SEIKO

Instruction Manual

SmartCS

Console server
NS-2250

Before using this console server, carefully read this instruction manual so you can use the console server correctly.
After reading this manual, store it in a safe place so can be accessed easily when necessary.

SEIKO SOLUTIONS INC.

When you dispose of the NS-2250, observe the regulations of local government. For details, contact your local government.

This equipment has been tested and found to comply with the limits for a Class A digital device, according 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 following 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.

Introduction

Thank you for purchasing the SmartCS NS-2250 console server (hereinafter referred to as the NS-2250).

This document is the instruction manual for the NS-2250. This manual describes the specifications, operation methods, maintenance methods, and other information of the NS-2250, for IT professionals who must remotely configure/manage the network equipment with serial ports
.

As shown in the following table, the number of serial ports of the NS-2250 depends on the model you are using. The examples in this manual may state that the serial port specification is 1-48. Change this value to 1-16 or 1-32 or 1-48 as appropriate for the model you are using.

Power	Model	Number of serial ports
AC power model	NS-2250-16	16 ports
	NS-2250-32	32 ports
	NS-2250-48	48 ports

For the installation and cable connections of the NS-2250, see the *NS-2250 SmartCS console server installation manual* (hereinafter referred to as the *Installation manual*). For details about commands for the SmartCS, see the *NS-2250 Console server command reference* (hereinafter referred to as the *Command Reference*).
Before installing the NS-2250, read the following Safety precautions and Handling precautions.

Safety precautions

Before using the NS-2250, carefully read these safety precautions so you can use the console server safely.

In this manual, the following symbols are used to call your attention to precautions so that you can use the NS-2250 safely and prevent damage to equipment.

The following table shows the meaning of these symbols. Understand the content of the table fully before reading this manual.

⚠ Warning	Ignoring the displayed contents and handling the console server incorrectly may result in death or serious injury.
⚠ Caution	Ignoring the displayed contents and handling the console server incorrectly may result in injury or physical damage.

Examples of symbols

⚠ This symbol indicates content that requires attention (including danger and warnings).
The display example on the left indicates a warning or precaution.

🚫 This symbol indicates a prohibited action.
The display example on the left indicates that disassembly is prohibited.

● This symbol indicates a required action or instruction.
The display example on the left indicates the removal of the power plug from the outlet.

Symbols used on the main unit and in this manual

This symbol indicates that improper handling through the disregard of this indication may lead to the "danger" of an electric shock.

This symbol indicates disconnection, all power plugs.

This symbol indicates that the AC power supply.

⚠️Warning

Do not disassemble or modify the NS-2250.

Doing so can result in heat generation, fire, electric shock, or malfunction.

Do not remove the metal cover of the NS-2250.

There are no user-serviceable parts inside.

Doing so can result in heat generation, fire, electric shock, or malfunction.

Never use the NS-2250 in a location of extremely high humidity or a location in which it may be exposed to water or other liquids.

Doing so can result in heat generation, fire, electric shock, or malfunction.

Never drop metal pieces or drip water or other liquids into the interior or gaps of the NS-2250.

Doing so can result in heat generation, fire, electric shock, or malfunction.

Do not connect or disconnect the power cable or other cables with wet hands.
Doing so can result in electric shock.

Do not block the heat vents of the NS-2250.

Heat generation may cause fire, electric shock, or malfunction.

In the following situations, remove the power plug from the outlet.

Continuing to use the NS-2250 under such abnormal conditions may cause an accident or fire.

◆ When you are repairing the NS-2250 or dealing with errors

◆ When you notice unusual odors, smoke, or unusual noises

◆ If metal pieces or water or other liquids enter the interior or gaps of the NS-2250

◆ If the NS-2250 has been dropped or the exterior surface of the NS-2250 has been damaged

Mechanical loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading. Personal injury or equipment damage might result if mishandled.

⚠️ Caution

🚫 Never perform the following actions.
These actions can cause fire, electric shock, accident, or malfunction.

◆ Do not place objects on the NS-2250.
◆ Do not apply impact to the NS-2250 with blows or other similar actions.
◆ Do not place the NS-2250 in an unstable location.
◆ Do not place objects on cables, twist cables, or pull cables strongly.

🚫 Do not install the NS-2250 in the following locations or conditions.
Doing so can result in malfunction.

◆ Direct sunlight
◆ Severe changes in temperature or humidity
◆ Very dusty locations
◆ Locations subject to vibrations
◆ Near a heating-cooling combination appliance

❗ Always perform the following actions.
Neglecting these actions can cause fire, electric shock, accident, or malfunction.

◆ Always use the NS-2250 at the specified power voltage.
   The power voltage of the NS-2250 is displayed on the nameplate on its bottom surface and near the AC inlet.
◆ The potential difference may be generated between the NS-2250 and connected equipment depending on the installation environment. When connecting a cable, do not touch the terminal of the connector section. Doing so can result in electric shock.
◆ Use an outlet that is near the NS-2250 and can be easily accessed

⏚ Always ground the power cable.
Neglecting to ground the power cable can result in fire or electric shock.

Alsofollow the warnings and precautions indicated in each section.

Handling precautions

- Never perform the following actions.
  They can result in malfunctions of the NS-2250 or USB memory or corrupt the contents of the USB memory.
  - ・ While the STATUS 4 light is on, do not remove the USB memory. If the USB memory is removed during the operation, the operation of the NS-2250 is not guaranteed.
  - ・ While the NS-2250 is running normally, do not cut the power of the NS-2250 by switching off the power switch or pulling out the power cable or press the RESET switch.
    Before you switch off the power, carry out the "shutdown" command to exit the system software. Next, either confirm that the "MON>" prompt is displayed on the console or wait for the STATUS 2 light on the front of the NS-2250 to switch on. Finally, switch off the power.
  - ・ Do not touch the connector of the USB memory with your hand or metal directly.

- To press the RESET switch, use an item with a narrow tip, such as the tip of a ballpoint pen.
  Do not use a mechanical pencil. A malfunction may result when mechanical pencil leads fall inside NS-2250

- After you cut the power by pushing the POWER switch off button or removing the power cable of the NS-2250, wait 10 seconds or more before the POWER switch on or inserting the power cable of the NS-2250.
  If power is supplied too quickly, the NS-2250 may not reset normally.
  When a redundant power is used, turn off both power.

- Clean the heat vents with a vacuum cleaner or similar device about once every two months.

- If the exterior of the NS-2250 becomes soiled, soak a soft cloth in a neutral detergent diluted with water, wring it well, and then wipe the exterior. Next, wipe with a dry cloth.

- This equipment is for indoor use and all the communication wirings are limited to the inside of the building.

- This equipment is not suitable for use in locations where children are likely to be present.

Third-party software licenses

Parts of the software of the NS-2250 use the following software. For details of the licenses of the following software, see Appendix D, "Third-party software licenses".

SysVinit
SysVinit-tools
bootlogd
busybox
dropbear
e2fsprogs
eglibc
ethtool
freeradius
ftp
iptables
kernel
Linux-PAM
libcap
libgcc
libpcap
linux
logrotate
net-snmp
net-snmp-libs
openssh
openssh-server
openssl
pam
pam_tacplus
procps
proftpd
rsyslog
strace
strongswan
tcl
tclx
tcpdump
tcp_wrappers
telnet-server
udev
u-boot
vzctl
xinetd
zlib

Table of contents

Chapter 6 Troubleshooting   6-1

Appendix A User privileges   1

Appendix B Examples of attributes and RADIUS authentication/accounting server settings   3

Appendix C Rom-Monitor 1

Appendix D Third-party software licenses 1

Chapter 1
Overview of the NS-2250

Chapter 1 describes the main functions and part names of the NS-2250.

Read this chapter before starting work.

1.1   Features and main functions

This chapter provides an overview of the features and main functions of the NS-2250. For details of each function, see Chapter 2, "Functions".

1.1.1 Features

The NS-2250 console server is equipped with up to 48 RS232-compliant RJ-45 (8-contact modular connector) serial ports.

Device name	Power	Model	Number of serial ports
SmartCS	AC power model	NS-2250-16	16 ports
		NS-2250-32	32 ports
		NS-2250-48	48 ports

This console server aggregates the console ports (serial ports for various settings, log output, and so on) of routers, switches, and other network equipment and server equipment (hereinafter referred to as monitored equipment) and offers a unified, maintainable environment.
The NS-2250 can automatically save messages that monitored equipment have output, send logs to syslog servers and NFS servers, transfer files to FTP servers, and send an e-mail.
To provide safe access to the NS-2250 and monitored equipment that has been connected to the NS-2250, the NS-2250 is equipped with the SSHv2/SFTP encryption protocol and public key authentication. Furthermore, to protect monitored equipment that has been connected to the NS-2250 from unauthorized access, the NS-2250 is equipped with a login authentication function for users that access serial ports and a function to limit serial ports to which users can access.

Features of the NS2250
- Aggregate the console ports of monitored equipment
- Save and transfer messages that monitored equipment output
- Encrypt communication and prevent unauthorized access
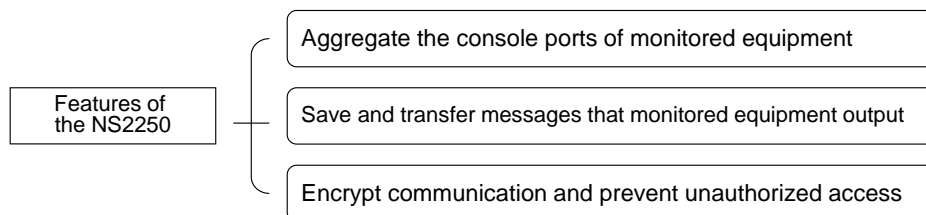
Figure 1-1 Features of the NS-2250

(1) Aggregate the console ports of monitored equipment

The NS-2250 aggregates the console ports of multiple units of monitored equipment and offers a unified, maintainable environment. Instead of connecting terminals to the console ports of monitored equipment, by connecting to the NS-2250, you can access the console ports of monitored equipment from a telnet/SSH client on the network.

Via the NS-2250, you can operate monitored equipment as if you are directly connected to its serial port.
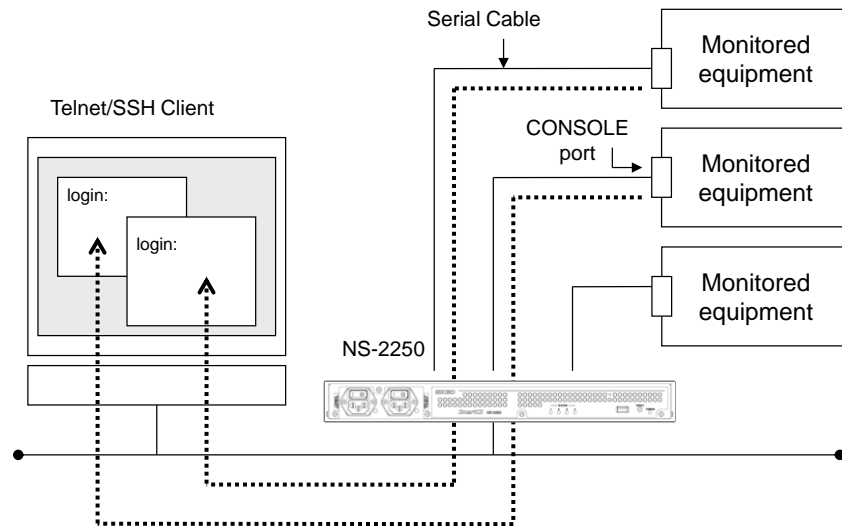
Figure 1-2 Aggregation of the console ports

If you use the NS-2250 to create a monitoring network as shown in Figure 1-3, you can reliably access the console ports of monitoring equipment that are connected to the NS-2250, even when an operational network problem occurs. This can reduce maintenance work greatly and minimize maintenance costs.
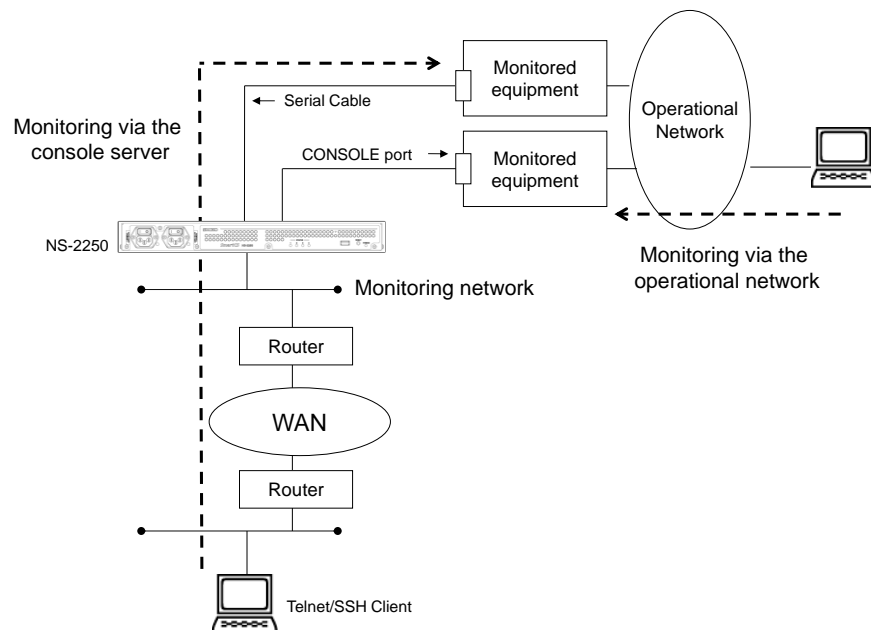
Figure 1-3 Remote monitoring via the NS-2250

Furthermore, the NS-2250 is equipped with a port selection function that allows you to access monitored equipment easily by simply selecting a number from a menu displaying a list of monitored equipment. By using this function, you can centrally control monitored equipment.
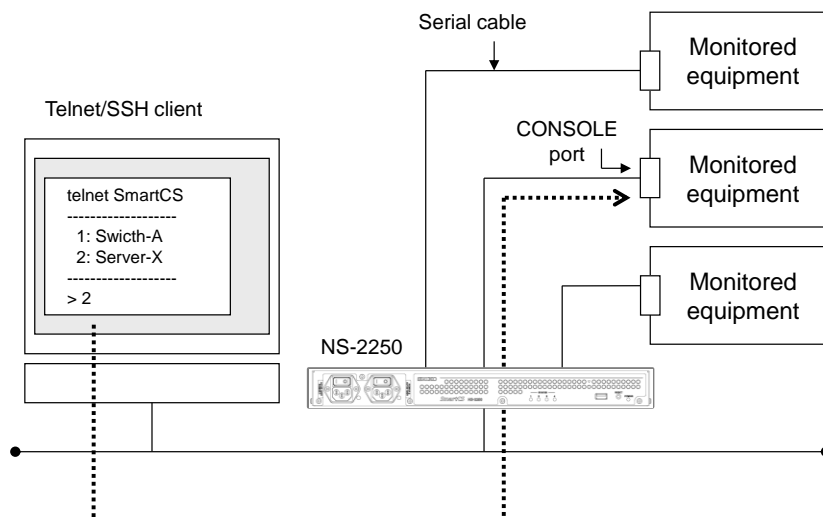
Figure 1-4 Central control of monitored equipment

Furthermore, with the NS-2250, you can access monitored equipment on a single serial port from multiple telnet/SSH clients at the same time. For example, you can operate the same monitored equipment from 2 telnet/SSH clients or operate monitored equipment from one telnet/SSH client, while at the same time monitoring from another telnet/SSH client. You can use this function to operate more efficiently when multiple people are managing and operating the same monitored equipment, such as in an environment to run a read-out check before inputting a configuration command to monitored equipment.
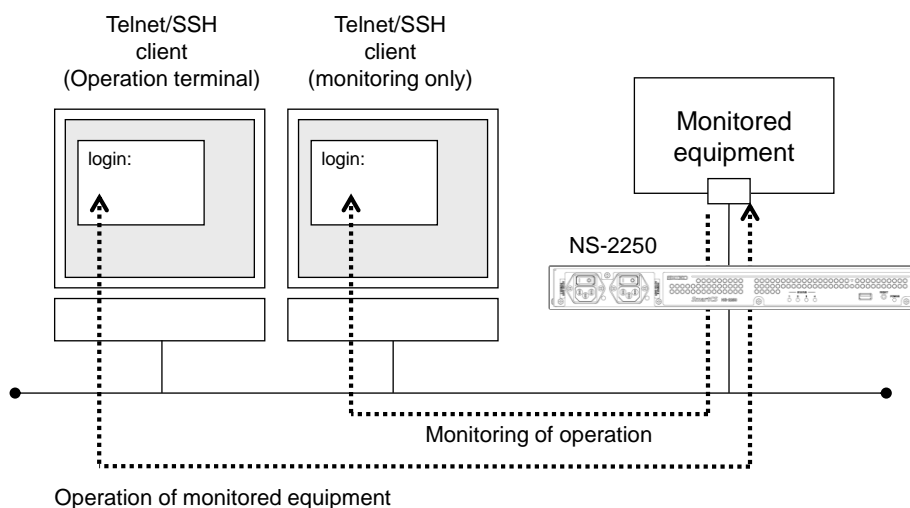
Figure 1-5 Operation and monitoring of monitored equipment

(2) Save, display, and send messages that monitored equipment have output
The NS-2250 saves and manages messages that monitored equipment have output as port logs.
You can view saved port logs when accessing monitored equipment via the NS-2250 from a telnet/SSH client.
You can also use the following methods to export port logs to external equipment.

Automatically save files to an NFS server
Automatically send files to an FTP server
Automatically send logs as mail data to a mail server
Automatically send messages to a syslog server
Download logs via external FTP/SFTP access
Manually send logs to an external TFTP server

By checking the port logs saved to the NS-2250 and the port logs sent to servers, you can analyze trouble with monitored equipment even when the monitored equipment restarted due to the trouble.
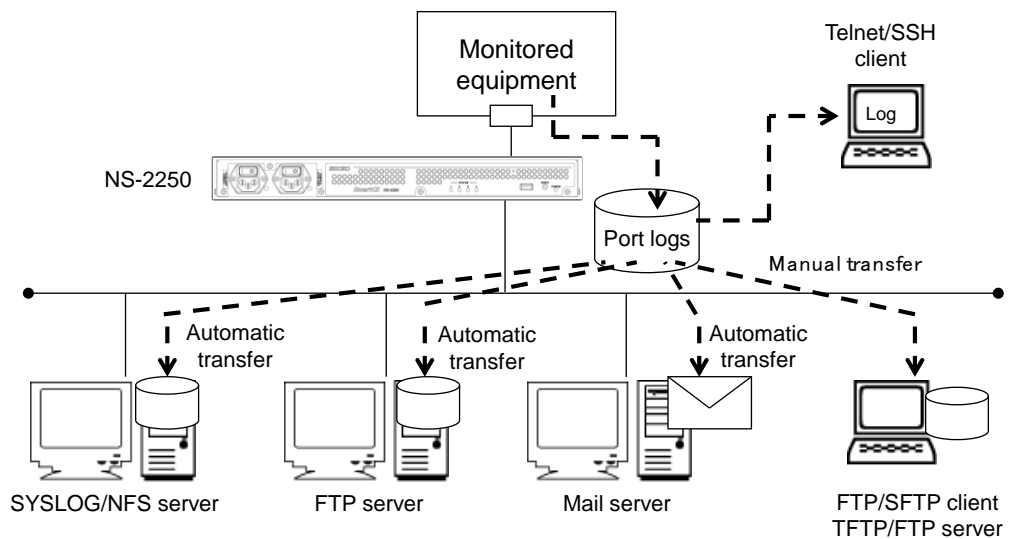
Figure 1-6 Save, display, and send messages that monitored equipment have output

(3) Encrypt communication and prevent unauthorized access

To provide safe access to the NS-2250 and monitored equipment that has been connected to the NS-2250, the NS-2250 is equipped with the SSHv2 (Secure Shell version 2)/SFTP (Secure File Transfer Protocol) encryption protocol and public key authentication. Because communication is concealed, you can use the NS-2250 with peace of mind from a security perspective.

You can also specify the network addresses of clients that can access the internal management services of the NS-2250 (telnet server, SSH server, etc.) and restrict access to these services.

In addition to user authentication using passwords and public keys, you can enable advanced security control by specifying the serial ports that the user can access.

User	Access Port
suzuki	1,2,3
tanaka	1,5,6
sato	7
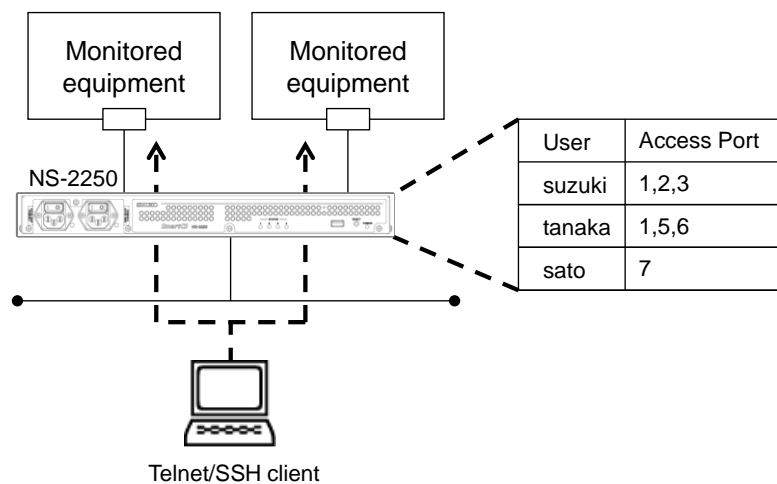
Figure 1-7 Access control of serial ports

1.1.2 Main functions

This section provides an overview of the main functions of the NS-2250.

(1) Port server functions
The port server functions receive connection requests from telnet/SSH clients and connect telnet/SSH sessions to the specified serial ports.
By using the port server menu included in the port server functions, you can view the logs of monitored equipment connected to a serial port and send Break signals to monitored equipment.

The port server functions have two connection modes.
When using the NS-2250, select the connection mode that suits your network environment.

Direct mode
Set the TCP port number mapped to a serial port of the NS-2250, and then access the monitored equipment directly.

Select mode (port selection function)
Use a standard TCP port for telnet/SSH access, select the serial port that you want to access from the port selection menu displayed by the monitored equipment, and then access the monitored equipment.

Also, the port server functions support two modes: Normal mode to manage monitored equipment connected to a serial port and Monitoring mode, which allows monitoring of monitored equipment only. You can access a single serial port in Normal mode from two telnet/SSH clients, and then operate monitored equipment or run both Normal mode and Monitoring mode to both operate and monitor monitored equipment.
For details, see Section 2.1, "Port server functions".

Aside from the port server functions by direct mode and select mode, SSH transparent connection (sshxpt) is available to access serial ports.
For details, please refer to Section 2.1.6, "SSH transparent connection (sshxpt)".

(2) Port log functions
The port log function saves data received from monitored equipment connected to the serial port of the NS-2250 as a port log. You can view port logs saved to a telnet/SSH client that accessed via the port server, save these logs to a syslog or NFS server in real-time, and send the logs to an FTP server or mail address specified for each port.
The port log function has the following functions.
Port log save function
Time stamp function
Login stamp function
Port log display function
Port log sending function (syslog/FTP/mail)

For details, see Section 2.2, "Port log functions".

(3) Security functions
With the security function, you can restrict the users who log into the NS-2250 and specify the serial ports that can be accessed by each user. With a RADIUS/TACACS+ function, you can centrally manage users who log into the NS-2250 and users who access the serial port of the NS-2250 and save accounting logs to the RADIUS/TACACS+ server.

You can further strengthen the security by controlling the access of the networks and hosts to various daemons running on the NS-2250 and also by using IPsec expanded in version 1.2 or the Firewall (ipfilter).
.

(4) Operation management functions
The following functions are included to operate the NS-2250:

> DNS client
> SNTP client
> Static routing
> SNMP agent
> Syslog client
> Telnet/SSH server
> FTP server
> FTP/TFTP client
> Firmware upgrade/downgrade
> Firmware restore/backup
> Automatic recovery
> Temperature sensor
> Time zone function
> Bonding function
> IPv6 communication function
> tty manage function
> Operation via Ansible

For details, see Section 2.4, "Operation management functions".

1.2   Part names

This section describes the part names and functions of the NS-2250. For detailed hardware specifications, connector connections, and other details, see the *Installation Manual*.

1.2.1 Front of NS-2250

NS-2250-16/32/48 are generally referred to as SmartCS models. The following figure shows the front side of the SmartCS.

[NS-2250-16/32/48]
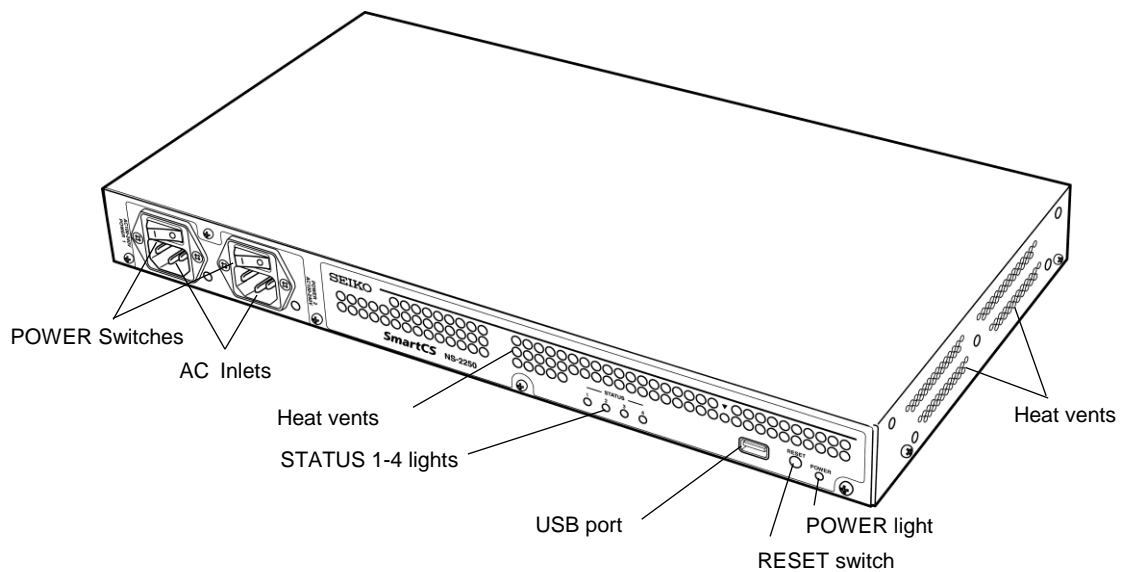
Figure 1-8 Part names (Front of NS-2250-16/32/48)

(1) Lights (POWER/STATUS)

Light name	Color	Functions
POWER	Green	On when power is on.
STATUS 1	Green	On when a self-diagnostic test (POC) is running.
STATUS 2	Green	On when Rom-Monitor is running.
STATUS 3	Green	On when the system is running.
STATUS 4	Green	On when accessing a USB memory.

(2) USB port
   Insert the USB memory into the USB port.

(3) RESET switch
   Use this switch to reset the NS-2250.

(4) POWER switch

Switch the power of the NS-2250 on or off.

When the switch is switched to the (|) side or (O) side, the power is switched on or off, respectively.

(5) AC inlet

Connect the AC power cable.

Before you pull out the AC power cable, carry out the "shutdown" command to exit the system software. Next, either confirm that the "MON>" prompt is displayed on the console or wait for the STATUS 2 light on the front of the NS-2250 to switch on. Finally, pull out the AC power cable.

Refer to the *Installation manual* for the specifications of the AC power cable to be used.

1.2.2 Rear of NS-2250

The following figure shows the rear side of the SmartCS.
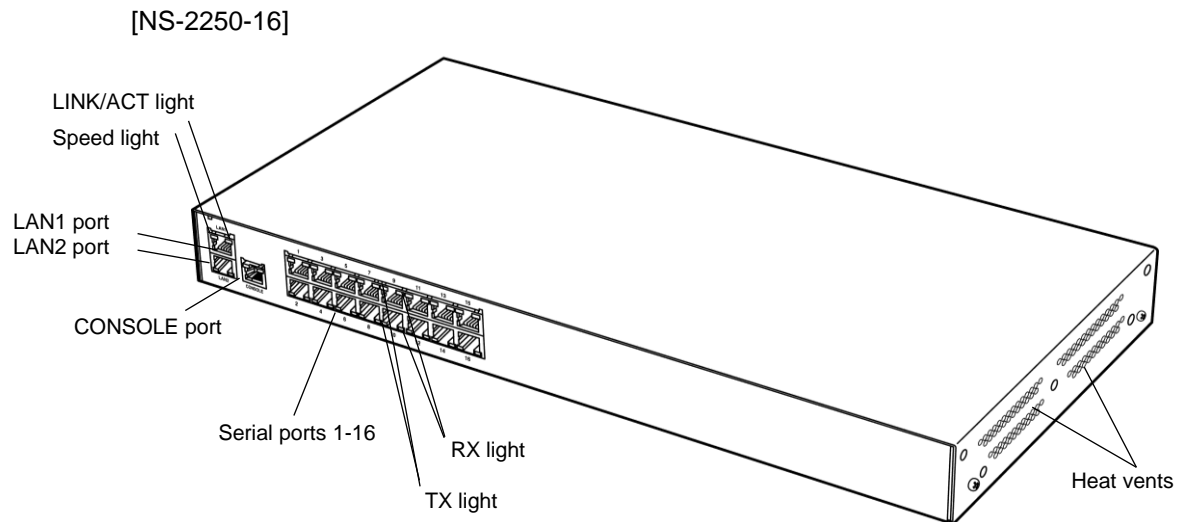
[NS-2250-16]

Figure 1-12 Part names (Rear of NS-2250-16)
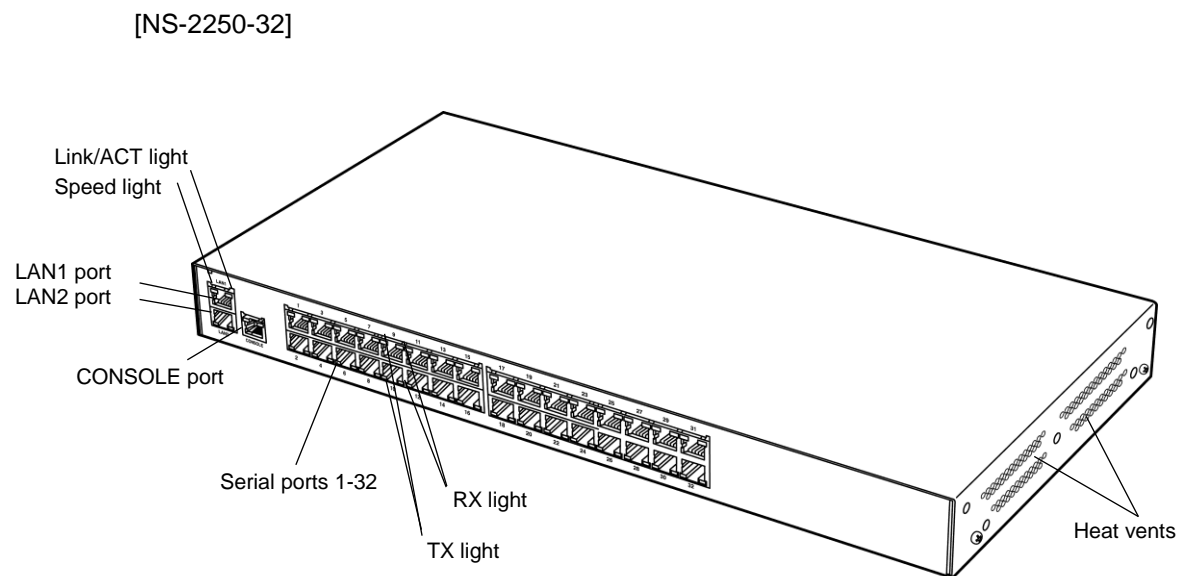
[NS-2250-32]

Figure 1-13 Part names (Rear of NS-2250-32)

[NS-2250-48]
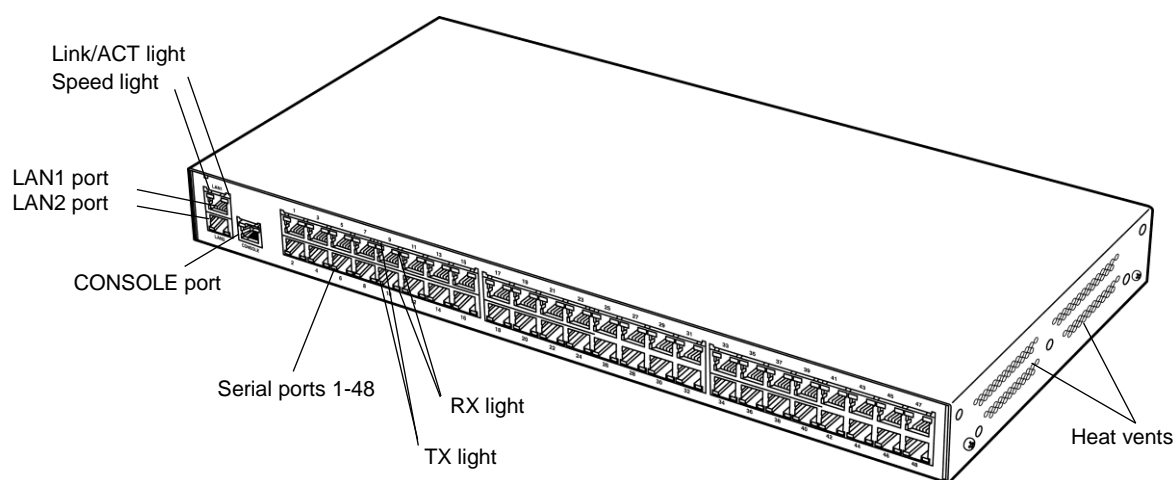
Figure 1-14 Part names (Rear of NS-2250-48)

(1) Interface ports

Port	Functions
CONSOLE port	Serial port to configure the initial settings of the NS-2250 and perform other operations.
Serial ports	Serial ports to connect with monitored equipment. The number of serial ports depends on the model you are using. NS-2250-16 (16 ports) NS-2250-32 (32 ports) NS-2250-48 (48 ports)
LAN1 port	10BASE-T/100BASE-TX/1000BASE-T port to connect with client terminals.
LAN2 port	10BASE-T/100BASE-TX/1000BASE-T port to connect with client terminals.

(2) Lights (Serial ports)

Light	Color	Functions
TX light	Green	On when sending data.
RX light	Green	On when receiving data.

(3) Lights (LAN port)

Light	Color	Functions
Speed light	Green	On when link speed is 1000M. Off when link speed is 10/100M
LINK/ACT light	Green	On when a link test pulse is detected. Flashes when sending or receiving data.

1.3   Interface specifications

This section describes the interface specifications of the NS-2250.
The default settings are underlined.

(1) LAN port

Functions	Description
Number of ports	2
Speed	<u>Auto</u>, 10 Mbps, 100 Mbps, 1000Mbps
Duplex	<u>Auto</u>, Full-duplex, Half-duplex

(2) CONSOLE port

Functions	Description
Number of ports	1
Connector	RJ-45 (RS232 compliant)
Transfer speed (bps)	2400/4800/<u>9600</u>/19200/38400/57600/115200
Data length (bit)	7 / <u>8</u>
Parity	even / odd / <u>none</u>
Stop bit	<u>1</u> / 2
Flow control	<u>xon</u> / rs / none

(3) Serial ports

Functions	Description
Number of ports	16: (NS-2250-16) 32: (NS-2250-32) 48: (NS-2250-48)
Connector	RJ-45 (RS232 compliant)
Transfer speed (bps)	2400/4800/<u>9600</u>/19200/38400/57600/115200
Data length (bit)	7 / <u>8</u>
Parity	even / odd / <u>none</u>
Stop bit	<u>1</u> / 2
Flow control	xon/rs/<u>none</u>
DSR signal transition detection function (*)	<u>on</u> / off

*   Detects change of the DSR signal.

Chapter 2
Functions

Chapter 2 describes the functions of the NS-2250 in detail.

Read this chapter before starting work.

2.1 Port server functions

2.1.1 Overview of port server functions

The port server functions receive connection requests from telnet/SSH clients and connect telnet/SSH sessions to the specified serial port. You can use a telnet/SSH client as a remote console of monitored equipment.

There are two supported methods to access monitored equipment: Normal mode (rw) and Monitoring mode (ro). In Normal mode (rw), you communicate in a bidirectional manner with monitored equipment connected to a serial port. In Monitoring mode (ro), you only monitor the data exported by monitored equipment connected to a serial port.
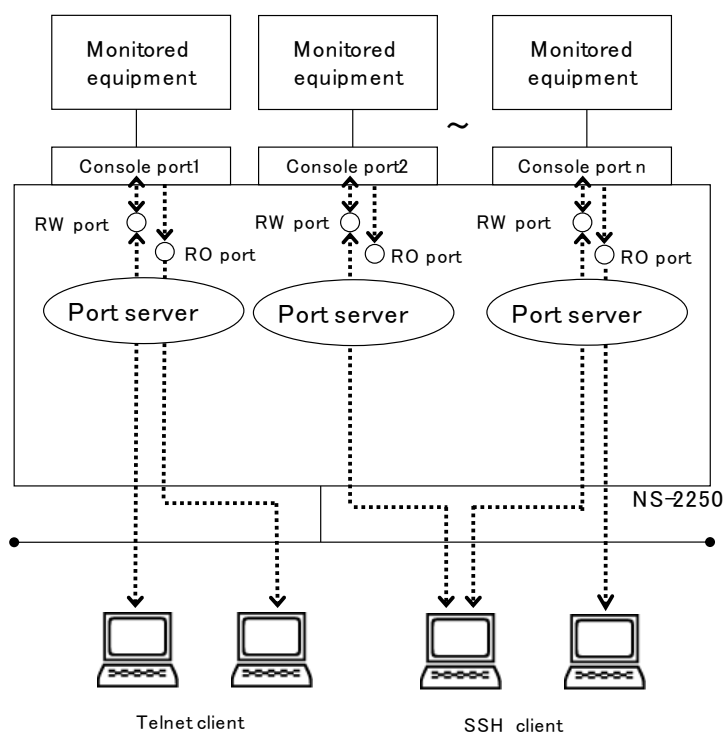
Figure 2-1 Overview of port server functions

You can connect up to two sessions in Normal mode and three sessions in Monitoring mode to a single serial port.

	Maximum number of sessions that can connect to a single serial port
Normal mode (RW)	2
Monitoring mode (RO)	3

The following table shows the number of connections of the entire device when combining Normal mode and Monitoring mode.

Model	Maximum number of sessions	
	Telnet only	SSH only
NS-2250-16	80	80
NS-2250-32	96	96
NS-2250-48	96	96

The following tables show the telnet and SSH protocol and servers supported by the port server.

Telnet	Details
Protocol	RFC854 compliant
Break signal processing	NVT break character conversion

SSH	Details
Protocol	SSH Version 2 (compliant with RFC4250-4254, 4256)
Authentication method	ID and password using plain text, public key
Public key	RSA encryption key (key length: maximum 4,096 bits) DSA encryption key (key length: 1,024 bits) ECDSA encryption key (key length: 128/256/521 bits)
Encryption method	3DES/Blowfish/AES
Break signal processing	Break over SSH

Note that there are two modes to connect to the port server: Direct mode and Select mode (also called a port selection function).
For details on the Direct mode and Select mode functions, see Section 2.1.2, "Connect to a port server (Direct mode)" and Section 2.1.3, "Connect to a port server (Select mode)".

Aside from the port server functions by direct mode and select mode, SSH transparent connection (sshxpt) is available to access serial ports.
For details please refer to Section 2.1.6, "SSH transparent connection (sshxpt)".

2.1.2 Connect to a port server (Direct mode)

In Direct mode, assign a TCP port number to each serial port, and then specify the TCP port number of the serial port to which the target device is connected from the telnet/SSH client to connect to the device directly. If you know the TCP port number to access the monitored equipment, it is easier to access the monitored equipment using Direct mode.
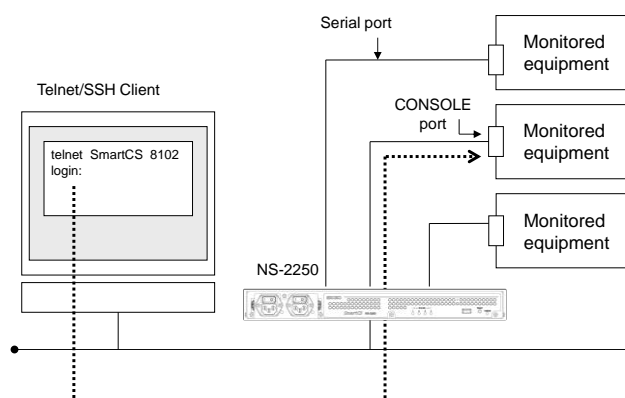
Figure 2-2 Connect to a port server (Direct mode)

To manage monitored equipment via the NS-2250, use Normal mode for bidirectional communication with monitored equipment connected to the serial port. To monitor monitored equipment connected to a serial port from one client while at the same time managing from another client, run Normal mode and Monitoring mode on the serial port at the same time.

When you want to manage from two clients at the same time, connect both sessions in Normal mode.
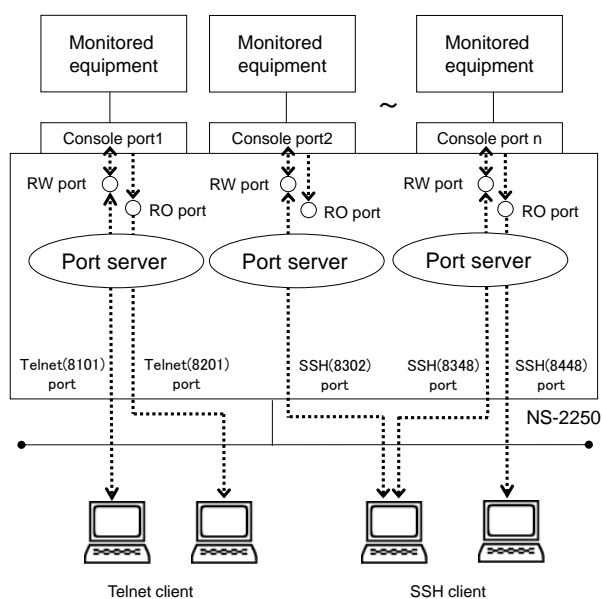
Figure 2-3 Normal mode and Monitoring mode

To connect in Direct mode, use the port numbers in the following table for access.

Mode	Privileges	Default port number	Notes
Normal mode	RW(Read/Write)	Telnet (8101 to 8148) SSH (8301 to 8348)	Enable bidirectional communication with monitored equipment connected to the serial port. You can connect up to two sessions to one serial port.
Monitoring mode	RO(Read-Only)	Telnet (8201 to 8248) SSH (8401 to 8448)	Monitor the data exported by monitored equipment connected to a serial port. You cannot transmit from a telnet/SSH client. You can connect up to three sessions to one serial port.

Connection example for Direct mode (when the TCP port number is the default setting)

To connect to serial port 11 of the NS-2250 in Normal mode from a telnet client, specify the option of the "telnet" command as shown in the following box.

```
# telnet NS-2250 8111↵
```

To connect to serial port 11 of the NS-2250 in Monitoring mode from a telnet client, specify the option of the "telnet" command as shown in the following box.

```
# telnet NS-2250 8211↵
```

To connect to serial port 11 of the NS-2250 in Normal mode from an SSH client as a port user (portuser01), specify the option of the "SSH" command as shown in the following box.

```
# ssh portuser01@NS-2250 -p 8311↵
```

To connect to serial port 11 of the NS-2250 in Monitoring mode from an SSH client as a port user (portuser01), specify the option of the "SSH" command as shown in the following box.

```
# ssh portuser01@NS-2250 -p 8411↵
```

2.1.3 Connect to a port server (Select mode)

In Select mode, you can enable connections to monitored equipment simply by accessing the NS-2250 from a telnet/SSH client and selecting the number of the serial port you want to access from the "Port selection menu". (For details, see 2.1.4, "Port selection menu".) This function is also referred to as a port selection function.
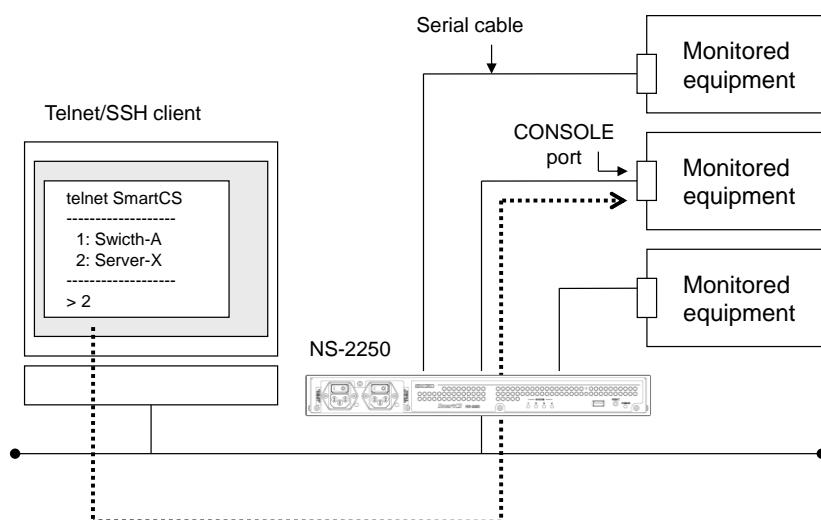
Figure 2-4 Connect to a port server (Select mode)

Using this function has the following merits.

(1) Simple access using the port selection menu

If you register the device name of monitored equipment to the label of the serial port in advance, you can confirm the corresponding serial port number and device name in the port selection menu. You can easily access monitored equipment by selecting the serial port number from this port selection menu. Also, even when a device name has not been added to the label, you can maintain the telnet/SSH session, search for the target monitored equipment, and then access it (by moving between serial ports).

Note that the port selection menu displays only information of serial ports to which the accessing user has permission. Users without access rights to a serial port cannot learn what kind of device is connected to the serial port.

(2) Simplified firewall policy

To use Direct mode when a firewall is configured between the telnet/SSH client and the NS-2250, you must set the firewall to allow all TCP ports used by Direct mode. If you use Select mode, you enable access to monitored equipment by simply allowing the standard port (TCP:23/22) of telnet/SSH.

Note that, in Select mode, the same telnet server (TCP:23)/SSH server (TCP:22) is used to access monitored equipment and log into the NS-2250.

In Select mode, when a normal user requests access, it is regarded as a login to the NS-2250. When a port user requests access, it is regarded as access to monitored equipment, and the port selection menu appears.
The user can access a serial port by selecting that serial port and the connection method (Normal mode/Monitoring mode) in the port selection menu that appears.
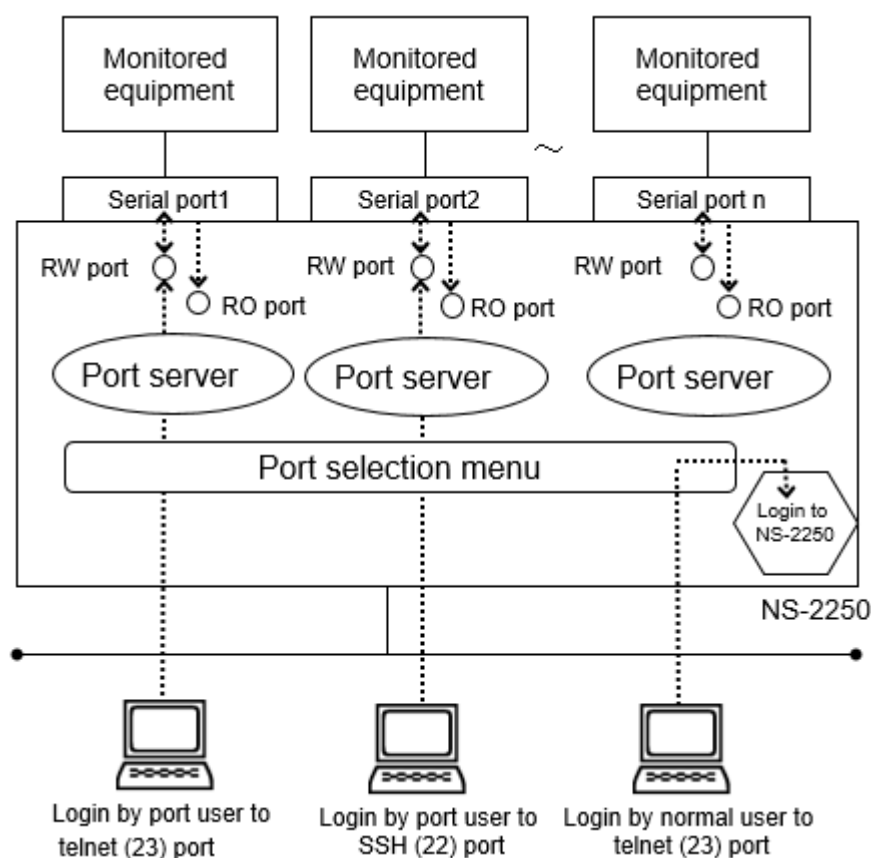
Figure 2-5 Sorting login to the NS-2250 and access to monitored equipment

As shown in the preceding illustration, the operation changes by the name of the user attempting access in Select mode. Therefore, you must switch on the port server authentication function to use the port selection function.

2.1.4 Port selection menu

The port selection menu appears when Select mode was selected, and a port user accesses the NS-2250.

The port selection menu shows the label information of the serial ports the user can access and the usage status of serial ports.

If you use this menu, you can grasp the usage status of monitored equipment and more easily access monitored equipment.

Example of the port selection menu

```
# telnet NS-2250↵
Console Server Authentication.
login: user1↵
Password: ↵

Host : "SmartCS-1"
login from 192.168.1.1
user (user1) Access TTY List
=========================================================================
 tty : Label                                        RW    RO
-------------------------------------------------------------------------
   1 : Switch-Tokyo-6F-00001                         1     0
   2 : Switch-Tokyo-6F-00002                         2     1
   3 : Server-A                                      0     N/A
   4 : Server-B                                      0     N/A
   5 : Switch-Tokyo-7F-00001                         1     0
             : (omitted)
-------------------------------------------------------------------------
Enter tty number to access serial port
 <ttyno>           : connect to serial port RW session ( 1  - 48  )
 <ttyno>r          : connect to serial port RO session ( 1r - 48r )
 l                 : show tty list
 l<ttyno>-<ttyno> : show a part of tty list
 d                 : show detail tty list
 d<ttyno>-<ttyno> : show a part of detail tty list
 h                 : help message
 e                 : exit
=========================================================================

 tty> 3↵
```

The port selection menu shows the information in the following table.

Output information	Display content
Tty	Serial ports numbers to which connections are possible.
Label	Label information configured to each port.
RW	Current Normal mode connection information. Numbers : The number of port users currently connected. Full : The number of sessions has reached the maximum. Connections are not possible. N/A : Connections are not permitted to this port.
RO	Current Monitoring mode connection information is displayed. Content is the same as RW. See above.

The following table shows the commands that can be used in the port selection menu.

Command	Description	Example entry
<ttyno>	Connect to the specified serial port in Normal mode.	tty> <u>1</u> tty> <u>24</u>
<ttyno>r	Connect to the specified serial port in Monitoring mode.	tty> <u>1r</u> tty> <u>24r</u>
l (lowercase L (l))	Refresh a list of serial ports to which connection is possible.	tty> <u>l</u>

l<ttyno>-<ttyno>	Refresh a list of serial ports to which connection is possible within the specified range of serial ports.
	
	    <ttyno> range specification
	        2-24 Specify ports from 2 through 24
	        -12 Specify ports from 1 through 12
	        3- Specify port 3 and higher
		tty> <u>l2-24</u>
		tty> <u>l16-32</u>
		tty> <u>l-12</u>
		tty> <u>l20-</u>

d	Display detailed information of the user connected to the serial port (IP address, port number, and user name of telnet/SSH client).
	
	 (Display example)
	tty 1 : Switch-1 RW:2 / RO:3
	     rw 1 telnet:4731 10.1.1.1:23 userA
	     rw 2 telnet:3495 10.1.1.2:23 userB
	
	tty 2 : Switch-2 RW:2 / RO:3
	     rw 1 telnet:4740 10.1.1.3:23 userC
	     ro 1 telnet:3851 10.1.1.4:23 userD
		tty>d

d<ttyno>-<ttyno>	Displays detailed information of the user connected to the serial port (IP address, port number, and user name of telnet/SSH client) within the specified range. The display format is the same as the "d" command.
	
	    <ttyno> range specification
	        2-24 Specify ports from 2 through 24
	        -12 Specify ports from 1 through 12
	        3- Specify port 3 and higher
		tty>d2-24
		tty>d16-32
		tty>d-12
		tty>d20-

h/?/<TAB>	Display the help section for commands that can be entered in the port selection menu. The same content is displayed when a "?" or <TAB> is entered.	tty> <u>h</u> tty> <u>?</u> tty> <u><TAB></u>
e	Close the port selection menu and disconnect the telnet/SSH session.	tty> <u>e</u>

(Connection example for Select mode)

To connect to serial port 1 of the NS-2250 in Normal mode from a telnet client, access the telnet server (TCP:23) of the NS-2250, and then select "1" in the port selection menu.

```
# telnet NS-2250↵
Console Server Authentication.
login: user1↵
Password: ↵

Host : "SmartCS-1"
login from 192.168.1.1
user (user1) Access TTY List
=========================================================================
 tty : Label                                      RW    RO
-------------------------------------------------------------------------
   1 : Switch-Tokyo-6F-00001                       1     0
   2 : Switch-Tokyo-6F-00002                       2     1
   3 : Server-A                                    0     N/A
   4 : Server-B                                    0     N/A
   5 : Switch-Tokyo-7F-00001                       1     0
               : (omitted)
-------------------------------------------------------------------------
Enter tty number to access serial port
 <ttyno>            : connect to serial port RW session ( 1 - 48 )
 <ttyno>r           : connect to serial port RO session ( 1r - 48r )
 l                  : show tty list
 l<ttyno>-<ttyno> : show a part of tty list
 d                  : show detail tty list
 d<ttyno>-<ttyno> : show a part of detail tty list
 h                  : help message
 e                  : exit
=========================================================================

 tty> 1↵
```

To connect to serial port 1 of the NS-2250 in Monitoring mode from a telnet client, select "1r" in the port selection menu, and then access the port.

```
 # telnet NS-2250↵
 Console Server Authentication.
 login: user1↵
 Password: ↵

   : The port selection menu appears


 tty> 1r↵
```

To connect to serial port 1 of the NS-2250 in Normal mode from an SSH client, access the SSH server (TCP:22) of the NS-2250, and then select "1" in the port selection menu.

```
# ssh portuser01@NS-2250↵
 Console Server Authentication.
 portuser01@192.168.1.1's password: ↵

    : The port selection menu appears

tty> 1↵
```

To connect to serial port 1 of the NS-2250 in Monitoring mode from an SSH client, select "1r" in the port selection menu, and then access the port, as shown in the following box.

```
# ssh portuser01@NS-2250↵
 Console Server Authentication.
 portuser01@192.168.1.1's password: ↵

    : The port selection menu appears

tty> 1r↵
```

2.1.5 Port server menu

The port server menu appears when you access a serial port from a telnet/SSH client.
In the port server menu, you can manage port logs, access monitored equipment, send Break signals to monitored equipment, and carry out other operations.

By configuring in advance the substitute character code (session suspension character code) to return to the port server menu, you can display the port server menu after accessing monitored equipment.

Furthermore, you can also access monitored equipment directly without displaying the port server menu. For the method to limit the display of the port server menu, see Section 4.4.2, "Show the port server menu".

The following table shows the commands that can be used in the port server menu.

Number	Menu	Description
0	return Port Select Menu	Return to the port selection menu. This menu appears only when Select mode is selected. It does not appear when Direct mode is selected.
1	display Port Log	Display the port logs of serial ports from the start.
2	display Port Log (LAST)	Display the most recent port logs of serial ports.
3	start tty connection	Connect to the monitored equipment.
4	close Telnet/SSH session	Close the telnet/SSH session.
5	show all commands	Show all commands.
6	display & erase Port Log	Display the port logs of serial ports and delete them.
7	erase Port Log	Delete the port logs of serial ports.
8	send Port Log	Force the sending of the port logs of serial ports to an e-mail address/FTP server configured in advance.
9	show Port Log configuration	Display configuration information, such as the log size, transfer interval, and transfer destination server of port logs of serial ports.
10	send break to tty	Send a Break signal to a serial port.

For details of port server menu commands, see the *Command Reference*.

To carry out commands in the port server menu, enter the numbers displayed in the menu.

```
# telnet NS-2250 8101↵
-- RW1 -----------------------
 Host  : "SmartCS-No1"
 Label : "Switch-Tokyo-6F-00001"
------------------------------
1 : display Port Log
2 : display Port Log (LAST)
3 : start tty connection
4 : close telnet/ssh session
5 : show all commands


tty-1:rw>1 ↵
Sep  8 11:16:15 ether: port 1 LINK DOWN.
Sep  8 11:16:15 ether: port 2 LINK DOWN.

tty-1:rw>3↵
Welcome to XXXXX
XXXXX login:
```

If you access the port server of the NS-2250, the port server menu is displayed.

Display the logs of monitored equipment

You can access monitored equipment.

To display a list of all commands in the port server menu, select "5: show all commands".

```
tty-1:rw> 5↵
-- RW1 -----------------------
 Host  : "SmartCS-No1"
 Label : "Switch-Tokyo-6F-00001"
------------------------------
 1 : display Port Log
 2 : display Port Log (LAST)
 3 : start tty connection
 4 : close telnet/ssh session
 5 : show all commands
 6 : display & erase Port Log
 7 : erase Port Log
 8 : send Port Log
 9 : show Port Log configuration
10 : send break to tty
tty-1:rw>
```

To refresh the port server menu, enter either "?" or a <TAB>.

```
tty-1:rw> ?
-- RW1 -----------------------
 Host  : "SmartCS-No1"
 Label : "Switch-Tokyo-6F-00001"
------------------------------
 1 : display Port Log
 2 : display Port Log (LAST)
 3 : start tty connection
 4 : close telnet/ssh session
 5 : show all commands
 6 : display & erase Port Log
 7 : erase Port Log
 8 : send Port Log
 9 : show Port Log configuration
10 : send break to tty
tty-1:rw>
```

You can also return to the port server menu after accessing monitored equipment.
For example, if you set Ctrl+A in advance as the session suspension character code for the port server menu, you can return to the port server menu by entering Ctrl+A even after accessing monitored equipment.

```
# telnet NS-2250 8101↵
-- RW1 -----------------------
 Host  : "SmartCS-No1"
 Label : "Switch-Tokyo-6F-00001"
------------------------------
1 : display Port Log
2 : display Port Log (LAST)
3 : start tty connection
4 : close telnet/ssh session
5 : show all commands

tty-1:rw>3↵
Press "CTRL-A" to return this MENU.
Welcome to XXXXX
XXXXX login: ******↵
Password: ****** ↵
Sep  8 14:51:45 login: successful (root/console)
#

 Enter Ctrl+A
-- RW1 -----------------------
 Host  : "SmartCS-No1"
 Label : "Switch-Tokyo-6F-00001"
------------------------------
1 : display Port Log
2 : display Port Log (LAST)
3 : start tty connection
4 : close telnet/ssh session
5 : show all commands
tty-1:rw>
```

2.1.6 SSH transparent connection (sshxpt)

SSH transparent connection (sshxpt) is the function for transparent communication with target devices by specifying TCP port number assigned to each serial port of NS-2250 from SSH client. Unlike the communication using direct mode or select mode of the port server function, it starts communicating with target devices without displaying the port server menu.

This function enables third-party Ansible modules to work via NS-2250 when operating target devices via Ansible.

When operating target devices through NS-2250, it needs to use a normal mode which performs two-way communication between NS-2250 and target devices connected to serial ports.

To enable SSH transparent connection (sshxpt), specify "sshxpt" option at the end of "set portd tty session" command. Then the TCP port of specified serial port for this function will be opened.

```
(0)NS-2250# set portd tty 1-32 session both sshxpt↵
```

When connecting by SSH transparent connection (sshxpt), the TCP port number shown in the table below is used to access.

Mode	Privilege	The default value of the port number	Description
Normal mode	RW(Read/Write)	SSH(9301～9348) *1	In this mode, it can perform two-way communication between target devices connected to serial ports of NS-2250. At most 2 sessions are available to one serial port.

*1 The range of port numbers depends on the number of serial ports of NS-2250.

Also, it can set to send line feed code when accessing to target devices by SSH transparent connection (sshxpt). Choose from "none", "CR", "CR+LF", "LF". The default setting is "none".

For example, execute the following command to send CR as line feed code when accessing the target device connected to serial port 1 of NS-2250.

```
(c)NS-2250# set portd tty 1 connted send_nl cr↵
```

2.1.7 Port user authentication

With the port user authentication function, users are authenticated when they access monitored equipment. When a user accesses the port server from a telnet/SSH client, this function requests entry of a user name and password to prevent unauthorized access to monitored equipment connected to the serial port.

Also, you can use a RADIUS authentication server or TACACS+ server for port user authentication.

For details, see Section 2.3.2, "RADIUS authentication function/RADIUS accounting function" and Section 2.3.4 "TACACS+ function".
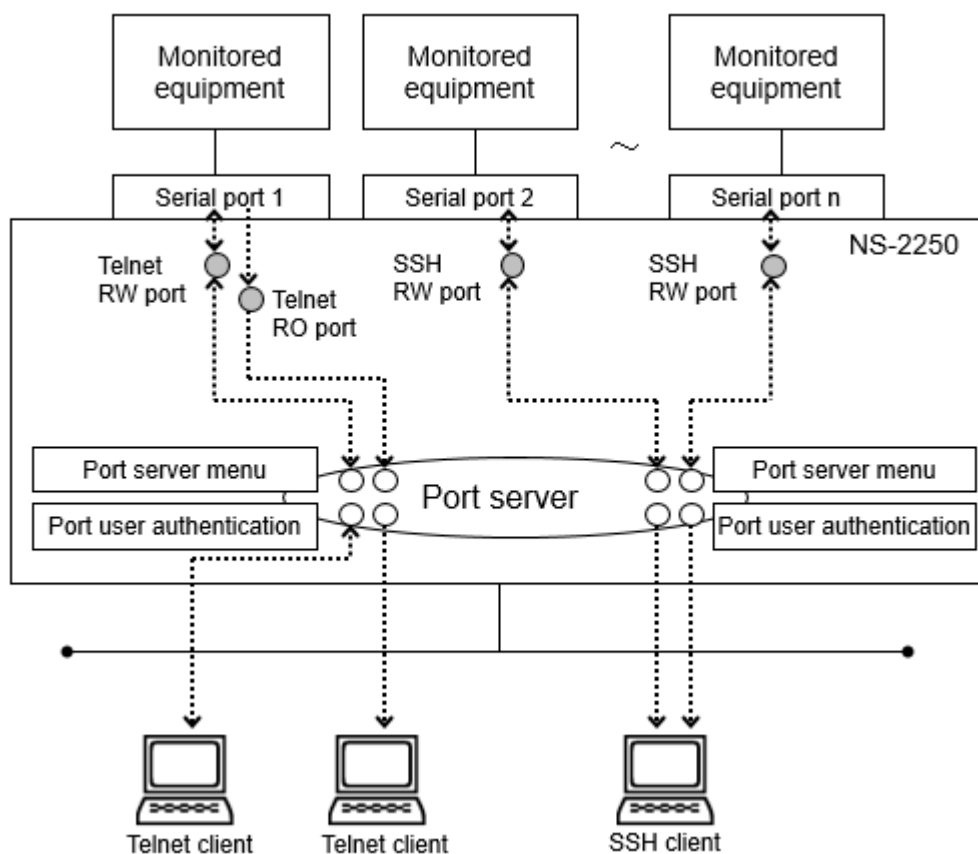
Figure 2-6 Port user authentication

The default port user authentication setting of the NS-2250 is off. When port user authentication is off, the prompt requesting login is not displayed.

If port user authentication is on, a prompt requesting login is displayed for all serial ports.

To use the port selection function (Select mode), enable this function.

When port user authentication is on and the port server menu is off

```
# telnet NS-2250 8101↵
Console Server Authentication.
login: user1↵                         Port user authentication of the NS-2250
Password: ********↵


Welcome to XXXXX     Prompt of monitored equipment
XXXXX login:
```

When port user authentication is on and the port server menu is on

```
# telnet NS-2250 8102↵
Console Server Authentication.
login: user1↵                         Port log authentication of the NS-2250
Password: ********↵
-- RW1 -----------------------
 Host  : "SmartCS-No1"
 Label : "Switch-Tokyo-6F-00001"
------------------------------
1 : display Port Log
2 : display Port Log (LAST)
3 : start tty connection
4 : close telnet/ssh session
5 : show all commands


tty-2:rw>3↵
Welcome to XXXXX     Prompt of monitored equipment
XXXXX login:
```

To use port user authentication, you must register port users, and then configure the serial ports to which the registered port users are permitted access. With the default settings (port user authentication is off), users can access all serial ports. If port user authentication is on, serial ports cannot be accessed until you configure the serial ports to which the registered users are permitted access.
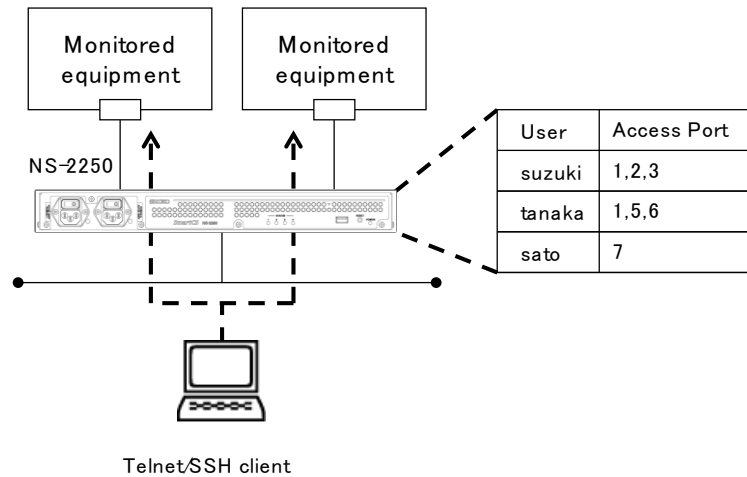
Figure 2-7 Access control of serial ports for port users

2.1.8 Other port server functions

The port server functions support the following functions.

Function	Description
Break signal processing	Transmit a Break signal to monitored equipment connected to a serial port when a Break request has arrived from a telnet/SSH client. The default setting is off.
Processing of received line feed code	Convert line feed code received from a telnet client. For line feed code conversion, select from "No conversion", "Convert CR+LF to CR", or "Convert CR+LF to LF". The default setting is "Convert CR+LF to CR".
Processing of sending line feed code	It can send line feed code when connecting to target devices by SSH transparent connection (sshxpt). This setting is needed when making third-party Ansible modules work via NS-2250. The default setting is off.
Serial port labeling	You can set a device name or other label to the serial port so that you can identify the device connected to the serial port. You can use up to 32 characters for labels. At the default setting, no labels are set for any serial ports.
Automatic disconnection by the idle timer (idle monitoring time)	If the idle timer expires, the session is disconnected automatically. This function runs in the following conditions. ・ After access to the port selection menu ・ After access to the port server menu ・ After access to a serial port in Normal mode (RW). The setting range for the idle timer is from 1 through 60 minutes. The default setting is off. The disconnection of the session occurs in stages. (Example) 　After the idle timer has expired, access to the serial port is ended, and then the port server menu is displayed. 　↓ 　After the idle timer has expired, the port server menu is closed, and then the Select menu is displayed 　↓ 　After the idle timer has expired, the Select menu is closed, and then the session is disconnected.
Automatic disconnection by session timer (continuous connection time)	If the specified time passes after connecting from a telnet/SSH terminal to a serial port in Monitoring mode (RO), the session is disconnected forcibly. The setting range for the session timer from 1 through 1440 minutes. The default setting is off.
Exclusion of sessions	It can set exclusion between portd normal session(rw) and tty manage function. When the exclusive function is enabled, users can not access target devices when a session of portd normal (rw session) or tty manage function already exists.

2.2   Port log functions

2.2.1 Overview of the port log function

The port log function saves data received from monitored equipment connected to a serial port to a FLASH memory or the internal memory (RAM) of the NS-2250. This function works even when a telnet/SSH client is not connected to the monitored equipment.

You can view saved port logs when accessing monitored equipment via the NS-2250 from a telnet/SSH client.
You can also use the following methods to export port logs to external equipment.
   Automatically save files to an NFS server
   Automatically send files to an FTP server
   Automatically send logs as mail data to a mail server
   Automatically send messages to a syslog server
   Acquire logs via external FTP/SFTP access
   Automatically send logs to an external FTP/TFTP server
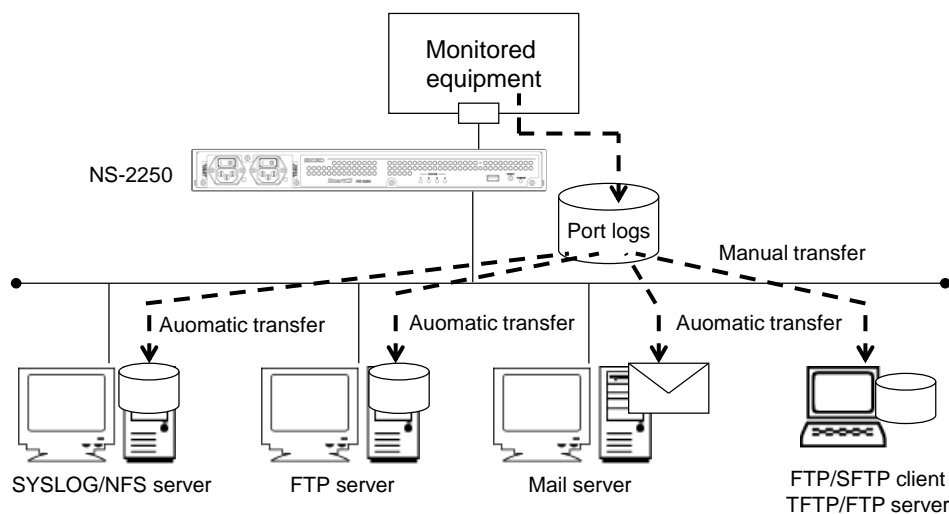
Figure 2-8 Port log functions

Port log functions are made up of the following functions.
   Port log save function
   Time stamp function
   Login stamp function
   Port log display function
   Port log sending function (syslog/NFS/FTP/mail)
The following section describes the functions in detail.

2.2.2 Port log saving function

The port log saving function saves logs output by monitored equipment connected to a serial port to a FLASH memory inserted in the NS-2250 or the RAM of the NS-2250.

The free space in which port logs can be saved to the NS-2250 depends on such factors as your model. The following table lists the maximum amount of free space in which port logs can be saved to the NS-2250 and the configuration range for free space in which port logs can be saved for each serial port. The free space to save port logs is the total of the port log spaces configured for each serial port. Calculate and set the values so the free space does not exceed the maximum amount of free space in which port logs can be saved to the NS-2250.

Port log save destination	The maximum amount of free space in which port logs can be saved to the NS-2250	Configuration range for free space in which port logs can be saved for each serial port
When saving to the FLASH memory	NS-2250-16 48 MByte NS-2250-32 96 MByte NS-2250-48 144 MByte	100 Kbyte to 8 MByte (Default:3 MByte)
When saving to the RAM of the NS-2250	NS-2250-16 8 MByte NS-2250-32 16 MByte NS-2250-48 24 MByte	100 Kbyte to 2 MByte (Default:500 KByte)

When the received port log volume exceeds the specified free save space for port logs, old information is overwritten.

You can also save port logs to a FLASH memory as a text file, as well as use an FTP/SFTP client to download port logs or send port logs to an FTP/TFTP server manually. For details, see Section 5.6, "Save and acquire port logs manually".

2.2.3 Time stamp function

The time stamp function for port logs adds time to a port log. When the time stamp function is on, the time is added to the port log following the time stamp interval specified for each port.

When logs are output continually from monitored equipment, the time is added at the specified time stamp interval. If the time stamp interval time has passed since the last log was output to the NS-2250, the date is added when a new log is output from monitored equipment.
If this function is enabled, the free space to save port logs is reduced by the amount of data of the added time stamps.

Time stamp function	Setting	Notes
Time stamp function operation	ON/OFF	Default: OFF
Time stamp interval	3 seconds to 65535 seconds	Default: 60 seconds

The time stamp format is as follows: day, month, date, time, timezone, and year.

```
<Mon Aug 10 17:42:38 JST 2015>  ←Time stamp
ether: port 1 LINK DOWN.
ether: port 2 LINK DOWN.
ether: port 1 LINK UP  100M FULL.
ether: port 2 LINK UP  100M FULL.
ether: port 3 LINK DOWN.                Log of monitored equipment
ether: port 4 LINK DOWN.
ether: port 3 LINK UP  100M FULL.
ether: port 4 LINK UP  100M FULL.

<Mon Aug 10 17:43:38 JST 2015>  ←Time stamp
ether: port 1 LINK DOWN.
ether: port 2 LINK DOWN.
ether: port 1 LINK UP  100M FULL.        Log of monitored equipment
ether: port 2 LINK UP  100M FULL.
```

2.2.4 Login stamp function

The login stamp function for port logs adds the login and logout times of the user who accessed the serial port.

This function can be configured for each serial port, and the default setting is off. If this function is enabled, a login stamp like the one shown in the following box is added to the port log.
Note that the free space to save port logs is reduced by the amount of data of the added login stamps.

```
<Mon Aug 10 13:00:26 JST 2012 login RW1:userA 10.1.1.1>
<Mon Aug 10 13:05:30 JST 2012 logout RW1:userA 10.1.1.1>
```

2.2.5 Port log display function

The port log display function displays saved port logs through the port server menu.
You can show port logs saved in the NS-2250 by selecting "1: display Port Log" or "2: display Port Log(LAST)" from the port server menu. When there is a large volume of logs stored in the NS-2250, and you want to view the latest logs, select "2: display Port Log(LAST)" to display approximately 5,000 characters from the end of the log file.

When the log displayed by the port server menu cannot be contained on a single page, the port log display function uses the "more" function to display the log one page at a time. At a screen displaying the "-- more <Press SPACE for another page, 'q' to quit> --" message, you can use the SPACE key to display the next page and the Return key to display the next line. You can use the "q" command to exit the "more" function.

```
# telnet NS-2250 8101↵
-- RW1 -----------------------
 Host  : "SmartCS-No1"
 Label : "Switch-Tokyo-6F-00001"
 -----------------------------
1 : display Port Log
2 : display Port Log (LAST)
3 : start tty connection
4 : close telnet/ssh session
5 : show all commands
tty-1:rw> 1↵
ROM BOOT...
1st-boot Ver 1.0
        :
Boot Status          : Normal Reboot          Log of monitored equipment
System Up Time       : Wed Sep  6 13:11:30
Serial No.           : 99900080
-- more <Press SPACE for another page, 'q' to quit> --
```

To delete the port logs displayed at the port log menu, select "6: display & erase Port Log" or "7: erase Port Log".

When this operation is carried out, port logs saved to the internal memory of the NS-2250 are not deleted. This operation simply hides the logs displayed by "1: display Port Log".

```
tty-1:rw> 5↵     ←Select "5" to display the commands to delete port logs
-- RW1 -----------------------
 Host  : "SmartCS-No1"
 Label : " Switch-Tokyo-6F-00001"
-----------------------------
 1 : display Port Log
 2 : display Port Log (LAST)
 3 : start tty connection
 4 : close telnet/ssh session
 5 : show all commands
 6 : display & erase Port Log      ←Display the port logs and delete them
 7 : erase Port Log                ←Delete the port logs
 8 : send Port Log
 9 : show Port Log configuration
10 : send break to tty
tty-1:rw> 7 ↵                      ←Select "7" to delete the port logs
tty-1:rw>
```

2.2.6 Port log sending function (syslog/NFS/FTP/mail)

The port log sending function sends port logs stored in the NS-2250 to the specified send destination server. You can save port logs to a syslog or NFS server and send the logs to an FTP server or mail address specified for each port. You can register multiple send-destination servers to a single serial port, but you cannot use a mail server and FTP server at the same time.

Port log sentdestination	Notes
Syslog server	Send port logs to a syslog server registered in the NS-2250. You can set syslog sending to on or off for each serial port. The maximum number of syslog servers that can be registered to the NS-2250 is two. If data is received from monitored equipment, the log is sent to the syslog server registered in the NS-2250 in real-time.
NFS server	Save port logs to an NFS server registered to the NS-2250. You can set NFS saving to on or off for each serial port. The maximum number of NFS servers that can be registered to the NS-2250 is two. If data is received from monitored equipment, the log is saved to the NFS server registered in the NS-2250 in real-time.
FTP server	Send port logs to a user of an FTP server registered to the serial port. Port logs are sent when the send conditions in the following table are met. A maximum of two FTP servers (FTP users) can be registered to a single serial port. You can register the following number of servers to the NS-2250: number of equipped ports x 2.
Email address	Send port logs to an email address of a mail server registered to the serial port. Port logs are sent when the send conditions in the following table are met. A maximum of two mail servers (email addresses) can be registered to a single serial port. You can register the following number of servers to the NS-2250: number of equipped ports x 2. You can send an email to a mail server that supports SMTP-Auth as well.

The following table shows the conditions to send port logs to a mail/FTP server. If the specified send conditions are met, the port log sending function sends port logs automatically to the specified send destination. If both the send interval and port log usage rate are specified in the send conditions for port logs, the port log sending function sends port logs to the specified send destination when either of the conditions is met.

Port log send condition	Setting range	Notes
Send interval	0 to 65535 (minutes)	Send port logs at the specified send interval. If the send interval is set to "0", the send interval setting is disabled, and logs are sent according to the usage rate. The default is 60 minutes.
Port log usage rate	10 to 80 (%)	Send port logs when the size of the received logs reaches the specified proportion of port log free space. The default is 80%.

Also, you can send port logs manually by selecting "8: send Port Log" in the port server menu.

Note that sent logs are not resent when logs sent by FTP or email do not reach the server.

2.3 Security functions

As security functions, the NS-2250 is equipped with a user management/authentication function and access control functions for various servers.

2.3.1 User management/authentication function

The NS-2250 is equipped with functions to manage and authenticate users, including registration and deletion functions.
With the default settings, users are registered to the NS-2250 using the group names and user IDs in the following table.
The user IDs in the following table are fixed IDs within the NS-2250 and configured with special roles defined in groups.

User name	User ID	Group	Class	Notes
root	0	root	Device management user	Registered by default and has special privileges to operate and manage the NS-2250. Can configure the NS-2250 and carry out various maintenance commands. Can log in from the CONSOLE port, but not directly from a telnet/SSH client. To log in from a telnet/SSH client, log in as a normal user or an extension user, and then use the "su" command to change to a device management user. Cannot be deleted.
somebody	100	normal	Normal user	Registered by default and is a normal user. Can carry out commands, such as the "ping" command to check connectivity. Cannot configure the NS-2250.
setup	198	setup	Setup user	Used to send and receive NS-2250 settings (startup file) via an FTP client. Registered by default. Cannot log in from a telnet/SSH client or the CONSOLE port.
verup	199	verup	Upgrade user	Used to upgrade or downgrade the system software of the NS-2250 via an FTP/SFTP client. Registered by default. Cannot log in from a telnet/SSH client or the CONSOLE port.
log	200	log	Port log download user	Used to download port logs via an FTP/SFTP client. Registered by default. Cannot log in from a telnet/SSH client or the CONSOLE port.
portusr	500	portusr	Port user	The special user used internally within the NS-2250 when port user authentication is off. Registered by default. Cannot log in from a telnet/SSH client or the CONSOLE port. Cannot be deleted.

An administrator can register the following users and passwords following intended usage and security policies.

User name	User ID	Group	Class	Notes
\<Normal user\>	100 to 190	normal	Normal user	Normal user can be registered by an administrator of the NS-2250. Same as a "somebody" user except that they are not registered by default.
\<Extension user\>	401 to 410	extusr	Extension user	Some permissions can be granted to extension users by settings. When they are not granted, their authority is the same as a normal group. It's necessary to access NS-2250 via SSH by extension user. You can access target devices after several settings (permission of tty manage function, accessible ports, etc.). For details of required settings, see the section 4.7.7" Configure console access function (operating via Ansible)"
\<Port user\>	501 to 599	portusr	Port user	Port user can be registered by an administrator of the NS-2250. When port user authentication is on, you can access the port server from a telnet/SSH client. You cannot log in to the NS-2250 from a telnet/SSH client or the CONSOLE port.

For details about user privileges, see Appendix B, "User privileges".

If a user with management privileges for RADIUS, TACACS+, or other external authentication servers is created, this user can log in to the NS-2250 directly from a telnet/SSH client or the CONSOLE port as an administrator.

For details, see the "create auth access_group root" and "set auth radius server root filter_id_head" commands in the *Command Reference*, and Appendix B, "Examples of attributes and RADIUS authentication/accounting server settings".

2.3.2 RADIUS authentication / accounting function

The NS-2250 is equipped with a RADIUS authentication client to authenticate users by the RADIUS authentication server and a RADIUS accounting client to send login, logout, and other accounting information to the RADIUS accounting server.
You can centrally manage user information and access history by registering users to the RADIUS authentication server/RADIUS accounting server.
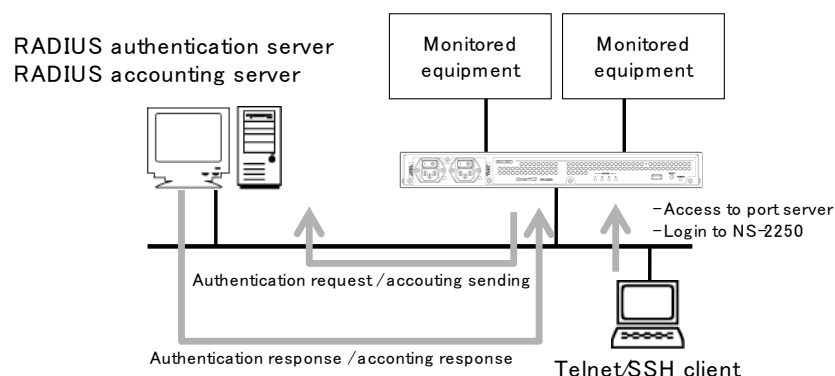
Figure 2-9 User management by RADIUS authentication/accounting server

The RADIUS authentication client and RADIUS accounting client of the NS-2250 support the following functions. For details of the settings and attributes on the RADIUS server, see Section 4.6.3, "Configure the RADIUS authentication function/RADIUS accounting function" and Appendix B, "Examples of attributes and RADIUS authentication/accounting server settings".

・ RADIUS authentication client

Function	Description
Maximum number of registered RADIUS authentication servers	2
RADIUS authentication port	Select between 1812 and 1645 (Default: 1812)
Access control	You can limit the serial ports to which port users can access by configuring the Filter-Id attributes sent from the RADIUS authentication server.

・ RADIUS accounting client

Function	Description
Maximum number of registered RADIUS accounting servers	2
RADIUS accounting port	Select between 1813 and 1646 (Default: 1813)
Accounting information	Accounting information (START/STOP) is sent when service usage is started and ended.

The RADIUS authentication client and RADIUS accounting client of the NS-2250 operate independently. You can use both authentication and accounting or authentication only.

If you use this function, you can authenticate users by the RADIUS authentication server when there is a login from the console or access to monitored equipment from a telnet/SSH client. Three types of users can be authenticated by the RADIUS authentication server: normal users, device management users, and port users. When the "su" command was carried out, authentication is carried out by the user name "root".

Note that users using the FTP/SFTP server of the NS-2250 cannot be authenticated by the RADIUS authentication server. Furthermore, users using SSH to access the NS-2250 or serial ports of the NS-2250 cannot be authenticated by the RADIUS authentication server when the user authentication type of the SSH server has been set to the public key. Set a user name and password in the NS-2250 before use.

	User						
	Normal user (normal group)	Device management user (root)	Extension user (extusr group)	Port user (portusr group)	Setup user (setup group)	Upgrade user (verup group)	Log user (log group)
Console	○	○					
Telnet	○	□		○			
SSH (Basic)	○	□	-	○			
SSH (Public)	-	-	-	-			
FTP					-	-	-
SFTP					-	-	-

○: Can be authenticated by the RADIUS authentication server.
□: After logging in as a normal user or an extension user, can be authenticated by the RADIUS
   authentication server when the "su" command has been carried out.
   If a user with management privileges for RADIUS or other external authentication servers is created, this user can log in to the NS-2250 directly from a telnet/SSH client or console port as an administrator. For details, see the "create auth access_group root" and "set auth radius server root filter_id_head" commands in the *Command Reference*, and Appendix B, "Examples of attribute and RADIUS authentication/accounting server settings" in this manual.
- : RADIUS authentication is not supported. Use local authentication by the NS-2250.

Note that to carry out RADIUS authentication for normal, device management, and port users, you must register Filter-Id attributes to the user definitions of the RADIUS authentication server to distinguish the user types. When there are no Filter-Id attributes or when Filter-Id attributes have been set but it is not possible to identify the user group by the setting, authentication is carried out according to the setting value of the "set auth radius def_user" command.

For details of the settings and attributes on the RADIUS authentication/accounting server, see Section 4.6.3, "Configure the RADIUS authentication function/RADIUS accounting function" and Appendix B, "Examples of attributes and RADIUS authentication/accounting server settings".

(1) Order of user authentication

When RADIUS authentication client settings have been configured in the NS-2250, user authentication is carried out in the following order: NS-2250 local authentication, and then RADIUS authentication.
If local user authentication fails because the user in question has not been registered or because of a password mismatch after local authentication within the NS-2250, the NS-2250 sends an authentication request to the RADIUS authentication server.

If RADIUS authentication client settings have not been configured for the NS-2250, the operation occurs as expected, meaning only local authentication within the NS-2250.
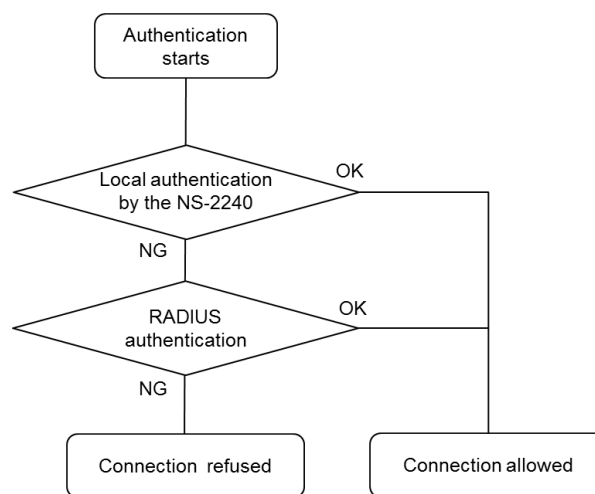
Figure 2-10 Order of user authentication (RADIUS)

(2) Operation of RADIUS authentication client

If the RADIUS authentication client of the NS-2250 has been configured, the RADIUS client of the NS-2250 carries out user authentication by sending an authentication request packet to the RADIUS authentication server when a user logged in to the NS-2250 or when monitored equipment was accessed.
If the RADIUS authentication server returns an authentication-allowed packet, log in to the NS-2250, and access to the port server are allowed.
If the RADIUS authentication server returns an authentication-refused packet, the authentication client of the NS-2250 ends the authentication request to the server at that point.

RADIUS authentication success   RADIUS authentication failure
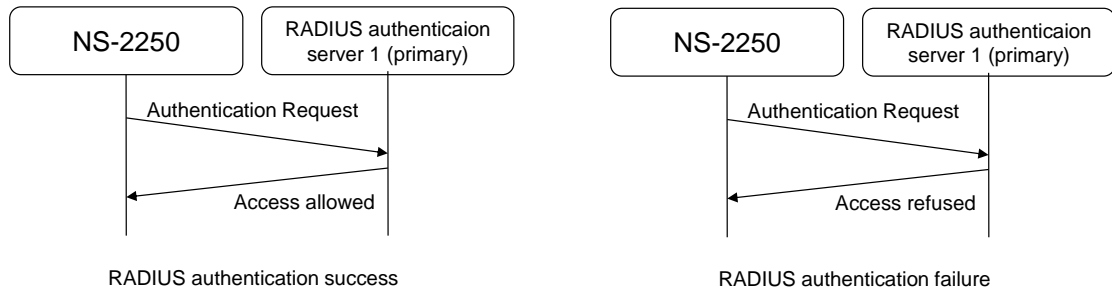
Figure 2-11 When there is a response from the RADIUS authentication server

When the RADIUS authentication client of the NS-2250 sends an authentication-request packet to the RADIUS authentication server but there is no response from the RADIUS authentication server, NS-2250 waits the specified timeout period and then carries out retries the specified number of times.

The default settings for the number of retries and the timeout time of the RADIUS authentication client are 3 times and 5 seconds, respectively. You can change the number of retries and the timeout time.

The accounting START and accounting STOP packets sent by the RADIUS accounting client to the RADIUS accounting server are resent in the same manner.
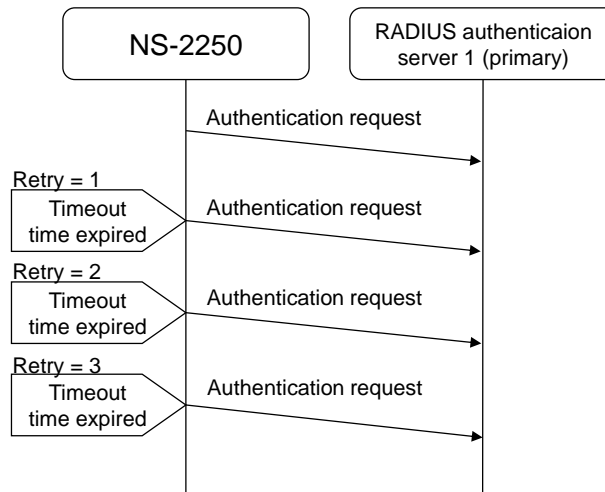
Figure 2-12 When there is no response from the RADIUS authentication server

If NS-2250 is configured to use two RADIUS authentication servers, NS-2250 sends the authentication request to RADIUS authentication server 1 (the RADIUS authentication server with ID number 1). When there is no response from RADIUS authentication server 1, NS-2250 sends the authentication-request to RADIUS authentication server 2 (the RADIUS authentication server with ID number 2). Regardless of the status of the RADIUS authentication server 1, the initial authentication request is always sent to RADIUS authentication server 1.

The accounting START and accounting STOP packets sent by the RADIUS accounting client to the RADIUS accounting server are resent in the same manner.
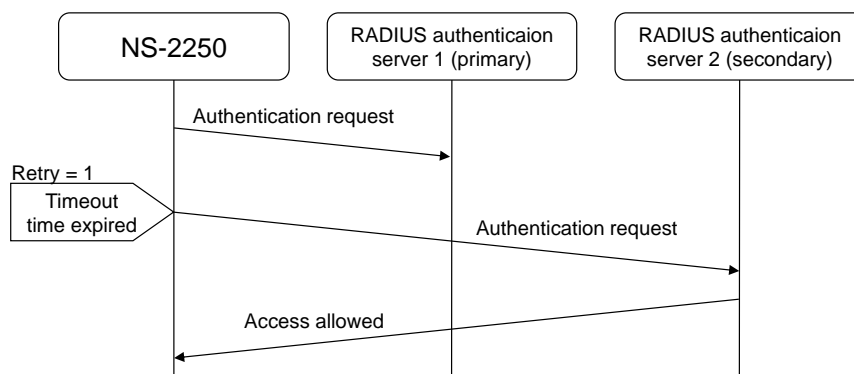
Figure 2-13 Authentication when there are 2 RADIUS authentication servers registered

When there are network or RADIUS authentication server problems and neither RADIUS authentication server 1 nor RADIUS authentication server 2 respond, the RADIUS authentication client of the NS-2250 sends authentication requests alternatively to RADIUS authentication server 1 and RADIUS authentication server 2 until it reaches the specified number of retries.

For example, when the number of retries configured for the RADIUS authentication client is 5 times, the first authentication request is sent to RADIUS authentication server 1. After this, authentication request packets are resent 5 times in the following order: RADIUS authentication server 2->RADIUS authentication server 1-> and then RADIUS authentication server 2.

The accounting START and accounting STOP packets sent by the RADIUS accounting client to the RADIUS accounting server are resent in the same manner.
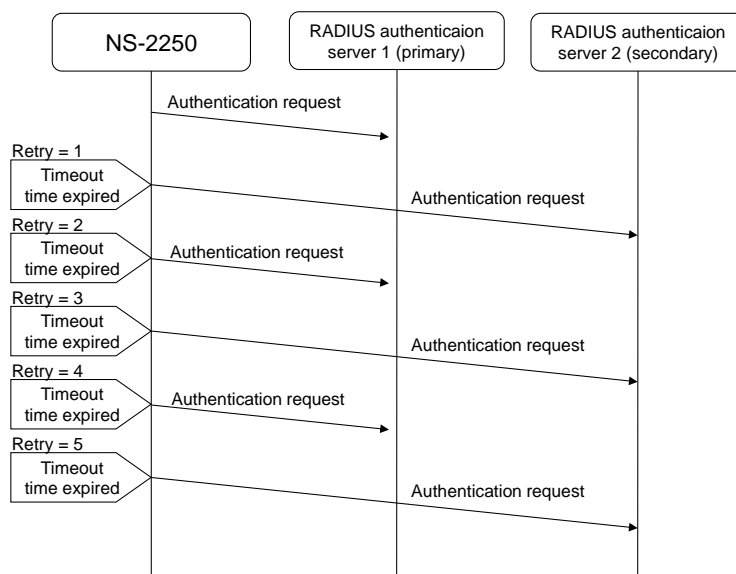
If the specified number of retries is reached but there is no response, the authentication has failed.

Figure 2-14 Authentication when there is no response from 2 RADIUS authentication servers

2.3.3 User group identification and access control of serial ports by RADIUS

On the NS-2250, you can use the RADIUS authentication server to identify user groups such as device management users, normal users, and port users, and centrally manage access to the serial ports by port users. The following section describes the two configuration methods.

(1) Use "filter_id_head"

When you use this function, set the identifiers for user types and the information about serial ports to which port users can access in the Filter-Id attributes of users registered to the RADIUS server and set only the identifiers for user types in the NS-2250. This function is useful when there are a comparatively low number of NS-2250 units or when you want to manage port user access privileges to serial ports and all other settings using the RADIUS authentication server only.

RADIUS server settings

User name	Group name (Filter-Id)
somebody	Normal
root	Admin
suzuki	Port1-10
tanaka	Port11-20
yamada	Port21-32

RADIUS server

NS-2250-1

Filter_Id_head settings

User type	Group name
Normal user	Normal
Device management user	Admin
Port user	Port

NS-2250-2

Filter_Id_head settings

User type	Group name
Normal user	Normal
Device management user	Admin
Port user	Port

Figure 2-15 User group identification and access control of serial ports (filter_id_head)

(2) Use the access grouping function

Before you use this function, carry out the following configuration. In the RADIUS server, set the group name to which the user belongs. In the NS-2250, set the group name for each user type. Configure the access privileges to serial ports for the port user group in the same manner.

This function is useful when the access privileges for serial ports are different for each NS-2250 (for example, when users in Group1 can access serial ports 1 through 10 on the NS-2250-1, serial ports 15 through 20 on the NS-2250-2, etc.), when there are multiple access groups to be registered, or when the individual user settings of the RADIUS authentication server increase and management becomes difficult.

RADIUS server setting

User name	Group name
somebody	Normal
root	Admin
suzuki	Group1
tanaka	Group2

RADIUS server

NS-2250-1

Access grouping setting

User type	Group name	Port access rights
Normal user	Normal	Cannot be configured
Device management user	Admin	
Port user	Group1	Serial port 1~10
Port user	Group2	Serial port 11~20

NS-2250-2

Access grouping setting

User type	Group name	Port access rights
Normal user	Normal	Cannot be configured
Device management user	Admin	
Port user	Group1	Serial port 15~20
Port user	Group2	Serial port 21~30

Figure 2-16 User group identification and access control of serial ports (access grouping)

For details, see the "set auth radius server { portusr | root | normal } filter_id_head" and "create auth access_group" commands in the *Command Reference*, Section 4.6.3, "Configure the RADIUS authentication function/RADIUS accounting function", and Appendix B, "Examples of attributes and RADIUS authentication/accounting server settings" in this manual.

2.3.4 TACACS+ function

The NS-2250 is equipped with a TACACS+ client function to authenticate users, approve user groups, and carry out accounting for user logins and logouts.

You can centrally manage user information and access history by registering users to the TACACS+ server.

Because up to two TACACS+ servers can be added to the NS-2250, the TACACS+ servers can be used in a redundant configuration.
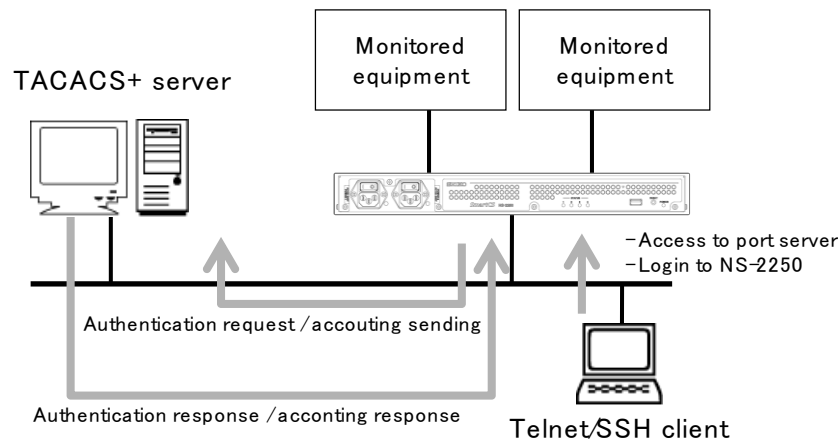
Figure 2-17 User management by TACACS+ server

The NS-2250 supports the TACACS+ client function.
The following table lists the supported functions.

・ TACACS+ function

Function	Description
Maximum number of registered TACACS+ servers	2
TACACS+ port	Fixed to TCP (49)
Access control	You can limit the serial ports to which port users can access by setting the attributes to be sent from the TACACS+ server.
Accounting	Accounting information (START/STOP) is sent when service usage is started and ended.

The TACACS+ function on the NS-2250 runs authentication/approval and accounting independently. You can use the authentication, approval, and accounting functions together or authentication and approval only.

For details of the settings and attributes of the TACACS+ server, see Section 4.6.4, "Configure the TACACS+ function".

If you use this function, you can authenticate users by the TACACS+ server when there is a login from the console or access to monitored equipment from a telnet/SSH client. Three types of users can be authenticated by the TACACS+ server: normal users, device management users, and port users. When the "su" command was carried out, authentication is carried out by the user name "root". This user name can be changed through settings.

Note that users using the FTP/SFTP server of the NS-2250 cannot be authenticated by the TACACS+ server. Furthermore, users using SSH to access the NS-2250 or a serial port of the NS-2250 cannot be authenticated by the TACACS+ server when the user authentication type of the SSH server has been set to the public key. Set a user name and password in the NS-2250 before use.

	User						
	Normal user (normal group)	Device management user (root)	Extension user (etxusr group)	Port user (portusr group)	Setup user (setup group)	Upgrade user (verup group)	Log user (log group)
Console	○	○					
Telnet	○	□		○			
SSH (Basic)	○	□	-	○			
SSH (Public)	-	-	-	-			
FTP					-	-	-
SFTP					-	-	-

○ : Can be authenticated by TACACS+ server.

□ : After logging in as a normal user or an extension user, can be authenticated by the TACACS+
    authentication server when the "su" command has been carried out.
    If a user with management privileges for the TACACS+ server is created, this user can log in to the NS-2250 directly from a telnet/SSH client or console port as an administrator. For details, see the "create auth access_group root" command in the *Command Reference*.

- : Cannot be authenticated by TACACS+ server. Use local authentication by the NS-2250.

Note that to carry out TACACS+ authentication for normal, device management, and port users, you must register attribute and value pairs to distinguish the user types, such as normal, device management, and port users, to the user definitions of the TACACS+ server. The attribute name and value pair can be determined as desired by a device administrator. When there are no attributes to identify the user type or when the user cannot be identified by this setting, authentication processing is carried out according to the setting value of the "set auth tacacs def_user" command.

For details of the settings and attributes of the TACACS+ server, see Section 4.6.4, "Configure the TACACS+ function".

(1)   Order of user authentication

When TACACS+ has been configured, user authentication is carried out in the following order: NS-2250 local authentication, and then TACACS+ authentication.
If user authentication fails because the user in question has not been registered or because of a password mismatch after local authentication within the NS-2250, the NS-2250 sends an authentication request to the TACACS+ server.

If TACACS+ has not been configured, the operation occurs as expected, meaning only local authentication within the NS-2250.
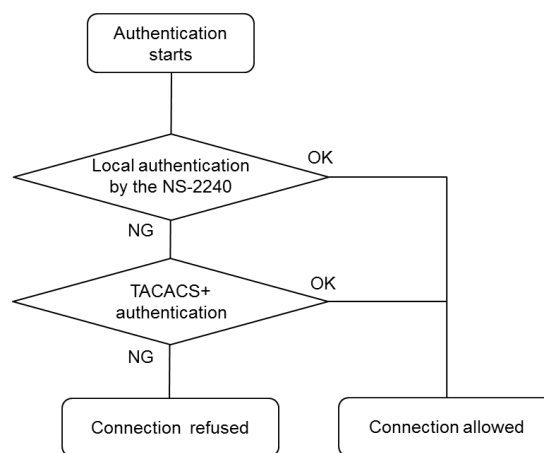
Figure 2-18 Order of user authentication (TACACS+)

(2)   TACACS+ operation

TACACS+ is made up of authentication, approval, and accounting.

Function	Content
Authentication	Authenticates users by user ID and password.
Approval	Approves service attributes sent by the NS-2250. Confirms that the service attribute is "smartcs", and then responds with the user type (normal user, device management user, or port user) configured for the authenticated user.
Accounting	Carries out accounting for the login and logout of users.

User authentication by TACACS+ is carried out in the following manner.
For user authentication, at least authentication and approval must be successful. If either authentication or approval fails, the session is ended.
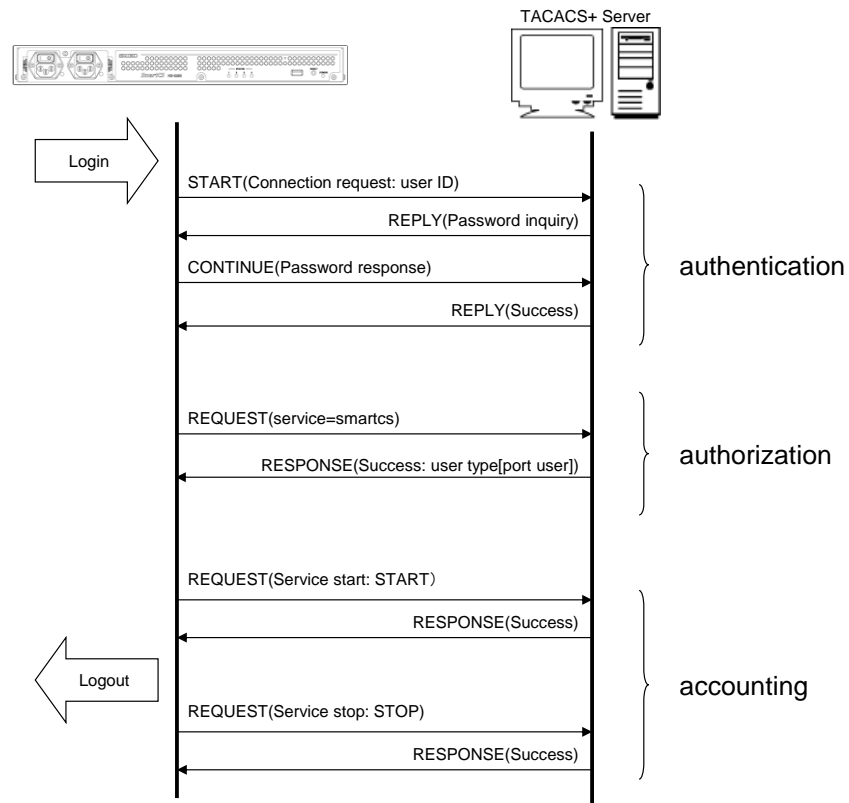
Figure 2-19 Authentication, approval, and accounting flow (TACACS+)

If there is one TACACS+ server registered to the NS-2250, and there is no response from the TACACS+ server within the timeout time, the connection request fails.

If there are two TACACS+ servers registered, an authentication request is sent to TACACS+ server 1 (the TACACS+ server with ID number 1).
When there is no response from TACACS+ server 1, an authentication request is sent to TACACS+ server 2 (the TACACS+ server with ID number 2).
The initial authentication request is always sent to TACACS+ server 1.

The approval function sends a REQUEST package to the successfully authenticated server.
If there is no response from the server within the timeout time, approval is ended.
The accounting function operates the same way as the authentication function.
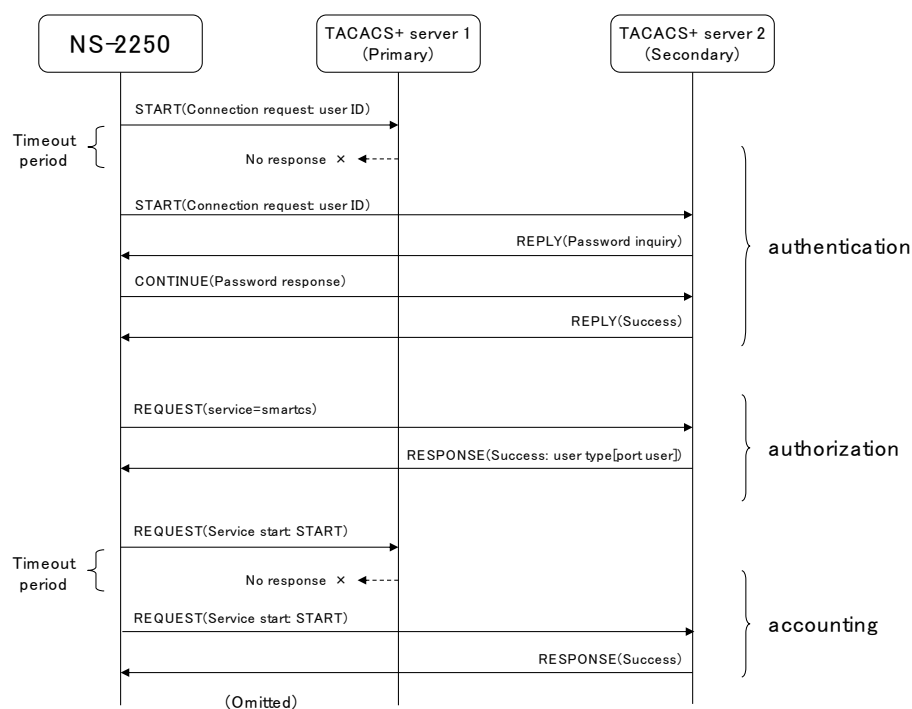
Figure 2-20 Authentication when there are two TACACS+ servers registered

2.3.5 User group identification and access control of serial ports by TACACS+

You can use the TACACS+ server and NS-2250 access grouping function to identify user groups such as device management users, normal users, and port users, and centrally manage access to the serial ports by port users.

Before you use this function, carry out the following configuration. In the TACACS+ server, set the group name to which the user belongs. In the NS-2250, set the group name for each user type. Configure the access privileges to serial ports for the port user group in the same manner.

This function is useful when the access privileges for serial ports are different for each NS-2250 (for example, when users in Group1 can access serial ports 1 through 10 on the NS-2250-1, serial ports 15 through 20 on the NS-2250-2, etc.), when there are multiple access groups to be registered, or when the individual user settings of the TACACS+ authentication server increase and management becomes difficult.

TACACS+ server setting

User name	Group name
somebody	Normal
root	Admin
suzuki	Group1
tanaka	Group2

TACACS+ server

NS-2250-1

NS-2250-2

Access grouping settings

User type	Group name	Port access rights
Normal user	Normal	Cannot be configured
Device management user	Admin	
Port user	Group1	Serial port 1-10
Port user	Group2	Serial port 11-20

Access grouping settings

User type	Group name	Port access rights
Normal user	Normal	Cannot be configured
Device management user	Admin	
Port user	Group1	Serial port 15~20
Port user	Group2	Serial port 21~30

Figure 2-21 User group identification and access control of serial ports (TACACS+)

For details, see the "create auth access_group" command in the *Command Reference*, and Section 4.6.4, "Configure the TACACS+ function".

2.3.6 Control access to servers (allowhost)

You can register the network addresses and masks that are allowed connections for each server of the NS-2250.
The following table shows the servers of the NS-2250 for which you can restrict access.

Server	Description
Access control of telnet server	Restrict clients that access the telnet server of the NS-2250.
Access control of SSH server	Restrict clients that access the SSH server of the NS-2250.
Access control of FTP servers	Restrict clients that access the FTP server (used for the upgrade, setup file, and port log operations) of the NS-2250.
Access control of port server	Restrict clients that access the port server. You can specify the communication method (telnet/SSH) and connection mode (Normal mode/Monitoring mode).

With the default settings of the NS-2250, client terminals that can access the NS-2250 are limited to the following conditions.

Restricted item	Setting
Networks allowed connection	All
Services allowed connection	Telnet/port server
Connection control of serial ports	Telnet Normal mode

2.3.7 Firewall (ipfilter)

With the Firewall (ipfilter) you can achieve the access control by respective filter conditions such as IP address, protocol type, and port number.
The firewall (ipfilter) is evaluated in advance of the previous chapter of "2.3.6 Control access to servers". The below table shows available filter types in the Firewall (ipfilter).

Item		Description
Filter type	Built-in filter (receive)	The built-in filter is a filter that is configured in the system in advance. It accepts the following received packets. (1)　Return packet for a packet sent by NS-2250 The following packets are also subject to this filter. ・SYN/ACK and ACK packet at 3-way handshake ・FIN, FIN+ACK and RST packet at end of session ・TCP connection request packet (SYN) of FTP-DATA session (passive) when accessing ftpd function ・TCP connection request packet (SYN) of FTP-DATA session (active) when ftp command is executed ・IKE packet after establishing ISAKMP-SA ・ESP packet after establishing IPSEC-SA ・ICMP error message packet (2)　Packet sent out from loopback device of NS-2250 Triggered by enabling the Firewall. (Default: disable) Deleting or modifying the built-in filter is not possible.
	Custom filter (receive)	User-configurable filter processed at the input of the interface. Processed after the built-in filter. Max. 64 entries can be stored.
Filter condition	Interface	eth1: LAN1 port eth2: LAN2 port bond1: Bonding port
	IP address	SA: Source IP address DA: Destination IP address
	Protocol	ICMP: ICMP type(0-255) TCP: TCP port number(1-65535) UDP: UDP port number(1-65535) ESP: ESP protocol
	Processing	accept: accept the packet drop: drop the packet

When the Firewall (ipfilter) becomes enabled each filter will be evaluated in the order shown below.
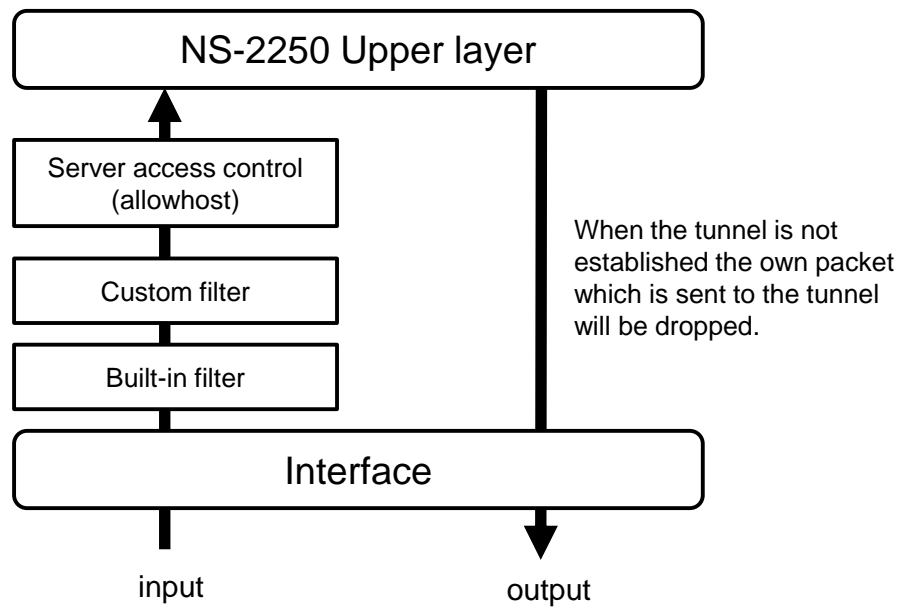
Figure 2-22 The filter evaluation order when the Firewall (ipfilter) is enabled.

2.3.8 IPsec

NS-2250 supports IPsec which performs the VPN on the encryption of the packet to establish secure communication as well as the internet key exchange protocol.
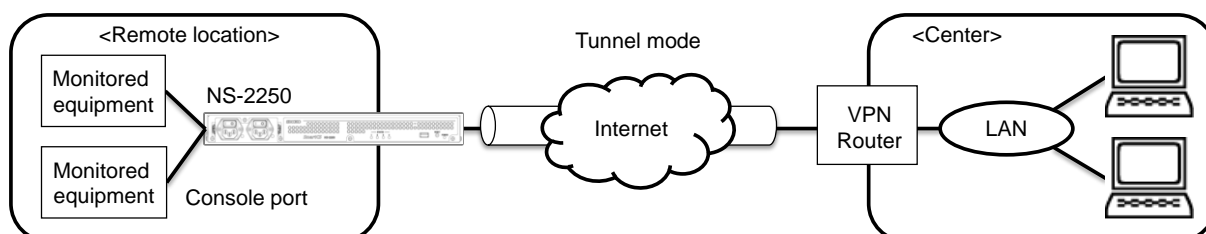
Figure 2-23 IPsec VPN connection

The below table shows the connection mode and the operation mode as well as the number of the available connections.

Item	Description
Connection mode	Cryptographic key authentication by the pre-shared key (PSK)
Operation mode	Tunnel mode
The number of the available connections	Max. 8 connections. The configuration to establish the IPsec connection by the opposite network (subnet) is required.
Monitoring	Detect disconnection of tunnel interface by DPD
Others	NAT traversal (UDP capsuling for ESP)

NS-2250 supports the following IKE ISAKMP-SA (Phase1).

Item	Description
IKE protocol	IKEv1/IKEv2
Encryption algorithm	3DES/AES128/AES128CTR/AES256
Authentication algorithm	MD5/SHA1
DH group	2(1024bit)/5(1536bit)/14(2048bit)
ISAKMP-SA lifetime	3600～86400 sec. (Default: 10800 sec.)

NS-2550 supports the following IPsec-SA (Phase2)

Item	Description
Encryption algorithm	3DES/AES128/AES128CTR/AES256
Authentication algorithm	HMAC-MD5/HMAC-SHA1
DH group (during PFS)	2(1024bit)/5(1536bit)/14(2048bit)
IPsec-SA lifetime	3600～86400sec. (Default: 3600 sec.)

The multiple uses of IPsec and bonding are not possible.

2.4   Operation management functions

The NS-2250 has the following operation management functions.

(1)   DNS client function
This function resolves names when applications, such as the "ping" and "telnet" command, of the NS-2250 contact the DNS server. The number of DNS servers that can be registered to the NS-2250 is two.

(2)   SNTP client function
This function synchronizes the time of the NS-2250 with a time of the NTP server.
The number of NTP servers that can be registered to the NS-2250 is two.

(3)   Static routing function
This function manages network route information using static routing. 99 static routes can be registered to the NS-2250.

(4)   SNMP agent function
You can use the SNMP agent function to carry out alive monitoring from outside the NS-2250. The NS-2250 supports SNMP Version 1/Version 2c/Version 3.
If the SNMP agent function is enabled, it responds to MIB access from external SNMP servers. When the function receives a Get request in the Version 1 format from an SNMP server, it responds using Version 1. When it receives a Get request in the Version 2c format, it responds using Version 2c. When it receives a Get request in the Version 3 format, it responds using Version 3.
The maximum number of SNMP servers that can be registered to the NS-2250 is four.
Also, the trap also supports Version 1, Version 2 and Version 3, and a maximum of four trap-send destinations can be registered to the NS-2250. The following table lists the supported traps.

Trap	Description
Coldstart Trap	Trap sent when the NS-2250 starts. With the default settings of the NS-2250, Coldstart Trap is on.
Link Trap	Trap sent when the LAN port link moves up or down. If the LAN port links up, the Link Up trap is sent. If the LAN port links down, the Link Down trap is sent. With the default settings of the NS-2250, Link Trap is on.
Authentication Failure Trap	Trap sent when an authentication fails (when an SNMP request is received from an unauthorized SNMP server or unauthorized community). With the default settings of the NS-2250, Authentication Failure Trap is on.
Serial DSR Trap	Trap sent when the serial port DSR signal moves up or down. If the NS-2250 detects that the DSR signal of the serial port is on, a DSR On trap is sent. If the NS-2250 detects that the DSR signal of the serial port is off, a DSR Off trap dissent. With the default settings of the NS-2250, Serial DSR Trap is off for all serial ports.
Power Trap	Trap sent when the power moves on or off. With the default settings of the NS-2250, Power Trap is on.
Bonding Active Switch Trap	Trap sent when detecting the switching of the active port in bonding function. With the default settings of the NS-2250, Bonding Active Switch Trap is on.

(5)   Syslog client function
       You can send syslog messages to external syslog servers. The NS-2250 can send syslog
       messages and port logs output by the NS-2250 to a syslog server.
       Syslog messages and port logs output by the NS-2250 are send to the same syslog server.
       The maximum number of syslog servers that can be registered to the NS-2250 is two.

Syslog function	Description
Protocol	RFC3164 compliant
Syslog facility	For facility, "Local0" through "Local7" are supported. The default setting is "Local1".
Port log facility	For facility, "Local0" through "Local7" are supported. The default setting is "Local0".

(6)   Telnet/SSH server function
       A telnet/SSH server receives requests from telnet and SSH clients. You can perform
       maintenance on the NS-2250 from a remote network.
       The maximum number of sessions that can access a telnet/SSH server of the NS-2250 is
       five for both telnet and SSH.

(7)   Telnet client function
       You can access the Telnet server in the network using the Telnet command.

(8)   FTP/SFTP server function
       An FTP server sends and receives system software files, startup files, and port logs of the
       NS-2250 from an FTP client on the network.
       You can transfer, like FTP, files encrypted using SFTP.
       The maximum number of sessions that can access an FTP server of the NS-2250 is two.
       The maximum number of sessions that can access an FTP/SFTP server of the NS-2250 is
       one.

(9)   FTP/TFTP client function
       This function sends startup files and port log files to an FTP/TFTP server and acquires
       startup files and system software from an FTP/TFTP server.

(10)   Upgrade/downgrade function
       You can upgrade or downgrade the system software of the NS-2250 by using an
       FTP/TFTP client or FTP/SFTP server to deliver the system software file to the NS-2250.
       For the methods to upgrade or downgrade the NS-2250, see Chapter 5, "Management and
       maintenance".

(11)   DSR signal transition detection function
       This function detects the following transitions of the DSR signal: on→off/off→on. By using
       this function, you can quickly detect problems with monitored equipment and detect the
       connection and disconnection of serial cables.

(12) Automatic recovery function
If a problem occurs within the NS-2250, this function monitors the trouble using a watchdog timer and performs a reboot automatically.

(13) Temperature sensor function
This function measures the temperature by using a temperature sensor.

(14) Time zone function
This function configures the time zone to which the NS-2250 belongs.

(15) bonding function
NS-2250 supports Ethernet bonding function, which enables port redundancy by bonding 2 physical ports to virtual 1 port.
"Active port" transmits/receives the packets, meanwhile received packets from "Standby port" are discarded.

By enabling this function, virtual port "bond1" is automatically configured as a master interface, and physical port eth1/eth2 belong as a slave interface.
Also, using the bonding function, the IP address of NS-2250 is configured to this virtual port "bond1" instead of physical ports eth1/eth2.
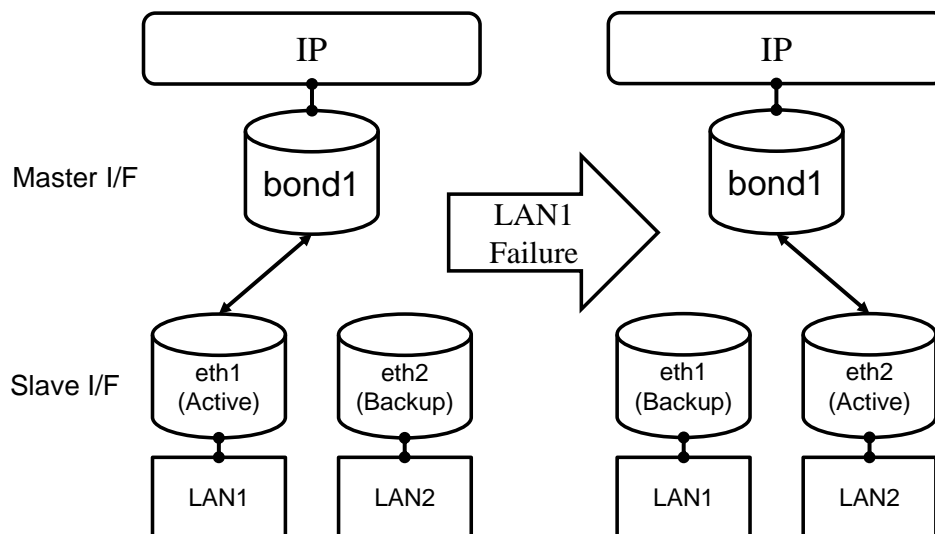
Figure 2-22 Bonding function

Specification of the bonding function is as follows:

Function	Description
Redundant type	Fault-torelance (Active-Backup) In bonding mode, NS-2250 uses only 1 physical port to transmit/receive the packets even if both LAN ports are linked up. Basically, eth1 is configured as an Active port.
Switch of the active port	- automatically switch by sensing the link failure of active port - manually switch by CLI command
GARP	NS-2250 transmits the GARP when the active port is switched. The virtual interface "bond1" uses the MAC address of eth1. Even the active port is changed from eth1 to eth2, the MAC address of GARP sent from eth2 is still eth1.
Linkup wait timer (option)	This wait timer is the delay period enabling backup interface after the detection of link-up. The period can be configured 1-60 sec. The default value is "off (no delay)".

(16) IPv6 communication function
NS-2250 supports IPv6 communication function in the system software of version 1.3 and later.
About the functions corresponding to IPv6, refer to the following table.

Category	Function	V1.3-2.1	V2.2 and more
Port access function	Port server function	○	○
	Port log sending function (SYSLOG/NFS/FTP/Mail)	-	○
Management function	DNS client function	○	○
	Static routing function	○	○
	Telnet/SSH server function	○	○
	Telnet client function	○	○
	FTP/SFTP server function	FTP – SFTP ○	FTP ○ SFTP ○
	Bonding function	○	○
	SNTP client function	-	○
	SNMP agent function	-	○
	SYSLOG client function	-	○
	FTP/TFTP client function	-	○
Security function	Access control function(allowhost)	○	○
	RADIUS authentication/accounting function	-	○
	TACACS+ function	-	○
	Firewall(ipfilter) function	-	○
	IPsec function	-	-

You can use the "ping6" and "traceroute6" command and so on as the maintenance command of IPv6 communication.

About how to use each command, refer to "Chapter6 Troubleshooting".

(17) tty manage function
This function enables the configuration and maintenance of of target devices connected to serial ports of NS-2250 by sending specified characters to them. This is supported in the system software version 2.0 and later. The specification is shown in the table below.

Item	Detail
User	To use this function, it requires creating new users in extusr group and granting tty manage permission. If you do not have tty manage privileges, you will have the same privileges as a user in the normal group. When executing commands such as "ttysend" and "ttylog", you must configure the serial ports accessible to the user. Up to 10 users in extusr group can be registered. (UID: 401-410)
Activation	This function will be enabled by "enable ttymanage" command.
Protocol	This function has to be used via SSH and it is unable to connect via Telnet or Console.
Command	The following operations can be executed after logging in as a user of extusr group. "ttysend" command: sending and receiving characters "ttylog" command: displaying and deleting port logs
Access to target devices	Only one command, such as ttysend, can be executed at a time on one serial port of NS-2250.
Exclusion with portd normal session	Users cannot access target devices using ttymanage function when portd normal session (rw) has already existed. Users can not access target devices using portd normal sessions when the session of ttymanage function has already existed as well. However, this function can be disabled by the "set portd service exclusive" command. portd monitor session (ro) is exempt from this exclusion.
Display the log of the sent character	For each serial port, users can confirm the commands which had been sent to target devices using tty manage function. They are shown by executing the "show log manage send tty" command after changing to device management user by "su" command.

(18) Operation via Ansible
You can operate NS-2250 and target devices connected to serial ports of NS-2250 via Ansible. In this operation, 2 functions are available as below.

- CLI command function
Using this function, it's possible to execute CLI commands of NS-2250 via Ansible.
This function enables automatic execution of the configuration and maintenance via Ansible. CLI command function is supported in the system software of all versions.

- Console Access function

Using this function, it's possible to execute commands for target devices connected to serial ports of NS-2250 via Ansible. This function is supported in the system software version 2.0 and later because it needs to use tty manage function.

For details of the required commands and Ansible module, see section 4.7.6 "Configure CLI command function (operating via Ansible)", 4.7.7 "Configure console access function (operating via Ansible)", "Command Reference" and "Ansible operation guide".

Chapter 3
Configuration procedures

Chapter 3 provides an overview of start, stop, and setup procedures.
Read this chapter before starting work.

3.1　Start, check and stop the NS-2250

3.1.1　Insert a USB memory

The setup information of the NS-2250 can be stored on flash memory of the NS-2250 or the included USB memory. When the USB memory is set, setup information is read from the USB memory when the NS-2250 is started.

For details about using the USB memory, see the *Instruction Manual*.

(1) insert the USB memory into the USB port.
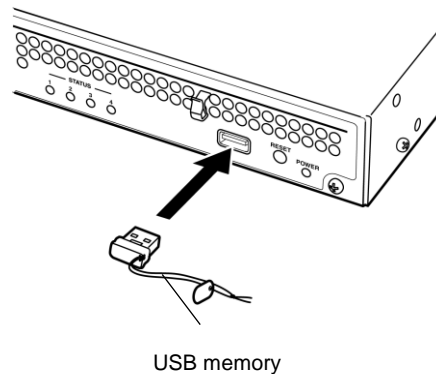
USB memory

Figure 3-1 Insert a USB memory

Because the NS-2250 stores the system software internally, the system software starts even when no USB memory is inserted.

Note that if the device is started without inserting a USB memory, read locations, save locations, and other settings switch to the settings inside the NS-2250

If the settings are saved on the USB memory, you can use the NS-2250 with the original settings by simply inserting the original USB memory and then starting the NS-2250 after an equipment exchange when a malfunction has occurred.

For the installation and setup of the NS-2250, see the *Installation manual*.

Caution　Be sure to insert the USB memory into the USB port of NS-2250 fully.

Caution　While the STATUS 4 light is on, do not remove the USB memory. If the USB memory is removed during the operation, the operation of the NS-2250 is not guaranteed.

Caution The USB memory is intended for the NS-2250. Do not use the USB memory with another device. If the USB memory has been inserted into a PC or another device, the NS-2250 may no longer recognize the USB memory normally or another malfunction may occur.

3.1.2 Connect a device management terminal

To operate the NS-2250, you must configure the functions of the NS-2250 in advance. The functions settings of the NS-2250 are configured from a device management terminal, so connect a device management terminal before switching on the power of the NS-2250.

The device management terminal can be connected to either the CONSOLE port of the NS-2250 or via the network to the LAN port of the NS-2250.

When you connect the device management terminal to the CONSOLE port, the device management terminal displays a message while the NS-2250 is booting. Note that this message does not appear when the terminal is connected via the network.

(1) Connect to the CONSOLE port
Using an Ethernet cable (straight-through Category 5 UTP cable) with the included NS-354 DB9-RJ45 adapter, connect the CONSOLE port (RJ-45 8-pin connector) of the NS-2250 and the COM port (D-sub 9-pin connector) of the device management terminal.

Connect to CONSOLE port

Connect to COM port of device management terminal

Fixing screws

Ethernet cable

NS-354 DB9-RJ45 adapter
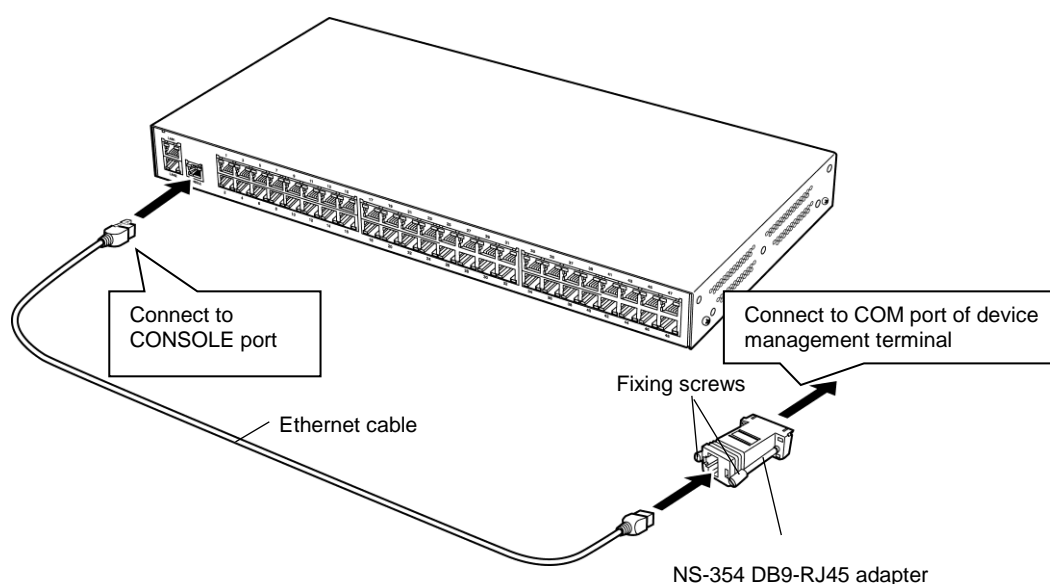
Figure 3-3 Connect the NS-2250 and the COM port of the device management terminal

The following table shows the settings (default state) of the CONSOLE port of the NS-2250. Match the settings of the serial port of the device management terminal with the settings of the CONSOLE port of the NS-2250.

Item	Default value
Transfer speed	9600 bps
Data length	8 bit
Parity	None
Stop bit	1 bit
Flow control	XON/XOFF

(2) Connect to a network

Connect the device management terminal to the network, and then log into the NS-2250 from a telnet client via the LAN port of the NS-2250.
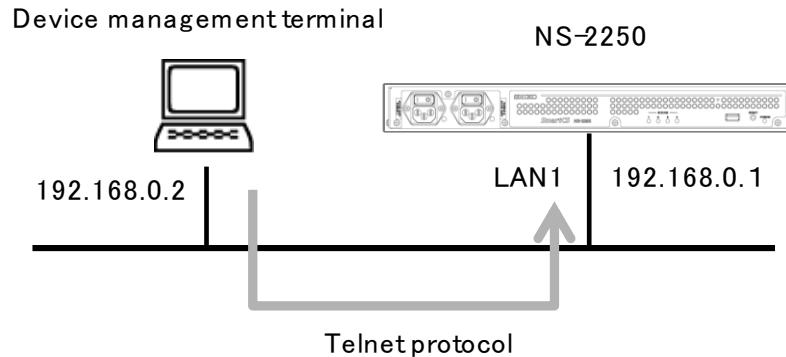
Figure 3-5 Connect the NS-2250 and the device management terminal via a network

With the default settings of the NS-2250, the parameters in the following table of been set in advance so that the NS-2250 can be configured from a management terminal on the network. To configure the NS-2250 via the network, match the network settings of the device management terminal with the network address to which the NS-2250 belongs.
The default value of IPv6 communication function is "disable".

Item	Default value
Host name	NS-2250
IP address	LAN1: 192.168.0.1/24 LAN2: none
Connectable IP address	ALL
Connectable service	Telnet
LAN port	LAN1: Auto Negotiation LAN2: Auto Negotiation

After starting the NS-2250, connect to the NS-2250 from a telnet client of the device management terminal, change to administrator mode, and then carry out the "console" command. If this command is carried out, the console messages of the NS-2250 are output to the telnet client of the device management terminal.

3.1.3 Start the NS-2250

For the NS-2250, connect either the AC power cable. At the rear of the NS-2250, flip the power switch to the " | " side to switch on the power and start the NS-2250. (The "O" side is off.)

When you will use an NS-2250, see the *Installation manual*.
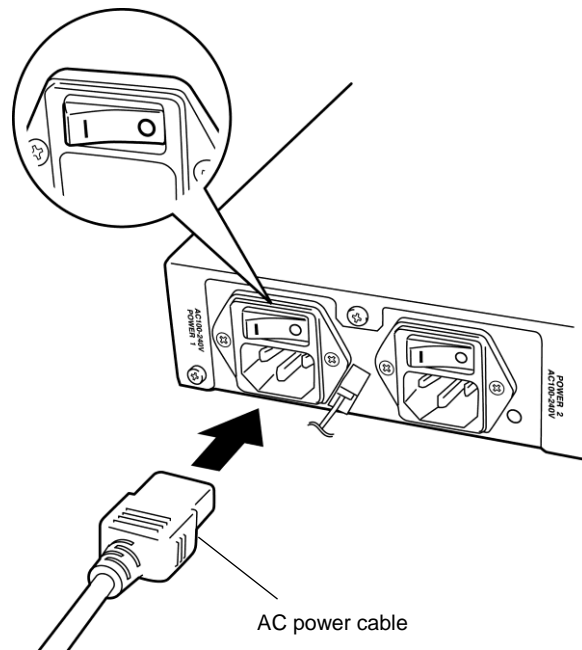
Figure 3-6 Switch on the power of the NS-2250

If the NS-2250 is started while an Ethernet cable is inserted in the LAN port, a GARP packet and Unsolicited NA packet are sent automatically. This is useful because the ARP table and NDP table of the network device or server are updated automatically when NS-2250 is installed or replaced.

NS-2250 sends the GARP packet and Unsolicited NA packet by the following times.

  Link Up of LAN port
  Change of IP address

3.1.4 Check the NS-2250

If the power of the NS-2250 is switched on, the boot process starts. Use the four STATUS lights on the front of the NS-2250 to check that the boot process is proceeding normally. While the NS-2250 is booting, the STATUS lights switch on in the following order. If an error occurs, the STATUS lights flash. If the boot process ends normally, all four STATUS lights switch off.

STATUS light *1				Boot progress status
1	2	3	4	
●	●	●	●	Hardware initialization complete
●	○	○	○	A self-diagnostic test (POC) is running
○	●	○	○	Rom-Monitor is running
○	○	●	○	System software starting (1nd Boot)
●	○	●	○	System software starting
●	○	●	●	System software starting (during USB memory access)
○	○	○	○	System software start complete

*1: STATUS light symbols: ○ : off, ● : on

Caution If STATUS light 1 through 4 flashes or stay on, the NS-2250 has probably malfunctioned. Resolve the trouble following Chapter 6, "Troubleshooting".

If the power is switched on, a self-diagnostic test is run, and then the system software starts. If the system software starts, a start message and "NS-2250 login:" prompt appear on the device management terminal. Make sure that no error messages appeared during the start message.

```
INIT: version X.XX booting

Welcome to NS-2250 Console Server

Starting Bootlog daemon: bootlogd.


System                : System Software Ver 1.0 (Build 2015-XX-XX)

Boot Status           : Power on (00:01:00)

System Up Time        : 2015/09/03 21:12:07

Local MAC Address     : 08:00:83:ff:4c:b8

Number of MAC Address : 2

Model                 : NS-2250-48 (48 port)

Serial No.            : XXXXXXXX

BootROM               : Ver X.X.X

Main Board CPU        : e500v2 (533.333328MHz)

Main Memory           : 1025264 KBytes


   : (omitted)

Welcome to NS-2250 Console Server
NS-2250 login:
```

3.1.5 Stop the NS-2250

To stop the NS-2250, save the settings of the NS-2250 to the startup file, and then use the following procedure to carry out the "shutdown" command. Next, either confirm that the "MON>" prompt is displayed on the console or wait for the STATUS 2 light on the front of the NS-2250 to switch on. Finally, switch off the power or unplug the power cable.

⚠ Warning

Do not operate the POWER switch with wet hands.

Doing so can result in electric shock.

⚠ Caution

Risk of electric shock.

To provide instruction that all power sources shall be disconnected before replacing to avoid shock hazard

(1) Log in to the NS-2250, and then change to a device management user. For details of login and logout, see Section 3.2, "Set up the NS-2250".
(2) Carry out the "write" command to save the running configuration to the startup file.
(3) Carry out the "shutdown" command.

```
(c)NS-2250> su↵
Password: ↵

(c)NS-2250# write↵
Do you really want to write external startup1 [y/n] ? y↵
write external startup1
...................writing
write internal startup1
...................writing
(c)NS-2250#
(c)NS-2250# shutdown↵
Do you really want to shutdown [y/n] ? y↵
          :
MON>
```

(4) If the system software stops, the STATUS 2 light on the front of the NS-2250 switches on, and then ROM Monitor prompt "MON>" appears on the system console.
(5) After confirming that the system software stopped, switch off the power of the NS-2250.
Flip the POWER switch on the front of the NS-2250 to the "O" side to switch the power off.

3.2   Set up the NS-2250

Figure 3-10 shows the setup procedure for the NS-2250. For details of commands to configure functions, see the *Command Reference*.

```
         ┌───────────────┐
         │     Start      │
         └───────────────┘
                 │
         ┌───────────────────────┐
         │  Login to  NS-2240     │
         └───────────────────────┘
                 │
         ┌───────────────────────┐
         │  Switch to a device    │
         │  management user       │
         └───────────────────────┘
                 │
         ┌───────────────────────┐
         │  Configuration         │
         │  (command execution)   │
         └───────────────────────┘
                 │
         ┌───────────────────────┐
         │ Save the configuration │
         │ to the file (startup file) │
         └───────────────────────┘
                 │
         ┌───────────────┐
         │     End        │
         └───────────────┘
```

From a management terminal connected to the CONSOLE port or over the network, specify a user name and password registered to the NS-2250 to login.

Switch to a device management user to configure the settings.

Carry out the setting commands to configure the NS-2250. The information configured here is reflected in the operations of the NS-2250, but it is not saved to the settings file (startup file). If the power is switched off, the configured information is lost.

Save the configuration to the file (startup file).
If the settings are saved, changes are not lost even when the power switched off, and the saved settings are applied the next time the NS-2250 is started.

Figure 3-10 Set up the NS-2250

3.2.1 Log in and log out

This section describes how to log into and log out of the NS-2250 from a device management terminal connected to the CONSOLE port or a client terminal on the network.

(1)   Users who can log in
      At the default settings, the following users are registered as users that can log in to the NS-2250: normal user "somebody" and device management user "root". Note that passwords are not set for these users.

User name	Group name	Class	Notes
root	root	Device management user	Registered by default. (Password not set.) Can configure the NS-2250 and carry out maintenance commands. Cannot be deleted.
somebody	normal	Normal user	Registered by default. (Password not set.) Can carry out commands, such as the "ping" command to check connectivity.

(2)   Log in from a device management terminal connected to the CONSOLE port
      If the NS-2250 is started, the "login:" prompt appears on the device management terminal. Enter the user name and password of a normal user or device management user registered to the NS-2250. (With the default settings, normal user "somebody" and device management user "root" do not have passwords configured.)

・ Log in as a normal user "somebody"

```
NS-2250 login: somebody↵
Password: ↵
(c)NS-2250>
```

・ Log in as a device management user "root"

```
NS-2250 login: root↵
Password: ↵
(c)NS-2250#
```

The last character of the prompt differs by the type of login user. For normal users, a ">" is displayed. For device management users, a "#" is displayed.

(3)   Log in from a client terminal on the network
      If you connect to the NS-2250 (with the default settings, the IP address is 192.168.0.1) from a client terminal on the network via a telnet connection, the "login:" prompt appears. Enter the user name and password of a normal user to log in.
      Device management users cannot log in directly from a telnet client on the network. Log in as a normal user and then change to a device management user.

```
$ telnet 192.168.0.1↵
login: somebody↵
Password: ↵
(0)NS-2250>
```

The first character of the prompt differs by the type of connection port. When logging in from a device management terminal connected to the CONSOLE port, a "(c)" is displayed. When logging in from a telnet client on the network, a "(0)" is displayed.

The number of the prompt when you have logged in from the telnet client on the network is an open number assigned in order from zero for each connection.

(4)   Change from a normal user to a device management user
      To change from a normal user to a device management user, carry out the "su" command, and then enter the password of a device management user. (With default settings, device management user "root" does not have a password configured.)

```
(c)NS-2250> su↵
Password: ↵
(c)NS-2250#
```

(5)   Log out
      To log out, carry out the "logout" or "exit" command. Also, carry out the "logout" or "exit" command when you want to return to a normal user after using the "su" command to change to a device management user.
      If you log out from a terminal connected to the CONSOLE port, the "NS-2250 login:" prompt is displayed, and the system waits for a login. If you log out from a telnet client on the network, the system returns to the prompt of the client terminal.

After logging out from a terminal connected to the CONSOLE port

```
(c)NS-2250> logout↵        (same for "exit" command)
NS-2250 login:
```

After logging out from telnet client on the network

```
(0)NS-2250> logout↵        (or "exit" command)
$                          (The prompt depends on the client terminal.)
```

(6)   Other setup procedures
      The addition and deletion of users and changing passwords can be carried out by device management users only.
      To add and delete users, use the "create user" and "delete user" commands. To change a password, use the "set user password" command. For details of commands, see the *Command Reference.*

3.2.2 Use the CLI

This section describes how to use the CLI of the NS-2250.

(1)   Command line editing function
       The following table lists the command line editing functions of the CLI.

Edit key	Operation
[Backspace] [Ctrl]+[H]	Deletes one character just before the cursor.
[Delete] [Ctrl]+[D]	Deletes characters at the location of the cursor.
[←] (Left arrow) [Ctrl]+[B]	Moves the cursor one character to the left.
[→] (Right arrow) [Ctrl]+[F]	Moves the cursor one character to the right.
[Ctrl]+[A]	Moves the cursor to the beginning of the command line.
[Ctrl]+[E]	Moves the cursor to the end of the command line.
[Ctrl]+[U]	Deletes all characters.
[Ctrl]+[K]	Deletes the character string after the cursor.
[Ctrl]+[R]	Refreshes all characters.
[Ctrl]+[W]	Deletes the character string before the cursor.

(2)   History function
       The following table lists the history functions of the CLI.

Edit key	Operation
[↑] (Up arrow) [Ctrl]+[P]	Displays the previously registered command.
[↓] (Down arrow) [Ctrl]+[N]	Displays the next registered command.

(3)   Composition help function/completion function
       The following table lists the composition help function/completion function of the CLI.

Edit key	Operation
[Tab]	Show candidates of commands that can be entered (no explanation)
[?]	Show candidates of commands that can be entered (with explanation)
[Ctrl]+[I]	Show candidates of commands that can be entered (no explanation)

(4)   Command abbreviation function

If a single candidate command or a keyword is determined from the partially entered text, the remaining characters can be omitted.

For example, the "show log console" command to display the console log can be abbreviated to "sh log con".

```
(c)NS-2250# show log console↵
Oct  6 12:37:12 port_logd: <TTY1> started
Oct  6 12:37:12 port_logd: <TTY2> started
Oct  6 12:37:14 port_logd: <TTY3> started
Oct  6 12:37:14 port_logd: <TTY4> started
Oct  6 12:37:14 port_logd: <TTY5> started

(c)NS-2250# sh log con↵
Oct  6 12:37:12 port_logd: <TTY1> started
Oct  6 12:37:12 port_logd: <TTY2> started
Oct  6 12:37:14 port_logd: <TTY3> started
Oct  6 12:37:14 port_logd: <TTY4> started
Oct  6 12:37:14 port_logd: <TTY5> started
```

3.2.3 Insert configuration commands

On the NS-2250, you can copy and paste configuration commands created in a text file in advance (insert configuration commands), and then configure the NS-2250. By using this function, you can minimize command entry errors, and carry out configuration work for the NS-2250 efficiently.

To use this function, carry out the "terminal editing disable" command to disable line editing before importing the setting commands. After the insertion is complete, carry out the "terminal editing enable" command to enable line editing. Be aware that while line editing is disabled, you cannot use cursor keys or insert characters at the command line.

```
create ip host term01 192.168.0.101 ⎫
create ip host term02 192.168.0.102 ⎭ Commands to be inserted
```

```
(c)NS-2250# show ip host↵
Hostname        IPaddress                            Port
--------------------------------------------------------------

(c)NS-2250# terminal editing disable↵

 (↓ Insertion of setting commands)
(c)NS-2250# create ip host term01 192.168.0.101
(c)NS-2250# create ip host term09 192.168.0.109

(c)NS-2250# terminal editing enable↵
(c)NS-2250#
(c)NS-2250# show ip host↵
Hostname        IPaddress                            Port
--------------------------------------------------------------
term01          192.168.0.101                        -
term02          192.168.0.102                        -
```

The NS-2250 also supports the transfer of the settings file by FTP/SFTP. For details, see Chapter 5, "Management and maintenance".

> Caution To insert configuration commands on a terminal connected to the CONSOLE port, set the sending delay of the terminal software to about 1 second per line.

> Caution A telnet client cannot set a send delay. As a result, if you insert configuration commands on a telnet client of a client terminal on the network, the configuration may fail. To insert configuration commands on a telnet client, for example, prepare a macro that waits for the receipt of a character string from the NS-2250 after one line is sent.

3.2.4 Save settings

When the settings of the NS-2250 have been changed, the changes are reflected in the running configuration. The running configuration is a file in the internal memory (RAM), so if the NS-2250 is stopped or restarted, the changed settings are discarded. To save the changed settings, carry out the "write" command to save the running configuration to the startup file.

For the startup files of the NS-2250, there are four files each on the USB memory and internal memory of the NS-2250. When the NS-2250 is started, the content of the startup file is imported as the running configuration. There is one running configuration in the internal memory, and it is handled as the configuration of the NS-2250.

When there is a USB memory inserted in the USB port of NS-2250, the default startup file of the USB memory is imported at startup as the running configuration. If there is no USB memory inserted, the default startup file saved in the internal memory of the NS-2250 is imported as the running configuration.

The default startup file is the "startup1" file.
The startup file imported at startup can be changed by carrying out the "default startup" command.
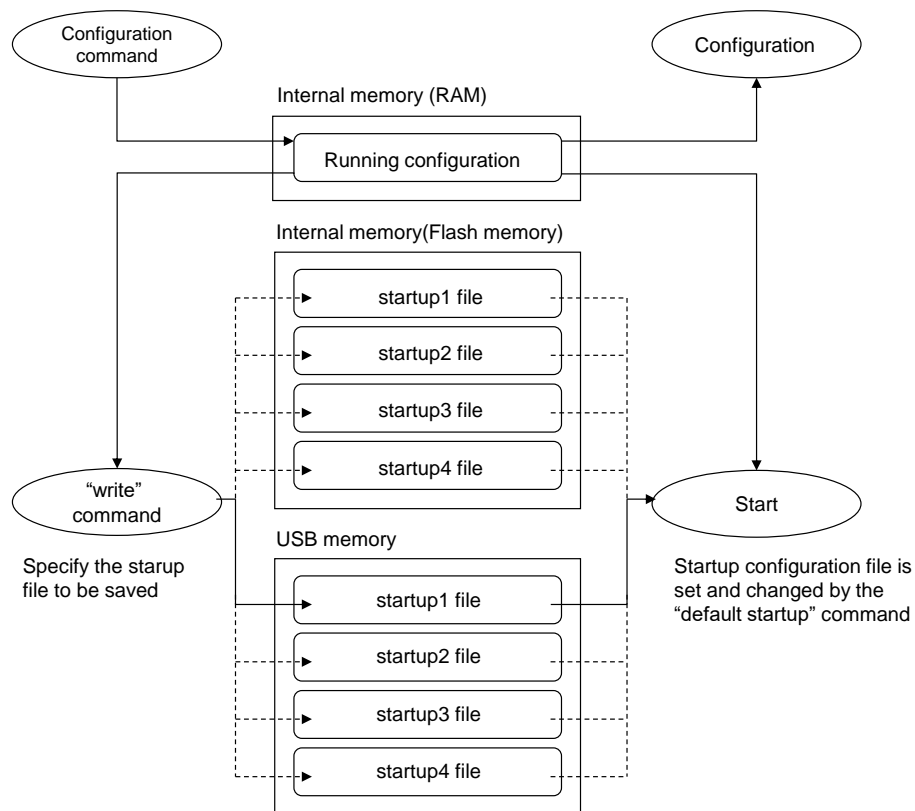
Figure 3-12 Save settings

(1) Save settings normally (when a save destination for settings is not specified)
Carry out the "write" command with no options. If the "write" command is carried out without specifying options, the settings are saved to the startup file that was imported at startup.
If a USB memory is inserted and the NS-2250 is started in a default state, the "startup1" file on the USB memory and internal memory is imported.

```
(c)NS-2250# write↵
Do you really want to write internal & external startup1 [y/n]?y↵
write external startup1
...................writing
write internal startup1
...................writing
(c)NS-2250#
```

(2) Save settings to the "startup2" file of the USB memory
On the SmartCS, carry out the "write" command while specifying "startup 2 external" in the parameters.
On the SmartCSmini, carry out the "write" command while specifying "startup 2" in the parameters.

```
(c)NS-2250# write startup 2 external↵
Do you really want to write external startup2 [y/n] ? y↵
................writing
(c)NS-2250#
```

(3) Save settings to the "startup2" file of the inside the NS-2250
On the SmartCS, carry out the "write" command while specifying "startup 2 internal" in the parameters.
On the SmartCSmini, the startup file is on the USB memory only and cannot be saved inside the NS-2250.

```
(c)NS-2250# write startup 2 internal↵
Do you really want to write internal startup2 [y/n] ? y↵
................writing
(c)NS-2250#
```

3.2.5 Restart the NS-2250

To restart the NS-2250, carry out the "reboot" command.

(1)   Restart normally (when no particular options are specified)
       If the "reboot" command is carried out with no options, the default startup file is imported,
       and the NS-2250 restarts.

```
(c)NS-2250# reboot↵
Do you really want to reboot with main system and startup1 [y/n] y↵
```

(2)   Import settings from the "startup2" file of the USB memory and start the NS-2250
       On the SmartCS, carry out the "reboot" command while specifying "startup 2 external" in
       the parameters.

```
(c)NS-2250# reboot startup 2 external↵
Do you really want to reboot with main system and external startup2 [y/n] y↵
```

(3)   When importing settings of the "startup2 file" inside the NS-2250 and rebooting
       On the SmartCS, carry out the "reboot" command while specifying "startup 2 internal" in the
       parameters. The device is restarted using the settings that have been saved to the "startup
       2 file" inside it.

```
(c)NS-2250# reboot startup 2 internal↵
Do you really want to reboot with main system and internal startup2 [y/n] y↵
```

Chapter 4

Settings

Chapter 4 describes the settings of the functions of the NS-2250.

Read this chapter before starting work.

4.1 Configure the network

4.1.1 Change the host name or IP address of the NS-2250

The default host name of the NS-2250 is "NS-2250".
To change the host name, carry out the "set hostname" command.
In the host name, you can use half-width alphanumeric characters, underbars "_", hyphens "-", and periods ".". Note that the first and last characters of the character string must be alphanumeric characters. Furthermore, a hyphen, period, or underbar cannot be used after a period. The maximum number of characters for a host name is 64.

```
(c)NS-2250# set hostname SmartCS↵
(c)SmartCS#
```

The default IP address of the NS-2250 is "192.168.0.1/24" ("/24" means 24bit nemask). To change the IP address, carry out the "set ipaddr" command.

```
(c)NS-2250# set ipaddr eth1 192.168.0.100/24↵
(c)NS-2250#
```

To set the IPv6 address, carry out the "set ip6addr" command.
After enabling IPv6 communication function by the "create ip6" command, carry out the "set ip6addr" command.
The default value is "disable", and IPv6 address is not set.

```
(c)NS-2250# create ip6↵
(c)NS-2250#
(c)NS-2250# set ip6addr eth1 2001:db8::1/64↵
(c)NS-2250#
```

When using 2 LAN ports, either IP address of a subnet different from both of LAN1 and LAN2 is defined, or bonding function is enabled to bond 2 LAN port as 1 virtual port.

- to use 2 LAN port in different IP subnet
```
(c)NS-2250# set ipaddr eth1 192.168.0.100/24↵
(c)NS-2250# set ipaddr eth2 192.168.1.100/24↵
(c)NS-2250#
```

- to use 2 LAN port in same IP subnet (enabling bonding function)
```
(c)NS-2250# enable bonding↵
(c)NS-2250# set ipaddr bond1 192.168.0.100/24↵
(c)NS-2250#
```

To disable the bonding function, carry out the "disable bonding" command.

Caution   When the bonding function is enabled, the setting of IP address and routing at

eth1 is automatically inherited to bond1, and the configuration of IP address/routing at eth1/eth2 is deleted.

When the bonding function is disabled, the setting of IP address/routing at bond1 is inherited to eth1 as well.

You can check the host name, IP address, and other information of the NS-2250 by using the "show ip" command.

- When the bonding function is disabled.

```
(c)NS-2250# show ip↵
Hostname        : SmartCS
TcpKeepAlive    : 180
IPaddress(eth1) : 192.168.0.100/24
IPaddress(eth2) : 192.168.1.100/24
(c)NS-2250#
```

- When the bonding function is enabled.

```
(c)NS-2250# show ip↵
Hostname        : SmartCS
TcpKeepAlive    : 180
IPaddress(eth1)  : -
IPaddress(eth2)  : -
IPaddress(bond1) :192.168.0.100/24
(c)NS-2250#
```

You can check the IPv6 address of the NS-2250 by using the "show ip6" command.

- When the bonding function is disabled.

```
(c)NS-2250# show ip6↵
IPaddress(eth1) : 2001:db8::2/64
IPaddress(eth2) : 2001:db9::2/64
(c)NS-2250#
```

- When the bonding function is enabled.

```
(c)NS-2250# show ip6↵
IPaddress(eth1) : ---
IPaddress(eth2) : ---
IPaddress(bond1): 2001:db8::2/64
(c)NS-2250#
```

You can check the IPv4 address, the IPv6 address(including link local address), the value of MTU, and the state of the link of the NS-2250 by using the "show ipinterface" command.

- When the bonding function is disabled.

```
(c)NS-2250# show ipinterface↵
ifname  state mtu   attr    address/mask
-------------------------------------------------------------------
lo      up    65536 static  127.0.0.1/8
                    static  ::1/128
eth1    up    1500  static  2001:db8::2/64
                    link    fe80::a00:83ff:feff:dede/64
eth2    up    1500  static  192.168.0.1/24
                    link    fe80::a00:83ff:feff:dedf/64
(c)NS-2250#
```

- When the bonding function is enabled.

```
(c)NS-2250# show ipinterface↵
ifname  state mtu   attr    address/mask
-------------------------------------------------------------------
lo      up    65536 static  127.0.0.1/8
                    static  ::1/128
eth1    up    1500  -       ---
eth2    up    1500  -       ---
bond1   up    1500  static  2001:db8::2/64
                    link    fe80::a00:83ff:feff:dede/64
(c)NS-2250#
```

Status of bonding function can be checked by the following command.

```
(c)NS-2250# show bonding↵
 <bonding information>
   Status           : enable
   Mode             : active-backup

 <master bond1 information>
   Status           : up
   Up Delay Time(sec) : off
   Last change time  : Fri Apr 25 13:04:51 JST 2016
   <slave information>
     interface  active status    failure_count
     ------------------------------------------
     eth1        *      up                   0
     eth2               up                   0
(c)NS-2250#
```

An active port can be switched by the following command.

```
(c)NS-2250# switch bonding eth2↵
 Fri Apr 25 13:30:21 bonding: bond1 Switch succeeded (eth2 selected.)
(c)NS-2250#
```

4.1.2 Configure the static routing function

To configure the static route, carry out the "create ip route" command.

```
(c)NS-2250# create ip route default gateway 192.168.0.254↵
(c)NS-2250#
```

To configure the static route and default routing, carry out the "create ip route" command.

```
(c)NS-2250# create ip route 172.16.1.0/24 gateway 192.168.0.2↵
(c)NS-2250# create ip route default gateway 192.168.0.254↵
(c)NS-2250#
```

When using 2 LAN ports by redundant composition, metrics (range: 0-100) is set as a route. Metrics of default is 0(high priority). The route is switched by a link down in a LAN port.

```
(c)NS-2250# create ip route default gateway 192.168.0.254↵
(c)NS-2250# create ip route default gateway 192.168.1.254 metric 100↵
(c)NS-2250#
```

To configure the static route, carry out the "create ip6route" command.
In the following example,define the static route 2001:dba::/64 to LAN1(2001:db8::2) and the default route to LAN2(2001:db9::2).

```
(c)NS-2250# create ip6route 2001:dba::/64 gateway 2001:db8::ffff↵
(c)NS-2250# create ip6route default gateway 2001:db9::ffff↵
(c)NS-2250#
```

To define the metric, specify the metric option in the "create ip6route" command as with IPv4.

```
(c)NS-2250# create ip6route default gateway 2001:db8::ffff ↵
(c)NS-2250# create ip6route default gateway 2001:db9::ffff metric 100↵
(c)NS-2250#
```

You can check the routing table information by using the "show ip route" command.

- When the bonding function is disabled.

```
(c)NS-2250# show ip route↵
destination     netmask        gateway        met   iface status
-----------------------------------------------------------------
192.168.0.0     255.255.255.0 ---                 0   eth1  -
192.168.1.0     255.255.255.0 ---                 0   eth2  -
172.16.1.0      255.255.255.0 192.168.0.254   0   eth1  -
0.0.0.0         0.0.0.0        192.168.1.254   0   eth2  -
(c)NS-2250#
```

- When the bonding function is enabled.

```
(c)NS-2250# show ip route↵
destination     netmask        gateway        met   iface status
-----------------------------------------------------------------
192.168.0.0     255.255.255.0 ---                 0   bond1 -
0.0.0.0         0.0.0.0        192.168.0.254   0   bond1 -
(c)NS-2250#
```

You can check the routing table information of IPv6 by using the "show ip6route" command.

- When the bonding function is disabled.

```
(c)NS-2250# show ip6route↵
destination         gateway              met   iface status
------------------------------------------------------------------------
2001:db8::/64       ---                      0    eth1 -
2001:db9::/64       ---0eth2-
::/0                2001:db8::ffff        0    eth1 inact
::/0                2001:db9::ffff        100   eth2 inact
(c)NS-2250#
```

- When the bonding function is enabled.

```
(c)NS-2250# show ip6route↵
destination         gateway              met   iface status
------------------------------------------------------------------------
2001:db8::/64       ---                      0   bond1 -
::/0                2001:db8::ffff        0   bond1 inact
(c)NS-2250#
```

4.1.3 Configure the DNS client

To configure the DNS client, carry out the "set dns" command and "set dns localdomain" command.

```
(c)NS-2250# set dns 1 192.168.0.21↵
(c)NS-2250# set dns localdomain example.co.jp↵
(c)NS-2250#
```

You can check the DNS client information by using the "show dns" command.

```
(c)NS-2250# show dns↵
Local Domain:example.co.jp

No.  DNS Server
-------------------
1    192.168.0.21
2    -
(c)NS-2250#
```

In the case of IPv6 network, configure the DNS client as with IPv4.

```
(c)NS-2250# set dns 1 2001:db8::12↵
(c)NS-2250# set dns localdomain example.co.jp↵
(c)NS-2250#
```

```
(c)NS-2250# show dns↵
Local Domain:example.co.jp

No.  DNS Server
-------------------
1    2001:db8::12
2    -
(c)NS-2250#
```

Caution   If the DNS client is configured, performance may drop depending on the status of the DNS server. In environments in which port log transfers are frequent, we recommend specifying and configuring the IP address and not resolving the names of the servers (mail, FTP, and syslog) using the DNS server.

4.2   Configure the CONSOLE port

The following table shows the configured values for the CONSOLE port of the NS-2250 at the default settings.

Item	Default value
Transfer speed	9600 bps
Data length	8 bit
Parity	None
Stop bit	1 bit
Flow control	XON/XOFF

To change the CONSOLE port settings, carry out the "set console" command.

```
(c)NS-2250# set console baud 115200↵
(c)NS-2250# set console bitchar 7↵
(c)NS-2250# set console parity even↵
(c)NS-2250# set console stop 2↵
(c)NS-2250# set console flow none↵
(c)NS-2250#
```

If you change the settings of the CONSOLE port of the NS-2250, the "(c)NS-2250#" prompt may no longer display normally because the settings do not match with the settings of the serial port of the device management terminal. After matching the settings of the CONSOLE port of the NS-2250 with settings of the serial port of the device management terminal, press the Enter key, and then confirm that the prompt is displayed correctly.

To change the CONSOLE port information, carry out the "show console" command.

```
(c)NS-2250# show console↵
Baud      : 115200
BitChar   : 7
Parity    : even
Stop      : 2
Flow      : none
Syslog    : on
(c)NS-2250#
```

4.3   Configure the serial ports

The following table shows the configured values for all serial ports of the NS-2250 at the default settings.

Item	Default value
Transfer speed	9600 bps
Data length	8 bit
Parity	None
Stop bit	1 bit
Flow control	NONE
DSR signal detection function	ON

To change the serial port settings, carry out the "set tty" command.

```
(c)NS-2250# set tty 1-16 baud 9600↵
(c)NS-2250# set tty 1-16 bitchar 8↵
(c)NS-2250# set tty 1-16 parity none↵
(c)NS-2250# set tty 1-16 stop 1↵
(c)NS-2250# set tty 1-16 flow none↵
(c)NS-2250# set tty 1-16 detect_dsr off↵

(c)NS-2250# set tty 32 baud 115200↵
(c)NS-2250# set tty 32 bitchar 7↵
(c)NS-2250# set tty 32 parity even↵
(c)NS-2250# set tty 32 stop 2↵
(c)NS-2250# set tty 32 flow xon↵
(c)NS-2250# set tty 32 detect_dsr on↵
(c)NS-2250#
```

You can check the serial port information by using the "show tty" command.

```
(c)NS-2250# show tty 1↵
tty : 1
    baud        : 9600
    bitchar     : 8
    parity      : none
    stop        : 1
    flow        : none
    drhup       : off
    detect_dsr  : on (edge)
(c)NS-2250#
```

```
(c)NS-2250# show tty↵
        ----------base---------- -dsr-
tty     baud bc parity st flow   dct
-------------------------------------
  1     9600 8   none  1  none   off
  2     9600 8   none  1  none   off
  3     9600 8   none  1  none   off
  4     9600 8   none  1  none   off
  5     9600 8   none  1  none   off
  6     9600 8   none  1  none   off
  7     9600 8   none  1  none   off
  8     9600 8   none  1  none   off
    : (omitted)
(c)NS-2250#
```

4.4 Configure the port server

4.4.1 Configure the connection modes (Direct mode/Select mode)

At the default settings, the connection mode of the port server is configured to Direct mode. If you want to use the port selection menu, carry out the "set portd connect select" command.

```
(c)NS-2250# set portd connect select↵
(c)NS-2250#
```

If you want to use the Direct mode of the port server, carry out the "set portd connect direct" command. Because Direct mode is the default setting, carry out the following commands when you want to change the connection mode from Select mode to Direct mode.

```
(c)NS-2250# set portd connect direct↵
(c)NS-2250#
```

Notes

To use Select mode, you must enable the Port user authentication function, and then register port users. Also, it is easier to configure the labeling of serial ports and session suspension character codes for the port server menu in Select mode. To use Select mode, configure the "set portd auth basic", "set portd tty label", and "set portd tty cmdchar" commands.

```
(c)NS-2250# set portd auth basic↵
(c)NS-2250# set portd tty 1 cmdchar 01↵
(c)NS-2250# set portd tty 1 label Osaka-L3SW-1↵
(c)NS-2250# create user port01usr group portusr password↵
New password: ↵
Retype new password: ↵
(c)NS-2250# set user port01usr port 1-32↵
(c)NS-2250#
```

4.4.2 Show the port server menu

The port server menu display setting is configured by the "set portd menu" command.
There are three settings for the display of the port server menu: Auto, show, and hide. This display is dependent on the port log setting that determines whether port logs are saved. The following table shows the relationship between the settings.

Port log save the setting of the entire NS-2250 (set logd output)	Port log save the setting for tty port (set logd tty log)	Port server menu setting (set portd menu)		
		Auto (default)	on	off
flash/ram (default)	on (default)	○ (show)	○ (show)	- (hide)
	off	- (hide)	○ (show)	- (hide)
off	off	- (hide)	○ (show)	- (hide)

As the table shows, the display method for the port server menu at the default settings of the NS-2250 is "Auto". Furthermore, because the save setting for the port log of the tty port is on, when you use the default settings, the port server menu is displayed automatically.

To display the port server menu regardless of port log saving, configure "set portd menu on" command.

```
(c)NS-2250# set portd menu on↵
(c)NS-2250#
```

To hide the port server menu regardless of port log saving, configure "set portd menu off" command.

```
(c)NS-2250# set portd menu off↵
(c)NS-2250#
```

To automatically determine the display of port server menu, carry out the "set portd menu auto" command.

```
(c)NS-2250# set portd menu auto↵
(c)NS-2250#
```

4.4.3 User authentication of the port server (port user authentication)

Port user authentication runs when a telnet client accesses the port server of the NS-2250. The default setting is "No authentication" To switch on port user authentication, carry out the "set portd auth" command.
If the port user authentication is set to on, the port user authentication function operates for all serial ports of the NS-2250.

```
(c)NS-2250# set portd auth basic↵
(c)NS-2250#
```

To use an SSH client, see Section 4.6.6, "Configure the SSH server".

4.4.4 Access control of the port server (connection protocol and connection mode)

Access control of the port server at the default settings (communication protocol and communication mode) allows telnet/SSH Normal mode (RW) only.
To change access control of the port server so you can use both telnet/SSH Normal mode and Monitoring mode (RO), carry out the following commands.

```
(c)NS-2250# set portd tty 1-32 session telnet both↵
(c)NS-2250# set portd tty 1-32 session ssh both↵
or
(c)NS-2250# set portd tty 1-32 session both both↵
(c)NS-2250#
```

To disable SSH transparent connection (sshxpt), specify only communication protocol and communication mode which are currently set and do not add sshxpt option in the end of the command

```
(0)NS-2250# set portd tty 1-32 session both both↵
```

4.4.5 Connect multiple sessions of the port server

The function was extended to allow up to two connections in Normal mode and three connections in Monitoring mode for a single serial port.
However, it's not able to connect by Normal mode to the serial port which is communicating by tty manage function.
To increase the number of sessions that can be connected, carry out the following commands.

```
(c)NS-2250# set portd tty 1-32 limit rw 2 ro 3↵
(c)NS-2250#
```

4.4.6 Change the TCP port number of the port server (Direct mode)

You can change the TCP port number of telnet/SSH Normal mode and Monitoring mode running at each serial port by using the "set portd telrw/telro/sshrw/sshro" commands. To change the service port number of telnet/SSH Normal mode and Monitoring mode, set an unused port number in the range from 1,025 through 65,000.

```
(c)NS-2250# set portd telrw 10001↵
(c)NS-2250# set portd telro 11001↵
(c)NS-2250# set portd sshrw 12001↵
(c)NS-2250# set portd sshro 13001↵
(c)NS-2250#
```

You can check the TCP port numbers of the port server by using the "show portd" command.

```
(c)NS-2250# show portd↵
portd status   : enable
auth status    : none
connect status : direct
base port number
          telnet    rw :  8101  ro :  8201
          ssh       rw :  8301  ro :  8401
timeout status
          idle_timeout : on  (  60min)
          ro_timeout   : on  ( 120min)
menu status    : auto
----------------------------------------------------------------
tty Label                      Listen Port              TimeOut
                               telrw  telro sshrw sshro idle  ro
----------------------------------------------------------------
  1 L3SW-1                     8101   8201  8301  8401   60  120
  2 L3SW-2                     8102   8202  8302  8402   60  120
  3 Server1                    8103   8203  8303  8403   60  120
  4                            8104   8204  8304  8404   60  120
  5                            8105   8205  8305  8405   60  120
       : (omitted)
 31                            8131   8231  8331  8431   60  120
 32                            8132   8232  8332  8432   60  120
(c)NS-2250#
```

4.4.7 Change the reception port number for SSH transparent connection (sshxpt)

The port numbers for SSH transparent connection of each serial port can be changed by set portd sshxpt command. Choose the vacant port numbers from 1025-65000.

```
(c)NS-2250# set portd sshxpt 20001↵
```

4.4.8 Add a port user

To add a port user, carry out the "create user" command.
Because you must configure the serial ports to which a port user can access, use the "port" option of the "create user" command or the "set user port" command to configure the serial ports that can be accessed.

In the following example, a port user "port01usr" is created who can access serial port 1 through 8 and serial port 17 for a total of 9 ports.

```
(c)NS-2250# create user port01usr group portusr port 1-8,17
Password ↵
New password: ↵
Retype new password: ↵
```

You can make the same settings by using the following commands.

```
(c)NS-2250# create user port01usr group portusr password↵
New password: ↵
Retype new password: ↵
(c)NS-2250# set user port01usr port 1-8,17↵
```

You can check the port user list and attributes by using the "show user" command.

```
(c)NS-2250# show user↵
User-Name       Category(Uid)    Public-Key   Port-Access-List
---------------------------------------------------------------
root            root(0)
setup           setup(198)
verup           verup(199)
log             log(200)
somebody        normal(100)
portusr         portusr(500)                  1-32
port01usr       portusr(501)                  1-8,17
(c)NS-2250#
```

4.4.9 Configure the labeling of serial ports

You can set a device name or other label to a serial port so that you can identify the monitored equipment connected to the serial port. Up to 32 characters can be used for labels.

In the label, you can use half-width alphanumeric characters, underbars "_", hyphens "-", periods ".", and at marks "@" and spaces " ".

Specify the label within double quotation marks if space characters " " are included.

```
(c)NS-2250# set portd tty 1 label DB-server↵
(c)NS-2250# set portd tty 2 label "Tokyo L3SW 1"↵
(c)NS-2250#
```

The label configured for a serial port is shown by the port server Select mode (port select menu), the "show port" command, the "show portd session" command, and so on.

```
(c)NS-2250# show portd session↵
telnet  rw : 3   ro : 0
ssh     rw : 0   ro : 0
available session (telnet only : 93 / ssh only : 93)
 -----------------------------------------------------------------------
 tty   : Label                              Session-Limit
    Type Login-User       Local      Remote
 -----------------------------------------------------------------------
 tty  1 : DB-server                             RW: 2 / RO: 3
    rw 1 port01usr       tel:23     192.168.30.145: 4731
    rw 2 port02usr       tel:23     192.168.30.146: 3495

 tty  2 : L3SW No.08                            RW: 2 / RO: 3
    rw 1 port03usr       tel:4740   2001:dba::2.4740
(c)NS-2250#
```

4.4.10 Configure the automatic session disconnection function of the port server

The NS-2250 is equipped with two automatic session disconnection functions: one that operates according to an idle timer (idle monitoring time) and one that operates according to a session timer (continuous connection time).
To enable this function, carry out the following commands.

When the idle timer (idle_timeout) has been configured, the session is forcibly disconnected if an idle state (no entered data is coming from a telnet/SSH terminal) of the configured time is detected when the Select menu or port server menu is displayed or during a Normal mode (RW) connection with the serial port. The setting range for the idle timer is from 1 through 60 minutes, and the default setting is off.

The disconnection of the session occurs in stages.
(Example)
　　After the idle timer has expired, access to the serial port is ended, and then the port server menu is displayed.
　　↓
　　After the idle timer has expired, the port server menu is closed, and then the Select menu is displayed
　　↓
　　After the idle timer has expired, the Select menu is closed, and then the session is disconnected.

When the session timer (ro_timeout) has been configured, the session is forcibly disconnected if the specified time passes after connecting from a telnet/SSH terminal to a serial port in Monitoring mode (RO). The setting range for the idle timer is 1 to 1,440 minutes, and the default setting is off.

```
(c)NS-2250# set portd idle_timeout on 30↵
(c)NS-2250# set portd ro_timeout on 180
(c)NS-2250# set portd tty 1-32_timeout on
(c)NS-2250#
```

4.4.11 Configure other port server functions

(1)　Change Break signal processing
　　The NS-2250 can transmit a Break signal to monitored equipment connected to a serial port when a Break request arrives from a telnet/SSH client. The default setting is off. When the setting is "brk_char none", a Break signal is not sent to the serial port even, when a Break signal is sent from a terminal or the "10: send a break to tty" command is carried out from the Port menu.
　　To configure this function to serial port 1 through 16 and serial port 32, carry out the following commands.

```
(c)NS-2250# configure↵
(c)NS-2250# set portd tty 1-16 brk_char brk↵
(c)NS-2250# set portd tty 32 brk_char brk↵
(c)NS-2250#
```

(2) Change line feed code
     The NS-2250 can convert line feed code received from a telnet client and send it to a serial
     port. For line feed code conversion, select from "No conversion", "Convert CR+LF to CR",
     or "Convert CR+LF to LF". The default setting is "Convert CR+LF to CR".
     To change the line feed code (CR+LF) to "LF", carry out the following commands.

```
(c)NS-2250# set portd tty 1-16 nl lf↵
(c)NS-2250#
```

(3) Change the session suspension character code for the port server menu
     To display the port server menu after accessing monitored equipment,
     configure the session suspension character code of the port server menu.
     The following table shows the character codes that can be registered. The character
     assigned to the code may differ from the character in the table below depending on the
     terminal software you use.

Code	Session suspension character	Code	Session suspension character
00	[Ctrl-@]	10	[Ctrl-P]
01	[Ctrl-A]	11	[Ctrl-Q]
02	[Ctrl-B]	12	[Ctrl-R]
03	[Ctrl-C]	13	[Ctrl-S]
04	[Ctrl-D]	14	[Ctrl-T]
05	[Ctrl-E]	15	[Ctrl-U]
06	[Ctrl-F]	16	[Ctrl-V]
07	[Ctrl-G]	17	[Ctrl-W]
08	[Ctrl-H]	18	[Ctrl-X]
09	[Ctrl-I]	19	[Ctrl-Y]
0a	[Ctrl-J]	1a	[Ctrl-Z]
0b	[Ctrl-K]	1b	[Ctrl-[]
0c	[Ctrl-L]	1c	[Ctrl-/]
0d	[Ctrl-M]	1d	[Ctrl-]]
0e	[Ctrl-N]	1e	[Ctrl-^]
0f	[Ctrl-O]	1f	[Ctrl-_]

You can configure the session suspension character code of the port server menu by carrying out the "set portd tty cmdchar" command. To configure the session suspension character code for the port server menu to "0 x 01" (Ctrl+A), carry out the following command.

```
(c)NS-2250# set portd tty 1-16 cmdchar 01↵
(c)NS-2250# set portd tty 32 cmdchar 01↵
(c)NS-2250#
```

You can check the configuration information of the port server by using the "show portd tty" command.

```
(c)NS-2250# show portd tty↵
tty label                       rw  ro session mode to  brk  nl  cmd
--------------------------------------------------------------
  1 L3SW-1                        2   3 both     both off none cr  1
  2 L3SW-2                        2   3 both     rw   off none cr  1
       : (omitted)
(c)NS-2250#
```

4.5   Configure port logs

4.5.1 Enable and disable port log functions

(1)   Enable port log functions
        At the default settings, the port log functions run using the following configuration.

        Port log save location   : RAM (selectable from RAM, FLASH, and off)
        Port log setting of serial ports   : On for all serial ports
        Port log size for serial ports   : 500 Kbyte (default setting when RAM is set)

The port log functions of the NS-2250 run automatically if either RAM or FLASH is selected for the storage location of port logs, and the settings are configured to save the logs of each serial port. The default status of the port log functions is the same as when the following commands have been carried out.

```
(c)NS-2250# set logd output ram↵
(c)NS-2250# set logd tty 1-32 log on size 500↵
(c)NS-2250#
```

You can change the location for port logs from RAM to a FLASH memory. If you change the storage location for port logs to a FLASH memory, you can save more port logs than when RAM is set. For the port log size and configuration method, see Section 2.2.2, "Port log save function" and Section 4.5.2, "Configure port log size"

```
(c)NS-2250# set logd output flash↵
(c)NS-2250#
```

(2)   Disable port log functions
        There are two methods to disable the port log functions: set the entire NS-2250 to off or set individual serial ports to off. If the port log functions are set to off, the display of the port server menu is restricted as long as the "set portd menu on" command is not carried out. For details, see Section 4.4.2, "Show the port server menu".

        To set the port log function to off for the entire NS-2250, carry out the following commands. If these commands are carried out, the settings for all serial ports are switched off, even when the port log function is set to on for individual serial ports.

```
(c)NS-2250# set logd output off↵
(c)NS-2250#
```

To set the port log function to off for individual serial ports, carry out the "set logd tty log" command.

```
(c)NS-2250# set logd tty 1-32 log off↵
(c)NS-2250#
```

Caution   If the port log function is changed from off to on for the entire device, the port log function is switched to on for all serial ports, and the setting is reflected in the running configuration automatically.

4.5.2 Configure port log size

To change the port log size, carry out the "set logd tty log" command.
For the maximum amount of free space in which port logs can be saved on the NS-2250, the configuration range of port log size for each serial port, and the default setting values, see Section 2.2, "Port log functions".
To change the port log size for serial port 1 through 8 and serial port 32 to 1 MB and 2 MB respectively, carry out the following command.

```
(c)NS-2250# set logd tty 1-8 log on size 1000↵
(c)NS-2250# set logd tty 32 log on size 2000↵
(c)NS-2250#
```

4.5.3 Configure time stamps

To set the port log time stamp function to on, carry out the "set logd tstamp" command. The time stamp interval can be configured from 3 seconds through 65,535 seconds. Note that the default Time stamp function setting is off, and when the time stamp setting is changed to on, the default time stamp interval is 60 seconds.
To change the time stamp interval to 300 seconds, carry out the following commands.

```
(c)NS-2250# set logd tstamp on interval 300↵
(c)NS-2250#
```

4.5.4 Configure login stamps

To set the port log login stamp function to on, carry out the "set logd lstamp" command. If the login stamp function is set to on, the login and logout times of a user who accessed the serial port are added to the port log.
The default setting of the login stamp function is off.
To enable the login stamp for serial port 1, carry out the following commands.

```
(c)NS-2250# set logd tty 1 lstamp on↵
(c)NS-2250#
```

The following box shows examples of login stamps.

```
<Web Jun 24 13:00:26 JST 2015 login  RW1:userA 10.1.1.1>

<Web Jun 24 13:05:30 JST 2015 logout RW1:userA 10.1.1.1>
```

The login and logout times of a user who accessed serial ports by tty manage function are not added to the port log.

4.5.5 Configure email sending

To email for port logs periodically, carry out the "add logd tty mail" command and the "set logd tty sendlog" command. To send the port log of serial port 1 to "mgr@example.co.jp" of a mail server (192.168.1.1) at a 60-minute interval or when the port log reaches 80% capacity, carry out the following commands.

```
(c)NS-2250# add logd tty 1 mail 1 mgr@example.co.jp 192.168.1.1↵
(c)NS-2250# set logd tty 1 sendlog mail ratio 80↵
(c)NS-2250# set logd tty 1 sendlog mail interval 60↵
(c)NS-2250#
```

The following table shows the default settings for mail to be sent.

Subject	: portlog TTY_number
Email address of sender	: portuser@NS-2250 host name.local domain
Port logs	: Attachment file format
SMTP-Auth function	: OFF

To set the subject to "Data-Center L3SW", the email address of the sender to "smartcs@example.co.jp", and store the port log in the mail body for mail to be sent, carry out the following commands.

```
(c)NS-2250# add logd tty 1 mail 1 subject "Data-Center L3SW"↵
(c)NS-2250# set logd tty 1 mail 1 sender smartcs@example.co.jp↵
(c)NS-2250# set logd tty 1 mail 1 type body↵
(c)NS-2250#
```

If the settings are configured to store the port log as an attachment file (when the "set logd tty mail type attachment" command has been configured), the port log is attached with a file name including the serial port number and date information. (Example file name: "NS2250TTY01_20150807152011.log".)

To send e-mail to a mail server that requires the SMTP-Auth function, carry out the following command to configure the user name ("mailuser" in the following example) and password.

```
(c)NS-2250# set logd tty 1 mail 1 auth mailuser password↵
SMTP-Auth password ↵
Retype SMTP-Auth password ↵
(c)NS-2250#
```

Caution   In environments in which port log transfers are frequent, we recommend specifying and configuring the IP address directly and not resolving the name of the mail server using the DNS server.

4.5.6 Configure FTP sending

To send port logs by FTP periodically, carry out the "add logd tty ftp" command and the "set logd tty sendlog" command. To send the port log of serial port 5 to the FTP server (192.168.1.1) as user "loguser2" at a 60-minute interval or when the port log reaches 80% capacity, carry out the following commands.

```
(c)NS-2250# add logd tty 5 ftp 1 loguser2 192.168.1.1 password↵
FTP password ↵
Retype FTP password ↵
(c)NS-2250# set logd tty 5 sendlog ftp ratio 80↵
(c)NS-2250# set logd tty 5 sendlog ftp interval 60↵
(c)NS-2250#
```

The port log is saved with a file name including the serial port number and date information to the home directory of the user of the specified FTP server. (Example file name: "NS2250TTY02_20150807175530.log".)

Caution   In environments in which port log transfers are frequent, we recommend specifying and configuring the IP address directly and not resolving the name of the FTP server using the DNS server.

4.5.7 Configure syslog sending

To send port logs to the syslog server, carry out the "set logd tty syslog" command.
With syslog sending, if the port logs that should be sent arrive, they are sent to the syslog server immediately.
To send the port logs of serial port 1 through serial port 16 and serial port 32 to the syslog server, carry out the following commands.

```
(c)NS-2250# set logd tty 1-16 syslog on↵
(c)NS-2250# set logd tty 32 syslog on↵
(c)NS-2250# set syslog host 1 10.1.1.1 portlog_facility local0
syslog_facility local1 ↵
(c)NS-2250# enable syslog↵
(c)NS-2250#
```

To change the syslog transfer format of the port logs, carry out the following command.
You can add the NS-2250 host name or a time stamp and change TTY number to the label name. You can also combine multiple parameters when configuring this setting.

```
(c)NS-2250# set logd tty 1 syslog format hostname on↵
(c)NS-2250# set logd tty 1 syslog format tstamp on↵
(c)NS-2250# set logd tty 1 syslog format label on↵
```

Display example for syslog server

```
(Default setting)
Dec 10 10:45:40 port_logd: <TTY01> ether(3) :UP

(When "hostname on" is set)
Dec 10 10:45:40 NS-2250 port_logd: <TTY01> ether(3) :UP

(When "tstamp on" is set)
Dec 10 10:45:40 Dec 10 10:45:35  port_logd: <TTY01> ether(3) :UP

(When "label on" is set)
Dec 10 10:45:40 port_logd: <Tokyo-Switch-1> ether(3) :UP
```

You can check the syslog setting by using the "show syslog" command.

```
(c)NS-2250# show syslog↵

Syslog Status:enable

No. Syslog Host                    Portlog-Facility Syslog-Facility

----------------------------------------------------------------

1   10.1.1.1                       local0          local1
(c)NS-2250#
```

To configure the syslog server, see Section 4.7.3, "Configure the syslog client".

Caution   In environments in which port log transfers are frequent, we recommend specifying and configuring the IP address directly and not resolving the name of the syslog server using the DNS server.

4.5.8 Configure NFS sending

To save port logs to an NFS server, carry out the "set logd tty nfs" command.
If data is received from monitored equipment, port logs are saved to the NFS server immediately.
To save the port logs of serial port 1 through serial port 16 and serial port 32 to the NFS server, carry out the following command.
Logs saved to the NFS server can be rotated as well. With the following settings, the log file is rotated at midnight on the first of each month.

```
(c)NS-2250# set logd tty 1-16 nfs on↵
(c)NS-2250# set logd tty 32 nfs on↵
(c)NS-2250# set nfs server 1 10.1.1.1 path /mnt/nfslog↵
(c)NS-2250# set nfs rotate on 0 0 1 * *↵
(c)NS-2250# enable nfs↵
(c)NS-2250#
```

You can check the NFS setting by using the "show nfs" command.

```
(c)NS-2250# show nfs↵
<NFS information>
 Status          : enable
 Rotate          : on
  Minute         : 0
  Hour           : 0
  Day            : 1
  Month          : *
  Day of the week : *


 <NFS server 1>
 IP address      : 10.1.1.1
 Path            : /mnt/nfslog
 Protocol        : udp
 Mount status    : mount
   (---)


 <NFS server 2>
   : (omitted)
(c)NS-2250#
```

4.5.9 Check port log settings

You can check the configuration information of port logs by using the "show logd" command.

```
(c)NS-2250# show logd↵
Log stored in  : FLASH
Total Log Size : 144000 KB (Free 0 KB / Total 144000 KB)
Timestamp      : off, Interval Time : 60 sec


(c)NS-2250# show logd tty 1↵
tty : 1
   Log :  on, size : 1000 KB
   Syslog output    : on
        Timestamp   : off
        Hostname    : off
        Label       : on
   NFS output       : on
   loginstamp       : off
   Trigger : Interval : 60 min
             Ratio    : 80 %
   SendLog : mail
   FTP server(1)   : -
      Auth account : -
   FTP server(2)   : -
      Auth account : -
   SMTP server(1)  : 192.168.1.1
      Auth account : -
      Mail addr    : user1@example.co.jp
      From addr    : portuser@NS-2250 (default)
      Subject      : "portlog tty_1" (default)
      Type         : attachment
   SMTP server(2)  : 192.168.1.1
      Auth account : user2
      Mail addr    : user2@example.co.jp
      From addr    : portuser@NS-2250 (default)
      Subject      : "portlog tty_1" (default)
      Type         : attachment
(c)NS-2250#
```

4.6   Configure security settings

4.6.1 Register and delete users

On the NS-2250, you can add and delete users per objectives.
To register a normal user (user1) and port user (port1) to the NS-2250, carry out the "create user" command. For details of the "create user" command, see the *Command Reference*.

```
(c)NS-2250# create user user1 group normal password↵
New password: ↵
Retype new password: ↵


(c)NS-2250# create user port1 group portusr port 1-16 password↵
New password: ↵
Retype new password: ↵

```

To delete a normal user (user1) and port user (port1) from the NS-2250, carry out the "delete user" command.

```
(c)NS-2250# delete user user1↵
(c)NS-2250# delete user port1↵
(c)NS-2250#
```

You can check a list of users registered to the NS-2250 by using the "show user" command.

```
(c)NS-2250# show user↵
 User-Name       Category(Uid)   Public-Key   Port-Access-List
 ----------------------------------------------------------------
 root            root(0)
 setup           setup(198)
 verup           verup(199)
 log             log(200)
 somebody        normal(100)
 portusr         portusr(500)                 1-32
 port01usr       portusr(501)                 1-32
 (c)NS-2250#
```

For details about user information (functions, user IDs, and group names), see Section 2.3.1, "User management/authentication function".

4.6.2 Configure user passwords

Users registered by default do not have passwords configured. To configure a password, use the "set user password" command as shown below.
Use the same command when changing a password.

```
(c)NS-2250# set user root password↵
New password: ↵
Retype new password: ↵

(c)NS-2250# set user somebody password↵
New password: ↵
Retype new password: ↵

(c)NS-2250# set user log password↵
New password: ↵
Retype new password: ↵

(c)NS-2250# set user verup password↵
New password: ↵
Retype new password: ↵

(c)NS-2250#
```

Device management users can change the passwords of all users.
For a list of user privileges, see Appendix A, "User privileges".

4.6.3 Configure the RADIUS authentication / accounting function

To authenticate users using the RADIUS authentication server or save accounting logs to the RADIUS accounting server, carry out the following commands.

(1) Configure the RADIUS authentication client

To change the authentication method to RADIUS, set RADIUS authentication server 1 to "172.31.1.1", set the Radius authentication port to "1645", and register a secret key (abcdef), carry out the following commands. With the following settings, all users to be authenticated by RADIUS authentication are treated as port users. Normal users and device management users are authenticated by the internal authentication of NS-2250 (local authentication). The default setting for the RADIUS authentication port is "1812".

```
(c)NS-2250# set auth mode radius↵
(c)NS-2250# set auth radius server 1 addr 172.31.1.1↵
(c)NS-2250# set auth radius server 1 port 1645↵
(c)NS-2250# set auth radius server 1 key password↵
(Enter secret key (abcdef))
(c)NS-2250#
```

To authenticate normal users and device management users by using the RADIUS authentication server, see the following sections: (4) "Configure user group identification and access control of serial ports (filter_id_head)" and (5) "Configure user group identification and access control of serial ports (access grouping function)".

(2) Configure the RADIUS accounting client

To change the accounting method to RADIUS, set RADIUS accounting server 1 to "172.31.1.1", set the RADIUS accounting port to "1646", and register a secret key (abcdef), carry out the following commands. The default setting for the RADIUS accounting port is "1813".

```
(c)NS-2250# set acct mode radius↵
(c)NS-2250# set acct radius server 1 addr 172.31.1.1↵
(c)NS-2250# set acct radius server 1 port 1646↵
(c)NS-2250# set acct radius server 1 key password↵
(Enter secret key (abcdef))
(c)NS-2250#
```

(3) Configure the retry/timeout values for RADIUS authentication/accounting request packets.

To configure the number of retries for RADIUS authentication/accounting request packets and the timeout time of authentication/accounting response packets, carry out the following commands.
At the default settings, the number of retries is 3 times and the timeout value is 5 seconds.

```
(c)NS-2250# set auth radius retry 5↵
(c)NS-2250# set auth radius server 1 timeout 10↵
(c)NS-2250# set acct radius retry 5↵
(c)NS-2250# set acct radius server 1 timeout 10↵
(c)NS-2250#
```

(4) Configure user group identification and access control of serial ports (filter_id_head)

To identify user groups and control access of serial ports by using RADIUS authentication, configure and carry out the "set auth server {normal | root | portusr } filter_id_head" command so that the lead character string of the Filter-Id to be sent from the RADIUS authentication server during authentication is used as an identifier to identify user groups. One identifier can be configured for each user group.

When the following settings have been configured, the Filter-Id attribute values of users registered to the RADIUS authentication server result in the following actions.

```
(c)NS-2250# set auth radius server 1 root filter_id_head NS2250_ROOT↵
(c)NS-2250# set auth radius server 1 normal filter_id_head NS2250_NORMAL↵
(c)NS-2250# set auth radius server 1 portusr filter_id_head NS2250_PORT↵
(c)NS-2250#
```

・ When the Filter-Id attribute value character string starts with "NS2250_ROOT", the user is treated as a device management user.
・ When the Filter-Id attribute value character string starts with "NS2250_NORMAL", the user is treated as a normal user.
・ When the Filter-Id attribute value character string starts with "NS2250_PORT", the user is treated as a port user. When a character string indicating a port number follows "NS2250_PORT", such as "NS2250_PORT1-10", access privileges to the indicated port are configured.

■RADIUS server setting

User name	Attribute setting
somebody	Filter-Id = NS2250_NORMAL
root	Filter-Id = NS2250_ROOT
suzuki	Filter-Id = NS2250_PORT1-10
tanaka	Filter-Id = NS2250_PORT11-20
yamada	Filter-Id = NS2250_PORT30-32

RADIUS server

NS-2250

■filter_id_head setting

user type	filter_id_head setting
Device management user	NS2250_ROOT
Normal user	NS2250_NORMAL
Port user	NS2250_PORT

Figure4-1 User group identification and access control of serial ports (filter_id_head)

For the action when the user group cannot be identified even when RADIUS authentication is successful, see (6) "Configure access methods for users for which a user group cannot be identified".

Priority during login is as follows: 1) device management user (root), 2) normal user (normal), and 3) port user (portusr). In Direct mode, for device login, log in as the user with the higher priority of access privileges 1) and 2) You can access the port server only when you have access privileges of 3). When you log into Select mode, log in as the user with the highest priority of access privileges of 1), 2), and 3).

| RADIUS server Filter-Id settings "Set auth radius server {normal \| root \| portusr }filter_id_head" command configuration | Direct mode | | Select mode |
	Device access	Port access	
Device management user	Device management user	- (access not permitted)	Device management user
Normal user	Normal user	- (access not permitted)	Normal user
Port user	- (access not permitted)	Port user	Port user
Device management user/normal user	Device management user	- (access not permitted)	Device management user
Device management user/port user	Device management user	Port user	Device management user
Normal user/port user	Normal user	Port user	Normal user
Device management user/normal user/port user	Device management user	Port user	Device management user

Enable this function when there are few NS-2250 units or when you want to complete user management by a RADIUS server alone. For example, use this setting when there are few NS-2250 units, and you can fix the serial ports to which each port user can access. (User 1

can access serial port 1 through 10, and user 2 can access serial port 20 through 30, and so on)

> Caution The NS-2250 performs user authentication in the following order:
> 1) local authentication within the NS-2250 -> 2) RADIUS authentication.
> When normal users undergo RADIUS authentication, either delete normal users registered to the NS-2250 or configure a password different from the password registered to the RADIUS server. Be aware that when a password is not registered for normal users, simply pressing the Return key for the password makes it possible to pass local authentication of the NS-2250 and log in.
> The result is the same as when logging in as a device management user or carrying out the "su" command. Configure a password different from the password registered to the RADIUS server for device management users. Note that, unlike normal users, device management users (root) cannot be deleted.

For details, see "set auth radius server { portusr | root | normal } filter_id_head" in the Command Reference, and Appendix B, "Examples of attributes and RADIUS authentication/accounting server settings" in this manual.

(5) Configure user group identification and access control of serial ports (access grouping function)

The access grouping function strengthens the following two functions based on the previously mentioned "filter_id_head".

> You can register multiple identifiers for device management users, normal users, and port users.
> With the access grouping function, individual identifiers configured for user groups are called access groups.
> In the RADIUS server, you can configure different access control for serial ports for each NS-2250 to be accessed by defining only the access group to which the user belongs, and then configuring the access group definition and port user access privileges settings on each NS-2250.

To use the access grouping function, use the "create auth access_group" command to configure the device management user, normal user, and port user access groups in the NS-2250, and then change user authentication to RADIUS.

```
(c)NS-2250# create auth access_group root radius filter_id admin_grp↵
(c)NS-2250# create auth access_group normal radius filter_id normal_grp↵
(c)NS-2250# create auth access_group portusr port 1-10 radius filter_id port_grp ↵
(c)NS-2250#
```

When the following settings have been configured, the Filter-Id attribute values of users registered to the RADIUS authentication server result in the following actions.

When the Filter-Id attribute value is "admin_grp", the user is treated as a device management user.

When the Filter-Id attribute value is "normal_grp", the user is treated as a normal user.

When the Filter-Id attribute value is "port_grp", the user is treated as a port user that belongs to the "port_grp" access group. Also, users that belong to the "port_grp" access group are configured with access privileges to serial port 1 through serial port 10, which are specified by the command.

(In the case of "filter_id_head", the character string specified by the command and the head of the character string for the Filter-Id attribute are partially compared. However, with the access grouping function, they are compared for complete matches.)

■RADIUS server setting

User name	Attribute setting
somebody	Filter-Id = normal_grp
root	Filter-Id = admin_grp
suzuki	Filter-Id = port_grp
tanaka	Filter-Id = port_grp
yamada	Filter-Id = port_grp

RADIUS server

NS-2250

■Access grouping setting

user type	Group name	Access rights
Device management user	admin_grp	Cannot be configured
Normal user	normal_grp	
Port user	port_grp	Serial ports 1-10

Figure4-2 User group identification and access control of serial ports (access group)

For the action when the user group cannot be identified even when RADIUS authentication is successful, see (6), "Configure access methods for users for which a user group cannot be identified".

Priority during login is as follows: 1) device management user (root), 2) normal user (normal), and 3) port user (portusr). In Direct mode, for device login, log in as the user with the higher priority of access privileges 1) and 2). You can access the port server only when you have access privileges of 3). When you log into Select mode, log in as the user with the highest priority of access privileges of 1), 2), and 3).

RADIUS server Filter-Id settings "Create auth access_group" command configuration	Direct mode		Select mode
	Device access	Port access	
Device management user	Device management user	- (access not permitted)	Device management user
Normal user	Normal user	- (access not permitted)	Normal user
Port user	- (access not permitted)	Port user	Port user
Device management user/normal user	Device management user	- (access not permitted)	Device management user
Device management user/port user	Device management user	Port user	Device management user
Normal user/port user	Normal user	Port user	Normal user
Device management user/normal user/port user	Device management user	Port user	Device management user

Configuring this setting is useful when there are many NS-2250 units and you want to register multiple port user access groups or when the serial ports that can be accessed by port users are different for each NS-2250. (For example, User 1 can access serial ports 1 through 10 on the NS-2250-1, serial ports 15 through 20 on the NS-2250-2, and so on.)

As a reference, the following section provides an example in which two port-user access groups with different access privileges to the serial ports of two NS-2250 units are registered.

■ NS-2250-1 settings

Access group of device management users	:admin_grp
Access group of normal users	:normal_grp
Access group of port users	:port_grp1
Access privileges of serial ports for port_grp1	:1-10
Access group of port users	:port_grp2
Access privileges of serial ports for port_grp2	:31,32

```
(c)NS-2250-1# create auth access_group root radius filter_id admin_grp↵
(c)NS-2250-1# create auth access_group normal radius filter_id normal_grp↵
(c)NS-2250-1# create auth access_group portusr port 1-10 radius filter_id port_grp1↵
(c)NS-2250-1# create auth access_group portusr port 31,32 radius filter_id port_grp2↵
(c)NS-2250-1#
```

■ NS-2250-2 settings

Access group of device management users	:admin_grp
Access group of normal users	:normal_grp
Access group of port users	:port_grp1
Access privileges of serial ports for port_grp1	:15-20
Access group of port users	:port_grp2
Access privileges of serial ports for port_grp2	:1-5

```
(c)NS-2250-2# create auth access_group root radius filter_id admin_grp↵
(c)NS-2250-2# create auth access_group normal radius filter_id normal_grp↵
(c)NS-2250-2# create auth access_group portusr port 15-20 radius filter_id port_grp1↵
(c)NS-2250-2# create auth access_group portusr port 1-5 radius filter_id port_grp2↵
(c)NS-2250-2#
```

Caution The NS-2250 performs user authentication in the following order:

1) local authentication within the NS-2250 → 2) RADIUS authentication.

When normal users undergo RADIUS authentication, either delete normal users registered to the NS-2250 or configure a password different from the password registered to the RADIUS server. Be aware that when a password is not registered for normal users, simply pressing the Return key for the password makes it possible to pass local authentication of the NS-2250 and log in.

The result is the same as when logging in as a device management user or carrying out the "su" command. Configure a password different from the password registered to the RADIUS server for device management users. Note that, unlike normal users, device management users (root) cannot be deleted.

For details, see the "create auth access_group" command in the Command Reference, and Appendix B, "Examples of attributes and RADIUS authentication/accounting server settings" in this manual.

(6) Configure access methods for users for which a user group cannot be identified

In some cases, the user group of the user cannot be identified even when RADIUS authentication is successful. (Examples include when the Filter-Id attribute value was not sent from the RADIUS authentication server or when the Filter-Id attribute does not match the character string specified by either the "create auth access group" command or "set auth radius server {normal | root | portusr } filter_id_head" command.) The access method in such cases is determined by the configuration of the "set auth radius def_user" command.

If this command has not been configured, users for which the user group cannot be identified are treated as port users, and they are given privileges that allow access to all serial ports.

To refuse access for users for which a user group cannot be identified, carry out the following command.

```
(c)NS-2250# set auth radius def_user none↵
(c)NS-2250#
```

(7) Change the NAS-Id attribute

To configure the NAS-Id attribute value so that a client can be identified as an NS-2250 by the Radius authentication server or accounting server, carry out the following commands. If this command is not configured, the NAS-Id value is configured and sent as the name of the NS-2250.

```
(c)NS-2250# set auth radius server 1 nas_id SmartCS↵
(c)NS-2250# set acct radius server 1 nas_id SmartCS↵
(c)NS-2250#
```

(8) Change the authentication user name when the "su" command has been carried out

If you carry out the "su" command after logging in as a normal user, you can switch to a device management user. When the "su" command was carried out, the user name used for RADIUS authentication is "root".

To change the name of the user to be authenticated, carry out the following commands.

```
(c)NS-2250# set auth su_cmd username csadmin↵
(c)NS-2250#
```

(9) Configure the sending method of accounting STOP packets when user authentication has failed

The sending method of accounting STOP packets when user authentication has failed is configured by using the "set acct radius auth_deny_stop" command. If the setting is configured to "off" as shown below, accounting STOP packets are not sent even when authentication has failed. The default setting is "remote" (send an accounting STOP packet only when RADIUS authentication has failed.)

```
(c)NS-2250# set acct radius auth_deny_stop off↵
(c)NS-2250#
```

4.6.4 Configure the TACACS+ function

To authenticate/approve users by using the TACACS+ authentication server or to save accounting logs, carry out the following commands.

(1) Configure the TACACS+ function

To change the user authentication and accounting methods to TACACS+, set the IP address of the TACACS+ authentication server to "172.31.1.1", and configure the secret key to "abcdef", carry out the following commands. With the following settings, all users to be authenticated by TACACS+ authentication are treated as port users. Normal users and device management users are authenticated by the internal authentication of NS-2250 (local authentication).
On the NS-2250, the port number on the TACACS+ server is fixed to TCP (49).

```
(c)NS-2250# set auth mode tacacs↵
(c)NS-2250# set auth tacacs server 1 addr 172.31.1.1↵
(c)NS-2250# set auth tacacs server 1 key password↵
(Enter secret key (abcdef))
(c)NS-2250# set acct mode tacacs↵
(c)NS-2250# set acct tacacs server 1 addr 172.31.1.1↵
(c)NS-2250# set acct tacacs server 1 key password↵
(Enter secret key (abcdef))
(c)NS-2250#
```

To authenticate normal users and device management users by using the TACACS+ server, see (3) "Configure user group identification and access control of serial ports (access grouping)".

(2) Configure the timeout time value

To configure the timeout value for TACACS+ authentication/approval/accounting, carry out the following commands.
At the default settings, the timeout value is 5 seconds.

```
(c)NS-2250# set auth tacacs server 1 timeout 10↵
(c)NS-2250# set acct tacacs server 1 timeout 10↵
(c)NS-2250#
```

(3) Configure user group identification and access control of serial ports (access grouping)

To use the access grouping function, use the "create auth access_group" command to register the attribute and value pairs to identify device management users, normal users, and port users access groups in the NS-2250. Set the list of serial ports to which port users have access in the same manner.

The attribute name (in this example, grp) and value (in this example, grp=admin_grp, and so on) pair can be determined as desired by a device administrator. Configure the attribute and value pair specified by this command for the user definition of the TACACS+ server as well.

■TACACS+ server setting

User name	Pair of attribute and value
somebody	grp = normal_grp
root	grp = admin_grp
suzuki	grp = port_grp1
tanaka	grp = port_grp2

TACACS+ server

NS-2250-1

NS-2250-2

■Access grouping setting

user type	Pair of attribute and value	Serial port access control
Device management user	grp = admin_grp	Cannot be configured
Normal user	grp = normal_grp	
Port user	grp = port_grp1	1～10
	grp = port_grp2	11～20

■Access grouping setting

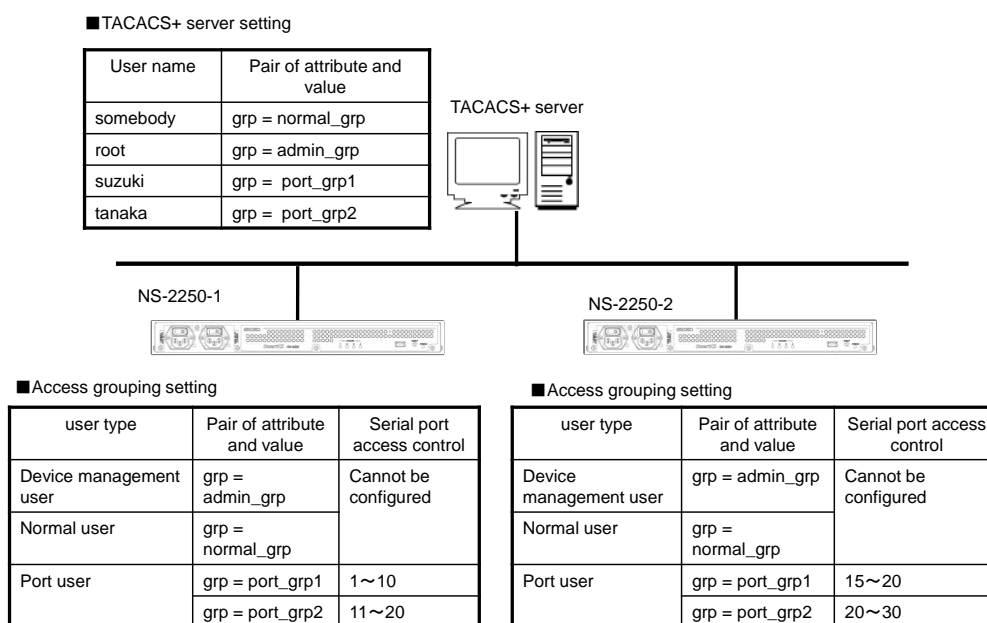| user type	Pair of attribute and value	Serial port access control
Device management user	grp = admin_grp	Cannot be configured
Normal user	grp = normal_grp	
Port user	grp = port_grp1	15～20
	grp = port_grp2	20～30

Figure 4-3 Configure user group identification and access control of serial ports (TACACS+)

When the NS-2250 has been configured with the following settings, user identification is determined by the attributes of users registered to the TACACS+ server, as shown below.

```
(c)NS-2250# create auth access_group root tacacs attr grp val admin_grp↵
(c)NS-2250# create auth access_group normal tacacs attr grp val normal_grp↵
(c)NS-2250# create auth access_group portusr port 1-10 tacacs attr grp val port_grp1 ↵
(c)NS-2250# create auth access_group portusr port 11-20 tacacs attr grp val port_grp2 ↵
(c)NS-2250#
```

When the "grp" attribute value is "admin_grp", the user is treated as the device management user.
When the "grp" attribute value is "normal_grp", the user is treated as a normal user.
When the "grp" attribute value is "port_grp1" or "port_grp2", this user is treated as a port user that belongs to the "port" access group. Also, configure access privileges to serial ports specified by the command for users that belong to the "port" access group.

For the action when the user group cannot be identified even when TACACS+

authentication/approval is successful, see (4), "Configure access methods for users for which a user group cannot be identified".

The priority during login when multiple groups have been configured for a user is as follows: 1) device management user (root), 2) normal user (normal), and 3) port user (portusr). In Direct mode, for device login, log in as the user with the higher priority of access privileges 1) and 2). You can access the port server only when you have access privileges of 3). When you log into Select mode, log in as the user with the highest priority of access privileges of 1), 2), and 3).

"Create auth access_group" command configuration	Direct mode		Select mode
	Device access	Port access	
Device management user	Device management user	- (access not permitted)	Device management user
Normal user	Normal user	- (access not permitted)	Normal user
Port user	- (access not permitted)	Port user	Port user
Device management user/normal user	Device management user	- (access not permitted)	Device management user
Device management user/port user	Device management user	Port user	Device management user
Normal user/port user	Normal user	Port user	Normal user
Device management user/normal user/port user	Device management user	Port user	Device management user

Configuring the access grouping function is useful when there are many NS-2250 units and you want to register multiple port-user access groups or when the serial ports that can be accessed by port users are different for each NS-2250. (For example, User 1 can access serial ports 1 through 10 on the NS-2250-1, serial ports 15 through 20 on the NS-2250-2, and so on.)

(4) Configure access methods for users for which a user group cannot be identified

In some cases, the user group of the user cannot be identified even when TACACS+ authentication/approval is successful. (Examples include when the attribute to identify the user type was not sent from the TACACS+ server or when the attribute and value pair does not match the character string specified by the "create auth access group" command.) The access method in such cases is determined by the configuration of the "set auth tacacs def_user" command.

If this command has not been configured, users for which the user group cannot be identified are treated as port users, and they are given privileges that allow access to all serial ports.

To refuse access for users for which a user group cannot be identified, carry out the following command.

```
(c)NS-2250# set auth tacacs def_user none↵
(c)NS-2250#
```

(5) Change the authentication user name when the "su" command has been carried out

If you carry out the "su" command after logging in as a normal user, you can switch to a device management user. When the "su" command was carried out, the user name used for TACACS+ authentication is "root".

To change the name of the user to be authenticated, carry out the following commands.

```
(c)NS-2250# set auth su_cmd username csadmin↵
(c)NS-2250#
```

(6) Configure the sending method of accounting STOP packets when user authentication has failed

The sending method of accounting STOP packets when user authentication has failed is configured by the "set acct_tacacs auth_deny_stop" command. If the setting is configured to "off" as shown below, accounting STOP packets are not sent even when authentication has failed. The default setting is "remote" (send an accounting STOP packet only when TACACS+ authentication has failed.)

```
(c)NS-2250# set acct tacacs auth_deny_stop off↵
(c)NS-2250#
```

4.6.5 Configure the telnet server

To change the TCP port number of the telnet server, carry out the following commands.
The port number of the telnet server can be set from 1,025 through 65,000, and the default
setting is 23.

```
(c)NS-2250# set telnetd port 2023↵
(c)NS-2250#
```

4.6.6 Configure the SSH server

To access the NS-2250 or port server from an SSH client, you must configure the SSH
server in the NS-2250.
The SSH server of the NS-2250 supports password (basic) authentication, which uses user
IDs and passwords, and public key (public) authentication, which uses public keys. When
security is important, select public key (public) authentication.
The default SSH authentication method is public key (public) authentication.

When configuring the SSH server, also refer to Section 4.4.3, "User authentication of the
port server" and Section 4.6.5, "Control access to servers".

(1)   Configure SSH password (basic) authentication

```
(c)NS-2250# set sshd auth basic↵
(c)NS-2250# enable sshd↵
(c)NS-2250#
```

(2)   Configure SSH public key (public) authentication

```
(c)NS-2250# set sshd auth public↵
(c)NS-2250# set user user1 sshkey public ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAztMPnE3aPKRbkn5/48ah6MmucLZbY8dzqT+p
dgmbJIZqOUqVXlffWtD9+8X8Wn0vZ6TK0E2vLNGDSlsQT+zZ7darBKiIugcuZAOh
IAEpPeUbaYqwaRXPCkcAnTCS9GTIN2lo9DB1P04bamJG//V3TYxH/rCaGE5TTjH4
kFADUrM= test↵
```
(Specify the public key generated by the SSH client terminal. The line above is a single line.)
```
(c)NS-2250# enable sshd↵
(c)NS-2250#
```

(3)   Change the TCP port number of the SSH server

To change the TCP port number of the SSH server, carry out the following command.
The port number of the SSH server can be set from 1,025 through 65,000, and the default
setting is 22.

```
(c)NS-2250# set sshd port 2022↵
(c)NS-2250#
```

You can check the SSH server status by using the "show service" command.

```
(c)NS-2250# show service↵
<telnetd>
 status   : enable
 port     : 23

<sshd>
 status   : disable
 port     : 22
 auth     : public
 host_key : device_depend

<ftpd>
 status   : enable
(c)NS-2250#
```

4.6.7 Control access to servers (allowhost)

The following table shows the servers of the NS-2250 for which you can restrict access. You can control access from client terminals by specifying the network address of client terminals that are allowed to connect to each server running on the NS-2250.

Server for which access control can be configured	Default access control	Network address allowed to connect at the default settings
Telnet server	Allow	All
SSH server	Refuse	-
FTP server	Refuse	-
Port server (telnet Normal mode)	Allow	All
Port server (telnet Monitoring mode)	Refuse	-
Port server (SSH Normal mode)	Refuse	-
Port server (SSH Monitoring mode)	Refuse	-

The default startup file of the NS-2250 is configured by the following commands.
("Allowhost" at default settings)

```
create allowhost all service telnetd
create allowhost all service portd telrw all
```

To add "192.168.1.0/24" and "2001:db8::/64" to the networks that can access the telnet server of the NS-2250 and add "192.168.1.0/24" and "2001:db8::/64" as an address allowed to connect in telnet Normal mode to the serial ports of the NS-2250 (port 1 through 8 and port 17), carry out the command as shown below.

```
(c)NS-2250#create allowhost 192.168.1.0/24 service telnetd↵
(c)NS-2250# create allowhost 192.168.1.0/24 service portd telrw 1-8,17↵
(c)NS-2250# create allowhost 2001:db8::/64 service telnetd↵
(c)NS-2250# create allowhost 2001:db8::/64 service portd telrw 1-8,17↵
```

You can check the list of servers that allow access by using the "show allowhost" command.

```
(c)NS-2250# show allowhost↵
Service        Address/Mask                      Access tty List
----------------------------------------------------------------
portd/telrw    192.168.1.0/24                     1-8,17
portd/telrw    2001:db8::/64                      1-8,17
telnetd        192.168.1.0/24                     -
telnetd        2001:db8::/64                      -
(c)NS-2250#
```

Caution   The "create allowhost" command is evaluated in order from the top line. For example, when the following two lines are registered, the second line is not evaluated. Delete unnecessary lines by using the "delete allowhost"

command.

Create allowhost all service telnetd

Create allowhost 192.168.1.0/24 service telnetd

4.6.8 Configure the Firewall(ipfilter/ip6filter)

You can achieve the access control by the IP address or the protocol type by configuring the Firewall (ipfilter/ip6filter) to the input interface.

The below table shows the example of the configuration when you set the Firewall(ipfilter) to LAN1 port and accept the ICMP/telnet/snmp only from the sender IP address of 172.16.0.0/24.

```
(c)NS-2250# create ipfilter input line 1 accept eth1 any 172.16.0.0/24 icmp↵
(c)NS-2250# create ipfilter input line 2 accept eth1 any 172.16.0.0/24 tcp 23↵
(c)NS-2250# create ipfilter input line 3 accept eth1 any 172.16.0.0/24 udp 161↵
(c)NS-2250# create ipfilter input line 4 drop eth1 any any any↵
(c)NS-2250# enable ipfilter↵
(c)NS-2250#
```

The setting of ip6filter is configured as follows.
The below table shows the example of the configuration when you set the Firewall(ip6filter) to LAN1 port and accept the ICMP/telnet/snmp only from the sender IP address of 2001:db8::/64.
In addition, please be sure to register ICMPv6 type 135(Neighbor solicitation) and 136(Neighbor advertisement) used for Neighbor Discovery to be permitted if only necessary filter settings are permitted and "drop" setting is registered to the last line as follows.

```
(c)NS-2250# create ip6filter input line 1 accept eth1 any 2001:db8::/64 icmp↵
(c)NS-2250# create ip6filter input line 2 accept eth1 any 2001:db8::/64 tcp 23↵
(c)NS-2250# create ip6filter input line 3 accept eth1 any 2001:db8::/64 udp 161↵
(c)NS-2250# create ip6filter input line 4 accept any any any icmp 135↵
(c)NS-2250# create ip6filter input line 5 accept any any any icmp 136↵
(c)NS-2250# create ip6filter input line 6 drop eth1 any any any↵
(c)NS-2250# enable ip6filter↵
(c)NS-2250#
```

The next table shows the example of the filter configuration when you establish the VPN connection while the IPsec is set.

When IPsec is utilized it is necessary to configure the filter of the decoded packet.

For example, if you establish the VPN connection by IPsec and access to NS-2250 via SSH/SFTP you need to register the filter configuration which allows IKE (UDP 500), NAT traversal (UDP 4500) and SSH/SFTP (TCP22) by the IPsec.

```
(c)NS-2250# create ipfilter input line 1 accept eth1 any any esp↵
(c)NS-2250# create ipfilter input line 2 accept eth1 any any udp 500↵
(c)NS-2250# create ipfilter input line 3 accept eth1 any any udp 4500↵
(c)NS-2250# create ipfilter input line 4 accept eth1 any any tcp 22↵
(c)NS-2250# create ipfilter input line 5 drop eth1 any any any↵
(c)NS-2250# enable ipfilter↵
(c)NS-2250#
```

You can view the configuration of the Firewall (ipfilter) by the below commands.

```
(c)NS-2250# show ipfilter input
status : enable

<ipfilter preset input table>
num  target  in    destination     source          prot
  1  ACCEPT  *     0.0.0.0/0       0.0.0.0/0       all REL,EST
  2  ACCEPT  lo    127.0.0.1       127.0.0.1       all


<ipfilter configurable input table>
num  target  in    destination     source          prot
  1  ACCEPT  eth1  0.0.0.0/0       0.0.0.0/0       esp
  2  ACCEPT  eth1  0.0.0.0/0       0.0.0.0/0       udp 500
  3  ACCEPT  eth1  0.0.0.0/0       0.0.0.0/0       udp 4500
  4  ACCEPT  eth1  0.0.0.0/0       0.0.0.0/0       tcp 22
  5  DROP    eth1  0.0.0.0/0       0.0.0.0/0       all
(c)NS-2250#
```

You can view the configuration of the Firewall (ip6filter) by the below commands.

```
(c)NS-2250# show ip6filter input
status : enable

<ip6filter preset input table>
num  target  in    destination              source                    prot
  1  ACCEPT  *     ::/0                      ::/0                      all  REL,EST
  2  ACCEPT  lo    ::1                       ::1                       all


<ip6filter configurable input table>
num  target  in    destination              source                    prot
  1  ACCEPT  eth1  ::/0                      2001:db8::/64             icmpv6
  2  ACCEPT  eth1  ::/0                      2001:db8::/64             tcp  23
  3  ACCEPT  eth1  ::/0                      2001:db8::/64             udp  161
  4  DROP    eth1  ::/0                      ::/0                      all
  5  ACCEPT  *     ::/0                      ::/0                      icmpv6 135
  6  ACCEPT  *     ::/0                      ::/0                      icmpv6 136
  7  ACCEPT  *     ::/0                      ::/0                      icmpv6 135
  8  ACCEPT  *     ::/0                      ::/0                      icmpv6 136


(c)NS-2250#
```

You can view the statistical information of the Firewall (ipfilter) by the below commands.

```
(c)NS-2250# show stats ipfilter input↵
<ipfilter preset input statistic>
    pkts  target in   destination        source         prot
       0  ACCEPT *    0.0.0.0/0          0.0.0.0/0      all REL,EST
       0  ACCEPT lo   127.0.0.1          127.0.0.1      all


<ipfilter configurable input statistic>
    pkts  target in   destination        source         prot
       0  ACCEPT eth1 0.0.0.0/0          0.0.0.0/0      esp
       0  ACCEPT eth1 0.0.0.0/0          0.0.0.0/0      udp 500
       0  ACCEPT eth1 0.0.0.0/0          0.0.0.0/0      udp 4500
       0  ACCEPT eth1 0.0.0.0/0          0.0.0.0/0      tcp 22
       0  DROP   eth1 0.0.0.0/0          0.0.0.0/0      all
(c)NS-2250#
```

You can view the statistical information of the Firewall (ip6filter) by the below commands.

```
(c)NS-2250# show stats ip6filter input
<ip6filter preset input statistic>
    pkts target in    destination                source                prot
      0 ACCEPT *    ::/0                       ::/0                  all  REL,EST
      0 ACCEPT lo   ::1                        ::1                   all


<ip6filter configurable input statistic>
    pkts target in    destination                source                prot
      0 ACCEPT eth1 ::/0                       2001:db8::/64         icmpv6
      0 ACCEPT eth1 ::/0                       2001:db8::/64         tcp  23
      0 ACCEPT eth1 ::/0                       2001:db8::/64         udp  161
      0 DROP   eth1 ::/0                       ::/0                  all
      0 ACCEPT *    ::/0                       ::/0                  icmpv6 135
      0 ACCEPT *    ::/0                       ::/0                  icmpv6 136
      0 ACCEPT *    ::/0                       ::/0                  icmpv6 135
      0 ACCEPT *    ::/0                       ::/0                  icmpv6 136


(c)NS-2250#
```

4.6.9 Configure the IPsec

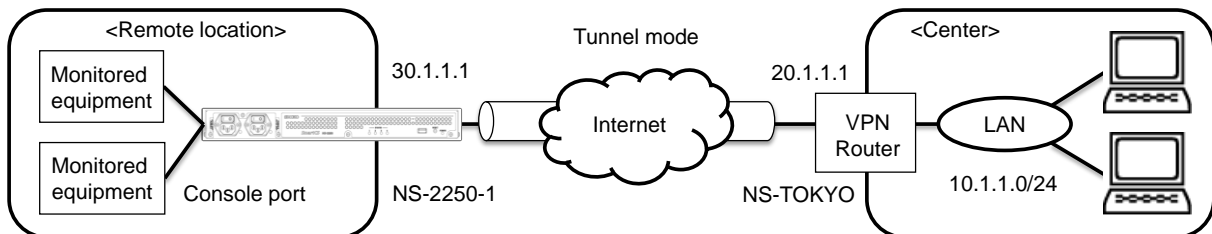You can create an IPsec tunnel and encrypt the data transmission by executing the below commands.

Figure 4-4 IPsec VPN connection

The next table shows the example of the connection of the IPsec tunnel by the responder configuration using the encryption algorithm, authentication algorithms, and the DH group 2 (1024 bit).

Register the pre-shared-key used by IKE designating NS-2250-1 to the security gateway ID and NS-TOKYO to the remote device ID respectively. Specify "set ipsec conn leftid" or "set ipsec conn rightid" in case the NAT device exists during IPsec tunnels.

```
(c)NS-2250# create ipsec secret psk NS-2250-1 NS-TOKYO password↵
Pre-Shared-Key password          (Set the pre-shared-key)
Retype Pre-Shared-Key password    (Set the pre-shared-key)
(c)NS-2250# set ipsec conn 1 auto add↵
(c)NS-2250# set ipsec conn 1 leftid NS-2250-1↵
(c)NS-2250# set ipsec conn 1 rightid NS-TOKYO↵
(c)NS-2250# set ipsec conn 1 left 30.1.1.1↵
(c)NS-2250# set ipsec conn 1 right 20.1.1.1↵
(c)NS-2250# set ipsec conn 1 leftsubnet 30.1.1.0/24↵
(c)NS-2250# set ipsec conn 1 rightsubnet 10.1.1.0/24↵
(c)NS-2250# set ipsec conn 1 keyexchange ikev1↵
(c)NS-2250# set ipsec conn 1 ike aec128-sha1-modp1024↵
(c)NS-2250# set ipsec conn 1 esp aec128-sha1-modp1024↵
(c)NS-2250# enable ipsec conn 1↵
(c)NS-2250#
```

Set an appropriate value to MTU by "set ipinterface mtu" command depending on the Network configuration. The LAN1 MTU is set to 1280 byte in the below example.

```
(c)NS-2250# set ipinterface eth1 mtu 1280↵
(c)NS-2250#
```

You can see the connection status of the IPsec by the below commands.

```
 (c)NS-2250# show ipsec status↵
Security Associations (1 up, 0 connecting):
  conn_01[37]: ESTABLISHED 118 minutes ago,30.1.1.1[NS-2250-1]...20.1.1.1[NS-TOKYO]
  conn_01{133}:  INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs:cc2ac764_i cf835d47_o
  conn_01{133}:   30.1.1.0/24 === 10.1.1.1/24
 (c)NS-2250#
```

4.7 Configure operation management

4.7.1 Configure the SNTP client

To configure the SNTP client, carry out the "set sntp server" command and the "set sntp polltime" command as shown below. To synchronize the time of the NS-2250 with the SNTP server (172.16.1.1) with a polling timer of 900 seconds, carry out the following commands.
The maximum number of SNTP servers that can be registered to the NS-2250 is two.

```
(c)NS-2250# set sntp server 172.16.1.1↵
(c)NS-2250# set sntp polltime 900↵
(c)NS-2250# enable sntp↵
(c)NS-2250#
```

You can check the SNTP client status by using the "show sntp" command.

```
(c)NS-2250# show sntp↵
<sntp information>
 status          : enable
 poll interval   : 600
 last sync server : 172.16.1.1

<primary server>
 server address  : 172.16.1.1
 last access time : 2015/06/05 20:17:10
 access result   : OK

<secondary server>
 server address  : ---
 last access time : ---
 access result   : ---
 (c)NS-2250#
```

4.7.2 Configure the SNMP agent

To configure the SNMP agent, first configure the SNMP server, SNMP trap, and other settings, and then enable the SNMP agent.

(1) Configure the SNMP server and community
When using SNMP Version 1 or Version 2, carry out the "set community" command to configure the SNMP server.
To allow read (ro) access from the SNMP server at 172.16.1.1 with the community "public", carry out the following commands.

```
(c)NS-2250# set community 1 name public view ro manager 172.16.1.1↵
(c)NS-2250# set community 2 name public view ro manager 172.16.1.2↵
(c)NS-2250#
```

If the above-mentioned commands are configured, and then the (4), "Enable the SNMP agent" is carried out, Version 1 and Version 2c Get requests from the SNMP server are supported.

(2) Configure the SNMP user
When using SNMP Version 3, carry out the "set snmpuser" command to configure the SNMP user.
To set the user "SmartCS" that uses the encryption algorithm "md5", carry out the following commands.

```
(c)NS-2250# set snmpuser 1 name SmartCS auth md5 password↵
authentication password
Retype authentication password
(c)NS-2250#
```

SmartCS gets to respond to the Version 3 Get request from SNMP server if the above commands are configured and "(6) Enable the SNMP agent" is executed.

(3) Configure the senddestination of the SNMP trap
To configure the send destination of the SNMP trap, carry out the "set trap manager" command.
To set the SNMP trap send destination to "172.16.1.1" and the trap community to "public"(Version 1/ Version 2), or the SNMP user to "user 1"(Version 3), carry out the following commands.

```
(c)NS-2250# set trap 1 manager 172.16.1.1 name public↵
(c)NS-2250# set trap 2 manager 172.16.1.2 name public version v2↵
(c)NS-2250# set trap 3 manager 176.16.1.3 version v3 snmpuser 1↵
(c)NS-2250#
```

You can specify the version format of the trap sent by the NS-2250 from Version 1 to 3.The

number of "snmpuser" must be specified from 1 to 4 when using SNMP Version 3. If a version format is not specified, the trap is sent in the SNMP Version 1 format.

(4)   Configure the SNMP management information
       To configure the SNMP management information (installation location and contact), carry out the "set snmp location" command and the "set snmp contact" command. To set the installation location to "Server Room in TOKYO" and the contact to "Administrator 03-1234-7777", carry out the following settings.

```
(c)NS-2250# set snmp location "Server Room in TOKYO" ↵
(c)NS-2250# set snmp contact "Administrator 03-1234-7777" ↵
(c)NS-2250#
```

(5)   Configure the snmpEngineID
       To configure the snmpEngineID notified in SNMP version 3 communication, carry out the "set snmp engineid" command. When snmpEngineID is configured the format notified to the manager is as follows.
       " 8000010704 " + ASCII string of setting values
       The MAC address of eth1 is specified as the snmpEngineID if this setting is omitted.
       " 8000010703 " + MAC address of eth1

```
(c)NS-2250# set snmp engineid "SmartCS001"↵
(c)NS-2250#
```

(6)   Enable the SNMP agent
       To enable the SNMP agent, carry out the "enable snmp" command.

```
(c)NS-2250# enable snmp↵
(c)NS-2250#
```

(7)   Change the traps to be monitored
       The following table shows the configuration values for the traps monitored by the SNMP agent at the default settings.

Trap	Setting
Coldstart Trap	ON
Authentication Failure Trap	ON
Link Trap	ON
Power Trap	ON
Bonding Active Switch Trap	ON
Serial DSR Trap	OFF(all serial ports are monitored)

To change the traps to be monitored, carry out the command that corresponds to each trap as shown below.

```
(c)NS-2250# set snmp coldstarttrap off↵
(c)NS-2250# set snmp authentrap on↵
(c)NS-2250# set snmp linktrap on↵
(c)NS-2250# set snmp powertrap on↵
(c)NS-2250# set snmp bondingactswtrap on↵
(c)NS-2250# set snmp tty 11 dsrtrap on↵
(c)NS-2250# set snmp tty 12 dsrtrap on↵
(c)NS-2250# enable snmp↵
```

You can check the SNMP agent status by using the "show snmp" command.

```
(c)NS-2250# show snmp↵
 status             : enable
 location           : "Server Room in TOKYO"
 contact            : "Administrator 03-1234-5678"
 engineid           : 8000010704536d6172744353303031
 linktrap           : on
 powertrap          : on
 authentrap         : on
 coldstarttrap      : off
 bondingactswtrap   : on
 dsrtrap(tty1-8)    : off  off  off  off  off  off  off  off
 dsrtrap(tty9-16)   : off  off  on   on   off  off  off  off
 dsrtrap(tty17-24)  : off  off  off  off  off  off  off  off
 dsrtrap(tty25-32)  : off  off  off  off  off  off  off  off
 --- trap configurations (3 entry) ---
 <trap 1>
   manager address  : 172.16.1.1
   community        : public
   version          : v1
 <trap 2>
   manager address  : 172.16.1.2
   community        : public
   version          : v2
 <trap 3>
   manager address  : 176.16.1.3
   community        : -
   version          : v3
   snmpuser         : 3
 --- community configurations (2 entry) ---
 <community 1>
   community        : public
   view             : ro
   manager address  : 172.16.1.1
 <community 2>
   community        : public
   view             : ro
   manager address  : 172.16.1.2
 --- snmpuser configurations (1 entry) ---
 <snmpuser 1>
   name             : SmartCS
   auth protocol    : md5
   priv protocol    : -
 <snmpuser 2>
   name             : -
   auth protocol    : -
   priv protocol    : -
 <snmpuser 3>
   name             : -
   auth protocol    : -
   priv protocol    : -
 <snmpuser 4>
   name             : -
   auth protocol    : -
   priv protocol    : -
 (c)NS-2250#
```

4.7.3 Configure the syslog client

To configure the syslog client, carry out the "set syslog host" command.
To carry out syslog transfer to the syslog server (172.16.1.1) with the syslog of the NS-2250 with the facility code "local1" and port logs with the facility code "local0", carry out the following command.

```
(c)NS-2250# set syslog host 1 172.16.1.1 syslog_facility
local1 portlog_facility local0↵
(c)NS-2250# enable syslog↵
(c)NS-2250#
```

You can check the syslog client information by using the "show syslog" command.

```
(c)NS-2250# show syslog↵
Syslog Status:enable
No. Syslog Host              Portlog-Facility    Syslog-Facility
-----------------------------------------------------------------
1   172.16.1.1               local0              local1
(c)NS-2250#
```

4.7.4 Configure the temperature sensor

The temperature sensor starts operating from the default status, and you can acquire the temperature without any particular configuration.
To configure the correction value for the temperature sensor　measure the approximate outdoor temperature, specify the correction value for adjustment in the "set temperature adjust" command.
You can specify the correction value from 0 through 20, and the default value is 0.
In the example below, the correction value is configured to -10 °C.

```
(c)NS-2250# set temperature adjust 10↵
(c)NS-2250#
```

You can check the temperature of the temperature sensor and the configuration of the correction value by using the "show temperature" command.

```
(c)NS-2250# show environment↵

<Environment status>

  Power information
    Power unit     : AC
    Power 1        : ON
    Power 2        : OFF

  Temperature information
    Current temp   : 38 deg C
    Sensor         : 38 deg C
    Adjust         : 0

(c)NS-2250#
```

4.7.5 Configure the time zone

To configure the time zone, carry out the "set timezone" command.
Specify a time zone name from the list displayed by the "show timezone list" command.
The default time zone is "Tokyo".

```
(c)NS-2250# show timezone↵
Timezone is "Tokyo"


(c)NS-2250# show timezone list H↵
  : omitted
Hongkong
Honolulu
  : omitted



(c)NS-2250# set timezone Hongkong↵
(c)NS-2250# write↵
Do you really want to write internal & external startup1 [y/n]? y↵
write external startup1
...................writing
write internal startup1
...................writing
(c)NS-2250# reboot↵
```

Caution   (1) From startup until settings are applied, time is displayed using the UTC
                time zone of default.
            (2) After configuring the time zone, always restart the NS-2250.
            (3) It may be necessary to acquire safety standards depending on the country.
            (4) If you will use the NS-2250 overseas, contact us or your dealer.

4.7.6 Configure CLI command function(operating via Ansible)

It's required to create a normal user, and enable to access NS-2250 via SSH to use the CLI
command function.

(1) Configure a user to execute CLI commands
It's necessary to create a user by the "create user" command.
If you will set "user01" as the username and "ansible" as the password, execute the
commands as below.

```
(c)NS-2250# create user user01 group normal password↵
New password: ansible
Retype new password: ansible
```

(2) Enable SSH server of NS-2250
It's necessary to execute "enable sshd" and "set sshd" command to configure the SSH
server.
If you will enable SSH server and set to use password(basic) authentication, execute the
commands as below.

```
(c)NS-2250# enable sshd
(c)NS-2250# set sshd auth basic
```

If the Firewall(ipfilter) function or access control function(allowhost) is enabled, it's required
to permit access from the management PC via SSH.

For details of the required commands and Ansible module, see "Command Reference" and
"Ansible operation guide".

4.7.7 Configure console access function(operating via Ansible)

It's required to enable tty manage object after creating an extension user and enabling to access NS-2250 via SSH to use tty manage function.

(1) Configure a user to use tty manage function
It's necessary to create a user by the "create user" command.
If you will set "user02" as the username and "ansible" as the password, execute the commands as below.

```
 (c)NS-2250# create user user02 group extusr password↵
New password: ansible
Retype new password: ansible
```

It's necessary to execute the "set user port" command to set accessible serial ports.
If you will set user02 to permit accessing serial port 1 to 10, execute the command as below.

```
 (c)NS-2250# set user user02 port 1-10↵
```

It's necessary to execute the "set user permission" command to grant the permission of tty manage function to the user.

```
 (c)NS-2250# set user user02 permission ttymanage on↵
```

(2) Enable SSH server of NS-2250
It's necessary to execute "enable sshd" and "set sshd" command to configure the SSH server.
If you will enable SSH server and set to use password(basic) authentication, execute the commands as below.

```
 (c)NS-2250# enable sshd
 (c)NS-2250# set sshd auth basic
```

If Firewall(ipfilter) function or access control function(allowhost) is enabled, it's required to permit access from management PC via SSH.

(3) Enable tty manage object
It's necessary to execute "enable ttymanage" command to enable tty to manage objects.

```
 (c)NS-2250# enable ttymanage
```

It's able to confirm the status of tty manage object by the "show ttymanage" command.

```
(c)NS-2250# show ttymanage
<ttymanage information>
status  : enable
```

For details of the required commands and Ansible module, see "Command Reference" and "Ansible operation guide".

4.8   Setting examples

4.8.1 Basic settings

This section describes the basic settings to access monitored equipment from a telnet client via the NS-2250.

Port server setting	:	Direct mode (default)
Method of connection	:	Telnet Normal mode (default)
Port user authentication	:	None (default)
Port log location	:	RAM (default)
Port log transfer function	:	Off (default)
Serial ports	:	Transfer speed of serial port 1 through serial port 8 (19,200 bps)
Session suspension character code	:	1 (Ctrl+A)

Configuration diagram
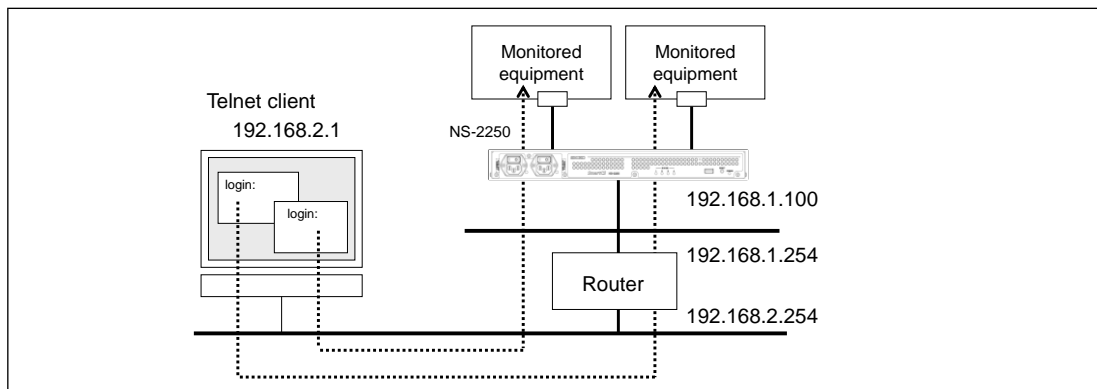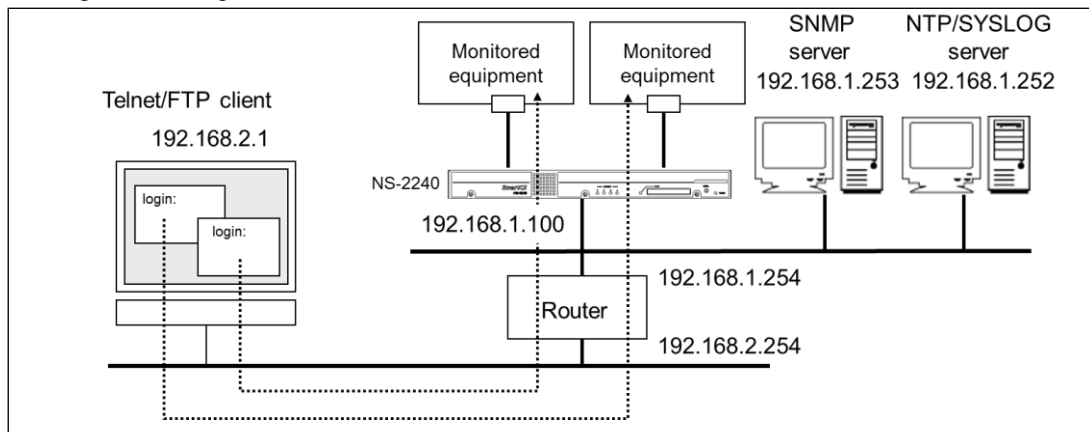

Figure 4-4 Basic settings

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254
set tty 1-8 baud 19200
set portd tty 1-8 cmdchar 1
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".

    set hostname SmartCS

    set ipaddr eth1 192.168.1.100/24

    create ip route default gateway 192.168.1.254

2. Set the transfer speed of serial port 1 through serial port 8 to 19,200 bps.

    set tty 1-8 baud 19200

3. Set the session suspension character code for serial port 1 through serial port 8 to "Ctrl+A".

```
set portd tty 1-8 cmdchar 1
```

Notes

The NS-2250 already stores the default settings in the startup file.

At the default settings, the host name is the NS-2250 and the LAN1 IP address is 192.168.0.1/24. Telnet Normal mode of the telnet server and port server of the NS-2250 is configured to allow access from all networks.

(Default setting)

```
(c)NS-2250# show config running
set timezone Tokyo
set hostname NS-2250
set ipaddr eth1 192.168.0.1/24
set tcpkeepalive 180
#
create user setup group setup uid 198
create user verup group verup uid 199
create user log group log uid 200
create user somebody group normal uid 100
#
create allowhost all service telnetd
create allowhost all service portd telrw all
(c)NS-2250#
```

4.8.2 Configure the services

This section describes the basic settings to access monitored equipment from a telnet client via the NS-2250 and the settings of the various services (SNMP agent, SNTP client, syslog client, and FTP server access control) to manage the NS-2250.

Port server setting   : Direct mode (default)
Method of connection   : Telnet Normal mode (default)
Port user authentication   : None (default)
Port log location   : RAM (default)
Port log transfer function   : OFF (default)
Settings   : SNMP agent
                                  SNTP client
                                  Syslog client
                                  Access control of FTP servers

Configuration diagram

Figure 4-5 Configuration of services

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set snmp location "Server Room in Tokyo"
set snmp contact "Administrator 03-1234-5678"
set trap 1 manager 192.168.1.253 name public
set community 1 name public view ro manager 192.168.1.253
enable snmp

set  syslog  host  1  192.168.1.252  portlog_facility  local0
syslog_facility local1
enable syslog
```

```
set sntp server 192.168.1.252
set sntp polltime 1200
enable sntp
create allowhost 192.168.2.0/24 service ftpd
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".

    set hostname SmartCS
    set ipaddr eth1 192.168.1.100/24
    create ip route default gateway 192.168.1.254

2. Configure the SNMP agent of the NS-2250.
For the SNMP agent of the NS-2250, set the installation location to "Server Room in Tokyo" and the contact to "Administrator 03-1234-5678".
Limit the SNMP server that can access the SNMP agent of the NS-2250 to IP address "192.168.1.253", a community string of "public", and access privileges to "read only".
SNMP traps sent from the NS-2250 are sent to the SNMP server (192.168.1.253) with a community string of "public".
After configuring the SNMP agent, carry out the "enable snmp" command to enable the SNMP agent.

    set snmp location "Server Room in Tokyo"
    set snmp contact "Administrator 03-1234-5678"
    set community 1 name public view ro manager 192.168.1.253
    set trap 1 manager 192.168.1.253 name public
    enable snmp

3. Configure the syslog client of the NS-2250.
Send to the syslog server (192.168.1.253) with the port log facility code of "local0" and the facility code of "local1" for syslog output by the NS-2250.
After configuring the syslog client, carry out the "enable syslog" command to enable the syslog client.

    set syslog host 1 192.168.1.252 portlog_facility local0 syslog_facility local1
    enable syslog

4. Configure the SNTP client function of the NS-2250.
Poll the time with the NTP server (192.168.1.252) every 1,200 seconds.
After configuring the SNTP client, carry out the "enable sntp" command to enable the SNTP function.

    set sntp server 192.168.1.252
    set sntp polltime 1200
    enable sntp

5. Enable the FTP server of the NS-2250, and then configure access control.
Allow access to the FTP server of the NS-2250 from the network of "192.168.2.0/24" only.

enable ftpd

to create allowhost 192.168.2.0/24 service ftpd

4.8.3 Configure port log transfer

This section describes the settings to output port logs like syslog, settings to send to specified FTP servers and mail addresses for each serial port, and settings to add time stamps to port logs.

Port server setting	: Direct mode (default)
Method of connection	: Telnet Normal mode (default)
Port user authentication	: None (default)
Port log location	: RAM(default)
Port log transfer function	: On (syslog/NFS/FTP/mail)
Time stamp function	: ON

Configuration diagram
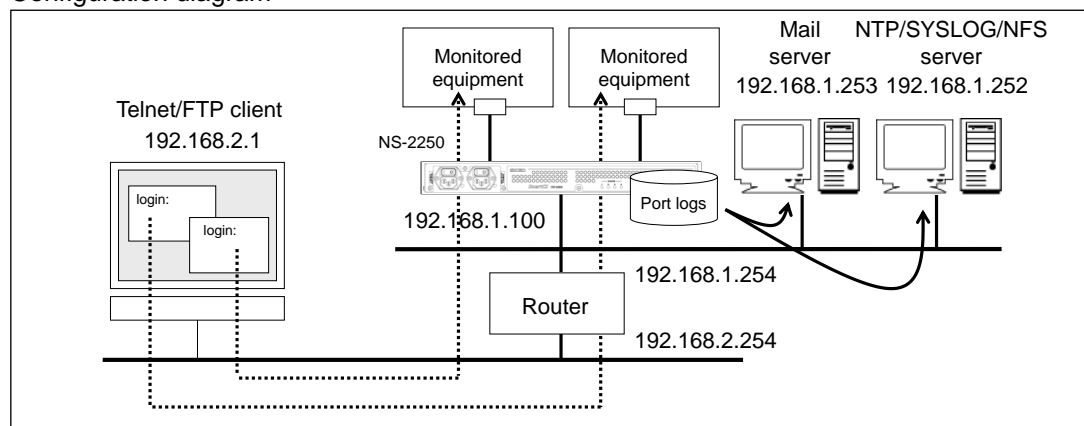
Figure 4-6 Configuration of port log transfer

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set syslog host 1 192.168.1.252 portlog_facility local0 syslog_facility local1
enable syslog

set nfs server 1 addr 192.168.1.252 path /mnt/nfslog
set nfs rotate 0 0 1 * *
enable nfs

set logd tstamp on interval 60
set logd tty 1 syslog on
set logd tty 1 sendlog mail interval 180 ratio 70
add logd tty 1 mail 1 mgr@example.co.jp 192.168.1.251

set logd tty 2 syslog on
set logd tty 2 sendlog mail interval 180 ratio 70
add logd tty 2 mail 1 user1@example.co.jp 192.168.1.251
set logd tty 2 mail 1 type body
set logd tty 2 mail 1 subject "Server Status"
set logd tty 2 mail 1 sender smartcs@example.co.jp

add logd tty 2 mail 2 user2@example.co.jp 192.168.1.251
set logd tty 2 mail 2 type body
set logd tty 2 mail 2 subject "Data-Center Server"
set logd tty 2 mail 2 sender smartcs@example.co.jp

set logd tty 3 syslog on
set logd tty 3 sendlog ftp interval 180 ratio 70
add logd tty 3 ftp 1 loguser1 192.168.1.252 password
(password entry)

set logd tty 4 syslog on
set logd tty 4 sendlog ftp interval 180 ratio 70
add logd tty 4 ftp 1 loguser1 192.168.1.252 password
(password entry)
add logd tty 4 ftp 2 loguser2 192.168.1.252 password
(password entry)

set logd tty 5 nfs on
set logd tty 6 nfs on
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to
    "192.168.1.100/24", and set the default route to "192.168.1.254".

    ```
    set hostname SmartCS
    set ipaddr eth1 192.168.1.100/24
    create ip route default gateway 192.168.1.254
    ```

2. Configure the syslog client of the NS-2250.
    Send to the syslog server (192.168.1.252) with the port log facility code of "local0" and
    the facility code of "local1" for syslog output by the NS-2250.
    After configuring the syslog client, carry out the "enable syslog" command to enable the
    syslog client.

    ```
    set syslog host 1 192.168.1.252 portlog_facility local0 syslog_facility local1
    enable syslog
    ```

3. Configure the NFS client of the NS-2250.
    Set the NFS server to "192.168.1.252", set the mount path of the NFS server to
    "/mnt/nfslog", and rotate logs saved to the NFS server at midnight on the first of each
    month.

    ```
    set nfs server 1 addr 192.168.1.252 path /mnt/nfslog
    set nfs rotate 0 0 1 * *
    enable nfs
    ```

4. Enable the time stamp function to add a time stamp to the port log every 60 seconds.

    ```
    set logd tstamp on interval 60
    ```

5. Set the syslog output of serial port 1 to on, and then configure the settings to send to the
    syslog server every time a message is output by monitored equipment. Furthermore,
    configure the settings to mail port logs periodically.
    With the following settings, a port log is sent to "mgr@example.co.jp" via the mail server
    (192.168.1.251) every 180 minutes or when the port-log size reaches 70% capacity.
    The subject of mails to be sent, the email address of the sender, and the sending
    method for port logs are reflected in the default settings. Port logs are sent as an email
    attachment file with the subject of "portlog TTY_number" and the email address of the
    sender of "portusr@NS-2250 host name.local domain".

    ```
    set logd tty 1 syslog on
    set logd tty 1 sendlog mail interval 180 ratio 70
    add logd tty 1 mail 1 mgr@example.co.jp 192.168.1.251
    ```

6. Set the syslog output of serial port 2 to on, and then configure the settings to send to the
    syslog server every time a message is output by monitored equipment. Furthermore,
    configure the settings to mail port logs periodically.
    With the following settings, a port log is sent to "user1@example.co.jp" and
    "user2@example.co.jp" via the mail server (192.168.1.251) every 180 minutes or when
    the port-log size reaches 70% capacity.
    Emails sent to "user1@example.co.jp" have the subject of "Server Status" and a sender

of "smartcs@example.co.jp".

Emails sent to "user2@example.co.jp" have the subject of "Data-Center Server" and a sender of "smartcs@example.co.jp".

Port logs are stored in the body of the mail when they are sent.

```
set logd tty 2 syslog on
set logd tty 2 sendlog mail interval 180 ratio 70
add logd tty 2 mail 1 user1@example.co.jp 192.168.1.251
set logd tty 2 mail 1 type body
set logd tty 2 mail 1 subject "Server Status"
set logd tty 2 mail 1 sender smartcs@example.co.jp
add logd tty 2 mail 2 user2@example.co.jp 192.168.1.251
set logd tty 2 mail 2 type body
set logd tty 2 mail 2 subject "Data-Center Server"
set logd tty 2 mail 2 sender smartcs@example.co.jp
```

7. Set the syslog output of serial port 3 to on, and then configure the settings to send to the syslog server every time a message is output by monitored equipment. Furthermore, configure the settings to send port logs by FTP periodically.
    With the following settings, a port log is sent by FTP as user "loguser1" to the FTP server (192.168.1.252) every 180 minutes or when the port-log size reaches 70% capacity.

```
set logd tty 3 syslog on
set logd tty 3 sendlog ftp interval 180 ratio 70
add logd tty 3 ftp 1 loguser1 192.168.1.252 password
(password entry)
```

8. Set the syslog output of serial port 4 to on, and then configure the settings to send to the syslog server every time a message is output by monitored equipment. Furthermore, configure the settings to send port logs by FTP periodically.
    With the following settings, a port log is sent by FTP as user "loguser1" and "loguser2" to the FTP server (192.168.1.252) every 180 minutes or when the port-log size reaches 70% capacity.

```
set logd tty 4 syslog on
set logd tty 4 sendlog ftp interval 180 ratio 70
add logd tty 4 ftp 1 loguser1 192.168.1.252 password
(password entry)
add logd tty 4 ftp 2 loguser2 192.168.1.252 password
(password entry)
```

9. Set the NFS output of serial port 5 and 6 to on, and then configure the settings to save to the NFS server every time a message is output by monitored equipment.

```
set logd tty 5 nfs on
set logd tty 6 nfs on
```

4.8.4 Change the port log location and size

This section describes the settings to change the location and save space of port logs.

|	
Port server setting	: Direct mode (default)
Method of connection nt	: Telnet Normal mode (default)
Port user authentication	: None (default)
Port log location	: FLASH (Change the port log size for each serial port)
Port log transfer function	: OFF(default)

Configuration diagram
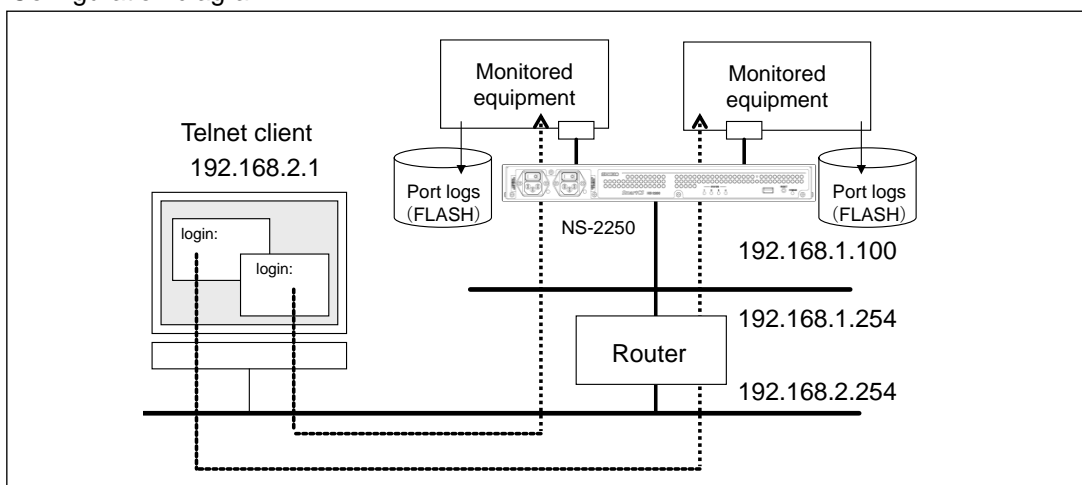
Figure 4-7 Change the port log location and size

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set logd output flash
set logd tty 1-4 log on size 500
set logd tty 5-8 log on size 1000
set logd tty 9-12 log on size 1500
set logd tty 13-16 log on size 2000
set logd tty 17-20 log on size 2500
set logd tty 21-24 log on size 3000
set logd tty 25-28 log on size 4000
set logd tty 29-32 log on size 8000
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to
   "192.168.1.100/24", and set the default route to "192.168.1.254".

        set hostname SmartCS
        set ipaddr eth1 192.168.1.100/24
        create ip route default gateway 192.168.1.254

2. Change the location of port logs from RAM to FLASH.

        set logd output flash

3. Configure the port log size for each serial port as shown below.

        Port log size for serial ports 1 to 4   :500 Kbyte
        Port log size for serial ports 5 to 8   :1 MByte
        Port log size for serial ports 9 to 12   :1.5 MByte
        Port log size for serial ports 13 to 16   :2 MByte
        Port log size for serial ports 17 to 20   :2.5 MByte
        Port log size for serial ports 21 to 24   :3 MByte
        Port log size for serial ports 25 to 28   :4 MByte
        Port log size for serial ports 29 to 32   :8 MByte

        set logd tty 1-4 log on size 500
        set logd tty 5-8 log on size 1000
        set logd tty 9-12 log on size 1500
        set logd tty 13-16 log on size 2000
        set logd tty 17-20 log on size 2500
        set logd tty 21-24 log on size 3000
        set logd tty 25-28 log on size 4000
        set logd tty 29-32 log on size 8000

4.8.5 Disable the port log function and control display of the port server menu

        Port server setting   : Direct mode (default)
        Method of connection   : Telnet Normal mode (default)
        Port server menu   : OFF
        Port user authentication   : None (default)
        Port log location   : None
        Port log transfer function   : OFF (default)

Configuration diagram
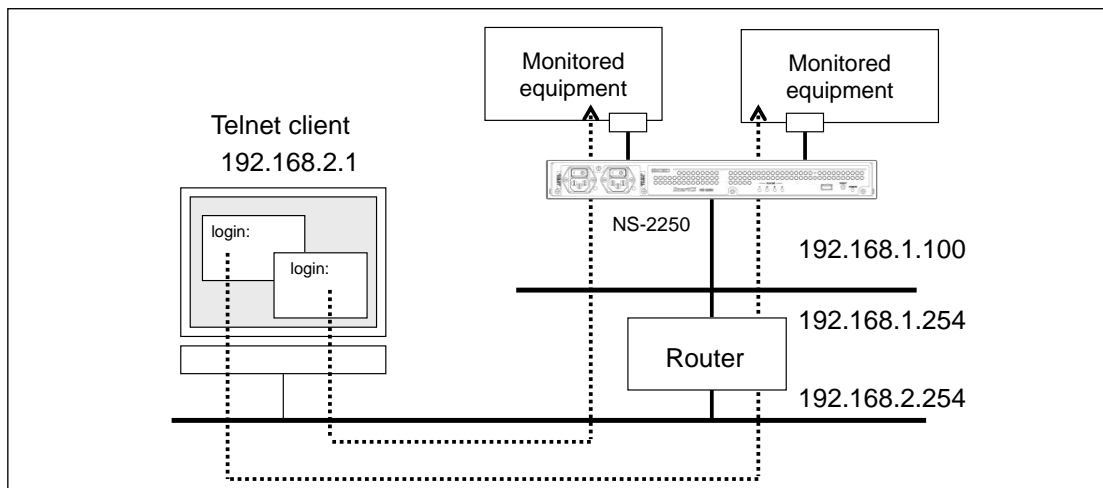
Figure4-8 Disable the port log function and controlling the display of the port server
menu

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254
set portd menu off
set logd output off
```

Explanation of settings
1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to
   "192.168.1.100/24", and set the default route to "192.168.1.254".
        set hostname SmartCS
        set ipaddr eth1 192.168.1.100/24
        create ip route default gateway 192.168.1.254

2. Control the display of the port server menu.
        set portd menu off

3. Disable the port log function
        set logd output off

4.8.6 Port user authentication

This section describes the settings to increase the security of serial ports by switching on the port user authentication function and limiting the serial ports that can be accessed by each port user.

    Port server setting   : Direct mode (default)
    Method of connection   : Telnet Normal mode (default)
    Port user authentication   : Yes (Login stamp function on)
    Port log location   : RAM(default)
    Port log transfer function : OFF(default)

Configuration diagram
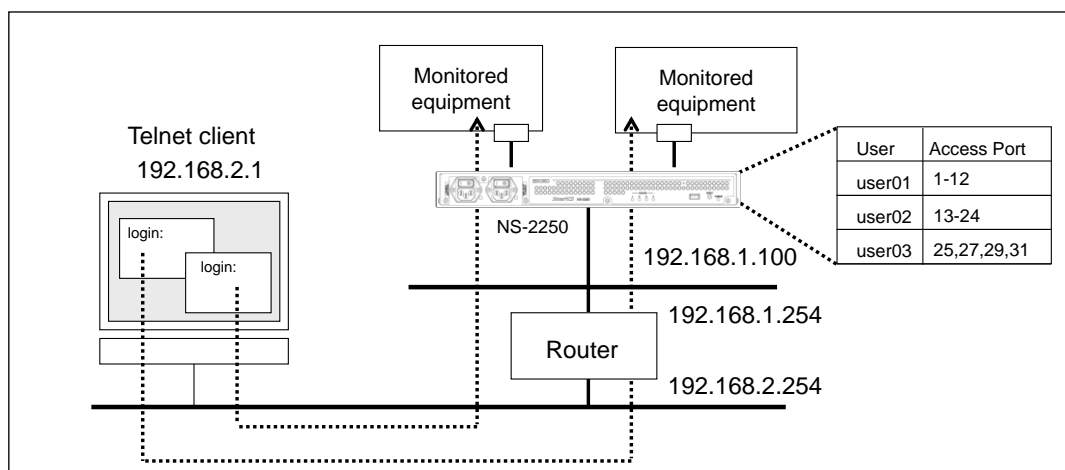
Figure4-9 Port user authentication

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set portd auth basic

create user user01 group portusr password
(password entry)
create user user02 group portusr password
(password entry)
create user user03 group portusr password
(password entry)

set user user01 port 1-12
set user user02 port 13-24
set user user03 port 25,27,29,31

set logd tty 1-32 lstamp on
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".

> set hostname SmartCS
> set ipaddr eth1 192.168.1.100/24
> create ip route default gateway 192.168.1.254

2. Switch on Port user authentication.

> set portd auth basic

3. Create port users (user01 to user03) to use port user authentication.

> create user user01 group portusr password
> (password entry)
> create user user02 group portusr password
> (password entry)
> create user user03 group portusr password
> (password entry)

4. Configure the serial ports that can be accessed by a port user.
   Configure the access privileges so that user01 can access serial port 1 through serial port 12, user02 can access serial port 13 through serial port 24, and user03 can access serial port 25, 27, 29, and 31.

> set user user01 port 1-12
> set user user02 port 13-24
> set user user03 port 25,27,29,31

5. Enable the login stamp to add the login/logout of port users who access serial port 1 through serial port 32 to port logs.

> set logd tty 1-32 lstamp on

If you specify the "port" option when carrying out the "create user" command, you can create a user and control serial ports with one command.

4.8.7 SSH password (basic) authentication

This section describes the basic settings to access monitored equipment from an SSH client via the NS-2250 using password (basic) authentication.
In this configuration example, telnet clients are also covered.

|	
Port server setting	: Direct mode (default)
Method of connection	: telnet/SSH Normal mode
SSH authentication	: Password (basic) authentication
Port user authentication	: Yes
Port log location	: RAM (default)
Port log transfer function	: OFF (default)
SSH server of NS-2250	: Enable

Configuration diagram
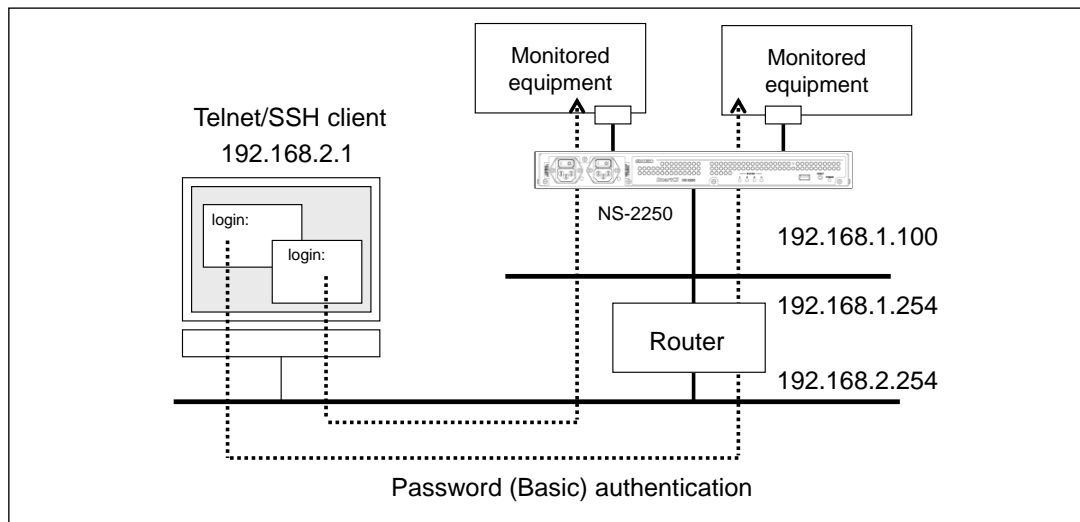
Figure 4-10 SSH password (basic) authentication

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set sshd auth basic
create allowhost all service portd sshrw all

set portd auth basic
create user user01 group portusr password
(password entry)
create user user02 group portusr password
(password entry)
create user user03 group portusr password
(password entry)

set user user01 port 1-32
set user user02 port 1-32
set user user03 port 1-32

enable sshd
create allowhost all service sshd
set user somebody password
(password entry)
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 P address to "192.168.1.100/24", and set the default route to "192.168.1.254".

> set hostname SmartCS
> set ipaddr eth1 192.168.1.100/24
> create ip route default gateway 192.168.1.254

2. Set the SSH authentication method to Password (basic) authentication, and then configure the settings to allow access to all serial ports in SSH Normal mode from all network addresses.

> set sshd auth basic
> create allowhost all service portd sshrw all

3. Switch on Port user authentication.

> set portd auth basic

4. Create port users (user01 to user03) to use port user authentication.

> create user user01 group portusr password
> (password entry)
> create user user02 group portusr password
> (password entry)
> create user user03 group portusr password
> (password entry)

5. Configure the serial ports that can be accessed by a port user.
   Configure the privileges so that user01 to user03 can access serial port 1 through 32.

   > set user user01 port 1-32
   > set user user02 port 1-32
   > set user user03 port 1-32

6. Configure the settings of the SSH server of the NS-2250 to allow login to the NS-2250 from an SSH client. Enable the SSH server of the NS-2250, and then configure the settings to allow access to the SSH server of the NS-2250 from all network addresses. Finally, configure the passwords of login users registered to the NS-2250.

   > enable sshd
   > create allowhost all service sshd
   > set user somebody password
   > (password entry)

Notes

The default settings of the NS-2250 are configured to allow access to the telnet server and port server of the NS-2250 from all networks. To delete telnet access and increase security, carry out the following commands.

> delete allowhost all service telnetd
> delete allowhost all service portd telrw all
> disable telnetd

4.8.8 SSH public key (public) authentication

In this configuration example, telnet clients are also covered.

Port server setting	: Direct mode (default)
Method of connection	: Telnet/SSH Normal mode
SSH server authentication	: Public key (public) authentication
Port user authentication	: Yes
Port log location	: RAM(default)
Port log transfer function	: OFF(default)
SSH server of NS-2250	: Enable

Configuration diagram
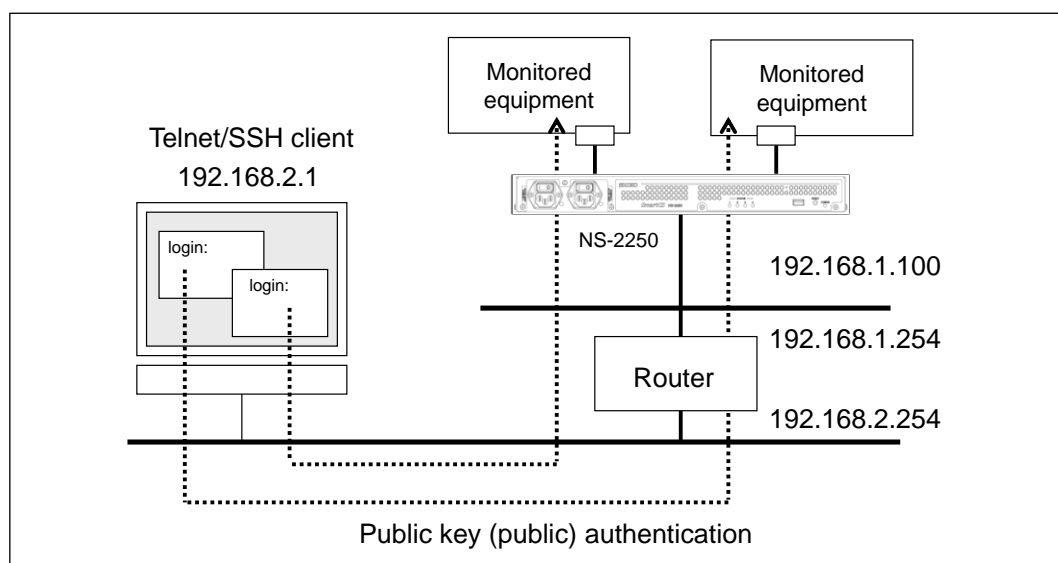
Figure 4-11 SSH public key (public) authentication

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set sshd auth public
create allowhost all service portd sshrw all

set portd auth basic
create user user01 group portusr password
(password entry)
create user user02 group portusr password
(password entry)
create user user03 group portusr password
(password entry)

set user user01 port 1-32
set user user02 port 1-32
set user user03 port 1-32

set user user01 sshkey public ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAv5Ic
URdW4mvc+FIAKxWxhv8mFaCM/Ro0Q4eVH+7uRV2hVuFpSndWivuCI0Gth7RHbVhUbkpdaz
OR9wtN265tPnmoDTHa3CHRzP17/6V4lmbHh0VNJjnDw730HKp0gnSZj0Udq1JrHXbPrKwd
pqcj7okZtlTxWHxPb2xmC8lu0= abcdef@test

set user user02 sshkey public ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAv5Ic
URdW4mvc+FIAKxWxhv8mFaCM/Ro0Q4eVH+7uRV2hVuFpSndWivuCI0Gth7RHbVhUbkpdaz
OR9wtN265tPnmoDTHa3CHRzP17/6V4lmbHh0VNJjnDw730HKp0gnSZj0Udq1JrHXbPrKwd
pqcj7okZtlTxWHxPb2xmC8lu0= abcdef@test

set user user03 sshkey public ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAv5Ic
URdW4mvc+FIAKxWxhv8mFaCM/Ro0Q4eVH+7uRV2hVuFpSndWivuCI0Gth7RHbVhUbkpdaz
OR9wtN265tPnmoDTHa3CHRzP17/6V4lmbHh0VNJjnDw730HKp0gnSZj0Udq1JrHXbPrKwd
pqcj7okZtlTxWHxPb2xmC8lu0= abcdef@test

enable sshd
create allowhost all service sshd
set user somebody password
(password entry)

set user somebody sshkey public ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAv5
IcURdW4mvc+FIAKxWxhv8mFaCM/Ro0Q4eVH+7uRV2hVuFpSndWivuCI0Gth7RHbVhUbkpd
azOR9wtN265tPnmoDTHa3CHRzP17/6V4lmbHh0VNJjnDw730HKp0gnSZj0Udq1JrHXbPrK
wdpqcj7okZtlTxWHxPb2xmC8lu0= abcdef@test
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to
   "192.168.1.100/24", and set the default route to "192.168.1.254".

   ```
   set hostname SmartCS
   set ipaddr eth1 192.168.1.100/24
   create ip route default gateway 192.168.1.254
   ```

2. Set the SSH authentication method to public key (public) authentication, and then
   configure the settings to allow access to all serial ports in SSH Normal mode from all
   network addresses.

   ```
   set sshd auth public
   create allowhost all service portd sshrw all
   ```

3. Switch on Port user authentication.

   ```
   set portd auth basic
   ```

4. Create port users (user01 to user03) to use port user authentication.

   ```
   create user user01 group portusr password
   (password entry)
   create user user02 group portusr password
   (password entry)
   create user user03 group portusr password
   (password entry)
   ```

5. Configure the serial ports that can be accessed by a port user.
   Configure the privileges so that user01 to user03 can access serial port 1 through 32.

   ```
   set user user01 port 1-32
   set user user02 port 1-32
   set user user03 port 1-32
   ```

6. Register the public key created by the SSH client for each port user.

   ```
   set user user01 sshkey public ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAv5Ic
   URdW4mvc+FIAKxWxhv8mFaCM/Ro0Q4eVH+7uRV2hVuFpSndWivuCI0Gth7R
   HbVhUbkpdazOR9wtN265tPnmoDTHa3CHRzP17/6V4lmbHh0VNJjnDw730HKp
   0gnSZj0Udq1JrHXbPrKwdpqcj7okZtlTxWHxPb2xmC8lu0= abcdef@test

   set user user02 sshkey public ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAv5Ic
   URdW4mvc+FIAKxWxhv8mFaCM/Ro0Q4eVH+7uRV2hVuFpSndWivuCI0Gth7R
   HbVhUbkpdazOR9wtN265tPnmoDTHa3CHRzP17/6V4lmbHh0VNJjnDw730HKp
   0gnSZj0Udq1JrHXbPrKwdpqcj7okZtlTxWHxPb2xmC8lu0= abcdef@test

   set user user03 sshkey public ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAv5Ic
   URdW4mvc+FIAKxWxhv8mFaCM/Ro0Q4eVH+7uRV2hVuFpSndWivuCI0Gth7R
   HbVhUbkpdazOR9wtN265tPnmoDTHa3CHRzP17/6V4lmbHh0VNJjnDw730HKp
   0gnSZj0Udq1JrHXbPrKwdpqcj7okZtlTxWHxPb2xmC8lu0= abcdef@test
   ```

7. Configure the settings of the SSH server of the NS-2250 to allow login to the NS-2250 from an SSH client. Enable the SSH server of the NS-2250, and then configure the settings to allow access to the SSH server of the NS-2250 from all network addresses. Finally, configure the passwords of login users registered to the NS-2250.

```
enable sshd
create allowhost all service sshd
set user somebody password
(password entry)
```

8. Register the public key created by the SSH client for users (somebody) of the NS-2250.

```
set user somebody sshkey public ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAv5IcURdW4mvc+FIAKxWxhv8mFaCM/Ro
0Q4eVH+7uRV2hVuFpSndWivuCI0Gth7RHbVhUbkpdazOR9wtN265tPnmoDTH
a3CHRzP17/6V4lmbHh0VNJjnDw730HKp0gnSZj0Udq1JrHXbPrKwdpqcj7okZtlT
xWHxPb2xmC8lu0= abcdef@test
```

Notes
The default settings of the NS-2250 are configured to allow access to the telnet server and port server of the NS-2250 from all network addresses. To delete telnet access and increase security, carry out the following commands.

```
delete allowhost all service telnetd
delete allowhost all service portd telrw all
disable telnetd
```

4.8.9 Configure the port selection function (Select mode of the port server)

This section describes the settings of the port selection function.

Port server setting   : Select mode
Method of connection   : Telnet Normal mode (default)
Port user authentication   : Yes
Port log location   : RAM (default)
Port log transfer function   : OFF (default)

Configuration diagram
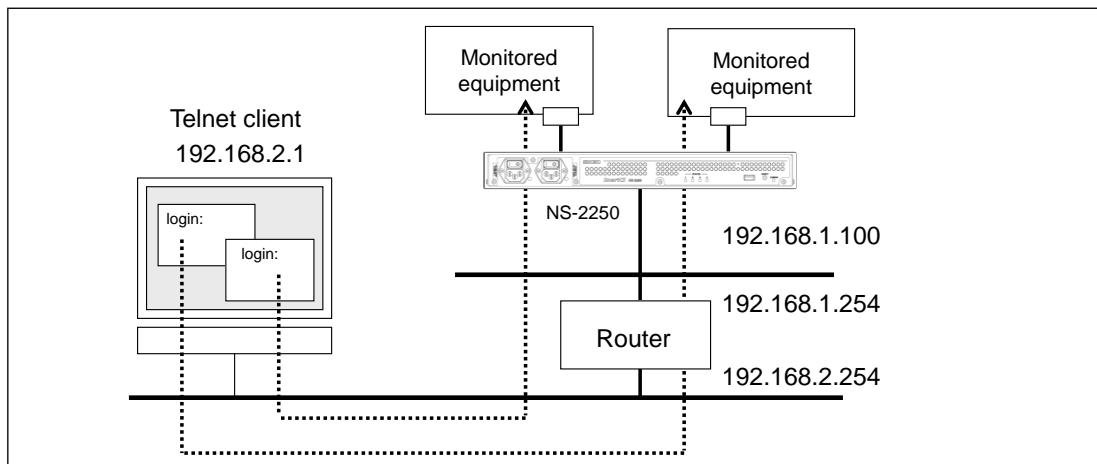
Figure 4-12 Port selection function (Select mode of the port server)

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set portd connect select

set portd auth basic
create user user01 group portusr port 1-32 password
(password entry)
create user user01 group portusr port 1-32 password
(password entry)

set portd tty 1-32 cmdchar 01
set portd tty 1 label Tokyo-L3SW-1
set portd tty 2 label Tokyo-L3SW-2
set portd tty 3 label Tokyo-L3SW-3
set portd tty 4 label Tokyo-L3SW-4
set portd tty 5 label Tokyo-SV-1
set portd tty 6 label Tokyo-SV-2
set portd tty 7 label Tokyo-SV-3
set portd tty 8 label Tokyo-SV-4
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".

> set hostname SmartCS
> set ipaddr eth1 192.168.1.100/24
> create ip route default gateway 192.168.1.254

2. Enable the port selection function. Change the port server connection mode to "select".

> set portd connect select

3. Switch on port user authentication.

> set portd auth basic

4. Create port users (user01 and user02) to use port user authentication.
   Configure the access privileges for serial port 1 through serial port 32 for port users.

> create user user01 group portusr port 1-32 password
> (password entry)
> create user user02 group portusr port 1-32 password
> (password entry)

5. Register "0x01" (Ctrl+A) as the session suspension character code of the port server menu for serial port 1 through serial port 32.

> set portd tty 1-32 cmdchar 01

6. Register the label for each serial port.

> set portd tty 1 label Tokyo-L3SW-1
> set portd tty 2 label Tokyo-L3SW-2
> set portd tty 3 label Tokyo-L3SW-3
> set portd tty 4 label Tokyo-L3SW-4
> set portd tty 5 label Tokyo-SV-1
> set portd tty 6 label Tokyo-SV-2
> set portd tty 7 label Tokyo-SV-3
> set portd tty 8 label Tokyo-SV-4

4.8.10 Configure the RADIUS authentication/accounting function (basic settings)

This section describes the basic settings to centrally manage port users that access the serial ports of the NS-2250 by using the RADIUS authentication/accounting server.

Port server setting : Direct mode (default)
Method of connection : Telnet Normal mode (default)
Port user authentication : Yes
Port log location : RAM (default)
Port log transfer function : OFF (default)
Authentication/accounting protocol: RADIUS
Use RADIUS authentication for port users only.
(Normal users and device management users are authenticated by local authentication)

Configuration diagram

Monitored equipment
Monitored equipment
RADIUS server1
192.168.1.252
RADIUS server2
192.168.1.253

Telnet/SSH client
192.168.2.1

login:
login:

NS-2250

192.168.1.100

192.168.1.254

Router

192.168.2.254

Figure 4-13 RADIUS authentication / accounting function (basic configuration)

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set user root password
(password entry)
set  user somebody password
(password entry)

set portd auth basic
set auth mode radius
set auth radius server 1 addr 192.168.1.252
set auth radius server 1 key password
(Secret key entry)
set auth radius server 2 addr 192.168.1.253
set auth radius server 2 key password
(Secret key entry)

set acct mode radius
set acct radius server 1 addr 192.168.1.252
set acct radius server 1 key password
(Secret key entry)
set acct radius server 2 addr 192.168.1.253
set acct radius server 2 key password
(Secret key entry)
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".

        set hostname SmartCS
        set ipaddr eth1 192.168.1.100/24
        create ip route default gateway 192.168.1.254

2. Normal users and device management users are authenticated by local authentication. Set a password for normal users "somebody" and device management users "root".

        set   user somebody password
        (password entry)
        set user root password
        (password entry)

3. Enable Port user authentication.

        set portd auth basic

4. Configure the authentication method and RADIUS authentication client. Set RADIUS server 1 to "192.168.1.252" and RADIUS server 2 to "192.168.1.253". For the authentication port, use the default of "1812".

        set auth mode radius
        set auth radius server 1 addr 192.168.1.252
        set auth radius server 2 addr 192.168.1.253

5. Register the secret key to be used by the RADIUS authentication client. Configure the secret key that was registered to the RADIUS authentication server.

        set auth radius server 1 key password
        (Secret key entry)
        set auth radius server 2 key password
        (Secret key entry)

6. Configure the accounting method and RADIUS accounting client. Set RADIUS server 1 to "192.168.1.252" and RADIUS server 2 to "192.168.1.253". For the accounting port, use the default of "1813".

        set acct mode radius
        set acct radius server 1 addr 192.168.1.252
        set acct radius server 2 addr 192.168.1.253

7. Register the secret key to be used by the RADIUS accounting client. Configure the secret key that was registered to the RADIUS accounting server.

        set acct radius server 1 key password
        (Secret key entry)
        set acct radius server 2 key password
        (Secret key entry)

RADIUS server settings

This section lists examples of attributes to be set to the user definition file of the RADIUS server.
The maximum length of a RADIUS user name that can be authenticated by the NS-2250 is 64 characters.

```
# Port user (user01)
user01 Password = "user01",

# Port user (user02)
user02 Password = "user02",
```

Note that the NS-2250 interprets only User-Name and Filter-Id of the received attributes. Accordingly, the connection is possible with the following attributes as well.

```
# Port user (user01)
user01 Password = "user01",
        Service-Type = Framed-User,
        Framed-Protocol = PPP,
        Idle-Timeout = 600

# Port user (user02)
user02 Password = "user02",
        Service-Type = Login,
        Login-Service = Telnet,
```

For details of attributes, see Appendix B, "Examples of attributes and RADIUS authentication/accounting server settings".

If the "create auth access_group" command or "set auth radius server {normal | root | portusr } filter_id_head" command to identify user groups has not to be carried out for the NS-2250, user authentication processing is carried out according to the setting value of the "set auth radius def_user" command. If the "set auth radius def_user" command has not been configured, users authenticated by the RADIUS authentication server for which the user group cannot be identified are treated as port users, and they are given privileges that allow access to all serial ports. If the "set auth radius def_user none" command has been configured, access is refused for the user in question.

To authenticate normal users and device management users by using the RADIUS authentication server or to configure serial ports to allow access for port users, see the following sections: Section 4.8.11, "Configure the RADIUS authentication function/RADIUS accounting function (applied setting 1: filter_id_head)" and Section 4.8.12, "Configure the RADIUS authentication function/RADIUS accounting function (applied setting 2: access grouping function)".

4.8.11 Configure the RADIUS authentication client function/RADIUS accounting client function (case 1: filter_id_head)

This section describes the settings to centrally manage users that access the NS-2250 by using the RADIUS authentication server/RADIUS accounting server.

This example list settings to determine whether the user in question is a device management user, normal user, or port user by the Filter-Id attribute value to be sent from the authentication server after user authentication by the RADIUS authentication server. Configuring these settings is useful when the serial ports that can be accessed by each port user can be fixed. (For example, user1 can access serial ports 1 through 10, user2 can access serial ports 20 through 30, and so on.) Configure access control of serial ports for each port user as Filter-Id attribute values at the RADIUS authentication server.

Port server setting	: Direct mode (default)
Method of connection	: Telnet Normal mode (default)
Port user authentication	: Yes
Port log location	: RAM(default)
Port log transfer function	: OFF(default)
Authentication/accounting protocol	: RADIUS
	Use RADIUS authentication for all users.
	Configure the access privileges for serial ports at the RADIUS authentication server.
	Refuse access to users for which a user group cannot be identified.

Configuration diagram
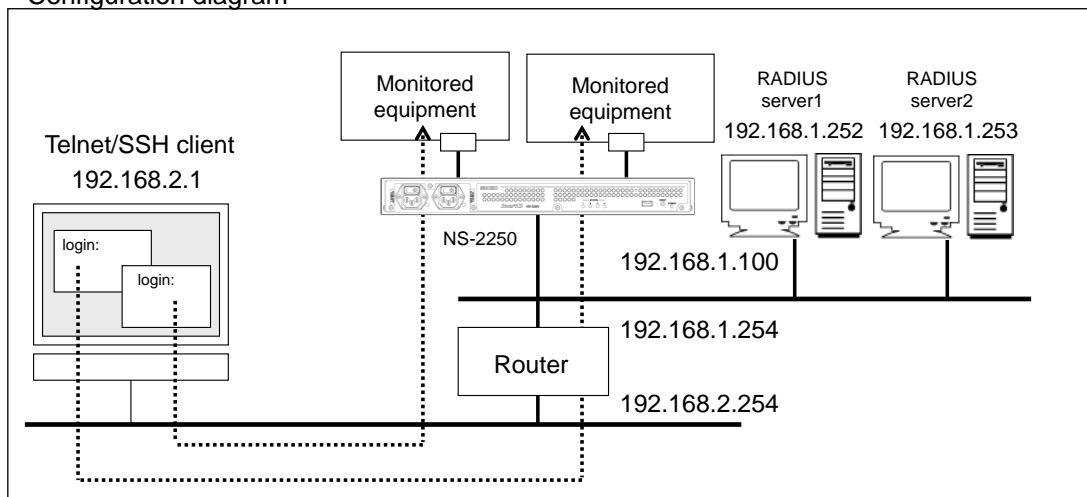
Figure 4-14 RADIUS authentication / accounting function (filter_id_head)

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set portd auth basic

set auth mode radius
set auth radius retry 5

set auth radius server 1 addr 192.168.1.252
set auth radius server 1 port 1645
set auth radius server 1 timeout 10
set auth radius server 1 key password
(Secret key entry)
set auth radius server 1 portusr filter_id_head NS2250_PORT
set auth radius server 1 normal filter_id_head NS2250_NORMAL
set auth radius server 1 root filter_id_head NS2250_ROOT

set auth radius server 2 addr 192.168.1.253
set auth radius server 2 port 1645
set auth radius server 2 timeout 10
set auth radius server 2 key password
(Secret key entry)
set auth radius server 2 portusr filter_id_head NS2250_PORT
set auth radius server 2 normal filter_id_head NS2250_NORMAL
set auth radius server 2 root filter_id_head NS2250_ROOT
set auth radius def_user none

set acct mode radius
set acct radius retry 5

set acct radius server 1 addr 192.168.1.252
set acct radius server 1 port 1646
set acct radius server 1 timeout 10
set acct radius server 1 key password
(Secret key entry)

set acct radius server 2 addr 192.168.1.253
set acct radius server 2 port 1646
set acct radius server 2 timeout 10
set acct radius server 2 key password
(Secret key entry)
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".

        set hostname SmartCS
        set ipaddr eth1 192.168.1.100/24
        create ip route default gateway 192.168.1.254

2. Enable Port user authentication.

        set portd auth basic

3. Configure the authentication method and RADIUS authentication client. Set RADIUS server 1 to "192.168.1.252" and RADIUS server 2 to "192.168.1.253". Set the authentication port to 1645.

        set auth mode radius
        set auth radius server 1 addr 192.168.1.252
        set auth radius server 2 addr 192.168.1.253
        set auth radius server 1 port 1645
        set auth radius server 2 port 1645

4. Register the secret key to be used by the RADIUS authentication client. Configure the secret key that was registered to the RADIUS authentication server.

        set auth radius server 1 key password
        (Secret key entry)
        set auth radius server 2 key password
        (Secret key entry)

5. Configure the retry/timeout values for the RADIUS authentication client. Configure retries to 5 times and timeout to 10 seconds.

        set auth radius retry 5
        set auth radius server 1 timeout 10
        set auth radius server 2 timeout 10

6. Register the user identifiers to identify normal users and device management users. Carry out the "set auth radius normal/set auth radius root" command so that normal users and device management users are identified when the front of the character string of the Filter-ID attribute to be sent from the RADIUS authentication server is "NS2250_NORMAL" or "NS2250_ROOT", respectively.

        set auth radius server 1 normal filter_id_head NS2250_NORMAL
        set auth radius server 1 root filter_id_head NS2250_ROOT
        set auth radius server 2 normal filter_id_head NS2250_NORMAL
        set auth radius server 2 root filter_id_head NS2250_ROOT

7. Register the user identifier to identify port users. Carry out the "set auth radius server portusr" command so that port users are identified when the front of the character string of the Filter-ID attribute to be sent from the RADIUS authentication server is "NS2250_PORT".

        set auth radius server 1 portusr filter_id_head NS2250_PORT
        set auth radius server 2 portusr filter_id_head NS2250_PORT

To configure the serial ports to which a port user can access (1-16, 24), configure the Filter-ID attribute value at the RADIUS authentication server to "NS2250_PORT1-16,24". If the number is not listed, as in "NS2250_PORT", the NS-2250 gives access privileges to all serial ports.

8. Configure access methods for users for which a user group cannot be identified.
   Carry out the "set auth radius def_user" command so that users for which a user group cannot be identified are refused access (for example, when the Filter-ID attribute is not sent from the RADIUS authentication server or when the Filter-ID attribute value is in a format that the NS-2250 cannot recognize).

   ```
   set auth radius def_user none
   ```

9. Configure the accounting method and RADIUS accounting client.
   Set RADIUS server 1 to "192.168.1.252" and RADIUS server 2 to "192.168.1.253".
   Set the accounting port to "1646".

   ```
   set acct mode radius
   set acct radius server 1 addr 192.168.1.252
   set acct radius server 2 addr 192.168.1.253
   set acct radius server 1 port 1646
   set acct radius server 2 port 1646
   ```

10. Register the secret key to be used by the RADIUS accounting client.
    Configure the secret key that was registered to the RADIUS accounting server.

    ```
    set acct radius server 1 key password
    (Secret key entry)
    set acct radius server 2 key password
    (Secret key entry)
    ```

Notes

The NS-2250 performs user authentication in the following order: local authentication within the NS-2250 → RADIUS authentication.

When normal users undergo RADIUS authentication, either delete normal users registered to the NS-2250 or configure a password different from the password registered to the RADIUS server. Be aware that when a password is not registered for normal users, simply pressing the Return key for the password makes it possible to pass local authentication of the NS-2250 and log in.

The result is the same as when logging in as a device management user or carrying out the "su" command. Configure a password different from the password registered to the RADIUS server for device management users. Note that, unlike normal users, device management users (root) cannot be deleted.

RADIUS server settings

This section lists examples of attributes to be set to the user definition file of the RADIUS authentication server.
The maximum length of a RADIUS user name that can be authenticated by the NS-2250 is 64 characters.

```
# Port user registration

portuser01 Password = "portuser01",
      Filter-Id = "NS2250_PORT1-16",
      # Permit access to serial ports (1 to 16)

portuser02 Password = "portuser02",
      Filter-Id = "NS2250_PORT5-9,20,24",
      # Permit access to serial ports (5 to 9, 20, 24)

portuser03 Password = "portuser03",
      # In this case, this user is refused access because
      # the setting of the NS-2250 is "set auth radius def_user none"
      and the user type cannot be identified.


# Normal user registration

somebody Password = "network",
      Filter-Id = "NS2250_NORMAL",

abc01 Password = "abcdef",
      Filter-Id = "NS2250_NORMAL",

# Device management user

root Password = "admin",
      Filter-Id = "NS2250_ROOT",
```

Note that of the attributes received by the NS-2250, only a Username and Filter-ID are interpreted. Accordingly, the connection is possible with the following attributes as well.

```
# Port user registration

portuser01 Password = "portuser01",
        Service-Type = Framed-User,
        Framed-Protocol = PPP,
        Idle-Timeout = 600,
        Filter-Id = "NS2250_PORT1-16"
        # Permit access to serial ports (1 to 16)

portuser02 Password = "portuser02",
        Service-Type = Framed-User,
        Framed-Protocol = PPP,
        Idle-Timeout = 600,
        Filter-Id = "NS2250_PORT5-9,20,24"
        Filter-Id = "access.include.filter-A"
        # Permit access to serial ports (5 to 9, 20, 24)

portuser03 Password = "portuser03",
        Idle-Timeout = 600
        # In this case, this user is refused access because
        # the setting of the NS-2250 is "set auth radius def_user none"
        and the user type cannot be identified.


# Normal user registration

somebody Password = "network",
        Service-Type = Login,
        Login-Service = Telnet,
        Filter-Id = "NS2250_NORMAL"

abc01 Password = "abcdef",
        Service-Type = Login,
        Login-Service = Telnet,
        Filter-Id = "NS2250_NORMAL"


# Device management user

root Password = "admin",
        Filter-Id = "NS2250_ROOT",
        Idle-Timeout = 600
```

For details of attributes, see Appendix B, "Examples of attributes and RADIUS authentication/accounting server settings".

4.8.12 Configure the RADIUS authentication function/RADIUS accounting function
     (case 2: access grouping function)

This section describes the settings to centrally manage users that access the NS-2250 by using an access grouping function with the RADIUS authentication/accounting server.

This example lists settings to determine the access group to which the user in question belongs and whether the user is a device management user, normal user, or port user by the Filter-Id attribute value to be sent from the authentication server after user authentication by the RADIUS authentication server.
Configuring this setting is useful when the serial ports that can be accessed by port users are different for each SmartCS. (For example, User 1 can access serial ports 1 through 10 on the SmartCS1, serial ports 15 through 20 on the SmartCS2, etc.) Use this method to configure the access privileges to serial ports for the port user access group to the NS-2250.

    Port server setting   : Direct mode (default)
    Method of connection   : Telnet Normal mode (default)
    Port user authentication   : Yes
    Port log location   : RAM (default)
    Port log transfer function   : OFF (default)
    Authentication/accounting protocol   : RADIUS
                                 Use RADIUS authentication for all users.
                                 Configure the access privileges to serial ports for the
                                 port user access group to the NS-2250.
                                 Refuse access to users for which a user group
                                 cannot be identified.

Configuration diagram

Figure 4-15 RADIUS authentication/accounting function (access grouping)

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set portd auth basic

set auth mode radius
set auth radius retry 5

set auth radius server 1 addr 192.168.1.252
set auth radius server 1 port 1645
set auth radius server 1 timeout 10
set auth radius server 1 key password
(Secret key entry)

set auth radius server 2 addr 192.168.1.253
set auth radius server 2 port 1645
set auth radius server 2 timeout 10
set auth radius server 2 key password
(Secret key entry)

create auth access_group root radius filter_id admin_grp
create auth access_group normal radius filter_id normal_grp
create auth access_group portusr port 1-16,24 radius filter_id grp1
create auth access_group portusr port 20-32 radius filter_id grp2
set auth radius def_user none

set acct mode radius
set acct radius retry 5

set acct radius server 1 addr 192.168.1.252
set acct radius server 1 port 1646
set acct radius server 1 timeout 10
set acct radius server 1 key password
(Secret key entry)

set acct radius server 2 addr 192.168.1.253
set acct radius server 2 port 1646
set acct radius server 2 timeout 10
set acct radius server 2 key password
(Secret key entry)
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".
    ```
    set hostname SmartCS
    set ipaddr eth1 192.168.1.100/24
    create ip route default gateway 192.168.1.254
    ```

2. Enable Port user authentication.
    ```
    set portd auth basic
    ```

3. Configure the authentication method and RADIUS authentication client.
    Set RADIUS server 1 to "192.168.1.252" and RADIUS server 2 to "192.168.1.253".
    Set the authentication port to 1645.
    ```
    set auth mode radius
    set auth radius server 1 addr 192.168.1.252
    set auth radius server 2 addr 192.168.1.253
    set auth radius server 1 port 1645
    set auth radius server 2 port 1645
    ```

4. Register the secret key to be used by the RADIUS authentication client.
    Configure the secret key that was registered to the RADIUS authentication server.
    ```
    set auth radius server 1 key password
    (Secret key entry)
    set auth radius server 2 key password
    (Secret key entry)
    ```

5. Configure the retry times/timeout values for the RADIUS authentication client.
    Configure retries to 5 times and timeout to 10 seconds.
    ```
    set auth radius retry 5
    set auth radius server 1 timeout 10
    set auth radius server 2 timeout 10
    ```

6. Register access groups to identify normal users and device management users. Carry out the "create auth access_group" command so that normal users and device management users are identified when the Filter-ID attribute to be sent from the RADIUS authentication server is "normal_grp" or "admin_grp", respectively.
    ```
    create auth access_group normal radius filter_id normal_grp
    create auth access_group root radius filter_id admin_grp
    ```

7. Register the access group to identify port users.
    Carry out the "create auth access_group" command so that port users are identified and access is allowed to serial ports (1 to 16, 24) when the Filter-ID attribute to be sent from the RADIUS authentication server is "grp1". In the same manner, configure to allow access to serial ports (20 to 32) when the access group is "grp2".
    ```
    create auth access_group portusr port 1-16,24 radius filter_id grp1
    create auth access_group portusr port 20-32 radius filter_id grp2
    ```

8. Configure authentication processing for users for which an access group cannot be identified.

Carry out the "set auth radius def_user" command so that users for which an access group cannot be identified are refused access (for example, when the Filter-ID attribute is not sent from the RADIUS authentication server or when the Filter-ID attribute character string and the access group registered to the SmartCS do not match).

    set auth radius def_user none

9. Configure the accounting method and RADIUS accounting client.

Set RADIUS server 1 to "192.168.1.252" and RADIUS server 2 to "192.168.1.253". Set the accounting port to "1646".

    set acct mode radius
    set acct radius server 1 addr 192.168.1.252
    set acct radius server 2 addr 192.168.1.253
    set acct radius server 1 port 1646
    set acct radius server 2 port 1646

10. Register the secret key to be used by the RADIUS accounting client.

Configure the secret key that was registered to the RADIUS accounting server.

    set acct radius server 1 key password
    (Secret key entry)
    set acct radius server 2 key password
    (Secret key entry)

Notes

The NS-2250 performs user authentication in the following order: local authentication within the NS-2250 → RADIUS authentication.

When normal users undergo RADIUS authentication, either delete normal users registered to the NS-2250 or configure a password different from the password registered to the RADIUS server. Be aware that when a password is not registered for normal users, simply pressing the Return key for the password makes it possible to pass local authentication of the NS-2250 and log in.

The result is the same as when logging in as a device management user or carrying out the "su" command. Configure a password different from the password registered to the RADIUS server for device management users. Note that, unlike normal users, device management users (root) cannot be deleted.

RADIUS server settings

This section lists examples of attributes to be set to the user definition file of the RADIUS authentication server.

The maximum length of a RADIUS user name that can be authenticated by the NS-2250 is 64 characters.

```
# Port user registration

portuser01 Password = "portuser01",
       Filter-Id = "grp1",
       # Permit access to serial ports (1 to 16, 24)

portuser02 Password = "portuser02",
       Filter-Id = "grp2",
       # Permit access to serial ports (20 to 32)

portuser03 Password = "portuser03",
       # In this case, this user is refused access because the setting
       of the NS-2250 is "set auth radius def_user none" and the user
       type cannot be identified.


# Normal user registration

somebody Password = "network",
       Filter-Id = "normal_grp",

abc01 Password = "abcdef",
       Filter-Id = "normal_grp",

# Device management user

root Password = "root",
       Filter-Id = "admin_grp",

manager1 Password = "manager1",
       Filter-Id = "admin_grp",

suzuki Password = "suzuki",
       Filter-Id = "admin_grp",
```

For details of attributes, see Appendix B, "Examples of attributes and RADIUS authentication/accounting server settings".

4.8.13 Configure the TACACS+ function (basic settings)

This section describes the basic settings to centrally manage port users that access the serial ports of the NS-2250 by using the TACACS+ server.

Port server setting	: Direct mode (default)
Method of connection	: Telnet Normal mode (default)
Port user authentication	: Yes
Port log location	: RAM (default)
Port log transfer function	: OFF (default)
Authentication/accounting protocol	: TACACS+

Use TACACS+ authentication for port users only.
(Normal users and device management users are
authenticated by local authentication)

Configuration diagram

Figure 4-16 TACACS+ function (basic configuration)

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254

set user root password
```
(password entry)
```
set  user somebody password
```
(password entry)

```
set portd auth basic

set auth mode tacacs
set auth tacacs server 1 addr 192.168.1.252
set auth tacacs server 1 key password
```
(Secret key entry)
```
set auth tacacs server 2 addr 192.168.1.253
set auth tacacs server 2 key password
```
(Secret key entry)

```
set acct mode tacacs
set acct tacacs server 1 addr 192.168.1.252
set acct tacacs server 1 key password
```
(Secret key entry)
```
set acct tacacs server 2 addr 192.168.1.253
set acct tacacs server 2 key password
```
(Secret key entry)

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".

        set hostname SmartCS
        set ipaddr eth1 192.168.1.100/24
        create ip route default gateway 192.168.1.254

2. Normal users and device management users are authenticated by local authentication. Set a password for normal users "somebody" and device management users "root".

        set user somebody password
        (password entry)
        set user root password
        (password entry)

3. Enable Port user authentication.

        set portd auth basic

4. Configure TACACS+ authentication/approval.
   In the following example, TACACS+ server 1 is set to "192.168.1.252" and TACACS+ server 2 is set to "192.168.1.253".
   Configure the secret key that was registered to the TACACS+ server.

        set auth mode tacacs
        set auth tacacs server 1 addr 192.168.1.252
        set auth tacacs server 1 key password
        (Secret key entry)
        set auth tacacs server 2 addr 192.168.1.253
        set auth tacacs server 2 key password
        (Secret key entry)

5. Configure TACACS+ accounting.
   In the following example, TACACS+ server 1 is set to "192.168.1.252" and TACACS+ server 2 is set to "192.168.1.253".
   Configure the secret key that was registered to the TACACS+ server.

        set acct mode tacacs
        set acct tacacs server 1 addr 192.168.1.252
        set acct tacacs server 1 key password
        (Secret key entry)
        set acct tacacs server 2 addr 192.168.1.253
        set acct tacacs server 2 key password
        (Secret key entry)

TACACS+ server settings

The following section lists a configuration example for the free TACACS+ server of Shrubbery Networks, Inc. (examples of attributes to be configured to the user definition file).

After TACACS+ user authentication was successful, the NS-2250 sends an attribute (service=smartcs) to the TACACS+ server and then carries out approval. With the following configuration, the service attribute is not checked at the TACACS+ server, and access is permitted as long as the ID and password match. In this configuration example, an authenticated user is treated as a port user with the default settings of the NS-2250 (set auth tacacs def_user portuser) because the user type has not been configured to the TACACS+ server.
The maximum length of a TACACS+ user name that can be authenticated by the NS-2250 is 64 characters.

```
accounting file = /var/log/tac_plus.acct

# Port user (user01)
user = user01
      default service = permit
      login = cleartext "user01"

# Port user (user02)
user = user02
      default service = permit
      login = cleartext "user02"
```

You can manage by using a one user definition even when various NS-2250 units are used if you configure the attribute and value pair to be sent as a reply to the NS-2250 for each service attribute.
The attribute to be returned to the NS-2250 (grp=port in this example) must be configured to the NS-2250 in advance. If the NS-2250 receives an unregistered attribute, the received attribute is ignored.

```
# Port user (user01)
user = user01
      login = cleartext "user01"
      service = smartcs {
         grp = port
      }
      service = PPP {
         grp = abc
      }
```

A TACACS+ server can also return multiple attributes to the NS-2250.
Be aware that the free TACACS+ server of Shrubbery Networks, Inc. cannot return multiple instances of the same attribute name. To return multiple attributes, change the attributes (grp, attr1, attr2, etc.) on the left side as shown in the example below.

```
# Port user (user02)
     login = cleartext "user02"
     service = smartcs {
         grp = port
         attr1 = def
         attr2 = xyz
     }
```

When the "create auth access_group" command, which identifies user groups, has not been configured to the NS-2250, user authentication processing is carried out according to the setting value of the "set auth tacacs def_user" command. If the "set auth tacacs def_user" command has not been configured, of users authenticated by the TACACS+ authentication server, users for which the user group cannot be identified are treated as port users, and they are given privileges that allow access to all serial ports. If this setting is "normal", users for which the user group cannot be identified are treated as normal users. If this setting is "none", the user in question is denied access.

To authenticate normal users and device management users by using the TACACS+ server or to configure the serial ports to which port users are allowed access, see Section 4.8.14, "Configure the TACACS+ function" on the next and following pages.

4.8.14 Configure the TACACS+ function (access grouping function)

This section describes the settings to centrally manage users that access the NS-2250 by using an access grouping function with the TACACS+ server.

This example lists settings to determine the access group to which the user in question belongs (device management user, normal user, or port user) and the access privileges to serial ports of port users by the attribute and value pair to be sent from the TACACS+ server after user authentication by the TACACS+ server.

Configuring this setting is useful when the serial ports that can be accessed by port users are different for each SmartCS. (For example, User 1 can access serial ports 1 through 10 on the SmartCS1, serial ports 15 through 20 on the SmartCS2, etc.) Use this method to configure the access privileges to serial ports for the port user access group to the NS-2250.

Port server setting	: Direct mode (default)
Method of connection	: Telnet Normal mode (default)
Port user authentication	: Yes
Port log location	: RAM (default)
Port log transfer function	: OFF (default)
Authentication/accounting protocol	: TACACS+
	Use TACACS+ authentication for all users.
	Configure the access privileges to serial ports for the port user access group to the NS-2250.
	Refuse access to users for which a user group cannot be identified.

Configuration diagram

Figure 4-17 TACACS+ function (access grouping)

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254


set portd auth basic


set auth mode tacacs
set auth su_cmd username admin
set auth tacacs server 1 addr 192.168.1.252
set auth tacacs server 1 timeout 10
set auth tacacs server 1 key password
(Secret key entry)
set auth tacacs server 2 addr 192.168.1.253
set auth tacacs server 2 timeout 10
set auth tacacs server 2 key password
(Secret key entry)


set acct mode tacacs
set acct tacacs server 1 addr 192.168.1.252
set acct tacacs server 1 timeout 10
set acct tacacs server 1 key password
(Secret key entry)
set acct tacacs server 2 addr 192.168.1.253
set acct tacacs server 2 timeout 10
set acct tacacs server 2 key password
(Secret key entry)


create auth access_group root tacacs attr grp val admin_grp
create auth access_group normal tacacs attr grp val normal_grp
create auth access_group portusr port 1-16,24 tacacs attr grp val grp1
create auth access_group portusr port 20-32 tacacs attr grp val grp2
set auth tacacs def_user none
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".
   ```
   set hostname SmartCS
   set ipaddr eth1 192.168.1.100/24
   create ip route default gateway 192.168.1.254
   ```

2. Enable Port user authentication.
   ```
   set portd auth basic
   ```

3. Configure TACACS+ authentication/approval.
   In the following example, TACACS+ server 1 is set to "192.168.1.252" and TACACS+ server 2 is set to "192.168.1.253". Configure the timeout to 10 seconds.
   Configure the secret key that was registered to the TACACS+ server.
   When the "su" command to transition to a device management user has been carried out, authentication with the TACACS+ server is carried out by "admin", not "root".
   ```
   set auth mode tacacs
   set auth tacacs server 1 addr 192.168.1.252
   set auth tacacs server 1 timeout 10
   set auth tacacs server 1 key password
   (Secret key entry)
   set auth tacacs server 2 addr 192.168.1.253
   set auth tacacs server 2 timeout 10
   set auth tacacs server 2 key password
   (Secret key entry)
   set auth su_cmd username admin
   ```

4. Configure TACACS+ accounting. Set TACACS+ server 1 to "192.168.1.252" and TACACS+ server 2 to "192.168.1.253". Configure the timeout to 10 seconds.
   Configure the secret key that was registered to the TACACS+ server.
   ```
   set acct mode tacacs
   set acct tacacs server 1 addr 192.168.1.252
   set acct tacacs server 1 timeout 10
   set acct tacacs server 1 key password
   (Secret key entry)
   set acct tacacs server 2 addr 192.168.1.253
   set acct tacacs server 2 timeout 10
   set acct tacacs server 2 key password
   (Secret key entry)
   ```

5. Register access groups to identify normal users and device management users.
   Carry out the "create auth access_group" command so that normal users and device management users are identified when the attribute ("grp" in this example) value to be sent from the TACACS+ authentication server is "normal_grp" or "admin_grp", respectively. The pairing of the attribute specified for "attr" and the value specified for "val" can be determined as desired by a device administrator.
   ```
   create auth access_group normal tacacs attr grp val normal_grp
   create auth access_group root tacacs attr grp val admin_grp
   ```

6. Register the access group to identify port users.

    Carry out the "create auth access_group" command so that port users are identified and access is allowed to serial ports (1 to 16, 24) when the attribute ("grp" in this example) to be sent from the TACACS+ authentication server is "grp1". In the same manner, configure to allow access to serial ports (20 to 32) when the attribute is "grp2". The pairing of the attribute name specified for "attr" and the value specified for "val" can be determined as desired by a device administrator.

    ```
    create auth access_group portusr port 1-16,24 tacacs attr grp val grp1
    create auth access_group portusr port 20-32 tacacs attr grp val grp2
    ```

7. Configure authentication processing for users for which an access group cannot be identified.

    The user is refused access when the access group cannot be identified (in this configuration example, when the "grp" attribute is not sent or when the "grp" attribute value does not match the value configured by the "create auth access_group" command).

    ```
    set auth tacacs def_user none
    ```

Notes

The NS-2250 performs user authentication in the following order: local authentication within the NS-2250 → TACACS+ authentication.

When normal users undergo TACACS+ authentication, either delete normal users registered to the NS-2250 or configure a password different from the password registered to the TACACS+ server. Be aware that when a password is not registered for normal users, simply pressing the Return key for the password makes it possible to pass local authentication of the NS-2250 and log in.

The result is the same as when logging in as a device management user or carrying out the "su" command. Configure a password different from the password registered to the TACACS+ server for device management users. Note that, unlike normal users, device management users (root) cannot be deleted.

TACACS+ server settings

This section lists examples of attributes to be set to the user definition file of the TACACS+ server.

The maximum length of a TACACS+ user name that can be authenticated by the NS-2250 is 64 characters.

```
accounting file = /var/log/tac_plus.acct

# Normal user registration

user = somebody
      login = cleartext "network"
      service = smartcs {
          grp = normal_grp
      }

user = abc01
      login = cleartext "abcdef"
      service = smartcs {
          grp = normal_grp
      }

# Device management user

user = admin
      login = cleartext "network"
      service = smartcs {
          grp = admin_grp
      }

user = manager1
      login = cleartext "manager1"
      service = smartcs {
          grp = admin_grp
      }

# Port user registration

user = portuser01
      login = cleartext "portuser01"
      service = smartcs {
          grp = grp1
      }
      # Permit access to serial ports (1 to 16, 24)

user = portuser02
      login = cleartext "portuser02"
      service = smartcs {
          grp = grp2
      }
       # Permit access to serial ports (20 to 32)

user = portuser03
      login = cleartext "portuser03"
      default service = permit
       # In this case, this user is refused access because
       # the setting of the NS-2250 is "set auth tacacs def_user none"
       and the user type cannot be identified.
```

You can also configure multiple privileges to a single user. (For example, you can configure access privileges of device management users and port users). Note that if you use a TACACS+ server, such as a server of the Shrubbery Networks, Inc., which cannot return multiple instances of the same attribute to the client, you must register attributes for each user group.

```
accounting file = /var/log/tac_plus.acct

user = portuser01
      login = cleartext "portuser01"
      service = smartcs {
          admin = admin_grp
          port = grp1
      }
      # Permit access to serial ports (1 to 16, 24)

user = portuser02
      login = cleartext "portuser02"
      service = smartcs {
          admin = admin_grp
          port = grp2
      }
      # Permit access to serial ports (1 to 16, 24)
```

In this case, the configuration of the NS-2250 is as follows.

```
create auth access_group root tacacs attr admin val admin_grp
create auth access_group portusr port 1-16,24 tacacs attr port val grp1
create auth access_group portusr port 20-32 tacacs attr port val grp2
set auth tacacs def_user none
```

4.8.15 LAN Redundant (using 2 LAN ports in different IP subnet)

This section describes about the setting of LAN redundant composition using different IP subnet.

Port server setting	:	Direct mode (default)
Method of connection	:	Telnet Normal mode (default)
Port user authentication	:	None (default)
Port log location	:	RAM (default)
Port log transfer function	:	Off (default)
Serial ports	:	Transfer speed of serial port 1 through serial port 48 (9,600 bps)

Configuration diagram

Figure 4-18 LAN redundant (using 2 LAN ports in different IP subnet)

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
set ipaddr eth2 192.168.2.100/24
create ip route default gateway 192.168.1.254
create ip route default gateway 192.168.2.254 metric 100
```

Explanation of settings
1. Set the name of the NS-2250. In this case, the IP address of a subnet different from both LAN1 and LAN2 is defined. Metrics (range: 0-100) is set as a route. Metrics of a default is 0(high priority). The route is switched by a link down in a LAN port.

     set hostname SmartCS
     set ipaddr eth1 192.168.1.100/24
     set ipaddr eth2 192.168.2.100/24
     create ip route default gateway 192.168.1.254
     create ip route default gateway 192.168.2.254 metric 100

4.8.16 LAN Redundant (using bonding function)

This section describes about the setting of LAN redundant composition using bonding function.

Port server setting	:	Direct mode (default)
Method of connection	:	Telnet Normal mode (default)
Port user authentication	:	None (default)
Port log location	:	RAM (default)
Port log transfer function	:	Off (default)
Serial ports	:	Transfer speed of serial port 1 through serial port 48 (9,600 bps)

Configuration diagram

Figure 4-19 LAN redundant (using bonding function)

Settings of the NS-2250

```
enable bonding
set hostname SmartCS
set ipaddr bond1 192.168.1.100/24
create ip route default gateway 192.168.1.254
```

Explanation of settings
1. Enable the bonding function.
    enable bonding

2. Set the name of the NS-2250 to the "SmartCS", set the bond1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".
    set hostname SmartCS
    set ipaddr bond1 192.168.1.100/24
    create ip route default gateway 192.168.1.254

4.8.17 Configure the IPsec

This section describes the basic settings of IPsec.

Port server setting	: Select mode
Method of connection	: SSH Normal mode
Port user authentication	: Yes
Port log location	: RAM (default)
Port log transfer function	: OFF (default)
Serial ports	: Transfer speed of serial port 1 through serial port 48 (9,600 bps)
IPsec	: Responder, Encrypt (AES128/SHA1/modp1024)

Configuration diagram
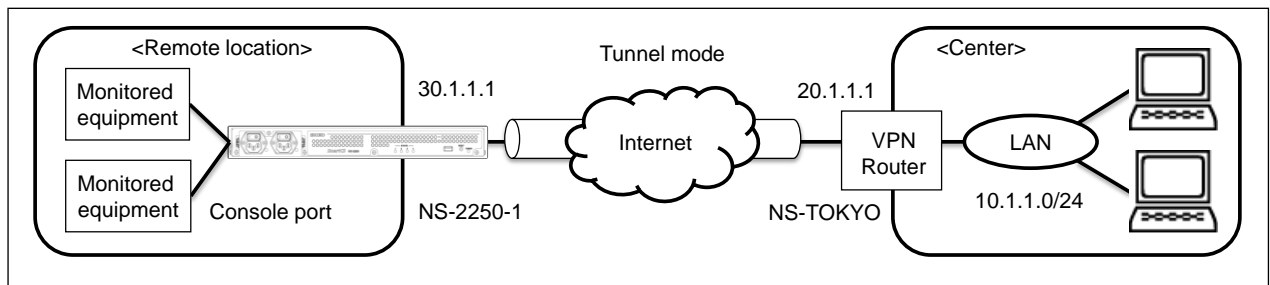
Figure 4-20 IPsec VPN

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 30.1.1.1/24
create ip route default gateway 30.1.1.2

set portd connect select
set portd auth basic

create user user01 group portusr port 1-48 password
(password entry)
create user user02 group portusr port 1-48 password
(password entry)

set user user01 port 1-48
set user user02 port 1-48

set portd tty 1-48 cmdchar 01

set portd tty 1 label Tokyo-L3SW-1
set portd tty 2 label Tokyo-L3SW-2
set portd tty 3 label Tokyo-L3SW-3
set portd tty 4 label Tokyo-L3SW-4
set portd tty 5 label Tokyo-SV-1
set portd tty 6 label Tokyo-SV-2
```

```
set portd tty 7 label Tokyo-SV-3
set portd tty 8 label Tokyo-SV-4

set sshd auth basic
create allowhost all service portd sshrw all

enable sshd
create allowhost all service sshd
set user somebody passwd
(password entry)

create ipsec secret psk NS-2250-1 NS-TOKYO password
 Pre-Shared-Key password
 Retype Pre-Shared-Key password
set ipsec conn 1 auto add
set ipsec conn 1 leftid NS-2250-1
set ipsec conn 1 rightid NS-TOKYO
set ipsec conn 1 left 30.1.1.1
set ipsec conn 1 right 20.1.1.1
set ipsec conn 1 leftsubnet 30.1.1.0/24
set ipsec conn 1 rightsubnet 10.1.1.0/24
set ipsec conn 1 keyexchange ikev1
set ipsec conn 1 ike aec128-sha1-modp1024
set ipsec conn 1 esp aec128-sha1-modp1024
enable ipsec conn 1

set ipinterface eth1 mtu 1280

create ipfilter input line 1 accept eth1 any any esp
create ipfilter input line 2 accept eth1 any any udp 500
create ipfilter input line 3 accept eth1 any any udp 4500
create ipfilter input line 4 accept eth1 any any tcp 22
create ipfilter input line 5 accept eth1 any any icmp any
create ipfilter input line 6 drop eth1 any any any
enable ipfilter
```

Explanation of settings

1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "30.1.1.1/24", and set the default route to "30.1.1.2".

   set hostname SmartCS
   set ipaddr eth1 30.1.1.1/24
   create ip route default gateway 30.1.1.2

2. Enable the port selection function. Change the port server connection mode to "select".

   set portd connect select

3. Switch on port user authentication.

   set portd auth basic

4. Create port users (user01 and user02) to use port user authentication.

   Configure the access privileges for serial port 1 through serial port 48 for port users.

   create user user01 group portusr port 1-48 password
   (password entry)
   create user user02 group portusr port 1-48 password

(password entry)

5. Configure the serial ports that can be accessed by a port user.
   Configure the privileges so that user01 to user02 can access serial port 1 through 48.
   > set user user01 port 1-48
   > set user user02 port 1-48

6. Register "0x01" (Ctrl+A) as the session suspension character code of the port server menu for serial port 1 through serial port 48.
   > set portd tty 1-48 cmdchar 01

7. Register the label for each serial port.
   > set portd tty 1 label Tokyo-L3SW-1
   > set portd tty 2 label Tokyo-L3SW-2
   > set portd tty 3 label Tokyo-L3SW-3
   > set portd tty 4 label Tokyo-L3SW-4
   > set portd tty 5 label Tokyo-SV-1
   > set portd tty 6 label Tokyo-SV-2
   > set portd tty 7 label Tokyo-SV-3
   > set portd tty 8 label Tokyo-SV-4

8. Set the SSH authentication method to Password (basic) authentication, and then configure the settings to allow access to all serial ports in SSH Normal mode from all network addresses.
   > set sshd auth basic
   > create allowhost all service portd sshrw all

9. Configure the settings of the SSH server of the NS-2250 to allow login to the NS-2250 from an SSH client. Enable the SSH server of the NS-2250, and then configure the settings to allow access to the SSH server of the NS-2250 from all network addresses. Finally, configure the passwords of login users registered to the NS-2250.
   > enable sshd
   > create allowhost all service sshd
   > set user somebody password
   (password entry)

10. Configure the IPsec connection. Register the pre-shared-key used by IKE. Specify NS-2250-1 as the security gateway ID and NS-TOKYO as the ID of the remote device.
    > create ipsec secret psk NS-2250-1 NS-TOKYO password
    Pre-Shared-Key password
    Retype Pre-Shared-Key password

11. Set the NS-2250 as a responder, and register the IP address and the network information of the NS-2250 and the remote device. Set IKEv1 as IKE protocol and set the encryption or authentication algorithm, or DH group to aec128-sha1-modp1024.
    > set ipsec conn 1 auto add
    > set ipsec conn 1 leftid NS-2250-1

set ipsec conn 1 rightid NS-TOKYO
set ipsec conn 1 left 30.1.1.1
set ipsec conn 1 right 20.1.1.1
set ipsec conn 1 leftsubnet 30.1.1.0/24
set ipsec conn 1 rightsubnet 10.1.1.0/24
set ipsec conn 1 keyexchange ikev1
set ipsec conn 1 ike aec128-sha1-modp1024
set ipsec conn 1 esp aec128-sha1-modp1024
enable ipsec conn 1

12.Set the appropriate MTU value by "set ipinterface mtu" command depending on the Network configuration. The below example set MTU of LAN1 to 1280 byte.

set ipinterface eth1 mtu 1280

13.If required the Firewall(ipfilter) setting is necessary. The filter setting for the decoded packet is also necessary for IPsec communication. For example, in case you want to access NS-2250 via SSH/SFTP with VPN connection in IPsec it is necessary to create the below filter setting which allows IKE (UDP 500), NAT traversal (UDP 500), SSH/SFTP (TCP 22) and ICMP.

create ipfilter input line 1 accept eth1 any any esp
create ipfilter input line 2 accept eth1 any any udp 500
create ipfilter input line 3 accept eth1 any any udp 4500
create ipfilter input line 4 accept eth1 any any tcp 22
create ipfilter input line 5 accept eth1 any any icmp any
create ipfilter input line 6 drop eth1 any any any
enable ipfilter

4.8.18 Configure the Firewall (ipfilter)

This section describes the firewall settings that apply to the receiving interface of the NS-2250.

Port server setting	:	Direct mode (default)
Method of connection	:	Telnet Normal mode (default)
Port user authentication	:	None (default)
Port log location	:	RAM (default)
Port log transfer function	:	Off (default)
Serial ports	:	Transfer speed of serial port 1 through serial port 8 (19,200 bps)
Firewall (ipfilter) function	:	Register custom filter
Session suspension character code	:1 (Ctrl+A)	

Configuration diagram
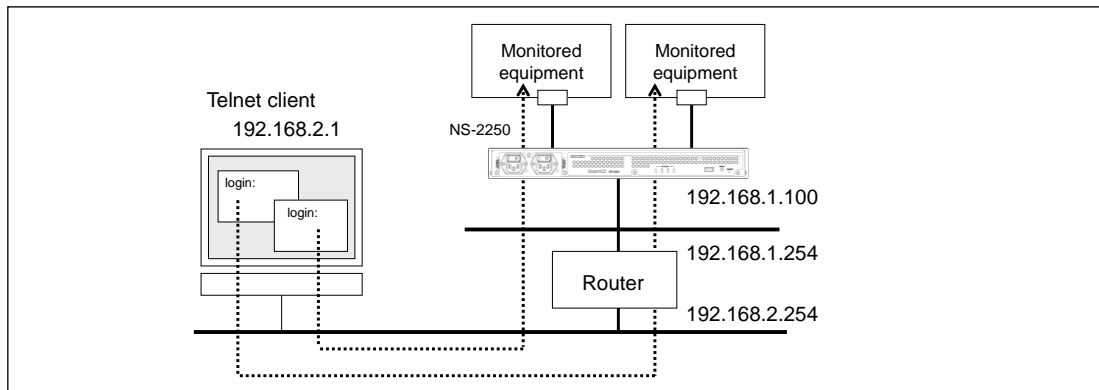
Figure 4-21 Firewall settings

Settings of the NS-2250

```
set hostname SmartCS
set ipaddr eth1 192.168.1.100/24
create ip route default gateway 192.168.1.254
set tty 1-8 baud 19200
set portd tty 1-8 cmdchar 1

create ipfilter input line 1 accept eth1 any 192.168.2.0/24 icmp
create ipfilter input line 2 accept eth1 any 192.168.2.0/24 tcp 23
create ipfilter input line 3 accept eth1 any 192.168.2.0/24 udp 161
create ipfilter input line 4 accept eth1 any 192.168.2.0/24 tcp 8101-8108
create ipfilter input line 5 drop eth1 any any any
enable ipfilter
```

Explanation of settings
1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IP address to "192.168.1.100/24", and set the default route to "192.168.1.254".

    set hostname SmartCS
    set ipaddr eth1 192.168.1.100/24
    create ip route default gateway 192.168.1.254

2. Set the transfer speed of serial port 1 through serial port 8 to 19,200 bps.

    set tty 1-8 baud 19200

3. Set the session suspension character code for serial port 1 through serial port 8 to "Ctrl+A".

    set portd tty 1-8 cmdchar 1

4. Create the firewall setting to LAN1 port and create the setting which accepts only ICMP/telnet/snmp and telnet normal mode (TCP 8108-8108) from 192.168.2.0/24.

    create ipfilter input line 1 accept eth1 any 192.168.2.0/24 icmp
    create ipfilter input line 2 accept eth1 any 192.168.2.0/24 tcp 23
    create ipfilter input line 3 accept eth1 any 192.168.2.0/24 udp 161
    create ipfilter input line 4 accept eth1 any 192.168.2.0/24 tcp 8101-8108
    create ipfilter input line 5 drop eth1 any any any
    enable ipfilter

4.8.19 Configure the IPv6

This section describes the IPv6 settings in the case NS-2250 is used in IPv6 network.

Port server setting	:	Direct mode (default)
Method of connection	:	Telnet Normal mode (default)
Port user authentication	:	None (default)
Port log location	:	RAM (default)
Port log transfer function	:	ON (SYSLOG/NFS/FTP/Mail)
Other settings	:	DNS client
		Access control to the Telnet server
		Access control to the port server

Configuration diagram
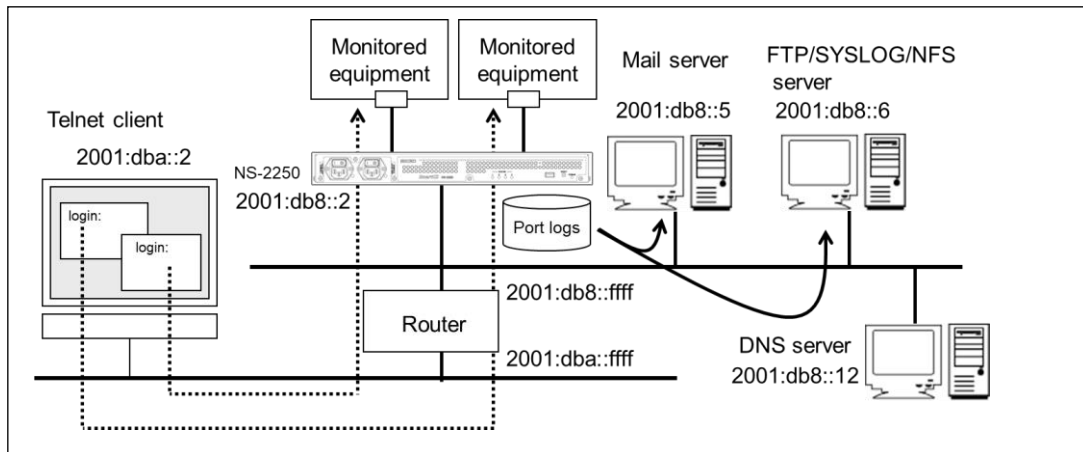
Figure 4-22 IPv6 settings

Settings of the NS-2250

```
set hostname SmartCS
set ip6addr eth1 2001:db8::2/64
create ip6route default gateway 2001:db8::ffff

set syslog host 1 2001:db8::6 portlog_facility local0 syslog_facility local1
enable syslog

set nfs server 1 addr 2001:db8::6 path /mnt/nfslog
set nfs rotate on 0 0 1 * *
enable nfs

set logd tty 1 syslog on
set logd tty 1 sendlog mail interval 180 ratio 70
add logd tty 1 mail 1 mgr@example.co.jp 2001:db8::5

set logd tty 2 syslog on
set logd tty 2 sendlog mail interval 180 ratio 70
add logd tty 2 mail 1 user1@example.co.jp 2001:db8::5
set logd tty 2 mail 1 type body
```

```
set logd tty 2 mail 1 subject "Server Status"
set logd tty 2 mail 1 sender smartcs@example.co.jp

add logd tty 2 mail 2 user2@example.co.jp 2001:db8::5
set logd tty 2 mail 2 type body
set logd tty 2 mail 2 subject "Data-Center Server"
set logd tty 2 mail 2 sender smartcs@example.co.jp

set logd tty 3 syslog on
set logd tty 3 sendlog ftp interval 180 ratio 70
add logd tty 3 ftp 1 loguser1 2001:db8::6 password
[enter password]

set logd tty 4 syslog on
set logd tty 4 sendlog ftp interval 180 ratio 70
add logd tty 4 ftp 1 loguser1 2001:db8::6 password
[enter password]
add logd tty 4 ftp 2 loguser2 2001:db8::6 password
[enter password]

set logd tty 5 nfs on
set logd tty 6 nfs on
set dns 1 2001:db8::12
set dns localdomain example.co.jp

delete allowhost allentry
create allowhost 2001:dba::/64 service telnetd
create allowhost 2001:dba::/64 service portd telrw all
```

Explanation of settings
1. Set the name of the NS-2250 to the "SmartCS", set the LAN1 IPv6 address to "2001:db8::2/64", and set the default route to "2001:db8::ffff".

      set hostname SmartCS
      set ip6addr eth1 2001:db8::2/64
      create ip6route default gateway 2001:db8::ffff

2. Set the SYSLOG client function of the NS-2250.
  Set portlog facility to "local0" and SYSLOG facility of NS-2250 system logs to "local1", and send logs to the SYSLOG server(2001:db8::6).
  Enable the SYSLOG client by "enable syslog" command after the SYSLOG setting is executed.

      set syslog host 1 2001:db8::6 portlog_facility local0 syslog_facility local1
      enable syslog

3. Set the NFS client function of the NS-2250.
  Set the NFS server to "2001:db8::6", the mount path to "/mnt/nfslog" and the timing so that log rotation works at 0:00 on 1st every month.

      set nfs server 1 addr 2001:db8::6 path /mnt/nfslog
      set nfs rotate 0 0 1 * *
      enable nfs

4. Enable the SYSLOG output of serial port 1 to send logs of target devices to SYSLOG server every time NS-2250 receives them. Moreover, set the log output to send logs to Mail server periodically.

   NS-2250 sends port logs to "mgr@example.co.jp" via Mail server "2001:db8::5" every 180 minutes or when the log data stored in NS-2250 exceeds 70 percent of the maximum size with the following settings.

   The subject and sender mail address of the mail and the sending method of port log are applied to the factory default settings as follows.

   - Subject: portlog TTY number
   - Sender mail address: portusr@"hostname of NS-2250"."local domain"
   - Method: Log file attached to the mail

   ```
   set logd tty 1 syslog on
   set logd tty 1 sendlog mail interval 180 ratio 70
   add logd tty 1 mail 1 mgr@example.co.jp 2001:db8::5
   ```

5. Enable the SYSLOG output of serial port 2 to send logs of target devices to SYSLOG server every time NS-2250 receives them. Moreover, set the log output to send logs to Mail server periodically.

   NS-2250 sends port logs to "user1@example.co.jp" and "user2@example.co.jp" via Mail server "2001:db8::5" every 180 minutes or when the log data stored in NS-2250 exceeds 70 percent of the maximum size with the following settings.

   Regarding the mail to "user1@example.co.jp", set the subject to "Server Status" and sender address to "smartcs@example.co.jp".

   Regarding the mail to "user2@example.co.jp", set the subject to "Data-Center Server" and sender address to "smartcs@example.co.jp".

   Send port logs added in the body of the mail.

   ```
   set logd tty 2 syslog on
   set logd tty 2 sendlog mail interval 180 ratio 70
   add logd tty 2 mail 1 user1@example.co.jp 2001:db8::5
   set logd tty 2 mail 1 type body
   set logd tty 2 mail 1 subject "Server Status"
   set logd tty 2 mail 1 sender smartcs@example.co.jp
   add logd tty 2 mail 2 user2@example.co.jp 2001:db8::5
   set logd tty 2 mail 2 type body
   set logd tty 2 mail 2 subject "Data-Center Server"
   set logd tty 2 mail 2 sender smartcs@example.co.jp
   ```

6. Enable the SYSLOG output of serial port 3 to send logs of target devices to SYSLOG server every time NS-2250 receives them. Moreover, set the log output to send logs to FTP server periodically.

   NS-2250 sends port logs to FTP server "2001:db8::6" using the user "loguser1" every 180 minutes or when the log data stored in NS-2250 exceeds 70 percent of the maximum size with the following settings.

   ```
   set logd tty 3 syslog on
   set logd tty 3 sendlog ftp interval 180 ratio 70
   ```

```
add logd tty 3 ftp 1 loguser1 2001:db8::6 password
[enter password]
```

7. Enable the SYSLOG output of serial port 4 to send logs of target devices to SYSLOG
   server every time NS-2250 receives them. Moreover, set the log output to send logs to
   FTP server periodically.
   NS-2250 sends port logs to FTP server "2001:db8::6" using the user "loguser1" and
   "loguser2" every 180 minutes or when the log data stored in NS-2250 exceeds 70
   percent of the maximum size with the following settings.

   ```
   set logd tty 4 syslog on
   set logd tty 4 sendlog ftp interval 180 ratio 70
   add logd tty 4 ftp 1 loguser1 2001:db8::6 password
   [enter password]
   add logd tty 4 ftp 2 loguser2 2001:db8::6 password
   [enter password]
   ```

8. Enable the NFS output of serial port 5 and 6 to save logs of target devices on NFS
   server every time NS-2250 receives them.

   ```
   set logd tty 5 nfs on
   set logd tty 6 nfs on
   ```

9. Set the DNS client function of the NS-2250.
   Set the DNS server as "2001:db8::12" when the name resolution is carried out.
   Set the local domain as "example.co.jp".

   ```
   set dns 1 2001:db8::12
   set dns localdomain example.co.jp
   ```

10. Set the access control to the Telnet server and port server of the NS-2250.
    Allow only 2001:dba::/64 network to access the Telnet server and port server of the
    NS-2250.
    By default, all networks are allowed to access the Telnet server and port server of the
    NS-2250 so carry out deleting the settings by the "delete" command firstly.

    ```
    delete allowhost allentry
    create allowhost 2001:dba::/64 service telnetd
    create allowhost 2001:dba::/64 service portd telrw all
    ```

Chapter 5
Management and maintenance

Chapter 5 describes the management andmaintenance of NS-2250.

5.1 View information of the NS-2250

5.1.1 View hardware and software information

To view information about the hardware configuration and system software of the NS-2250, carry out the "show version" command. This command shows the system software version, boot status, system uptime, serial number, and other information.

```
(c)NS-2250# show version↵
System                : System Software Ver 1.0 (Build 2015-XX-XX)
Boot Status           : Reboot (05:80:00)
System Up Time        : 2015/07/03 21:12:07
Local MAC Address     : 00:80:15:XX:XX:XX
Number of MAC Address : 2
Model                 : NS-2250-48 (48 port)
Serial No.            : XXXXXXXX
BootROM               : Ver X.X.X
Main Board CPU        : e500v2 (533.333328MHz)
Main Memory           : 1025264 KBytes
Boot System           : main (Ver 1.0)
Boot Config           : external startup1
Main System           : Ver 1.0
Backup System         : Ver 1.0
(c)NS-2250#
```

5.1.2 View a summary of the information of the NS-2250

To display settings, statistical information, logs, and other information of the NS-2250 together, carry out the "show support" command.

The following table shows the NS-2250 information output by the "show support" command.

The information displayed by the "show support" command	
Version information	Syslog information
SYSTEM information	NFS information
Host information	AUTH Access_Group information
slot information	AUTH information
USB Port information	ACCT information
CPU information	Portd information
Memory information	Portd session information
Process information	tty manage information
Bonding information	TTY information
Ether port information	TTY stats information
Ether port statistics information	Logd information
IP6 information	Logd stats information
IP host information	Console information
IP route information	Console stats information
IP6 route information	Service information
ipfilter information	Allowhost information
ip6filter information	Startup config information
ipsec information	Running configuration
IP/IP6 statistics information	system information
DNS information	network information
ARP/NDP/TCP/UDP information	i2c information
User information	temprature information
Login User information	System profile
SNMP information	Command log
SNTP information	Console log
	Boot log
	System log

This command displays the boot messages, statistical information, and other large-volume logs. Therefore, it is more appropriate to carry out this command from a telnet/SSH client connected via a network than via the CONSOLE port, which is configured to a low-speed transfer rate.

Note that the "show support" command can display a maximum of 500 lines for each log. To display all logs, carry out the "show support detail" command.

The output of this command is used for our support system so we cannot answer inquiries relating to its content.

The following section shows an actual output of the "show support" command.

```
(c)NS-2250# show support↵
===== start of show support =====
Fri Jul 03 19:32:04 JST 2015

===== Version information
System                : System Software Ver 1.0 (Build 2015-XX-XX)
Boot Status           : Reboot (05:80:00)
System Up Time        : 2015/07/03 21:12:07
Local MAC Address     : 00:80:15:XX:XX:XX
Number of MAC Address : 2
Model                 : NS-2250-48 (48 port)
Serial No.            : XXXXXXXX
BootROM               : Ver X.X.X
Main Board CPU        : e500v2 (533.333328MHz)
Main Memory           : 1025264 KBytes
Boot System           : main (Ver 1.0)
Boot Config           : external startup1
Main System           : Ver 1.0
Backup System         : Ver 1.0

===== Host information
Timezone is "Tokyo"

===== Host information
Hostname          : NS-2250
TCPkeepAlive      : 180
IPaddrress(eth1)  : 192.168.0.1/24
IPaddrress(eth2)  : -

hostname
NS-2250

   : omitted

===== end of show support ====
(c)NS-2250#
```

5.2   Manage the configuration

5.2.1 View a list of startup files

The NS-2250 stores and manages the settings in the startup file. The SmartCS has a maximum of eight startup files (four files on the USB memory and four files on the internal memory of the device). USB memory

If there is a USB memory inserted in the NS-2250, the default startup file of the USB memory is read as the starting configuration.
If there is no USB memory inserted, the SmartCS reads the default startup file saved in the internal memory of the NS-2250.
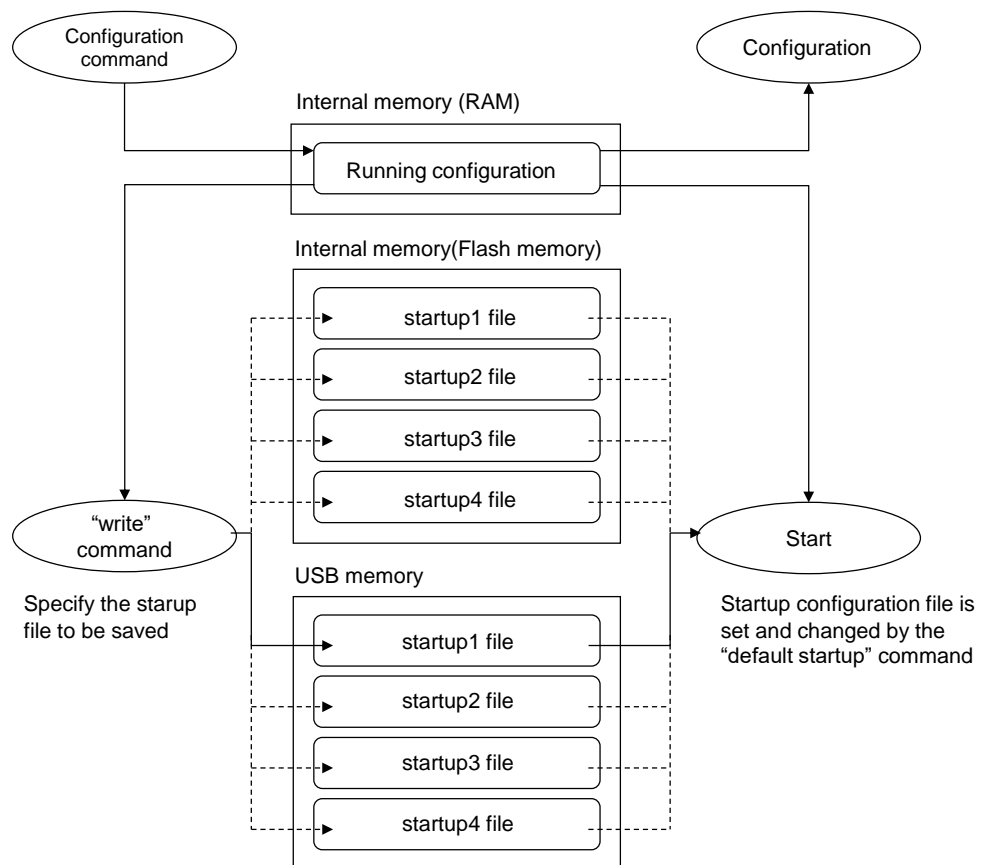
Figure 5-1 Startup file (SmartCS)

To view a list of startup files, carry out the "show config info" command.

```
(c)NS-2250# show config info↵
boot startup : external startup1

internal startup files
name         date            size default
------------------------------------------
startup1     Jul 3 19:28      762    *
startup2     Jul 2 09:35      445
startup3     Jul 2 09:35      445
startup4     Jul 2 09:35      445

external startup files
name         date            size default
------------------------------------------
startup1     Jul 3 19:28      762    *
startup2     Jul 2 09:35      445
startup3     Jul 2 09:35      445
startup4     Jul 2 09:35      445
(c)NS-2250#
```

5.2.2 View the content of startup files

To view information on the startup file that the NS-2250 read at startup, carry out the "show config startup" command.

```
(c)NS-2250# show config startup↵
=== show external startup1 ===

echo "SYSTEM configuration..."
#
set timezone Tokyo
#
echo "IP configuration..."
#
set hostname NS-2250
set ipaddr eth1 192.168.0.1
#
echo "User configuration..."
#
create user somebody group normal uid 100
create user setup group normal uid 198
create user verup group normal uid 199
create user log group normal uid 200
#
echo "Network service configuration..."
#
create allowhost all service telnetd
create allowhost all service portd telrw all
  : omitted
(c)NS-2250#
```

To view a specified startup file (for example, "startup4" file of the USB memory), carry out the "show config startup" command while specifying the options shown below.

```
(c)NS-2250# show config startup 4 external↵
=== show external startup4 ===

#
# System configuration
set timezone Tokyo
#
# IP configuration
set hostname NS-2250
set ipaddr eth1 192.168.0.1
  : omitted
```

5.2.3 Change the startup file to be imported at startup

Concerning the startup file to be read at startup, the SmartCS stores files on both a USB memory and internally. At the default settings, the NS-2250 uses the "startup1" file as the default startup file.

If there is a USB memory inserted in the device, the default startup file of the USB memory is always read. If there is no USB memory inserted, the SmartCS reads the default startup file saved in the internal memory.

To change the startup file read at startup, carry out the "default startup" command. For example, to change the default startup file of the USB memory to the "startup3" file, carry out the "default startup" command while specifying the options shown below.

```
(c)NS-2250# default startup 3 external↵
(c)NS-2250#
```

You can check the default startup file by carrying out the "show config info" command. The default startup file is indicated by the asterisk (*) in the "default" column.

```
(c)NS-2250# show config info↵
boot startup : external startup1

internal startup files
name          date            size default
-------------------------------------------
startup1     Jul 3 19:28       762     *
startup2     Jul 2 09:35       445
startup3     Jul 2 09:35       445
startup4     Jul 2 09:35       445


external startup files
name          date            size default
-------------------------------------------
startup1     Jul 3 19:28       762     *
startup2     Jul 2 09:35       445
startup3     Jul 2 09:35       445
startup4     Jul 2 09:35       445
(c)NS-2250#
```

5.2.4 Copy a startup file

To copy a startup file, carry out the "copy startup" command. For example, to copy the "startup1" file of the USB memory to the "startup2" file of the USB memory, carry out the "copy startup" command while specifying the options shown below.

```
(c)NS-2250# copy startup 1 external to startup 2 external↵
Do you really want to copy external startup1 to external startup2 [y/n] ? y↵
(c)NS-2250#
```

5.2.5 Clear the content of a startup file

To clear the content of a startup file (return to default settings), carry out the "clear startup" command. For example, to clear the content of the "startup 2" file of the external and internal, carry out the "clear startup" command while specifying the options shown below.

```
(c)NS-2250# clear startup 2
Do you really want to clear external & internal startup2 [y/n] ? y↵
(c)NS-2250#
```

To clear all startup files, carry out the command while specifying the "all" option shown below.

```
(c)NS-2250# clear startup all↵
Do you really want to clear internal & external startup1-startup4 [y/n] ? y↵
(c)NS-2250#
```

5.2.6 View the running configuration

The NS-2250 manages the configuration commands stored in the startup file read at startup, the configuration commands carried out by the device administrator after the NS-2250 has started, and other configuration commands as the running configuration in the internal memory of the NS-2250.

To view the running configuration of the NS-2250, carry out the "show config running" command.

```
(c)NS-2250# show config running↵
...............
#
echo "SYSTEM configuration..."
#
Set timezone Tokyo
#
echo "IP configuration..."
#
set hostname NS-2250
set ipaddr eth1 192.168.1.1/24
#
echo "IP6 configuration..."
#
create ip6
set ip6addr eth1 2001:db8::2/64
#
echo "User configuration..."
#
create user setup group setup uid 198
create user verup group verup uid 199
create user log group log uid 200
create user somebody group normal uid 100
#
#
echo "IP ROUTE configuration..."
#
create ip route default gateway 192.168.1.254
#
#
echo "IP6 ROUTE configuration..."
#
create ip6route default gateway 2001:db8::ffff
#
#
echo "Network service configuration..."
#
enable sshd
create allowhost all service telnetd
create allowhost all service portd telrw all
#
```

5.2.7 Transfer startup files via FTP server

You can access the FTP server of NS-2250 from an FTP client, and then store the startup files of the NS-2250 in the FTP client or save startup files managed by the FTP client to the NS-2250.

The procedure to manage startup files by file transfer is described using the following conditions: IP address of NS-2250: "192.168.1.100", IP address of the FTP client: "192.168.1.1".

(1) Advanced settings

Before managing startup files, configure the NS-2250.

Use the "enable ftp" command to start the FTP server, and then carry out the "create allowhost" command so that the FTP client can access the FTP server of the NS-2250. Next, configure the password for the "setup" user used by this operation.

To use an SFTP client, which uses the SSH protocol, refer to Section 4.6.6, "Configure the SSH server" and Section 4.6.7, "Control access to servers", and then configure the SSH server of the NS-2250.

```
 (c)NS-2250# enable ftpd↵
 (c)NS-2250# create allowhost all service ftpd↵
 (c)NS-2250# set user setup password↵
Changing password for user setup.
New password: ↵
Retype new password: ↵
passwd: all authentication tokens updated successfully.
 (c)NS-2250#
```

(2) Save startup files of the NS-2250 to the FTP client

To save startup files of the NS-2250 to the FTP client, carry out the following operation using the FTP client. This section describes the procedure to save the "startup1" file of the USB memory to the FTP client.

Using the FTP client, carry out the "ftp" command, and then log in as a "setup" user.

```
$ ftp 192.168.1.100↵
Connected to 192.168.1.100 (192.168.1.100).
220 Welcome to FTP Service.
Name (192.168.1.100:setup): setup↵
331 Please specify the password.
Password: ↵
230 Login successful.
ftp>
```

After logging into the NS-2250 via FTP, carry out the "ls" command to check the startup file. The internal startup files (startup 1 to 4 files) are saved in the "internalfiles" directory and the startup files (startup 1 to 4 files) of the USB memory are saved in the "externalfiles" directory.

To save the "startup1" file of the USB memory to the FTP client, carry out the "cd" command to move to the "externalfiles" directory, and then carry out the "ls" command again to check the startup files. Do not carry out other directory or file operations.

```
ftp> ls↵
227 Entering Passive Mode (192.168.1.100,83,33)
150 Here comes the directory listing.
lrwxrwxrwx   1 0       0               10 Oct 06 07:51 externalfiles
lrwxrwxrwx   1 0       0               10 Oct 06 07:51 internalfiles
226 Directory send OK.

ftp> cd externalfiles↵
250 Directory successfully changed.

ftp> ls↵
227 Entering Passive Mode (192.168.1.100,43,110)
150 Here comes the directory listing.
-rw-rw-r--   1 0      198           720 Oct 08 12:52 startup1
-rw-rw-r--   1 0      198           534 Oct 06 10:33 startup2
-rw-rw-r--   1 0      198           534 Oct 06 10:34 startup3
-rw-rw-r--   1 0      198           534 Oct 06 10:34 startup4
-rw-rw-r--   1 0      198             2 Jun 25 10:21 startup_number
226 Directory send OK.
ftp>
```

Save the "startup1" file of the USB memory to the FTP client, and then exit the FTP client.

```
ftp> get startup1 CS1-startup1↵
local: startup1 remote: startup1
227 Entering Passive Mode (192.168.1.100,191,54)
150 Opening ASCII mode data connection for startup1 (720 bytes).
226 File send OK.
720 bytes received in 0.00026 secs (2.7e+03 Kbytes/sec)

ftp> quit↵
221 Goodbye.
$
```

(3) Save startup files managed by the FTP client to the NS-2250

To save startup files managed by the FTP client to the NS-2250, carry out the following operation using the FTP client. This section describes the procedure to save startup files managed by the FTP client to the "startup1" file of the USB memory.

Using the FTP client, carry out the "ftp" command, and then log in as a "setup" user.

```
$ ftp 192.168.1.100↵
Connected to 192.168.1.100 (192.168.1.100).
220 Welcome to FTP service.
Name (192.168.1.100:setup): setup↵
331 Please specify the password.
Password:↵
230 Login successful.
ftp>
```

After logging into the NS-2250 via FTP, carry out the "ls" command to check the startup file. The internal startup files (startup 1 to 4 files) are saved in the "internalfiles" directory and the startup files (startup 1 to 4 files) of the USB memory are saved in the "externalfiles" directory.

To save startup files managed by the FTP client to the "startup1" file of the USB memory, carry out the "cd" command to move to the "externalfiles" directory, and then carry out the "ls" command again to check the startup files. Do not carry out other directory or file operations.

```
ftp> ls↵
227 Entering Passive Mode (192.168.1.100,83,33)
150 Here comes the directory listing.
lrwxrwxrwx    1 0        0              10 Oct 06 07:51 externalfiles
lrwxrwxrwx    1 0        0              10 Oct 06 07:51 internalfiles
226 Directory send OK.

ftp> cd externalfiles↵
250 Directory successfully changed.

ftp> ls↵
227 Entering Passive Mode (192.168.1.100,43,110)
150 Here comes the directory listing.
-rw-rw-r--    1 0       198            720 Oct 08 12:52 startup1
-rw-rw-r--    1 0       198            534 Oct 06 10:33 startup2
-rw-rw-r--    1 0       198            534 Oct 06 10:34 startup3
-rw-rw-r--    1 0       198            534 Oct 06 10:34 startup4
-rw-rw-r--    1 0       198              2 Jun 25 10:21 startup_number
226 Directory send OK.
ftp>
```

Save the startup files managed by the FTP client to the "startup1" file of the USB memory, and then exit the FTP client.

```
ftp> put CS1-startup1 startup1↵
local: startup1 remote: startup1
227 Entering Passive Mode (192.168.1.100,191,54)
150 Opening ASCII mode data connection for startup1 (720 bytes).
226 File send OK.
720 bytes received in 0.00026 secs (2.7e+03 Kbytes/sec)

ftp> quit↵
221 Goodbye.
$
```

Even after saving the startup files managed by the FTP client to the "startup1" file of the USB memory, the settings of the "startup1" file are not applied to the running configuration. To apply the settings of the "startup1" file to the running configuration, restart the NS-2250.

```
(c)NS-2250# reboot↵
Do you really want to reboot with main system and startup1 [y/n] y↵
```

5.2.8 Transfer startup files via an FTP client

You can access the FTP server from an FTP client of NS-2250, and then store the startup files of the NS-2250 in the FTP server or save startup files managed by the FTP server to the NS-2250.

The procedure to manage startup files by file transfer is described using the following conditions: IP address of NS-2250: "192.168.1.100", IP address of the FTP client: "192.168.1.1".

(1) Save startup files of the NS-2250 to the FTP server

To save startup files of the NS-2250 to the FTP server, carry out the following operation using the FTP command. This section describes the procedure to save the "startup1" file of the USB memory to the FTP server.

Using the NS-2250, carry out the "ftp" command, and then log in as an FTP server user.

```
(c)NS-2250# ftp setup external 192.168.1.1↵
220 FTP Server ready.
Name (192.168.1.1:root): user1↵
331 Password required for user1
Password:
230 User ne logged in.
ftp> put startup1 CS1-startup1↵
local: startup1 remote: CS1-startup1
227 Entering Passive Mode (192.168.1.1,170,246).
150 Opening BINARY mode data connection for CS1-startup1
ftp> quit↵
221 Goodbye.
(c)NS-2250#
```

(2) Save startup files managed by the FTP server to the NS-2250

To save startup files managed by the FTP server to the NS-2250, carry out the following operation using the ftp command of NS-2250. This section describes the procedure to save startup files managed by the FTP server to the "startup1" file of the USB memory.

Using the NS-2250, carry out the "ftp" command, and then log in as a FTP server user.

```
(c)NS-2250# ftp setup external 192.168.1.1↵
Connected to 10.5.31.171 (10.5.31.171).
220 FTP Server ready.
Name (192.168.1.1:root): user1↵
331 Password required for user1
Password:
230 User ne logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get CS1-startup1 startup1↵
local: startup1 remote: CS1-startup1
227 Entering Passive Mode (10,5,31,171,216,249).
150 Opening BINARY mode data connection for CS-startup1 (1476 bytes)
ftp>
```

5.2.9 Transfer startup files via TFTP client

You can save the startup files of the NS-2250 to the TFTP server and copy startup files managed by the TFTP server to the NS-2250.
The procedure to manage startup files via TFTP is described using the following conditions:
IP address of NS-2250: "192.168.1.100", IP address of the TFTP server: "192.168.1.1".

(1)   Save startup files of the NS-2250 to the TFTP server
To save startup files of the NS-2250 to the TFTP server, carry out the following operation.
This section describes the procedure to save the "startup1" file to the TFTP server.

```
(c)NS-2250# tftp put setup startup 1 external 192.168.1.1↵
(c)NS-2250#
```

(2)   Save startup files managed by the TFTP server to the NS-2250
To save startup files managed by the TFTP server to the NS-2250, carry out the following operation. This section describes the procedure to save the "startup1" file managed by the TFTP server to the NS-2250.

To apply the transferred startup file, you must restart the NS-2250.

```
(c)NS-2250# tftp get setup startup 1 external 192.168.1.1↵
(c)NS-2250#
```

5.3   View console logs

Console messages of the NS-2250 are displayed on a device management terminal connected to the CONSOLE port. Also, displayed console messages are saved inside the NS-2250 as console logs.

To view the console log (20 most recent lines) of the NS-2250, carry out the "show log console" command while specifying the number of lines to be displayed.

```
(c)NS-2250# show log console 20↵

Sep 23 15:24:03 port_logd: <TTY22> started
Sep 23 15:24:03 port_logd: <TTY23> started
Sep 23 15:24:04 port_logd: <TTY24> started
Sep 23 15:24:04 port_logd: <TTY25> started
Sep 23 15:24:04 port_logd: <TTY26> started
Sep 23 15:24:04 port_logd: <TTY27> started
Sep 23 15:24:05 port_logd: <TTY28> started
Sep 23 15:24:05 port_logd: <TTY29> started
  :

(c)NS-2250#
```

To view all console logs saved in the NS-2250 again, carry out the "show log console" command without specifying options.

```
(c)NS-2250# show log console↵
                :
(c)NS-2250#
```

To display console messages on telnet/SSH client terminals on the network at the same time as console messages are displayed on a device management terminal connected to the CONSOLE port, carry out the "console" command from the telnet/SSH client.
After the command is carried out, output console messages appear on the screen of the telnet/SSH client.
To stop the display of console messages, carry out the "console off" command.

```
(0)NS-2250# console↵      Show console messages
(0)NS-2250# console off↵      Hide console messages
(0)NS-2250#
```

You can send console logs to syslog servers for saving. For a method to specify a syslog server, see Section 4.7.3, "Configure the syslog client".

5.4   Manage the NS-2250 via SNMP

The NS-2250 supports SNMP Version 1, Version 2c and Version 3. If the NS-2250 receives a MIB request sent by an SNMP server, it responds to the request on the SNMP server with a MIB value in the supported version format.

Furthermore, because the NS-2250 has an SNMP trap sending function, it can send an SNMP trap to the SNMP server to warn of trouble when the NS-2250 restarts for some reason or when monitored equipment connected to the NS-2250 is down. For traps, you can specify whether to send in the Version 1, Version 2 or version 3 format.
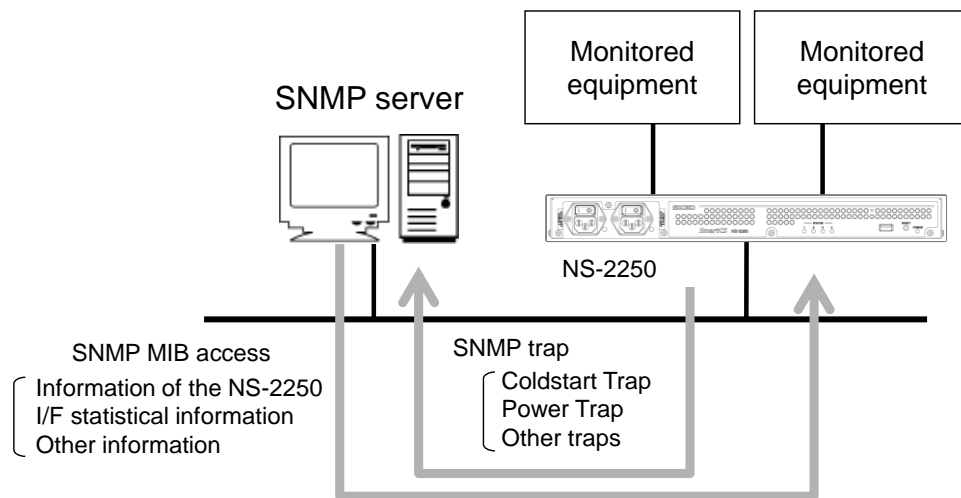
Figure 5-3 SNMP function

To use the SNMP function of the NS-2250, carry out the following procedure to configure the NS-2250 and the SNMP server.

(1)Configure the SNMP agent function of the NS-2250.

For the SNMP agent function of the NS-2250, see Section 2.4, "Operation management functions".

To configure the SNMP agent function of the NS-2250, see Section 4.7.2, "Configure the SNMP agent".

(2)Configure the information to manage the NS-2250 (IP address of the NS-2250, community, and access privileges) to the SNMP server.

(3)Import the MIB file of the NS-2250 into the SNMP server, if necessary.

Download the MIB file of the NS-2250 from our website (http://www.seiko-sol.co.jp/).

5.5   Manage system software

This section describes the configuration of the system software of the NS-2250.

The NS-2250 stores the system software internally. NS-2250 has two sets of system software: system software (main), which is normally used, and system software (backup), which is used when system software (main) cannot be used.

You can switch between the two types of systems software manually.
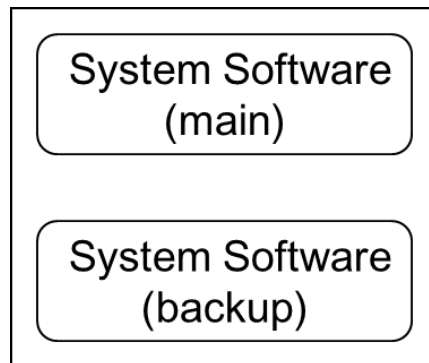
Figure 5-4 System software configuration

5.5.1 Switch the system software to be started

There are two ways to specify the system software to be started: using the "reboot" command and using Rom-Monitor.

(1)   Switch the system software to be started by using the "reboot" command
You can specify the system software to be read during a restart by using the "reboot" command.
To read the system software (backup) during a restart, carry out the following command.

```
(c)NS-2250# reboot backup↵
Do you really want to reboot with backup system and startup1 [y/n] ? y↵
```

(2)   Switch the system software to be started by using Rom-Monitor
You can specify the system software to be read when the power of the NS-2250 switched on or after a "shutdown" command by using Rom-Monitor.
If the system software (main) cannot be started for some reason, use Rom-Monitor to carry out the "boot-b" command to restart using the system software (backup).

The following procedure shows how to switch the system software to be started by using Rom-Monitor.

(1) Connect a device management terminal to the CONSOLE port of the NS-2250.

(2) Switch on the power of the NS-2250. After the message "Hit [Enter] key to Enter Rom-Monitor..." appears on the device management terminal, quickly press the Enter key to display the "MON>" prompt of Rom-Monitor.

```
Hit [Enter] key to Enter Rom-Monitor...
MON>
```

(3) Carry out the "boot" command while specifying the "-b" option to start the system software (backup).

```
MON> boot -b↵
ROM Boot
            :
```

For details of Rom-Monitor, see Appendix C, "Rom-Monitor".

(3) Check the system software
If system software (backup) is started, the prompt changes as shown below. (An asterisk (*) is displayed at the front of the prompt.)

```
NS-2250 login: root↵
Password: ↵
*(c)NS-2250#
```

To confirm that the specified system software was started, carry out the "show version" command, and then check the system software and version that started.

```
*(c)NS-2250# show version↵
System              : System Software Ver 1.0 (Build 2015-XX-XX)
Boot Status         : Reboot (05:80:00)
System Up Time      : 2015/07/03 21:12:07
Local MAC Address   : 00:80:15:XX:XX:XX
Number of MAC Address : 2
Model               : NS-2250-48 (48 port)
Serial No.          : XXXXXXXX
BootROM             : Ver X.X.X
Main Board CPU      : e500v2 (533.333328MHz)
Main Memory         : 1025264 KBytes
Boot System         : backup (Ver 1.0)
Boot Config         : external startup1
Main System         : Ver 1.0.1
Backup System       : Ver 1.0
*(c)NS-2250#
```

5.5.2 Copy system software

For the system software of the NS-2250, you can copy the system firmware that is currently running to the system firmware that is not running.

To copy system software (main) to system software (backup), carry out for the "copy system" command as shown below.

```
(c)NS-2250# copy system main to backup↵
Do you copy main system to backup system [y/n] ? y↵
Please wait a few minutes...done.
copy successful
```

5.5.3 Restore system software

In the unlikely event that the system software (main) is corrupted and cannot be started, you can recover the system software (main) if you use the system software copy function to copy the system software (backup) to the system software (main).

To copy system software (backup) to system software (main), start system software (backup), and then carry out for the "copy system" command as shown below.

```
MON> boot -b↵
ROM Boot
   :

NS-2250 login: root↵
Password:
*(c)NS-2250# copy system backup to main↵
Do you copy backup system to main system [y/n] ? y↵
Please wait a few minutes...done.
copy successful
*(c)NS-2250#
```

For details of Rom-Monitor, see Appendix C, "Rom-Monitor".

5.5.4 Upgrade or downgrade system software

This section describes the procedure to upgrade or downgrade the system software of the NS-2250. While the system software file sent to the NS-2250 is different, the upgrade and downgrade operations and procedures are the same.

The procedures to upgrade or downgrade the NS-2250 are described using the following conditions: IP address of NS-2250: "192.168.1.100", IP address of the FTP/TFTP server or FTP client: "192.168.1.101".

(1) Obtaining the difference file
Obtain the difference file (example: system.2250.Verxxx), and then save it to the FTP/TFTP server or FTP client.
For the method to obtain the difference file, contact your dealer or our support department.

(2) Clear the difference file area
Before transmitting the difference file, clear the area to be used by the upgrade/downgrade as a precaution.

```
(c)NS-2250# verup cleanup↵
clean up successful
(c)NS-2250#
```

(3) Transfer the difference file
Transfer difference file to the NS-2250 by the following either one of the ways below.
        - Way using the tftp command of NS-2250
        - Way using the ftp command of NS-2250
        - Way using the FTP/SFTP client

■ Way using the tftp command of NS-2250

Before starting work, prepare a difference file with the name "system" on the TFTP server. Next, carry out the following command to acquire the difference file from the TFTP server (192.168.1.101).

```
(c)NS-2250# tftp get verup system 192.168.1.101↵
(c)NS-2250#
```

■ Way using the ftp command of NS-2250

Before starting work, prepare a difference file with the name "system" on the FTP server. Next, carry out the following command to acquire the difference file from the FTP server (192.168.1.101). Carry out the FTP "get" command to transfer the difference file (example: system.2250.Verxxx) with the file name "system". If the FTP transfer fails, try again. Always transmit system software using binary mode. Do not carry out other directory or file operations.

```
(c)NS-2250# ftp verup 192.168.1.101↵
Connected to 10.5.31.171 (192.168.1.101).
220 FTP Server ready.
Name (192.168.1.101:root): XXXX↵
331 Password required for XXXX
Password:
230 User user1 logged in.
ftp> hash↵
Hash mark printing on (1024 bytes/hash mark).
ftp> binary↵
200 Type set to I
ftp> get system.2250.v101 system↵
local: system remote: system.2250.v101
227 Entering Passive Mode (192.168.1.101,218,103).
150 Opening BINARY mode data connection for system.v101 (3866548 bytes)
#################################################
#################################################
#################################################
#################################################
###################################################
226 Transfer complete
3866548 bytes received in 0.333 secs (11607.59 Kbytes/sec)
ftp> exit↵
221 Goodbye.
#
```

■ Way using the FTP/SFTP client

Carry out the "enable ftpd" command to enable the FTP server of the NS-2250. Next, carry out the "create allowhost" command to allow FTP/SFTP connections from the client terminal.
Configure the password for the upgrade user (verup).
To use an SFTP client, which uses the SSH protocol, refer to Section 4.6.6, "Configure the SSH server" and Section 4.6.7, "Control access to servers", and then configure the SSH server of the NS-2250.

```
(c)NS-2250# enable ftpd↵
(c)NS-2250# create allowhost 192.168.1.0/24 service ftpd↵
(c)NS-2250# set user verup password↵
Changing password for user verup.
New password: ↵
Retype new password:↵
Password for verup changed
(c)NS-2250#
```

From the client terminal, carry out the "ftp" command, and then log in to the NS-2250 as an upgraded user (verup). Carry out the FTP "put" command to transfer the difference file (example: system.2250.Verxxx) with the file name "system". If the FTP transfer fails, try again. Always transmit system software using binary mode. Do not carry out other directory or file operations.

```
$ ftp 192.168.1.100↵
Connected to 192.168.1.100 (192.168.1.100).
220 10.5.31.186 FTP server ready
Name (192.168.1.100:ne): verup↵
Password: ↵
------------------------------------------
Welcome to NS-2250.
"/verupfiles" : version-up files
"/support" : support files
------------------------------------------
230 User verup logged in
ftp> hash↵
Hash mark printing on (1024 bytes/hash mark).
ftp> binary↵
200 Type set to I
ftp> cd verupfiles↵
250 CWD command successful
ftp> put system.2250.v101 system↵
local: system.2250.v101 remote: system
227 Entering Passive Mode (192,168,1,100,179,8).
150 Opening BINARY mode data connection for system.2250.v101
#####################
ftp> quit↵
221 Goodbye.
$
```

(4) Run the upgrade/downgrade
Carry out the "verup execute" command to run the upgrade/downgrade. If the upgrade finishes, a restart confirmation message appears. Enter "y". If "y" is entered, the NS-2250 restarts.

```
(c)NS-2250# verup execute↵
Do you update main-system version [y/n] ? y↵
```

> Caution Carry out the "verup execute" command to confirm that the system software sent via FTP is appropriate. If an error message appears after you carry out the "verup execute" command, send the system software to the NS-2250 again, and then carry out the "verup execute" command.

> Caution Rebooting may take a long time after the "verup execute" command and upgrade/downgrade have been carried out. Do not switch off the power or press the RESET switch until the NS-2250 starts. Otherwise, the system software will no longer start.

(5) Restart the NS-2250
NS-2250 is restarted.

```
(c)NS-2250# reboot↵
Do you really want to reboot with main system and startup1 [y/n] ? y↵
```

(6) Check the results of the upgrade/downgrade
After the NS-2250 restarts, carry out the "show version" command and then check the version of the system software. Furthermore, confirm that the functions of the NS-2250 are operating normally.

```
(c)NS-2250> show version↵
System                : System Software Ver 1.0.1 (Build 2015-XX-XX)
Boot Status           : Reboot (05:80:00)
System Up Time        : 2015/07/03 21:12:07
Local MAC Address     : 00:80:15:XX:XX:XX
Number of MAC Address : 2
Model                 : NS-2250-48 (48 port)
Serial No.            : XXXXXXXX
BootROM               : Ver X.X.X
Main Board CPU        : e500v2 (533.333328MHz)
Main Memory           : 1025264 KBytes
Boot System           : main (Ver 1.0.1)
Boot Config           : external startup1
Main System           : Ver 1.0.1
Backup System         : Ver 1.0
(c)NS-2250#
```

(7)   Copy system software

If necessary, make sure that the system software (backup) is the same version as that of the system software (main). To copy system software (main) to system software (backup), carry out for the "copy system" command.

```
 (c)NS-2250# copy system main to backup↵
Do you copy main system to backup system [y/n] ? y↵
Please wait a few minutes...done.
copy successful
```

5.5.5 Replace system software

This section describes the procedure to replace the system software of the NS-2250.
The procedures to replace the NS-2250 are described using the following conditions: IP address of NS-2250: "192.168.1.100", IP address of the FTP/TFTP server or FTP client: "192.168.1.101".

(1) Obtaining the system image file
Obtain the system image file (example: NS-2250.sys.vXXX), and then save it to the FTP/TFTP server or FTP client.
For the method to obtain the system image file, contact your dealer or our support department.

(2) Clear the system image file area
Before transmitting the system image file, clear the area to be used by the restoration as a precaution.

```
(c)NS-2250# clear system-image↵
Do you really clear NS-2250.sys system-image [y/n]? y↵
clear successful
(c)NS-2250#
```

(3) Transfer the system image file
Transfer system image file to the NS-2250 by the following either one of the ways below.
        - Way using the tftp command of NS-2250
        - Way using the ftp command of NS-2250
        - Way using the FTP/SFTP client

■ Way using the tftp command of NS-2250

Before starting work, prepare a system image file with the name "NS-2250.sys" on the TFTP server. Next, carry out the following command to acquire the system image file from the TFTP server (192.168.1.101).

```
(c)NS-2250# tftp get verup system 192.168.1.100↵
(c)NS-2250#
```

■ Way using the ftp command of NS-2250

Before starting work, prepare a system image file with the name "NS-2250.sys" on the FTP server. Next, carry out the following command to acquire the system image file from the FTP server (192.168.1.101). Carry out the FTP "get" command to transfer the system image file (example: NS-2250.sys.vXXX) with the file name "NS-2250.sys". If the FTP transfer fails, try again. Always transmit system software using binary mode. Do not carry out other directory or file operations.

```
(c)NS-2250# ftp verup 192.168.1.101↵
Connected to 10.5.31.171 (192.168.1.101).
220 FTP Server ready.
Name (192.168.1.101:root): XXXX↵
331 Password required for XXXX
Password:
230 User user1 logged in.
ftp> hash↵
Hash mark printing on (1024 bytes/hash mark).
ftp> binary↵
200 Type set to I
ftp> get NS-2250.sys.v101 NS-2250.sys↵
local: NS-2250.sys remote: NS-2250.sys.v101
227 Entering Passive Mode (192.168.1.101,218,103).
150 Opening BINARY mode data connection for NS-2250.sys (11337695 bytes)
#################################################
#################################################
#################################################
#################################################
###################################################
226 Transfer complete
11337695 bytes received in 0.333 secs (11607.59 Kbytes/sec)
ftp> exit↵
221 Goodbye.
#
```

■ Way using the FTP/SFTP client

Carry out the "enable ftpd" command to enable the FTP server of the NS-2250. Next, carry out the "create allowhost" command to allow FTP/SFTP connections from the client terminal.
Configure the password for the upgrade user (verup).
To use an SFTP client, which uses the SSH protocol, refer to Section 4.6.6, "Configure the SSH server" and Section 4.6.7, "Control access to servers", and then configure the SSH server of the NS-2250.

```
 (c)NS-2250# enable ftpd↵
 (c)NS-2250# create allowhost 192.168.1.0/24 service ftpd↵
 (c)NS-2250# set user verup password↵
Changing password for user verup.
New password: ↵
Retype new password:↵
Password for verup changed
 (c)NS-2250#
```

From the client terminal, carry out the "ftp" command, and then log in to the NS-2250 as an upgraded user (verup). Carry out the FTP "put" command to transfer the system image file (example: NS-2250.sys.vXXX) with the file name "NS-2250.sys". If the FTP transfer fails, try again. Always transmit system software using binary mode. Do not carry out other directory or file operations.

```
$ ftp 192.168.1.100↵
Connected to 192.168.1.100 (192.168.1.100).
220 10.5.31.186 FTP server ready
Name (192.168.1.100:user1): verup↵
Password: ↵
-----------------------------------------
Welcome to NS-2250.
"/verupfiles" : version-up files
"/support" : support files
-----------------------------------------
230 User verup logged in
ftp> hash↵
Hash mark printing on (1024 bytes/hash mark).
ftp> binary↵
200 Type set to I
ftp> cd verupfiles↵
250 CWD command successful
ftp> put NS-2250.sys.v101 NS-2250.sys↵
local: NS-2250.sys.v101 remote: NS-2250.sys
227 Entering Passive Mode (192,168,1,100,179,8).
150 Opening BINARY mode data connection for NS-2250.sys
####################
ftp> quit↵
221 Goodbye.
$
```

(4) Check the version of the system image
After the system image file transferred, carry out the "show system-image" command, and then check the version of the system image.

```
(c)NS-2250# show system-image↵
System Image Name : NS-2250.sys
Product           : NS-2250
Version           : 1.0.1
Date              : 2015-XX-XX
Status            : available
(c)NS-2250#
```

(5) Restore the system software
Restore the transferred system image in the main system.

```
(c)NS-2250# restore system-image to main↵
Do you restore NS-2250.sys to main-system [y/n] ? y↵
Please wait a few minutes... done.
restore successful
(c)NS-2250#
```

(6) Restart the NS-2250
NS-2250 is restarted.

```
(c)NS-2250# reboot↵
Do you really want to reboot with main system and startup1 [y/n] ? y↵
```

(7) Check the results of the upgrade/downgrade
After the NS-2250 restarts, carry out the "show version" command and then check the version of the system software. Furthermore, confirm that the functions of the NS-2250 are operating normally.

```
(c)NS-2250> show version↵
System              : System Software Ver 1.0.1 (Build 2015-XX-XX)
Boot Status         : Reboot (05:80:00)
System Up Time      : 2015/07/03 21:12:07
Local MAC Address   : 00:80:15:XX:XX:XX
Number of MAC Address : 2
Model               : NS-2250-48 (48 port)
Serial No.          : XXXXXXXX
BootROM             : Ver X.X.X
Main Board CPU      : e500v2 (533.333328MHz)
Main Memory         : 1025264 KBytes
Boot System         : main (Ver 1.0.1)
Boot Config         : external startup1
Main System         : Ver 1.0.1
Backup System       : Ver 1.0
(c)NS-2250#
```

(8)   Copy system software

If necessary, make sure that the system software (backup) is the same version as that of the system software (main). To copy system software (main) to system software (backup), carry out for the "copy system" command.

```
 (c)NS-2250# copy system main to backup↵
Do you copy main system to backup system [y/n] ? y↵
Please wait a few minutes...done.
copy successful
```

5.5.6 Save system software

This section describes the procedure to save the system software of the NS-2250.
The procedures to replace the system image of NS-2250 are described using the following
conditions: IP address of NS-2250: "192.168.1.100", IP address of the FTP/TFTP server or
FTP client: "192.168.1.101".

(1) Save the system image file
Create the system image file, choose from a system software of one main or backup.

```
■An example of system software(main)
(c)NS-2250# backup system-image main↵
Do you really create NS-2250.sys system-image [y/n] ? y↵
Please wait a few minutes... done.
backup successful
(c)NS-2250#


■An example of system software(backup)
(c)NS-2250# backup system-image backup↵
Do you really create NS-2250.sys system-image [y/n] ? y↵
Please wait a few minutes... done.
backup successful
(c)NS-2250#
```

(2) Check the system image
After the system image file transferred, carry out the "show system-image" command, and
then check the version of the system image.

```
(c)NS-2250# show system-image↵
System Image Name : NS-2250.sys
Product           : NS-2250
Version           : 1.0.1
Date              : 2015-XX-XX
Status            : available
(c)NS-2250#
```

(3) Transfer the system image file
Transfer system image file to the NS-2250 by the following either one of the ways below.
- Way using the tftp command of NS-2250
- Way using the ftp command of NS-2250
- Way using the FTP/SFTP client

■ Way using the tftp command of NS-2250

Save an image file of the name as NS-2250.sys in a TFTP server. Carry out the following command to transfer the system image file to the TFTP server (192.168.1.101).

```
(c)NS-2250# tftp put verup system-image 192.168.1.101↵
(c)NS-2250#
```

■ Way using the ftp command of NS-2250

Backup an image file of the name as NS-2250.sys in a FTP server. Carry out the following command to transfer the system image file to the FTP server (192.168.1.101). If the FTP transfer fails, try again. Always transmit system software using binary mode. Do not carry out other directory or file operations.

```
(c)NS-2250# ftp verup 192.168.1.101↵
Connected to 10.5.31.171 (192.168.1.101).
220 FTP Server ready.
Name (192.168.1.101:root): XXXX↵
331 Password required for XXXX
Password:
230 User user1 logged in.
ftp> hash↵
Hash mark printing on (1024 bytes/hash mark).
ftp> binary↵
200 Type set to I
ftp> put NS-2250.sys NS-2250.sys.v101↵
local: NS-2250.sys.v101 remote: NS-2250.sys
227 Entering Passive Mode (192.168.1.101,218,103).
150 Opening BINARY mode data connection for NS-2250.sys.v101 (11337695 bytes)
##################################################
##################################################
########################################################
226 Transfer complete
11337695 bytes received in 0.333 secs (11607.59 Kbytes/sec)
ftp> exit↵
221 Goodbye.
#
```

■ Way using the FTP/SFTP client

Carry out the "enable ftpd" command to enable the FTP server of the NS-2250. Next, carry out the "create allowhost" command to allow FTP/SFTP connections from the client terminal.
Configure the password for the upgrade user (verup).
To use an SFTP client, which uses the SSH protocol, refer to Section 4.6.6, "Configure the SSH server" and Section 4.6.7, "Control access to servers", and then configure the SSH server of the NS-2250.

```
(c)NS-2250# enable ftpd↵
(c)NS-2250# create allowhost 192.168.1.0/24 service ftpd↵
(c)NS-2250# set user verup password↵
Changing password for user verup.
New password: ↵
Retype new password:↵
Password for verup changed
(c)NS-2250#
```

From the client terminal, carry out the "ftp" command, and then log in to the NS-2250 as an upgraded user (verup). Carry out the FTP "get" command to transfer the system image file "NS-2250.sys" with the file name (example: NS-2250.sys.vXXX). If the FTP transfer fails, try again. Always transmit system software using binary mode. Do not carry out other directory or file operations.

```
$ ftp 192.168.1.100↵
Connected to 192.168.1.100 (192.168.1.100).
220 10.5.31.186 FTP server ready
Name (192.168.1.100:user1): verup↵
Password: ↵
-----------------------------------------
Welcome to NS-2250.
"/verupfiles" : version-up files
"/support" : support files
-----------------------------------------
230 User verup logged in
ftp> hash↵
Hash mark printing on (1024 bytes/hash mark).
ftp> binary↵
200 Type set to I
ftp> cd verupfiles↵
250 CWD command successful
ftp> get NS-2250.sys NS-2250.sys.v101↵
local: NS-2250.sys.v101 remote: NS-2250.sys
227 Entering Passive Mode (192,168,1,100,179,8).
150 Opening BINARY mode data connection for NS-2250.sys
####################
ftp> quit↵
221 Goodbye.
$
```

5.6   Save and download port logs manually

This section describes the procedures to save port logs of the NS-2250 to a FLASH memory, download port logs by an FTP client, and send them to a TFTP server.

(1) Save port logs manually
To save the port logs of serial port 1 to the FLASH memory, carry out the "logsave" command as shown below. If you carry out the "logsave" command while specifying a serial port, port logs of the specified serial port are saved to the FLASH memory with the following file name: *tty number_ YYMMDDHHMM*.log

```
(c)NS-2250# logsave tty 1↵
(c)NS-2250#
```

You can check a list of the saved port logs by carrying out the "loginfo" command.

```
(c)NS-2250# loginfo↵
Total(1K-blocks)    Used      Available      Use%
----------------------------------------------
          308983    3064          286447        1%


Size        SaveTime      Name
----------------------------------------------
        82  Jul 9 21:09   tty01_1507092109.log
                  :

(c)NS-2250#
```

(2)   Transfer port logs saved to a FLASH memory

To save port logs to the TFTP server, carry out the following command.

```
(c)NS-2250# tftp put log tty01_1507092109.log 192.168.1.100↵
(c)NS-2250#
```

To download port logs using the FTP client, carry out the following work.
Before downloading port logs using the FTP client, configure to allow access from the FTP client to the NS-2250 as a log download user (log).
To use an SFTP client, which uses the SSH protocol, refer to Section 4.6.6, "Configure the SSH server" and Section 4.6.7, "Control access to servers", and then configure the SSH server of the NS-2250.

```
(c)NS-2250# enable ftp↵
(c)NS-2250# create allowhost all service ftpd↵
(c)NS-2250# set user log password↵
Changing password for user log.
New password: ↵
Retype new password: ↵
Password for log changed
```

From the FTP client, log in to the NS-2250 as a log download user (log), and then confirm that the saved port logs are present. (Do not carry out other directory or file operations.)

```
$ ftp 192.168.1.100↵
Connected to 192.168.1.100
220 (Welcome to FTP service.)
530 Please login with USER and PASS.
Name (192.168.1.100:log): log↵
331 Please specify the password.
Password: ↵
230 Login successful.

ftp> ls↵
227 Entering Passive Mode (192.168.1.100,222,247)
150 Here comes the directory listing.
drwxr-xr-x   3 200     0          1024 Oct 16 12:02 logfiles
226 Directory send OK.

ftp> cd logfiles↵
250 Directory successfully changed.

ftp> ls↵
227 Entering Passive Mode (192.168.1.100,222,247)
150 Here comes the directory listing.
-rw-rw-rw-  1 200   200      118902 Oct 11 05:41 tty01_1507092109.log
-rw-rw-rw-  1 200   200     3072016 Oct 12 01:21 tty01_1507121021.log
-rw-rw-rw-  1 200   200      102420 Oct 11 05:47 tty02_1507111447.log
-rw-rw-rw-  1 200   200     3072016 Oct 11 01:22 tty03_1507121022.log
226 Directory send OK.
ftp>
```

Download the saved port log files to the FTP client.

```
ftp> get tty01_1507092109.log↵
local: tty01_0610111441.log remote: tty01_0610111441.log
227 Entering Passive Mode (192.168.1.100,200,242)
150 Opening ASCII mode data connection for tty01_1507092109.log (28 bytes).
#
226 File send OK.
28 bytes received in 0.0013 seconds (22 Kbytes/s)
ftp>
```

Finally, delete the port log files, and then exit the FTP client.

```
ftp> delete tty01_1507092109.log↵
250 Delete operation successful.
ftp> quit↵
$
```

5.7   Reset to the default setting

To reset the NS-2250 to default settings, carry out the "clear startup" command.
You can initialize particular startup files only or specify the "all" option to initialize all startup files (startup1 to 4 files on the USB memory and within the NS-2250).
To initialize various log files at the same time, carry out the "shutdown logclear" command. After the "MON>" prompt appears, switch off the power of the NS-2250.

```
(c)NS-2250# clear startup all↵
```

Caution Do not carry out the "write" command. If you carry out the "write" command, the current running configuration overwrites the default startup file.

To initialize various log files, carry out the "shutdown logclear" command. After the "MON>" prompt appears, switch off the power of the NS-2250.

```
(c)NS-2250# shutdown logclear↵
Do you really want to shutdown and clear log files [y/n] ? y↵
     :
MON>
```

Chapter 6
Troubleshooting

Chapter 6 describes the troubleshooting of NS-2250.

6.1   Overview of troubleshooting

The trouble with the NS-2250 is separated into the following sections: NS-2250 hardware errors, connection trouble with network communication, and connection trouble with serial communication.

When some trouble has occurred within NS-2250, list the symptoms or phenomenon, and then refer to this chapter to resolve the problem.

Furthermore, the Technical Information section on our web site includes frequently asked questions about the NS-2250 and other technical information. See the following URL.

http://www.seiko-sol.co.jp/

6.2   NS-2250 hardware trouble

This section describes how to deal with trouble related to the hardware of the NS-2250.

6.2.1 The power does not switch on

If the power of the NS-2250 does not switch on (the POWER light is not on) even after checking the following, the NS-2250 is likely malfunctioning. Switch off the power of the NS-2250 immediately, unplug the power cable, and then request for repair.

Is the power cable connected?
It is the POWER switch on?
It is power being supplied to the outlet?

6.2.2 The STATUS lights are on or flashing

If the power of the NS-2250 is switched on, the POWER light switch on, and the startup process begins. The STATUS lights switch on in the following order. If the NS-2250 starts normally, all the STATUS lights switch off.

If the power of the NS-2250 is switched on and the STATUS lights remain on or are flashing, refer to the following table, and then carry out troubleshooting.

*1 STATUS light 1	2	3	4	Status and action
●	●	●	●	Hardware initialization has been completed. Just after the power is switched on, the NS-2250 enters this status for an instant. If this status continues after the power has been switched on, the NS-2250 is likely to malfunctioning. Repair is necessary.
●	○	○	○	A self-diagnostic test (POC) is running (about 30 seconds). If this status continues, the NS-2250 is likely malfunctioning. Repair is necessary.
○	●	○	○	Rom-Monitor is running (about 3 seconds). If this status continues, the NS-2250 is likely malfunctioning. Repair is necessary.
○	○	●	○	System software starting (1st Boot). If this status continues, the NS-2250 is likely malfunctioning. Repair is necessary.
●	○	●	○	The system software is starting. If this status continues, there is likely a problem with the system software. Contact your dealer.
●	○	●	●	The system software is starting (during USB memory access). This makes take a long time depending on the settings. If this status continues for 30 minutes or longer, there is likely a problem with the system software. Contact your dealer.
◎	◎	◎	◎	A hardware error was detected. The NS-2250 is likely malfunctioning. Repair is necessary.
◎	○	○	○	An error was detected while a self-diagnostic test (POC) was running. The NS-2250 is likely malfunctioning. Repair is necessary.
○	◎	○	○	An error was detected while a Rom-Monitor was running. Repair is necessary. If the Enter key is pressed, an error message appears. Furthermore, if the "err" command is carried out at the "MON>" prompt, a detailed error message appears. Note the error messages, and then request a repair.
○	○	◎	○	An error was detected while system software was running. Repair is necessary. If the Enter key is pressed, an error message appears. Furthermore, if the "err" command is carried out at the "MON>" prompt, a detailed error message may appear. Note the error messages, and then request a repair.
○	○	○	○	The start of the system software has completed. The operation is normal.
○	○	○	●	During USB memory accessing. (During write command execution) If this status continues, the NS-2250 is likely malfunctioning. Repair is necessary.

*1: STATUS light symbols: ○ : off, ● : on, ◎ : flashing

6.3　Communication trouble

Communication troubleshooting can be separated into the following methods.

Check error messages saved in the console logs
If an error message is displayed when the NS-2250 is started or during communication, this message is saved in the console logs. When trouble occurs, you can deal with the trouble by checking error messages saved in the console logs.
Check settings
If the NS-2250 is not operating as intended, you may be able to deal with the problem by checking settings.
Check the cable connection and communication status from the status of the lights of the NS-2250
You can perform a basic check by checking whether cables are connected correctly or whether physical damage has occurred.
Check the communication status by using commands
You can check the communication status or statistical information of the NS-2250.

For details of commands used to resolve the trouble, see the following sections and the *Command Reference*.

6.3.1　Check console logs

Messages displayed by the NS-2250 (console messages) are output to the CONSOLE port and saved to the console logs simultaneously. When trouble has occurred, refer to the console logs and check for errors.

If you want to check the console messages of the NS-2250 in real-time, connect a device management terminal (such as a personal computer equipped with terminal software) to the CONSOLE port of the NS-2250. When you have used a telnet client to log into the NS-2250 from a network terminal, use the "su" command to change to a device management user, and then carry out the "console" command to display the console messages on the telnet client as well.
Note that you can display the console logs again by carrying out the "show log" command after using the "su" command to become a device management user.

Display all console logs

```
(c)NS-2250# show log console↵
```

Display of the 20 most recent lines of the console log

```
(c)NS-2250# show log console 20↵
```

6.3.2 Check settings

If the NS-2250 is not operating as intended, check the settings of the NS-2250.

You can check the settings of the NS-2250 by viewing the running configuration.

```
(c)NS-2250# show config running↵
...............
#
echo "SYSTEM configuration..."
#
set timezone Tokyo
#
#
echo "IP configuration..."
#
set hostname NS-2250
set ipaddr eth1 192.168.1.1/24
#
#
echo "IP6 configuration..."
#
create ip6
set ip6addr eth1 2001:db8::2/64
#
#
echo "User configuration..."
#
create user setup group setup uid 198
create user verup group verup uid 199
create user log group log uid 200
create user somebody group normal uid 100
create user port02usr group portusr uid 501 encrypt
$1$g6Zk1eRm$60Tw3/CeqfvLjVLnjn5Mh/
set user port02usr port 1,2,3,4,5,6,7,8,9,10
#
echo "IP ROUTE configuration..."
#
create ip route default gateway 192.168.1.254
#
#
echo "IP6 ROUTE configuration..."
#
create ip6route default gateway 2001:db8::ffff
#
    :
(c)NS-2250#
```

6.3.3 Network communication connection trouble

(1) Check the LINK/ACT light

If the LAN port LINK/ACT light on or flashing the rear of NS-2250 is off even after checking the following items or (3) below, the NS-2250 is likely malfunctioning. Switch off the power of the NS-2250 immediately, unplug the power cable, and then request for repair.

It is the LAN cable connected to the LAN port of the NS-2250 correctly?

Is the LAN cable connected to network equipment (such as a hub or switch) of the LAN port of the NS-2250 correctly?

Does the LINK light remain off even after exchanging the LAN cable?

(2) Check by using the "ping/ping6" command

Carry out the "ping/ping6" command from the console of the NS-2250, and then check that the ping reaches from the NS-2250 to the client terminal.

```
(c)NS-2250# ping 192.168.1.100↵
PING 192.168.1.254 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=0 ttl=64 time=0.497 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.352 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.345 ms

--- 192.168.1.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.345/0.398/0.497/0.070 ms, pipe 2
(c)NS-2250#
```

```
(c)NS-2250# ping6 2001:db8::22↵
PING 2001:db8::22 (2001:db8::22):56 data bytes
64 bytes from 2001:db8::22: seq=0 ttl=64 time=0.117 ms
64 bytes from 2001:db8::22: seq=1 ttl=64 time=0.150 ms
64 bytes from 2001:db8::22: seq=2 ttl=64 time=0.148 ms

--- 2001:db8::22 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.148/0.158/0.177 ms
(c)NS-2250#
```

(3) Check by using the "show" commands

If you cannot confirm communication by carrying out the "ping/ping6" command, check the following items.

Make sure the settings of the LAN port of the NS-2250 and the settings of the networking equipment (such as a hub or switch) match.
In particular, make sure the auto-negotiation setting (enabled or disabled) of the NS-2250 and the networking equipment match.

```
(c)NS-2250# show ether↵
Eth   Link    Nego    Speed     Duplex  MDI
----------------------------------------------
eth1  UP      enable  1000Mb/s  full    mdi
eth2  DOWN    enable  ---       ---     ---
(c)NS-2250#
```

Check the transceiver counter and error counter of the LAN port of the NS-2250 and make sure there are no errors.

```
(c)NS-2250# show stats ether
           <Receive Statistics>      <Transmit Statistics>
             Frames         Bytes        Frames         Bytes
 ------------------------------------------------------------
  eth1       687962      45761090          332         23382
  eth2            1            60            0             0


(c)NS-2250# show stats ether 1↵
Statistics eth1
<Receive information>           <Transmit information>
 ------------------------------------------------------------
Bytes                 688847   Bytes                   332
Packets            45818311   Packets               23382
Errs                       0   Errs                     0
Drop                       0   Drop                     0
Fifo                       0   Fifo                     0
Frame                      0   Colls                    0
Compressed                 0   Compressed               0
Multicast                  0   Carrier                  0
(c)NS-2250#
```

Make sure the IP address and net mask of the NS-2250 are correct.

```
(c)NS-2250# show ip↵
Hostname        :NS-2250
IPaddress(eth1)  :192.168.1.1/24
IPaddress(eth2)  :-
(c)NS-2250#
```

```
(c)NS-2250# show ip6↵
IPaddress(eth1)  :2001:db8::2/64
IPaddress(eth2)  :-
(c)NS-2250#
```

If the client terminal is connected to a different network address, carry out the "show ip route/show ip6route" command and make sure the static route of the client terminal has been configured correctly.

```
(c)NS-2250# show ip route
destination     netmask         gateway         met  iface status
-------------------------------------------------------------
192.168.1.0     255.255.255.0   ---             0    eth1  -
0.0.0.0         0.0.0.0         192.168.1.1     0    eth1  -
(c)NS-2250#
```

```
(c)NS-2250# show ip6route
destination             gateway             met iface status
-------------------------------------------------------------
2001:db8::/64           ---                 0   eth1  -
::/0                    2001:db8::ffff      0   eth1  inact
(c)NS-2250#
```

(4) Check access control of the servers
    If you cannot connect to the NS-2250 from a telnet or FTP client, check the status and
    access control of the servers of the NS-2250.

```
(c)NS-2250# show service↵
<telnetd>
 status    : enable
 port      : 23

<sshd>
 status    : enable
 port      : 22
 auth      : public
 host_key  : device_depend

<ftpd>
 status    : enable

(c)NS-2250# show allowhost↵
Service         Address/Mask                    Access tty List
------------------------------------------------------------
portd/telrw    all                              all
telnetd        all                              -

(c)NS-2250#
```

(5) Disconnect the ftp connections
    When a session of ftp/ftpd/sftpd can't be established, disconnect by the following
    command.

```
(c)NS-2250# disconnect ftp↵
(c)NS-2250# disconnect ftpd↵
(c)NS-2250# disconnect sftpd↵
```

6.3.4 Serial communication connection trouble

(1) Check the Tx and Rx light

If the Tx and Rx light on the rear of NS-2250 are off and serial communication is not possible even after checking the following items, the NS-2250 is likely malfunctioning. Switch off the power of the NS-2250 immediately, unplug the power cable, and then request for repair.

It is the serial cable connected to the serial port of the NS-2250 correctly?

Is this serial cable connected to monitored equipment correctly?

Is the serial cable wiring connected correctly?

Has an incorrect serial cable conversion connector been used? (NS-354 (DB9-RJ45 conversion connector)/NS-490 (DB9-RJ45 conversion connector (cross-type))

Do the Tx and Rx light not switch on even after you exchanged the serial cable?

For serial ports and conversion connector wiring connections, see the *Installation Manual*.

Caution   Depending on the connected network equipment, it may be possible to communicate even when the Tx and Rx light is off.

(2)   Check by using the "show" commands

Carry out the "show" commands, and then check the status of serial ports, the port server, and services.

Make sure the serial port settings are correct.

```
(c)NS-2250# show tty 3↵
tty : 3   "Tokyo-Switch-3"
   baud      : 9600
   bitchar   : 8
   parity    : none
   stop      : 1
   flow      : xon
   detect_dsr : off
(c)NS-2250#
```

- Check the status of the port server and make sure the port numbers are correct.

```
(c)NS-2250# show portd↵
auth status    : none
connect status : direct
base port number
        telnet rw : 8101  ro :  8201
        ssh    rw : 8301  ro :  8401
timeout status
  idle_timeout : off
  ro_timeout   : off
menu status    : on
--------------------------------------------------------------------
tty Label                          Listen Port            TimeOut
                                   telrw telro sshrw sshro idle  ro
--------------------------------------------------------------------
  1 -                              8101    - 8301    -    -    -
  2 -                              8102    - 8302    -    -    -
  3 -                              8103    - 8303    -    -    -
  4 -                              8104    - 8304    -    -    -
  5 -                              8105    - 8305    -    -    -
  6 -                              8106    - 8306    -    -    -
  7 -                              8107    - 8307    -    -    -
  8 -                              8108    - 8308    -    -    -
  9 -                              8109    - 8309    -    -    -
 10 -                              8110    - 8310    -    -    -
(c)NS-2250#
```

- When you are using the port user authentication function, make sure that the target serial port has been registered to the specified port user.

```
(c)NS-2250# show user↵
User-Name            Category(Uid)   Public-Key Port-Access-List
 -------------------------------------------------------
 root                root(0)
 setup               setup(198)
 verup               verup(199)
 log                 log(200)
 somebody            normal(100)
 portusr             portusr(500)               1-32
 port02usr           portusr(501)               1-10,13
(c)NS-2250#
```

- Check the usage status of the serial port to which you want to connect and make sure that is possible to connect.

When exclusive control function is enabled, it's not able to connect by extension user to the serial port which is already connected by the normal user.

```
(c)NS-2250# show portd session↵
telnet  rw : 3   ro : 0
ssh     rw : 0   ro : 0
available session (telnet only : 69 / ssh only : 46)
-----------------------------------------------------------------
tty   : Label                             Session-Limit
     Type Login-User       Local       Remote
-----------------------------------------------------------------
tty  1 : DB-server                            RW: 2 / RO: 3
     rw 1 port01usr       tel:23    192.168.30.145: 4731
     rw 2 port02usr       tel:23    192.168.30.146: 3495

tty  2 : L3SW No.08                           RW: 2 / RO: 3
     rw 1 port03usr       tel:4740  2001:dba::2.4740
(c)NS-2250#
```

If there are no open sessions, you can forcibly disconnect unnecessary sessions by carrying out the "disconnect" command.

```
 (c)NS-2250# disconnect portd tty 1 rw 1↵
 (c)NS-2250#
```

- Check there are no sessions of extension users in the serial port to which you want to connect. When exclusive control function is enabled, it's not able to connect by the normal user to the serial port which is already connected by extension user.

```
 (c)NS-2250# show ttymanage session

 -----------------------------------------------------------------

 tty Login-User           Remote

 -----------------------------------------------------------------

   1 ext01usr            172.31.100.67:37726

   2 ext02usr            172.21.100.69:50961

   3 ext03usr            2002::200c:417b.36876
 (c)NS-2250#
```

If there are any sessions, check the device number of the logged in user.

```
(c)NS-2250# show user login

User-Name      Dev Login-Time      Idle Remote-Host

-----------------------------------------------------------------

 ext01usr       0   Mar 25 11:24:13 00:00 172.31.100.67

 ext02usr       1   Mar 25 20:09:38 00:34 172.21.100.69

 ext03usr       2   Mar 25 21:05:10 00:20 2002::200c:417b

(c)NS-2250#
```

If there are no open sessions, you can forcibly disconnect sessions of extension users by carrying out the "disconnect" command specifying the device number.

```
(c)NS-2250# disconnect device 0

(c)NS-2250#
```

- When you are using the SSH server function, make sure the SSH server authentication method is correct.

```
(c)NS-2250# show service↵
<telnetd>
 status    : enable
 port      : 23

<sshd>
 status    : enable
 port      : 22
 auth      : public
 host_key : device_depend

<ftpd>
 status    : enable
(c)NS-2250#
```

- Make sure access control of the port server allows the serial port in question.

```
(c)NS-2250# show allowhost↵
Service        Address/Mask                Access tty List
--------------------------------------------------------
portd/sshrw    all                         all
portd/telrw    all                         all
telnetd        all                         -
(c)NS-2250#
```

- Check the transceiver counter and error counter of the serial port of the NS-2250 and make sure there are no errors.

```
(c)NS-2250# show stats tty 3↵
tty : 3
   TX Octets    : 1152
   RX Octets    : 2432
   Error Parity : 0
   Error Framing: 0
   Error Overrun: 0
   Break Count  : 0
   Status       : DSR :on, CTS :on, DTR :on, RTS :on, CD :on
(c)NS-2250#
```

(3) Check by using the "hangup" command
If you checked the conditions by carrying out the "show" commands and still cannot communicate with monitored equipment connected to a serial port, carry out the "hangup" command to reset the serial ports, and then check whether the communication has been restored.

```
(c)NS-2250# hangup tty 1↵
(c)NS-2250#
```

6.3.5 The trouble with the RADIUS authentication/accounting function
When the RADIUS authentication function/RADIUS accounting function of the NS-2250 is not operating correctly, carry out the following checks.

(1)   Check the RADIUS authentication server/RADIUS accounting server
Make sure the RADIUS authentication server/RADIUS accounting server is running and configured correctly.

Can you ping the RADIUS authentication server/RADIUS accounting server from the NS-2250?
Is the RADIUS server program running on the RADIUS authentication server/RADIUS accounting server?
Do the authentication port of the RADIUS authentication server and accounting port of the RADIUS accounting server match the settings of the NS-2250?
Do the secret keys of the RADIUS authentication server/RADIUS accounting server and the NS-2250 match?
Are users registered correctly to the RADIUS authentication server?

(2) Check by the RADIUS authentication function/RADIUS accounting function by using the "show" commands

Carry out the "show" commands listed below, and then make sure the authentication/accounting method, RADIUS authentication client/RADIUS accounting client settings, and access group settings of the NS-2250 are correct.

Check the authentication method and RADIUS authentication client settings
("show auth", "show auth radius", and "show auth access_group" commands)

```
(c)NS-2250# show auth↵
<auth information>
Mode            : radius
su_cmd username  : root

(c)NS-2250# show auth radius↵
<auth radius information>
Retry        : 3
Default User  : none

<radius server 1>
IP address          : 192.168.1.1
Port number         : 1812
Password            : stored
Timeout             : 3
NAS_ID              : SmartCS
Attribute of portusr : ---
Attribute of normal  : ---
Attribute of root    : ---

<radius server 2>
IP address          : 192.168.1.2
Port number         : 1812
Password            : stored
Timeout             : 3
NAS_ID              : SmartCS
Attribute of portusr : ---
Attribute of normal  : ---
Attribute of root    : ---
```

```
(c)NS-2250# show auth access_group↵

Protocol  : Radius                                              6-19
Attribute : Filter-ID
--------------------------------------------------------
<root>
   attr : admin_grp
--------------------------------------------------------
<normal>
   attr : normal_grp
--------------------------------------------------------
<portusr>
   attr : port_grp
          port : 1-32
```

Check the accounting method and RADIUS accounting client settings ("show acct" and
"show acct radius" commands)

```
(c)NS-2250# show acct↵
<acct information>
Mode  : radius

(c)NS-2250# show acct radius↵
<acct radius information>
Retry               : 3
Auth_deny_stop      : remote
Session-id          : 1815249

<radius server 1>
IP address          : 192.168.1.1
Port number         : 1813
Password            : stored
Timeout             : 3
NAS_ID              : SmartCS

<radius server 2>
IP address          : 192.168.1.2
Port number         : 1813
Password            : stored
Timeout             : 3
NAS_ID              : SmartCS
```

Check the statistical information of the RADIUS authentication (show stats auth radius)

```
(c)NS-2250# show stats auth radius↵
<auth radius statistics>
Id IP address        Send   Rcv_Allow   Rcv_Deny   Rcv_Error   Timeout
-----------------------------------------------------------------------
 1 192.168.1.1       121        110          8           0         3
 2 192.168.1.2         3          0          0           0         3
```

Check the statistical information of the RADIUS accounting (show stats acct radius)

```
(c)NS-2250# show stats acct radius↵
<acct radius statistics>
Id IP address       Send_Start  Send_Stop  Rcv_Resp  Rcv_Error  Timeout
-----------------------------------------------------------------------
 1 192.168.1.1           121        110         8          0        3
 2 192.168.1.2             3          0         0          0        3
```

(3)   Check by using the "trace" command

If the settings of the RADIUS authentication client/RADIUS accounting client are correct, carry out the "trace" command to perform a trace of the RADIUS protocol between the NS-2250 and the RADIUS authentication server/RADIUS accounting server. Analyze the results of the "trace" command to confirm that the responses and attributes are returned correctly from the RADIUS authentication server/RADIUS accounting server to the NS-2250.

The "trace" command supports three levels: level 1 (basic), level 2 (advanced), and level 3 (advanced + hex dump). Specify the trace level that meets your objectives.

Note that the "trace" command can trace up to 1,000 packets. The default setting is 50 packets. To end the trace midway, stop the command by pressing Ctrl+C.

Level 1 (basic)

```
(c)NS-2250# trace radius level 1↵


13:49:00.626823 IP 10.1.1.1.16494 >10.1.1.2.radius: RADIUS, Access
Request (1), id: 0xaa length: 70
13:49:00.627522 IP 10.1.1.2.radius > 10.1.1.1.16494: RADIUS, Access
Accept (2), id: 0xaa length: 33
13:49:00.663995 IP 10.1.1.1.16604 > 10.1.1.2.radius-acct: RADIUS,
Accounting Request (4), id: 0xf6 length: 70
13:49:00.670326 IP 10.1.1.2.radius-acct > 10.1.1.1.16604: RADIUS,
Accounting Response (5), id: 0xf6 length: 20
13:49:11.646968 IP 10.1.1.1.16714 > 10.1.1.2.radius-acct: RADIUS,
Accounting Request (4), id: 0x8b length: 82
13:49:11.648192 IP 10.1.1.2.radius-acct > 10.1.1.1.16714: RADIUS,
Accounting Response (5), id: 0x8b length: 20
```

Level 2 (advanced)

```
(c)NS-2250# trace radius level 2↵


13:49:42.287299 IP (tos 0x0, ttl  64, id 0, offset 0, flags [DF], proto 17, length:
98) 10.1.1.1.16510 > 10.1.1.2.radius: RADIUS, length: 70
    Access Request (1), id: 0x36, Authenticator: db690ce1ef1d774451fec2bcfa651857
      Username Attribute (1), length: 6, Value: root
      Password Attribute (2), length: 18, Value:
      NAS IP Address Attribute (4), length: 6, Value: 10.1.1.1
      NAS ID Attribute (32), length: 9, Value: NS-2250
      Accounting Session ID Attribute (44), length: 11, Value: 234661181

13:49:42.287431 IP (tos 0x0, ttl  64, id 0, offset 0, flags [DF], proto 17, length:
61) 10.1.1.2.radius > 10.1.1.1.16510: RADIUS, length: 33
    Access Accept (2), id: 0x36, Authenticator: faa3a7d57a244bbb74f581a62b970364
      Filter ID Attribute (11), length: 13, Value:NS-2250_ROOT

13:49:42.325874 IP (tos 0x0, ttl  64, id 0, offset 0, flags [DF], proto 17, length:
98) 10.1.1.1.16636 > 10.1.1.2.radius-acct: RADIUS, length: 70
    Accounting Request (4), id: 0xb6, Authenticator: 55059f3f0ce697bdb606325686a447f0
      Username Attribute (1), length: 6, Value: root
      NAS IP Address Attribute (4), length: 6, Value: 10.1.1.1
      NAS ID Attribute (32), length: 9, Value: NS-2250
      Accounting Status Attribute (40), length: 6, Value: Start
      Accounting Session ID Attribute (44), length: 11, Value: 234661181
      NAS Port Attribute (5), length: 6, Value: 20000
      Accounting Authentication Attribute (45), length: 6, Value: RADIUS

13:49:42.326965 IP (tos 0x0, ttl  64, id 0, offset 0, flags [DF], proto 17, length:
48) 10.1.1.2.radius-acct > 10.1.1.1.16636: RADIUS, length: 20
    Accounting Response (5), id: 0xb6, Authenticator: 54f30340feaf432ec3126f66dcdd4d8a

13:49:46.318409 IP (tos 0x0, ttl  64, id 0, offset 0, flags [DF], proto 17, length:
110) 10.1.1.1.16762 > 10.1.1.2.radius-acct: RADIUS, length: 82
    Accounting Request (4), id: 0x5c, Authenticator: 6d5bd82dfe5913f294ad2128ede30780
      Username Attribute (1), length: 6, Value: root
      NAS IP Address Attribute (4), length: 6, Value: 10.1.1.1
      NAS ID Attribute (32), length: 9, Value: NS-2250
      Accounting Status Attribute (40), length: 6, Value: Stop
      Accounting Session ID Attribute (44), length: 11, Value: 234661181
      NAS Port Attribute (5), length: 6, Value: 20000
      Accounting Authentication Attribute (45), length: 6, Value: RADIUS
      Accounting Termination Cause Attribute (49), length: 6, Value: User Request
      Accounting Session Time Attribute (46), length: 6, Value: 04 secs

13:49:46.319471 IP (tos 0x0, ttl  64, id 0, offset 0, flags [DF], proto 17, length:
48) 10.1.1.2.radius-acct > 10.1.1.1.16762: RADIUS, length: 20
    Accounting Response (5), id: 0x5c, Authenticator: 9881fcdab1b0fd70b436429f9cbdd84c
```

6.3.6 The trouble with the TACACS+ function

When the TACACS+ function of the NS-2250 is not operating correctly, carry out the following checks.

(1)   Check the TACACS+ server

Make sure TACACS+ server is running and configured correctly.

Can you ping the TACACS+ server from the NS-2250?
Is the TACACS+ server program running on the TACACS+ server?
Is the port number of the TACACS+ server TCP (49)?
Do the secret keys of the TACACS+ server and the NS-2250 match?
Are users registered correctly to the TACACS+ server?

(2)   Check by the TACACS+ function by using the "show" command

Carry out the "show" commands listed below, and then make sure the authentication/approval/accounting method, TACACS+ settings, and access group settings of the NS-2250 are correct.

Check the TACACS+ authentication/approval settings
("show auth", "show auth tacacs", and "show auth access_group" commands)

```
(c)NS-2250# show auth↵
<auth information>
Mode            : tacacs
su_cmd username : root

(c)NS-2250# show auth tacacs↵
<auth tacacs+ information>
Default User  : none
Service Name  : smartcs

<tacacs+ server 1>
IP address          : 192.168.1.1
Port number         : 49
Password            : stored
Timeout             : 5

<tacacs+ server 2>
IP address          : 192.168.1.2
Port number         : 49
Password            : stored
Timeout             : 5
```

```
 (c)NS-2250# show auth access_group↵
Protocol  : Tacacs+
Attribute : UserSpecific (Attribute Value Pair)
--------------------------------------------------------
<root>
   attr_val : grp=admin_grp
--------------------------------------------------------
<normal>
   attr_val : grp=normal_grp
--------------------------------------------------------
<portusr>
   attr_val : grp=port_grp
        port : 1-32
```

Check the TACACS+ accounting settings ("show acct" and "show acct tacacs" command)

```
(c)NS-2250# show acct↵
<acct information>
Mode  : tacacs

(c)NS-2250# show acct tacacs↵
<acct tacacs+ information>
Auth_deny_stop       : remote
Task-id              : 31

<tacacs+ server 1>
IP address           : 192.168.1.1
Port number          : 49
Password             : stored
Timeout              : 5

<tacacs+ server 2>
IP address           : 192.168.1.2
Port number          : 49
Password             : stored
Timeout              : 5
```

Check the statistical information of the TACACS+ authentication/approval (show stats auth tacacs)

```
(c)NS-2250# show stats auth tacacs↵
<authentication tacacs+ statistics>
Id IP address          Send Rcv_Allow Rcv_Deny Rcv_Error Timeout
-----------------------------------------------------------------------
 1 192.168.1.1          121       110        8         0        3
 2 192.168.1.2            3         0        0         0        3
<authorization tacacs+ statistics>
Id IP address          Send Rcv_Allow Rcv_Deny Rcv_Error Timeout
-----------------------------------------------------------------------
 1 192.168.1.1          121       110        8         0        3
 2 192.168.1.2            3         0        0         0        3

```

Check the statistical information of the TACACS+ accounting (show stats acct tacacs)

```
(c)NS-2250# show stats acct tacacs↵
<acct tacacs+ statistics>
Id IP address     Send_Start Send_Stop Rcv_Resp Rcv_Error Timeout
-----------------------------------------------------------------------
 1 192.168.1.1          121       110        8         0        3
 2 192.168.1.2            3         0        0         0        3

```

(3)   Check by using the "trace" command

If the TACACS+ settings are correct, carry out the "trace" command to perform a trace of the TACACS+ protocol between the NS-2250 and the TACACS+ server and check for a response from the TACACS+ server.
Note that the "trace" command can trace up to 1,000 packets. The default setting is 50 packets. To end the trace midway, stop the command by pressing Ctrl+C.

```
(c)NS-2250# trace tacacs↵

Apr 19 14:00:02 port_telnetd: LOGIN BY somebody FROM 10.5.30.145
14:00:02.913056  IP  10.5.31.186.1477  >  10.5.31.178.tacacs:  S
1949630245:1949630245(0)  win  5840  <mss  1460,sackOK,timestamp
215552175 0,nop,wscale 2>
14:00:03.034334  IP  10.5.31.178.tacacs  >  10.5.31.186.1477:  S
1621187922:1621187922(0)   ack   1949630246   win   5792   <mss
1460,sackOK,timestamp 537047041 215552175,nop,wscale 2>
14:00:03.035030 IP 10.5.31.186.1477 > 10.5.31.178.tacacs: . ack 1 win
1460 <nop,nop,timestamp 215552176 537047041>
14:00:02.937741 IP 10.5.31.186.1477 > 10.5.31.178.tacacs: P 1:13(12)
ack 1 win 1460 <nop,nop,timestamp 215552187 537047041>
14:00:02.938023 IP 10.5.31.178.tacacs > 10.5.31.186.1477: . ack 13
win 1448 <nop,nop,timestamp 537047069 215552187>
14:00:02.938169 IP 10.5.31.186.1477 > 10.5.31.178.tacacs: P 13:69(56)
ack 1 win 1460 <nop,nop,timestamp 215552187 537047069>
14:00:02.938436 IP 10.5.31.178.tacacs > 10.5.31.186.1477: . ack 69
win 1448 <nop,nop,timestamp 537047069 215552187>
14:00:02.938716 IP 10.5.31.178.tacacs > 10.5.31.186.1477: P 1:18(17)
ack 69 win 1448 <nop,nop,timestamp 537047069 215552187>
14:00:02.938827 IP 10.5.31.186.1477 > 10.5.31.178.tacacs: . ack 18
win 1460 <nop,nop,timestamp 215552187 537047069>
14:00:02.938901 IP 10.5.31.178.tacacs > 10.5.31.186.1477: F 18:18(0)
ack 69 win 1448 <nop,nop,timestamp 537047069 215552187>
14:00:02.972637 IP 10.5.31.186.1477 > 10.5.31.178.tacacs: . ack 19
win 1460 <nop,nop,timestamp 215552191 537047069>
14:00:03.037855 IP 10.5.31.186.1477 > 10.5.31.178.tacacs: F 69:69(0)
ack 19 win 1460 <nop,nop,timestamp 215552197 537047069>
14:00:03.038097 IP 10.5.31.178.tacacs > 10.5.31.186.1477: . ack 70
win 1448 <nop,nop,timestamp 537047094 215552197>
```

6.3.7 The trouble with the IPsec
When the IPsec of the NS-2250 is not operating correctly, carry out the following checks.

(1)   Check the configuration parameter of NS-2250 and VPN router
Check whether each configuration is correct or not.
Has the VPN rooter already running?
Has the Ping from NS-2250 reached to VPN rooter?
Has the pre-shared key with the VPN router match?
Has the various setting with the VPN router correct?

(2)   Check by the IPsec by using the "show" command
Execute the "show" commands listed below, and then check the IPsec status.

```
# show ipsec status detail
# show ipsec spd
# show ipsec sad
```

(3)   Check by the "trace" command
Execute the below "trace" command and view whether there is a response from the VPN rooter by tracing the ISAKMP protocol and the ESP protocol between NS-2250 and the VPN router.

```
# trace eth1 ipsec level 2
```

(4)   Check by the "loglevel" command
Execute the below "loglevel" command and output the communication such as ISAKMP protocol between NS-2250 and the VPN router.

```
# loglevel ipsec 2
```

6.3.8 The trouble with tty manage function
When you cannot communicate by tty manage function of the NS-2250 correctly, carry out
the following checks in addition to the checks written in section 6.3.4" Serial communication
connection trouble".

(1) Check the extension user exists.

```
(c)NS-2250# show user
 User-Name           Category(Uid)    Public-Key  Port-Access-List


 --------------------------------------------------------------
 root                root(0)
 setup               setup(198)
 verup               verup(199)
 log                 log(200)
 somebody            normal(100)
 ext01usr            extusr(401)      1-32
 portusr             portusr(500)                 1-32
 port02usr           portusr(501)                 1-10,13

 (c)NS-2250#
```

(2) Check the permission of tty manage function and the permission of accessing the serial port
which you want to connect is granted to the extension user.

```
(c)NS-2250# show user ext01usr ↵
User-Name     :ext01usr
Category(Uid)  :extusr(401)
Permission
  normal       :on
  ttymanage    :on
Port-Access-List:1-48
Public-Key    :

(c)NS-2250#
```

6.4　Other trouble

This section describes methods to deal with other trouble.

6.4.1　When the password of the device management user has been forgotten

If the password of the device management user has been forgotten, connect a device management terminal to the serial port of the NS-2250, and then start Rom-Monitor. Then start the system software with the unspecified startup file and then initialize the settings.

It is not possible to initialize only the password of the device management user..The password can be initialized by initializing the entire startup file.

For the initialization procedure, see the following section.

(1) Switch on the power of the NS-2250. After the message "Hit [Enter] key to Enter Rom-Monitor..." appears, press the Enter key to display the "MON>" prompt.

```
Hit [Enter] key to Enter Rom-Monitor...
MON>
```

(2) Either carry out the "boot" command while specifying the "fileno" option without saving the settings or import the startup file that clarifies the administrator password. In the following example, the "startup4" file on the USB memory referenced at startup is imported.

```
MON> boot fileno=4↵
ROM Boot
1st-Boot Ver 1.0.0
2nd-Boot Ver 1.0.0
        :                   A start message appears.
NS-2250 login:
```

(3) Log in to the NS-2250, display the startup file to be imported at startup, and then paste it into a file and save it.

```
(c)NS-2250# show config startup 1 external↵
   :
```

(4) Initialize the startup file to be imported at startup (example: "startup1" file on the USB memory).

```
(c)NS-2250# clear startup 1 external↵
   :
```

(5) Restart the NS-2250.

```
(c)NS-2250# reboot↵
Do you really want to reboot with main system and default startup [y/n] ?
y↵
```

Appendix A

User privileges

Appendix A describes user privileges.

A.1 User privileges list

Users registered to the NS-2250 are given the following privileges according to the groups to which they belong.

A <normal user> belongs to the "normal" group created by a device administrator. A <port user> belongs to the "portusr" group created by a device administrator. A <extension user> belongs to the "extusr" group created by a device administrator. Other users are registered in advance as default users of the NS-2250. Add or delete users following your usage or security policies.

For details of user information, see Section 2.3, "Security functions".
Note that user privileges cannot be changed.

User name	Group name	Privileges						
		Configure the NS-2250	Change/set password	Telnet/SSH login to NS-2250	FTP/SFTP login to NS-2250	Login from CONSOLE port	Access to the port server (Access of monitored equipment)	Execute the tty manage function(Access to target devices)
root[*1]	root	○	○	-	-	○	-	-
<Device management user>[*5]	root	○	○	○	-	○	-	-
somebody[*2]	normal	-	-	○	-	○	-	-
<Normal user>[*2]	normal	-	-	○	-	○	-	-
<extension user>[*2]	extusr	-	-	○	-	-	-	○
setup	setup	-	-	-	○	-	-	-
verup	verup	-	-	-	○	-	-	-
log	log	-	-	-	○	-	-	-
portusr[*1]	portusr	-	-	-	-	-	○[*3]	-
<Port user>	portusr	-	-	-	-	-	○[*4]	-

*1　"root" and "portusr" users cannot be deleted, and the names cannot be changed.
*2　User in normal group and extusr group can change to a device management user by carrying out the "su" command.
*3　User "portusr" is used internally by the NS-2250 when the port user authentication function is off.
　　Users cannot use this user name to access the port server.
*4　For a <port user> to access a serial port, you must configure access privileges to the serial port.
*5　If a user with administrative privileges for an external authentication server such as RADIUS or TACACS+ servers is created, the created user can log in directly to the NS-2250 as an administrator from a telnet/SSH client or console port.
　　For details, see the "create auth access_group root" and "set auth radius server root" commands in the *Command Reference*, and Appendix B, "Examples of attributes and RADIUS authentication/accounting server settings".
*6　<extusr> can login to NS-2250 only via SSH.
*7　It's necessary to give <extusr> access to serial ports to execute the tty manage function.
　　For the required settings, see the section4.7.7" Configure console access function(when operating via ansible)".

Appendix B
Examples of attributes and RADIUS authentication/accounting server settings

Appendix B describes examples of attributes and RADIUS authentication/accounting server settings.

B.1   RADIUS authentication client / accounting client function

If the RADIUS authentication function of the NS-2250 has been configured, the RADIUS authentication client of the NS-2250 carries out user authentication by sending an authentication request (Access Request packet) to the specified RADIUS authentication server after login to the NS-2250 or access to the serial ports of the NS-2250.

When user authentication by the RADIUS authentication server is successful, the RADIUS authentication server sends an authentication-successful packet (Access Accept packet) to the NS-2250. The NS-2250 operates based on the attribute information included in the received successful-authentication packet.

When user authentication by the RADIUS authentication server is not successful, the RADIUS authentication server sends an authentication-failed packet (Access Reject packet) to the NS-2250.

If the RADIUS accounting function is configured for the NS-2250, user logins, logouts, and other accounting information are sent to the RADIUS accounting server and the accounting information is saved.

If authentication by the RADIUS authentication server is successful, the RADIUS accounting client of NS-2250 sends an accounting START packet to the RADIUS accounting server.

If the user ends the use of the NS-2250 (logs out) or authentication by the RADIUS authentication server is not successful, the RADIUS accounting client of NS-2250 sends an accounting STOP packet to the RADIUS accounting server.

B.2 Attributes sent to the RADIUS authentication server

The following table shows the attributes the RADIUS authentication client of the NS-2250 sends to the RADIUS authentication server.

TableB-1 Attributes sent to the RADIUS authentication server

Attribute name	Number	Value form	Content
User-Name	1	STRING	Name of the user to receive authentication. The NS-2250 can authenticate user names up to a maximum of 64 characters.
User-Password	2	STRING	The password of the user to receive authentication. Hashed with a private key and a random number.
NAS-IP-Address	4	IPADDR	The IP address of the NS-2250. Used to identify clients that sent attributes.
NAS-Id	32	STRING	Host name of the NS-2250. Used to identify clients that sent attributes. If the "set auth radius server nas_id" command is used, an arbitrary character string is stored in the NAS-Id before it is sent.
Acct-Session-Id	44	STRING	ID to identify the session. A unique decimal number within the NS-2250 is used. Incremental value is used for the session ID with every access request. The session ID used by an authentication packet uses the same number as the accounting START/STOP packet.

B.3   Attributes of the RADIUS authentication server processed by the NS-2250

The following table shows the attributes of the RADIUS authentication server processed by the NS-2250.

If the NS-2250 receives an attribute not in the table, it ignores the received attribute.

Table B-2 Attributes of the RADIUS authentication server processed by the NS-2250

Attribute name	Number	Value form	Content
Filter-Id	11	STRING	Filter name configured to the user. Specify the serial ports that can be accessed by the user type or port user. ■ Normal user In the following cases, the user is regarded as a normal user. a. When the "set auth radius server normal filter_id_headNS-2250_NORMAL" setting was configured to the NS-2250 and the start of the Filter-Id received by the NS-2250 is "NS2250_NORMAL". b. When the "create auth access_group normal radius filter_id normal_grp" setting was configured to the NS-2250 and the Filter-Id specified as "normal_grp" received by the NS-2250. ■ Device management user In the following cases, the user is regarded as a device management user. a. When the "set auth radius server root filter_id_head NS2250_ROOT" setting was configured to the NS-2250 and the start of the Filter-Id received by the NS-2250 is "NS2250_ROOT". b. When the "create auth access_group root radius filter_id admin_grp" setting was configured to the NS-2250 and the Filter-Id specified as "admin_grp" received by the NS-2250. ■ Port user In the following cases, the user is regarded as a port user. a. When the "set auth radius server portusr filter_id_head NS2250_PORT" setting was configured to the NS-2250 and the start of the Filter-Id received by the NS-2250 is "NS2250_PORT". Note that if "NS2250_PORT1-16,24" is configured, this port user can access serial port 1 through serial port 16 and serial port 24. b. When the "create auth access_group portusr port 1-16,24 radius filter_id port_grp" setting was configured to the NS-2250 and the Filter-Id specified as "port_grp" received by the NS-2250. Note that this port user can access serial port 1 through serial port 16 and serial port 24. Also, authentication processing is carried out according to the established value of the "set auth radius def_user" command in the following cases: when the Filter-ID is not registered or when the Filter-Id value does not match the character string specified by either the "set auth radius server {normal|root|portusr} filter_id_head" command or the "create auth access_group {normal | root | portusr } radius filter_id" command.

When multiple Filter-Id attributes have been configured for users of the RADIUS authentication server and either the "set auth radius server { normal | root | portusr } filter_id_head" or "create auth access_group" command has been configured corresponding to each user, log in as a user in the following table.

Priority during login is as follows: 1. device management user (root), 2. normal user (normal), and 3. port user (portusr).

In Direct mode, for device login, log in as the user with the higher priority of access privileges 1. and 2. You can access the port server only when you have access privileges of 3. When you log into Select mode, log in as the user with the highest priority of access privileges of 1, 2, and 3.

Table B-3 Applicable users when multiple Filter-Id attributes are registered

Filter-Id settings "Set auth radius server {normal | root | portusr }filter_id_head" command or "create auth access_group" command configuration	Direct mode		Select mode
	Device access	Port access	
Device management user	Device management user	- (access not permitted)	Device management user
Normal user	Normal user	- (access not permitted)	Normal user
Port user	- (access not permitted)	Port user	Port user
Device management user/normal user	Device management user	- (access not permitted)	Device management user
Device management user/port user	Device management user	Port user	Device management user
Normal user/port user	Normal user	Port user	Normal user
Device management user/normal user/port user	Device management user	Port user	Device management user

B.4   Attributes sent to the RADIUS accounting server

The following table shows the attributes the RADIUS accounting client of the NS-2250 sends to the RADIUS accounting server.

Attributes with a mark (○) in the START column store an accounting START packet.

Attributes with a mark (○) in the STOP column store an accounting STOP packet.

Table 0-4 Attributes sent to the RADIUS accounting server

Attribute name	Number	Value form	START	STOP	Content
User-Name	1	STRING	○	○	Name of the user to receive authentication. The NS-2250 can authenticate user names up to a maximum of 64 characters.
NAS-IP-Address	4	IPADDR	○	○	The IP address of the NS-2250. Used to identify clients that sent attributes.
NAS-Id	32	STRING	○	○	Host name of the NS-2250. Used to identify clients that sent attributes. If the "set auth radius server nas_id" command is used, an arbitrary character string is stored in the NAS-Id before it is sent.
NAS-Port	5	INTEGER	○	○	Tty number of the NS-2250. Port user of Direct mode: tty number (1 to 48) Port user of Select mode: 0 Normal or administrator user of the console: 10000 Normal or administrator user of telnet/SSH: 20000 + pty number within the NS-2250 Extension user: 20000+ pty number within the NS-2250
Acct-Status-Type	40	ENUM	○	○	Accounting log type. The accounting START packet contains 1 (START), and the accounting STOP packet contains 2 (STOP). 1 : START 2 : STOP
Acct-Session-Id	44	STRING	○	○	The session ID of the accounting. An incremental value (a unique decimal number value) is used with every access request.
Acct-Authentic	45	ENUM	○	○	Method of user authentication. 1: RADIUS authentication 2: LOCAL authentication
Acct-Session-Time	46	INTEGER	-	○	Amount of time (seconds) the user received service.
Acct-Terminate-Cause	49	ENUM	-	○	Reason for the session disconnection. 1: User-Request Disconnection due to a disconnection request from the user. 15: Service-Unavailable Disconnection because the NS-2250 could not provide the service requested by the user. (Examples: authentication failure, no access privileges to tty port, etc.)

B.5   Examples of RADIUS authentication/accounting server settings

This section describes setting examples for a Livingston RADIUS server.

Because setting file names and attributes differ by RADIUS server, always check the manual of the RADIUS authentication/accounting server you are using.

B.5.1   Client registration

Register the client (NS-2250) that will use the RADIUS authentication/accounting server with the RADIUS authentication/accounting server.

On a Livingston RADIUS authentication/accounting server, register the IP address, host name, and secret key (example: "test123") of the NS-2250 to the "clients" file.

Register the same secret key for the NS-2250 and RADIUS authentication/accounting server.

Example of the "clients" file settings of the RADIUS authentication/accounting server

```
#client Name        Key
SmartCS             test123
```

If the host name of the NS-2250 has been registered to the "clients" file of the RADIUS authentication/accounting server, register the IP address of the NS-2250 to the "hosts" file of the RADIUS authentication/accounting server.

Example of the "hosts" file settings of the RADIUS authentication/accounting server

```
192.168.1.100          SmartCS
```

B.5.2   User registration

Register users to the RADIUS authentication server.

On a Livingston RADIUS authentication server, register user information to the "users" file.

The maximum length of a RADIUS user name that can be authenticated by the NS-2250 is 64 characters.

When only port users will be registered to the RADIUS authentication server, register the user name and password as shown below.

users file settings example 1

```
# Port user (User01) settings
User01     Password = "pass1111"


# Port user (User02) settings
User02     Password = "pass2222"


# Port user (User03) settings
User03     Password = "pass3333"
```

If you will use a RADIUS authentication server that is already using another service, the "users" file of the RADIUS server may be configured with attributes that the NS-2250 does not support.

However, even in such cases, the NS-2250 evaluates only Filter-ID attributes so authentication can be performed without any particular problems.

For example, authentication can be performed even when the following attributes have been configured.

"Users" file settings example 2

```
# Port user (User01) settings
User01    Password = "pass1111"
   Service-Type = Framed-User,
   Framed-protocol = PPP,
   Framed-IP-Address = 255.255.255.254,
   Idle-Timeout = 3600

# Port user (User02) settings
User02    Password = "pass2222"
   Service-Type = Callback-Framed-User,
   Framed-protocol = PPP,
   Framed-IP-Address = 255.255.255.254,
   Idle-Timeout = 1800

# Port user (User03) settings
User03 Password = "pass3333"
   Service-Type = Login-User,
```

Notes

If the "set auth radius def_user none" command has been configured, user access is refused with the above-mentioned settings.

To allow access as a port user, configure the "set auth radius def_user portusr" command.

If you want to identify user groups such as device management users, normal users, and port users, see the setting example that uses Filter-ID attributes on the next page.

If you want normal users and device management users to undergo RADIUS authentication along with port users, use one of the following commands to configure user identifiers to identify user groups with NS-2250.

When using "filter_id_head"

set auth radius server normal filter_id_headNS-2250_NORMAL	[Normal user]
set auth radius server root filter_id_head NS2250_ROOT	[Device management user]
set auth radius server portusr filter_id_head NS2250_PORT	[Port user]

When using the access grouping function

create auth access_group normal radius filter_id normal_grp	[Normal user]
create auth access_group root radius filter_id admin_grp	[Device management user]
create auth access_group portusr port 1-16 radius filter_id port_grp	[Port user]

Configure the Filter-ID attributes to the RADIUS authentication server as shown below.

"Users" file settings example 3 (when using "filter_id_head")

```
# Normal user settings
somebody    Password = "abc"
   Filter-Id = "NS2250_NORMAL",

# Device management user settings
root     Password = "def"
   Filter-Id = "NS2250_ROOT",

# Port user settings (when ports are not specified,
# access is allowed for all serial ports)
port01 Password = "port01"
   Filter-Id = "NS2250_PORT",

# Port user settings (restrict serial ports that can be accessed
to:
# 1 to 16, and 24)
port02 Password = "port02"
   Filter-Id = "NS2250_PORT1-16,24",

# Port user settings (restrict serial ports that can be accessed
to:
# 20 to 24)
port03 Password = "port03"
   Filter-Id = "NS2250_PORT20-24",
```

"Users" file settings example 3 (when using the access grouping function)

```
# Normal user settings
somebody     Password = "abc"
    Filter-Id = "normal_grp",

# Device management user settings
root     Password = "def"
    Filter-Id = "admin_grp",

# Port user settings (Specify access privileges of serial ports
by
# carrying out the "create auth access_group" command)
portZZ Password = "portZZ"
    Filter-Id = "port_grp",
```

B.6   Accounting logs of the RADIUS accounting server

This section lists examples of the accounting logs stored in the RADIUS accounting server. Livingston RADIUS accounting servers store the account logs in the "detail" file.
The output of accounting logs depends on the RADIUS accounting server. For details of the accounting logs, see the manual of the RADIUS accounting server you are using.

```
Tue Sep 23 13:51:12 2008
Acct-Status-Type = Start
NAS-IP-Address = 192.168.1.100
NAS-Port = 32
User-Name = "portuser1"
Acct-Session-Id = "25008291"
Acct-Authentic = RADIUS

Tue Sep 23 13:51:58 2008
Acct-Status-Type = Stop
NAS-IP-Address = 192.168.1.100
Acct-Terminate-Cause = User-Request
Acct-Session-Time = 46
NAS-Port = 32
User-Name = "portuser1"
Acct-Session-Id = "25008291"
Acct-Authentic = RADIUS

Tue Sep 23 14:20:00 2008
Acct-Status-Type = Start
NAS-IP-Address = 192.168.1.100
NAS-Port = 16
User-Name = "portuser2"
Acct-Session-Id = "25001234"
Acct-Authentic = RADIUS

Tue Sep 23 14:30:58 2008
Acct-Status-Type = Stop
NAS-IP-Address = 192.168.1.100
Acct-Terminate-Cause = User-Request
Acct-Session-Time = 658
NAS-Port = 16
User-Name = "portuser2"
Acct-Session-Id = "25001234"
Acct-Authentic = RADIUS

Tue Sep 23 15:01:11 2008
Acct-Status-Type = Start
NAS-IP-Address = 192.168.1.100
NAS-Port = 10000
User-Name = "somebody"
Acct-Session-Id = "25002251"
Acct-Authentic = LOCAL
```

```
Tue Sep 23 15:02:13 2008
Acct-Status-Type = Start
NAS-IP-Address = 192.168.1.100
NAS-Port = 10000
User-Name = "root"
Acct-Session-Id = "25002654"
Acct-Authentic = LOCAL

Tue Sep 23 15:04:15 2008
Acct-Status-Type = Stop
NAS-IP-Address = 192.168.1.100
Acct-Terminate-Cause = User-Request
Acct-Session-Time = 122
NAS-Port = 10000
User-Name = "root"
Acct-Session-Id = "25002654"
Acct-Authentic = LOCAL

Tue Sep 23 15:04:14 2008
Acct-Status-Type = Stop
NAS-IP-Address = 192.168.1.100
Acct-Terminate-Cause = User-Request
Acct-Session-Time = 183
NAS-Port = 10000
User-Name = "somebody"
Acct-Session-Id = "25002251"
Acct-Authentic = LOCAL
```

Appendix C
Rom-Monitor

Appendix C describes Rom-Monitor of the NS-2250.

C.1   Rom-Monitor

If the following operations or conditions occur on the NS-2250, the system switches to Rom-Monitor.

> The NS-2250 has been shut down by the "shutdown" command.
> The NS-2250 was started and then the Enter key was pressed from the console when the "Hit Enter key to stop autoboot:" message was displayed.
> The system software of the NS-2250 is down for some reason.

If the system changes to Rom-Monitor, the "MON>" prompt is displayed.

You can carry out the following operations from Rom-Monitor.

Command	Function/description

err	Show error messages.
	
	 If you carry out this command when the system software is down for some reason, the reason the software is down is displayed.
	
	  (Example) Shutdown by "shutdown" command.
	     MON> error
	     BOOT FACTOR: SHUTDOWN [80/02]

boot
  [{-m|-b}]
  [{-i|-e}]
  [fileno=]
	Specify start options and start the system software.
	
	 -m: start system software (main)
	 -b: start system software (backup)
	 -i: use the startup file inside the NS-2250 and then start.
	 -e: use the startup file on the USB memory and then start.
	 fileno=: use the startup file with a specified number and then start. You can specify a number from 1 through 4.
	
	  (Example)
	     MON> boot -b
	
	 Note that when the "boot" command is carried out without any options specified, the system starts in the following manner.
	     The system starts system software (main).
	     If a USB memory is inserted, the startup file on the USB memory is used. If a USB memory is not inserted, the internal startup file of the NS-2250 is used.
	     The startup file with the number specified by the "default startup" command of the system settings is used.

Appendix D
Third-party software licenses

Appendix D describes the third-party software licenses used by the NS-2250.

D.1 Third-party software licenses

License for

**SysVinit, SysVinit-tools, bootlogd, busybox, e2fsprogs, ethtool,
freeradius, iptables, kernel, libgcc, linux, logrotate, pam_tacplus,
procps, proftpd, strongswan, u-boot, udev, vzctl, Linux-PAM**

GNU GENERAL PUBLIC LICENCE

Version2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA   02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute, and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution, and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION, AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution, and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices.

Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

License for rsyslog

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works.   By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users.   We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors.   You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.   Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights.   Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received.   You must make sure that they, too, receive or can get the source code.   And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software.   For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so.   This is fundamentally incompatible with the aim of protecting users' freedom to change the software.   The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable.   Therefore, we have designed this version of the GPL to prohibit the practice for those products.   If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary.   To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License.   Each licensee is addressed as "you".   "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy.   The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy.   Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies.   Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License.   If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form.   A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities.   However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work.   For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source.   This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge.   You need not require recipients to copy the Corresponding Source along with the object code.   If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source.   Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling.   In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage.   For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user
actually uses, or expects or is expected to use, the product.   A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or

other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source.   The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information.   But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed.   Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law.   If additional permissions
apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it.   (Additional permissions may be written to require their own removal in certain cases when you modify the work.)   You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10.   If the Program as you received it, or any part of it, contains a notice stating that it is

governed by this License along with a term that is a further restriction, you may remove that term.   If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License.   If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance.   However, nothing other than this License grants you permission to propagate or modify any covered work.   These actions infringe copyright if you do not accept this License.   Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License.   You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations.   If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License.   For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

License for eglibc, u-boot

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA   02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL.   It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.
Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom.

The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

   A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

   The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

   "Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on

the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

* a) The modified work must itself be a software library.
* b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
* c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
* d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for

distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

* a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

* b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

* c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

* d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

* e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined

library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

   * a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

   * b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

License for u-boot

GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

  [This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it.   By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it.   You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price.   Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you.   You must make sure that they, too, receive or can get the source code.   If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it.   And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library.   If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents.   We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software.   To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

   A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

   The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

   "Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this

License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) The modified work must itself be a software library.

   b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

   d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application.   Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

   These requirements apply to the modified work as a whole.   If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works.   But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

   In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library.   To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.)   Do not make any other change in these notices.

   Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

   This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

   If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library".   Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

   However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library".   The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

   When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library.   The threshold for this to be true is not precisely defined by law.

   If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

   Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

   You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License.   You must supply a copy of this License.   If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License.   Also, you must do one of these things:

   a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library.   (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

   b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

   c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

   d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

   a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

   b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.
    You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded.   In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number.   If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation.   If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this.   Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

License for u-boot, xinetd

Berkeley-based copyrights:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

License for libpcap, ftp, strace, telnet-server, tcpdump, u-boot

Berkeley-based copyrights:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

License for dropbear

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

License for libcap

Redistribution and use in source and binary forms of libcap, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License, in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2004, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

*   Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
*   Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
*   Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.   IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

License for openssh, openssh-server

1)
```
     * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
     *                       All rights reserved
     *
     * As far as I am concerned, the code I have written for this software
     * can be used freely for any purpose.   Any derived versions of this
     * software must be clearly marked as such, and if the derived work is
     * incompatible with the protocol description in the RFC file, it must be
     * called by a name other than "ssh" or "Secure Shell".
```

[Tatu continues]
```
     *    However, I am not implying to give any licenses to any patents or
     * copyrights held by third parties, and the software includes parts that
     * are not under my direct control.   As far as I know, all included
     * source code is used in accordance with the relevant license agreements
     * and can be used freely for any purpose (the GNU license being the most
     * restrictive); see below for details.
```

[However, none of that term is relevant at this point in time.   All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide.   More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions.   Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.   EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.   THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU.   SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU

OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)

The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

```
* Cryptographic attack detector for ssh - source code
*
* Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.
*
* All rights reserved. Redistribution and use in source and binary
* forms, with or without modification, are permitted provided that
* this copyright notice is retained.
*
* THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
* WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE
* LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR
* CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS
* SOFTWARE.
*
* Ariel Futoransky <futo@core-sdi.com>
* <http://www.core-sdi.com>
```

3)

ssh-keygen was contributed by David Mazieres under a BSD-style license.

```
* Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
*
* Modification and redistribution in source and binary forms is
* permitted provided that due credit is given to the author and the
* OpenBSD project by leaving this copyright notice intact.
```

4)

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

```
* @version 3.0 (December 2000)
*
* Optimised ANSI C code for the Rijndael cipher (now AES)
*
* @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
* @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
* @author Paulo Barreto <paulo.barreto@terra.com.br>
*
* This code is hereby placed in the public domain.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS
* OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.   IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE
* LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
* OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
* BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
* LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
* NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
* SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Darren Tucker

```
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1.Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2.Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
* IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
* IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
* INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
* ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
* THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

8) Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

```
* "THE BEER-WARE LICENSE" (Revision 42):
* <phk@login.dknet.dk> wrote this file.   As long as you retain this
* notice you can do whatever you want with this stuff. If we meet
* some day, and you think this stuff is worth it, you can buy me a
* beer in return.    Poul-Henning Kamp
```

b) snprintf replacement

```
* Copyright Patrick Powell 1995
* This code is based on code written by Patrick Powell
* (papowell@astart.com) It may be used for any purpose as long as this
* notice remains intact on all source code distributions
```

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code
in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following
copyright holders:

Todd C. Miller
Theo de Raadt
Damien Miller
Eric P. Allman
The Regents of the University of California

```
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*notice, this list of conditions and the following disclaimer in the
*     documentation and/or other materials provided with the distribution.
* 3. Neither the name of the University nor the names of its contributors
*may be used to endorse or promote products derived from this software
*without specific prior written permission.
```

License for OpenSSL, SSLeay

LICENSE ISSUES
==============

The OpenSSL toolkit stays under a double license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts.

OpenSSL License

```
/* ====================================================================
 * Copyright (c) 1998-2019 The OpenSSL Project.   All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *      notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *      notice, this list of conditions and the following disclaimer in
 *      the documentation and/or other materials provided with the
 *      distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *      software must display the following acknowledgment:
 *      "This product includes software developed by the OpenSSL Project
 *      for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *      endorse or promote products derived from this software without
 *      prior written permission. For written permission, please contact
 *      openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *      nor may "OpenSSL" appear in their names without prior written
 *      permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *      acknowledgment:
 *      "This product includes software developed by the OpenSSL Project
 *      for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.   IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).   This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
```

```
 *
 */
```

Original SSLeay License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.   The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.   The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.   IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.   i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

License for tcl

License for tclx

License for tcp_wrappers

License for u-boot

The eCos license version 2.0

This file is part of eCos, the Embedded Configurable Operating System.
Copyright (C) 1998, 1999, 2000, 2001, 2002 Red Hat, Inc.

eCos is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 or (at your option) any later version.

eCos is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with eCos; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA.

As a special exception, if other files instantiate templates or use macros or inline functions from this file, or you compile this file and link it with other works to produce a work based on this file, this file does not by itself cause the resulting work to be covered by the GNU General Public License. However the source code for this file must still be made available in accordance with section (3) of the GNU General Public License.

This exception does not invalidate any other reasons why a work based on this file might be covered by the GNU General Public License.

Alternative licenses for eCos may be arranged by contacting Red Hat, Inc. at http://sources.redhat.com/ecos/ecos-license/

####ECOSGPLCOPYRIGHTEND####

References
 1. http://www.gnu.org/licenses/license-list.html

License for zlib

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

    1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software   in a product, an acknowledgment in the product documentation would be appreciated but is not required.

    2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

    3. This notice may not be removed or altered from any source distribution.