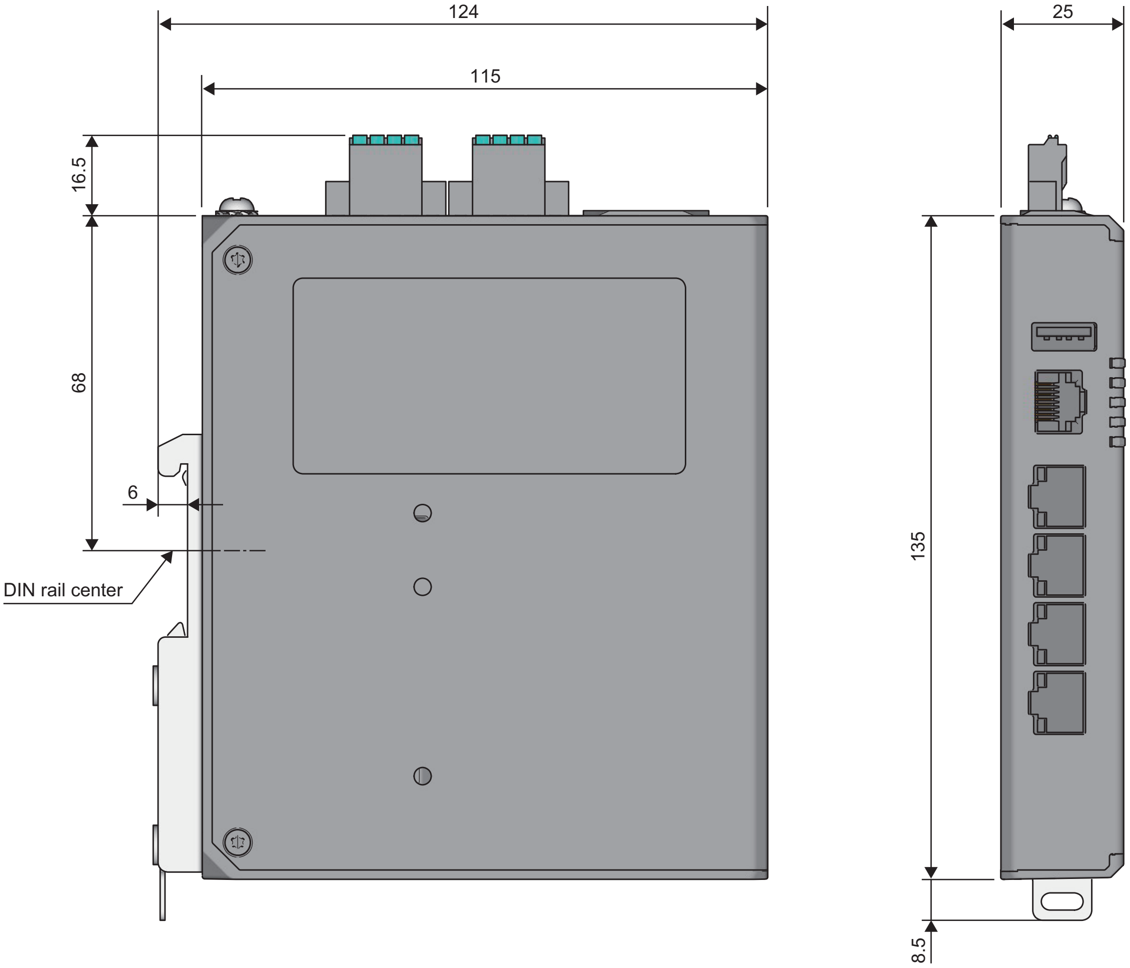
This section describes the external dimensions of the managed switch.

NZ2MHG-TSNT8F2



(Unit: mm)

NZ2MHG-TSNT4



(Unit: mm)

Appendix 8 Added and Enhanced Functions

The following table lists added or enhanced functions for the managed switch.

Added and enhanced function	Firmware version	
	NZ2MHG-TSNT8F2	NZ2MHG-TSNT4
Supported USB flash drives (connectable products)	"05" or later	"05" or later

MEMO

INDEX

REVISIONS

*The manual number is given on the bottom left of the back cover.

Revision date	*Manual number	Description
November 2021	SH(NA)-082449ENG-A	First edition
April 2022	SH(NA)-082449ENG-B	■Added or modified parts Section 8.11, 8.13, Appendix 1
July 2022	SH(NA)-082449ENG-C	■Added model NZ2MHG-TSNT4 ■Added or modified parts SAFETY PRECAUTIONS, INTRODUCTION, TERMS, Chapter 1, Section 2.2, 4.1, 5.3, Chapter 6, Section 7.1, Chapter 8, Appendix 1, 3, 7, TRADEMARKS
November 2022	SH(NA)-082449ENG-D	■Added or modified parts Section 2.2, Chapter 7, Section 8.2, Appendix 1
June 2023	SH(NA)-082449ENG-E	■Added model USB flash drive (connectable products) ■Added or modified parts SAFETY PRECAUTIONS, INTRODUCTION, Chapter 1, Section 2.2, 5.3, 7.1, 8.1, 8.9, 10.1, 10.2, Appendix 1, 8
October 2023	SH(NA)-082449ENG-F	■Added or modified parts Section 6.2

Japanese manual number: SH-082448-F

This manual confers no industrial property rights or any rights of any other kind, nor does it confer any patent licenses. Mitsubishi Electric Corporation cannot be held responsible for any problems involving industrial property rights which may occur as a result of using the contents noted in this manual.

WARRANTY

Please confirm the following product warranty details before using this product.

1. Gratis Warranty Term and Gratis Warranty Range

If any faults or defects (hereinafter "Failure") found to be the responsibility of Mitsubishi occurs during use of the product within the gratis warranty term, the product shall be repaired at no cost via the sales representative or Mitsubishi Service Company.

However, if repairs are required onsite at domestic or overseas location, expenses to send an engineer will be solely at the customer's discretion. Mitsubishi shall not be held responsible for any re-commissioning, maintenance, or testing on-site that involves replacement of the failed module.

[Gratis Warranty Term]

The gratis warranty term of the product shall be for one year after the date of purchase or delivery to a designated place. Note that after manufacture and shipment from Mitsubishi, the maximum distribution period shall be twenty-four (24) months, and the longest gratis warranty term after manufacturing shall be sixty (60) months. The gratis warranty term of repair parts shall not exceed the gratis warranty term before repairs.

[Gratis Warranty Range]

(1) The range shall be limited to normal use within the usage state, usage methods and usage environment, etc., which follow the conditions and precautions, etc., given in the instruction manual, user's manual and caution labels on the product.

(2) Even within the gratis warranty term, replacement shall be charged for in the following cases.

1. Failure occurring from inappropriate storage or handling, carelessness or negligence by the user. Failure caused by the user's hardware or software design.
2. Failure caused by unapproved modifications, etc., to the product by the user.
3. When the Mitsubishi product is assembled into a user's device, Failure that could have been avoided if functions or structures, judged as necessary in the legal safety measures the user's device is subject to or as necessary by industry standards, had been provided.
4. Failure that could have been avoided if consumable parts (battery, backlight, fuse, etc.) designated in the instruction manual had been correctly serviced or replaced.
5. Failure caused by external irresistible forces such as fires or abnormal voltages, and Failure caused by force majeure such as earthquakes, lightning, wind and water damage.
6. Failure caused by reasons unpredictable by scientific technology standards at time of shipment from Mitsubishi.
7. Any other failure found not to be the responsibility of Mitsubishi or that admitted not to be so by the user.

2. Onerous repair term after discontinuation of production

(1) Mitsubishi shall accept onerous product repairs for five (5) years after production of the product is discontinued. Discontinuation of production shall be notified with Mitsubishi Technical Bulletins, etc.

(2) Product supply (including repair parts) is not available after production is discontinued.

3. Overseas service

Overseas, repairs shall be accepted by Mitsubishi's local overseas FA Center. Note that the repair conditions at each FA Center may differ.

4. Exclusion of loss in opportunity and secondary loss from warranty liability

Regardless of the gratis warranty term, Mitsubishi shall not be liable for compensation to:

(1) Damages caused by any cause found not to be the responsibility of Mitsubishi.

(2) Loss in opportunity, lost profits incurred to the user by Failures of Mitsubishi products.

(3) Special damages and secondary damages whether foreseeable or not, compensation for accidents, and compensation for damages to products other than Mitsubishi products.

(4) Replacement by the user, maintenance of on-site equipment, start-up test run and other tasks.

5. Changes in product specifications

The specifications given in the catalogs, manuals or technical documents are subject to change without prior notice.

TRADEMARKS

Google Chrome is either a registered trademark or a trademark of Google LLC.
The company names, system names and product names mentioned in this manual are either registered trademarks or trademarks of their respective companies.
In some cases, trademark symbols such as '™' or '®' are not specified in this manual.

COPYRIGHTS

The screens (screenshots) are used in accordance with the Microsoft Corporation guideline.

Moxa Inc.　www.moxa.com/en

SH(NA)-082449ENG-F(2310)MEE

MODEL:　NZ2MHG-TSN-U-E

MODEL CODE: 13JX5E

MITSUBISHI ELECTRIC CORPORATION

HEAD OFFICE: TOKYO BLDG., 2-7-3, MARUNOUCHI, CHIYODA-KU, TOKYO 100-8310, JAPAN
NAGOYA WORKS: 1-14, YADA-MINAMI 5-CHOME, HIGASHI-KU, NAGOYA 461-8670, JAPAN

When exported from Japan, this manual does not require application to the Ministry of Economy, Trade and Industry for service transaction permission.

Specifications subject to change without notice.