

SmartCS

Console server
NS-2250



Before using this console server, carefully read this command reference so you can use the console server correctly.

After reading this command reference, store it in a safe place so that it can be accessed easily when necessary.

U00135011200	2015 Dec
U00135011201	2016 Jun
U00135011202	2016 Dec
U00135011203	2017 Apr

©Seiko Solutions Inc., 2015

No copying.

The content of this manual may change without notice.

”SEIKO” is a registered trademark of Seiko Holdings Corporation.

Ethernet is a registered trademark of Fuji Xerox Co., Ltd.

Seiko Solutions Inc. is not responsible for damage caused by the use of this manual or products described in this manual, or expenses necessary to compensate for such damage.

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, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

VCCI-A

Introduction

Thank you for purchasing the SmartCS NS-2250 console server (hereinafter referred to as the NS-2250). This document is the command reference manual for the NS-2250. It explains the command functions and formats, and the meaning of parameters. It also gives usage and execution examples, commentaries and cautionary notes.

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 as appropriate for the model you are using.

	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
	DC power model	NS-2250-16D	16 ports
		NS-2250-32D	32 ports
		NS-2250-48D	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 the NS-2250 usage and specifications, see the NS-2250 Console server instruction manual (hereinafter referred to as the Instruction Manual).

Contents

1	Command overview	12
1.1	Objects and commands	13
1.2	Object commands overview	13
1.3	Object setting sequence	14
1.4	List specification	15
2	Command list	16
2.1	Setting command overview	17
2.2	Display commands overview	25
2.3	Maintenance command overview	28
2.4	Other commands overview	30
3	Command reference format	31
4	Setting commands	33
4.1	System setting commands	34
	set hostname	34
	set ipaddr	35
	unset ipaddr	36
	set tcpkeepalive	37
4.2	bonding setting commands	38
	set bonding up_delay	38
	enable bonding	39
	disable bonding	40
4.3	ipinterface setting commands	41
	set ipinterface mtu	41
4.4	IPv6 setting commands	42
	create ip6	42
	set ip6addr	43
	unset ip6addr	44
	delete ip6	45
4.5	IP host setting commands	46
	create ip host	46
	delete ip host	47
4.6	IP route setting commands	48
	create ip route	48
	delete ip route	49
4.7	IPv6 route setting commands	50
	create ip6route	50
	delete ip6route	51
4.8	ipfilter setting commands	52
	create ipfilter	52
	delete ipfilter	54
	delete ipfilter line	56
	delete ipfilter allentry	57

enable ipfilter	58
disable ipfilter	59
4.9 ipsec setting commands	60
create ipsec secret psk	60
delete ipsec secret psk	62
set ipsec conn auto	63
set ipsec conn leftid	64
set ipsec conn left	65
set ipsec conn leftsubnet	66
set ipsec conn leftsourceip	67
set ipsec conn rightid	68
set ipsec conn right	69
set ipsec conn rightsubnet	70
set ipsec conn rightsourceip	71
set ipsec conn keyexchange	72
set ipsec conn ike	73
set ipsec conn esp	74
set ipsec conn ikelifetime	75
set ipsec conn lifetime	76
set ipsec conn forceencaps	77
set ipsec conn dpdaction	78
unset ipsec conn	79
unset ipsec conn leftid	80
unset ipsec conn left	81
unset ipsec conn leftsubnet	82
unset ipsec conn leftsourceip	83
unset ipsec conn rightid	84
unset ipsec conn right	85
unset ipsec conn rightsubnet	86
unset ipsec conn rightsourceip	87
unset ipsec conn ike	88
unset ipsec conn esp	89
enable ipsec conn	90
disable ipsec conn	91
4.10 DNS setting command	92
set dns	92
set dns localdomain	93
unset dns	94
unset dns localdomain	95
4.11 LAN setting commands	96
set ether nego	96
4.12 User management and authentication setting commands	97
create user	97
set user password	99
set user port	100
set user sshkey	101
unset user sshkey	103
delete user	104
4.13 SNMP agent setting commands	105
set snmp location	105
set snmp contact	106
set snmp authentrap	107
set snmp linktrap	108
set snmp dsrtrap	109
set snmp coldstarttrap	110
set snmp powertrap	111
set snmp bondingactswtrap	112

unset snmp location	113
unset snmp contact	114
enable snmp	115
disable snmp	116
4.14 SNMP trap setting commands	117
set trap manager	117
unset trap manager	118
4.15 SNMP community setting commands	119
set community	119
unset community	120
4.16 Syslog setting commands	121
set syslog host	121
unset syslog host	122
enable syslog	123
disable syslog	124
4.17 NFS setting commands	125
set nfs server addr	125
set nfs server proto	126
set nfs rotate	127
unset nfs server addr	128
enable nfs	129
disable nfs	130
4.18 SNTP setting commands	131
set sntp server	131
set sntp polltime	132
unset sntp server	133
enable sntp	134
disable sntp	135
4.19 TTY setting commands	136
set tty baud	136
set tty bitchar	137
set tty parity	138
set tty stop	139
set tty flow	140
set tty detect_dsr	141
4.20 logd setting commands	142
add logd tty mail	142
add logd tty ftp	143
set logd output	145
set logd tstamp	146
set logd tty log	147
set logd tty lstamp	148
set logd tty syslog	149
set logd tty nfs	150
set logd tty sendlog	151
set logd tty mail port	152
set logd tty mail type	153
set logd tty mail subject	154
set logd tty mail sender	155
set logd tty mail auth	156
unset logd tty mail auth	157
remove logd tty mail	158
remove logd tty ftp	159
4.21 portd setting commands	160
set portd connect	160
set portd menu	161
set portd auth	162

set portd telrw	163
set portd telro	164
set portd sshrw	165
set portd sshro	166
set portd idle_timeout	167
set portd ro_timeout	168
set portd tty session	169
set portd tty limit	170
set portd tty brk_char	171
set portd tty nl	172
set portd tty cmdchar	173
set portd tty label	174
set portd tty timeout	175
unset portd tty label	176
4.22 Console setting commands	177
set console	177
4.23 Telnet command setting commands	178
set telnet cmdchar	178
4.24 Telnetd setting commands	179
set telnetd port	179
enable telnetd	180
disable telnetd	181
4.25 sshd setting commands	182
set sshd auth	182
set sshd port	183
set sshd host_key	184
enable sshd	185
disable sshd	186
4.26 ftpd setting commands	187
enable ftpd	187
disable ftpd	188
4.27 Security setting commands	189
create allowhost	189
delete allowhost	191
4.28 Authentication setting commands	192
create auth access_group	192
set auth mode	195
set auth su_cmd username	196
set auth radius retry	197
set auth radius server addr	198
set auth radius server port	199
set auth radius server key	200
set auth radius server timeout	201
set auth radius server portusr	202
set auth radius server normal	204
set auth radius server root	206
set auth radius server nas_id	208
set auth radius server def_user	209
set auth tacacs server addr	210
set auth tacacs server key	211
set auth tacacs server timeout	212
set auth tacacs def_user	213
unset auth radius server addr	214
unset auth radius server portusr	215
unset auth radius server normal	216
unset auth radius server root	217
unset auth radius server nas_id	218

unset auth tacacs server addr	219
delete auth access_group	220
4.29 Accounting setting commands	222
set acct mode	222
set acct radius retry	223
set acct radius auth_deny_stop	224
set acct radius server addr	225
set acct radius server port	226
set acct radius server key	227
set acct radius server timeout	228
set acct radius server nas_id	229
set acct tacacs auth_deny_stop	230
set acct tacacs server addr	231
set acct tacacs server key	232
set acct tacacs server timeout	233
unset acct radius server addr	234
unset acct radius server nas_id	235
unset acct tacacs server addr	236
4.30 terminal output control setting commands	237
set terminal default editing	237
set terminal default height	238
set terminal default width	239
set terminal default page	240
set terminal default prompt	241
set terminal default redisp	242
set terminal default timeout	243
4.31 Time zone setting commands	244
set timezone	244
4.32 Temperature sensor setting commands	245
set temperature adjust	245
5 Status display commands	246
5.1 System status display commands	247
show version	247
show environment	249
show slot	250
show cpu	251
show memory	252
show log	253
show support	254
5.2 Bonding display commands	257
show bonding	257
5.3 Network information display commands	259
show ether	259
show stats ether	262
show ipinterface	264
show ip	265
show ip6	266
show ip host	267
show ip route	268
show ip6route	269
show tcp	270
show udp	271
show stats ip	272
show stats ip6	274
show stats icmp6	276
show arp	278

show ndp	279
show stats tcp	280
show stats udp	281
show dns	282
5.4 Ipfiler status display commands	283
show ipfilter	283
show stats ipfilter	285
5.5 Ipsec status display commands	287
show ipsec secret	287
show ipsec conn	288
show ipsec status	291
show ipsec spd	293
show ipsec sad	294
5.6 User status display commands	295
show user	295
show user login	296
5.7 SNMP status display command	297
show snmp	297
5.8 SNTP status display command	299
show sntp	299
5.9 Syslog status display command	300
show syslog	300
5.10 NFS status display command	301
show nfs	301
5.11 Port server status display commands	303
show portd	303
show portd tty	305
show portd session	307
show tty	309
show stats tty	311
show logd	313
show stats logd tty	316
5.12 CONSOLE port status display command	318
show console	318
show stats console	319
5.13 Display command for the internal management servers	320
show service	320
5.14 Display command for the list of hosts and services authorized for connection	321
show allowhost	321
5.15 Setting file display commands	322
show config	322
show config startup	324
show config info	325
5.16 Terminal setting information display command	326
show terminal	326
5.17 Authentication/accounting function display commands	327
show auth	327
show auth radius	328
show auth tacacs	330
show auth access_group	331
show stats auth radius	335
show stats auth tacacs	336
show acct	340
show acct radius	341
show acct tacacs	342
show stats acct radius	343
show stats acct tacacs	344

5.18	Time zone display command	346
	show timezone	346
6	Maintenance commands	347
6.1	Basic maintenance commands	348
	date	348
	engineering	349
	exit	350
	logout	351
	ping	352
	ping6	353
	reboot	354
	shutdown	355
	su	356
	telnet	357
	traceroute	358
	traceroute6	359
	switch bonding	360
	hangup	361
	history	362
	logsave	363
	loginfo	364
	clear arp	365
	trace	366
	disconnect	367
	tftp setup	368
	tftp verup	369
	tftp log	370
	tftp support	371
	ftp	372
6.2	Management commands for settings files	374
	write	374
	clear startup	375
	default startup	376
	copy startup	377
	echo	378
6.3	Management command for the system software	379
	copy system	379
	verup execute	380
	verup cleanup	381
	backup system-image	382
	restore system-image	383
	clear system-image	384
	show system-image	385
6.4	Console output control commands	386
	console	386
	loglevel	387
6.5	Terminal output control commands	388
	terminal timeout	388
	terminal editing	389
	terminal page	390
	terminal height	391
	terminal width	392
	terminal prompt	393
	terminal redisp	394

7 Other commands	395
7.1 Port server menu commands	396
0 (return Port Select Menu)	396
1 (display Port Log)	398
2 (display Port Log (LAST))	399
3 (start tty connection)	400
4 (close telnet/ssh session)	401
5 (show all commands)	402
6 (display & erase Port Log)	403
7 (erase Port Log)	404
8 (send Port Log)	405
9 (show Port Log configuration)	406
10 (send break to tty)	407
7.2 Port selection menu commands	408
<i>ttyno</i>	408
<i>ttynor</i>	409
<i>l</i>	410
<i>lttyno-ttyno</i>	411
<i>d</i>	412
<i>dttyno-ttyno</i>	413
<i>h</i>	414
<i>e</i>	415
Index	416

Chapter1

Command overview

Chapter 1 describes the command types, and gives an overview of objects and commands.

1.1 Objects and commands

The built-in system software of the NS-2250 manages the physical and virtual components making up the NS-2250 as objects. They are dynamically created, deleted, merged, and combined to operate the NS-2250. The command is used for setting to an object, status display and maintenance of this equipment.

1.2 Object commands overview

This section gives a list of commands to operate the objects used to configure or display the status of the NS-2250.

Table 1-1: Object command list

Command name	Command description
create	Create a new object or profile.
add to	Add an object to another object.
set	Set attributes to an object.
unset	Remove an attribute set to an object.
enable	Enable an object (make it usable).
disable	Disable an object (make it unusable).
remove from	Remove an object from another object.
delete	Delete an existing object.
show	Display the status of an object.
show stats	Display the statistical information of an object.

1.3 Object setting sequence

The correlation between the object commands can be defined as shown in the setting sequence in Figure 1-1.

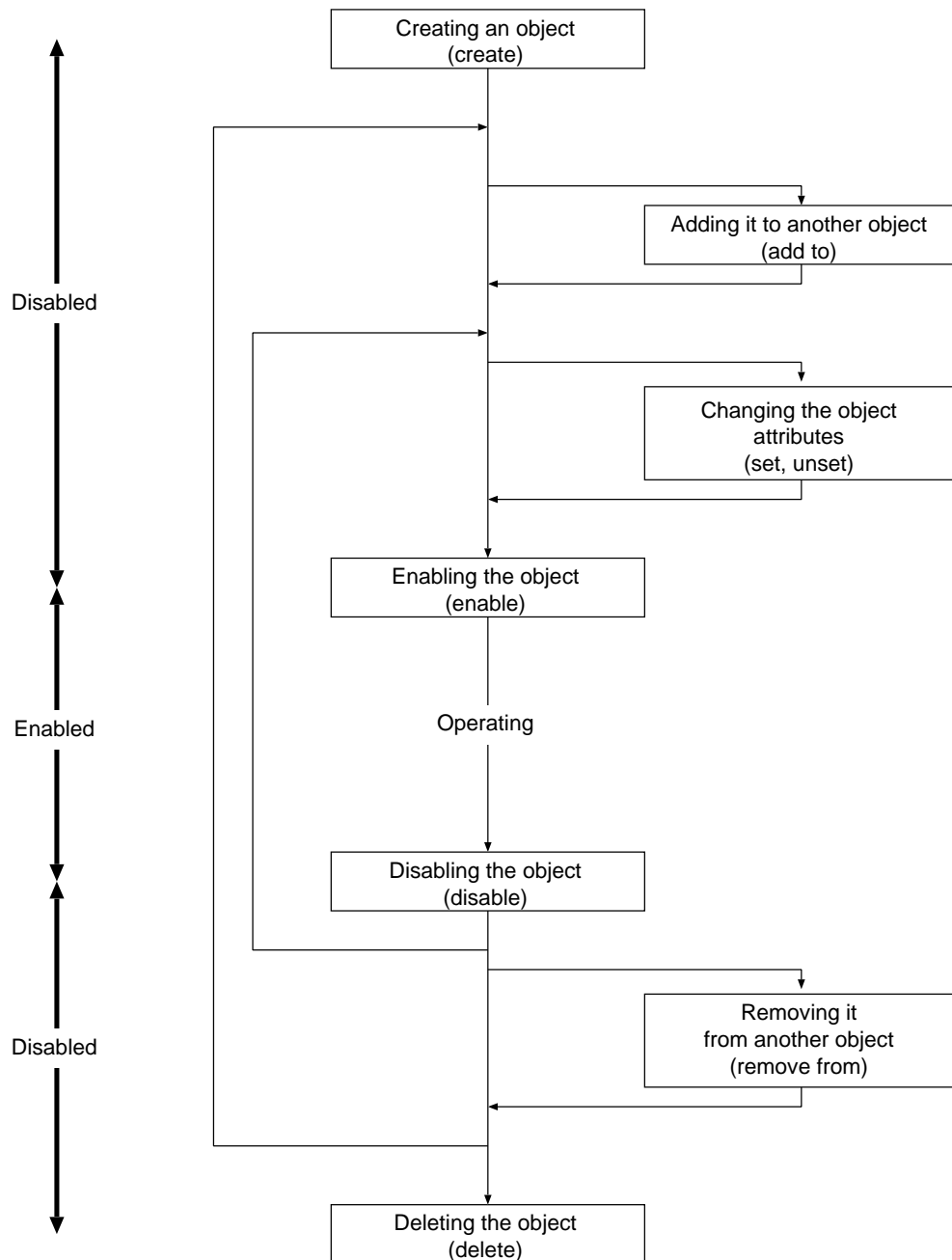


Figure 1-1: Object setting sequence

1.4 List specification

An object and the value are listed by a parameter of the command, it's possible to specify it. Use method is as follows.

”_”

Specify the value which continued.

Usage example : tty 2-4

”,”

Specify the value which doesn't continued and the name of the plural.

Usage example : tty 1,3

Chapter2

Command list

Chapter 2 describes overview of the command.

2.1 Setting command overview

This section gives a list of setting commands that can be used on the NS-2250.

Table 2-1: Setting command list

Class	Command	Description
System setting commands	set hostname	Configure the NS-2250 host name.
	set ipaddr	Set the NS-2250 IP address.
	unset ipaddr	Unset the NS-2250 IP address.
	set tcpkeepalive	Set the TCP keepalive time for the NS-2250.
bonding setting commands	set bonding up_delay	configure the wait timer which is the delay period enabling slave interface after the detection of physical linkup.
	enable bonding	Enable the bonding function.
	disable bonding	Disable the bonding function.
ipinterface setting commands	set ipinterface mtu	Set the MTU of each interface.
IPv6 setting commands	create ip6	Enable the IPv6 communication function.
	set ip6addr	Set the NS-2250 IPv6 address.
	unset ip6addr	Unset the NS-2250 IPv6 address.
	delete ip6	Disable the IPv6 communication function.
IP host setting commands	create ip host	Register a pair of a host name and an IP address (host entry).
	delete ip host	Delete the host entry.
IP route setting commands	create ip route	Create a static route to an IP address.
	delete ip route	Delete the static route.
IPv6 route setting commands	create ip6route	Create static routes for IPv6.
	delete ip6route	Delete the static route.
ipfilter setting commands	create ipfilter	Register the filter conditions.
	delete ipfilter	Delete the registered filter conditions.
	delete ipfilter line	Delete the registered filter condition by specifying a line number.
	delete ipfilter allentry	Delete all filter conditions.
	enable ipfilter	Enable the filter function.
	disable ipfilter	Disable the filter function.
ipsec setting commands	create ipsec secret psk	Register a pre-shared key used in the IKE.
	delete ipsec secret psk	Delete a pre-shared key used in the IKE.
	set ipsec conn auto	Set initiator or responder of key exchange.
	set ipsec conn leftid	Set the ID of the security gateway of own side.
	set ipsec conn left	Set the IP address of the security gateway of own side.
	set ipsec conn leftsubnet	Set the network address of own side which communicates under encrypted by using IPsec.

Continued on next page

Table 2-1: Setting command list(continued)

Class	Command	Description
	<code>set ipsec conn leftsourceip</code>	Set the source IP address of own side which communicates in the IPsec tunnel.
	<code>set ipsec conn rightid</code>	Set the ID of the security gateway of the opposite side.
	<code>set ipsec conn right</code>	Set the IP address of the security gateway of the opposite side.
	<code>set ipsec conn rightsubnet</code>	Set the network address of the opposite side which communicates under encrypted by using IPsec.
	<code>set ipsec conn rightsourceip</code>	Set the source IP address of the opposite side which communicates in the IPsec tunnel.
	<code>set ipsec conn keyexchange</code>	Set the version of the IKE protocol.
	<code>set ipsec conn ike</code>	Set the encryption algorithm of the ISAKMP-SA(Phase1).
	<code>set ipsec conn esp</code>	Set the encryption algorithm of the IPSEC-SA(Phase2).
	<code>set ipsec conn ikelifetime</code>	Set the lifetime of the ISAKMP-SA.
	<code>set ipsec conn lifetime</code>	Set the lifetime of the IPSEC-SA.
	<code>set ipsec conn forceencaps</code>	Set whether to encapsulate the ESP protocol communication of the IPSEC-SA by UDP always or not.
	<code>set ipsec conn dpdaction</code>	Set whether to execute DPD(Dead Peer Detection) or not.
	<code>unset ipsec conn</code>	Delete all settings of the specified connection.
	<code>unset ipsec conn leftid</code>	Delete the ID setting of the security gateway of own side.
	<code>unset ipsec conn left</code>	Delete the IP address of the security gateway of own side.
	<code>unset ipsec conn leftsubnet</code>	Delete the network address of own side which communicates under encrypted by using IPsec.
	<code>unset ipsec conn leftsourceip</code>	Delete the source IP address of own side which communicates in the IPsec tunnel.
	<code>unset ipsec conn rightid</code>	Delete the ID setting of the security gateway of the opposite side.
	<code>unset ipsec conn right</code>	Delete the IP address of the security gateway of the opposite side.
	<code>unset ipsec conn rightsubnet</code>	Delete the network address of the opposite side which communicates under encrypted by using IPsec.
	<code>unset ipsec conn rightsourceip</code>	Delete the source IP address of the opposite side which communicates in the IPsec tunnel.
	<code>unset ipsec conn ike</code>	Delete the encryption algorithm setting of the ISAKMP-SA(Phase1).
	<code>unset ipsec conn esp</code>	Delete the encryption algorithm of the IPSEC-SA(Phase2).

Continued on next page

Table 2-1: Setting command list(continued)

Class	Command	Description
DNS setting command	enable ipsec conn	Enable the IPsec function.
	disable ipsec conn	Disable the IPsec function.
	set dns	Register the DNS server used for name resolution.
	set dns localdomain	Configure the local domain to which the NS-2250 belongs.
LAN setting commands	unset dns	Delete the information of a registered DNS server.
	unset dns localdomain	Delete the settings of the local domain to which the NS-2250 belongs.
	set ether nego	Configure the auto-negotiation operation for the LAN port.
User management and authentication setting commands	create user	Create a user.
	set user password	Change the user password for login.
	set user port	Configure the port users access privileges for the serial ports.
	set user sshkey	Configure the public key for user SSH authentication.
	unset user sshkey	Delete user settings for SSH authentication public key.
	delete user	Delete a user.
SNMP agent setting commands	set snmp location	Set sysLocation (system location).
	set snmp contact	Set sysContact (contact information).
	set snmp authentrap	Set whether or not to send a trap when SNMP authentication failed.
	set snmp linktrap	Set whether or not to send link traps.
	set snmp dsrtrap	Set whether or not to send DSR traps.
	set snmp coldstarttrap	Set whether or not to send cold start traps.
	set snmp powertrap	Set whether or not to send power traps.
	set snmp bondin-gactswtrap	Set whether or not to send the active port switched traps.
	unset snmp location	Remove sysLocation settings.
	unset snmp contact	Remove sysContact settings.
	enable snmp	Enable the SNMP agent function.
	disable snmp	Disable the SNMP agent function.
SNMP trap setting commands	set trap manager	Set the address of the SNMP server to send the traps to and the community name used when sending the traps.
	unset trap manager	Remove the settings of the destination SNMP server.
SNMP community setting commands	set community	Set the community name and SNMP server that can use it to access the NS-2250.

Continued on next page

Table 2-1: Setting command list(continued)

Class	Command	Description
Syslog setting commands	unset community	Remove the settings of the community name and SNMP server that can use it to access the NS-2250.
	set syslog host	Set the facility and syslog server where to send the syslog messages.
	unset syslog host	Remove the settings of the syslog server where to send the syslog messages.
	enable syslog	Enable the syslog client.
NFS setting commands	disable syslog	Disable the syslog client.
	set nfs server addr	Set the NFS server where to save the port logs.
	set nfs server proto	Set the NFS protocol.
	set nfs rotate	Set the rotation interval of the port logs.
	unset nfs server addr	Remove the NFS server settings.
	enable nfs	Enable the NFS client function.
SNTP setting commands	disable nfs	Disable the NFS client function.
	set sntp server	Set NTP servers to which you want to synchronize.
	set sntp polltime	Set polling interval to the NTP servers.
	unset sntp server	Remove settings of NTP servers.
	enable sntp	Enable the SNTP client function.
TTY setting commands	disable sntp	Disable the SNTP client function.
	set tty baud	Set the operation conditions and operation of the serial ports.
	set tty bichar	Set the data bit length.
	set tty parity	Set the parity.
	set tty stop	Set the stop bit length.
	set tty flow	Set the flow control.
logd setting commands	set tty detect_dsr	Set the DSR signal transition detection function.
	add logd tty mail	Register a destination email address and email server to send the port logs.
	add logd tty ftp	Register a destination FTP server for port logs.
	set logd output	Set the port log save destination.
	set logd tstamp	Set port log time stamps.
	set logd tty log	Set the port log save space for each serial port.
	set logd tty lstamp	Set the login stamp function for port logs.
	set logd tty syslog	Set whether to send port logs to a syslog server.
	set logd tty nfs	Set whether to save port logs to a NFS server.
	set logd tty sendlog	Set the conditions to send the port logs to an email or an FTP server.
	set logd tty mail port	Set SMTP port for the port log emails.
	set logd tty mail type	Set how the port logs are sent by email (sending method).
	set logd tty mail subject	Set the email subject for port logs.

Continued on next page

Table 2-1: Setting command list(continued)

Class	Command	Description
	set logd tty mail sender	Set the email address of the sender for port logs.
	set logd tty mail auth	Set SMTP authentication for the port log emails.
	unset logd tty mail auth	Remove settings of SMTP authentication for port log emails.
	remove logd tty mail	Remove the settings for the destination email address and email server used to send port logs.
	remove logd tty ftp	Remove settings of a destination FTP server for port logs.
portd setting commands	set portd connect	Set the connection mode of the port server.
	set portd menu	Set the display method of the port server menu.
	set portd auth	Set whether or not to use port user authentication when connecting from a Telnet client.
	set portd telrw	Specify the service port start number for Telnet Normal mode.
	set portd telro	Specify the service port start number for Telnet Monitoring mode.
	set portd sshrw	Specify the service port start number for SSH Normal mode.
	set portd sshro	Specify the service port start number for SSH Monitoring mode.
	set portd idle.timeout	Set a value for the idle timer for the select menu, port server menu, and Normal mode (rw) sessions.
	set portd ro.timeout	Set a value for the session timer of Monitoring mode (ro) sessions.
	set portd tty session	Set the authorized protocols and modes for connection to the serial ports.
	set portd tty limit	Set a number of sessions for a serial port.
	set portd tty brk_char	Set the NVT break character.
	set portd tty nl	Set the conversion method for the line feed format received from the network.
	set portd tty cmdchar	Set a substitute character code to go to the port server menu.
	set portd tty label	Set serial port labels.
	set portd tty timeout	Set the timeout function on and off for the port server menu, Normal mode (rw) sessions, and Monitoring mode (ro) sessions.
	unset portd tty label	Remove serial port label settings.
Console setting commands	set console	Set the console.
Telnet command setting commands	set telnet cmdchar	Set the character code to transit to the command mode while executing the telnet command.

Continued on next page

Table 2-1: Setting command list(continued)

Class	Command	Description
Telnetd setting commands	set telnetd port	Set the Telnet server port number.
	enable telnetd	Enable the Telnet server.
	disable telnetd	Disable the Telnet server.
sshd setting commands	set sshd auth	Set the user authentication type for the SSH server.
	set sshd port	Set the SSH server port number.
	set sshd host_key	Set the SSH server host_key.
	enable sshd	Enable the SSH server.
	disable sshd	Disable the SSH server.
ftpd setting commands	enable ftpd	Enable the FTP server.
	disable ftpd	Disable the FTP server.
Security setting commands	create allowhost	Create a list of hosts and services authorized for connection.
	delete allowhost	Delete a list of hosts and services authorized for connection.
Authentication setting commands	create auth access_group	Create access groups and serial port access privileges.
	set auth mode	Set the user authentication method.
	set auth su_cmd user-name	In the RADIUS authentication or TACACS+ authentication/approval function, set the user name used when executing the "su" command with external authentication.
	set auth radius retry	Set the number of times the authentication request packet is resent to the RADIUS authentication server.
	set auth radius server addr	Set the IP address of the RADIUS authentication server.
	set auth radius server port	Set the authentication port number of the RADIUS authentication server.
	set auth radius server key	Set the secret key of the RADIUS authentication server.
	set auth radius server timeout	Set the timeout time for the response packet sent back from the RADIUS authentication server.
	set auth radius server portusr	Set the port user identifier used with RADIUS authentication.
	set auth radius server normal	Set the normal user identifier used with RADIUS authentication.
	set auth radius server root	Set the device management user identifier used with RADIUS authentication.
	set auth radius server nas_id	Register the NAS-ID attribute notified to the RADIUS authentication server.
	set auth radius server def_user	Configure access methods for users for which a user group cannot be identified.
	set auth tacacs server addr	Set the IP address of the TACACS+ server (authentication/approval).

Continued on next page

Table 2-1: Setting command list(continued)

Class	Command	Description
	<code>set auth tacacs server key</code>	Set the secret key of the TACACS+ server (authentication/approval).
	<code>set auth tacacs server timeout</code>	Set the timeout time for the response packet sent back from the TACACS+ server (authentication/approval).
	<code>set auth tacacs def_user</code>	Configure access methods for users for which a user group cannot be identified when using TACACS+ authentication and approval.
	<code>unset auth radius server addr</code>	Remove the IP address of the RADIUS authentication server.
	<code>unset auth radius server portusr</code>	To remove the port user identifier when using RADIUS authentication.
	<code>unset auth radius server normal</code>	To remove the normal user identifier when using RADIUS authentication.
	<code>unset auth radius server root</code>	To remove the device management user identifier when using RADIUS authentication.
	<code>unset auth radius server nas_id</code>	Remove the NAS-ID attribute notified to the RADIUS authentication server.
	<code>unset auth tacacs server addr</code>	Remove the IP address of the TACACS+ server (authentication/approval).
	<code>delete auth access_group</code>	Delete access groups and serial port access privileges.
Accounting setting commands	<code>set acct mode</code>	Set the saving mode for accounting logs.
	<code>set acct radius retry</code>	Set the number of times accounting packets are resent to the RADIUS accounting server.
	<code>set acct radius auth_deny_stop</code>	Set the sending method of accounting STOP packets when user authentication has failed.
	<code>set acct radius server addr</code>	Set the IP address of the RADIUS accounting server.
	<code>set acct radius server port</code>	Set the accounting port number of the RADIUS accounting server.
	<code>set acct radius server key</code>	Set the secret key of the RADIUS accounting server.
	<code>set acct radius server timeout</code>	Set the timeout time for the response packet sent back from the RADIUS accounting server.
	<code>set acct radius server nas_id</code>	Register the NAS-ID attribute notified to the RADIUS accounting server.
	<code>set acct tacacs auth_deny_stop</code>	Set the sending method of accounting STOP packets when TACACS+ authentication or approval has failed.
	<code>set acct tacacs server addr</code>	Set the IP address of the TACACS+ server (accounting).
	<code>set acct tacacs server key</code>	Set the secret key of the TACACS+ server (accounting).

Continued on next page

Table 2-1: Setting command list(continued)

Class	Command	Description
	<code>set acct tacacs server timeout</code>	Set the timeout time for the response packet sent back from the TACACS+ server (accounting).
	<code>unset acct radius server addr</code>	Remove the IP address of the RADIUS accounting server.
	<code>unset acct radius server nas_id</code>	Remove the NAS-ID attribute notified to the RADIUS accounting server.
	<code>unset acct tacacs server addr</code>	Remove the IP address of the TACACS+ server (accounting).
terminal output control setting commands	<code>set terminal default editing</code>	Set the default setting for enabling or disabling terminal line editing.
	<code>set terminal default height</code>	Set the default setting for the number of lines on one page of the terminal.
	<code>set terminal default width</code>	Set the default setting for the number of characters on one line of the terminal.
	<code>set terminal default page</code>	Set the default setting for enabling or disabling the terminal paging function.
	<code>set terminal default prompt</code>	Set the default setting for the display format of the terminal prompt.
	<code>set terminal default re-disp</code>	Set whether or not to redisplay by default the previously entered command string on the next prompt screen after a command input error has occurred.
	<code>set terminal default timeout</code>	Set the default value for the terminal automatic logout time.
Time zone setting commands	<code>set timezone</code>	Set the time zone.
Temperature sensor setting commands	<code>set temperature adjust</code>	Set the temperature correction value of the temperature sensor.

2.2 Display commands overview

This section gives a list of display commands that can be used on the NS-2250.

Table 2-2: Display command list

Class	Command	Description
System status display commands	show version	Display the system hardware configuration, system software version, boot information, etc.
	show environment	Display the information of power and Temperature.
	show slot	Display the USB port information.
	show cpu	Display the CPU utilization rate.
	show memory	Display the memory usage rate.
	show log	Display the console log or the command execution log.
	show support	Command used to display support information.
Bonding display commands	show bonding	Display the bonding information.
Network information display commands	show ether	Display information about the NS-2250 LAN port.
	show stats ether	Display statistical information about the NS-2250 LAN port.
	show ipinterface	Display information about the NS-2250 IP interface.
	show ip	Display the NS-2250 host name and IP address, and the TCP keepalive time.
	show ipv6	Display the NS-2250 IPv6 address.
	show ip host	Display a list of the host names and IP addresses registered to the NS-2250.
	show ip route	Display the static routes registered to the NS-2250.
	show ipv6route	Display static routes of IPv6 registered in NS-2250.
	show tcp	Display the status of the TCP session.
	show udp	Display the status of UDP.
	show stats ip	Display the IP statistical information.
	show stats ipv6	Display the IPv6 statistical information.
	show stats icmp6	Display the ICMPv6 statistical information.
	show arp	Display the content of ARP entries.
	show ndp	Display the contents the address mapping table used in Neighbor Discovery Protocol(NDP).
	show stats tcp	Display TCP statistical information.
	show stats udp	Display UDP statistical information.
	show dns	Display the settings of the NS-2250 DNS client function.
Ipfiler status display commands	show ipfilter	Display the registration status of the ipfilter.

Continued on next page

Table 2-2: Display command list(continued)

Class	Command	Description
	show stats ipfilter	Display the statistics information of the ipfilter.
Ipssec status display commands	show ipsec secret	Display the registration list of apre-shared key used in the IKE.
	show ipsec conn	Display the information of the connection setting.
	show ipsec status	Display the information of ISAKMP-SA/IPSEC-SA.
	show ipsec spd	Display the information of the security policy database.
	show ipsec sad	Display the information of the security association database.
User status display commands	show user	Display a list of created users.
	show user login	Display a list of currently logged in users.
SNMP status display command	show snmp	Display the status of the SNMP agent.
SNTP status display command	show sntp	Display the status of the SNTP client.
Syslog status display command	show syslog	Display the status of the syslog client.
NFS status display command	show nfs	Display the status of the NFS client function.
Port server status display commands	show portd	Display the port server status.
	show portd tty	Display the port server setting for each serial port.
	show portd session	Display the status of port server sessions.
	show tty	Displays the status of the serial ports.
	show stats tty	Displays the serial ports statistical information.
	show logd	Display the port log status of each serial port.
	show stats logd tty	Display the port log statistical information of each serial port.
CONSOLE port status display command	show console	Display the CONSOLE port status.
	show stats console	Display the CONSOLE port statistical information.
Display command for the internal management servers	show service	Display status of internal management servers.
Display command for the list of hosts and services authorized for connection	show allowhost	Display a list of hosts and services authorized for connection.
Setting file display commands	show config	Display the NS-2250 current settings.
	show config startup	Display the content of the startup files.

Continued on next page

Table 2-2: Display command list(continued)

Class	Command	Description
	show config info	Display information related to the startup files.
Terminal setting information display command	show terminal	Display the settings of the used terminal.
Authentication/accounting function display commands	show auth	Display the user authentication method.
	show auth radius	Display the RADIUS authentication client settings.
	show auth tacacs	Display the settings for TACACS+ authentication and approval.
	show auth access_group	Display the access group setting information.
	show stats auth radius	Display the statistical information of RADIUS authentication client.
	show stats auth tacacs	Displays TACACS+ statistical information.
	show acct	Display the account saving method.
	show acct radius	Display the RADIUS accounting client settings.
	show acct tacacs	Display the settings for TACACS+ accounting.
	show stats acct radius	Display statistical information of the RADIUS accounting client.
	show stats acct tacacs	Display statistical information of TACACS+ accounting.
Time zone display command	show timezone	Display the NS-2250 time zone and a list of the time zones that can be set.

2.3 Maintenance command overview

This section gives a list of maintenance commands that can be used on the NS-2250.

Table 2-3: Maintenance command list

Class	Command	Description
Basic maintenance commands	<code>date</code>	Set and display the NS-2250 date and time.
	<code>engineering</code>	Switch the NS-2250 operating mode to engineering mode.
	<code>exit</code>	This command is alias of <code>logout</code>
	<code>logout</code>	Log out from the NS-2250.
	<code>ping</code>	Confirm the communication with the connected host on an IP network.
	<code>ping6</code>	Confirm IPv6 communication with the connected host on the IP network.
	<code>reboot</code>	Reboot the NS-2250.
	<code>shutdown</code>	Shut down the NS-2250.
	<code>su</code>	Log in as a device management user.
	<code>telnet</code>	Log in to a connected host via a Telnet client.
	<code>tracert</code>	Examine the information of the route to the specified host.
	<code>tracert6</code>	Examine the information of the route to the specified host
	<code>switch bonding</code>	Switch the active port.
	<code>hangup</code>	Reset the service of a specific serial port.
	<code>history</code>	Display the command execution history.
	<code>logsave</code>	Save the port logs of serial ports.
	<code>loginfo</code>	Display a list of port log files saved in a FLASH memory, and the used and free space.
	<code>clear arp</code>	Delete all dynamic ARP entries registered in the NS-2250.
	<code>trace</code>	Perform tracing of the packets sent and received by the NS-2250 for each protocol.
	<code>disconnect</code>	Disconnect the TCP session connected to the specified service.
	<code>tftp setup</code>	Send and receive the startup files by TFTP.
	<code>tftp verup</code>	Send and receive the upgrade files for system by TFTP.
	<code>tftp log</code>	Send the log files by TFTP.
	<code>tftp support</code>	Send the supportlog files by TFTP.
	<code>ftp</code>	Various files is sent and received between the FTP server.
Management commands for settings files	<code>write</code>	Save the NS-2250 current settings in the specified startup file.
	<code>clear startup</code>	Return the specified startup file to the default settings.
	<code>default startup</code>	Specify the startup file to be imported at startup.

Continued on next page

Table 2-3: Maintenance command list(continued)

Class	Command	Description
Management command for the system software	copy startup	Copy a startup file.
	echo	Display the specified character string.
	copy system	Copy the system software image.
	verup execute	Upgrade or downgrade the system software using a file sent via FTP or SFTP.
	verup cleanup	Delete the system software upgrade or downgrade file sent via FTP or SFTP.
	backup system-image	Made the backup of system software.
	restore system-image	Restore the backup of system software.
	clear system-image	Delete the backup file of system software.
Console output control commands	show system-image	Displays the backup file and restore file of system software.
	console	The output destination of a console message is controlled.
Terminal output control commands	loglevel	Change the output level of the console messages.
	terminal timeout	Set the terminal automatic logout time.
	terminal editing	Enable or disable the terminal line editing function.
	terminal page	Enable or disable the terminal paging function.
	terminal height	Specify the number of lines per page of the terminal.
	terminal width	Specify the number of characters per line of the terminal.
	terminal prompt	Specify the display format of the terminal prompt.
	terminal redisp	Specify whether or not to redisplay the previously entered command string on the next prompt screen after a command input error has occurred.

2.4 Other commands overview

This section gives a list of port server menu and port selection menu commands that can be used on the NS-2250.

Table 2-4: List of port server menu commands

Class	Command	Description
Port server menu commands	0 (return Port Select Menu)	Return to port selection menu.
	1 (display Port Log)	Display the port log of the currently connected serial port.
	2 (display Port Log (LAST))	Display the most recent part of the ports log of the currently connected serial port.
	3 (start tty connection)	Access the monitored equipment.
	4 (close telnet/ssh session)	Close the session of the currently connected serial port.
	5 (show all commands)	Display a list of port server menu commands.
	6 (display & erase Port Log)	Display and delete the port log of the currently connected serial port.
	7 (erase Port Log)	Delete the port log of the currently connected serial port.
	8 (send Port Log)	Forcibly send the port log of the currently connected serial port to the external FTP/email server that has been set.
	9 (show Port Log configuration)	Display setting information, such as the save space, transfer interval, and transfer destination server of the port log of the currently connected serial port.
	10 (send break to tty)	Send a break signal to the currently connected serial port.
Port selection menu commands	<i>ttyno</i>	Connect to the specified serial ports in Normal mode.
	<i>ttynor</i>	Connect to the specified serial ports in Normal mode.
	<i>l</i>	Refresh the list of ports to which connection is possible.
	<i>l ttyno-ttyno</i>	Refresh the specified range of ports from list of ports to which connection is possible.
	<i>d</i>	Refresh detailed information of the user connected to the serial port (port number, user name, and IP address of Telnet/SSH client).
	<i>d ttyno-ttyno</i>	Refresh detailed information of the users connected to a range serial ports (port number, user name, and IP address of Telnet/SSH client).
	<i>h</i>	Display a list of port selection menu commands.
	<i>e</i>	Close the port selection menu and disconnect the Telnet/SSH session.

Chapter3

Command reference format

Chapter 3 describes the format used in this command reference.

The commands in this reference manual are explained by class and by object following the format described below.

Command name [Users who can use the command/mode in which the command is available]

Function The command function is explained here.

Format The command input format is described here.
command param1 param2 { param3a | param3b } [param4 param5]
The strings in bold are the command or parameter strings to be entered as they are.
The strings in italic are parameters that can be replaced by a string of your choosing.
{ } enclose multiple parameters separated by the character | from which one must be chosen.
[] enclose parameters that can be omitted.

Parameters The types and functions of the parameters are explained here.

Note Cautionary notes on using the command are given here.

Usage example A usage example of the command is given here.

Execution example
An example of the command execution is given here.

Explanation An explanation such as the contents of the message that is displayed result of executing the command is given here.

Error message The meaning and content of the message that is displayed when an error occurs is given here.

[Users who can use the command/Mode in which the command is available] shows the users with the privilege required to use the command and the modes in which the command can be used. One or several of the following four types of users and modes are specified for each command.

[Normal user]	A normal user
[Administrator]	A device management user
[Port user]	A user who can access the NS-2250 serial ports

[Required version] shows the system software version in which the command has been added.

Chapter4

Setting commands

Chapter 4 describes the setting commands that can be used on the NS-2250.

4.1 System setting commands

Commands used to configure the host name, IP address, netmask, and other objects defining the NS-2250.

set hostname

[Administrator]

Function Configure the NS-2250 host name.

Format **set hostname** *name*

Parameters *name*

Specify the host name of the NS-2250.

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 before or after a period.

The maximum number of characters that can be set for a host name is 64.

The default setting for this parameter in the startup file is "NS-2250".

Usage example To set "SmartCS" as the NS-2250 host name.

set hostname SmartCS

set ipaddr**[Administrator]**

Function Set the NS-2250 IP address.

Format **set ipaddr** [{ **eth1** | **eth2** | **bond1**}] *ipaddr/mask*

Parameters [{ **eth1** | **eth2** | **bond1** }]

Specify the interface of the NS-2250.

The default setting for this parameter is eth1.

ipaddr/mask

Specify the network address of the NS-2250 as IP address/prefix size.

The IP address must be specified in the dot-decimal notation

(xxx.xxx.xxx.xxx).

If the prefix size is omitted, the setting is made according to the class.

The default setting for this parameter in the startup file is

"192.168.0.1/24".

Note

- The registered static routes are deleted if you change the IP address of the NS-2250.
- It is recommend to operate from the console terminal or from a terminal on the same segment as the NS-2250 to change the IP address of the NS-2250.
- When the bonding function is enabled, eth1 and eth2 interface designation is error.
- When the bonding function is disabled, bond1 interface designation is error.
- When the bonding function is disabled, the default setting for this parameter is eth1.
- When the bonding function is enabled, the default setting for this parameter is bond1.
- When the bonding function is enabled, SNMPv1 trap of agent-address field and the RADIUS NAS-IP-address is set to the IP address of bond1 interface.
- If you disable the bonding function, it is set to the IP address of the eth1 interface.
- This command can not be executed when the IPsec function is enabled.

Usage example To set the 192.168.1.1 as the NS-2250 IP address with a prefix size of 24.

set ipaddr eth1 192.168.1.1/24

unset ipaddr**[Administrator]**

Function	Unset the NS-2250 IP address.
Format	unset ipaddr { eth1 eth2 bond1 }
Parameters	{ eth1 eth2 bond1 } Specify the interface of the NS-2250. The default setting for this parameter is eth1.
Note	<ul style="list-style-type: none"> • The registered static routes are deleted if you change the IP address of the NS-2250. • It is recommend to operate from the console terminal or from a terminal on the same segment as the NS-2250 to change the IP address of the NS-2250. • When the bonding function is enabled, eth1 and eth2 interface designation is error. • When the bonding function is disabled, bond1 interface designation is error. • When the bonding function is disabled, the default setting for this parameter is eth1. • When the bonding function is enabled, the default setting for this parameter is bond1. • When the bonding function is enabled, SNMPv1 trap of agent-address field and the RADIUS NAS-IP-address is set to the IP address of bond1 interface. • If you disable the bonding function, it is set to the IP address of the eth1 interface. • This command can not be executed when the IPsec function is enabled.
Usage example	Unset the 192.168.1.1 as the NS-2250 IP address <pre>unset ipaddr eth1</pre>

set tcpkeepalive**[Administrator]**

Function	Set the TCP keepalive time for the NS-2250.
Format	set tcpkeepalive <i>time</i>
Parameters	<i>time</i> Specify the TCP keepalive time for the NS-2250 (the time until a keepalive probe is sent in idle condition in TCP connection) in seconds in the range of 60 to 7200. The default setting for this parameter in the startup file is 180 seconds.
Note	<ul style="list-style-type: none">• If there is no response to the keepalive probe packet, the packet is sent at 5 second intervals thereafter. If there is no response six times consecutively, reset the connection.
Usage example	To set the TCP keepalive time for the NS-2250 to 10 minutes. set tcpkeepalive 600
Explanation	The changed value is applied from the next session.

4.2 bonding setting commands

set bonding up_delay

[Administrator]

Function	configure the wait timer which is the delay period enabling slave interface after the detection of physical linkup.
Format	set bonding up_delay { on <i>delay_time</i> off }
Parameters	<p>{ on <i>delay_time</i> off }</p> <p>configure the wait timer which is the delay period enabling slave interface after the detection of physical linkup. This parameter is "off" by default.</p> <p>on <i>delay_time</i> Specify the period by a second to wait before enabling a slave interface. The setting range is from 1 through 60 seconds.</p> <p>off No wait. The slave interface is in an available condition immediately when detect a physical linkup.</p>
Note	<ul style="list-style-type: none"> • When bonding master interface is down, the slave interface is in an available condition immediately with or without this setting. • If this parameter is "on", the condition of slave interface is going back during waiting period. • When detect physical link down during a going back state, the slave interface becomes the state to down.
Usage example	<p>To set a period for 30 seconds.</p> <p>set bonding up_delay on 30</p>

enable bonding**[Administrator]****Function** Enable the bonding function.**Format** **enable bonding****Parameters** None

Note

- The bonding function is disabled by default.
- When the bonding function is enabled, the setting of IP address/routing at eth1 is automatically inherited to bond1, and the configuration of IP address/routing at eth1/eth2 are deleted.
- When the bonding function is enabled, the setting information by the "set ip-interface mtu" command is canceled.
- This command can not be executed when the IPsec function is enabled.

Usage example **enable bonding**

disable bonding**[Administrator]****Function** Disable the bonding function.**Format** **disable bonding****Parameters** None

Note

- When the bonding function is disabled, the setting of IP address/routing at bond1 is automatically inherited to eth1.
- When the bonding function is disabled, routing information set by the "create ip route" command is inherited.
- When the bonding function is disabled, the setting information by the "set ipinterface mtu" command is canceled.

Usage example **disable bonding**

4.3 ipinterface setting commands

set ipinterface mtu

[Administrator]

Function	Set the MTU of each interface.
Format	set ipinterface { eth1 eth2 bond1 } mtu <i>mtu_size</i>
Parameters	<p>{ eth1 eth2 bond1 } Specify the interface to set the MTU.</p> <p><i>mtu_size</i> Specify the MTU in the range from 1000 to 1500 in an integer. (The unit : Byte) The default value is "1500".</p>
Note	<ul style="list-style-type: none"> • If you enable / disable the bonding function, the information of the MTU setting by this command is deleted. • If the bonding function is enabled, specifying the interface eth1 and eth2 occurs an error. If the bonding function is disabled, specifying the interface bond1 occurs an error. • If you set the MTU to less than 1280, IPv6 communication function can not be enabled. • When the IPv6 communication function is enabled, MTU can not be set to less than 1280.
Usage example	<p>The case of setting the MTU of eth1 as 1280(bytes).</p> <p>set ipinterface eth1 mtu 1280</p>

4.4 IPv6 setting commands

create ip6**[Administrator]****Function** Enable the IPv6 communication function.**Format** **create ip6****Parameters** None

Note

- The IPv6 communication function is disabled by default.
- When IPv6 communication function is enabled, the following commands can be executed.
 - set ip6addr
 - unset ip6addr
 - create ip6route
 - delete ip6route
 - ping6
- If you set the MTU to less than 1280, IPv6 communication function can not be enabled. (set ipinterface)
- When the IPv6 communication function is enabled, MTU can not be set to less than 1280.

Usage example The case of enabling the IPv6 communication function.

create ip6

set ip6addr**[Administrator]**

Function Set the NS-2250 IPv6 address.

Format **set ip6addr { eth1 | eth2 | bond1 } ip6addr/mask**

Parameters **{ eth1 | eth2 | bond1 }**

Specify the interface of the NS-2250.

ip6addr/mask

Specify the IPv6 address of this device with "IPv6 address/mask length".

Specify the IPv6 address in x:x:x:x:x:x:x format.

The "x" in each field of the address is represented by the hexadecimal of the 16 bit part.

If there are consecutive 0 in the front of the field they can be omitted.

The field composed of only 0 can also be omitted only once by specifying as "::" in the address.

Specify the length of mask in the range of 3 to 128.

Note

- When setting this command, you need to enable the IPv6 communication function.(create ip6)
- When IPv6 communication function is disabled, the setting by this command is canceled.
- If you change the IPv6 address of this device, the corresponding IPv6 static route will be deleted.
- It is recommend to operate from the console terminal or from a terminal on the same segment as the NS-2250 to change the IPv6 address of the NS-2250.
- When the bonding function is enabled, eth1 and eth2 interface designation is error.
- When the bonding function is disabled, bond1 interface designation is error.
- The range of the IPv6 address that can be set with this command is the global unicast address (2000 :: / 3).
- When the IPv6 communication function is enabled, the link local address is automatically generated from the MAC address at the time of the linking-up of a target port, and it becomes available regardless of the setting.

Usage example To set the 2001::200c:417a as the NS-2250 IPv6 address with a prefix size of 64.

set ip6addr eth1 2001::200c:417a/64

unset ip6addr**[Administrator]****Function** Unset the NS-2250 IPv6 address.**Format** **unset ip6addr { eth1 | eth2 | bond1 }****Parameters** **{ eth1 | eth2 | bond1 }**
Specify the interface of the NS-2250.**Note**

- If you delete the IPv6 address of this device, the corresponding IPv6 static route is deleted.
- It is recommend to operate from the console terminal or from a terminal on the same segment as the NS-2250 to change the IPv6 address of the NS-2250.
- When the bonding function is enabled, eth1 and eth2 interface designation is error.
- When the bonding function is disabled, bond1 interface designation is error.

Usage example Unset the IPv6 address of eth1 on the NS-2250.**unset ip6addr eth1**

delete ip6**[Administrator]****Function** Disable the IPv6 communication function.**Format** **delete ip6****Parameters** None

- Note**
- The IPv6 communication function is disabled by default.
 - When IPv6 communication function is disabled, the following commands cannot be executed.
 - set ip6addr
 - unset ip6addr
 - create ip6route
 - delete ip6route
 - ping6
 - traceroute6
 - When IPv6 communication function is disabled, the setting by the following command will be deleted.
 - set ip6addr
 - create ip6route

Usage example The case of disabling the IPv6 communication function.

delete ip6

4.5 IP host setting commands

These are objects managing the handling of host names and IP addresses.
Pairs of these objects are registered as host entries.

create ip host

[Administrator]

Function	Register a pair of a host name and an IP address (host entry).
Format	create ip host <i>hostname</i> { <i>ipaddr</i> <i>ip6addr</i> } [port <i>port_num</i>]
Parameters	<p><i>hostname</i></p> <p>Specify the host name to be registered.</p> <p>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.</p> <p>Furthermore, a hyphen, period, or underbar cannot be used before or after a period.</p> <p>The maximum number of characters that can be set for a host name is 64.</p> <p>{ <i>ipaddr</i> <i>ip6addr</i> }</p> <p>Specify an IP address for the host name.</p> <p><i>ipaddr</i></p> <p>Specify the IPv4 address.</p> <p>The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).</p> <p><i>ip6addr</i></p> <p>Specify the IPv6 address in x:x:x:x:x:x:x:x format.</p> <p>The "x" in each field of the address is represented by the hexadecimal of the 16 bit part.</p> <p>If there are consecutive 0 in the front of the field they can be omitted.</p> <p>The field composed of only 0 can also be omitted only once by specifying as "::" in the address.</p> <p>[port <i>port_num</i>]</p> <p>Specify the TCP port number of the device to which you want to connect with Telnet commands.</p> <p>You can specify a number from 0 through 65535 for the port number.</p> <p>This port number is valid only for Telnet clients of the NS-2250. It is not used by other clients (ping or Sntp, syslog, FTP, SNMP, etc.).</p>
Note	<ul style="list-style-type: none"> • A host with the name "localhost" cannot be registered. • If IPv6 address is specified, port option can not be specified. • Do not set multiple IPv4 addresses with the same host name or multiple IPv6 addresses with the same host name.
Usage example	<p>To register a host with "host10" as the host name, and "192.168.1.10" as the IP address.</p> <pre>create ip host host10 192.168.1.10</pre>
Explanation	You can create up to 99 host entries.

delete ip host**[Administrator]****Function** Delete the host entry.**Format** **delete ip host** *hostname* { *ipaddr* | *ip6addr* }**Parameters** *hostname*

Specify the host name to delete.

{ *ipaddr* | *ip6addr* }

Specify an IP address for the host name.

ipaddr

Specify the IPv4 address.

The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).

ip6addr

Specify the IPv6 address in x:x:x:x:x:x:x format.

The "x" in each field of the address is represented by the hexadecimal of the 16 bit part.

If there are consecutive 0 in the front of the field they can be omitted.

The field composed of only 0 can also be omitted only once by specifying as "::" in the address.

Usage example To delete the host entry with the host name "host10(IP address 192.168.0.100)".**delete ip host host10 192.168.0.100**

4.6 IP route setting commands

These are objects managing the static routing settings for the NS-2250.
Set the destination network address and the gateway address.

create ip route

[Administrator]

Function	Create a static route to an IP address.
Format	create ip route { <i>ipaddr/mask</i> default } gateway <i>gwaddr</i> [metric <i>metric</i>]
Parameters	<p>{ <i>ipaddr/mask</i> default }</p> <p>Set the host address or the network address of the destination in the "IP address/prefix size" format.</p> <p><i>ipaddr/mask</i></p> <p>The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx). If the prefix size is omitted, the setting is made according to the class.</p> <p>default</p> <p>This represents the default gateway. The parameter is set to the default gateway also if you specify "0.0.0.0/0".</p> <p>gateway <i>gwaddr</i></p> <p>Specify the IP address of the gateway used to forward the IP packets.</p> <p>[metric <i>metric</i>]</p> <p>Specify the value of metric in the 0 to 100 range. The parameter is set to the default value 0 if omitted.</p>
Usage example	<p>To set 192.168.1.1 as the NS-2250 default gateway.</p> <p>create ip route default gateway 192.168.1.1</p>
Explanation	<p>You can create up to 99 static routes.</p> <p>To modify a static route, first delete it with the "delete ip route" command, and then add a new one with the "create ip route" command.</p>

delete ip route**[Administrator]****Function** Delete the static route.**Format** **delete ip route { *ipaddr/mask* | **default** } gateway *gwaddr*****Parameters** **{ *ipaddr/mask* | **default** }**

Specify the destination host address or network address to be deleted in the "IP address/prefix size" format.

ipaddr/mask

The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).

If the prefix size is omitted, the setting is made according to the class.

default

This represents the default gateway.

The parameter is set to the default gateway also if you specify "0.0.0.0/0".

gateway *gwaddr*

Specify the IP address of the gateway to delete.

Usage example **delete ip route default gateway 192.168.1.1****Explanation** To modify a static route, first delete it with the "delete ip route" command, and then add a new one with the "create ip route" command.

4.7 IPv6 route setting commands

create ip6route

[Administrator]

Function Create static routes for IPv6.

Format **create ip6route** { *ip6addr/mask* | **default** } **gateway** *gw6addr* [**metric** *metric*]

Parameters { *ip6addr/mask* | **default** }

Specify the host address or network address of the destination.

ip6addr/mask

Specify the host address or network address of the destination in "IPv6 address/length of mask" format.

Specify the IPv6 address in x:x:x:x:x:x:x format.

The "x" in each field of the address is represented by the hexadecimal of the 16 bit part.

If there are consecutive 0 in the front of the field they can be omitted.

The field composed of only 0 can also be omitted only once by specifying as "::" in the address.

Specify the length of mask in the range of 0 to 128.

default

This represents the default gateway.

The parameter is set to the default gateway also if you specify "::/0".

gateway *gw6addr*

Specify the IPv6 gateway address where the IP packet is forwarded.

Specify the IPv6 address in x:x:x:x:x:x:x format.

The "x" in each field of the address is represented by the hexadecimal of the 16 bit part.

If there are consecutive 0 in the front of the field they can be omitted.

The field composed of only 0 can also be omitted only once by specifying as "::" in the address.

Note

- You can create up to 99 static routes.
- To modify a static route, first delete it with the "delete ip6route" command, and then add a new one with the "create ip6route" command.
- If IPv6 communication function is disabled with "delete ip 6" command, the setting by this command will be deleted.

Usage example To set 2001:db8::100 as the NS-2250 default gateway.

create ip6route default gateway 2001:db8::100

delete ip6route**[Administrator]****Function** Delete the static route.**Format** **delete ip6route { ip6addr/mask | default } gateway gw6addr****Parameters** **{ip6addr/mask | default}**

Specify the host address or network address of the static route to delete.

ip6addr/mask

Specify the host address or network address of the static route to delete in "IPv6 address/length of mask" format.

Specify the IPv6 address in x:x:x:x:x:x:x format.

The "x" in each field of the address is represented by the hexadecimal of the 16 bit part.

If there are consecutive 0 in the front of the field they can be omitted.

The field composed of only 0 can also be omitted only once by specifying as "::" in the address.

Specify the length of mask in the range of 0 to 128.

default

This represents the default gateway.

The parameter is set to the default gateway also if you specify "::/0".

gateway gw6addr

Specify the IPv6 gateway address where the IP packet is forwarded.

Specify the IPv6 address in x:x:x:x:x:x:x format.

The "x" in each field of the address is represented by the hexadecimal of the 16 bit part.

If there are consecutive 0 in the front of the field they can be omitted.

The field composed of only 0 can also be omitted only once by specifying as "::" in the address.

Usage example Delete the default route whose gateway is 2001:db8::100.**delete ip6route default gateway 2001:db8::100**

4.8 ipfilter setting commands

These are objects managing the ipfilter function of the NS-2250.

create ipfilter

[Administrator]

Function	Register the filter conditions.
Format	<pre>create ipfilter input [line line] { accept drop } { eth1 eth2 bond1 any } { dstaddr/mask any } { srcaddr/mask any } { esp icmp [{ type any }] tcp [{ dport any }] udp [{ dport any }] any }</pre>
Parameters	<p>input [line line] Register the filter condition for the received packet.</p> <p>line line It specifies the line number to register the filter conditions (1 to 64). If you omit this setting, it will be registered on the bottom line. In filter processing, the condition judgment is performed in order from the filter condition with the smallest line number.</p> <p>line Insert the filter condition in the line.</p> <p>{ accept drop } It specifies the behavior of the matched packets to filter conditions.</p> <p>accept If it matches the condition, the packet is transparent.</p> <p>drop If it matches the condition, discard the packet.</p> <p>{ eth1 eth2 bond1 any } It specifies the interface that has passed through as a filter condition.</p> <p>eth1 A packet that has passed through the eth1 specified as a filter condition.</p> <p>eth2 A packet that has passed through the eth2 specified as a filter condition.</p> <p>bond1 A packet that has passed through the bond1 specified as a filter condition.</p> <p>any Interface is not specified as a filter condition.</p> <p>{ dstaddr/mask any } Specify the destination IP address of the packet as a filter condition.</p> <p>dstaddr/mask The destination IP address of the packet specified in the "IP address/mask length". If you omit the mask length assumes that the 32bit mask.</p> <p>any The destination IP address of the packet does not specify as a filter condition.</p> <p>{ srcaddr/mask any } Specify the source IP address of the packet as a filter condition.</p> <p>srcaddr/mask The source IP address of the packet specified in the "IP address / mask length". If you omit the mask length assumes that the 32bit mask.</p>

any

The source IP address of the packet does not specify as a filter condition.

```
{ esp | icmp [{ type | any }] | tcp [{ dport | any }] | udp [{ dport | any }]
| any }
```

Specify the IP-level protocol as a filter condition.

esp

To IP-level protocol to specify the esp (protocol number = 50) as a filter condition.

```
icmp [{ type | any }]
```

To IP-level protocol to specify the ICMP (protocol number = 1) as a filter condition.

type

The type of ICMP protocol Specify a value in the range of 0 to 255.

any

Type of ICMP protocol does not specify as a filter condition.

```
tcp [{ dport | any }]
```

To IP-level protocol to specify the TCP (protocol number = 6) as a filter condition.

dport

The TCP destination port number you specified in the range of value of from 1 to 65535.

any

The TCP destination port number is not specified as a filter condition.

```
udp [{ dport | any }]
```

To IP-level protocol to specify the UDP (protocol number = 17) as a filter condition.

dport

The UDP destination port number you specified in the range of value of from 1 to 65535.

any

The UDP destination port number is not specified as a filter condition.

any

The IP-level protocol does not specify as a filter condition.

Note

- If you specify a line number in-line parameters, there is a case where the registration line or registration line of a new filter condition setting of the existing filter condition setting is automatically changed as follows.
- If you already have a filter condition to the specified line has been registered, the deviation in the back one of the existing filter condition setting the row number of the specified line or later, the specified line will be replaced with the new setting.
- If the filter condition setting than the specified line in a small line of line number is not registered, it will automatically pre-filling of the line number is done.

Usage example Register the following conditions in the second line of the filter.

```
receive interface : eth1
source IP address : 172.31.0.0/16
port number : TCP23
filter behavior : accept
```

```
create ipfilter input line 2 accept eth1 any 172.31.0.0/16 tcp 23
```

Explanation

The number can be registered filter conditions in the entire device can be up to 64.
If you do not match all the registered filter conditions, and then transmits the packet.

delete ipfilter**[Administrator]**

Function Delete the registered filter conditions.

Format **delete ipfilter input { accept | drop } { eth1 | eth2 | bond1 | any }
 { dstaddr/mask | any } { srcaddr/mask | any }
 { esp | icmp [{ type | any }] | tcp [{ dport | any }] | udp [{ dport | any }] | any }}**

Parameters **input**
 Deletes the filter condition registered for the received packet.

{ accept | drop }
 Specify the delete filter conditions.

accept
 Specify the filter conditions which transmits the packet.

drop
 Specify the filter conditions which discards the packet.

{ eth1 | eth2 | bond1 | any }
 It specifies the interface that has passed through as a filter condition.

eth1
 A packet that has passed through the eth1 specified as a filter condition.

eth2
 A packet that has passed through the eth2 specified as a filter condition.

bond1
 A packet that has passed through the bond1 specified as a filter condition.

any
 Interface is not specified as a filter condition.

{ dstaddr/mask | any }
 Specify the destination IP address of the packet as a filter condition.

dstaddr/mask
 The destination IP address of the packet specified in the "IP address/mask length". If you omit the mask length assumes that the 32bit mask.

any
 The destination IP address of the packet does not specify as a filter condition.

{ srcaddr/mask | any }
 Specify the source IP address of the packet as a filter condition.

srcaddr/mask
 The source IP address of the packet specified in the "IP address/mask length". If you omit the mask length assumes that the 32bit mask.

any
 The source IP address of the packet does not specify as a filter condition.

{ esp | icmp [{ type | any }] | tcp [{ dport | any }] | udp [{ dport | any }] | any }
 Specify the IP-level protocol as a filter condition.

esp
 To IP-level protocol to specify esp the (protocol number = 50) as a filter condition.

icmp [{ type | any }]
 To IP-level protocol to specify the ICMP (protocol number = 1) as a filter condition.

tcp [{ *dport* | **any** }]

To IP-level protocol to specify the TCP (protocol number = 6) as a filter condition.

udp [{ *dport* | **any** }]

To IP-level protocol to specify the UDP (protocol number = 17) as a filter condition.

any

The IP-level protocol does not specify as a filter condition.

Note

After specifying the line number by the parameter "line", if the filter condition is deleted the line number of the filter condition registered to the behind line is moved forward one by one.

Usage example

Delete the following conditions in the second line of the filter.

receive interface : eth1

source IP address : 172.31.0.0/16

port number : TCP23

filter behavior : accept

delete ipfilter input accept eth1 any 172.31.0.0/16 tcp 23

delete ipfilter line**[Administrator]**

Function Delete the registered filter condition by specifying a line number.

Format **delete ipfilter input line** *line*

Parameters **input**

Delete the registered filter condition for received packets.

line *line*

Delete the filter condition by specifying the line number.

line

Specify the line number(1 to 64) to delete.

Note

- Execute the command "show ipfilter" to confirm the filter condition and line number to delete.
- After specifying the line number by the parameter "line", if the filter condition is deleted the line number of the filter condition registered to the behind line is moved forward one by one.

Usage example The case of deleting the third line of the filter condition for received packets.

delete ipfilter input line 3

delete ipfilter allentry**[Administrator]****Function** Delete all filter conditions.**Format** **delete ipfilter input allentry****Parameters** **input**

Delete a registered filter condition for received packets.

allentry

Delete all registered filter conditions.

Usage example The case of deleting all registered filter conditions for received packets.**delete ipfilter input allentry**

enable ipfilter**[Administrator]****Function** Enable the filter function.**Format** **enable ipfilter****Parameters** None

Note

- The filter function is disabled by default.
- The target of this command is an IPv4 packet transmitted and received by the NS-2250.

Usage example The case of enabling the filter function.

enable ipfilter

disable ipfilter**[Administrator]**

Function	Disable the filter function.
Format	disable ipfilter
Parameters	None
Usage example	The case of disabling the filter function. disable ipfilter

4.9 ipsec setting commands

These are objects managing the ipsec function of the NS-2250.

create ipsec secret psk

[Administrator]

Function	Register a pre-shared key used in the IKE.
Format	create ipsec secret psk { <i>id1</i> [<i>id2</i>] any } { password encrypt <i>string</i> }
Parameters	<p>secret psk Register a pre-shared key used in the IKE.</p> <p>{ <i>id1</i> [<i>id2</i>] any } Specify a condition to select a pre-shared key.</p> <p><i>id1</i> [<i>id2</i>] Specify the ID as a condition.</p> <p><i>id1</i> Specify the first ID as a condition.</p> <p>[<i>id2</i>] Specify the second ID as a condition.</p> <p>any Do not specify the ID as a condition.</p> <p>{ password encrypt <i>string</i> } Register a pre-shared key.</p> <p>password Register a pre-shared key. If you specify this parameter to execute the command, the message to input a pre-shared key is displayed. So enter a pre-shared key according to the message. After inputting a pre-shared key, the re-input message to confirm a pre-shared key is displayed if you push the Enter key. So enter the same pre-shared key. If you set a pre-shared key by this command, a form of the command recorded in the startup file is replaced the one to specify the encrypt parameter. The set pre-shared key becomes the string after it has been encrypted. You can confirm a converted pre-shared key by executing the command "show config".</p> <p>encrypt <i>string</i> Set a pre-shared key using the encrypted string. If you specify this parameter to execute the command, the message to input and confirm a pre-shared key is not displayed. Use this parameter in the case of pouring the startup file.</p>

Note A pre-shared key is registered in the order you executed this command.
 SA is created using a registered pre-shared key.
 In the case of registering a pre-shared key, specify two IDs as a selection condition. They are the security gateway ID of the own side(This is the value set by the command "set ipsec conn leftid". If it is not set, this is the value set by the command "set ipsec conn left".) and the security gateway ID of the opposite side(This is the value set by the command "set ipsec conn rightid".
 If it is not set, this is the value set by the command "set ipsec conn right".).
 If there are some registered pre-shared keys, one of them chosen according to the following priority is used.

1.A pre-shared key set both the security gateway ID of the own side(This is the value set by the command "set ipsec conn leftid". If it is not set, this is the value set by the command "set ipsec conn left".) and the security gateway ID of the opposite side(This is the value set by the command "set ipsec conn rightid". If it is not set, this is the value set by the command "set ipsec conn right".).

2.A pre-shared key set the security gateway ID of the opposite side(This is the value set by the command "set ipsec conn rightid". If it is not set, this is the value set by the command "set ipsec conn right".).

3.A pre-shared key set the security gateway ID of the own side(This is the value set by the command "set ipsec conn leftid".).

4.A pre-shared key not specified the ID as a selection condition(The setting value is "any".).

5.A pre-shared key set the security gateway ID of the own side(This is the value set by the command "set ipsec conn left".).

If there are some pre-shared key whose priority is same, the lower one is used preferentially.

Usage example The case of registering a pre-shared key whose condition is that both the security gateway ID "200.0.0.1" of the own side and the security gateway ID "100.0.0.1" of the opposite side are selected.

```
create ipsec secret psk 200.0.0.1 100.0.0.1 password
```

```
New password : Input a pre-shared key(not displayed)
```

```
Retype new password : Input a pre-shared key(not displayed)
```

delete ipsec secret psk**[Administrator]**

Function Delete a pre-shared key used in the IKE.

Format **delete ipsec secret psk { id1 [id2] | any | allentry }**

Parameters **secret psk**

Delete a pre-shared key used in the IKE.

{ id1 [id2] | any | allentry }

Specify a condition to select a pre-shared key you delete.

id1 [id2]

Specify the ID as a condition.

id1

Specify the first ID as a condition.

[id2]

Specify the second ID as a condition.

any

Do not specify the ID as a condition.

allentry

Delete all registered pre-shared keys.

Usage example The case of deleting a pre-shared key whose condition is that both the security gateway ID "200.0.0.1" of the own side and the security gateway ID "100.0.0.1" of the opposite side are selected.

delete ipsec secret psk 200.0.0.1 100.0.0.1

set ipsec conn auto**[Administrator]**

Function	Set initiator or responder of key exchange.
Format	set ipsec conn <i>connlist</i> auto { start add }
Parameters	<p>conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".</p> <p>auto { start add } Set initiator or responder of key exchange. The default value is "start".</p> <p>start Set this parameter to the side of initiating a key exchange.</p> <p>add Set this parameter to the side of responding.</p>

Note

- In the case of setting this parameter "start" and the SA established after NS-2250 initiating a key exchange, it becomes the initiator of the SA. In the case of the SA established after the opposite side initiates a key exchange, NS-2250 becomes the responder of the SA regardless of the setting by this command.
- In the case of setting this parameter "start" and enabling the target connection, NS-2250 initiates a key exchange. In the case of the IPSEC-SA deleted because of the case IPSEC-SA is not generated, it is judged by DPD that the SA to the opposite side is not established, and a process of rekey failed, NS-2250 initiates a key exchange once again.

Usage example The case of setting the connection 1 the side to initiate a key exchange.

set ipsec conn 1 auto start

set ipsec conn leftid**[Administrator]**

Function Set the ID of the security gateway of own side.

Format **set ipsec conn connlist leftid id**

Parameters **conn connlist**

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

leftid id

Set the ID of the security gateway of own side.

If you do not specify this parameter, an IPv4 address set by the command "set ipsec conn left" is set.

id

Set the ID of the security gateway of own side.

If you specify a string in the dot notation format (the format like xxx.xxx.xxx.xxx), in the IKE protocol the ID is used as an IPv4 address type.

If you specify the character "@" except the head of a string, in the IKE protocol the ID is used as USER_FQDN / RFC822(e-mail address) type.

If you specify the character "@" at the head of a string, in the IKE protocol the ID is used as FQDN(host name) type. In this case, the character "@" at the head of a string is removed.

If you specify the characters "@@" at the head of a string, in the IKE protocol the ID is used as RFC822 type. In this case, the characters "@@" at the head of a string is removed.

If you specify a string except the above, in the IKE protocol the ID is used as FQDN type.

Usage example The case of setting the ID of the security gateway of own side in the connection 1 "alice@example.net".

set ipsec conn 1 leftid alice@example.net

set ipsec conn left**[Administrator]**

Function Set the IP address of the security gateway of own side.

Format **set ipsec conn *connlist* left *ipaddr***

Parameters **conn *connlist***

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

left *ipaddr*

Set the IP address(The IP address of own side executing a key exchange in the IKE protocol) of the security gateway of own side.

ipaddr

Specify the IP address of the security gateway of own side in the dot notation format (the format like xxx.xxx.xxx.xxx).

Note Specify the IP address set by the command "set ip addr".

Usage example The case of setting the IP address of the security gateway of own side in the connection 1 "100.0.0.1".

set ipsec conn 1 left 100.0.0.1

set ipsec conn leftsubnet**[Administrator]**

Function Set the network address of own side which communicates under encrypted by using IPsec.

Format **set ipsec conn *connlist* leftsubnet *ipaddr/mask***

Parameters **conn *connlist***

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

leftsubnet *ipaddr/mask*

Set the network address of own side which communicates under encrypted by using IPsec in the "IP address / mask length" format.

Specify the IP address in the dot notation format (the format like xxx.xxx.xxx.xxx).

If you omit the length of mask, the length of mask is set corresponding to the class.

Usage example The case of setting the network address of own side which communicates under encrypted by using IPsec in the connection 1 "192.168.100.0/24".

set ipsec conn 1 leftsubnet 192.168.100.0/24

set ipsec conn leftsourceip**[Administrator]**

Function	Set the source IP address of own side which communicates in the IPsec tunnel.
Format	set ipsec conn <i>connlist</i> leftsourceip <i>ipaddr</i>
Parameters	<p>conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".</p> <p>leftsourceip <i>ipaddr</i> Set the source IP address of own side which communicates in the IPsec tunnel. <i>ipaddr</i> Specify the source IP address of own side which communicates in the IPsec tunnel in the dot notation format (the format like xxx.xxx.xxx.xxx).</p>
Note	This setting is required depending on the security gateway of the opposite device which communicates using IPsec or the version of the IKE.
Usage example	The case of setting the source IP address of own side which communicates in the IPsec tunnel of the connection 1 "192.168.100.1".
	set ipsec conn 1 leftsourceip 192.168.100.1

set ipsec conn rightid**[Administrator]**

Function	Set the ID of the security gateway of the opposite side.
Format	set ipsec conn <i>connlist</i> rightid <i>id</i>
Parameters	<p>conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".</p> <p>rightid <i>id</i> Set the ID of the security gateway of the opposite side. If you do not specify this parameter, an IPv4 address set by the command "set ipsec conn right" is set.</p> <p><i>id</i> Set the ID of the security gateway of the opposite side. If you specify a string in the dot notation format (the format like xxx.xxx.xxx.xxx), in the IKE protocol the ID is used as an IPv4 address type. If you specify the character "@" except the head of a string, in the IKE protocol the ID is used as USER_FQDN / RFC822(e-mail address) type. If you specify the character "@" at the head of a string, in the IKE protocol the ID is used as FQDN(host name) type. In this case, the character "@" at the head of a string is removed. If you specify the characters "@@" at the head of a string, in the IKE protocol the ID is used as RFC822 type. In this case, the characters "@@" at the head of a string is removed. If you specify a string except the above, in the IKE protocol the ID is used as FQDN type.</p>
Usage example	The case of setting the ID of the security gateway of the opposite side in the connection 1 "bob@example.net".

```
set ipsec conn 1 rightid bob@example.net
```

set ipsec conn right**[Administrator]**

Function	Set the IP address of the security gateway of the opposite side.
Format	set ipsec conn <i>connlist</i> right <i>ipaddr</i>
Parameters	<p>conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".</p> <p>right <i>ipaddr</i> Set the IP address(The IP address of own side executing a key exchange in the IKE protocol) of the security gateway of the opposite side.</p> <p><i>ipaddr</i> Specify the IP address of the security gateway of the opposite side in the dot notation format (the format like xxx.xxx.xxx.xxx).</p>
Usage example	<p>The case of setting the IP address of the security gateway of the opposite side in the connection 1 "200.0.0.1".</p> <p>set ipsec conn 1 right 200.0.0.1</p>

set ipsec conn rightsubnet**[Administrator]**

Function	Set the network address of the opposite side which communicates under encrypted by using IPsec.
Format	set ipsec conn <i>connlist</i> rightsubnet <i>ipaddr/mask</i>
Parameters	<p>conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".</p> <p>rightsubnet <i>ipaddr/mask</i> Set the network address of the opposite side which communicates under encrypted by using IPsec in the "IP address / mask length" format. Specify the IP address in the dot notation format (the format like xxx.xxx.xxx.xxx). If you omit the length of mask, the length of mask is set corresponding to the class.</p>
Usage example	<p>The case of setting the network address of the opposite side which communicates under encrypted by using IPsec in the connection 1 "10.0.0.0/24".</p> <p>set ipsec conn 1 rightsubnet 10.0.0.0/24</p>

set ipsec conn rightsourceip**[Administrator]**

Function	Set the source IP address of the opposite side which communicates in the IPsec tunnel.
Format	set ipsec conn <i>connlist</i> rightsourceip <i>ipaddr</i>
Parameters	<p>conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".</p> <p>rightsourceip <i>ipaddr</i> Set the source IP address of the opposite side which communicates in the IPsec tunnel. <i>ipaddr</i> Specify the source IP address of the opposite side which communicates in the IPsec tunnel in the dot notation format (the format like xxx.xxx.xxx.xxx).</p>
Note	<ul style="list-style-type: none"> • This setting is necessary depending on the security gateway facing IPsec and the version of IKE.
Usage example	<p>The case of setting the source IP address of the opposite side which communicates in the IPsec tunnel of the connection 1 "192.168.200.1".</p> <p>set ipsec conn 1 rightsourceip 192.168.200.1</p>

set ipsec conn keyexchange**[Administrator]****Function** Set the version of the IKE protocol.**Format** **set ipsec conn *connlist* keyexchange { ike | ikev1 | ikev2 }****Parameters** **conn *connlist***

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

keyexchange { ike | ikev1 | ikev2 }

Set the version of the IKE protocol.

The default value is "ike".

ike

Specify the version of the IKE protocol as "IKEv1/IKEv2". In this case, NS-2250 responds to both IKEv1 and IKEv2. In the case of initiating a key exchange, NS-2250 initiates a key exchange using the IKEv2 protocol.

ikev1

Specify the version of the IKE protocol as "IKEv1". In this case, NS-2250 responds to only IKEv1. In the case of initiating a key exchange, NS-2250 initiates a key exchange using the IKEv1 protocol.

ikev2

Specify the version of the IKE protocol as "IKEv2". In this case, NS-2250 responds to only IKEv2. In the case of initiating a key exchange, NS-2250 initiates a key exchange using the IKEv2 protocol.

Usage example The case of specifying the version of the IKE protocol in the connection 1 as "IKEv2".**set ipsec conn 1 keyexchange ikev2**

set ipsec conn ike**[Administrator]**

Function Set the encryption algorithm of the ISAKMP-SA(Phase1).

Format **set ipsec conn connlist ike cipher-suites [strict]**

Parameters **conn connlist**

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

ike cipher-suites [strict]

Set the encryption algorithm of the ISAKMP-SA(Phase1).

cipher-suites

Specify the cipher algorithm, the authentication algorithm and the Diffie-Hellman group separately with a hyphen.

There are following cipher-suites you can specify using the NS-2250.

3des-md5-modp1024	3des-md5-modp1536	3des-md5-modp2048
3des-sha1-modp1024	3des-sha1-modp1536	3des-sha1-modp2048
aes128-md5-modp1024	aes128-md5-modp1536	aes128-md5-modp2048
aes128-sha1-modp1024	aes128-sha1-modp1536	aes128-sha1-modp2048
aes128ctr-md5-modp1024	aes128ctr-md5-modp1536	aes128ctr-md5-modp2048
aes128ctr-sha1-modp1024	aes128ctr-sha1-modp1536	aes128ctr-sha1-modp2048
aes256-md5-modp1024	aes256-md5-modp1536	aes256-md5-modp2048
aes256-sha1-modp1024	aes256-sha1-modp1536	aes256-sha1-modp2048

If you do not specify this parameter, "aes128-sha1-modp2048" and "3des-sha1-modp2048" are used in the negotiation.

[strict]

Only specified encryption parameter is used in the negotiation. If it is used except the specified one, ISAKMP-SA is not established.

Note The encryption algorithm whose cipher algorithm is "aes128ctr" can not be used in the IKEv1. Use it in the IKEv2.

Usage example Regarding the encryption algorithm of the ISAKMP-SA (Phase1) of the connection 1, in the case of setting the cipher algorithm as "AES128" the authentication algorithm as "SHA1" and the Diffie-Hellman group as "Group14(modp2048)".

set ipsec conn 1 ike aes128-sha1-modp2048

set ipsec conn esp**[Administrator]****Function** Set the encryption algorithm of the IPSEC-SA(Phase2).**Format** **set ipsec conn connlist esp cipher-suites [strict]****Parameters** **conn connlist**

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

esp cipher-suites [strict]

Set the encryption algorithm of the IPSEC-SA(Phase2).

cipher-suites

Specify the cipher algorithm and the authentication algorithm separately with a hyphen. If the PFS(Perfect Forward Secrecy) is executed, the Diffie-Hellman group is also.

There are following cipher-suites you can specify using the NS-2250.

(In the case the PFS is not executed.)

3des-md5
3des-sha1
aes128-md5
aes128-sha1
aes128ctr-md5
aes128ctr-sha1
aes256-md5
aes256-sha1

(In the case the PFS is executed.)

3des-md5-modp1024	3des-md5-modp1536	3des-md5-modp2048
3des-sha1-modp1024	3des-sha1-modp1536	3des-sha1-modp2048
aes128-md5-modp1024	aes128-md5-modp1536	aes128-md5-modp2048
aes128-sha1-modp1024	aes128-sha1-modp1536	aes128-sha1-modp2048
aes128ctr-md5-modp1024	aes128ctr-md5-modp1536	aes128ctr-md5-modp2048
aes128ctr-sha1-modp1024	aes128ctr-sha1-modp1536	aes128ctr-sha1-modp2048
aes256-md5-modp1024	aes256-md5-modp1536	aes256-md5-modp2048
aes256-sha1-modp1024	aes256-sha1-modp1536	aes256-sha1-modp2048

If you do not specify this parameter, NS-2250 operates as follows.

In the case of using IKEv1, all specifiable encryption algorithms are used in the negotiation when NS-2250 responds. When it initiates a key exchange "aes128-sha1-modp2048" and "3des-sha1-modp2048" are used.

In the case of using IKEv2, all specifiable encryption algorithms are used in the negotiation when NS-2250 responds. When it initiates a key exchange "aes128-sha1-modp 2048", "3des-sha1-modp 2048" and other specifiable encryption algorithms are used in order in the negotiation.

[strict]

Only specified encryption parameter is used in the negotiation. If it is used except the specified one, IPSEC-SA is not established.

Usage example Regarding the encryption algorithm of the IPSEC-SA(Phase2) of the connection 1, in the case of setting the cipher algorithm as "AES128" and the authentication algorithm as "SHA1" (The PFS is not executed.).**set ipsec conn 1 esp aes128-sha1**

set ipsec conn ikelifetime**[Administrator]**

Function Set the lifetime of the ISAKMP-SA.

Format **set ipsec conn** *connlist* **ikelifetime** *lifetime*

Parameters **conn** *connlist*

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

ikelifetime *lifetime*

Specify the lifetime(seconds) of the ISAKMP-SA(Phase1) in the range of 3600 to 86400.

The default value is "10800".

Usage example The case of setting the lifetime of the ISAKMP-SA of the connection 1 as 24 hours(86400 seconds).

set ipsec conn 1 ikelifetime 86400

set ipsec conn lifetime**[Administrator]**

Function Set the lifetime of the IPSEC-SA.

Format **set ipsec conn** *connlist* **lifetime** *lifetime*

Parameters **conn** *connlist*

Specify the number of a connection in the range of 1 to 8.

The range of ports that you can specify varies depending on the model.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

lifetime *lifetime*

Specify the lifetime(seconds) of the IPSEC-SA in the range of 3600 to 86400.

The default value is "3600".

Usage example The case of setting the lifetime of the IPSEC-SA of the connection 1 as 3 hours(10800 seconds).

set ipsec conn 1 lifetime 10800

set ipsec conn forceencaps**[Administrator]**

Function	Set whether to encapsulate the ESP protocol communication of the IPSEC-SA by UDP always or not.
Format	set ipsec conn <i>connlist</i> forceencaps { yes no }
Parameters	<p>conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".</p> <p>forceencaps { yes no } Set whether the ESP protocol communication of the IPSEC-SA is always encapsulated by UDP or not. The default value is "no".</p> <p>yes Always encapsulate the ESP protocol communication of the IPSEC-SA by UDP(port 4500).</p> <p>no In the Phase1 of the IPSEC-SA if it is confirmed that NAT is executed in the middle of the communication path, the encapsulating by UDP is executed.</p>
Note	In the case the version of the IKE protocol is version 2, this parameter is enabled.
Usage example	The case the ESP protocol communication of the IPSEC-SA of the connection 1 is always encapsulated by UDP.

```
set ipsec conn 1 forceencaps yes
```

set ipsec conn dpdaction**[Administrator]**

Function	Set whether to execute DPD(Dead Peer Detection) or not.
Format	set ipsec conn <i>connlist</i> dpdaction { none clear }
Parameters	<p>conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".</p> <p>dpdaction { none clear } Set whether to execute DPD(Dead Peer Detection) or not. The default value is "clear".</p> <p>none The DPD is not executed.</p> <p>clear Confirm whether SA with the opposite device is established by the regular communication using DPD. If it is judged that SA with the opposite device is not established, the information of the ISAKMP-SA and IPSEC-SA is cleared. If you set the command "set ipsec conn auto start", start a key exchange of the ISAKMP-SA(Phase1) within one minute.</p>
Usage example	The case of executing DPD of the connection 1.
	set ipsec conn 1 dpdaction clear

unset ipsec conn**[Administrator]****Function** Delete all settings of the specified connection.**Format** **unset ipsec conn** *connlist***Parameters** **conn** *connlist*

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

Usage example The case of deleting all settings of the connection 1.**unset ipsec conn 1**

unset ipsec conn leftid**[Administrator]**

Function	Delete the ID setting of the security gateway of own side.
Format	unset ipsec conn <i>connlist</i> leftid
Parameters	conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",". leftid Delete the ID setting of the security gateway of own side.
Usage example	The case of deleting the ID setting of the security gateway of own side of the connection 1. unset ipsec conn 1 leftid

unset ipsec conn left**[Administrator]**

Function	Delete the IP address of the security gateway of own side.
Format	unset ipsec conn <i>connlist</i> left
Parameters	conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",". left Delete the IP address of the security gateway of own side.
Usage example	The case of deleting the IP address of the security gateway of own side of the connection 1. unset ipsec conn 1 left

unset ipsec conn leftsubnet**[Administrator]**

Function	Delete the network address of own side which communicates under encrypted by using IPsec.
Format	unset ipsec conn <i>connlist</i> leftsubnet <i>ipaddr/mask</i>
Parameters	conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",". leftsubnet Delete the network address of own side which communicates under encrypted by using IPsec.
Usage example	The case of deleting the network address of own side which communicates under encrypted by using IPsec in the connection 1. unset ipsec conn 1 leftsubnet

unset ipsec conn leftsourceip**[Administrator]**

Function	Delete the source IP address of own side which communicates in the IPsec tunnel.
Format	unset ipsec conn <i>connlist</i> leftsourceip
Parameters	conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",". leftsourceip Delete the source IP address of own side which communicates in the IPsec tunnel.
Usage example	The case of deleting the source IP address of own side which communicates in the IPsec tunnel of the connection 1. unset ipsec conn 1 leftsourceip

unset ipsec conn rightid**[Administrator]**

Function	Delete the ID setting of the security gateway of the opposite side.
Format	unset ipsec conn <i>connlist</i> rightid
Parameters	conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",". rightid <i>ipaddr</i> Delete the ID setting of the security gateway of the opposite side.
Usage example	The case of deleting the ID setting of the security gateway of the opposite side of the connection 1. unset ipsec conn 1 rightid

unset ipsec conn right**[Administrator]****Function** Delete the IP address of the security gateway of the opposite side.**Format** **unset ipsec conn *connlist* right****Parameters** **conn** *connlist*

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

right *ipaddr*

Delete the IP address of the security gateway of the opposite side.

Usage example The case of deleting the IP address of the security gateway of the opposite side of the connection 1.**unset ipsec conn 1 right**

unset ipsec conn rightsubnet**[Administrator]**

Function	Delete the network address of the opposite side which communicates under encrypted by using IPsec.
Format	unset ipsec conn <i>connlist</i> rightsubnet
Parameters	conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",". rightsubnet Delete the network address of the opposite side which communicates under encrypted by using IPsec.
Usage example	The case of deleting the network address of the opposite side which communicates under encrypted by using IPsec in the connection 1. unset ipsec conn 1 rightsubnet

unset ipsec conn rightsourceip**[Administrator]**

Function	Delete the source IP address of the opposite side which communicates in the IPsec tunnel.
Format	unset ipsec conn <i>connlist</i> rightsourceip
Parameters	conn <i>connlist</i> Specify the number of a connection in the range of 1 to 8. You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",". rightsourcemip Delete the source IP address of the opposite side which communicates in the IPsec tunnel.
Usage example	The case of deleting the source IP address of the opposite side which communicates in the IPsec tunnel of the connection 1. unset ipsec conn 1 rightsourcemip

unset ipsec conn ike**[Administrator]**

Function Delete the encryption algorithm setting of the ISAKMP-SA(Phase1).

Format **unset ipsec conn *connlist* ike**

Parameters **conn *connlist***

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

ike

Delete the encryption algorithm setting of the ISAKMP-SA(Phase1).

Usage example The case of deleting the encryption algorithm of the ISAKMP-SA(Phase1) of the connection 1.

unset ipsec conn 1 ike

unset ipsec conn esp**[Administrator]****Function** Delete the encryption algorithm of the IPSEC-SA(Phase2).**Format** **unset ipsec conn *connlist* esp****Parameters** **conn** *connlist*

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

esp

Delete the encryption algorithm of the IPSEC-SA(Phase2).

Usage example The case of deleting the encryption algorithm of IPSEC-SA(Phase2) of the connection 1.**unset ipsec conn 1 esp**

enable ipsec conn**[Administrator]****Function** Enable the IPsec function.**Format** **enable ipsec conn** *connlist***Parameters** **conn** *connlist*

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

Note

- In the case you specify several connections at the same time, the error message is not displayed even if the IPsec function is not enabled because of the connection error. In the case you specify several connections at the same time, after that confirm using the command "show".
- Regarding the connection unset following commands, this command results in an error.
 - set ipsec conn left
 - set ipsec conn leftsubnet
 - set ipsec conn right
 - set ipsec conn rightsubnet
- If the bonding function is enabled, this command results in an error.
- If the IPsec function is enabled, the following settings result in an error.
 - set ipaddr / unset ipaddr
 - set ipsec conn / unset ipsec conn
- If the parameters set in the command "set ipsec conn left" is different from set in the command "set ipaddr", an error occurs.

Usage example The case of enabling the IPsec function of the connection 1.**enable ipsec conn 1**

disable ipsec conn**[Administrator]****Function** Disable the IPsec function.**Format** **disable ipsec conn** *connlist***Parameters** **conn** *connlist*

Specify the number of a connection in the range of 1 to 8.

You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".

Note In the case you specify several connections at the same time, the error message is not displayed even if the IPsec function is not disabled because of the connection error. In the case you specify several connections at the same time, after that confirm using the command "show".**Usage example** The case of disabling the IPsec function of the connection 1.**disable ipsec conn 1**

4.10 DNS setting command

These are objects managing the operating conditions of the NS-2250 DNS client function.
Up to two DNS servers can be register to the NS-2250.

set dns**[Administrator]**

Function	Register the DNS server used for name resolution.
Format	set dns { 1 2 } { <i>ipaddr</i> <i>ip6addr</i> }
Parameters	<p>{ 1 2 } Specify 1 or 2 for the identification number of the DNS server to register.</p> <p>{ <i>ipaddr</i> <i>ip6addr</i> } Specify the IP address of the DNS server.</p> <p><i>ipaddr</i> Specify the IPv4 address. The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).</p> <p><i>ip6addr</i> Specify the IPv6 address in x:x:x:x:x:x:x:x format. The "x" in each field of the address is represented by the hexadecimal of the 16 bit part. If there are consecutive 0 in the front of the field they can be omitted. The field composed of only 0 can also be omitted only once by specifying as "::" in the address.</p>
Note	<ul style="list-style-type: none"> • When you register a DNS server, the server program storing the port logs restarts. Therefore, the session of the Telnet/SSH client accessing the serial ports is disconnected. • 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 addresses, and not using the DNS server for name resolution of the servers (email, FTP, and syslog).
Usage example	To set the DNS server with the address 192.168.1.100 as the DNS server No. 1.
	set dns 1 192.168.1.100
Explanation	<p>(1) You can make the settings for two DNS servers.</p> <p>(2) The DNS server No. 1 is the primary server. The DNS server No. 2 is the secondary server.</p>

set dns localdomain**[Administrator]**

Function	Configure the local domain to which the NS-2250 belongs.
Format	set dns localdomain <i>domain_name</i>
Parameters	<i>domain_name</i> Specify the name of the local domain to which the NS-2250 belongs. In the local domain 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 before or after a period. The maximum number of characters that can be specified for a domain name is 64.
Note	When you set the local domain, the server program storing the port logs restarts. Therefore, the session of the Telnet/SSH client accessing the serial ports is disconnected.
Usage example	To specify "example.co.jp" as the NS-2250 local domain. set dns localdomain example.co.jp

unset dns**[Administrator]**

Function Delete the information of a registered DNS server.**Format** **unset dns { 1 | 2 }****Parameters** **{ 1 | 2 }**

Specify the identification number (1 or 2) of the DNS server whose information you want to delete.

Note When you delete the information of a DNS server, the server program storing the port logs restarts. Therefore, the session of the Telnet/SSH client accessing the serial ports is disconnected.**Usage example** To delete the information of the DNS server No. 1.**unset dns 1**

unset dns localdomain**[Administrator]**

Function	Delete the settings of the local domain to which the NS-2250 belongs.
Format	unset dns localdomain
Parameters	None
Note	When you delete the local domain settings, the server program storing the port logs restarts. Therefore, the session of the Telnet/SSH client accessing the serial ports is disconnected.
Usage example	unset dns localdomain

4.11 LAN setting commands

These are objects managing the NS-2250 physical LAN port.

set ether nego

[Administrator]

Function	Configure the auto-negotiation operation for the LAN port.
Format	<pre>set ether [{ eth1 eth2 }] nego { enable disable { full-100 full-10 half-100 half-10 } } [{ mdi mdix mdi-auto }]</pre>
Parameters	<p>[{ eth1 eth2 }] Specify the interface of the NS-2250. The default setting for this parameter is eth1.</p> <p>nego { enable disable { full-100 full-10 half-100 half-10 } } Enable or disable auto-negotiation. This parameter is enabled by default.</p> <p>enable Specify "enable" to use auto-negotiation. The speed and the full duplex/half duplex settings are configured automatically.</p> <p>disable { full-100 full-10 half-100 half-10 } Set "disable" to not use auto-negotiation. In this case, you have to specify the speed and full duplex/half duplex settings.</p> <p>full-100 Specify "full-100" to set the speed to 100 Mbps in full duplex.</p> <p>full-10 Specify "full-10" to set the speed to 10 Mbps in full duplex.</p> <p>half-100 Specify "half-100" to set the speed to 100 Mbps in half duplex.</p> <p>half-10 Specify "half-10" to set the speed to 10 Mbps in half duplex.</p> <p>[{ mdi mdix mdi-auto }] Specify the connection mode. The default of parameter is mdi-auto with the "nego enable" and mdi with the "nego disable".</p> <p>mdi Specify "mdi" to set the mdi mode.</p> <p>mdix Specify "mdix" to set the mdix mode.</p> <p>mdi-auto Specify "mdi-auto" to set the mdi-auto mode.</p>
Note	<ul style="list-style-type: none"> • The link may be down for several seconds when this command is executed. • When "nego disable" is specified, mdi - auto can not be specified.
Usage example	<p>To disable auto-negotiation for the LAN1 port and set a speed of 10 Mbps in full duplex.</p> <pre>set ether eth1 nego disable full-10</pre>

4.12 User management and authentication setting commands

Commands used to configure settings such as users and passwords with NS-2250 user management objects.

create user

[Administrator]

Function	Create a user.
Format	<pre>create user <i>username</i> group { setup verup log normal portusr } [uid <i>userid</i>] [port <i>enable_port_list</i>] [{ password encrypt <i>string</i> }]</pre>
Parameters	<p>username Specify the name of the user to create. In the user name, you can use half-width alphanumeric characters, underbars "_", and hyphens "-". The maximum number of characters is 16 (64 if you use RADIUS authentication function).</p> <p>group { setup verup log normal portusr } Specify the group of the user you want to create.</p> <p>setup Setup user group</p> <p>verup Upgrade user group</p> <p>log Port log acquisition user group</p> <p>normal Normal user group</p> <p>portusr Port user group</p> <p>[uid <i>userid</i>] Specify the ID number of the user to create. If you do not specify this parameter, user ID numbers are assigned from available user IDs in the same group, starting from the smallest number.</p> <p>[port <i>enable_port_list</i>] Specify the ports that can be used by port users in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command. This parameter is enabled only when you have specified the port user group (group portusr).</p> <p>[{ password encrypt <i>string</i> }] password Specify the password of the user to create. When the command is executed with this parameter specified, a message prompting you to enter a password is displayed. Enter a password. When you press the Enter key after entering the password, a message prompting you to confirm the password is displayed. Enter the same password again. If you do not specify this parameter and the encrypt parameter, no passwords are allocated to created users.</p>

Setting a password using this command changes the format of the commands written in the startup file to the format specified with the `encrypt` parameter. The set password becomes a character string that has been converted using a hash function.

You can check the converted password with the "show config" command.

encrypt string

Set the passwords of users to create using the character string after the conversion with the hash function.

When the command is executed with this parameter specified, no password entry or confirmation messages are displayed. This parameter is convenient to embed a startup file containing login user settings with passwords.

If you do not specify this parameter and the password parameter, no passwords are allocated to created users.

Note

- (1) The following users are registered by default in the NS-2250 without password. "root" and "portusr" users cannot be deleted.

user	uid
root	0
somebody	100
setup	198
verup	199
log	200
portusr	500

- (2) When registering a port user, if you have not configured with the "port" parameter the serial ports to which this user can access, configure them using the "set user port" command.

- (3) For users using the SSH public key authentication method, it is necessary to register the SSH public key using the "set user sshkey" command after executing this command.

- (4) To send a setup file to the NS-2250 or download it from the NS-2250 via FTP/SFTP, you must be logged in as a setup user (setup).

- (5) To send an upgrade file to the NS-2250 via FTP/SFTP, you must be logged in as an upgrade user (verup).

- (6) To acquire a port log file via FTP/SFTP, you must be logged in as a port log acquisition user (log).

- (7) User such as "adm" and "operator" are reserved in advance in the system and cannot be created.

- (8) The number of users that can be created in the NS-2250 is as follows.

Normal users:

Up to 91 users can be registered with IDs from 100 to 190.

Port users:

Up to 99 users can be registered with IDs from 501 to 599.

For details on user privileges of each user category, see Appendix B, "User privileges" in the Instruction Manual.

Usage example To create a normal user named "user1" with the ID "101" and a password.

create user user1 group normal uid 101 password

New password : Password entry (not displayed)

Retype new password : Password entry (not displayed)

set user password**[Administrator]****Function** Change the user password for login.**Format** **set user** *username* { **password** | **encrypt** *string* }**Parameters** *username*

Specify the name of the user whose password you want to change.

In the user name, you can use half-width alphanumeric characters, underbars "_", and hyphens "-".

The maximum number of characters is 16.

{ **password** | **encrypt** *string* }

Specify the password setting method.

password

When the command is executed with the "password" parameter specified, a message prompting you to enter a new password is displayed. Enter a password. When you press the Enter key after entering the password, a message prompting you to confirm the password is displayed. Enter the same password again.

encrypt *string*

When the command is executed with the "encrypt" parameter specified, the subsequent character string is handled as the password string converted using a hash function. Set the password as this converted character string.

Changing a password using this command changes the format of the commands written in the startup file to the format specified with the encrypt parameter used with the "create user" command. The changed password becomes a character string that has been converted using a hash function.

You can check the converted password with the "show config" command.

Usage example To change the password of user1**set user user1 password****Changing password for user user1****New password : Password entry (not displayed)****Retype new password : Password entry (not displayed)****Password for user1 changed****Explanation** To delete the password, execute the "set user password" command and press the Enter key twice.

set user port**[Administrator]**

Function Configure the port users access privileges for the serial ports.

Format **set user** *username* **port** *enable_port_list*

Parameters *username*

Specify the name of the port user who will access the serial ports.

In the user name, you can use half-width alphanumeric characters, underbars "_", and hyphens "-".

The maximum number of characters is 16.

enable_port_list

Specify the ports that can be used in the 1 to 48 range. The range of ports that you can specify varies depending on the model.

You can specify multiple serial ports by separating their numbers with commas ", ".

You can also specify a range of ports using an hyphen "-" between two numbers.

Usage example To authorize port user "user1" to access the ports 1, 2, 3, 16, and 32.

set user user1 port 1-3,16,32

Explanation

- (1) Users cannot access serial ports for which they do not have access privileges.
- (2) Only users registered as port users can be specified with this command.

set user sshkey**[Administrator]**

Function	Configure the public key for user SSH authentication.
Format	set user <i>username</i> sshkey [public] <i>method</i> <i>public-key</i> [<i>comment</i>]
Parameters	<p><i>username</i></p> <p>Specify the name of the user who will use SSH.</p> <p>In the user name, you can use half-width alphanumeric characters, underbars "_", and hyphens "-".</p> <p>The maximum number of characters is 16.</p> <p>sshkey [public] <i>method</i> <i>public-key</i> [<i>comment</i>]</p> <p>Specify the public key for SSH authentication using the character strings string. The SSH authentication public key (string1string2string3) is created on the client machine.</p> <p><i>method</i></p> <p>Specify the encryption method for the SSH authentication public key.</p> <p>ssh-rsa</p> <p>RSA encryption</p> <p>ssh-dss</p> <p>DSA encryption</p> <p>ecdsa-sha2-nistp128</p> <p>ECDSA encryption 128bit</p> <p>ecdsa-sha2-nistp256</p> <p>ECDSA encryption 256bit</p> <p>ecdsa-sha2-nistp521</p> <p>ECDSA encryption 521bit</p> <p><i>public-key</i></p> <p>Specify the public key for SSH authentication.</p> <p>[<i>comment</i>]</p> <p>Specify a comment for the SSH authentication public key.</p>
Usage example	<p>To set a SSH authentication public key for user "user1" using RSA encryption method.</p> <pre>set user user1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAyHYtUWDRB OxfBx8Nk0PAPcOO9z07Rurqijd8CUXx6dp7w2tFanDnRdY KGkQkchZMUWkAKYl+bI9jDbePBzaK9xR0wxlv0mQ1bP6A PVAP3vqdkRxz6YFNi6pszEEdWskKe7RXmz0S+MP4Mjpvx TkWzK8FyJJy1htLTVv/sBTaudc=</pre> <p>(Line breaks should not be included in the actual command.)</p>
Explanation	<p>(1) The RSA and DSA encryption methods of the version 2 of the SSH protocol can be used for the public key.</p> <p>(2) If you set a SSH authentication public key using this command, it is necessary to send the public key created on the client machine to the NS-2250 device management user in advance.</p> <p>(3) The SSH authentication public key must be registered using this command to port users and users who log in to the NS-2250 from a SSH or SFTP client.</p> <p>(4) Only users registered as NS-2250 users can be specified with this command.</p> <p>(5) The maximum key length is 2048 bits with the RSA method and 1024 bits with the DSA method and 521 bits with the ECDSA .</p>

Note

- (1) Always add a comment to the public key.
- (2) Half-width and full-width space characters cannot be used in the public key strings.

unset user sshkey**[Administrator]**

Function Delete user settings for SSH authentication public key.**Format** **unset user** *username* **sshkey** [**public**]**Parameters** *username*

Specify the name of the user whose public key settings you want to delete.

In the user name, you can use half-width alphanumeric characters, underbars "_", and hyphens "-".

The maximum number of characters is 16.

sshkey [**public**]

Specify "public" to delete the public key settings.

Usage example To delete the settings for SSH authentication public key of user "user1".**unset user user1 sshkey**

delete user**[Administrator]****Function** Delete a user.**Format** **delete user** *username***Parameters** *username*

Specify the name of the user to delete.

In the user name, you can use half-width alphanumeric characters, underbars "_", and hyphens "-".

The maximum number of characters is 16.

Note The device management user (root) and port user (portusr) cannot be deleted.**Usage example** To delete the user "user1"**delete user user1**

4.13 SNMP agent setting commands

These are objects managing the operating conditions of the NS-2250 SNMP agent function.

set snmp location

[Administrator]

Function Set sysLocation (system location).

Format **set snmp location** "*location*"

Parameters **location** "*location*"

Specify the location of the system within double quotation marks. You can use alphanumeric and space characters. The maximum number of characters is 128.

Note he SNMP agent restarts if it is enabled when you make this setting.

Usage example To specify "Server Room in TOKYO" for sysLocation.

set snmp location "Server Room in TOKYO"

set snmp contact**[Administrator]****Function** Set sysContact (contact information).**Format** **set snmp contact "syscontact"****Parameters** **contact "syscontact"**

Specify information such as the name, position, and phone number of the NS-2250 administrator within double quotation marks. You can use alphanumeric and space characters. The maximum number of characters is 128.

Note The SNMP agent restarts if it is enabled when you make this setting.**Usage example** To specify "Administrator 03-1234-7777" for sysContact.**set snmp contact "Administrator 03-1234-7777"**

set snmp authentrap**[Administrator]**

Function	<p>Set whether or not to send a trap when SNMP authentication failed.</p> <p>SNMP authentication failure traps are sent if one of the following cases occurs.</p> <ul style="list-style-type: none">• The community name of the SNMP request packet does not match the setting.• The community name of the SNMP request packet matches the settings, but not the IP address of the manager.
Format	set snmp authentrap { on off }
Parameters	<p>authentrap { on off }</p> <p>Specify whether or not to send a trap when SNMP authentication failed. This parameter is "on" by default.</p> <p>on</p> <p>Set "on" to send SNMP authentication failure traps.</p> <p>off</p> <p>Set "off" not to send SNMP authentication failure traps.</p>
Note	<ul style="list-style-type: none">• These traps are not sent if the SNMP agent is disabled.• The SNMP agent restarts if it is enabled when you make this setting.
Usage example	<p>To send SNMP authentication failure traps.</p> <p>set snmp authentrap on</p>

set snmp linktrap**[Administrator]**

Function	Set whether or not to send link traps. Send the link up trap when a link is detected on a LAN port, and send the link down trap when the link is not detected anymore.
Format	set snmp linktrap { on off }
Parameters	linktrap { on off } Specify whether or not to send link traps. This parameter is "on" by default. on Set "on" to send link traps. off Set "off" not to send link traps.
Note	The SNMP agent restarts if it is enabled when you make this setting.
Usage example	To send link up and down traps. set snmp linktrap on
Explanation	(1) These traps are not sent if the SNMP agent is disabled. (2) link down trap are not sent if the only one LAN port is used.

set snmp dsrtrap**[Administrator]**

Function	Set whether or not to send DSR traps. Send the "nsRs232DsrUp" trap when a DSR signal is detected on a serial port, and send the "nsRs232DsrDown" trap when the DSR signal is not detected anymore.
Format	set snmp tty <i>ttylist</i> dsrtrap { on off }
Parameters	tty <i>ttylist</i> Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command. dsrtrap { on off } Specify whether or not to send DSR traps. This parameter is "off" by default. on Set "on" to send DSR traps. off Set "off" not to send DSR traps.
Note	The SNMP agent restarts if it is enabled when you make this setting.
Usage example	To send DSR traps with the serial port 1. set snmp tty 1 dsrtrap on
Explanation	These traps are not sent if the SNMP agent is disabled.

set snmp coldstarttrap**[Administrator]**

Function	Set whether or not to send cold start traps. Send a cold start trap when starting the NS-2250.
Format	set snmp coldstarttrap { on off }
Parameters	coldstarttrap { on off } Specify whether or not to send cold start traps. This parameter is "on" by default. on Set "on" to send cold start traps. off Set "off" not to send cold start traps.
Note	The SNMP agent restarts if it is enabled when you make this setting.
Usage example	To send cold start traps. set snmp coldstarttrap on
Explanation	(1) These traps are not sent if the SNMP agent is disabled. (2) A cold start trap is sent when the SNMP agent, which must be enabled, starts after the NS-2250 has been powered on.

set snmp powertrap**[Administrator]**

Function	Set whether or not to send power traps. Send the "PowerSupplyUp" trap when a power is detected on a power supply, and send the "PowerSupplyDown" trap when the power is not detected anymore.
Format	set snmp powertrap { on off }
Parameters	powertrap { on off } Specify whether or not to send power traps. This parameter is "on" by default. on Set "on" to send power traps. off Set "off" not to send power traps.
Note	The SNMP agent restarts if it is enabled when you make this setting.
Usage example	To send power traps. set snmp powertrap on
Explanation	(1) These traps are not sent if the SNMP agent is disabled. (2) A power trap is sent when the SNMP agent, which must be enabled, starts after the NS-2250 has been powered on.

set snmp bondingactswtrap**[Administrator]**

Function	Set whether or not to send the active port switched traps. When detecting the switching of the active port in bonding function, send the active port switched trap(nsBondingActiveSwitch trap).
Format	set snmp bondingactswtrap { on off }
Parameters	bondingactswtrap { on off } Specify whether or not to send bonding active switch traps when active slave interface switched. This parameter is "on" by default. on Set "on" to send the active port switched traps. off Set "off" not to send the active port switched traps.
Usage example	To send the active port switched traps when detecting the switching of the active port in bonding function. set snmp bondingactswtrap off
Explanation	(1) These traps are not sent if the SNMP agent is disabled. (2) The SNMP agent restarts if it is enabled when you make this setting.

unset snmp location**[Administrator]**

Function	Remove sysLocation settings.
Format	unset snmp location
Parameters	None
Note	The SNMP agent restarts if it is enabled when you make this setting.
Usage example	unset snmp location

unset snmp contact**[Administrator]**

Function	Remove sysContact settings.
Format	unset snmp contact
Parameters	None
Note	The SNMP agent restarts if it is enabled when you make this setting.
Usage example	unset snmp contact

enable snmp**[Administrator]**

Function	Enable the SNMP agent function.
Format	enable snmp
Parameters	None
Usage example	enable snmp
Explanation	The SNMP agent function is disabled by default.

disable snmp**[Administrator]****Function** Disable the SNMP agent function.**Format** **disable snmp****Parameters** None**Usage example** **disable snmp**

4.14 SNMP trap setting commands

These are objects managing the notification destinations of the SNMP trap function of the NS-2250.

set trap manager

[Administrator]

Function	Set the address of the SNMP server to send the traps to and the community name used when sending the traps.
Format	set trap { 1 2 3 4 } manager { <i>ipaddr</i> <i>hostname</i> } [<i>name</i> <i>community_name</i>] [version { <i>v1</i> <i>v2</i> }]
Parameters	{ 1 2 3 4 } Specify the number from 1 through 4 of the trap destination. manager { <i>ipaddr</i> <i>hostname</i> } Specify the IP address or the host name of the destination SNMP server. <i>ipaddr</i> The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx). <i>hostname</i> 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 before or after a period. The maximum number of characters that can be set for a host name is 64. [<i>name</i> <i>community_name</i>] Specify the community name used when sending the traps. In the community name, you can use half-width alphanumeric characters, underbars "_", hyphens "-", pluses "+", commas ",", at marks "@", periods ".", carets "^", and tildes "~". The maximum number of characters that can be set for a community name is 64. The community name "public" is set if this parameter is omitted. [version { <i>v1</i> <i>v2</i> }] Specify the format (version 1 or version 2) of the traps. The parameter is set to the default value "v1" if omitted. v1 Set "v1" to send traps in the SNMP version 1 format. v2 Set "v2" to send traps in the SNMP version 2 format.
Usage example	To set the IP address 192.168.0.50 to the trap destination 1 and "public1" as the community name.

set trap 1 manager 192.168.0.50 name public1

unset trap manager**[Administrator]****Function** Remove the settings of the destination SNMP server.**Format** **unset trap { 1 | 2 | 3 | 4 } manager****Parameters** **{ 1 | 2 | 3 | 4 }**
Specify the number from 1 through 4 of the trap destination whose settings you want to remove.**Usage example** To remove the settings of trap destination 1.**unset trap 1 manager**

4.15 SNMP community setting commands

These are objects managing the community of the NS-2250 SNMP agent function.

You can create up to four of these objects within the NS-2250. They will be identified using the community numbers set by the user.

set community

[Administrator]

Function	Set the community name and SNMP server that can use it to access the NS-2250.
Format	set community { 1 2 3 4 } name <i>community_name</i> [view { ro rw }] [manager { <i>ipaddr</i> <i>hostname</i> }]
Parameters	{ 1 2 3 4 } Specify the number from 1 through 4 of the community to set. <i>name community_name</i> Specify the name of the community. In the community name, you can use half-width alphanumeric characters, underbars "_", hyphens "-", pluses "+", commas ",", at marks "@", periods ".", carets "^", and tildes "~". The maximum number of characters that can be set for a community name is 20. [view { ro rw }] Specify "ro" in "view" to authorize read only. Specify "rw" in "view" to authorize both read and write. [manager { <i>ipaddr</i> <i>hostname</i> }] Specify the IP address or the host name of the SNMP server that can access the NS-2250 with this community name. The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx). 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 before or after a period. The maximum number of characters that can be set for a host name is 64. If this parameter is omitted, the NS-2250 will be accessible from any SNMP server.
Note	The SNMP agent restarts if it is enabled when you execute this command.
Usage example	To set "public" as the name of community 1 and authorize access from the SNMP server 192.168.0.50. <pre>set community 1 name public manager 192.168.0.50</pre>
Explanation	(1) You can specify only one SNMP server for one community object. To specify multiple SNMP servers to the same community name, create a community object for each SNMP server. (2) SNMP version 1 and version 2c "Get" requests are supported when the SNMP agent is enabled. When the agent receives a "Get" request in the version 1 format from an SNMP server, it responds using version 1, and when it receives a "Get" request in the version 2c format, it responds using version 2c.

unset community**[Administrator]**

Function Remove the settings of the community name and SNMP server that can use it to access the NS-2250.

Format **unset community { 1 | 2 | 3 | 4 } name**

Parameters **{ 1 | 2 | 3 | 4 }**
Specify the number from 1 through 4 of the community whose settings you want to remove.

Note The SNMP agent restarts if it is enabled when you execute this command.

Usage example To remove the name of community 1 and the settings of the corresponding SNMP server.

unset community 1 name

4.16 Syslog setting commands

Commands used to transfer syslog messages from the NS-2250 to external syslog servers.

set syslog host

[Administrator]

Function	Set the facility and syslog server where to send the syslog messages.
Format	<pre>set syslog host { 1 2 } { ipaddr host } [portlog_facility { local0 local1 local2 local3 local4 local5 local6 local7 }] [syslog_facility { local0 local1 local2 local3 local4 local5 local6 local7 }]</pre>
Parameters	<p>{ 1 2 } Specify 1 or 2 for the identification number of the syslog server you want to register.</p> <p>{ ipaddr host }</p> <p><i>ipaddr</i> Specify the IP address of the syslog server. The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).</p> <p><i>host</i> Specify the host name of the syslog server. 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 before or after a period. The maximum number of characters that can be set for a host name is 64.</p> <p>portlog_facility { local0 local1 local2 local3 local4 local5 local6 local7 } Specify the facility of the port log to send to the syslog server. The current settings are applied if this parameter is omitted. This parameter is set to "local0" by default.</p> <p>syslog_facility { local0 local1 local2 local3 local4 local5 local6 local7 } Specify the facility of syslog messages to send to the syslog server. The current settings are applied if this parameter is omitted. This parameter is set to "local1" by default.</p>
Note	It is necessary to set the target serial ports with the "set logd tty syslog" command to transfer port logs to a syslog server.
Usage example	<p>To register the syslog server 192.168.1.105 with the identification No. 1, set the port log facility to "local0", and set syslog messages facility to "local1".</p> <pre>set syslog host 1 192.168.1.105 portlog_facility local0 syslog_facility local1</pre>
Explanation	You can make the settings for two syslog servers.

unset syslog host**[Administrator]**

Function	Remove the settings of the syslog server where to send the syslog messages.
Format	unset syslog host { 1 2 }
Parameters	{ 1 2 } Specify the identification number (1 or 2) of the syslog server whose settings you want to remove.
Usage example	To remove the settings of syslog server No. 1. unset syslog host 1

enable syslog**[Administrator]**

Function	Enable the syslog client.
Format	enable syslog
Parameters	None
Usage example	enable syslog
Explanation	The syslog client function is disabled by default.

disable syslog**[Administrator]**

Function	Disable the syslog client.
Format	disable syslog
Parameters	None
Usage example	disable syslog

4.17 NFS setting commands

These are objects managing the operating conditions of the NFS client function.

set nfs server addr

[Administrator]

Function Set the NFS server where to save the port logs.

Format **set nfs server { 1 | 2 } addr ipaddr path path-dir**

Parameters **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the NFS server to register.

addr ipaddr

Specify the IP address of the NFS server.

The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).

path path-dir

Specify the path of the NFS server where to save the port logs.

In the path name, you can use half-width alphanumeric characters, slashes "/", hyphens "-", underbars "_", periods ".", and commas ",".

The maximum number of characters that can be set for the path name is 128.

Usage example To set the address "192.168.1.105" and the path "/mnt/nfslog" for the NFS server 1.

set nfs server 1 addr 192.168.1.105 path /mnt/nfslog

Explanation (1) The NS-2250 supports NFS version 3.

(2) To save port logs to an NFS server, make NFS settings for the target serial ports with the "set logd tty nfs" command.

(3) The settings cannot be made when the NFS client function is enabled.

set nfs server proto**[Administrator]**

Function Set the NFS protocol.

Format **set nfs server { 1 | 2 } proto { tcp | udp }**

Parameters **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the NFS server to register.

proto { tcp | udp }

Specify the NFS protocol.

This parameter is set to "udp" by default.

tcp

Communicate with the NFS server using TCP.

udp

Communicate with the NFS server using UDP.

Usage example To communicate using TCP with the NFS server No 1.

set nfs server 1 proto tcp

Explanation (1) The NS-2250 supports NFS version 3.

(2) To save port logs to an NFS server, make NFS settings for the target serial ports with the "set logd tty nfs" command.

(3) The settings cannot be made when the NFS client function is enabled.

set nfs rotate**[Administrator]**

Function Set the rotation interval of the port logs.

Format **set nfs rotate { off | on minite hour day month day_of_week }**

Parameters Set the port log rotation on or off.

off

Port logs are not rotated.

on minite hour day month day_of_week

Port logs are rotated.

*minite***0-59**

Operate at the specified minutes.

You can specify a list of minutes using hyphens "-" and commas ",".

*hour***0-23**

Operate at the specified hours.

You can specify a list of hours using hyphens "-" and commas ",".

Operate every hour.

*day***1-31**

Operate at the specified days.

You can specify a list of days using hyphens "-" and commas ",".

Operate every day.

*month***1-12**

Operate at the specified months.

You can specify a list of months using hyphens "-" and commas ",".

Operate every month.

*day_of_week***0-7**

Operate at the specified days of the week. Sunday is 0 or 7, Monday is 1, Tuesday is 2, Wednesday is 3, Thursday is 4, Friday is 5, and Saturday is 6.

You can specify a list of days using hyphens "-" and commas ",".

Operate every day of the week.

Usage example To set the port logs to be rotated the first of every month at 00:00.

```
set nfs rotate on 0 0 1 * *
```

Explanation (1) The "or" condition is applied is both the days and the days of the week are specified. If one of these parameter is set to "*", rotation operates following the parameter for which a numeric value is registered.
(2) The settings cannot be made when the NFS client function is enabled.

unset nfs server addr**[Administrator]**

Function Remove the NFS server settings.**Format** **unset nfs server { 1 | 2 } addr****Parameters** **{ 1 | 2 }**

Specify identification number (1 or 2) of the NFS server whose settings you want to remove.

Usage example To remove the settings of the NFS server No. 1.**unset nfs server 1 addr****Explanation** (1) The settings cannot be made when the NFS client function is enabled.

enable nfs**[Administrator]**

Function	Enable the NFS client function.
Format	enable nfs
Parameters	None
Usage example	enable nfs
Explanation	The NFS client function is disabled by default.

disable nfs**[Administrator]****Function** Disable the NFS client function.**Format** **disable nfs****Parameters** None**Usage example** **disable nfs**

4.18 SNTP setting commands

These are objects managing the operating conditions of the NS-2250 SNTP client function.

set sntp server

[Administrator]

Function Set NTP servers to which you want to synchronize.

Format **set sntp server { *ipaddr* | *host* }**

Parameters { *ipaddr* | *host* }

Specify the IP address or the host name of the NTP server to which you want to send time requests.

ipaddr

The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).

host

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 before or after a period.

The maximum number of characters that can be set for a host name is 64.

Usage example To set the NTP servers 192.168.1.106 and 10.1.1.1.

```
set sntp server 192.168.1.106
```

```
set sntp server 10.1.1.1
```

Explanation

- (1) You can register up to two NTP servers.
- (2) The primary and secondary NTP servers are set following the registration order. The NTP server you registered first is the primary server, and the server you registered next is the secondary server.
- (3) The settings cannot be made when the SNTP client function is enabled.

set sntp polltime**[Administrator]****Function** Set polling interval to the NTP servers.**Format** **set sntp polltime** *time***Parameters** *time*

Set polling interval to the NTP servers.

The setting range for the polling interval is from 60 through 1800 seconds.

The unit is one second.

This parameter is set to "600" by default.

Usage example To set the polling interval to the NTP server to 300 seconds.**set sntp polltime 300****Explanation** (1) The settings cannot be made when the SNTP client function is enabled.

(2) The NS-2250 time is synchronized to the time from the NTP server response.

unset sntp server**[Administrator]**

Function Remove settings of NTP servers.

Format **unset sntp server** [{ *ipaddr* | *host* }]

Parameters [{ *ipaddr* | *host* }]

The setting of the NTP server corresponding to the IP address or host name (*ipaddr*/*host*) specified with this command is deleted.

If no IP address or host name is specified, the settings of both NTP servers are deleted.

ipaddr

Specify the IP address of the NTP server used.

The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).

host

Specify the host name of the NTP server used.

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 before or after a period.

The maximum number of characters that can be set for a host name is 64.

Usage example **unset sntp server**

Explanation (1) The settings cannot be removed when the SNTP client function is enabled.

(2) If you delete the setting of the primary NTP server (registered first), the secondary NTP server (registered next) automatically becomes the primary server.

enable sntp**[Administrator]**

Function	Enable the SNTP client function.
Format	enable sntp
Parameters	None
Usage example	enable sntp
Explanation	The SNTP client function is disabled by default.

disable sntp**[Administrator]****Function** Disable the SNTP client function.**Format** **disable sntp****Parameters** None**Usage example** **disable sntp**

4.19 TTY setting commands

These are objects managing the serial ports.

The tty No. 1 corresponds to serial port No. 1, the tty 2 to serial port 2, and so on.

The following operations can be carried out for these objects.

set tty baud

[Administrator]

Function Set the operation conditions and operation of the serial ports.

Format **set tty *tylist* baud { 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200 }**

Parameters **tty *tylist***

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

baud { 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200 }

Set the transmission rate.

This parameter is set to "9600" by default.

Usage example To set a transmission rate of 19200 bps for serial ports 1 to 32.

set tty 1-32 baud 19200

set tty bitchar**[Administrator]****Function** Set the data bit length.**Format** **set tty *ttylist* bitchar { 7 | 8 }****Parameters** **tty *ttylist***

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

bitchar { 7 | 8 }

Set the data bit length.

This parameter is set to "8" by default.

7

7-bit

8

8-bit

Set this parameter to "8" when transferring 8-bit code (binary or characters).

Usage example Set the data bit length to 7 for serial port 1.**set tty 1 bitchar 7**

set tty parity**[Administrator]****Function** Set the parity.**Format** **set tty *tylist* parity { even | odd | none }****Parameters** **tty *tylist***

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

parity { even | odd | none }

Set the parity.

This parameter is set to "none" by default.

even

Even parity

odd

Odd parity

none

No parity

Usage example Set parity to odd parity for serial port 1.**set tty 1 parity odd**

set tty stop**[Administrator]****Function** Set the stop bit length.**Format** **set tty *ttylist* stop { 1 | 2 }****Parameters** **tty** *ttylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

stop { 1 | 2 }

Set the stop bit length. The stop bit length applies to the data signal output from the NS-2250. The stop bit is always 1 bit for data signals received by the NS-2250.

This parameter is set to "1" by default.

1

1-bit

2

2-bit

Usage example Set the stop bit length to 2 for serial port 1.**set tty 1 stop 2**

set tty flow**[Administrator]****Function** Set the flow control.**Format** **set tty *tylist* flow { xon | rs | none }****Parameters** **tty *tylist***

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

flow { xon | rs | none }

Set the flow control.

This parameter is set to "none" by default.

xon

Control uses xon and xoff codes.

rs

Control the flow using RTS/CTS signals

none

Flow control is not used in both the transmitting and receiving directions.

Note

- Do not use xon when bidirectionally transferring 8-bit code (binary, kanji etc.).

Usage example Set flow control using RTS / CTS signal line for serial port 1.**set tty 1 flow rs**

set tty detect_dsr**[Administrator]**

Function	Set the DSR signal transition detection function.
Format	set tty <i>tylist</i> detect_dsr { on [{ edge polling }] off }
Parameters	<p>tty <i>tylist</i> Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>detect_dsr { on [{ edge polling }] off } This parameter is "off" by default.</p> <p>on [{ edge polling }] Enables the DSR signal transition detection function. When change is detected in the DSR signal status (OFF-¿ON or ON-¿OFF), it is displayed and exported as console and syslog messages. Use it in combination with the "set snmp tty dsrtrap on" command to send serial DSR signal traps to the SNMP server.</p> <p>{ edge polling } This parameter is "edge" by default.</p> <p>edge DSR signal status is detected strictly.</p> <p>polling DSR signal status is detected gently. When a change in a DSR signal continued for more than 10 msec, it's detected.</p> <p>off Disables the DSR signal transition detection function. DSR signal transitions are not detected even if they occur on the set port. If set to off, status transition messages are not exported to the console and syslog servers, serial DSR signal traps are not sent.</p>
Note	<ul style="list-style-type: none"> • In the following cases, an answer is obtained about the DSR signal status regardless of the settings made with this command. • When the DSR signal status is obtained with the "show stats tty" command When the DSR signal status is obtained via SNMP MIB access ("nsRs232PortDsrState" object in NS-RS232-MIB)
Usage example	To disable the DSR signal transition detection function for serial ports 1 to 32. set tty 1-32 detect_dsr off

4.20 logd setting commands

These are objects managing port log operation and sending methods.

add logd tty mail

[Administrator]

Function	Register a destination email address and email server to send the port logs.
Format	add logd tty <i>ttylist</i> mail { 1 2 } Mail-Address { <i>ipaddr</i> <i>host</i> }
Parameters	<p><i>ttylist</i></p> <p>Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>mail { 1 2 }</p> <p>Specify 1 or 2 for the identification number of the email server to register.</p> <p><i>Mail-Address</i></p> <p>Specify the destination email address.</p> <p>{ <i>ipaddr</i> <i>host</i> }</p> <p><i>ipaddr</i></p> <p>Specify the IP address of the email server. The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).</p> <p><i>host</i></p> <p>Specify the host name of the email server. 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 before or after a period. The maximum number of characters that can be set for a host name is 64. In environments in which port log transfers are frequent, we recommend specifying and configuring the IP address, and not using the DNS server for name resolution of the email server.</p>
Usage example	To send the port logs of serial port 1 to the "portlog_mgr@example.co.jp" email address via the email server 192.168.1.1.
	add logd tty 1 mail 1 portlog_mgr@example.co.jp 192.168.1.1
Explanation	A maximum of two email servers and destination email addresses can be registered for a single serial port.

add logd tty ftp**[Administrator]****Function** Register a destination FTP server for port logs.**Format** **add logd tty** *ttylist* **ftp** { **1** | **2** } *FTP-Account* { *ipaddr* | *host* }
[{ **password** | **encrypt** *string* }]**Parameters** *ttylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

ftp { **1** | **2** }

Specify 1 or 2 for the identification number of the FTP server to register.

FTP-Account

Set the FTP account.

{ *ipaddr* | *host* }*ipaddr*

Specify the IP address of the FTP server.

The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).

host

Specify the host name of the FTP server.

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 before or after a period.

The maximum number of characters that can be set for a host name is 64.

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

[{ **password** | **encrypt** *string* }]**password**

Set the account password.

When the command is executed with this parameter specified, a message prompting you to enter a password is displayed. Enter a password.

When you press the Enter key after entering the password, a message prompting you to confirm the password is displayed. Enter the same password again.

If you do not specify this parameter and the encrypt parameter, no passwords are allocated to created users.

Setting a password using this command changes the format of the commands written in the startup file to the format specified with the encrypt parameter. The set password becomes an encrypted character string.

encrypt *string*

Set the account password as an encrypted character string.

When the command is executed with this parameter specified, no password entry or confirmation messages are displayed. This parameter is convenient to embed a startup file containing settings of FTP accounts with passwords.

Usage example To send the port logs of serial ports 1 to 32 with the "portlog_mgr" account to the FTP server 192.168.1.1.

```
add logd tty 1-32 ftp 1 portlog_mgr 192.168.1.1
FTP password Password entry (not displayed)
Retype FTP password Password entry (not displayed)
```

Explanation A maximum of two FTP servers and FTP accounts can be registered for a single serial port.

set logd output**[Administrator]**

Function Set the port log save destination.

Format **set logd output { flash | ram | off | cf }**

Parameters **{ flash | ram | off | cf }**

Set the port log save destination.

This parameter is set to "ram" by default.

flash

Set FLASH memory for the port log save destination.

ram

Set the RAM for the port log save destination.

off

Do not save port logs.

cf

This parameter is alias of flash.

Usage example To save the ports logs to an FLASH memory.

set logd output flash

Note

(1) When the port log save destination is changed from RAM to FLASH memory, the port logs saved in the RAM are not copied to the FLASH memory. The port log save space is also set to 3MBytes.

(2) When the port log save destination is changed from FLASH memory to RAM, the port logs saved in the FLASH memory are not copied to the RAM. The port log save space is also set to the default value of 500KBytes.

(3) When log saving is set to on (set logd tty log on) in the serial port settings, the logs are not saved anymore for all serial ports if the "set logd output off" command is executed.

(4) When log saving is set to off (set logd tty log off) in the serial port settings, log saving is enabled for all serial ports if the "set logd output ram" or the "set logd output flash" command is executed.

set logd tstamp**[Administrator]****Function** Set port log time stamps.**Format** **set logd tstamp { on [interval *interval_time*] | off }****Parameters** **{ on [interval *interval_time*] | off }**

Set the time stamps on or off for all serial ports.

This parameter is "off" by default.

on [interval *interval_time*]

When set to "on", specify the time stamp interval in seconds for all serial ports .

The setting range is from 3 through 65535 seconds.

This parameter is set to "60" by default.

If no data is received for a time longer than the interval, the time stamp is added at the time the next data is received data and this time is set as the start of the timing interval.

off

Disable the time stamp function.

Usage example To set an interval of 30 seconds for the time stamp of port logs.**set logd tstamp on interval 30****Explanation** If this function is enabled, the free space to save port logs is reduced by the amount of data of the added time stamps. Note also that the actual time stamp interval may differ slightly from the set value.

set logd tty log**[Administrator]****Function** Set the port log save space for each serial port.**Format** **set logd tty *ttylist* log { on [size *log_size*] | off }****Parameters** *ttylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

log { on [size *log_size*] | off }

This parameter is "on" by default.

on [size *log_size*]

Save the log to the port logs.

Specify the log size of each port within the following range. The unit is KByte.

- In the RAM : 100 to 2000 KBytes
- In FLASH memory : 100 to 8000 KBytes The limits for the total log size that can be specified are as follows.
- In the RAM : 24000Kbyte
- In FLASH memory : 144000KByte The default values for this parameter are as follows.
- In the RAM : 500KByte
- In FLASH memory : 3000KByte

off

Do not save the log to the port logs.

Usage example To set 512 KBytes for the port log save space of serial ports 1 to 8.**set logd tty 1-8 log on size 512**

set logd tty lstamp**[Administrator]**

Function Set the login stamp function for port logs.

Format **set logd tty *ttylist* lstamp { off | on }**

Parameters *ttylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

lstamp { off | on }

This parameter is "off" by default.

off

Disable the login stamp function.

on

Enable the login stamp function.

Usage example To add a login stamp in the port log of serial ports 1 to 8.

set logd tty 1-8 lstamp on

Explanation (1) When this function is enabled, a login stamp containing the port user name, the login or logout information, and the login/logout time is added to the port log when a port user starts or ends access to a serial port. Note that the free space to save port logs is reduced by the amount of data of the added login stamps.

set logd tty syslog**[Administrator]**

Function	Set whether to send port logs to a syslog server.
Format	set logd tty <i>ttylist</i> syslog { off on format { hostname { off on } label { off on } tstamp { off on } } }
Parameters	<p><i>ttylist</i></p> <p>Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model.</p> <p>Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>syslog { off on format { hostname { off on } label { off on } tstamp { off on } } }</p> <p>This parameter is "off" by default.</p> <p>off</p> <p>Do not send port logs to the syslog server.</p> <p>on</p> <p>Send port logs to the syslog server.</p> <p>format { hostname { off on } label { off on } tstamp { off on } }</p> <p>Change the format of the port logs and sent them to the syslog server. You can also combine multiple parameters when configuring this setting to on.</p> <p>hostname { off on }</p> <p>This parameter is "off" by default.</p> <p>off</p> <p>Do not add the NS-2250 host name to the port logs.</p> <p>on</p> <p>Add the NS-2250 host name to the port logs.</p> <p>label { off on }</p> <p>This parameter is "off" by default.</p> <p>off</p> <p>Do not change <i>TTY No.</i> in the port logs to <i>label name</i>.</p> <p>on</p> <p>Change <i>TTY No.</i> in the port logs to <i>label name</i>. Label names are enclosed in " ". If no label name is set, <i>TTY No.</i> is used as when this parameter is set to off.</p> <p>tstamp { off on }</p> <p>This parameter is "off" by default.</p> <p>off</p> <p>Do not add the NS-2250 time stamp to the port logs.</p> <p>on</p> <p>Add the NS-2250 time stamp to the port logs. Time stamps show the following information: month, day, time. Example: Jan 22 10:45:35</p>

Usage example To send the port logs of serial ports 1 to 32 to the syslog server.

set logd tty 1-32 syslog on

set logd tty nfs**[Administrator]**

Function Set whether to save port logs to a NFS server.

Format **set logd tty *ttylist* nfs { off | on }**

Parameters *ttylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

syslog { off | on }

This parameter is "off" by default.

off

Do not save port logs to the NFS server.

on

Save port logs to the NFS server.

Usage example To save the port logs of serial ports 1 to 32 to the NFS server.

set logd tty 1-32 nfs on

set logd tty sendlog**[Administrator]**

Function	Set the conditions to send the port logs to an email or an FTP server.
Format	set logd tty <i>ttylist</i> sendlog { { mail ftp } [interval <i>interval.time</i>] [ratio <i>percent</i>] off }
Parameters	<p><i>ttylist</i></p> <p>Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>{ { mail ftp } [interval <i>interval.time</i>] [ratio <i>percent</i>] off }</p> <p>Set the conditions to send the port logs to an email server and an FTP server. This parameter is "off" by default.</p> <p>{ mail ftp } [interval <i>interval.time</i>] [ratio <i>percent</i>]</p> <p>mail</p> <p>Send the port logs to an email server.</p> <p>ftp</p> <p>Send the port logs to an FTP server.</p> <p>[interval <i>interval.time</i>]</p> <p>Set the interval to send the port logs to the email server or the FTP server. The setting unit is one minute. The setting range is from 0 through 65535 minutes. Specify "0" to disable the interval time and send the port logs according to the port log usage rate setting. This parameter is set to "60" by default.</p> <p>[ratio <i>percent</i>]</p> <p>Set the threshold for the port log usage rate used to send the port logs to the email or FTP server. The logs are sent when the usage rate reaches this value. The setting unit is a percentage. Set a value between 10% and 80% in units of 1%. This parameter is set to "80" by default.</p> <p>off</p> <p>Do not send the port logs.</p>
Usage example	To send the port logs of serial ports 1 to 32 to the email server.
	set logd tty 1-32 sendlog mail
Explanation	Specify "0" for the interval time to disable it and use only the usage rate to send the port logs.

set logd tty mail port**[Administrator]**

Function Set SMTP port for the port log emails.

Format **set logd tty *ttylist* mail { 1 | 2 } port *smtp-port***

Parameters *ttylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

mail { 1 | 2 }

Specify the identification number (1 or 2) of the email server.

port *smtp-port*

Specify SMTP port for the port log emails.

The setting range is from 1 through 65535.

This parameter is set to "25" by default.

Usage example To send the port logs of serial ports 1 to 32 at port 10025

set logd tty 1-32 mail 1 port 10025

Explanation This setting is also deleted if the email server registration settings are removed.

set logd tty mail type**[Administrator]**

Function	Set how the port logs are sent by email (sending method).
Format	set logd tty <i>ttylist</i> mail { 1 2 } type { body attachment }
Parameters	<p><i>ttylist</i></p> <p>Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>mail { 1 2 }</p> <p>Specify the identification number (1 or 2) of the email server.</p> <p>type { body attachment }</p> <p>Specify how the port logs are sent to the email server. This parameter is set to "attachment" by default.</p> <p>body</p> <p>The port logs are inserted in the message body and sent.</p> <p>attachment</p> <p>The port logs are sent as an attachment file.</p>
Usage example	<p>To send the port logs of serial ports 1 to 32 as message body of emails.</p> <p>set logd tty 1-32 mail 1 type body</p>
Explanation	This setting is also deleted if the email server registration settings are removed.

set logd tty mail subject**[Administrator]**

Function	Set the email subject for port logs.
Format	set logd tty <i>ttylist</i> mail { 1 2 } subject "<i>string</i>"
Parameters	<p><i>ttylist</i></p> <p>Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>mail { 1 2 }</p> <p>Specify the identification number (1 or 2) of the email server.</p> <p>subject "<i>string</i>"</p> <p>Specify the subject of emails to send to the server in a maximum of 64 characters. This parameter is set to "portlog TTY No." by default.</p>
Usage example	<p>To specify "this is a portlog" for the subject of email of serial port 1 sent to the email destination No. 1.</p> <p>set logd tty 1 mail 1 subject "this is a portlog."</p>
Explanation	This setting is also deleted if the email server registration settings are removed.

set logd tty mail sender**[Administrator]**

Function	Set the email address of the sender for port logs.
Format	set logd tty <i>ttylist</i> mail { 1 2 } sender <i>fromaddr</i>
Parameters	<p><i>ttylist</i></p> <p>Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model.</p> <p>Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>mail { 1 2 }</p> <p>Specify the identification number (1 or 2) of the email server.</p> <p>sender <i>fromaddr</i></p> <p>Specify the email address of the sender. This parameter is set to the following format by default: portusr@NS-2250 host name.NS-2250 local domain</p>
Usage example	<p>To specify "portlog1@example.co.jp" for the sender address of emails of serial port 1 sent to the email destination No. 1.</p> <p>set logd tty 1 mail 1 sender portlog1@example.co.jp</p>
Explanation	This setting is also deleted if the email server registration settings are removed.

set logd tty mail auth**[Administrator]**

Function Set SMTP authentication for the port log emails.

Format **set logd tty *ttylist* mail { 1 | 2 } auth *auth-Account***
[{ password | encrypt *string* }]

Parameters *ttylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

mail { 1 | 2 }

Specify the identification number (1 or 2) of the email server.

auth *auth-Account*

Specify the account and password for SMTP authentication.

The SMTP authentication is enabled for the corresponding email destination when this setting is configured.

[{ password | encrypt *string* }]

password

Set the password of the account used to access the email server.

This setting is required when the email server uses SMTP authentication.

When the command is executed with this parameter specified, a message prompting you to enter a password is displayed. Enter a password.

When you press the Enter key after entering the password, a message prompting you to confirm the password is displayed. Enter the same password again.

If you do not specify this parameter and the encrypt string parameter, no password will be used for the created users.

Setting a password using this command changes the format of this command written in the startup file to a character string corresponding to the encrypted password.

encrypt *string*

Set the account password as an encrypted character string.

When the command is executed with this parameter specified, no password entry or confirmation messages are displayed. This parameter is convenient to embed a startup file containing settings of SMTP authentication accounts with passwords.

Usage example To set a password to "portlog2" account used with SMTP authentication.

set logd tty 1 mail 1 auth portlog2 password

SNMP-Auth password Password entry (not displayed)

Retype SNMP-Auth password Password entry (not displayed)

Explanation This setting is also deleted if the email server registration settings are removed.

unset logd tty mail auth**[Administrator]**

Function Remove settings of SMTP authentication for port log emails.**Format** **unset logd tty *ttylist* mail { 1 | 2 } auth****Parameters** *ttylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

mail { 1 | 2 }

Specify the identification number (1 or 2) of the email server.

Usage example To remove the SMTP authentication settings for port logs of serial ports 1 to 32.**unset logd tty 1-32 mail 1 auth**

remove logd tty mail**[Administrator]**

Function	Remove the settings for the destination email address and email server used to send port logs.
Format	remove logd tty <i>ttylist</i> mail { 1 2 }
Parameters	<p><i>ttylist</i></p> <p>Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>mail { 1 2 }</p> <p>Specify the identification number (1 or 2) of the email server.</p>
Usage example	<p>To remove the settings of the email address and email server No. 2 used for the serial ports 1 to 32.</p> <p>remove logd tty 1-32 mail 2</p>
Explanation	The email settings (sending method, subject, and destination email address) with the ID number for which the settings have been removed return to their default values.

remove logd tty ftp**[Administrator]**

Function	Remove settings of a destination FTP server for port logs.
Format	remove logd tty <i>ttylist</i> ftp { 1 2 }
Parameters	<i>ttylist</i> Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command. Specify identification number (1 or 2) of the FTP server whose settings you want to remove.
Usage example	To remove the settings of FTP destination No. 2 to send port logs of serial ports 1 to 32. remove logd tty 1-32 ftp 2

4.21 portd setting commands

These are objects managing NS-2250 port server function.

set portd connect

[Administrator]

Function Set the connection mode of the port server.

Format **set portd connect { direct | select }**

Parameters **{ direct | select }**

When you specify "direct", the port server uses the direct mode available since the first version for the access method. Direct mode is an access method in which you specify the TCP port number corresponding to the serial port to access the monitored device directly.

(Example) To access the serial port 1 of the NS-2250 in Direct mode, specify the TCP port No. 8101 of the connection destination from a Telnet client.
telnet SmartCS 8101

When you specify "select", the port server operates in Select mode (port selection function). Select mode is an access method in which you log in to the NS-2250 (TCP: 23/22) from a Telnet/SSH client, and select a serial port number from the port selection menu to access a monitored device.

(Example) To access the serial port 1 of the NS-2250 in Select mode, connect to the normal TCP port (23) from a Telnet client and select the serial port No. 1 from the port selection menu.

telnet SmartCS

This parameter is set to "direct" by default.

Usage example To set Select mode.

set portd connect select

Explanation (1) In Select mode, the user whether log in to the NS-2250 or access to a monitored device depending on its login user name. Therefore, set also "set portd auth basic" when using Select mode.

(2) When using Select mode, set "set tty drhup off" to prevent automatic hang up caused by DSR signals.

set portd menu**[Administrator]**

Function Set the display method of the port server menu.

Format **set portd menu { auto | on | off }**

Parameters **{ auto | on | off }**

This parameter is set to "auto" by default.

auto

Specify "auto" to use the same display method as the Direct mode.

When the port log save function is on in an RW session: The port server menu is displayed.

When the port log save function is off: The port server menu is not displayed.

on

Specify "on" to always display the port server menu.

off

Specify "off" to always hide the port server menu.

Usage example To hide the port server menu.

set portd menu off

set portd auth**[Administrator]**

Function	Set whether or not to use port user authentication when connecting from a Telnet client.
Format	set portd auth { none basic }
Parameters	auth { none basic } This parameter is set to "none" by default. none Specify "none" not to use the port user authentication when accessing NS-2250 serial ports from a Telnet client. basic Specify "basic" to use the port user authentication when accessing NS-2250 serial ports from a Telnet client.
Usage example	To use port user authentication. set portd auth basic
Explanation	Port user authentication is possible when accessing NS-2250 serial ports from both Telnet and SSH clients. When accessing NS-2250 serial ports from an SSH client, user authentication is used regardless of this setting.

set portd telrw**[Administrator]**

Function Specify the service port start number for Telnet Normal mode.

Format **set portd telrw** *port_num*

Parameters *port_num*
Specify a decimal value for the port number.
(Port number setting range: 1025 - 65000)
This parameter is set to "8101" by default.

Usage example To set "10001" as the service port start number for Telnet Normal mode.

set portd telrw 10001

Explanation (1) Normal mode enables bidirectional communication with monitored equipment connected the serial port.
(2) The service port numbers are allocated to each serial port starting from the service port start number specified with this command. Service port numbers are allocated only for the ports equipped on the model used (16/32/48).

set portd telro**[Administrator]**

Function Specify the service port start number for Telnet Monitoring mode.

Format **set portd telro** *port_num*

Parameters *port_num*
Specify a decimal value for the port number.
(Port number setting range: 1025 - 65000)
This parameter is set to "8201" by default.

Usage example To set "11001" as the service port start number for Telnet Monitoring mode.

set portd telro 11001

Explanation (1) Monitoring mode enables monitoring of the data exported by monitored equipment connected to a serial port.
(2) The service port numbers are allocated to each serial port starting from the service port start number specified with this command. Service port numbers are allocated only for the ports equipped on the model used (16/32/48).

set portd sshrw**[Administrator]**

Function Specify the service port start number for SSH Normal mode.

Format **set portd sshrw** *port_num*

Parameters *port_num*
Specify a decimal value for the port number.
(Port number setting range: 1025 - 65000)
This parameter is set to "8301" by default.

Usage example To set "12001" as the service port start number for SSH Normal mode.

set portd sshrw 12001

Explanation (1) Normal mode enables bidirectional communication with monitored equipment connected to a serial port.
(2) The service port numbers are allocated to each serial port starting from the service port start number specified with this command. Service port numbers are allocated only for the ports equipped on the model used (16/32/48).

set portd sshro**[Administrator]**

Function Specify the service port start number for SSH Monitoring mode.

Format **set portd sshro** *port_num*

Parameters *port_num*
Specify a decimal value for the port number.
(Port number setting range: 1025 - 65000)
This parameter is set to "8401" by default.

Usage example To set "13001" as the service port start number for SSH Monitoring mode.

set portd sshro 13001

Explanation (1) Monitoring mode enables monitoring of the data exported by monitored equipment connected to a serial port.
(2) The service port numbers are allocated to each serial port starting from the service port start number specified with this command. Service port numbers are allocated only for the ports equipped on the model used (16/32/48).

set portd idle_timeout**[Administrator]**

Function Set a value for the idle timer for the select menu, port server menu, and Normal mode (rw) sessions.

Format **set portd idle_timeout { on [*interval_time*] | off }**

Parameters **idle_timeout { on [*interval_time*] | off }**
Specify "on" or "off" for the idle timer for the select menu, port server menu, and Normal mode (rw) sessions.

This parameter is "off" by default.

interval_time

When set to "on", specify the idle timer value in minutes. This timer is used when connected to the select menu, port server menu, and Normal mode (rw) sessions.

The setting range is from 1 through 60 minutes. This parameter is set to "10" by default.

Usage example To set 20 minutes for the timeout value used when connected to the select menu, port server menu, and Normal mode (rw) sessions.

set portd idle_timeout on 20

Explanation (1) When you enable this function, the select menu idle timer is also enabled.
(2) When you enable the idle timer for select menu, port server menu, and Normal mode (rw) session connection, set also "set portd tty timeout on".

(3) The following occurs when the set time has elapsed.

- In select menu, the session is disconnected.
- In port server menu, the session is disconnected when in Direct mode, or the selection menu is displayed in Select mode.
- In Normal mode (rw) sessions, an operation similar to when you enter "cmdchar" is performed. (4) In Normal mode (rw) sessions, the timer monitors the input from the Telnet/SSH terminal. The timer is reset when something is entered from the Telnet/SSH terminal. The timer is not reset when data is received from the monitored equipment.

set portd ro_timeout**[Administrator]**

Function Set a value for the session timer of Monitoring mode (ro) sessions.

Format **set portd ro_timeout { on [interval_time] | off }**

Parameters **{ on [interval_time] | off }**

Specify "on" or "off" for the session timer of Monitoring mode (ro) sessions. This parameter is "off" by default.

interval_time

When set to "on", specify a value in minutes for the session timer of Monitoring mode (ro) sessions. The setting range is from 1 through 1440 minutes.

This parameter is set to "10" by default.

Usage example To set 60 minutes for the timeout value used when connected to Monitoring mode (ro) sessions.

set portd ro_timeout on 60

Explanation

- (1) When you enable the session timer, set also "set portd tty timeout on" for the target port.
- (2) The Monitoring mode (ro) session is disconnected when the set time has elapsed.
- (3) The timer is not reset even if data is sent or received from the Telnet/SSH terminal or the monitored equipment.

set portd tty session**[Administrator]**

Function	Set the authorized protocols and modes for connection to the serial ports.
Format	set portd tty <i>ttylist</i> session { { telnet ssh both none } { ro rw both } }
Parameters	<p>tty <i>ttylist</i> Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>{ telnet ssh both none } { ro rw both } This parameter is set to "both rw" by default.</p> <p>{ telnet ssh both none }</p> <p>telnet Authorize only Telnet connection.</p> <p>ssh Authorize only SSH connection.</p> <p>both Authorize both Telnet and SSH connections.</p> <p>none Refuse Telnet and SSH connections. Use this command to close TCP ports with a service port number for which no protocols and connection modes have been authorized.</p> <p>{ ro rw both }</p> <p>ro Authorize connection in Monitoring mode only</p> <p>rw Authorize connection in Normal mode only</p> <p>both Authorize connection in both Monitoring and Normal modes</p>

Usage example To set Telnet Normal mode for the connection protocol of serial port 1.

```
set portd tty 1 session telnet rw
```

set portd tty limit**[Administrator]**

Function Set a number of sessions for a serial port.

Format **set portd tty *ttylist* limit rw *number* ro *number***

Parameters *ttylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

limit rw *number* ro *number*

Specify the authorized number of sessions for connection.

rw *number*

Number of sessions in Normal mode. You can specify a number from 0 through 2. The default setting is 1.

ro *number*

Number of sessions in Monitoring mode. You can specify a number from 0 through 3. The default setting is 1.

Usage example To authorize 2 sessions in Normal mode and 3 sessions in Monitoring mode for the serial port 1.

set portd tty 1 limit rw 2 ro 3

set portd tty brk_char**[Administrator]**

Function Set the NVT break character.**Format** **set portd tty *ttylist* brk_char { none | brk }****Parameters** **tty *ttylist***

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

brk_char { none | brk }

This parameter is set to "none" by default.

none

none

brk

Set the NVT break character.

Usage example To set the NVT break character for serial port 1.**set portd tty 1 brk_char brk**

set portd tty nl**[Administrator]**

Function	Set the conversion method for the line feed format received from the network.
Format	set portd tty <i>tylist</i> nl { none cr lf }
Parameters	<p>tty <i>tylist</i> Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>nl { none cr lf } This parameter is set to "cr" by default.</p> <p>none No conversion</p> <p>cr Convert CR/LF to CR.</p> <p>lf Convert CR/LF to LF.</p>
Usage example	To convert to LF the line feed format received from the network for the serial port 1. set portd tty 1 nl lf
Explanation	This command is valid only with Telnet clients.

set portd tty cmdchar**[Administrator]**

Function Set a substitute character code to go to the port server menu.

Format **set portd tty *ttylist* cmdchar { none | *char_number* }**

Parameters **tty *ttylist***

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

cmdchar { none | *char_number* }

This parameter is set to "none" by default.

none

No character

char_number

Set a substitute character (keyboard key) to go to the port server menu in hexadecimal code (00 to 1F).

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

Usage example To set "01" (Ctrl-A) for the substitute character code for the port server menu of the serial port 1.

After making this setting, the "Press "CTRL-A" to return this menu" is displayed when accessing the monitored equipment.

set portd tty 1 cmdchar 01

Explanation

(1) The substitute character code is processed by the NS-2250 when registered. Therefore, the registered code is not sent to the device connected to the serial port.

(2) Enter the substitute character code when the port server menu is enabled to return to the port server menu. Enter the substitute character code when the port server menu is disabled to disconnect the session.

(3) The substitute character assigned to the code may differ from the character in the table above depending on the terminal software you use.

set portd tty label**[Administrator]****Function** Set serial port labels.**Format** **set portd tty *ttylist* label "*string*"****Parameters** *ttylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

label "*string*"

Specify a label for a serial port within 32 characters.

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.

Usage example To set the label "Tokyo L3SW" to the serial port 1.**set portd tty 1 label "Tokyo L3SW"**

set portd tty timeout**[Administrator]**

Function	Set the timeout function on and off for the port server menu, Normal mode (rw) sessions, and Monitoring mode (ro) sessions.
Format	set portd tty <i>ttylist</i> timeout { on off }
Parameters	<p>tty <i>ttylist</i> Specify the tty number corresponding to the serial port in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.</p> <p>timeout { on off } Specify "on" or "off" for the timeout function for the port server menu, Normal mode (rw) sessions, and Monitoring mode (ro) sessions. This parameter is "off" by default.</p>
Usage example	To set the timeout function for the port server menu, Normal mode (rw) sessions, and Monitoring mode (ro) sessions for serial port 1.
	set portd tty 1 timeout on
Explanation	(1) When you enable the timeout function, set also "set portd idle_timeout on" and "set portd ro_timeout on".

unset portd tty label**[Administrator]**

Function Remove serial port label settings.**Format** **unset portd tty *ttylist* label****Parameters** **tty *ttylist***

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

Usage example To remove the label set to the serial port 1.**unset portd tty 1 label**

4.22 Console setting commands

Objects managing the operating conditions of the NS-2250 console function.

set console

[Administrator]

Function	Set the console.
Format	<pre>set console { baud { 2400 4800 9600 19200 38400 57600 115200 } bichar { 7 8 } parity { even odd none } stop { 1 2 } flow { xon rs none } }</pre>
Parameters	<p>baud { 2400 4800 9600 19200 38400 57600 115200 } Set the transmission rate. This parameter is set to "9600" by default.</p> <p>bichar { 7 8 } Set the data bit length. This parameter is set to "8" by default.</p> <p>parity { even odd none } Set the parity. This parameter is set to "none" by default.</p> <p>even Even parity</p> <p>odd Odd parity</p> <p>none No parity</p> <p>stop { 1 2 } Set the stop bit length. This parameter is set to "1" by default.</p> <p>flow { xon rs none } Set the flow control. This parameter is set to "xon" by default.</p> <p>xon Control uses xon and xoff codes.</p> <p>rs Control the flow using RTS/CTS signals.</p> <p>none Flow control is not used.</p>
Usage example	<p>To set a transmission rate of 19200 bps for the CONSOLE port.</p> <pre>set console baud 19200</pre>
Explanation	This command applies only to the CONSOLE port. Refer to the "set tty" command for the serial port settings.

4.23 Telnet command setting commands

set telnet cmdchar

[Administrator]

Function Set the character code to transit to the command mode while executing the telnet command.

Format **set telnet cmdchar { none | char_number }**

Parameters **cmdchar { none | char_number }**

Set the character code to transit to the command mode.

The default value is "1d".

none

Not set the character code to transit to the command mode.

char_number

Set the character code(the key of the keyboard) to transit to the command mode in the code of the hexadecimal number(from 00 to 1f).

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

Usage example The case of setting the character code to transit to the command mode as "01(Ctrl-A)".

set telnet cmdchar 01

Explanation Depending on a using terminal software, the substitute character assigned the code may be different from the above table.

In the case of setting this command, this setting become enabled since the next telnet command.

4.24 Telnetd setting commands

These are objects managing NS-2250 Telnet server function.

set telnetd port

[Administrator]

Function Set the Telnet server port number.

Format **set telnetd port { *port_number* | default }**

Parameters **port { *port_number* | default }**

port_number

Specify a port number.

You can specify a number from 1025 through 65000 for the port number.

default

Specify the Telnet server default port 23 for the port number.

Note If the port number set here is the same as one specified with "set portd telrw", "set portd telro", "set portd sshrw", "set portd sshro", or "set sshd port", this command generates an error.

Usage example To specify 10023 for the Telnet server port number.

set telnetd port 10023

enable telnetd**[Administrator]**

Function	Enable the Telnet server.
Format	enable telnetd
Parameters	None
Note	The Telnet server is enabled by default.
Usage example	enable telnetd

disable telnetd**[Administrator]****Function** Disable the Telnet server.**Format** **disable telnetd****Parameters** None**Usage example** **disable telnetd**

4.25 sshd setting commands

These are objects managing NS-2250 SSH server function.

set sshd auth

[Administrator]

Function	Set the user authentication type for the SSH server.
Format	set sshd auth { basic public }
Parameters	auth { basic public } This parameter is set to "public" by default. basic Specify "basic" to use password authentication with the SSH server. public Specify "public" to use public key authentication.
Usage example	To set password authentication for SSH server authentication. set sshd auth basic

set sshd port**[Administrator]****Function** Set the SSH server port number.**Format** **set sshd port { port_number | default }****Parameters** *port_number*

Specify a port number.

You can specify a number from 1025 through 65000 for the port number.

default

Specify the SSH server default port 22 for the port number.

Usage example To specify 20022 for the SSH server port number.**set sshd port 20022****Explanation** (1) If the port number set here is the same as one specified with "set portd telrw", "set portd telro", "set portd sshrw", "set portd sshro", or "set telnetd port", this command generates an error.

set sshd host_key**[Administrator]****Function** Set the SSH server host_key.**Format** **set sshd host_key { *number* | device_depend }****Parameters** **host_key { *number* | device_depend }***number*

Specify the seed of server host_key.

You can specify a number from 0 through 4294967295 for the number.

device_depend

Set the original value as a server host_key.

Usage example To specify 256 for the SSH server host_key.**set sshd host_key 256****Note** (1) When designating the seed value of this parameter, a server host key of the identical SSH server is made.

When exchanging NS-2250, please set it as the same seed value.

enable sshd**[Administrator]**

Function Enable the SSH server.**Format** **enable sshd****Parameters** None**Note** (1) Both SSH access and SFTP access to the NS-2250 are made possible.
 (2) The SSH server is disabled by default.**Usage example** **enable sshd**

disable sshd**[Administrator]****Function** Disable the SSH server.**Format** **disable sshd****Parameters** None**Usage example** **disable sshd**

4.26 ftpd setting commands

These are objects managing NS-2250 FTP server function.

enable ftpd

[Administrator]

Function	Enable the FTP server.
Format	enable ftpd
Parameters	None
Note	The FTP server is disabled by default.
Usage example	enable ftpd

disable ftpd**[Administrator]****Function** Disable the FTP server.**Format** **disable ftpd****Parameters** None**Usage example** **disable ftpd**

4.27 Security setting commands

These are objects managing authorizations for host and service connection via the network.

create allowhost

[Administrator]

Function Create a list of hosts and services authorized for connection.

Format **create allowhost** { **all** | *ipaddr/mask* | *ip6addr/mask* }
service { **all** | **telnetd** | **sshd** | **ftpd** |
portd { **telrw** | **telro** | **sshrw** | **sshro** } { **all** | *ttylist* } }

Parameters { *ipaddr/mask* | *ip6addr/mask* | **all** }
Specify the IP address of the host authorized for connection as IP address/prefix size.

ipaddr/mask

A 32-bit prefix is used if the prefix size is omitted.

To allow connections from all IPv4 hosts, specify 0.0.0.0/0.

ip6addr/mask

Specify the IPv6 address in x:x:x:x:x:x:x:x format.

The "x" in each field of the address is represented by the hexadecimal of the 16 bit part.

If there are consecutive 0 in the front of the field they can be omitted.

The field composed of only 0 can also be omitted only once by specifying as "::" in the address.

Specify the length of mask in the range of 0 to 128.

To allow connections from all IPv6 hosts, specify ::/0.

all

When "all" is specified, the connection is authorized from all hosts.

The default setting for this parameter in the startup file is "all".

service { **all** | **telnetd** | **sshd** | **ftpd** | **portd** { **telrw** | **telro** | **sshrw** | **sshro**
} { **all** | *ttylist* } }

Specify the services authorized for connection.

The default settings for this parameter are "create allowhost all telnetd" and "create allowhost all portd telrw all".

all

Specify "all" to authorize connection with all services.

telnetd

Specify "telnetd" to authorize connection using Telnet.

sshd

Specify "sshd" to authorize connection using SSH and SFTP.

ftpd

Specify "ftpd" to authorize connection using FTP.

portd { **telrw** | **telro** | **sshrw** | **sshro** } { **all** | *ttylist* }

When you specify "portd" specify also one of the following options.

telrw

Specify "telrw" to authorize connection in Telnet Normal mode to the specified serial ports.

telro

Specify "telro" to authorize connection in Telnet Monitoring mode to the specified serial ports.

sshrw

Specify "sshrw" to authorize connection in SSH Normal mode to the specified serial ports.

sshro

Specify "sshro" to authorize connection in SSH Monitoring mode to the specified serial ports.

all

Specify "all" to authorize connection with all serial ports.

ttylist

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

Note

- You can make the settings for a maximum of 99 "allowhost" parameters.

Usage example To authorize Telnet connection to the NS-2250 from 192.168.1.0/24.

```
create allowhost 192.168.1.0/24 service telnetd
```

delete allowhost**[Administrator]**

Function Delete a list of hosts and services authorized for connection.

Format **delete allowhost** {
 { **all** | *ipaddr/mask* | *ip6addr/mask* } **service** { **all** | **telnetd** | **sshd** | **ftpd** |
 portd { **telrw** | **telro** | **sshrw** | **sshro** } { *ttylist* | **all** } } |
 allentry }

Parameters { **all** | *ipaddr/mask* | *ip6addr/mask* } **service** { **all** | **telnetd** | **sshd** | **ftpd** |
portd { **telrw** | **telro** | **sshrw** | **sshro** } { *ttylist* | **all** } }

 { **all** | *ipaddr/mask* | *ip6addr/mask* }

Specify the IP address of the host whose connection authorization you want to remove as IP address/prefix size. When "all" is specified, the connection authorization is removed for all hosts.

service { **all** | **telnetd** | **sshd** | **ftpd** | **portd** { **telrw** | **telro** | **sshrw** |
sshro } { *ttylist* | **all** } }

Specify the services whose connection authorization you want to remove.

telnetd

Specify "telnetd" to remove authorization for Telnet connection.

sshd

Specify "sshd" to remove authorization for SSH and SFTP connections.

ftpd

Specify "ftpd" to remove authorization for FTP connection.

portd { **telrw** | **telro** | **sshrw** | **sshro** } { *ttylist* | **all** }

Specify "portd" to remove authorization for portd connections.

allentry

Delete a list authorizing connection for all hosts.

Usage example To remove authorization for Telnet connection to the NS-2250 from 192.168.1.0/24.

delete allowhost 192.168.1.0/24 service telnetd

4.28 Authentication setting commands

These are objects managing the operating conditions of user authentication and authentication using RADIUS/TACACS+ clients.

create auth access_group

[Administrator]

Function

Create access groups and serial port access privileges.

You can set roles and access privileges for each group you have created.

The following functions have been enhanced in this command compared to the "set auth radius server { root | normal | portusr } filter_id_head" command.

- You can register multiple identifiers (access groups) for device management users, normal users, and port users.
- You can define the access groups to which users belong only in the RADIUS server, and set the group definitions and port user access privileges on the NS-2250. Therefore, you can define different serial port access privileges for the same access group on multiple NS-2250.

Format

```
create auth access_group { root | normal | portusr port enable_port_list }
{ radius filter_id string | tacacs attr string val string }
```

Parameters

```
{ root | normal | portusr port enable_port_list }
```

root

Specify "root" to set the access group of device management users who log in to the NS-2250. Users in this group who log in to the NS-2250 are handled as device management users.

normal

Specify "normal" to set the access group of normal users who log in to the NS-2250. Users in this group who log in to the NS-2250 are handled as normal users.

portusr

Specify "portusr" to set the access group of port users who access the serial ports of the NS-2250. Users in this group are handled as port users. Configure the serial port access privileges using the option below.

port enable_port_list

Specify the ports that can be used in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

If different serial ports are already registered to the same group through multiple commands, the serial ports are added to the command line already registered. The commands are gathered together in one line.

```
{ radius filter_id string | tacacs attr string val string }
```

radius filter_id string

Set the character string string of the RADIUS Filter-Id attribute that will be used for the access group name. You can specify from 1 through 64 characters for string. You can use half-width alphanumeric characters, underbars "_", hyphens "-", at marks "@", and periods ".".

tacacs attr string val string

Set the character strings of the TACACS+ server attribute (attr) and value (val) pair that will be used for the access group name. You can specify from 1 through 32 characters for string. You can use half-width alphanumeric characters, underbars "_", hyphens "-", at marks "@", and periods ".".

Usage example (1) To set the group identifier "admin" for the access group of device management users (RADIUS).

```
create auth access_group root radius filter_id admin
```

(2) To set the group identifier "general" for the normal user access group (RADIUS).

```
create auth access_group normal radius filter_id general
```

(3) To set the group identifier "grp1" for the access group of port users with access privileges for the serial ports 1 to 5 (RADIUS).

```
create auth access_group portusr port 1-5 radius filter_id grp1
```

(4) To set the user definition attribute and value pair "grp1=root" for the access group of device management users (TACACS+).

```
create auth access_group root tacacs attr grp1 val root
```

(5) To set the user definition attribute and value pair "grp2=tech1" for the access group of port users with access privileges for the serial ports 1 to 5 (TACACS+).

```
create auth access_group portusr port 1-5 tacacs attr grp2 val tech1
```

Explanation

(1) You can register up to 100 lines of access groups (number of lines of the "create auth access_group" command). When multiple "create auth access_group" commands are executed for the same access group identifier, they are registered as one line. Examples of registration line calculation are given below.

- When you register the access group "admin" for device management users: 1 line
- When you register the same access group "grp1" for port users to the serial ports 1 to 32: 1 line
- When you register different access groups (grp1 to grp32) for port users to the serial ports 1 to 32: 32 lines (2) Access group priority during login is as follows: (1)device management user (root), (2)normal user (normal), and (3)port user (portusr).

When you log in to the NS-2250 in Select mode, log in as the user with the highest priority of access privileges of (1),(2),and (3).

For example, with the settings below log in to the NS-2250 as a device management user.

When you log in to the NS-2250 in Direct mode, 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 using RADIUS authentication with the settings below, log in to the NS-2250 as a device management user. Access the port server as a port user.

(Settings of the NS-2250)

```
# create auth access_group root radius filter_id admin
# create auth access_group normal radius filter_id general
# create auth access_group portusr port 1-5 radius filter_id grp1
```

(Setting example for RADIUS authentication server)

```

user1 Password = "user1"
      Filter-Id = "admin"
      Filter-Id = "general"
      Filter-Id = "grp1"

```

(3) If you use this command together with the "set auth radius server { root | normal | portusr } filter_id_head" command, with which you can specify roles and access privileges for RADIUS users individually, all the settings are handled with the "or" condition.

For example, with the NS-2250 configured as follows and the two following Filter-Id attributes registered to the RADIUS authentication server, the port user "port1" has access to the serial ports 1 to 5, authorized for the access group "grp1", as well as the serial ports 6 to 10, authorized with "NS2240_PORT6-10".

(Settings of the NS-2250)

```

# create auth access_group portusr port 1-5 radius filter_id grp1
# set auth radius server 1 portusr filter_id_head NS2250_PORT

```

(RADIUS authentication server settings)

```

port1 Password = "port1"
      Filter-Id = "grp1"
      Filter-Id = "NS2250_PORT6-10"

```

(4) When using the TACACS+ function, set the attribute as the attribute value pair. Although you can set the character strings of your choosing for both, the attribute value pair must match between the NS-2250 and the TACACS+ server.

(Settings of the NS-2250)

```

# create auth access_group root tacacs attr grp1 val root
# create auth access_group portusr port 1-5 tacacs attr grp2 val tech1

```

(TACACS+ server settings)

```

user = user1 {
    service = smartcs {
        grp1 = root
        grp2 = tech1
    }
}

```

(5) With users for which the user group cannot be identified, user authentication is performed according to "set auth radius def_user" or "set auth tacacs def_user" settings.

The user group cannot be identified in following cases.

- If this command or the "set auth radius server { portusr | normal | root } filter_id_head" command has not been set when using RADIUS authentication
- If this command has not been set when using TACACS+ function
- If attributes for the RADIUS authentication server or the TACACS+ server have not been set
- If the format of all attributes received by the NS-2250 cannot be recognized (do not match the settings of this command or the "filter_id_head" command)

Note

RADIUS authentication and TACACS+ authentication/approval function cannot be used at the same time. After specifying the mode using the "set auth mode" command, set the corresponding attributes.

You cannot set the same access group identifier to multiple user groups.

set auth mode**[Administrator]**

Function Set the user authentication method.

Format **set auth mode { local | radius | tacacs }**

Parameters **{ local | radius | tacacs }**

This parameter is set to "local" by default.

local

Specify "local" to use only NS-2250 local authentication for user authentication. Local authentication checks that the name and password of the user accessing the NS-2250 match the settings registered in the NS-2250.

radius

Specify "radius" to perform user authentication in the following order: local authentication within the NS-2250 -i, RADIUS authentication. When the name and password of the user accessing the NS-2250 match the settings registered in the NS-2250, local authentication is successful. If the accessing user is not registered in the NS-2250, or if the password mismatches the setting, the NS-2250 sends an authentication request to the RADIUS authentication server to perform RADIUS authentication.

tacacs

Specify "tacacs" to perform user authentication in the following order: local authentication within the NS-2250 -i, TACACS+ authentication and approval. The flow of authentication operations is the same as with the "radius" parameter.

Usage example To use RADIUS authentication.

set auth mode radius

Explanation (1) To authenticate an NS-2250 normal user with the RADIUS authentication server or TACACS+ server, make the settings so that the user local authentication within the NS-2250 fails. You can either delete the user from the NS-2250 or set a password for that user different from the RADIUS or TACACS+ server settings. Be aware that when no password is registered for normal users, simply pressing the Return key for the password makes it possible to pass local authentication of the NS-2250 and login.

It is the same when logging in as a device management user or executing the "su" command. Set a password different from the password registered to the RADIUS or TACACS+ server for device management users. Note that, unlike normal users, device management users (root) cannot be deleted.

Note Even if "radius" or "tacacs" has been specified with this command, only local authentication is used with the following types of access.

- FTP/SFTP access to the NS-2250
- SSH access to the NS-2250 or the NS-2250 serial ports when a public key is set for SSH server user authentication (set sshd auth public)

set auth su_cmd username**[Administrator]**

Function	In the RADIUS authentication or TACACS+ authentication/approval function, set the user name used when executing the "su" command with external authentication.
Format	set auth su_cmd username <i>user</i>
Parameters	<p>username <i>user</i></p> <p>In the RADIUS authentication or TACACS+ authentication/approval function, set the user name used for authentication and approval when executing the "su" command. The "su" command is used to change NS-2250 normal users to users with administrator privileges.</p> <p>For user, you can use half-width alphanumeric characters, underbars "_", and hyphens "-". Note that the first character of the character string must be an alphanumeric character. The 1 to 64 characters can be set for user.</p> <p>This parameter is set to "root" by default.</p>
Usage example	<p>To set the user name used when executing the "su" command to "admin".</p> <p>set auth su_cmd username admin</p>
Explanation	<p>(1) When executing the "su" command, the user name used for local authentication is "root" even if you set this command. Local authentication is always performed first even if you made the settings for RADIUS authentication or TACACS+ authentication. Therefore, if the "root" user password set in the NS-2250 matches the password set in the RADIUS authentication server or TACACS+ server for the user specified with this command, local authentication is successful. To fail the local authentication, you can change the "root" user password for local authentication.</p> <p>(2) The user specified with this command must be set as an attribute in the RADIUS authentication server or TACACS+ server, and this attribute must be set as an NS-2250 device management user with the "set auth radius server { portusr normal root } filter_id_head" command or the "create auth access_group" command.</p>

set auth radius retry**[Administrator]**

Function	Set the number of times the authentication request packet is resent to the RADIUS authentication server.
Format	set auth radius retry <i>number</i>
Parameters	retry <i>number</i> Set the number of times the authentication request packet is resent to the RADIUS authentication server. You can specify a number from 0 through 5. Specify "0" to not resend the authentication request packet. This parameter is set to "3" by default.
Usage example	To set to 5 the number of times the authentication request packet is resent. set auth radius retry 5

set auth radius server addr**[Administrator]****Function** Set the IP address of the RADIUS authentication server.**Format** **set auth radius server { 1 | 2 } addr *ipaddr***

Parameters **server { 1 | 2 }**
Specify 1 or 2 for the identification number of the RADIUS authentication server.

addr *ipaddr*
Specify the IP address of the RADIUS authentication server.

Usage example To set the RADIUS authentication server 192.168.1.1 as the RADIUS server 1.

set auth radius server 1 addr 192.168.1.1

set auth radius server port**[Administrator]**

Function	Set the authentication port number of the RADIUS authentication server.
Format	set auth radius server { 1 2 } port { 1812 1645 }
Parameters	server { 1 2 } Specify 1 or 2 for the identification number of the RADIUS authentication server. port { 1812 1645 } Specify the authentication port number of the RADIUS authentication server. This parameter is set to "1812" by default. 1812 Set the authentication port number to UDP: 1812. 1645 Set the authentication port number to UDP: 1645.
Usage example	To set "1645" for the authentication port number of RADIUS server 1. set auth radius server 1 port 1645

set auth radius server key**[Administrator]**

Function	Set the secret key of the RADIUS authentication server.
Format	set auth radius server { 1 2 } key { password encrypt string }
Parameters	<p>server { 1 2 } Specify 1 or 2 for the identification number of the RADIUS authentication server.</p> <p>key { password encrypt string } Set the secret key of the RADIUS authentication server. The maximum number of characters that can be set for the secret key is 64.</p> <p>password When the command is executed with the "password" parameter specified, a message prompting you to enter the new secret key is displayed. Enter the new secret key. When you press the Enter key after entering the secret key, a message prompting you to confirm the secret key is displayed. Enter the same secret key again. The secret key is deleted if you only press the Enter key when registering the secret key.</p> <p>encrypt string Specify the secret key to set using the character string after conversion with the hash function.</p>
Usage example	<p>To set the secret key "ABCDEF" to the RADIUS authentication server 1.</p> <pre>set auth radius server 1 key password</pre> <p>Radius Server's password : Enter the secret key "ABCDEF". Retry Radius Server's password : Enter the secret key "ABCDEF". (The entered secret key is not displayed.)</p>
Explanation	Register the same secret key to the NS-2250 as the one registered to the RADIUS authentication server.

set auth radius server timeout**[Administrator]**

Function Set the timeout time for the response packet sent back from the RADIUS authentication server.

Format **set auth radius server { 1 | 2 } timeout *time***

Parameters **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the RADIUS authentication server.

timeout *time*

Specify the timeout time for the response packet sent back from the RADIUS authentication server. You can specify from 1 through 30 seconds.

This parameter is set to "5" by default.

Usage example To set 10 seconds for the timeout time.

set auth radius server 1 timeout 10

set auth radius server portusr**[Administrator]**

Function Set the port user identifier used with RADIUS authentication.

Format `set auth radius server { 1 | 2 } portusr filter_id_head string`

Parameters `{ 1 | 2 }`

Specify 1 or 2 for the identification number of the RADIUS authentication server.

filter_id_head string

When the Filter_Id attribute of the received RADIUS authentication packet contains a character string starting with string, the user is identified as a port user.

For string, you can use half-width alphanumeric characters, underbars "_", and hyphens "-". Note that the first character of the character string must be an alphanumeric character. The maximum number of characters that can be set for the string is 64.

For details on the setting method of Filter_Id attributes for a RADIUS authentication server, see Appendix D, "Examples of attributes and RADIUS authentication/accounting server settings".

Usage example To set the port user identifier used with RADIUS authentication.

```
set auth radius server 1 portusr filter_id_head NS2250_PORT
```

When the following Filter-Id attribute is received from the RADIUS authentication server, the user is identified as a port user by the NS-2250 and is authorized to access the serial ports 8 to 16, and 24.

```
Filter-Id = "NS2250_PORT8-16,24"
```

Explanation

(1) You can register only one port user identifier.

(2) With users for which the user group cannot be identified, user authentication is performed according to "set auth radius def_user" setting

The user group cannot be identified in following cases.

- If the "set auth radius server { portusr | normal | root } filter_id_head" command or "create auth access_group" command has not been set on the NS-2250
- If attributes for the RADIUS authentication server have not been set
- If the format of all Filter-Id attributes received by the NS-2250 cannot be recognized (3) All Filter-Id recognized by the NS-2250 are evaluated. Priority during login is as follows: (1) device management users (root), (2) normal users (normal), and (3) port users (portusr).

When you log in to the NS-2250 in Select mode, log in as the user with the highest priority of access privileges of (1), (2), and (3).

For example, with the settings below log in to the NS-2250 as a device management user.

When you log in to the NS-2250 in Direct mode, 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).

For example, with the settings below, log in to the NS-2250 as a device management user. Access the port server as a port user.

(Settings of the NS-2250)

```
# set auth radius server 1 root filter_id_head NS2250_ROOT
# set auth radius server 1 normal filter_id_head NS2250_NORMAL
# set auth radius server 1 portusr filter_id_head NS2250_PORT
```

(RADIUS authentication server settings)

```
user1 Password = "user1"
      Filter-Id = "NS2250_ROOT"
      Filter-Id = "NS2250_NORMAL"
      Filter-Id = "NS2250_PORT1-24"
```

(4) If you use the "set auth radius server { root | normal | portusr } filter_id_head" command together with the "create auth access_group" command, all the settings are handled with the "or" condition.

For example, with the NS-2250 configured as follows and the two following Filter-Id attributes registered to the RADIUS authentication server, the port user "port1" has access to the serial ports 1 to 5, authorized for the access group "grp1", as well as the serial ports 6 to 10, authorized with "NS2240_PORT6-10".

(Settings of the NS-2250)

```
# create auth access_group portusr port 1-5 radius filter_id grp1
# set auth radius server 1 portusr filter_id_head NS2250_PORT
```

(RADIUS authentication server settings)

```
port1 Password = "port1"
      Filter-Id = "grp1"
      Filter-Id = "NS2250_PORT6-10"
```

set auth radius server normal**[Administrator]**

Function Set the normal user identifier used with RADIUS authentication.

Format **set auth radius server { 1 | 2 } normal filter_id_head string**

Parameters **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the RADIUS authentication server.

filter_id_head string

When the Filter_Id attribute of the received RADIUS authentication packet contains a character string starting with string, the user is identified as a normal user.

For string, you can use half-width alphanumeric characters, underbars "_", and hyphens "-". Note that the first character of the character string must be an alphanumeric character. The maximum number of characters that can be set for the string is 64.

For details on the setting method of Filter_Id attributes for a RADIUS authentication server, see Appendix D, "Examples of attributes and RADIUS authentication/accounting server settings".

Usage example To set the normal user identifier.

```
set auth radius server 1 normal filter_id_head NS2250_NORMAL
```

When the following Filter-Id attribute is received from the RADIUS authentication server, the user is identified as a normal user by the NS-2250.

```
Filter-Id = "NS2250_NORMAL"
```

Explanation

(1) You can register only one normal user identifier.

(2) With users for which the user group cannot be identified, user authentication is performed according to "set auth radiusdef_user" setting. The user group cannot be identified in following cases.

- If the "set auth radius server { portusr | normal | root } filter_id_head" command or "create auth access_group" command has not been set on the NS-2250
- If attributes for the RADIUS authentication server have not been set
- If the format of all Filter-Id attributes received by the NS-2250 cannot be recognized (3) All Filter-Id recognized by the NS-2250 are evaluated. Priority during login is as follows: (1) device management users (root), (2) normal users (normal), and (3) port users (portusr).

When you log in to the NS-2250 in Select mode, log in as the user with the highest priority of access privileges of (1), (2), and (3).

For example, with the settings below log in to the NS-2250 as a device management user.

When you log in to the NS-2250 in Direct mode, 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).

For example, with the settings below, log in to the NS-2250 as a device management user. Access the port server as a port user.

(Settings of the NS-2250)

```
# set auth radius server 1 root filter_id_head NS2250_ROOT
# set auth radius server 1 normal filter_id_head NS2250_NORMAL
# set auth radius server 1 portusr filter_id_head NS2250_PORT
```

(RADIUS authentication server settings)

```
user1 Password = "user1"  
      Filter-Id = "NS2250_ROOT"  
      Filter-Id = "NS2250_NORMAL"  
      Filter-Id = "NS2250_PORT1-24"
```

(4) If you use the "set auth radius server { root | normal | portusr } filter_id_head" command together with the "create auth access_group" command, all the settings are handled with the "or" condition.

set auth radius server root**[Administrator]**

Function	Set the device management user identifier used with RADIUS authentication.
Format	set auth radius server { 1 2 } root filter_id_head string
Parameters	{ 1 2 } Specify 1 or 2 for the identification number of the RADIUS authentication server. filter_id_head string When the Filter_Id attribute of the received RADIUS authentication packet contains a character string starting with string, the user is identified as a device management user. For string, you can use half-width alphanumeric characters, underbars "_", and hyphens "-". Note that the first character of the character string must be an alphanumeric character. The maximum number of characters that can be set for the string is 64. For details on the setting method of Filter_Id attributes for a RADIUS authentication server, see Appendix D, "Examples of attributes and RADIUS authentication/accounting server settings".

Usage example To set the device management user identifier.

```
set auth radius server 1 root filter_id_head NS2250_ROOT
```

When the following Filter-Id attribute is received from the RADIUS authentication server, the user is identified as a device management user by the NS-2250.

```
Filter-Id = "NS2250_ROOT"
```

Explanation (1) You can register only one device management user identifier.
(2) With users for which the user group cannot be identified, user authentication is performed according to "set auth radius def_user" setting

The user group cannot be identified in following cases.

- If the "set auth radius server { portusr | normal | root } filter_id_head" command or "create auth access_group" command has not been set on the NS-2250
- If attributes for the RADIUS authentication server have not been set
- If the format of all Filter-Id attributes received by the NS-2250 cannot be recognized (3) All Filter-Id recognized by the NS-2250 are evaluated. Priority during login is as follows: (1) device management users (root), (2) normal users (normal), and (3) port users (portusr).

When you log in to the NS-2250 in Select mode, log in as the user with the highest priority of access privileges of (1), (2), and (3).

For example, with the settings below log in to the NS-2250 as a device management user.

When you log in to the NS-2250 in Direct mode, 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).

For example, with the settings below, log in to the NS-2250 as a device management user. Access the port server as a port user.

(Settings of the NS-2250)

```
# set auth radius server 1 root filter_id_head NS2250_ROOT  

# set auth radius server 1 normal filter_id_head NS2250_NORMAL  

# set auth radius server 1 portusr filter_id_head NS2250_PORT
```

(RADIUS authentication server settings)

```
user1 Password = "user1"  
      Filter-Id = "NS2250_ROOT"  
      Filter-Id = "NS2250_NORMAL"  
      Filter-Id = "NS2250_PORT1-24"
```

(4) If you use the "set auth radius server { root | normal | portusr } filter_id_head" command together with the "create auth access_group" command, all the settings are handled with the "or" condition.

set auth radius server nas_id**[Administrator]**

Function	Register the NAS-ID attribute notified to the RADIUS authentication server.
Format	set auth radius server { 1 2 } nas_id string
Parameters	{ 1 2 } Specify 1 or 2 for the identification number of the RADIUS authentication server. nas_id string Specify the character string to save in the NAS-ID attribute. You can specify from 1 through 64 characters for string. You can use half- width alphanumeric characters, underbars "_", hyphens "-", at marks "@", and periods ".". The host name is saved in the NAS-ID attribute if this parameter is omitted.
Usage example	To set "SmartCS" in the NAS-ID attribute. set auth radius server 1 nas_id SmartCS

set auth radius server def_user**[Administrator]**

Function Configure access methods for users for which a user group cannot be identified.

Format **set auth radius def_user { portusr | none }**

Parameters **{ portusr | none }**

 This parameter is set to "portusr" by default.

portusr

Specify "portusr" to handle the users for which a user group cannot be identified (users with the access group or "filter_id_head" setting that does not match) as port users, and authorize access to all serial ports.

none

Specify "none " to refuse access to the users for which a user group cannot be identified (users with the access group or "filter_id_head" setting that does not match).

Usage example To refuse access to users for which a user group cannot be identified.

set auth radius def_user none

set auth tacacs server addr**[Administrator]**

-
- Function** Set the IP address of the TACACS+ server (authentication/approval).
- Format** **set auth tacacs server { 1 | 2 } addr ipaddr**
- Parameters** **{ 1 | 2 }**
Specify 1 or 2 for the identification number of the TACACS+ server.
- addr ipaddr**
Specify the IP address of the TACACS+ server.
- Usage example** To set the TACACS+ server 192.168.1.1 to server 1.
- set auth tacacs server 1 addr 192.168.1.1**

set auth tacacs server key**[Administrator]**

Function	Set the secret key of the TACACS+ server (authentication/approval).
Format	set auth tacacs server { 1 2 } key { password encrypt string }
Parameters	<p>{ 1 2 } Specify 1 or 2 for the identification number of the TACACS+ server.</p> <p>key { password encrypt string } Specify the secret key of the TACACS+ server. The maximum number of characters that can be set for the secret key is 64.</p> <p>password When the command is executed with the "password" parameter specified, a message prompting you to enter the new secret key is displayed. Enter the new secret key. When you press the Enter key after entering the secret key, a message prompting you to confirm the secret key is displayed. Enter the same secret key again. The secret key is deleted if you only press the Enter key when registering the secret key.</p> <p>encrypt string Specify the secret key to set using the character string after conversion with the hash function.</p>
Usage example	<p>To set the secret key "ABCDEF" to the TACACS+ server 1.</p> <pre>set auth tacacs server 1 key password</pre> <p>Tacacs+ Server's password : Enter the secret key "ABCDEF". Retry Tacacs+ Server's password : Enter the secret key "ABCDEF". (The entered secret key is not displayed.)</p>
Explanation	(1) Register the same secret key to the NS-2250 as the one registered to the TACACS+ server.

set auth tacacs server timeout**[Administrator]**

Function Set the timeout time for the response packet sent back from the TACACS+ server (authentication/approval).

Format **set auth tacacs server { 1 | 2 } timeout *time***

Parameters **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the TACACS+ server.

timeout *time*

Specify the timeout time for the response packet sent back from the TACACS+ server. You can specify from 1 through 30 seconds.

This parameter is set to "5" by default.

Usage example To set 10 seconds for the timeout time.

set auth tacacs server 1 timeout 10

set auth tacacs def_user**[Administrator]**

Function Configure access methods for users for which a user group cannot be identified when using TACACS+ authentication and approval.

Format **set auth tacacs def_user { portusr | normal | none }**

Parameters **{ portusr | normal | none }**

This parameter is set to "portusr" by default.

portusr

Specify "portusr" to handle the users for which a user group cannot be identified (users with the access group that does not match) as port users, and authorize access to all serial ports.

normal

Specify "normal" to handle the users for which a user group cannot be identified (users with the access group that does not match) as normal users.

none

Specify "none" to refuse access to the users for which a user group cannot be identified (users with the access group that does not match).

Usage example To refuse access to users for which a user group cannot be identified.

set auth tacacs def_user none

unset auth radius server addr**[Administrator]**

Function Remove the IP address of the RADIUS authentication server.**Format** **unset auth radius server { 1 | 2 } addr****Parameters** **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the RADIUS authentication server.

Usage example To remove the setting of RADIUS authentication server 1.**unset auth radius server 1 addr**

unset auth radius server portusr**[Administrator]**

Function To remove the port user identifier when using RADIUS authentication.**Format** **unset auth radius server { 1 | 2 } portusr****Parameters** **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the RADIUS authentication server.

Usage example To remove the identifier for port users.**unset auth radius server 1 portusr**

unset auth radius server normal**[Administrator]**

Function To remove the normal user identifier when using RADIUS authentication.**Format** **unset auth radius server { 1 | 2 } normal****Parameters** **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the RADIUS authentication server.

Usage example To remove the identifier for normal users.**unset auth radius server 1 normal**

unset auth radius server root**[Administrator]**

Function To remove the device management user identifier when using RADIUS authentication.**Format** **unset auth radius server { 1 | 2 } root****Parameters** **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the RADIUS authentication server.

Usage example To remove the identifier for device management users.**unset auth radius server 1 root**

unset auth radius server nas_id**[Administrator]**

Function Remove the NAS-ID attribute notified to the RADIUS authentication server.

Format **unset auth radius server { 1 | 2 } nas_id**

Parameters **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the RADIUS authentication server.

Usage example To remove the NAS-ID attribute for the RADIUS authentication server 1.

unset auth radius server 1 nas_id

Explanation (1) The host name is saved in the NAS-ID attribute when this command is executed.

unset auth tacacs server addr**[Administrator]**

Function Remove the IP address of the TACACS+ server (authentication/approval).**Format** **unset auth tacacs server { 1 | 2 } addr****Parameters** **{ 1 | 2 }**
Specify 1 or 2 for the identification number of the TACACS+ server.**Usage example** To remove the setting of TACACS+ server 1.**unset auth tacacs server 1 addr**

delete auth access_group**[Administrator]****Function** Delete access groups and serial port access privileges.**Format** **delete auth access_group { root | normal | portusr port disable_port_list }
{ all | radius filter_id string | tacacs attr string val value }****Parameters** **{ root | normal | portusr port disable_port_list }****root**

Specify "root" to delete the access group of device management users who log in to the NS-2250.

normal

Specify "normal" to delete the access group of normal users who log in to the NS-2250.

portusr port disable_port_list

Specify "portusr" to remove the access privileges for the specified serial ports from the access group of port users who access the serial ports of the NS-2250. When access privileges for all serial ports have been removed from an access group, this access group is deleted.

port disable_port_list

Specify the ports for which the access privileges will be removed in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

The target access group is deleted if you specify all the serial ports.

{ all | radius filter_id string | tacacs attr string val string }**all**

Specify "all" to delete all specified access groups.

radius filter_id string

Specify "radius filter_id string" to delete the specified access groups containing the character string string.

You can specify from 1 through 64 characters for string. You can use half-width alphanumeric characters, underbars "_", hyphens "-", at marks "@", and periods ".".

tacacs attr string val value

Specify "tacacs attr string val string" to delete the access groups containing the specified attribute character string (attr) and the specified value character string (val) pair.

You can specify from 1 through 32 characters for both the "attr" and "val" strings. You can use half-width alphanumeric characters, underbars "_", hyphens "-", at marks "@", and periods ".".

Usage example (1) To delete the access group "admin" of device management users (RADIUS).**delete auth access_group root radius filter_id admin**

(2) To delete the access group "grp1" of port users (RADIUS).

delete auth access_group portusr port 1-32 radius filter_id grp1

(3) To delete only the access privilege for serial port 5 from the port user access group "grp1" (RADIUS).

delete auth access_group portusr port 5 radius filter_id grp1

(4) To delete all port user access groups with access privileges for serial ports 1 to 32 (RADIUS).

delete auth access_group portusr port 1-32 all

(5) To delete the user definition attribute and value pair "grp2=tech1" registered for the access group of port users with access to serial ports 1 to 5 (TACACS+).

delete auth access_group portusr port 1-5 tacacs attr grp2 val tech1

Explanation

(1) When you remove some of the access privileges from a port user group, the valid access privileges are gathered in one command line (there is still one line registered for "create auth access_group").

```
create auth access_group portusr port 1-10 radius filter_id grp1
delete auth access_group portusr port 5-6 radius filter_id grp1
->
create auth access_group portusr port 1-4,7-10 radius filter_id grp1
```

4.29 Accounting setting commands

These are objects managing the operating conditions related to the accounting modes and RADIUS/TACACS+ client accounting.

set acct mode

[Administrator]

Function Set the saving mode for accounting logs.

Format **set acct mode { local | radius | tacacs }**

Parameters **{ local | radius | tacacs }**

This parameter is set to "local" by default.

local

Specify "local" to not save the accounting logs.

radius

Specify "radius" to save the accounting logs in the RADIUS accounting server.

tacacs

Specify "tacacs" to save the accounting logs in the TACACS+ server.

Usage example To save the accounting logs to the RADIUS accounting server.

set acct mode radius

set acct radius retry**[Administrator]**

Function Set the number of times accounting packets are resent to the RADIUS accounting server.

Format **set acct radius retry** *number*

Parameters **retry** *number*

Specify the number of times accounting packets are resent to the RADIUS accounting server. You can specify a number from 0 through 5. Specify "0" to not resend the accounting packets.

This parameter is set to "3" by default.

Usage example To set to 5 the number of times the accounting packets are resent.

set acct radius retry 5

set acct radius auth_deny_stop**[Administrator]**

Function	Set the sending method of accounting STOP packets when user authentication has failed.
Format	set acct radius auth_deny_stop { off remote local all }
Parameters	{ off remote local all } This parameter is set to "remote" by default. off Do not send accounting STOP packet to the RADIUS accounting server even when user local or external authentication has failed. remote Send an accounting STOP packet to the RADIUS accounting server when user external authentication has failed. local Send an accounting STOP packet to the RADIUS accounting server when user local authentication has failed. all Send an accounting STOP packet to the RADIUS accounting server when user local or external authentication has failed. When both local and external authentication failed, the accounting STOP packet is sent twice.
Usage example	To send an accounting STOP packet to the RADIUS accounting server when the user local or external authentication fails. set acct radius auth_deny_stop all

set acct radius server addr**[Administrator]****Function** Set the IP address of the RADIUS accounting server.**Format** **set acct radius server { 1 | 2 } addr** *ipaddr*

Parameters **{ 1 | 2 }**
 Specify 1 or 2 for the identification number of the RADIUS accounting server.

addr *ipaddr*
 Specify the IP address of the RADIUS accounting server.

Usage example To set the RADIUS accounting server 192.168.1.1 as the RADIUS server 1.

set acct radius server 1 addr 192.168.1.1

set acct radius server port**[Administrator]**

Function	Set the accounting port number of the RADIUS accounting server.
Format	set acct radius server { 1 2 } port { 1813 1646 }
Parameters	{ 1 2 } Specify 1 or 2 for the identification number of the RADIUS accounting server. port { 1813 1646 } This parameter is set to "1813" by default. 1813 Set the accounting port number to UDP: 1813. 1646 Set the accounting port number to UDP: 1646.
Usage example	To set "1646" for the accounting port number of RADIUS server 1. set acct radius server 1 port 1646

set acct radius server key**[Administrator]**

Function	Set the secret key of the RADIUS accounting server.
Format	set acct radius server { 1 2 } key { password encrypt string }
Parameters	<p>{ 1 2 } Specify 1 or 2 for the identification number of the RADIUS accounting server.</p> <p>key { password encrypt string } Set the secret key of the RADIUS accounting server. The maximum number of characters that can be set for the secret key is 64.</p> <p>password When the command is executed with the "password" parameter specified, a message prompting you to enter the new secret key is displayed. Enter the new secret key. When you press the Enter key after entering the secret key, a message prompting you to confirm the secret key is displayed. Enter the same secret key again. The secret key is deleted if you only press the Enter key when registering the secret key.</p> <p>encrypt string Specify the secret key to set using the character string after conversion with the hash function.</p>
Usage example	<p>To set the secret key "ABCDEF" to the RADIUS accounting server 1.</p> <pre>set auth radius server 1 key password</pre> <p>Radius Server's password : Enter the secret key "ABCDEF". Retry Radius Server's password : Enter the secret key "ABCDEF". (The entered secret key is not displayed.)</p>
Explanation	Register the same secret key to the NS-2250 as the one registered to the RADIUS accounting server.

set acct radius server timeout**[Administrator]**

Function Set the timeout time for the response packet sent back from the RADIUS accounting server.

Format **set acct radius server { 1 | 2 } timeout *time***

Parameters **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the RADIUS accounting server.

timeout *time*

Set the timeout time for the response packet sent back from the RADIUS accounting server. You can specify from 1 through 30 seconds.

This parameter is set to "5" by default.

Usage example To set 10 seconds for the timeout time.

set acct radius server 1 timeout 10

set acct radius server nas_id**[Administrator]**

Function Register the NAS-ID attribute notified to the RADIUS accounting server.

Format **set acct radius server { 1 | 2 } nas_id string**

Parameters **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the RADIUS accounting server.

nas_id string

Specify the character string to save in the NAS-ID attribute.

You can specify from 1 through 64 characters for string. You can use half-width alphanumeric characters, underbars "_", hyphens "-", at marks "@", and periods ".".

The host name is saved in the NAS-ID attribute if this parameter is omitted.

Usage example To set "SmartCS" in the NAS-ID attribute.

set acct radius server 1 nas_id SmartCS

set acct tacacs auth_deny_stop**[Administrator]**

Function	Set the sending method of accounting STOP packets when TACACS+ authentication or approval has failed.
Format	set acct tacacs auth_deny_stop { off remote local all }
Parameters	{ off remote local all } This parameter is set to "remote" by default. off Do not send accounting STOP packet to the TACACS+ server even when user local or external authentication has failed. remote Send an accounting STOP packet to the TACACS+ server when user external authentication has failed. local Send an accounting STOP packet to the TACACS+ server when user local authentication has failed. all Send an accounting STOP packet to the TACACS+ server when user local or external authentication has failed. When both local and external authentication failed, the accounting STOP packet is sent twice.
Usage example	To send an accounting STOP packet to the TACACS+ server when the user local or external authentication fails.

set acct tacacs auth_deny_stop all

set acct tacacs server addr**[Administrator]**

Function Set the IP address of the TACACS+ server (accounting).**Format** **set acct tacacs server { 1 | 2 } addr *ipaddr*****Parameters** **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the TACACS+ server.

addr *ipaddr*

Specify the IP address of the TACACS+ server.

Usage example To set the TACACS+ server 192.168.1.1 to server 1.**set acct tacacs server 1 addr 192.168.1.1**

set acct tacacs server key**[Administrator]**

Function	Set the secret key of the TACACS+ server (accounting).
Format	set acct tacacs server { 1 2 } key { password encrypt <i>string</i> }
Parameters	<p>{ 1 2 } Specify 1 or 2 for the identification number of the TACACS+ server.</p> <p>key { password encrypt <i>string</i> } Specify the secret key of the TACACS+ server. The maximum number of characters that can be set for the secret key is 64.</p> <p>password When the command is executed with the "password" parameter specified, a message prompting you to enter the new secret key is displayed. Enter the new secret key. When you press the Enter key after entering the secret key, a message prompting you to confirm the secret key is displayed. Enter the same secret key again. The secret key is deleted if you only press the Enter key when registering the secret key.</p> <p>encrypt <i>string</i> Specify the secret key to set using the character string after conversion with the hash function.</p>
Usage example	<p>To set the secret key "ABCDEF" to the TACACS+ server 1.</p> <pre>set acct tacacs server 1 key password</pre> <p>Tacacs+ Server's password : Enter the secret key "ABCDEF". Retry Tacacs+ Server's password : Enter the secret key "ABCDEF". (The entered secret key is not displayed.)</p>
Explanation	(1) Register the same secret key to the NS-2250 as the one registered to the TACACS+ server.

set acct tacacs server timeout**[Administrator]**

Function Set the timeout time for the response packet sent back from the TACACS+ server (accounting).

Format **set acct tacacs server { 1 | 2 } timeout *time***

Parameters **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the TACACS+ server.

timeout *time*

Specify the timeout time for the response packet sent back from the TACACS+ server. You can specify from 1 through 30 seconds.

This parameter is set to "5" by default.

Usage example To set 10 seconds for the timeout time.

set acct tacacs server 1 timeout 10

unset acct radius server addr**[Administrator]**

Function Remove the IP address of the RADIUS accounting server.

Format **unset acct radius server { 1 | 2 } addr**

Parameters **{ 1 | 2 }**
Specify 1 or 2 for the identification number of the RADIUS accounting server.

Usage example To remove the setting of RADIUS accounting server 1.

unset acct radius server 1 addr

unset acct radius server nas_id**[Administrator]**

Function Remove the NAS-ID attribute notified to the RADIUS accounting server.

Format **unset acct radius server { 1 | 2 } nas_id**

Parameters **{ 1 | 2 }**
Specify 1 or 2 for the identification number of the RADIUS accounting server.

Usage example To remove the NAS-ID attribute for the RADIUS accounting server 1.

unset auth radius server 1 nas_id

Explanation (1) The host name is saved in the NAS-ID attribute when this command is executed.

unset acct tacacs server addr**[Administrator]**

Function Remove the IP address of the TACACS+ server (accounting).**Format** **unset acct tacacs server { 1 | 2 } addr****Parameters** **{ 1 | 2 }**

Specify 1 or 2 for the identification number of the TACACS+ server (accounting).

Usage example To remove the setting of TACACS+ server 1.**unset acct tacacs server 1 addr**

4.30 terminal output control setting commands

These are objects used to set terminal output and operation.

set terminal default editing

[Administrator]

Function	Set the default setting for enabling or disabling terminal line editing.
Format	set terminal default editing { enable disable }
Parameters	{ enable disable } Set to enable or disable the editing of command lines using the terminal delete and arrow keys. This parameter is enabled by default. enable Specify "enable" to enable the line editing function. disable Specify "disable" to disable the line editing function.
Usage example	To disable by default the line editing function. set terminal default editing disable
Explanation	The settings made with this command apply to all users. The settings made with this command are enabled from the next login session.

set terminal default height**[Administrator]**

Function	Set the default setting for the number of lines on one page of the terminal.
Format	set terminal default height rows
Parameters	rows Specify the number of lines on one page. You can specify a number from 10 through 256. This parameter is set to "23" by default.
Usage example	To set to 32 the default number of lines on one page. set terminal default height 32
Explanation	The settings made with this command apply to all users. The settings made with this command are enabled from the next login session.

set terminal default width**[Administrator]**

Function	Set the default setting for the number of characters on one line of the terminal.
Format	set terminal default width <i>columns</i>
Parameters	<i>columns</i> Specify the number of characters on one line. You can specify a number from 40 through 256. This parameter is set to "80" by default.
Usage example	To set to 60 the default number of characters on one line. set terminal default width 60
Explanation	The settings made with this command apply to all users. The settings made with this command are enabled from the next login session.

set terminal default page**[Administrator]**

Function	Set the default setting for enabling or disabling the terminal paging function.
Format	set terminal default page { enable disable }
Parameters	{ enable disable } With this command you can enable the paging function that separates the output text into a different page when the text exceeds the specified number of lines per page. Disable the paging function to display the output text continuously. This parameter is enabled by default. enable Specify "enable" to enable the paging function. disable Specify "disable" to disable the paging function.
Usage example	To disable by default the paging function. set terminal default page disable
Explanation	The settings made with this command apply to all users. The settings made with this command are enabled from the next login session.

set terminal default prompt**[Administrator]**

Function	Set the default setting for the display format of the terminal prompt.
Format	set terminal default prompt { device { on off } hostname { on off } time { on off } }
Parameters	<p>{ device { on off } hostname { on off } time { on off } } Specify the default display format of the terminal prompt.</p> <p>device { on off } This parameter is "on" by default.</p> <p>on Specify "on" to display identification information (terminal number, etc.) of the terminal used on the prompt.</p> <p>off Specify "off" not to display identification information (terminal number, etc.) of the terminal used on the prompt.</p> <p>hostname { on off } This parameter is "on" by default.</p> <p>on Specify "on" to display the NS-2250 host name on the prompt.</p> <p>off Specify "off" not to display the NS-2250 host name on the prompt.</p> <p>time { on off } This parameter is "off" by default.</p> <p>on Specify "on" to display the current time on the prompt.</p> <p>off Specify "off" not to display the current time on the prompt.</p>
Usage example	To display the current time on the prompt.
	set terminal default prompt time on
Explanation	<p>The settings made with this command apply to all users.</p> <p>The settings made with this command are enabled from the next login session.</p>

set terminal default redisp**[Administrator]**

Function Set whether or not to redisplay by default the previously entered command string on the next prompt screen after a command input error has occurred.

Format **set terminal default redisp { on | off }**

Parameters **{ on | off }**

Specify "on" to redisplay the command string that caused the error.

Specify "off" not to redisplay the command string that caused the error.

This parameter is "on" by default.

Usage example To set not to redisplay by default the command string.

set terminal default redisp off

Explanation The settings made with this command apply to all users.

The settings made with this command are enabled from the next login session.

set terminal default timeout**[Administrator]**

Function Set the default value for the terminal automatic logout time.

Format **set terminal default timeout { on *time* | off }**

Parameters **{ on *time* | off }**

Specify the default value for the terminal automatic logout time. This setting applies to normal users and device management users who log in to the NS-2250. The user is automatically log out if no operation, such as entering a command, is performed during the specified time.

Specify the timeout time from 1 through 60 minutes if you have specified "on". The unit is one minute. This function runs independently of the Configuration mode or Operation mode.

Specify "off" to set an infinite timeout time so that the users are not automatically logged out.

This parameter is set to "on" by default with a timeout time of 10 minutes.

Usage example To set the default timeout time for automatic logout to 30 minutes.

set terminal default timeout on 30

Explanation The settings made with this command apply to all users.

The settings made with this command are enabled from the next login session.

4.31 Time zone setting commands

set timezone**[Administrator]****Function** Set the time zone.**Format** **set timezone** *string***Parameters** *string*

Specify the name of the time zone.

You can specify a time zone name from the list displayed using the "show timezone list" command.

This parameter is set to "UTC" by default.

Note

- (1) The default setting for this parameter in the startup file is "Tokyo".
- (2) From startup until the settings are imported, the time is displayed using the "UTC" of default.
- (3) It may be necessary to acquire safety standards depending on the country. If you will use the NS-2250 overseas, contact us or your dealer.

Usage example To set the time zone to Hong Kong.**set timezone Hongkong**

4.32 Temperature sensor setting commands

These are objects managing the temperature sensor.

set temperature adjust

[Administrator]

Function Set the temperature correction value of the temperature sensor.

Format **set temperature adjust** *temp*

Parameters *temp*

Set the temperature correction value of the temperature sensor.

The temperature used is the sensor temperature from which the correction value has been subtracted.

You can specify a number from 0 through 20 for the correction value.

This parameter is set to "0" by default.

Usage example To set a correction value of -10 degree Celsius.

set temperature adjust 10

Explanation With the "show temperature" command, both the sensor temperature and the temperature after subtracting the correction value are displayed.

The temperature saved in the SNMP MIB is the temperature after the correction value has been subtracted from the sensor temperature.

When the correction value is set to "0", the temperature obtained from the SNMP MIB is the same as the sensor temperature.

Chapter 5

Status display commands

Chapter 5 describes the status and statistics display commands that can be used on the NS-2250.

5.1 System status display commands

show version

[Normal user][Administrator]

Function Display the system hardware configuration, system software version, boot information, etc.

Format **show version**

Parameters None

Usage example **show version**

Execution example

```
(c)NS-2250> show version
System           : System Software Ver x.x (Build xxxx-xx-xx)
Boot Status      : Power on (xx:xx:xx)
System Up Time   : 20xx/xx/xx xx:xx:xx
Local MAC Address : xx:xx:xx:xx:xx:xx
Number of MAC Address : 2
Model            : NS-2250-xx (xx port)
Serial No.       : xxxxxxxx
BootROM          : Ver x.x
Main Board CPU   : e500v2 (533.333328MHz)
Main Memory      : 1033392 KBytes
Boot System      : main (Ver x.x)
Boot Config      : external startup1
Main System      : Ver x.x
Backup System    : Ver x.x
```

Explanation **System**

Displays information about the system.

Boot Status

Displays information about the booting method.

System Up Time

Displays the time when the system started.

Local MAC Address

Displays the Ethernet address of the NS-2250.

Number of MAC Address

Displays the number of Ethernet address.

Model

Displays the NS-2250 model.

Serial No.

Displays the NS-2250 serial number.

BootROM

Displays the version of the NS-2250 BootROM.

Main Board CPU

Displays the model and the clock rate of the CPU mounted on the main

Main Memory

Displays the capacity of the memory mounted on the main board.

Boot System

Displays the type of the system that has started.

Boot Config

Displays the startup file imported at startup.

Main System

Displays the system software version of the main system.

Backup System

Displays the system software version of the backup system.

show environment

[Normal user][Administrator]

Function Display the information of power and Temperature.**Format** **show environment****Parameters** None**Execution example**

```
(c)NS-2250> show environment
<Environment status>

Power information
  Power unit      : AC
  Power 1         : ON
  Power 2         : OFF
Temperature information
  Current temp    : 31 deg C
  Sensor          : 31 deg C
  Adjust          : 0
```

Explanation**Power information**

Displays the power information.

Power unit

Displays the type of power supply.

AC

AC Power supply

DC

DC Power supply

Power

Displays the status of power supply.

ON

Power on

OFF

Power off

Temperature information

Displays the type of the temperature information.

Current temp

Displays the current temperature. The current temperature is the sensor temperature from which the correction value has been subtracted.

Sensor

Display the temperature of the temperature sensor.

Adjust

Displays the set temperature correction value.

show slot**[Administrator]****Function** Display the USB port information.**Format** **show slot****Parameters** None**Usage example** **show slot****Execution example**

```
(c)NS-2250# show slot
external slot information
device : exist
type   : setup
```

Explanation **device**

Displays the device insertion status.

exist

device inserted

not exist

device not inserted type

type

Displays the type of the inserted device.

setup

setup USB memory

show cpu**[Administrator]****Function** Display the CPU utilization rate.**Format** **show cpu****Parameters** None**Execution example**

```
(c)NS-2250# show cpu
Total Info.      : 22 %
  (System        : 12 %)
  (User          : 10 %)
```

Explanation **Total Info.**

Displays the CPU utilization rate for the entire NS-2250.

System

Displays the CPU utilization rate in kernel space (system).

User

Displays the CPU utilization rate in user space (application).

show memory**[Administrator]****Function** Display the memory usage rate.**Format** **show memory****Parameters** None**Execution example**

```
(c)NS-2250# show memory
Total memory : 127308 Kbytes
Used memory : 9972 Kbytes ( 7%)
```

Explanation **Total memory**

Displays the capacity of the memory equipped in the NS-2250.

Used memory

Displays the amount and percentage (%) of memory currently used.

show log**[Administrator]**

Function	Display the console log or the command execution log.
Format	show log { console command } [{ lines detail }]
Parameters	<p>log { console command } Specify the log to display.</p> <p>console Specify "console" to display the console log.</p> <p>command Specify "command" to display the command execution log.</p> <p>[{ lines detail }]</p> <p><i>lines</i> Specify the number of lines to display from 1 through 1000. The specified number of lines of the most recent log are displayed.</p> <p>detail The entire log recorded in the NS-2250 is displayed if this parameter is omitted.</p>
Usage example	show log console 10

Execution example

```
(c)NS-2250# show log console 10
Jan 23 17:45:42 port_logd: <TTY42> started
Jan 23 17:45:42 port_logd: <TTY43> started
Jan 23 17:45:42 port_logd: <TTY45> started
Jan 23 17:45:42 port_logd: <TTY46> started
Jan 23 17:45:42 port_logd: <TTY47> started
Jan 23 17:45:42 port_logd: <TTY48> started
Jan 23 17:45:43 port_logd: <TTY44> started
Jan 23 17:45:43 ether: port eth1 LINK UP (1000Mbps, FULL-duplex).
Jan 26 10:39:18 port_telnetd: LOGIN BY somebody FROM 172.31.100.67
Jan 26 10:39:18 su: COMMAND(su) invoked by /0
(c)NS-2250#
```

show support**[Administrator]****Function** Command used to display support information.**Format** `show support [{ detail | file { write | info | delete } }]`**Parameters** `[{ detail | file { write | info | delete } }]`**detail**

Displays more detailed information than with the "show support" command and all the logs saved in the NS-2250.

file { write | info | delete }**write**

Support information is saved as a file in RAM. The file which can be saved is one. When a file exists already, it's overwritten.

When NS-2250 is restarted, a support information file is removed.

info

Display date and time when a support information file was saved.

This parameter also indicates a file size.

delete

Delete support information file in RAM.

Execution example

```

(c)NS-2250# show support
===== start of show support =====
Fri Sep 25 20:49:55 JST 2015

===== Version information =====
System           : System Software Ver x.x (Build xxxx-xx-xx)
Boot Status      : Power on (xx:xx:xx)
System Up Time   : 20xx/xx/xx xx:xx:xx
Local MAC Address : xx:xx:xx:xx:xx:xx
Number of MAC Address : 2
Model            : NS-2250-xx (xx port)
Serial No.       : xxxxxxxx
BootROM          : Ver x.x
Main Board CPU   : e500v2 (533.333328MHz)
Main Memory      : 1025216 KBytes
Boot System      : main (Ver x.x)
Boot Config      : external startup1
Main System      : Ver x.x
Backup System    : Ver x.x

===== SYSTEM information =====

show timezone
Timezone is "Tokyo"

ls /etc/localtime
lrwxrwxrwx 1 root root 36 Sep 20 19:56 /etc/localtime -> /usr/share/zoneinfo/p
osix/Asia/Tokyo

lrwxrwxrwx 1 root root 36 Sep 20 19:56 /etc_base/localtime -> /usr/share/zonei
nfo/posix/Asia/Tokyo

```

```
==== Host information ====
Hostname      :NS-2250
IPaddress     :192.0.2.1/24
TcpKeepAlive :180

:
:
:

==== end of show support ====
(c)NS-2250#
```

Explanation The following is displayed with this command.

- Version information
- SYSTEM information
- Host information
- External slot information
- CPU information
- Memory information
- Process information
- Ether port information
- Ether port statistics information
- IP6 information
- IP host information
- IP6 route information
- IP route information
- ipfilter information
- ipsed information
- IP/IP6 statistics information
- DNS information
- ARP/NDP/TCP/UDP information
- User information
- Login User information
- SNMP information
- SNTP information
- Syslog information
- NFS information
- AUTH Access.Group information
- AUTH information
- ACCT information
- TTY information
- TTY stats information
- Logd information
- Portd information
- Portd session information

- Console information
- Console stats information
- Service information
- Allowhost information
- Startup config information
- Running configuration
- system information
- network information
- i2c information
- system profile
- command log
- console log
- boot log
- system log

Note

This command displays the messages displayed at startup, statistical information and other large-volume logs. Therefore, it is more appropriate to execute this command from a Telnet/SSH client connected via a network than via the CONSOLE port, which is configured to a low-speed transmission rate.

Note that the "show support" command can display a maximum of 500 lines for each log. To display the entire logs, execute 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.

Usage example **show support file write**

5.2 Bonding display commands

show bonding

[Normal user][Administrator]

Function Display the bonding information.

Format **show bonding**

Parameters None

Execution example

If the bonding function is disabled.

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

<master bond1 information>
  Status          : ---
  Up Delay Time(sec) : off
```

If the bonding function is enabled.

```
(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 : Thu Mar 10 19:57:17 JST 2016
<slave information>
  interface active status      failure_count
  -----
eth1      *      up           0
eth2             down         0
```

Explanation <bonding information>

Status

Displays the status of the bonding function.

enable

The bonding function is enabled.

disable

The bonding function is disabled.

Mode

Displays the mode of the bonding function.

active-backup

Fault tolerant.

<master bond1 information>

Displays the virtual interface information which is used in bonding function.

Status

Displays the status of master interface.

Up Delay Time(sec)

Displays linkup wait timer.

<slave information>

Displays the physical interface information which belong to master interface.

interface

Name of slave interface.

active

Displays the slave interface which is used in transmission and reception.

status

status of slave interface.

up

The physical link is up,and available.

going back

The physical link is up,but not available because waiting period.

down

The physical link is up,and not available.

failure_count

The number of times that slave interface status changed in down from up.

5.3 Network information display commands

show ether

[Normal user][Administrator]

Function Display information about the NS-2250 LAN port.

Format **show ether** [{ **eth1** | **eth2** | **bond1** }]

Parameters { **eth1** | **eth2** | **bond1** }
Specify the interface of the NS-2250.
The status of all ports is displayed if this parameter is omitted.

Execution example

(c)NS-2250> show ether					
Eth	Link	Nego	Speed	Duplex	MDI

eth1	UP	enable	1000Mb/s	full	mdi
eth2	DOWN	enable	---	---	---
bond1	UP	---	---	---	---

Explanation

Eth

Displays the LAN ports.

Link

Displays the link of LAN ports.

UP

The link is up.

DOWN

The link is down.

Nego

Displays the auto-negotiation setting.

enable

Auto-negotiation is enabled.

disable

Auto-negotiation is disabled.

Speed

Displays the transmission speed.

1000Mb/s

Operates at a speed of 1Gbps.

100Mb/s

Operates at a speed of 100 Mbps.

10Mb/s

Operates at a speed of 10 Mbps.

The link is down.

Duplex

The full duplex/half duplex setting is displayed when auto-negotiation is disabled.

full

Operates in full duplex.

half

Operates in half duplex.

```

---
    The link is down.
MDI
    Displays the connection mode.
mdi
    Operates in mdi mode.
mdix
    Operates in mdix mode.
---
    The link is down.

```

Execution example

```

(c)NS-2250> show ether eth1
Link Status      : UP
Negotiation Mode : enable
Speed            : 1000Mb/s
Duplex           : full
MDI Status       : mdix
Hardware Address : 08:00:83:ff:4c:b2

```

Explanation**Link Status**

Displays the link of LAN ports.

UP

The link is up.

DOWN

The link is down.

Negotiation Mode

Displays the auto-negotiation setting.

enable

Auto-negotiation is enabled.

disable

Auto-negotiation is disabled.

Speed

Displays the transmission speed.

1000Mb/s

Operates at a speed of 1Gbps.

100Mb/s

Operates at a speed of 100 Mbps.

10Mb/s

Operates at a speed of 10 Mbps.

```
---
```

The link is down.

Duplex

The full duplex/half duplex setting is displayed when auto-negotiation is disabled.

full

Operates in full duplex.

half

Operates in half duplex.

The link is down.

MDI Status

Displays the connection mode.

mdi

Operates in mdi mode.

mdix

Operates in mdix mode.

The link is down.

Hardware Address

Displays the hardware address.

show stats ether**[Normal user][Administrator]****Function** Display statistical information about the NS-2250 LAN port.**Format** **show stats ether [{ eth1 | eth2 | bond1 }]****Parameters** **{ eth1 | eth2 | bond1 }**

Specify the interface of the NS-2250.

The statistical information of all ports is displayed if this parameter is omitted.

Execution example

```
(c)NS-2250> show stats ether
```

	<Receive Statistics>		<Transmit Statistics>	
	Frames	Bytes	Frames	Bytes
eth1	1032	96405	34	1844
eth2	0	0	0	0
bond1	1032	96405	34	1844

Explanation **Receive Statistics**

Statistics of receive data

Transmit Statistics

Statistics of transmit data

Frames

Number of frames

Bytes

Number of bytes

Execution example

```
(c)NS-2250> show stats ether eth1
```

Statistics eth1

<Receive Statistics>		<Transmit Statistics>	
Frames	0	Frames	0
Bytes	0	Bytes	0
Errs	0	Errs	0
Drop	0	Drop	0
Fifo	0	Fifo	0
Frame	0	Colls	0
Compressed	0	Compressed	0
Multicast	0	Carrier	0

Explanation **Receive statistics**

Statistics of receive data

Frames

Number of received frames

Bytes

Quantity of received data

Errs

Number of received errors

Drop

Number of discarding errors

Fifo

Number of fifo errors

Frame

Number of framing errors

Compressed

Number of compression errors

Multicast

Number of multicast and broadcast frames

Transmit statistics

Statistics of transmit data

Frames

Number of transmission frames

Bytes

Quantity of transmission data

Errs

Number of transmission errors

Drop

Number of discarding errors

Fifo

Number of fifo errors

Colls

Number of collision errors

Compressed

Number of compression errors

Carrier

Number of carrier errors

show ipinterface

[Normal user][Administrator]

Function Display information about the NS-2250 IP interface.**Format** **show ipinterface****Parameters** None**Execution example**

```
(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 172.31.8.20/16
link fe80::a00:83ff:feff:dede/64
eth2 up 1500 static 2001:db8::100/64
link fe80::a00:83ff:feff:dedf/64
```

Explanation **ifname**

Displays the name of the logical interface.

state

Displays the link state of the interface.

mtu

Displays the MTU value of interface.

attr

Display attribute of address.

static

The address which users set by the "set ipaddr" or "set ip6addr" command.

link

This is the link local address of the IPv6.

address/mask

Displays the IP address and mask value of the interface.

show ip**[Normal user][Administrator]****Function** Display the NS-2250 host name and IP address, and the TCP keepalive time.**Format** **show ip****Parameters** None**Execution example****If the bonding function is disabled.**

```
(c)NS-2250> show ip
Hostname       : NS-2250
TcpKeepAlive   : 180
IPaddress(eth1) : 192.168.0.1/24
IPaddress(eth2) : 10.0.0.2/8
```

If the bonding function is enabled.

```
(c)NS-2250> show ip
Hostname       : NS-2250
TcpKeepAlive   : 180
IPaddress(eth1) : -
IPaddress(eth2) : -
IPaddress(bond1) : 192.168.0.1/24
```

Explanation	Hostname Displays the NS-2250 host name. TcpKeepAlive Displays the current TCP keepalive time. IPaddress(eth1) Displays the IP address of LAN1. IPaddress(eth2) Displays the IP address of LAN2. IPaddress(bond1) Displays the IP address of bond1 interface which is used in bonding function.
--------------------	---

show ip6

[Normal user][Administrator]

Function Display the NS-2250 IPv6 address.**Format** **show ip6****Parameters** None**Execution example****If the bonding function is disabled.**

```
(c)NS-2250> show ip6
IPAddress(eth1) : 2001:db8::100/64
IPAddress(eth2) : 3fff:ffff:ffff:ffff:ffff:ffff:ffff:100/96
```

If the bonding function is enabled.

```
(c)NS-2250> show ip6
IPAddress(eth1) : ---
IPAddress(eth2) : ---
IPAddress(bond1) : 2001:db8::100/64
```

Explanation	IPAddress(eth1) Displays the IPv6 address of LAN1.
	IPAddress(eth2) Displays the IPv6 address of LAN2.
	IPAddress(bond1) Displays the IPv6 address of bond1 interface which is used in bonding function.

show ip host

[Normal user][Administrator]

Function Display a list of the host names and IP addresses registered to the NS-2250.**Format** **show ip host****Parameters** None**Execution example**

```
(c)NS-2250> show ip host
Hostname      IPaddress      Port
-----
host1         192.168.0.100  -
host2         172.16.1.1     8101
host3         172.16.1.1     8102
host100       2001:db8::100  -
```

Explanation **Hostname**

Displays the host names registered to the NS-2250.

IPaddress

Displays the IP addresses of the host names registered to the NS-2250.

Port

Displays the port number set when registered.

A hyphen "-" is displayed if the port number has not been set.

show ip route

[Normal user][Administrator]

Function Display the static routes registered to the NS-2250.**Format** **show ip route****Parameters** None**Execution example**

(c)NS-2250> show ip route						
destination	netmask	gateway	met	iface	status	
192.168.99.0	255.255.255.0	---	0	eth1	-	
192.168.102.0	255.255.255.0	---	0	eth2	-	
0.0.0.0	0.0.0.0	192.168.102.1	0	eth2	inactive	
172.31.0.0	255.255.0.0	192.168.102.1	0	eth2	inactive	
0.0.0.0	0.0.0.0	192.168.99.1	10	eth1	-	

Explanation **destination**

Displays the destination network or host address.

netmask

Displays the destination netmask.

gateway

Displays the IP address of the next hop router.

met

Displays the metric of the static route.

iface

Displays the name of the logical interface.

status

Displays the status of the static route.

inactive

static route is disable.

-

static route is enable.

Note

- When the link state of the logical interface is DOWN, the state of the static route targeted to that logical interface becomes inactive.

show ip6route

[Normal user][Administrator]

Function Display static routes of IPv6 registered in NS-2250.**Format** **show ip6route****Parameters** None**Execution example**

```
(c)NS-2250> show ip6route
destination          gateway                met iface status
-----
2001:db8::/64        ---                    0 eth1  -
3fff:ffff:ffff:ffff::/64 ---                    0 eth2  -
2001:db9::/64        2001:db8::ffff        0 eth1  -
::/0                 3fff:ffff:ffff:ffff::1 0 eth2  inact
::/0                 2001:db8::ffff        10 eth1  -
```

Explanation **destination**

Displays the destination network or host address.

gateway

Displays the IP address of the next hop router.

met

Displays the metric of the static route.

iface

Displays the name of the logical interface.

status

Displays the status of the static route.

inact

static route is disable.

-

static route is enable.

Note

- When the link state of the logical interface is DOWN, the state of the static route targeted to that logical interface becomes inactive.

show tcp

[Normal user][Administrator]

Function Display the status of the TCP session.**Format** **show tcp****Parameters** None**Execution example****When setting "delete ip6"**

```
(c)NS-2250> show tcp
State      SQ RQ LocalAddress RemoteAddress
-----
LISTEN     0 0 0.0.0.0:21 0.0.0.0:*
LISTEN     0 0 0.0.0.0:22 0.0.0.0:*
LISTEN     0 0 0.0.0.0:23 0.0.0.0:*
LISTEN     0 0 0.0.0.0:1402 0.0.0.0:*
LISTEN     0 0 0.0.0.0:8101 0.0.0.0:*
LISTEN     0 0 0.0.0.0:8103 0.0.0.0:*
LISTEN     0 0 0.0.0.0:8104 0.0.0.0:*
LISTEN     0 0 0.0.0.0:8105 0.0.0.0:*
LISTEN     0 0 0.0.0.0:8106 0.0.0.0:*
:
:
```

When setting "create ip6"

```
(c)NS-2250> show tcp
State      SQ RQ LocalAddress RemoteAddress
-----
LISTEN     0 0 0.0.0.0:21 0.0.0.0:*
LISTEN     0 0 :::22 :::*
LISTEN     0 0 :::23 :::*
LISTEN     0 0 :::8101 :::*
LISTEN     0 0 :::8102 :::*
LISTEN     0 0 :::8103 :::*
LISTEN     0 0 :::8104 :::*
LISTEN     0 0 :::8105 :::*
LISTEN     0 0 :::8106 :::*
:
:
```

Explanation **State**

Displays the status of the TCP session.

SQ

Displays the number of datagrams saved in the transmission queue.

RQ

Displays the number of datagrams saved in the reception queue.

LocalAddress

Displays the NS-2250 IP address and TCP port number.

RemoteAddress

Displays the destination host IP address and TCP port number.

show udp

[Normal user][Administrator]

Function Display the status of UDP.**Format** **show udp****Parameters** None**Execution example**

```
(c)NS-2250> show udp
SQ RQ  LocalAddress          RemoteAddress
-----
0  0    0.0.0.0:161                0.0.0.0:*
0  0    0.0.0.0:65514            0.0.0.0:*
```

Explanation **SQ**

Displays the number of datagrams saved in the transmission queue.

RQ

Displays the number of datagrams saved in the reception queue.

LocalAddress

Displays the NS-2250 IP address and UDP port number.

RemoteAddress

Displays the destination host IP address and UDP port number.

show stats ip**[Normal user][Administrator]****Function** Display the IP statistical information.**Format** **show stats ip****Parameters** None**Execution example**

```
(c)NS-2250> show stats ip
<IP statistic information>
  Forwarding Datagrams           0
  Input Datagrams                11302
  Input Discards                 0
  Input Unknown Protocol         0
  Output Datagrams              248
  Output Discards               0

<ICMP statistic information>
  message type           input    output
  -----
  Echo                   1        13
  Echo Reply             11         1
  Destination Unreachable 39        12
  Source Quench          0         0
  Redirect                0         0
  Time Exceeded          9         0
  Parameter Problem       0         0
  Timestamp              0         0
  Timestamp Reply        0         0
  Address Mask Request    0         0
  Address Mask Reply      0         0
  Errors                 0         0
  -----
  Total                  60        26
```

Explanation **IP statistic information****Forwarding Datagrams**

Displays the number of forwarded IP datagrams via IP.

Input Datagrams

Displays the number of received IP datagrams.

Input Discards

Displays the number of datagrams discarded at the time of reception.

Input Unknown Protocol

Displays the number of frames received in an unsupported protocol.

Output Datagrams

Displays the number of sent IP datagrams.

Output Discards

Displays the number of IP datagrams discarded at the time of transmission.

ICMP statistic information**Echo**

Displays the number of sent and received echo request messages.

Echo Reply

Displays the number of sent and received echo response messages.

Destination Unreachable

Displays the number of sent and received messages that do not reach the destination.

Source Quench

Displays the number of sent and received messages that have been suppressed.

Redirect

Displays the number of sent and received messages that have been rerouted.

Time Exceeded

Displays the number of sent and received messages for which the time has been exceeded.

Parameter Problem

Displays the number of sent and received messages with parameter errors.

Timestamp

Displays the number of sent and received time stamp request messages.

Timestamp Reply

Displays the number of sent and received time stamp response messages.

Address Mask Request

Displays the number of sent and received address mask request messages.

Address Mask Reply

Displays the number of sent and received address mask response messages.

Errors

Displays the number of sent and received error messages.

Total

Displays the totals regarding statistical information of received and sent messages.

show stats ip6**[Normal user][Administrator]****Function** Display the IPv6 statistical information.**Format** **show stats ip6****Parameters** None**Execution example**

```
(c)NS-2250> show stats ip6
<IPv6 statistics information>
      input      output
-----
Packets          417      214
Multicast Packets 229       63
Delivers          416      ---
Header Errors      0      ---
Too Big Errors     0      ---
No Routes          0         0
Address Errors     0      ---
Unknown Protocol   0      ---
Truncated Packets  0      ---
Reassemble Reqds   2      ---
Reassemble OKs     1      ---
Reassemble Fails   0      ---
Reassemble Timeout 0      ---
Fragment OKs      ---       1
Fragment Fails     ---       0
Fragment Creates   ---       2
Discards           0         0
```

Explanation **IPv6 statistic information****Packets**

Displays the number of IPv6 packets sent and received.

It also includes IPv6 packets discarded during transmission / reception.

Multicast Packets

Displays the number of IPv6 multicast packets sent and received.

Delivers

Displays the number of IPv6 packets delivered to the upper layer.

Header Errors

Displays the number of IPv6 packets discarded due to IPv6 header error.

Too Big Errors

Displays the number of IPv6 packets discarded due to IPv6 length error.

No Routes

Displays the number of IPv6 packets discarded because there is no route to the destination.

Address Errors

Displays the number of IPv6 packets discarded because the IP address is invalid.

Unknown Protocol

Displays the number of frames received in an unsupported protocol.

Truncated Packets

Displays the number of IPv6 packets discarded due to insufficient length.

Reassemble Reqds

Displays the number of fragments that require reassembly processing.

Reassemble OKs

Displays the number of IPv6 packets successfully reassembled.

Reassemble Fails

Displays the number of failed reassembly processes.

Reassemble Timeout

Displays the number of times the reassembly process failed due to timeout.

Fragment OKs

Displays the number of IPv6 packets successfully fragmented.

Fragment Fails

Displays the number of IPv6 packets that the fragment failed.

Fragment Creates

Displays the number of IP datagram fragments generated as a result of fragmentation.

Discards

Displays the number of IPv6 packets discarded.

Includes IPv6 packets received with the IPv6 communication function disabled.

show stats icmp6

[Normal user][Administrator]

Function Display the ICMPv6 statistical information.**Format** **show stats icmp6****Parameters** None**Execution example**

```
(c)NS-2250> show stats icmp6
<ICMPv6 statistics information>
message type          input      output
-----
Messages              64         100
Destination Unreachables 21         12
Packet Too Bigs        0          0
Time Exceededs         9          0
Parameter Problems     0          0
Echos                  3          6
Echo Replies           6          3
Group Member Queries    0          0
Group Member Responses  0          0
Group Member Reductions 0          0
Router Solicitations    0          0
Router Advertisements   0          0
Neighbor Solicitations  6          24
Neighbor Advertisements 19         15
Redirects               0          0
MLDv2 Reports           0          40
Errors                  0          0
```

Explanation **ICMPv6 statistic information****Messages**

Displays the totals regarding statistical information of received and sent messages.

Destination Unreachables

Displays the number of sent and received messages that do not reach the destination.

Packet Too Bigs

Displays the number of sent and received Too Big messages.

Time Exceededs

Displays the number of sent and received messages for which the time has been exceeded.

Parameter Problems

Displays the number of sent and received messages with parameter errors.

Echo

Displays the number of sent and received echo request messages.

Echo Reply

Displays the number of sent and received echo response messages.

Group Member Queries

Displays the number of sent and received Group Member Queries messages.

Group Member Responses

Displays the number of sent and received Group Member Responses messages.

Group Member Reductions

Displays the number of sent and received Group Member Reductions messages.

Router Solicitations

Displays the number of sent and received Router Solicitation messages.

Router Advertisements

Displays the number of sent and received Router Advertisement messages.

Neighbor Solicitations

Displays the number of sent and received Neighbor Solicitation messages.

Neighbor Advertisements

Displays the number of sent and received Neighbor Advertisement messages.

Redirects

Displays the number of sent and received Redirect messages.

MLDv2 Reports

Displays the number of sent and received MLDv2 Report messages.

Errors

Displays the number of sent and received error messages.

show arp

[Normal user][Administrator]

Function Display the content of ARP entries.**Format** **show arp****Parameters** None**Execution example**

```
(c)NS-2250> show arp
ip-address          mac-address          interface
-----
192.168.1.1         00:11:11:01:22:01    eth1
192.168.1.29        00:11:11:01:22:02    eth1
```

Explanation **ip-address**

Displays the IP address of the host.

mac-address

Displays the Ethernet address of the host.

interface

Displays the name of the corresponding IP interface.

```
show ndp
```

[Normal user][Administrator]

Function	Display the contents the address mapping table used in Neighbor Discovery Protocol(NDP).
-----------------	--

Format show ndp

Parameters None

Execution example

```
(c)NS-2250> show ndp
```

ip6address	mac-address	iface
3fff:ffff:ffff:ffff::116	52:54:00:48:50:fe	eth1
fe80::5054:ff:fe48:50fe	52:54:00:48:50:fe	eth1

Explanation	ip6address
-------------	------------

Displays the IPv6 address of the node.

mac-address

Displays the Ethernet address of the node.

iface

Displays the name of the corresponding IP interface.

show stats tcp**[Normal user][Administrator]****Function** Display TCP statistical information.**Format** **show stats tcp****Parameters** None**Execution example**

```
(c)NS-2250> show stats tcp
<TCP statistic information>
Active Open                0
Passive Open               96
Input Segments             1107
Input Errors               0
Input CSumErrors           0
Output Segments            1332
Output Reset               0
Retransmit Segments        0
Current Established        48
```

Explanation **Active Open**

Displays the number of connection requests made.

Passive Open

Displays the number of connection requests accepted.

Input Segments

Displays the number of received TCP segments.

Input Errors

Displays the number of TCP segments containing errors such as checksum errors.

Input CSumErrors

Displays the number of TCP segments that generated checksum errors at reception.

Output Segments

Displays the number of sent TCP segments.

Output Reset

Displays the number of sent resets.

Retransmit Segments

Displays the number of resent TCP segments.

Current Established

Displays the number of currently established TCP connections.

show stats udp**[Normal user][Administrator]****Function** Display UDP statistical information.**Format** **show stats udp****Parameters** None**Execution example**

```
(c)NS-2250> show stats udp
<UDP statistic information>
  Input Datagrams           3
  Input Errors              0
  Input CSumErrors          0
  Output Datagrams          4
  Port Unreachable          0
```

Explanation **Input Datagrams**

Displays the number of received UDP datagrams.

Input Errors

Displays the number of UDP datagrams that generated errors at reception.

Input CSumErrors

Displays the number of UDP datagrams that generated checksum errors at reception.

Output Datagrams

Displays the number of sent UDP datagrams.

Port Unreachable

Displays the number of UDP datagrams that do not reach the destination port and were discarded.

show dns

[Normal user][Administrator]

Function Display the settings of the NS-2250 DNS client function.**Format** **show dns****Parameters** None**Execution example**

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

No.  DNS Server
-----
1    192.168.0.100
2    3fff:ffff:ffff:ffff::1000
```

Explanation **Local Domain**

Displays the name of the local domain.

DNS Server

Displays the IP address of the primary and Secondary DNS server.

5.4 Ipfiler status display commands

show ipfilter

[Normal user][Administrator]

Function Display the registration status of the ipfilter.

Format **show ipfilter input**

Parameters **input**
Display the filter condition registered for received packets.

Execution example

```
(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 192.168.0.1 192.168.0.24 icmp
3 DROP eth2 0.0.0.0/0 0.0.0.0/0 icmp 8
4 DROP eth2 0.0.0.0/0 0.0.0.0/0 tcp 8101
5 DROP eth2 0.0.0.0/0 0.0.0.0/0 tcp 8140-8148
6 DROP eth1 0.0.0.0/0 0.0.0.0/0 udp
7 DROP bond1 0.0.0.0/0 0.0.0.0/0 udp 123
8 DROP bond1 192.168.0.0/24 192.168.1.0/24 tcp
9 DROP bond1 192.168.0.0/24 192.168.1.0/24 udp 1000-15000
10 DROP * 0.0.0.0/0 0.0.0.0/0 all
```

Explanation **status**

Operating status of the ipfilter object is displayed.

ipfilter preset input table

The filter condition registered automatically by the system is displayed.

ipfilter configurable input table

The registered filter condition is displayed.

num

The line number of the filter condition is displayed.

target

The operation of the registered filter condition is displayed.

ACCEPT

It means this is the filter condition to accept received packets.

DROP

It means this is the filter condition to drop received packets.

in

Display the interface of the registered filter condition.

eth1

Packets which passed through eth1 is specified as a filter condition.

eth2

Packets which passed through eth2 is specified as a filter condition.

bond1

Packets which passed through bond1 is specified as a filter condition.

No interface is specified as a filter condition.

destination

Display the registered destination IP address.

source

Display the registered source IP address.

prot

Display the registered upper protocol than IP.

esp

esp(protocol number = 50) is specified to the upper protocol than IP as a filter condition.

icmp

ICMP(protocol number = 1) is specified to the upper protocol than IP as a filter condition. In the case the type number of ICMP is specified, it is displayed behind "icmp".

tcp

TCP(protocol number = 6) is specified to the upper protocol than IP as a filter condition.

In the case the destination port number is specified, it is displayed behind "tcp".

udp

UDP(protocol number = 17) is specified to the upper protocol than IP as a filter condition.

In the case the destination port number is specified, it is displayed behind "udp".

all

No upper protocol of IP is specified as a filter condition.

show stats ipfilter

[Normal user][Administrator]

Function Display the statistics information of the ipfilter.**Format** **show stats ipfilter input****Parameters** **input**

Display the statistics information of the filter condition registered for received packets.

Execution example

```
(c)NS-2250> show stats ipfilter input
<ipfilter preset input statistic>
      pkts target in      destination      source      prot
      499 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     192.168.0.1    192.168.0.24 icmp
      0  DROP  eth2     0.0.0.0/0      0.0.0.0/0    icmp 8
      0  DROP  eth2     0.0.0.0/0      0.0.0.0/0    tcp  8101
      0  DROP  eth2     0.0.0.0/0      0.0.0.0/0    tcp  8140-8148
      8  DROP  eth1     0.0.0.0/0      0.0.0.0/0    udp
      0  DROP  bond1    0.0.0.0/0      0.0.0.0/0    udp  123
      0  DROP  bond1    192.168.0.0/24 192.168.1.0/24 tcp
      0  DROP  bond1    192.168.0.0/24 192.168.1.0/24 udp  1000-1500
      2  DROP  *        0.0.0.0/0      0.0.0.0/0    all
```

Explanation **ipfilter preset input statistic**

The number of packets which correspond to the filter condition registered automatically by the system is displayed.

ipfilter configurable input statistic

The number of packets which correspond to the registered filter condition is displayed.

pkts

The number of packets which correspond to the filter condition is displayed.

target

The operation the registered filter condition is displayed.

ACCEPT

It means this is the filter condition to accept received packets.

DROP

It means this is the filter condition to drop received packets.

in

Display the interface of the registered filter condition.

eth1

Packets which passed through eth1 is specified as a filter condition.

eth2

Packets which passed through eth2 is specified as a filter condition.

bond1

Packets which passed through bond1 is specified as a filter condition.

No interface is specified as a filter condition.

destination

Display the registered destination IP address.

source

Display the registered source IP address.

prot

Display the registered upper protocol than IP.

esp

esp(protocol number = 50) is specified to the upper protocol than IP as a filter condition.

icmp

ICMP(protocol number = 1) is specified to the upper protocol than IP as a filter condition. In the case the type number of ICMP is specified, it is displayed behind "icmp".

tcp

TCP(protocol number = 6) is specified to the upper protocol than IP as a filter condition.

In the case the destination port number is specified, it is displayed behind "tcp".

udp

UDP(protocol number = 17) is specified to the upper protocol than IP as a filter condition.

In the case the destination port number is specified, it is displayed behind "udp".

all

No upper protocol of IP is specified as a filter condition.

5.5 Isec status display commands

show ipsec secret

[Normal user][Administrator]

Function Display the registration list of apre-shared key used in the IKE.

Format **show ipsec secret**

Parameters None

Execution example

```
(c)NS-2250> show ipsec secret
<secret psk>
id selectors
-----
1.1.2.3
1.1.2.3 100.200.0.10
alice@example.com bob@example.com
(any)
```

Explanation **secret psk**

The registration list of a pre-shared key used in the IKE is displayed.

id selectors

The ID being a selection condition of a pre-shared key is displayed.

show ipsec conn [Normal user][Administrator]

Function Display the information of the connection setting.

Format **show ipsec conn** [connlist]

Parameters **conn** [connlist]
 Display the information of the connection setting.
 [connlist]
 Specify the number of a connection in the range of 1 to 8.
 You can execute a setting of some connections in one command if specifying the number of a connection in the list using a hyphen "-" or comma ",".
 If you omit this parameter, the summary of each connection of all ports in two lines is displayed.

Execution example

```
(c)NS-2250> show ipsec conn
<ipsec connections information>
conn_no : status   left      right
           leftsubnet  rightsubnet  auto
-----
conn_01 : enable   200.1.0.3    1.2.3.4
           192.168.1.0/24  200.0.0.0/8    add (responder)
conn_02 : disable  200.1.0.3    200.0.0.101
           192.168.1.3/32  172.31.0.0/16  start(initiator)
conn_03 : disable  200.1.0.3    200.0.0.203
           192.168.1.3/32  172.31.8.203/32 start(initiator)
conn_04 : enable   200.1.0.3    200.0.0.104
           192.168.1.0/24  172.31.0.0/16  start(initiator)
conn_05 : disable  ---
           ---
conn_06 : disable  ---
           ---
conn_07 : disable  ---
           ---
conn_08 : disable  ---
           ---
```

Explanation **ipsec connections information**

The information of the connection setting is displayed.

conn_no

The connection number is displayed.

status

The status of the connection settings is displayed.

left

The IP address of the security gateway of own side is displayed.

right

The IP address of the security gateway of the opposite side is displayed.

leftsubnet

The network address of own side which communicates under encrypted by using IPsec is displayed.

rightsubnet

The network address of the opposite side which communicates under encrypted by using IPsec is displayed.

auto

The setting whether to initiate a key exchange or respond is displayed.

Execution example

```
(c)NS-2250> show ipsec conn 1
<conn_01>
status      : enable
auto        : add
leftid       : alice@example.com
rightid      : bob@example.com
left         : 200.1.0.3
right        : 1.2.3.4
leftsubnet   : 192.168.1.0/24
rightsubnet  : 200.0.0.0/8
leftsourceip : 192.168.1.3
rightsourceip : ---
keyexchange  : ike
ikelifetime  : 10800
lifetime     : 3600
ike          : aes256-sha1-modp1024
esp          : aes256-sha1
forceencaps  : no
dpdaction    : none
```

Explanation **<conn_XX>**

The connection number is displayed.

status

The status of the connection settings is displayed.

auto

The setting whether to initiate a key exchange or respond is displayed.

leftid

The ID of the security gateway of own side is displayed.

rightid

The ID of the security gateway of the opposite side is displayed.

left

The IP address of the security gateway of own side is displayed.

right

The IP address of the security gateway of the opposite side is displayed.

leftsubnet

The network address of own side which communicates under encrypted by using IPsec is displayed.

rightsubnet

The network address of the opposite side which communicates under encrypted by using IPsec is displayed.

leftsourceip

The source IP address of own side which communicates in the IPsec tunnel is displayed.

rightsourceip

The source IP address of the opposite side which communicates in the IPsec tunnel is displayed.

keyexchange

The version of the IKE protocol is displayed.

ikelifetime

The lifetime of ISAKMP-SA is displayed.

lifetime

The lifetime of IPSEC-SA is displayed.

ike

The encryption algorithm of ISAKMP-SA is displayed.

esp

The encryption algorithm of IPSEC-SA is displayed.

forceencaps

Whether to encapsulate the communication of the IPSEC-SA by UDP always or not is displayed.

dpdaction

Whether to execute DPD or not is displayed.

show ipsec status**[Normal user][Administrator]****Function** Display the information of ISAKMP-SA/IPSEC-SA.**Format** **show ipsec status [detail]****Parameters** **status [detail]**

The information of ISAKMP-SA/IPSEC-SA is displayed.

[detail]

The detail information of ISAKMP-SA / IPSEC-SA is displayed.

If you omit this parameter, the summary of it is displayed.

Execution example

```
(c)NS-2250> show ipsec status
Security Associations (1 up, 0 connecting):
  conn_04[42]: ESTABLISHED 106 minutes ago, 2.1.0.3[2.1.0.3]...2.0.0.4[2.0.0.4]
  conn_04{155}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c4405d52_i df27799d_o
  conn_04{155}:   192.168.1.0/24 === 172.31.0.0/16
```

Explanation **Security Associations**

The information of the established SA is displayed.

(X up, Y connecting)

Regarding the enabled connection setting, each the number of the established SA(X) and being established SA(Y) are displayed.

conn_XX[YY]

The information of ISAKMP-SA generated from the connection number(XX) is displayed. YY is the unique consecutive number of ISAKMP-SA.

The status, the elapsed time from generated, the address of the security gateway of own side and its ID and the address of the security gateway of the opposite side and its ID are displayed.

conn_XX{YY}

The information of IPSEC-SA generated from the connection number(XX) is displayed. YY is the unique consecutive number of IPSEC-SA.

In the line 1, the status, the mode(tunnel), reqid and SPI value of ESP(****_i is the input side, ****_o is the output side) are displayed.

In the line 2, the network information of own side and the opposite side which communicates under encrypted by using IPsec.

Execution example

```
(c)NS-2250> show ipsec status detail
Connections:
  conn_04: 2.1.0.3...2.0.0.4 IKEv1
  conn_04: local: [2.1.0.3] uses pre-shared key authentication
  conn_04: remote: [2.0.0.4] uses pre-shared key authentication
  conn_04: child: 192.168.1.0/24 === 172.31.0.0/16 TUNNEL
Security Associations (1 up, 0 connecting):
  conn_04[42]: ESTABLISHED 106 minutes ago, 2.1.0.3[2.1.0.3]...2.0.0.4[2.0.0.4]
  conn_04[42]: IKEv1 SPIs: d898be3904ad0193_i* 6cc53b53af2eb871_r, pre-shared key
reauthentication in 57 minutes
  conn_04[42]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
  conn_04{155}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c4405d52_i df27799d_o
  conn_04{155}:  AES_CBC_128/HMAC_SHA1_96, 128772 bytes_i (1533 pkts, 1s ago),
```

```
128772 bytes_o (1533 pkts, 1s ago), rekeying in 17 minutes
conn_04{155}: 192.168.1.0/24 === 172.31.0.0/16
```

Explanation**Connections**

The setting information of the enabled connection is displayed.

conn_XX

conn_XX

The setting information of the connection number(XX) is displayed.

In the line 1, the address of the security gateway of own side, the one of the opposite side and the version of IKE protocol are displayed.

In the line 2, ID information of own side and the way of authentication(pre-shared key) are displayed.

In the line 3, ID information of the opposite side and the way of authentication(pre-shared key) are displayed.

In the line 4, the network information of own side and the opposite side which communicates under encrypted by using IPsec in IPSEC-SA and the mode(tunnel) are displayed.

Security Associations

The information of the established SA is displayed.

(X up, Y connecting)

Regarding the enabled connection setting, each the number of the established SA(X) and being established SA(Y) are displayed.

conn_XX[YY]

The information of ISAKMP-SA generated from the connection number(XX) is displayed. YY is the unique consecutive number of ISAKMP-SA.

In the line 1, the status, the elapsed time from generated, the address of the security gateway of own side and the address of the security gateway of the opposite side are displayed.

In the line 2, the version of IKE protocol, the value of SPI(****.i is initiator side, ****.r is responder side), the way of authentication(pre-shared key) and the generated time are displayed.

In the line 3, the encryption algorithm decided in IKE protocol is displayed.

conn_XX{YY}

The information of IPSEC-SA generated from the connection number(XX) is displayed. YY is the unique consecutive number of IPSEC-SA.

In the line 1, the status, the mode(tunnel), reqid and SPI value of ESP(****.i is the input side, ****.o is the output side) are displayed.

In the line 2, the encryption algorithm decided in IKE protocol, the number of bytes of the decrypted received data(the number of the packet, the time from decrypted finally), the number of bytes of the encrypted sent data(the number of the packet, the time from encrypted finally) and the time by rekeying are displayed.

In the line 3, the network information of own side and the opposite side which communicates under encrypted by using IPsec are displayed.

show ipsec spd**[Normal user][Administrator]****Function** Display the information of the security policy database.**Format** **show ipsec spd****Parameters** None**Execution example**

```
(c)NS-2250> show ipsec spd
src 192.168.1.0/24 dst 172.31.0.0/16
    dir fwd priority 289760
src 172.31.0.0/16 dst 192.168.1.0/24
    dir fwd priority 189760
    tmpl src 200.0.0.104 dst 200.1.0.3
        proto esp reqid 1 mode tunnel
src 172.31.0.0/16 dst 192.168.1.0/24
    dir in priority 189760
    tmpl src 200.0.0.104 dst 200.1.0.3
        proto esp reqid 1 mode tunnel
src 192.168.1.0/24 dst 172.31.0.0/16
    dir out priority 189760
    tmpl src 200.1.0.3 dst 200.0.0.104
        proto esp reqid 1 mode tunnel
```

Explanation **src xxx.xxx.xxx.xxx/xx dst xxx.xxx.xxx.xxx/xx**

The source address/destination address of the IP packet to become the condition of the security policy is displayed.

dir fwd priority xxxx

The forwarded IP packet becomes the condition. This does not related to NS-2250 because it does not forward in IP protocol.

dir in priority xxxx

The received IP packet becomes the condition.

dir out priority xxxx

The sent IP packet becomes the condition.

tmpl src xxx.xxx.xxx.xxx dst xxx.xxx.xxx.xxx**proto esp reqid XX mode tunnel**

ESP protocol is distributed to SAD that reqid is XX.

show ipsec sad**[Normal user][Administrator]****Function** Display the information of the security association database.**Format** **show ipsec sad****Parameters** None**Execution example**

```
(c)NS-2250> show ipsec sad
src 200.1.0.3 dst 200.0.0.104
    proto esp spi 0xdf27799d reqid 1 mode tunnel
    replay-window 0 flag af-unspec
    auth-trunc hmac(sha1) 96
    enc cbc(aes)
src 200.0.0.104 dst 200.1.0.3
    proto esp spi 0xc4405d52 reqid 1 mode tunnel
    replay-window 32 flag af-unspec
    auth-trunc hmac(sha1) 96
    enc cbc(aes)
```

Explanation **src XXX.XXX.XXX.XXX dst YYY.YYY.YYY.YYY**

The information of the security association whose source address is XXX.XXX.XXX.XXX and destination address is YYY.YYY.YYY.YYY.

proto esp spi 0xXXXXXXXXX reqid Y mode tunnel

The value of SPI(0xXXXXXXXXX), reqid (Y) and the mode(tunnel) are displayed.

replay-window X flag af-unspec

The replay window(X) and the flag information are displayed.

auth-trunc XXXX(XXX) 96

The authentication algorithm(XXXX(XXX)) and the number of bit(96 bits) are displayed.

enc XXX(XXX)

The cryptographic algorithm(XXX(XXX)) is displayed.

5.6 User status display commands

show user

[Normal user][Administrator]

Function Display a list of created users.

Format `show user [user name]`

Parameters None

Execution example

```
(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)    stored
portusr        portusr(500)   1-48
smartcs        portusr(501)   1-12
```

Explanation **User-Name**

Displays a list of created user names.

Category(Uid)

Displays the group name and the user ID corresponding to each user.

Public-Key

Displays the public key setting of SSH sessions for each user.

The public key is displayed in addition to the above when the user name is specified.

Port-Access-List

Displays a list of serial ports authorized for port users.

Execution example

```
(c)NS-2250> show user somebody
User-Name      :somebody
Category(Uid)  :normal(100)
Port-Access-List:
Public-Key     :
```

Explanation **User-Name**

Displays a list of created user names.

Category(Uid)

Displays the group name and the user ID corresponding to each user.

Port-Access-List

Displays a list of serial ports authorized for port users.

Public-Key

Displays the public key setting of SSH sessions for each user.

The public key is displayed in addition to the above when the user name is specified.

show user login

[Normal user][Administrator]

Function Display a list of currently logged in users.**Format** **show user login****Parameters** None**Execution example**

```
(c)NS-2250> show user login
User-Name      Dev  Login-Time      Idle  Remote-Host
-----
somebody        cons Feb 16 14:17:18 00:03
sshsomebody      0   Feb 16 14:50:15 00:00 fe80::a00:27ff:fe65:b879%eth1
somebody        1   Feb 16 14:51:57 00:01 172.31.1.194
somebody        2   Feb 16 15:03:14 00:00 3fff:ffff:ffff:ffff::1
```

Explanation **User-Name**

Displays the name of the users logged into the NS-2250.

Dev

Displays the name or the number of the NS-2250 device used for connection.

Login-Time

Displays the time when the user logged in.

Idle

Displays the time elapsed from the last operation.

Remote-Host

Displays the IP address or the name of the connected host.

5.7 SNMP status display command

show snmp

[Normal user][Administrator]

Function Display the status of the SNMP agent.

Format show snmp

Parameters None

Execution example

```
(c)NS-2250> show snmp
status          : enable
location        : Tokyo xxx
contact         : xxx@example.com
linktrap        : on
powertrap       : on
authentrap      : off
coldstarttrap   : on
bondingactswtrap : on
dsrtrap(tty1-8) : off off off off off off off off
dsrtrap(tty9-16) : off off off off 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
dsrtrap(tty33-40) : off off off off off off off off
dsrtrap(tty41-48) : off off off off off off off off
--- trap configurations (1 entry) ---
<trap 1>
  manager address : 172.16.1.1
  community       : public
  version         : v1
--- community configurations (1 entry) ---
<community 1>
  community       : public
  manager address : 172.16.1.1
```

Explanation status

Displays the status of the SNMP agent.

location

Displays the location where the device is installed.

contact

Display the administrator contact information.

linktrap

Displays the setting for the sending of link traps.

powertrap

Displays the setting for the sending of power traps.

authentrap

Displays the setting for the sending of authentication failure traps.

coldstarttrap

Displays the setting for the sending of cold start traps.

bondingactswtrap

Displays the setting for the sending of the active port switched traps.

dsrtrap

Displays the setting for the sending of DSR signal traps for each serial port.

trap configurations**manager address**

Displays the IP address of the trap destination SNMP server.

community

Displays the community name of the trap destination.

version

Displays the version of the trap.

community configurations**community**

Displays the community name corresponding to the community number.

manager address

Displays the IP address of the SNMP server.

5.8 SNTP status display command

show sntp

[Normal user][Administrator]

Function Display the status of the SNTP client.

Format **show sntp**

Parameters None

Execution example

```
(c)NS-2250> show sntp
<sntp information>
  status          : enable
  poll interval   : 300
  last sync server : 172.16.1.1

<primary server>
  server address   : 192.168.1.1
  last access time : 2015/04/28 09:44:30
  access result    : NG (ntp server no response)

<secondary server>
  server address   : 172.16.1.1
  last access time : 2015/04/28 09:44:32
  access result    : OK
```

Explanation **status**

Displays the status of the SNTP client.

poll interval

Displays the polling interval of SNTP packets.

last sync server

Displays the time and result of the last access to the SNTP server.

server address

Displays the IP address or host name of the SNTP server.

last access time

Displays the time of the last access to the SNTP server.

access result

Displays the result of the last access to the SNTP server.

5.9 Syslog status display command

show syslog

[Normal user][Administrator]

Function Display the status of the syslog client.**Format** show syslog**Parameters** None**Execution example**

```
(c)NS-2250> show syslog
Syslog Status:enable
```

No.	Syslog Host	Portlog-Facility	Syslog-Facility
1	172.31.1.197	local0	local7
2	172.31.1.210	local0	local1

Explanation **Syslog Status**

Displays the status of the syslog client.

Syslog Host

Displays the IP address of the syslog server.

Portlog-Facility

Displays the port log facility.

Syslog-Facility

Displays the syslog facility.

5.10 NFS status display command

show nfs

[Normal user][Administrator]

Function Display the status of the NFS client function.

Format **show nfs**

Parameters None

Usage example **show nfs**

Execution example

```
(c)NS-2240> 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>
IP address      : ---
Path            : ---
Protocol        : udp
Mount status    : umount
(---)
```

Explanation <NFS information>

Status

Display the status of the NFS client function.

Rotate

Displays the port log rotation on/off setting and interval.

<NFS server X>

IP address

Displays the IP address of the NFS server.

Path

Displays the path of the NFS server where the port logs are saved.

Protocol

Displays the NFS protocol (TCP/UDP).

Mount status

Display the NS-2250 mount status (mount/umount).

Displays (---) when the mounting process finished successfully or was not performed yet.

If an error occurs resulting in the unmount status, the reason is displays in the parentheses.

5.11 Port server status display commands

show portd

[Normal user][Administrator]

Function Display the port server status.

Format `show portd`

Parameters None

Usage example `show portd`

Execution example

```
(c)NS-2250> show portd
auth status      : basic
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      : off
-----
tty Label                                Listen Port                                TimeOut
                                telrw telro sshrw sshro  idle   ro
-----
 1 chiba_makuhari_1                8101  8201  8301  8401    -    -
 2 -                                -      -    -    -    -    -
 3 -                                8103    -    -    -    -    -
 4 fukuoka_2                        8104  8204  8304  8404    -    -
 5 osaka_3                          8105  8205  8305  8405    -    -
 6 tokyo_4                          8106  8206  8306  8406    -    -
:
:
```

Explanation **auth status**

Displays the port user authentication setting used with Telnet access.

connect status

Displays the connection mode to the port server.

direct

Direct mode

select

Select mode

base port number

Displays the Telnet/SSH start port number for port server.

timeout status

idle_timeout

Displays the idle timer setting of the port server.

ro_timeout

Displays the session timer setting of the port server.

menu status

Displays the display method of the port server menu.

auto

Operates according to the port log save function setting.

When the port log save function is enabled, the port server menu is displayed.

When it is disabled, the port server menu is not displayed.

on

The port server menu is always displayed.

off

The port server menu is not displayed.

tty

Displays the serial port number.

Label

Displays the label attached to the serial port.

Listen Port**telrw**

Displays the port number of Telnet Normal mode.

telro

Displays the port number of Telnet Monitoring mode.

sshrw

Displays the port number of SSH Normal mode.

sshro

Displays the port number of SSH Monitoring mode.

TimeOut**idle**

Displays the idle timeout of port server.

ro

Displays the session timeout of port server.

show portd tty**[Normal user][Administrator]****Function** Display the port server setting for each serial port.**Format** **show portd tty****Parameters** None**Execution example**

```
(c)NS-2250> show portd tty
tty label                rw ro session mode  to  brk nl cmd
-----
 1 TS-2910                1  1 both    rw   off -   cr -
 2 TS-2950                1  1 both    rw   off -   cr -
 3 SmartEMT               1  1 both    rw   off -   cr -
 4 -                      1  1 ssh     both off -   cr -
 5 -                      1  1 telnet  ro   off -   cr -
 6 -                      1  1 -       -   off -   cr -
 7 -                      1  1 both    rw   off -   cr -
 8 -                      1  1 both    rw   off -   cr -
 9 -                      1  1 both    rw   off -   cr -
10 -                      1  1 both    rw   off -   cr -
11 -                      1  1 both    rw   off -   cr -
12 -                      1  1 both    rw   off -   cr -
13 -                      1  1 both    rw   off -   cr -
14 -                      1  1 both    rw   off -   cr -
15 -                      1  1 both    rw   off -   cr -
16 -                      1  1 both    rw   off -   cr -
:
:
```

Explanation **tty**

Displays the serial port number.

label

Displays the label of the monitored equipment.

rw

Displays the maximum number of connection sessions.

ro

Displays the maximum number of connection sessions.

session

Displays the connectable sessions.

ssh

Displayed when SSH sessions are authorized.

tel

Displayed when Telnet sessions are authorized.

all

Displayed when both Telnet and SSH sessions are authorized.

-

No authorized.

mode

Displays the available modes.

rw	Displayed when Normal mode(rw) are authorized.
ro	Displayed when Monitoring mode(ro) are authorized.
all	Displayed when both modes are authorized.
-	No authorized.
to	Displays the setting of the session timeout.
on	session timeout is enable.
off	session timeout is disable.
brk	Displays the setting of the NVT break character conversion.
brk	Send the NVT break character.
-	Not send the NVT break character.
nl	Displays the setting of the line feed code conversion.
cr	line feed code change to CR.
lf	line feed code change to LF.
-	Not change the line feed code.
cmd	Displays the hexadecimal code used to return to the NS-2250 port server menu when connected to the monitored equipment.

show portd session

[Normal user][Administrator]

Function Display the status of port server sessions.**Format** **show portd session** [**tty** *ttylist*]**Parameters** [**tty** *ttylist*]

Specify the tty number corresponding to the serial ports to display in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

The status of all ports is displayed if this parameter is omitted.

Usage example **show portd session****Execution example**

```
(c)NS-2250> show portd session
telnet rw : 2   ro : 0
ssh   rw : 1   ro : 0
available session ( telnet only : 77 / ssh only : 77 )

-----
tty   : Label
      Type Login-User      Local      Remote      Session-Limit
-----
tty 1 : -
      rw 1 nsport1        tel:8101  172.31.100.67:37726
                                     RW: 1 / RO: 1

tty 2 : -
      rw 1 nsport2        ssh:8302  3fff:ffff:ffff:ffff::67.43181
                                     RW: 1 / RO: 1

tty 16 : -
      rw 1 nsport3        tel:8116  3fff:ffff:ffff:ffff::67.58826
                                     RW: 1 / RO: 1
```

Explanation **telnet**

Number of Telnet sessions currently accessing the serial ports.

When using Select mode, the session displaying the selection menu is not included.

ssh

Number of SSH sessions currently accessing the serial ports.

When using Select mode, the session displaying the selection menu is not included.

available session

Displays the number of remaining sessions that can connect to the NS-2250.

Number of sessions remaining in the case the future sessions are only Telnet and in the case they are only SSH are displayed.

tty

Displays the serial port number.

Label

Displays the label attached to the serial port.

Session-Limit

Displays the number of sessions that can connect to the port.

Type

Displays the connection mode (rw/ro) and the session number.

Login-User

Displays the names of the port users accessing the NS-2250 port server.

Local

Displays the connection protocol (Telnet/SSH) and the client port number

Remote

Displays the IP address of the client and the destination port number.

show tty

[Normal user][Administrator]

Function Displays the status of the serial ports.**Format** **show tty** [*ttylist*]**Parameters** **tty** [*ttylist*]

Specify the tty number corresponding to the serial ports to display in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

The status of all ports is displayed if this parameter is omitted.

Execution example

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

Explanation **tty**

Displays the serial port number.

baud

Displays the transfer speed of the serial port.

bc

Displays the data bit length for the serial port.

parity

Displays the serial port parity.

st

Displays the stop bit length for the serial port.

flow

Displays the serial port flow control.

dct

Displays the setting of automatic hang up that occurs when there is a change in the DSR signal.

Execution example

```
(c)NS-2250> show tty 1
tty : 1
  baud      : 115200
  bitchar   : 8
  parity    : none
  stop      : 1
```

```
flow      : none
detect_dsr : on
```

Explanation**tty**

Displays the serial port number.

baud

Displays the transfer speed of the serial port.

bitchar

Displays the data bit length for the serial port.

parity

Displays the serial port parity.

stop

Displays the stop bit length for the serial port.

flow

Displays the serial port flow control.

detect_dsr

Displays the setting of the DSR signal transition detection function.

show stats tty

[Normal user][Administrator]

Function Displays the serial ports statistical information.**Format** **show stats tty** [*ttylist*]**Parameters** **tty** [*ttylist*][*ttylist*]

Specify the tty number corresponding to the serial port in the 1 to 48 range.
 The range of ports that you can specify varies depending on the model.
 Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.
 The information for all ports is displayed if this parameter is omitted.

Execution example

```
(c)NS-2250> show stats tty
tty   TX Octets   RX Octets   DSR  CTS  DTR  RTS  CD
-----
  1           0           0   on  off  off   on  off
  2           0           0   on  off  off   on  off
  3           0           0   on   on   on   on   on
  4           0           0   on  off  off   on  off
  5           0           0   on  off  off   on  off
  6           0           0   on  off  off   on  off
  :
  :
```

Explanation **tty**

Displays the serial port number.

TX Octets

Displays the number of sent octets.

RX Octets

Displays the number of received octets.

DSR CTS DTR RTS CD

Displays the current status of signal lines (DSR/CTS/DTR/RTS/CD).

Execution example

```
(c)NS-2250> show stats tty 1
tty : 1
  TX Octets      : 0
  RX Octets      : 0
  Error Parity    : 0
  Error Framing   : 0
  Error Overrun   : 0
  Break Count     : 0
  Status          : DSR:on   CTS:off  DTR:off  RTS:on   CD:on
```

Explanation **tty**

Displays the serial port number.

TX Octets

Displays the number of sent octets.

RX Octets

Displays the number of received octets.

Error Parity

Displays the number of reception parity errors.

Error Framing

Displays the number of reception framing errors.

Error Overrun

Displays the number of reception overrun errors.

Break Count

Displays the number of received reception breaks.

Status

Displays the current status of signal lines (DSR/CTS/DTR/RTS/CD).

show logd

[Normal user][Administrator]

Function Display the port log status of each serial port.**Format** **show logd** [**tty** [*ttylist*]]**Parameters** [**tty** [*ttylist*]][*ttylist*]

Specify the tty number corresponding to the serial ports to display in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to display the port log status of multiple serial ports.

The port log status of all ports is displayed if this parameter is omitted.

Execution example

```
(c)NS-2250> show logd
Log stored in   : RAM
Total Log Size  : 24000 KB (Free 0 KB / Total 24000 KB)
Timestamp       : off, Interval Time : 60 sec
(c)NS-2250>
```

Explanation **Log stored in**

Displays the save destination of the port logs.

Total Log Size

Displays the size of the port logs.

Timestamp

Displays the information of time stamp.

Execution example

```
(c)NS-2250> show logd tty
-----log-----  --output--  -----sendlog-----
tty  log  size lstamp  syslog nfs  intvl ratio  send
-----
  1   on   500   off    off off    60   80  mail
  2   on   500   off    off off    60   80   off
  3   on   500   off    off off    60   80   off
  4   on   500   off    off off    60   80   off
  5   on   500   off    off off    60   80   off
  6   on   500   off    off off    60   80   off
  :
  :
```

Explanation **tty**

Displays the serial port number.

log

Displays the save destination of the port log.

size

Displays the size of the port logs.

lstamp

Displays the setting of login time stamp.

syslog

Displays the syslog output setting of the port log.

nfs

Displays the NFS storage setting of the port log.

intvl

Displays the interval setting of the port log.

ratio

Displays the ratio setting of the port log.

send

Displays the port log transfer method.

Execution example

```
(c)NS-2250> show logd tty 1
tty : 1
  Log : on, size : 500 KB
  Syslog output : off
    Timestamp : off
    Hostname : off
    Label : off
  NFS output : off
  loginstamp : off
  Trigger : Interval : 60 min
           Ratio : 80 %
  SendLog : mail
  FTP server(1) : -
    Auth account : -
  FTP server(2) : -
    Auth account : -
  SMTP server(1) : 172.31.1.197
    Auth account : -
    Mail addr : cs-tarou@example.co.jp
    From addr : portuser@NS-2250 (default)
    Subject : "portlog TTY_01" (default)
    Type : attachment
  SMTP server(2) : -
    Auth account : -
    Mail addr : -
    From addr : portuser@NS-2250 (default)
    Subject : "portlog TTY_01" (default)
    Type : attachment
```

Explanation **tty**

Displays the serial port number.

Log

Displays the size of the saved port log (KByte).

Syslog output

Displays the syslog output setting of the port log.

NFS output

Displays the NFS storage setting of the port log.

loginstamp

Displays the login stamp setting.

Trigger

Displays the condition of port log output to an external server.

Interval

Displays the interval setting of the port log.

Ratio

Displays the ratio setting of the port log.

SendLog

Displays the port log transfer method.

FTP server

Displays the address of the destination FTP server for port log external transfer.

Auth account

Displays the FTP account used when sending the port log.

SMTP server

Displays the address of the destination email server for port log external transfer.

Auth account

Displays the SMTP-Auth account used when sending the port log.

Mail addr

Displays the destination email address for sending the port log.

From addr

Displays the sender email address used when sending the port log.

Subject

Displays the email subject.

Type

Displays the port log sending method.

show stats logd tty**[Normal user][Administrator]****Function** Display the port log statistical information of each serial port.**Format** **show stats logd tty** [*ttylist*]**Parameters** **tty** [*ttylist*][*ttylist*]

Specify the tty number corresponding to the serial ports to display in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to display the port log status of multiple serial ports.

The port log status of all ports is displayed if this parameter is omitted.

Execution example

```
(c)NS-2250> show stats logd
  ---rest---  --result--  -----overflow-----
tty  ratio intvl  exec  last      display  ftp/mail  logsave
-----
  1      0   59    0  -          0          0          0
  2      0   59    0  -          0          0          0
  3      0   59    0  -          0          0          0
  4      0   59    0  -          0          0          0
  5      0   59    0  -          0          0          0
  6      0   59    0  -          0          0          0
  :
  :
```

Explanation **tty**

Displays the port number of the serial port.

ratio

Displays the current log usage rate.

intvl

Displays the remaining time for the interval timer.

exec

Displays the number of FTP/email executions result.

last

Displays the number of FTP/email last result.

display

Displays the number of overflow bytes in screen display.

ftp/mail

Displays the number of overflow bytes in FTP/email sending.

logsave

Displays the number of overflow bytes in the "logsave" command.

Execution example

```
(c)NS-2250> show stats log tty 1
tty : 1
  Overflow Display : 0 byte
```

```

          FTP/MAIL : 0 byte
          Save      : 0 byte
Log ratio      : 0 %
Interval rest  : 18 min
FTP/MAIL exec  : 0, Last return : -
(c)NS-2250>

```

Explanation **tty**

Displays the port number of the serial port.

Overflow Display

Displays the number of overflow bytes in screen display.

FTP/MAIL

Displays the number of overflow bytes in FTP/email sending.

Save

Displays the number of overflow bytes in the "logsave" command.

Log ratio

Displays the current log usage rate.

Interval rest

Displays the remaining time for the interval timer.

FTP/MAIL exec

Displays the number of FTP/email executions and the last result.

5.12 CONSOLE port status display command

show console

[Normal user][Administrator]

Function Display the CONSOLE port status.**Format** **show console****Parameters** None**Execution example**

```
(c)NS-2250> show console
Baud      : 9600
BitChar   : 8
Parity    : none
Stop      : 1
Flow      : xon
```

Explanation **Baud**

Displays the transfer speed of the CONSOLE port.

BitChar

Displays the data bit length for the CONSOLE port.

Parity

Displays the CONSOLE port parity.

Stop

Displays the stop bit length for the CONSOLE port.

Flow

Displays the CONSOLE port flow control.

show stats console**[Normal user][Administrator]****Function** Display the CONSOLE port statistical information.**Format** **show stats console****Parameters** None**Execution example**

```
(c)NS-2250> show stats console
<Console information>
-----
Receive Bytes           2056
Transmit Bytes          89715
Parity Errors            0
Framing Errors           0
Overrun Errors           0
Break Count              0
Status                  RTS|CTS|DTR|DSR
```

Explanation **Receive Bytes**

Displays the number of received octets.

Transmit Bytes

Displays the number of sent octets.

Parity Errors

Displays the number of reception parity errors.

Framing Errors

Displays the number of reception framing errors.

Overrun Errors

Displays the number of reception overrun errors.

Break Count

Displays the number of reception breaks.

Status

Displays the signal lines currently on (DSR/CTS/DTR/RTS/CD).

5.13 Display command for the internal management servers

show service

[Normal user][Administrator]

Function Display status of internal management servers.

Format `show service`

Parameters None

Execution example

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

<sshd>
  status   : enable
  port     : 22
  auth     : basic
  host_key : device_depend

<ftpd>
  status   : enable
```

Explanation **telnetd**

Displays the status of Telnet server.

status

Displays the Telnet server setting.

port

Displays the reception port number of Telnet server.

sshd

Displays the status of SSH server.

status

Displays the SSH server setting.

port

Displays the reception port number of SSH server.

auth

Displays the SSH server authentication method.

host_key

Displays the seed value into which a key for host authentication is formed.

ftpd

Displays the status of FTP server.

status

Displays the FTP server setting.

5.14 Display command for the list of hosts and services authorized for connection

show allowhost

[Normal user][Administrator]

Function Display a list of hosts and services authorized for connection.
The following command is categorized under this group.

Format **show allowhost**

Parameters None

Execution example

(c)NS-2250> show allowhost		
Service	Address/Mask	Access tty List

ftpd	10.0.0.0/16	-
portd/sshrw	10.0.0.0/16..	1,3,5,7
portd/sshrw	2001::/16	1-16
portd/telro	all	all
portd/telrw	2001::/16	10,12,14,16
portd/telrw	10.0.0.0/16	all
sshd	all	-
telnetd	all	-

Explanation **Service**

Displays the services authorized for connection.

The following services are available.

telnetd

Telnet server

sshd

SSH server

ftpd

FTP server

portd/telrw

Port server (Telnet Normal mode)

portd/telro

Port server (Telnet Monitoring mode)

portd/sshrw

Port server (SSH Normal mode)

portd/sshro

Port server (SSH Monitoring mode)

Address/Mask

Displays the host or network addresses corresponding to the authorized services.

Access tty List

Displays a list of serial ports authorized for connection.

5.15 Setting file display commands

show config

[Administrator]

Function Display the NS-2250 current settings.

Format **show config**

[running

[{ all | acct | auth | bonding | console | dns | ether |

ip [{ host | route }] | ip6 | ip6route | ipinterface | ipfilter |

ipsec | logd | maintenance | nfs | portd | service | snmp | sntp |

syslog | system | temperature | terminal | tty | user }]]

Parameters **running**

Specify "running" to display the NS-2250 settings currently running (running configuration).

[{ all | acct | auth | bonding | console | dns | ether | ip [{ host | route }] | ip6 | ip6route | ipinterface | ipfilter | ipsec | logd | maintenance | nfs | portd | service | snmp | sntp | syslog | system | temperature | terminal | tty | user }]]

Select a further category to display only the settings corresponding to that category.

The whole running configuration is displayed if this parameter is omitted.

all

Display all settings.

acct

Display the accounting method and the RADIUS accounting client settings.

auth

Display the authentication method and the RADIUS authentication client settings.

bonding

Display the configuration of the bonding function.

console

Display the console settings.

dns

Display the DNS client settings.

ether

Display the Ethernet settings.

ip

Display the IP settings.

ip host

Display the IP host settings.

ip route

Display the IP route settings.

ip6

Display the IPv6 settings.

ip6route

Display the IPv6 route settings.

ipinterface

Display the IP interface settings.

ipfilter

Display the IP filter settings.

ipsec

Display the configuration of the IPsec.

logd

Display the port log settings.

maintenance

Display the configuration of the maintenance function.

nfs

Display the NFS settings.

portd

Display the port server settings.

service

Display the service settings.

snmp

Display the SNMP agent settings.

sntp

Display the SNTP client settings.

syslog

Display the syslog client settings.

system

Display the system settings.

temperature

Display the temperature settings.

terminal

Display the terminal settings.

tty

Display the TTY port settings.

user

Display the user settings.

Execution example

```
(c)NS-2250# show config running ip
#
echo "IP configuration..."
#
set hostname NS-2250
set ipaddr eth1 192.168.1.1/24
set tcpkeepalive 360
#
```

show config startup**[Administrator]****Function** Display the content of the startup files.**Format** **show config startup** [*config-number* [{ **internal** | **external** }]]**Parameters** [*config-number* [{ **internal** | **external** }]]

The content of the startup file selected when the NS-2250 starts is displayed if this parameter is omitted.

config-number

Specify the number (1 to 4) of the startup file to display.

[{ **internal** | **external** }]

Specify "internal" to display the content of the startup file saved inside the NS-2250.

Specify "external" to display the content of the startup file saved in the USB memory.

Execution example

```
(c)NS-2250# show config startup 4
=== show external startup4 ===

#
echo "SYSTEM configuration..."
#
set timezone Tokyo
#
#
echo "IP configuration..."
#
set hostname NS-2250
set ipaddr eth1 172.31.3.97/16
set ipaddr eth2 192.168.254.1/24
#
#
echo "User configuration..."
#
create user setup group setup uid 198
set user setup sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApH5FigT/SLbGEM3n6Qs5s
qUJYq4V08CTK09bZPA+oTnRPnS372FB5l3XZBuz3KMl9PoGr/diWW/h9c/wmveupz8E9bYQWzShIsAL
iNo5aSI9u0rS
create user log group log uid 200
create user somebody group normal uid 100
:
:
```

Explanation The NS-2250 has four startup files in the USB memory and internal memory.

show config info**[Administrator]****Function** Display information related to the startup files.**Format** **show config info****Parameters** None**Execution example**

```
(c)NS-2250# show config info
boot startup : external startup1

internal startup files
name          date          size  default
-----
startup1      May 2  03:59      411   *
startup2      May 2  03:59      411
startup3      May 2  03:59      411
startup4      May 2  03:59      411

external startup files
name          date          size  default
-----
startup1      May 1  14:48     8302   *
startup2      Apr 28 09:58     9284
startup3      Apr 23 20:50      411
startup4      Apr 24 10:06     8496
```

Explanation **boot startup**

Displays the startup file imported at startup.

internal startup files

Displays the information of internal startup file.

external startup files

Displays the information of external startup file (USB memory).

name

Displays the filename.

date

Displays the date and time of the file.

size

Displays the file size. The unit is a byte.

default

"*" is shown to the startup file set as default.

5.16 Terminal setting information display command

show terminal

[Normal user][Administrator]

Function Display the settings of the used terminal.

Format **show terminal**

Parameters None

Execution example

```
(c)NS-2250> show terminal
timeout          : off
width            : 80
height          : 23
page            : disable
editing         : enable
redisp          : on
prompt device   : off
prompt hostname : on
prompt time     : off
```

Explanation **timeout**

Timeout time for automatic logout.

width

Maximum number of characters per line.

height

Number of lines per page.

page

Paging function setting (enable/disable).

editing

Line editing function setting (enable/disable).

redisp

Setting (on/off) for character string redisplay after an input error.

prompt device

Prompt display setting (on/off) for terminal information.

prompt hostname

Prompt display setting (on/off) for NS-2250 host name.

prompt time

Prompt display setting (on/off) for current time.

5.17 Authentication/accounting function display commands

show auth**[Normal user][Administrator]****Function** Display the user authentication method.**Format** **show auth****Parameters** None**Execution example**

```
(c)NS-2250> show auth
<auth information>
  Mode           : radius
  su_cmd username : root
```

Explanation **Mode**

Display the user authentication method.

local

Use NS-2250 local authentication for user authentication.

radius

Use NS-2250 local authentication and RADIUS authentication for user authentication.

tacacs

Use NS-2250 local authentication and TACACS+ authentication for user authentication.

su_cmd username

User name used for external authentication with RADIUS or TACACS+ servers when executing the "su" command.

show auth radius**[Normal user][Administrator]****Function** Display the RADIUS authentication client settings.**Format** **show auth radius****Parameters** None**Usage example** **show auth radius****Execution example**

```
(c)NS-2250> show auth radius
<auth radius information>
  Retry      : 3
  Default User : portusr

<radius server 1>
  IP address      : 172.31.1.197
  Port number     : 1812
  Password        : stored
  Timeout         : 5
  NAS_ID          : smartcs
  Attribute of portusr : ---
  Attribute of normal : ---
  Attribute of root  : ---

<radius server 2>
  IP address      : 172.31.100.67
  Port number     : 1812
  Password        : stored
  Timeout         : 5
  NAS_ID          : smartcs
  Attribute of portusr : ---
  Attribute of normal : ---
  Attribute of root  : ---
```

Explanation **<auth radius information>**

Display the RADIUS authentication settings.

Retry

Displays the number of retries for sending the RADIUS authentication packet.

Default User

Displays the access method for users for which a user group cannot be identified (access group or "filter_id_head" setting does not match).

<radius server>**IP address**

Displays the IP address of the RADIUS authentication server.

Port number

Displays the port number of the RADIUS authentication server.

Password

Display the secret key setting of the RADIUS authentication server.

Timeout

Displays the timeout time for the RADIUS authentication server. The unit is one second.

NAS_ID

This is the NAS-ID attribute notified to the RADIUS authentication server.
When "---" is displayed, the NS-2250 host name is automatically saved in the NAS-ID attribute.

Attribute of portusr

Displays the attribute identifier for port users.

Attribute of normal

Displays the attribute identifier for normal users.

Attribute of root

Displays the attribute identifier for device management users.

show auth tacacs**[Normal user][Administrator]****Function** Display the settings for TACACS+ authentication and approval.**Format** **show auth tacacs****Parameters** None**Usage example** **show auth tacacs****Execution example**

```
(c)NS-2250> show auth tacacs
<auth tacacs+ information>
  Default User : none
  Service Name : smartcs

<tacacs+ server 1>
  IP address      : 10.1.1.1
  Port number     : 49
  Password        : stored
  Timeout         : 5

<tacacs+ server 2>
  IP address      : 192.168.100.1
  Port number     : 49
  Password        : stored
  Timeout         : 5
```

Explanation**<auth tacacs+ information>**

Display the settings for TACACS+ authentication and approval.

Default User

Displays the access method for users for which a user group cannot be identified (access group setting does not match).

Service Name

Displays the service name of the TACACS+ server.

<tacacs+ server>**IP address**

Displays the IP address of the TACACS+ server.

Port numberDisplays the port number of the TACACS+ server.
The port number is fixed to TCP 49.**Password**

Display the secret key setting of the TACACS+ server.

Timeout

Displays the timeout time for the TACACS+ server. The unit is one second.

show auth access_group

[Normal user][Administrator]

Function	Display the access group setting information.
Format	show auth access_group [{ root normal portusr [port [<i>enable_port_list</i>]] attr <i>string</i> }]
Parameters	<p>[{ root normal portusr [port [<i>enable_port_list</i>]] attr <i>string</i> }]</p> <p>The settings of all access groups (normal users, device management users, and port users) are displayed when this parameter is omitted.</p> <p>root</p> <p>Display the settings of device management user access groups.</p> <p>normal</p> <p>Display the settings of the normal user access groups.</p> <p>portusr [port [<i>enable_port_list</i>]]</p> <p>Display the settings of the access group for port user. Specify only "portusr" to display the settings of port user access groups in the alphabetic order.</p> <p>port [<i>enable_port_list</i>]</p> <p>Display the settings of the access groups for the specified serial ports. Specify the numbers of the ports to display in the 1 to 48 range. The range of ports that you can specify varies depending on the model. Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command. Moreover, specify only "port" to display the settings of port user access groups in the order of serial port numbers.</p> <p>attr <i>string</i></p> <p>Display the settings of the access groups specified with string. You can specify from 1 through 64 characters for string. You can use half-width alphanumeric characters, underbars "_", hyphens "-", at marks "@", and periods ".".</p>

Execution example

[When using RADIUS]

```
(c)NS-2250> show auth access_group
Protocol   : Radius
Attribute  : Filter-ID
-----
<root>
  attr : admin
  attr : bbbb
  attr : root
-----
<normal>
  attr : aaaa
  attr : normal
-----
<portusr>
  attr : portusr
  port : 1-48
  attr : smartcs
  port : 1-32
```

[When using TACACS+]

```
(c)NS-2250> show auth access_group
```

```
Protocol   : Tacacs+
```

```
Attribute  : UserSpecific
```

```
-----
```

```
<root>
```

```
    attr_val : grp=admin
```

```
    attr_val : grp=manager
```

```
-----
```

```
<normal>
```

```
    attr_val : grp=general
```

```
-----
```

```
<portusr>
```

```
    attr_val : grp=grp1
```

```
        port : 1-10
```

```
    attr_val : grp=grp2
```

```
        port : 21-32
```

```
    attr_val : grp=grp3
```

```
        port : 21-32
```

Explanation

Protocol

Displays the set authentication protocol.

Attribute

Displays the attribute used for user group identification.

Filter-Id

The attribute is "Filter-Id" when using RADIUS.

User Specific(Attribute Value Pair)

The user specific pair (attribute value pair) can be freely defined by the device administrator.

<root>

Displays the user group of management user.

<normal>

Displays the user group of normal user.

<portusr>

Displays the user group of port user.

attr

Displays the registered access group name.

When using RADIUS, the attribute name freely defined by the device administrator are displayed.

attr_val

Displays the registered access group name.

When using TACACS+, the attribute name and value pair freely defined by the device administrator are displayed in the following format: attribute=value.

port

Displays the serial ports authorized for access.

Execution example

[When using RADIUS]

```
(c)NS-2250> show auth access_group portusr port 1
```

```
Protocol   : Radius
```

```
Attribute : Filter-ID
Category  : portusr
```

```
-----
port : 1
  attr : portusr
  attr : smartcs
```

[When using TACACS+]

```
(c)NS-2250> show auth access_group portusr port 1
Protocol :Tacacs+
Attribute : UserSpecific (Attribute Value Pair)
Category :portusr
-----
port : 1
  attr_val : grp=grp1
  attr_val : grp=grp2
```

Explanation	Protocol Displays the set authentication protocol.
	Attribute Displays the attribute used for user group identification.
	Filter-Id The attribute is "Filter-Id" when using RADIUS.
	User Specific(Attribute Value Pair) The user specific pair (attribute value pair) can be freely defined by the device administrator.
	Category Displays the user group.
	root Displays the user group of management user.
	normal Displays the user group of normal user.
	portusr Displays the user group of port user.
	port Display the settings of the access groups for the serial ports.
	attr Displays the registered access group name. When using RADIUS, the attribute name freely defined by the device administrator are displayed.
	attr_val Displays the registered access group name. When using TACACS+, the attribute name and value pair freely defined by the device administrator are displayed in the following format: attribute=value.

Execution example

[When using RADIUS]

```
(c)NS-2250> show auth access_group attr smartcs
Protocol : Radius
```

```
Attribute : Filter-ID
```

```
-----
<portusr>
  attr : smartcs
  port : 1-32
```

[When using TACACS+]

```
(c)NS-2250> show auth access_group attr grp
Protocol :Tacacs+
Attribute : UserSpecific (Attribute Value Pair)
-----
<portusr>
  attr_val : grp=grp1
  port : 1-10
```

Explanation

Protocol

Displays the set authentication protocol.

Attribute

Displays the attribute used for user group identification.

Filter-Id

The attribute is "Filter-Id" when using RADIUS.

User Specific(Attribute Value Pair)

The user specific pair (attribute value pair) can be freely defined by the device administrator.

<root>

Displays the user group of management user.

<normal>

Displays the user group of normal user.

<portusr>

Displays the user group of port user.

attr

Displays the registered access group name.

When using RADIUS, the attribute name freely defined by the device administrator are displayed.

attr_val

Displays the registered access group name.

When using TACACS+, the attribute name and value pair freely defined by the device administrator are displayed in the following format: attribute=value.

port

Displays the serial ports authorized for access.

show stats auth radius

[Normal user][Administrator]

Function Display the statistical information of RADIUS authentication client.**Format** **show stats auth radius****Parameters** None**Execution example**

```
(c)NS-2250> show stats auth radius
<auth radius statistics>
Id IP address          Send  Rcv_Allow  Rcv_Deny  Rcv_Error  Timeout
-----
1 172.31.1.197          12     12         0         0         0
2 172.31.100.67         0      0          0         0         0
```

Explanation**Id**

Displays the identification number of the RADIUS authentication server.

IP address

Displays the IP address of the RADIUS authentication server.

Send

Displays the number of authentication request packets sent by the RADIUS client.

Rcv_Allow

Displays the number of authentication accepted packets received by the RADIUS client.

Rcv_Deny

Displays the number of authentication denied packets received by the RADIUS client.

Rcv_Error

Displays the number of error packets received by the RADIUS client.

Timeout

Displays the number of RADIUS authentication timeout events.

show stats auth tacacs**[Normal user][Administrator]****Function** Displays TACACS+ statistical information.**Format** **show stats auth tacacs [detail]****Parameters** **[detail]**

Displays the detail of TACACS+ statistical information.

The outline of TACACS+ statistical information is displayed if this parameter is omitted.

Execution example

```
(c)NS-2250> show stats auth tacacs
<authentication tacacs+ statistics>
Id IP address          Send  Rcv_Allow  Rcv_Deny  Rcv_Error  Timeout
-----
 1 10.1.1.1             24      12         3          0          9
 2 ---                  0         0          0          0          0

<authorization tacacs+ statistics>
Id IP address          Send  Rcv_Allow  Rcv_Deny  Rcv_Error  Timeout
-----
 1 10.1.1.1             12      9          2          0          1
 2 ---                  0         0          0          0          0
```

Explanation **<authentication tacacs+ statistics>**

Displays the authentication statistics of the TACACS+ server.

<authorization tacacs+ statistics>

Displays the authorization statistics of the TACACS+ server.

Id

Displays the identification number of the TACACS+ server.

IP address

Displays the IP address of the TACACS+ server.

Send

Displays the number of sent TACACS+ authentication/approval request packets.

Rcv_Allow

Displays the number of received TACACS+ authentication/approval accepted packets.

Rcv_Deny

Displays the number of received TACACS+ authentication/approval denied packets.

Rcv_Error

Displays the number of received TACACS+ authentication/approval error packets.

Timeout

Displays the number of TACACS+ authentication/approval timeout events.

Execution example

```
(c)NS-2250> show stats auth tacacs detail
<authentication tacacs+ statistics>
```


Id	1	2
IP address	10.1.1.1	---

Connection_OK	1	0
Connection_NG	0	0
Send_Start	1	0
Send_Start_NG	0	0
Send_Continue	1	0
Send_Continue_NG	0	0
Recv_Pass	1	0
Recv_GetUser	0	0
Recv_GetPass	1	0
Recv_Fail	0	0
Recv_GetData	0	0
Recv_Restart	0	0
Recv_Error	0	0
Recv_Follow	0	0
Recv_LengthErr	0	0
Recv_SeqNoErr	0	0
Recv_SeqNoLimit	0	0
Recv_Illegal	0	0
Timeout	0	0
<authorization tacacs+ statistics>		
Id	1	2
IP address	10.1.1.1	---

Connection_OK	1	0
Connection_NG	0	0
Send_Request	1	0
Send_NG	0	0
Recv_PassAdd	1	0
Recv_PassReplace	0	0
Recv_Fail	0	0
Recv_Error	0	0
Recv_Follow	0	0
Recv_LengthErr	0	0
Recv_SeqNoErr	0	0
Recv_Illegal	0	0
Timeout	0	0

Explanation <authentication tacacs+ statistics>

Displays the authentication statistics of the TACACS+ server.

Id

Displays the identification number of the TACACS+ server.

IP address

Displays the IP address of the TACACS+ server.

Connection_OK

Number of successfully established connections.

Connection_NG

Number of connection failures.

Send_Start

Number of times SEND_START has been sent.

Send_Start_NG

Number of SEND_START transmission failures.

Send_Continue

Number of times SEND_CONTINUE has been sent.

Send_Continue_NG

Number of SEND_CONTINUE transmission failures.

Recv_Pass

Number of times the TAC_PLUS_AUTHEN_STATUS_PASS

AUTHEN_REPLY packet has been received.

The authentication is successful when you received this packet.

Recv_GetUser

Number of times the TAC_PLUS_AUTHEN_STATUS_GETUSER

AUTHEN_REPLY packet has been received.

Recv_GetPass

Number of times the TAC_PLUS_AUTHEN_STATUS_GETPASS

AUTHEN_REPLY packet has been received.

Recv_Fail

Number of times the TAC_PLUS_AUTHEN_STATUS_FAIL

AUTHEN_REPLY packet has been received.

Recv_GetData

Number of times the TAC_PLUS_AUTHEN_STATUS_GETDATA

AUTHEN_REPLY packet has been received.

Recv_Restart

Number of times the TAC_PLUS_AUTHEN_STATUS_RESTART

AUTHEN_REPLY packet has been received

Recv_Error

Number of times the TAC_PLUS_AUTHEN_STATUS.ERROR

AUTHEN_REPLY packet has been received

Recv_Follow

Number of times the TAC_PLUS_AUTHEN_STATUS.FOLLOW

AUTHEN_REPLY packet has been received

Recv_LengthErr

Number of received packets with an invalid length.

Recv_SeqNoErr

Number of received packets with an invalid sequence number.

Recv_SeqNoLimit

Number of received packets with a sequence number exceeding the maximum value (10)

Recv_Illegal

Number of received packets which are not prescribed Authentication_reply packets.

Timeout

Number of timeout events.

<authorization tacacs+ statistics>

Displays the authorization statistics of the TACACS+ server.

Connection_OK

Number of successfully established connections.

Connection_NG

Number of connection failures.

Send_Request

Number of times SEND_REQUEST has been sent.

Send_NG

Number of SEND_REQUEST transmission failures.

Recv_PassAdd

Number of times the TAC.PLUS.AUTHOR.STATUS.PASS.ADD
AUTHOR_RESPONSE packet has been received
The approval is successful when you received this packet.

Recv_PassReplace

Number of times the TAC.PLUS.AUTHOR.STATUS.PASS.REPL
AUTHOR_RESPONSE packet has been received

Recv_Fail

Number of times the TAC.PLUS.AUTHOR.STATUS.FAIL
AUTHOR_RESPONSE packet has been received

Recv_Error

Number of times the TAC.PLUS.AUTHOR.STATUS.ERROR
AUTHOR_RESPONSE packet has been received

Recv_Follow

Number of times the TAC.PLUS.AUTHOR.STATUS.FOLLOW
AUTHOR_RESPONSE packet has been received

Recv_LengthErr

Number of received packets with an invalid length.

Recv_SeqNoErr

Number of received packets with an invalid sequence number.

Recv_Illegal

Number of received packets which are not prescribed Authorization_response
packets.

Timeout

Number of timeout events.

show acct**[Normal user][Administrator]****Function** Display the account saving method.**Format** **show acct****Parameters** None**Usage example** **show acct****Execution example**

```
(c)NS-2250> show acct
<acct information>
Mode : radius
```

Explanation **Mode****local**

Accounts are not sent.

radius

Accounts are sent to a RADIUS accounting server.

tacacs

Accounts are sent to a TACACS+ server.

show acct radius**[Normal user][Administrator]****Function** Display the RADIUS accounting client settings.**Format** **show acct radius****Parameters** None**Usage example** **show acct radius****Execution example**

```
(c)NS-2250> show acct radius
<acct radius information>
  Retry      : 1
  Auth_deny_stop : remote
  Session_id  : 262780267

<radius server 1>
  IP address  : 172.16.1.1
  Port number : 1813
  Password    : stored
  Timeout     : 5
  NAS_ID      : SmartCS

<radius server 2>
  IP address  : 192.168.1.254
  Port number : 1813
  Password    : stored
  Timeout     : 5
  NAS_ID      : ---
```

Explanation **<acct radius information>**

Displays the accounting statistics of the RADIUS server.

Retry

Displays the number of retries for sending the RADIUS accounting.

Auth_deny_stop

Displays the sending method of RADIUS accounting STOP packets used when authentication fails.

Session_id

Displays the last session ID of the RADIUS accounting packet.

<radius server>**IP address**

Displays the IP address of the RADIUS accounting server.

Port number

Displays the port number of the RADIUS accounting server.

Password

Display the secret key setting of the RADIUS accounting server.

TimeoutDisplays the timeout time for the RADIUS accounting server.
The unit is one second.**NAS_ID**This is the NAS-ID attribute notified to the RADIUS accounting server.
When "---" is displayed, the NS-2250 host name is automatically saved in the NAS-ID attribute.

show acct tacacs**[Normal user][Administrator]****Function** Display the settings for TACACS+ accounting.**Format** **show acct tacacs****Parameters** None**Usage example** **show acct tacacs****Execution example**

```
(c)NS-2250> show acct tacacs
<acct tacacs+ information>
Auth_deny_stop : remote
Task_id       : 3

<tacacs+ server 1>
IP address   : 10.1.1.1
Port number  : 49
Password     : stored
Timeout      : 5

<tacacs+ server 2>
IP address   : 10.1.1.2
Port number  : 49
Password     : stored
Timeout      : 5
```

Explanation**<acct tacacs+ information>**

Displays the accounting statistics of the RADIUS server.

Auth_deny_stop

Displays the sending method of accounting STOP packets used when authentication fails.

Task_id

Displays the last task ID of the account.

<tacacs+ server>**IP address**

Displays the IP address of the TACACS+ server.

Port number

Displays the port number of the TACACS+ server.

Password

Display the secret key setting of the TACACS+ server.

Timeout

Displays the timeout time for the TACACS+ server. The unit is one second.

show stats acct radius**[Normal user][Administrator]****Function** Display statistical information of the RADIUS accounting client.**Format** **show stats acct radius****Parameters** None**Usage example** **show stats acct radius****Execution example**

```
(c)NS-2250> show stats acct radius
<acct radius statistics>
Id IP address      Send_Start  Send_Stop  Rcv_Resp  Rcv_Error  Timeout
-----
1 192.168.100.1      12         12         24         0          0
2 10.100.100.1       3          2          0          0          5
```

Explanation**Id**

Displays the identification number of the RADIUS accounting server.

IP address

Displays the IP address of the RADIUS accounting server.

Send_Start

Displays the number of accounting START packets sent to the RADIUS accounting server by the RADIUS client.

Send_Stop

Displays the number of accounting STOP packets sent to the RADIUS accounting server by the RADIUS client.

Rcv_Resp

Displays the number of accounting RESPONSE packets received from the RADIUS accounting server.

Rcv_Error

Displays the number of error packets received by the RADIUS client.

Timeout

Displays the number of RADIUS accounting timeout events.

show stats acct tacacs**[Normal user][Administrator]****Function** Display statistical information of TACACS+ accounting.**Format** **show stats acct tacacs [detail]****Parameters** **[detail]**

Displays the detail of TACACS+ accounting statistical information.

The outline of TACACS+ statistical information is displayed if this parameter is omitted.

Execution example

```
(c)NS-2250> show stats acct tacacs
<acct tacacs+ statistics>
Id IP address      Send_Start  Send_Stop  Rcv_Resp  Rcv_Error  Timeout
-----
1 10.1.1.1         12         12         24         0           0
2 ---              0          0          0          0           0
```

Explanation **Id**

Displays the identification number of the TACACS+ server.

IP address

Displays the IP address of the TACACS+ server.

Send_Start

Displays the number of sent TACACS+ accounting START packets.

Send_Stop

Displays the number of sent TACACS+ accounting STOP packets.

Rcv_Resp

Displays the number of accounting RESPONSE packets received from the TACACS+ server.

Rcv_Error

Displays the number of error packets received from the TACACS+ server.

Timeout

Displays the number of TACACS+ accounting timeout events.

Execution example

```
(c)NS-2250> show stats acct tacacs detail
<acct tacacs+ statistics>
Id              1              2
IP address      ---              ---
-----
Connection_OK   0                0
Connection_NG   0                0
Send_Start      0                0
Send_Stop       0                0
Send_NG         0                0
Recv_Success    0                0
Recv_Error      0                0
Recv_Follow     0                0
Recv_LengthErr  0                0
Recv_SeqNoErr   0                0
```


Recv_Illegal	0	0
Timeout	0	0

Explanation Display the detailed statistical information for each TACACS+ server.

Connection_OK

Number of successfully established connections.

Connection_NG

Number of connection failures.

Send_Start

Number of sent TAC_PLUS_ACCT_FLAG_START packets.

Send_Stop

Number of sent TAC_PLUS_ACCT_FLAG_STOP packets.

Send_NG

Number of accounting transmission failures.

Recv_Success

Number of times the TAC_PLUS_ACCT_STATUS_SUCCESS
ACCT_RESPONSE packet has been received

Recv_Error

Number of times the TAC_PLUS_ACCT_STATUS_ERROR
ACCT_RESPONSE packet has been received

Recv_Follow

Number of times the TAC_PLUS_ACCT_STATUS_FOLLOW
ACCT_RESPONSE packet has been received

Recv_LengthErr

Number of received packets with an invalid length.

Recv_SeqNoErr

Number of received packets with an invalid sequence number.

Recv_Illegal

Number of received packets which are not prescribed.

Timeout

Number of timeout events.

5.18 Time zone display command

show timezone

[Normal user][Administrator]

Function	Display the NS-2250 time zone and a list of the time zones that can be set.
Format	show timezone [list [<i>string</i>]]
Parameters	<p>[list [<i>string</i>]]</p> <p>The time zone currently set to the NS-2250 is displayed if this parameter is omitted.</p> <p>list</p> <p>Display a list of the time zones that can be set.</p> <p>[list [<i>string</i>]]</p> <p>Display the list of time zones whose beginning of their names matches the specified string.</p>

Execution example

```
(c)NS-2250> show timezone
Timezone is "Tokyo"
(c)NS-2250> show timezone list ja
Jakarta
Jamaica
Jan_Mayen
Japan
Jayapura
(c)NS-2250>
```

Explanation	<p>Timezone is</p> <p>Display the NS-2250 time zone.</p>
--------------------	---

Chapter6

Maintenance commands

Chapter 6 describes the maintenance commands that can be used on the NS-2250.

6.1 Basic maintenance commands

date

[Normal user][Administrator]

Function Set and display the NS-2250 date and time.

Format **date** [YYYY/MM/DD hh:mm:ss | **ntp** { ipaddr | host }]

Parameters [YYYY/MM/DD hh:mm:ss | **ntp** { ipaddr | host }]

This command displays the current date and time saved in the NS-2250 if this parameter is omitted.

YYYY/MM/DD hh:mm:ss

To set the date and time manually, enter the date in the "year/month/day" format, leave a space, and then enter the time in the "hours/minutes/seconds" format.

The maximum number of digits is four for the years, and two for the other values.

ntp { ipaddr | host }

To set a new date and time using an NTP server, specify "ntp" followed by the NTP server IP address or host name.

Note When you configure the date manually, the entered date must be after the first of January 2015 (2015/01/01), otherwise an error occurs.

Usage example To set the first of November 2015 for the date and 12:00:00 for the time.

date 2015/11/01 12:00:00

engineering**[Administrator]**

Function	Switch the NS-2250 operating mode to engineering mode.
Format	engineering [password]
Parameters	<p>[password]</p> <p>When the command is executed with this parameter specified, a message prompting you to enter a password is displayed. Enter a password.</p> <p>When you press the Enter key after entering the password, a message prompting you to confirm the password is displayed. Enter the same password again.</p> <p>If you do not specify this parameter, no passwords are allocated to maintenance engineer users.</p>
Usage example	engineering
Explanation	The engineering mode is a special mode accessible only by device management users. In the engineering mode, you can execute hidden commands and commands whose effects are not guaranteed. We will not describe the commands that can be executed in this mode.

exit**[Normal user][Administrator]**

Function

This command is alias of logout

logout**[Normal user][Administrator]****Function** Log out from the NS-2250.**Format** **logout****Parameters** None**Usage example** **logout**

Explanation When this command is executed in the following modes, you exit the mode.

You return to the normal user mode when executed in the device management user mode.

You return to the device management user mode when executed in the engineering mode.

ping

[Normal user][Administrator]

Function	Confirm the communication with the connected host on an IP network.
Format	ping [count <i>number</i>] [length <i>len</i>] [interval <i>sec</i>] { <i>dstaddr</i> <i>host</i> }
Parameters	<p>[count <i>number</i>]</p> <p>Specify the number of ping request packets to send in the 1 to 65535 range. This parameter is set to "3" by default.</p> <p>[length <i>len</i>]</p> <p>Specify the length of sent packet datagrams. The round-trip time cannot be calculated when the length is less than 8 octets. This parameter is set to "56" by default.</p> <p>[interval <i>sec</i>]</p> <p>Set the interval between sent packets in the 1 to 1800 seconds range. This parameter is set to "1" by default.</p> <p>{ <i>dstaddr</i> <i>host</i> }</p> <p>Specify the IP address or host name of the connected host with which you want to check the connection.</p>
Note	<ul style="list-style-type: none"> • In the case of host name specification, if there is an IPv4 address in the address acquired by name resolution, communication is performed in IPv4. • In the case of host name specification, if there is only IPv6 address acquired by name resolution, communication is performed in IPv6.
Usage example	To send the ping request 10 times to the host 192.168.0.105. ping count 10 192.168.0.105

ping6

[Normal user][Administrator]

Function	Confirm IPv6 communication with the connected host on the IP network.
Format	ping6 [count <i>number</i>] [length <i>len</i>] [interval <i>sec</i>] { <i>ip6addr[%if]</i> <i>host</i> }
Parameters	<p>[count <i>number</i>]</p> <p>Specify the number of times to send ICMPv6 Echo packets in the range from 1 to 65535.</p> <p>This parameter is set to "3" by default.</p> <p>[length <i>len</i>]</p> <p>Specify the datagram length of the packet to be transmitted in the range of 0 to 2048 octets.</p> <p>This parameter is set to "56" by default.</p> <p>[interval <i>sec</i>]</p> <p>Set the interval between sent packets in the 1 to 1800 seconds range.</p> <p>This parameter is set to "1" by default.</p> <p>{ <i>ip6addr[%if]</i> <i>host</i> }</p> <p>Specify the IP address or host name of the connected host with which you want to check the connection.</p> <p><i>ip6addr[%if]</i></p> <p>Specify the IPv6 address in x:x:x:x:x:x:x format.</p> <p>The "x" in each field of the address is represented by the hexadecimal of the 16 bit part.</p> <p>If there are consecutive 0 in the front of the field they can be omitted.</p> <p>The field composed of only 0 can also be omitted only once by specifying as "::" in the address.</p> <p>If the IPv6 address is a link local address, specify the interface to communicate subsequently to "%".</p> <p><i>host</i></p> <p>Specify the host name of the connected host with which you want to check the connection.</p>
Note	<ul style="list-style-type: none"> • In case of host name specification, it is an error if there is no IPv6 address in the address obtained by name resolution.
Usage example	To send the ping request 10 times to the host 2001:db8::192.
	ping6 count 10 2001:db8::192

reboot**[Administrator]**

Function Reboot the NS-2250.

Format **reboot** [{ **main** | **backup** }]
 [**startup** *config_number* [{ **internal** | **external** }]]

Parameters [{ **main** | **backup** }]

Select the system software to reboot.

The NS-2250 includes two system software units.

main

Specify "main" to reboot the main system software.

backup

Specify "backup" to reboot the backup system software.

[**startup** *config_number* [{ **internal** | **external** }]]

startup *config_number*

Specify the startup file (1 to 4) to be imported at startup.

[{ **internal** | **external** }]

Specify "internal" to import the startup file with the specified number saved inside the NS-2250.

When you omit both the "internal" and "external" parameters,

internal

Specify "external" to import the startup file with the specified number saved in the USB memory. A USB memory must be inserted into the USB port to use this function.

external

"external" is automatically selected if a USB memory is inserted in the USB port, otherwise "internal" is selected.

When the entire "startup" parameter is omitted, the default startup file is imported at startup. If a USB memory is inserted when the NS-2250 reboots, the default startup file saved in the USB memory is imported.

Usage example To reboot the NS-2250 using the default startup file.

reboot

To reboot the backup system software and import the startup file 2 from the USB memory.

reboot startup 2

shutdown**[Administrator]****Function** Shut down the NS-2250.**Format** **shutdown [logclear]****Parameters** [**logclear**]

Shut down the NS-2250 and delete the following logs at the same time.

- Console log
- Command log
- Log file created with the "logsave" command
- Previous login information displayed at login
- Port log Shut down the NS-2250 without deleting log if this parameter is omitted.

Note The settings changed after startup are lost when the NS-2250 is shut down.

To save the changed settings, execute the "write" command to save the running configuration to the startup file before shutting down the NS-2250.

Usage example To shut down the NS-2250 and delete the logs at the same time.**shutdown logclear**

su**[Normal user]****Function** Log in as a device management user.**Format** **su****Parameters** None**Usage example** **su**

telnet	[Normal user][Administrator]
Function	Log in to a connected host via a Telnet client.
Format	telnet { <i>ipaddr</i> <i>ip6addr[%if]</i> <i>host</i> } [<i>tcpport</i>]
Parameters	<p data-bbox="424 421 815 450">{ <i>ipaddr</i> <i>ip6addr[%if]</i> <i>host</i> }</p> <p data-bbox="483 454 1461 517">Specify the IP address or host name of the connected host to which you want to log in.</p> <p data-bbox="483 528 560 557"><i>ipaddr</i></p> <p data-bbox="533 564 831 593">Specify the IPv4 address.</p> <p data-bbox="533 598 1461 627">The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).</p> <p data-bbox="483 633 639 663"><i>ip6addr[%if]</i></p> <p data-bbox="533 669 1123 698">Specify the IPv6 address in x:x:x:x:x:x:x format.</p> <p data-bbox="533 703 1461 766">The "x" in each field of the address is represented by the hexadecimal of the 16 bit part.</p> <p data-bbox="533 770 1358 799">If there are consecutive 0 in the front of the field they can be omitted.</p> <p data-bbox="533 804 1461 866">The field composed of only 0 can also be omitted only once by specifying as "::" in the address.</p> <p data-bbox="533 871 1461 934">If the IPv6 address is a link local address, specify the interface to communicate subsequently to "%".</p> <p data-bbox="483 940 533 969"><i>host</i></p> <p data-bbox="533 974 1390 1003">Specify the host name of the connected host to which you want to log in.</p> <p data-bbox="424 1010 549 1039">[<i>tcpport</i>]</p> <p data-bbox="483 1043 1278 1072">Specify the TCP destination port number used by the Telnet client.</p> <p data-bbox="483 1077 963 1106">This parameter is set to "23" by default.</p>
Note	<ul style="list-style-type: none"> • In the case of host name specification, if there is an IPv4 address in the address acquired by name resolution, communication is performed in IPv4. • In the case of host name specification, if there is only IPv6 address acquired by name resolution, communication is performed in IPv6.
Usage example	<p data-bbox="424 1296 1422 1326">To log in to the host with the IP address 192.168.215.105 via port 1023 using Telnet.</p> <p data-bbox="483 1352 823 1382">telnet 192.168.1.105 1023</p>

traceroute**[Normal user][Administrator]**

Function Examine the information of the route to the specified host.

Format **traceroute** [**udp** *udpport*] { *dstaddr* | *host* }

Parameters [**udp** *udpport*]

Set the number of the UDP port to examine.

This parameter is set to "33434" by default.

{ *dstaddr* | *host* }

Specify the IP address or host name of the host of the route you want to examine.

Note

- In the case of host name specification, if there is an IPv4 address in the address acquired by name resolution, communication is performed in IPv4.
- In the case of host name specification, if there is only IPv6 address acquired by name resolution, communication is performed in IPv6.

Usage example To examine the route to the host 192.168.250.1.

traceroute 192.168.250.1

tracert6

[Normal user][Administrator]

Function	Examine the information of the route to the specified host
Format	tracert6 [udp <i>udpport</i>] { <i>ip6addr[%if]</i> <i>host</i> }
Parameters	<p>[udp <i>udpport</i>]</p> <p>Set the number of the UDP port to examine. This parameter is set to "33434" by default.</p> <p>{ <i>ip6addr[%if]</i> <i>host</i> }</p> <p>Specify the IP address or host name of the host of the route you want to examine.</p> <p><i>ip6addr[%if]</i></p> <p>Specify the IPv6 address in x:x:x:x:x:x:x format. The "x" in each field of the address is represented by the hexadecimal of the 16 bit part. If there are consecutive 0 in the front of the field they can be omitted. The field composed of only 0 can also be omitted only once by specifying as "::" in the address. If the IPv6 address is a link local address, specify the interface to communicate subsequently to "%".</p> <p><i>host</i></p> <p>Specify the host name of the host of the route you want to examine.</p>

Note

- In case of host name specification, it is an error if there is no IPv6 address in the address obtained by name resolution.

Usage example To examine the route to the host 2001:db8::192

tracert6 2001:db8::192

switch bonding**[Administrator]****Function** Switch the active port.**Format** **switch bonding { eth1 | eth2 }****Parameters** **{ eth1 | eth2 }**

Specify the slave interface which you want to switch to active port.

Note When a state of the slave interface is down or going back , you can't switch it to active port.

When the slave interface is already active port , you can't switch it to active port.

Usage example To switch active port to eth2.**switch bonding eth2****Explanation** The slave interface can be manually switched to active port by this command.

hangup**[Administrator]****Function** Reset the service of a specific serial port.**Format** **hangup tty** *tylist***Parameters** **tty** *tylist*

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Specify a list of serial ports separated by hyphens "-" and commas "," to set multiple ports in a single command.

Usage example To reset the service of serial port 1.**hangup tty 1**

history**[Normal user][Administrator]****Function** Display the command execution history.**Format** **history****Parameters** None**Note** The last 20 commands are displayed.**Execution example**

```
(c)NS-2250> history
 1 history
 2 date
 3 ping 192.168.1.1
 4 telnet 192.168.1.1
 5 history
```

logsave**[Administrator]****Function** Save the port logs of serial ports.**Format** **logsave tty *ttylist*****Parameters** **tty *ttylist***

Specify the tty number corresponding to the serial port in the 1 to 48 range.

The range of ports that you can specify varies depending on the model.

Save the log of the specified serial ports into a file.

Usage example To save the port log of serial port 1.**logsave tty 1****Explanation** (1) The log is created with the following name: ttyNN_yymmddhhmm.log (NN is the serial port number).

(2) To acquire the log file, connect to the NS-2250 FTP/SFTP server from an external FTP/SFTP client, log in as a port log acquisition user (log), and execute the "get" command.

(3) To delete the log file, log in as explained above and execute the "delete" command.

For details on how to acquire and delete a log file, see Section 5.6, "Save and acquire port logs manually" in the Instruction Manual.

loginfo**[Administrator]****Function** Display a list of port log files saved in a FLASH memory, and the used and free space.**Format** **loginfo****Parameters** None**Usage example** **loginfo****Execution example**

```
(c)NS-2250# loginfo
Total(1K-blocks)      Used   Available Use%
-----
          471620      2318     440434   1%

Size      SaveTime      Name
-----
  118902   Oct 11 14:41 tty01_0610111441.log
 3072016   Oct 12 10:21 tty01_0610121021.log
```

clear arp**[Administrator]****Function** Delete all dynamic ARP entries registered in the NS-2250.**Format** **clear arp****Parameters** None**Usage example** To delete the dynamic ARP entries of the NS-2250.**clear arp****Note** The ARP entry referred to from a routing cash table inside the NS-2250 isn't deleted.

trace**[Administrator]**

Function	Perform tracing of the packets sent and received by the NS-2250 for each protocol.
Format	trace { eth1 eth2 bond1 } { icmp icmp6 ipsec radius tacacs } [count count] [level level]
Parameters	{ eth1 eth2 bond1 } { icmp icmp6 ipsec radius tacacs } icmp Specify "icmp" to perform tracing for the ICMP protocol. icmp6 Specify "icmp6" to perform tracing for the ICMPv6 protocol. ipsec Specify "ipsec" to perform tracing for the IKE/ESP protocol. radius Specify "radius" to perform tracing for the RADIUS protocol. tacacs Specify "tacacs" to perform tracing for the TACACS protocol. count count Specify the packet count for tracing. Specify a number of packets from 1 through 1000. This parameter is set to "50" by default. level level Specify the trace level from 1 through 3. This parameter is set to "1" by default. Specify "1" to perform level 1 tracing (basic). The content of each packet is displayed in one line. Specify "2" to perform level 2 tracing (advanced). The content of each packet is analyzed and displayed in multiple lines. Specify "3" to perform level 3 tracing (advanced + hex dump). In addition to level 2 information, the packet content is displayed in hex dump.
Note	During usually using, please invalidate this function. The bond1 interface designation become the error if the bonding function is disabled.
Usage example	To perform a level 1 tracing of 100 RADIUS packets. trace eth1 radius level 1 count 100

disconnect**[Administrator]**

Function	Disconnect the TCP session connected to the specified service.
Format	disconnect { ftp ftpd sftpd portd tty <i>ttylist</i> } [{ all rw { all <i>session_id</i> } ro { all <i>session_id</i> } }]
Parameters	<p>{ ftp ftpd sftpd portd tty <i>ttylist</i> } Specify the service of the connected TCP session.</p> <p>ftp Disconnect session of the ftp client connected to the NS-2250.</p> <p>ftpd Disconnect session of the ftpd service connected to the NS-2250.</p> <p>sftpd Disconnect session of the sftpd service connected to the NS-2250.</p> <p>portd Disconnect session of the portd service connected to the NS-2250.</p> <p>tty <i>ttylist</i> Specify the tty number corresponding to the serial port in the 1 to 48 range.</p> <p>[{ all rw { all <i>session_id</i> } ro { all <i>session_id</i> } }] Specify the type of session. The parameter "all" is set if this parameter is omitted.</p> <p>all Disconnect all sessions connected to the specified serial port.</p> <p>rw { all <i>session_id</i> } Disconnect the Normal mode (rw) sessions connected to the specified serial port. This parameter is enabled only when you have specified the portd.</p> <p>all Disconnect all sessions.</p> <p><i>session_id</i> Disconnect the specified sessions.</p> <p>ro { all <i>session_id</i> } Disconnect the Monitoring mode (ro) sessions connected to the specified serial port. This parameter is enabled only when you have specified the portd.</p> <p>all Disconnect all sessions.</p> <p><i>session_id</i> Disconnect the specified sessions.</p>

Usage example To disconnect all Normal mode (rw) sessions connected to serial port 1.

disconnect portd tty 1 rw all

tftp setup**[Administrator]**

Function	Send and receive the startup files by TFTP.
Format	tftp { get put } setup startup { 1 2 3 4 number } { internal external } [bsize size] [remote "remote_file"] ipaddr
Parameters	<p>{ get put } Send and receive the startup files by TFTP.</p> <p>get Received a startup file from a TFTP server.</p> <p>put Send a startup file to a TFTP server.</p> <p>setup startup { 1 2 3 4 number } { internal external }</p> <p>startup { 1 2 3 4 number } { 1 2 3 4 } Specify the number of the startup file you want to obtain from the TFTP server.</p> <p>number Specify "number" to select the number of the startup file imported to the NS-2250 at startup.</p> <p>internal Specify "internal" to select the startup files saved inside the NS-2250.</p> <p>external Specify "external" to select the startup files saved to an USB memory.</p> <p>[bsize size] Specify the block size forwarded in TFTP. The setting range is from 1 through 65535. The parameter "512" is set if this parameter is omitted.</p> <p>[remote "remote_file"] Specify the name and path of the file to obtain from the TFTP server within double quotation marks. You can use alphanumeric and space characters. The maximum number of characters is 64. When received, the specified file is saved inside the NS-2250 or in the USB memory and overwrites the file "startup+specified number". When you do not specify this option, an error occurs if there is no file named "startup+1 to 4" in the TFTP server.</p> <p>ipaddr Specify the IP address of the TFTP server. The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).</p>

Usage example To acquire the startup file 2 in the internal from the TFTP server 192.168.0.1.

tftp get setup startup 2 internal remote startup 192.168.0.1

tftp verup**[Administrator]**

Function	Send and receive the upgrade files for system by TFTP.
Format	tftp { get put } verup { system system-image } [bsize <i>size</i>] [remote " <i>remote_file</i> "] <i>ipaddr</i>
Parameters	<p>{ get put } Send and receive the upgrade files for system by TFTP.</p> <p>get Received a upgrade file from a TFTP server.</p> <p>put Send a upgrade file to a TFTP server.</p> <p>verup { system system-image } Specify the upgrade file you want to obtain from the TFTP server.</p> <p>system Upgrade file is sent between the TFTP server.</p> <p>system-image System image file is sent and received between the TFTP server.</p> <p>[bsize <i>size</i>] Specify the block size forwarded in TFTP. The setting range is from 1 through 65535. The parameter "512" is set if this parameter is omitted.</p> <p>[remote "<i>remote_file</i>"] Specify the IP address of the TFTP server, and the name and path of the upgrade file to obtain from the TFTP server within double quotation marks. You can use alphanumeric and space characters. The maximum number of characters is 64. When received, the specified file is saved in the upgrade file save area inside the NS-2250 and overwrites the file "system". When you do not specify this option, an error occurs if there is no file named "system" in the TFTP server.</p> <p><i>ipaddr</i> Specify the IP address of the TFTP server. The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).</p>

Usage example To acquire the upgrade file from the TFTP server 192.168.0.1.

tftp get verup system 192.168.0.1

tftp log**[Administrator]**

Function Send the log files by TFTP.

Format **tftp put log** *logfiles* [**bsize** *size*] [**remote** "*remote_file*"] *ipaddr*

Parameters **put**

Send a log file to a TFTP server.

log *logfiles*

Enter a character string within double quotation marks to specify the log file created using the "logsave" command. You can use alphanumeric and space characters. The maximum number of characters is 64.

When specifying logsave_file, execute the "loginfo" command to check the log file names of the corresponding port.

[**bsize** *size*]

Specify the block size forwarded in TFTP.

The setting range is from 1 through 65535.

The parameter "512" is set if this parameter is omitted.

[**remote** "*remote_file*"]

Specify the name and path of the file to save in the TFTP server within double quotation marks. You can use alphanumeric and space characters. The maximum number of characters is 64.

You can save the file in the TFTP server with a name of your choosing.

The file is saved in the TFTP server with the same name as the logsave_file file if this parameter is omitted.

ipaddr

Specify the IP address of the TFTP server.

The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).

Usage example To send the log file of TTY1 to the TFTP server 192.168.0.1.

tftp put log tty01_1501051503.log 192.168.0.1

tftp support**[Administrator]**

Function Send the supportlog files by TFTP.

Format **tftp put support** [**bsize** *size*] [**remote** "*remote_file*"] *ipaddr*

Parameters **put support**

Send the supportlog files by TFTP.

[**bsize** *size*]

Specify the block size forwarded in TFTP.

The setting range is from 1 through 65535.

The parameter "512" is set if this parameter is omitted.

[**remote** "*remote_file*"]

Specify the name and path of the file to save in the TFTP server within double quotation marks. You can use alphanumeric and space characters. The maximum number of characters is 64.

You can save the file in the TFTP server with a name of your choosing.

The file is saved in the TFTP server with the same name as the *logsave_file* file if this parameter is omitted.

ipaddr

Specify the IP address of the TFTP server.

The IP address must be specified in the dot-decimal notation (*xxx.xxx.xxx.xxx*).

Usage example To send the support log file to the TFTP server 192.168.0.1.

tftp put support 192.168.0.1

ftp**[Administrator]**

Function	Various files is sent and received between the FTP server.
Format	ftp { setup { internal external } verup support log } <i>ftp_server</i>
Parameters	<p>{ setup { internal external } verup support log } Various files is sent and received between the TFTP server.</p> <p>setup { internal external } internal Specify "internal" to select the startup files saved inside the NS-2250. external Specify "external" to select the startup files saved to an USB memory.</p> <p>verup Upgrade files is send and received between the FTP server.</p> <p>support Support log files is send and received between the FTP server.</p> <p>log Log files is send and received between the FTP server.</p> <p><i>ftp_server</i> Specify the IP address of the FTP server. The IP address must be specified in the dot-decimal notation (xxx.xxx.xxx.xxx).</p>
Usage example	<p>To sent and received the startup file 1 saved inside the NS-2250 to the FTP server 192.168.0.1.</p> <p>ftp setup internal 192.168.0.1</p>
Explanation	<p>NS-2250 functions as a FTP client.</p> <p>After login, the following command can be used for a FTP server.</p> <p>pwd Displays the current directory on the server.</p> <p>cd Change the current directory on the server.</p> <p>mkdir Create the directory on the server.</p> <p>{ ls dir } Displays the list of files on the server.</p> <p>get [<remote>] <local> Received the file on the server.</p> <p>[<remote>] The remote filename <local> is set if this parameter is omitted.</p> <p><local> Specify character strings are startup1-4, startup_number, system and NS-2250.sys</p> <p>put <local> [<remote>] Send the file to a server.</p> <p><local> Specify character strings are startup1-4, startup_number, system and NS-2250.sys</p>

[**<remote>**]

The remote filename **<local>** is set if this parameter is omitted.

mget

Received the files on the server.

mput

Send the files to a server.

prompt

Switched the interactive mode.

hash

Switched the hash indication function when send and received data.

passive

Switched the passive mode.

binary

Switched the transfer mode to binary.

ascii

Switched the transfer mode to ascii.

status

Displays the information of FTP.

verbose

Displays the detail of FTP connection.

debug

Displays the inside processing of FTP client.

{ **quit** | **exit** | **bye** }

Exit the FTP command.

{ **help** | **?** }

Displays the list of commands.

6.2 Management commands for settings files

write**[Administrator]**

Function Save the NS-2250 current settings in the specified startup file.

Format **write** [**startup** *config_number* [{ **internal** | **external** }]]

Parameters [**startup** *config_number* [{ **internal** | **external** }]]

startup *config_number*

Specify "startup" and the number (1 to 4) of a startup file to select the destination startup file.

The settings are saved to the startup file selected when the NS-2250 starts if this parameter is omitted.

[{ **internal** | **external** }]

Specify the save destination of the startup file.

When omitting this parameter, it's saved by both of inside the NS-2250 and USB memory.

internal

Specify "internal" to save the settings to a startup file saved inside the NS-2250.

external

Specify "external" to save the settings to a startup file saved in an USB memory.

Execution example

```
(c)NS-2250# write
Do you really want to write default startup1 [y/n] ? y
write external startup1
.....writing
write internal startup1
.....writing
(c)NS-2250# write startup 2 internal
Do you really want to write internal startup2 [y/n] ? y
.....writing
```

Explanation This command displays the progress situation "...."

The NS-2250 has eight startup files (four files in the USB memory and four files in the internal memory of the NS-2250).

When you execute this command, a message such as "Do you really want to write ... [y/n] ?" is displayed, asking you if you want to save the settings to the imported or specified startup file. Press "y" to save the settings.

clear startup**[Administrator]**

Function Return the specified startup file to the default settings.

Format **clear startup** { *config_number* | **all** } [{ **internal** | **external** }]

Parameters { *config_number* | **all** }

config_number

Specify the number (1 to 4) of the startup file to return to the default settings in *config_number*.

all

Specify "all" to select all the four startup files (1 to 4).

[{ **internal** | **external** }]

internal

Specify "internal" to select the startup files saved inside the NS-2250.

external

Specify "external" to select the startup files saved to the USB memory.

Usage example To return the "startup1" file in the USB memory to the default settings.

clear startup 1 external

To return all startup files to the default settings.

clear startup all

Explanation

(1) You can check that the startup files correctly returned to the default settings with the "show config info" command. Check the displayed startup file date and size.

(2) The NS-2250 has eight startup files (four files in the USB memory and four files in the internal memory of the NS-2250).

(3) When you execute this command, a message such as "Do you really want to clear ... [y/n] ?" is displayed, asking you if you want to initialize the settings of the specified startup file. Press "y" to initialize the settings.

default startup**[Administrator]**

Function	Specify the startup file to be imported at startup.
Format	default startup <i>config_number</i> [{ internal external }]
Parameters	<p>startup <i>config_number</i></p> <p>Specify the number (1 to 4) of the startup file to set as the default startup file.</p> <p>[{ internal external }]</p> <p>internal</p> <p>Specify "internal" to select the startup files saved inside the NS-2250.</p> <p>external</p> <p>Specify "external" to select the startup files saved to the USB memory.</p>

Execution example

To make the "startup2" file in the USB memory the default startup file.

```
(c)NS-2250# default startup 2
Do you really want to set default config startup2 [y/n] ? y
(c)NS-2250#
```

Explanation	<p>(1) The NS-2250 has eight startup files (four files in the USB memory and four files on the internal memory of the device).</p> <p>(2) When you execute this command, a message such as "Do you really want to set default config ... [y/n] ?" is displayed, asking you if you want to set the specified startup file as the default startup file to be imported at startup. Press "y" to make the setting.</p>
--------------------	--

copy startup**[Administrator]****Function** Copy a startup file.**Format** **copy startup** *config_number1* { **internal** | **external** }
to startup *config_number2* { **internal** | **external** }

Parameters **startup** *config_number1*
Specify the number (1 to 4) of the startup file to copy.
{ internal | external }

internal
Specify "internal" to select the startup files saved inside the NS-2250.

external
Specify "external" to select the startup files saved to the USB memory.

to startup *config_number2*
Specify the number (1 to 4) of the destination startup file.
{ internal | external }

internal
Specify "internal" to select the startup files saved inside the NS-2250.

external
Specify "external" to select the startup files saved to the USB memory.

Execution example

To copy the "startup1" file in the NS-2250 to the "startup2" in the USB memory.

```
(c)NS-2250# copy startup 1 internal to startup 2 external
Do you really want to copy startup1 internal to startup2 external [y/n] ? y
(c)NS-2250#
```

Explanation (1) The NS-2250 has eight startup files (four files in the USB memory and four files in the internal memory of the device).

(2) When you execute this command, a message such as "Do you really want to copy internal startup1 to external startup1 [y/n] ?" is displayed, asking you if you want to copy the specified startup file. Press "y" to copy the file.

echo**[Administrator]**

Function Display the specified character string.**Format** **echo** *string***Parameters** *string*

Specify the character string to display. You can specify from 1 through 128 characters.

Enter the character strings within double quotation marks (") to display multiple strings.

After system has started, this command doesn't display a specified character strings.

6.3 Management command for the system software

copy system**[Administrator]**

Function	Copy the system software image.
Format	copy system { main backup } to { main backup }
Parameters	system { main backup } Specify "main" or "backup" for the system software to copy. main backup to { main backup } Specify "main" or "backup" for the destination system software. main backup
Usage example	To copy the main system software to the backup system software. copy system main to backup

verup execute**[Administrator]**

Function	Upgrade or downgrade the system software using a file sent via FTP or SFTP.
Format	verup execute [{ main backup }]
Parameters	execute [{ main backup }] main backup
Note	New system is applied by this command from the next system start. After confirming the command result, execute the reboot command.
Explanation	Rebooting may take a long time after the "verup execute" command and upgrade/downgrade have been executed. Do not switch off the power or press the RESET switch until the NS-2250 starts. Otherwise, the system software will no longer start.

verup cleanup**[Administrator]**

Function Delete the system software upgrade or downgrade file sent via FTP or SFTP.

Format **verup cleanup**

Parameters None

Execution example

```
(c)NS-2250# verup cleanup
clean up successful
(c)NS-2250#
```

backup system-image**[Administrator]**

Function	Made the backup of system software. Backup file is made on the RAM.
Format	backup system-image { main backup }
Parameters	{ main backup } Specify the system software which makes a backup. main Made the backup of main system software. backup Made the backup of backup system software.

Usage example Made the backup of main system software.

backup system-image main

Execution example

```
(c)NS-2250# backup system-image main
Please wait a few minutes... done.
backup successful
(c)NS-2250#
```

- Note**
- When NS-2250 is restarted, backup file is deleted.
 - For details of backup operation, see the NS-2250 Instruction Manual.

restore system-image**[Administrator]**

Function	Restore the backup of system software.
Format	restore system-image to { main backup }
Parameters	to { main backup } Specify the system software which restores a backup. main Restore the main system software. backup Restore the backup system software.

Usage example Restore the main system software.

restore system-image to main

Execution example

```
(c)NS-2250# restore system-image to main
Please wait a few minutes... done.
restore successful
(c)NS-2250#
```

Note For details of restore operation, see the NS-2250 Instruction Manual.

clear system-image**[Administrator]****Function** Delete the backup file of system software.**Format** **clear system-image****Parameters** None

Note

- This commands are the backup file made by the backup command and the command from which forwarded backup file is send by TFTP/SFTP/FTP.
- For details of restore operation, see the NS-2250 Instruction Manual.

show system-image**[Administrator]****Function** Displays the backup file and restore file of system software.**Format** **show system-image****Parameters** None**Execution example**

```
(c)NS-2250> show system-image
System Image Name : NS-2250.sys
Product           : NS-2250
Version           : 1.0
Date              : 2015-10-01
Status            : available
```

Explanation **System Image Name**

Display the name of system image.

Product

Displays the name of product.

Version

Displays the version of system software.

Date

Displays the date and time when an image was made are created.

Status

Displays the status of system image.

available

The image it possible to restore.

not available

The image it isn't possible to restore.

6.4 Console output control commands

console**[Administrator]**

Function	The output destination of a console message is controlled.
Format	console [{ on off }]
Parameters	[{ on off }] Displays the status of system image. The parameter "on" is set if this parameter is omitted. on The terminal where this command has been executed becomes an output destination for console messages. off Stop the console message output to the terminal where this command is executed.

Usage example This command is the same as the "console on" command.

console on

loglevel**[Administrator]**

Function Change the output level of the console messages.

Format **loglevel ipsec level**

Parameters **ipsec**

 Change the output level of the console messages the ipsec object outputs.

level

 Specify the output level in the range from 0 to 3.

 If you specify as "3", it is the most detail level.

 If you specify as "0", the log messages are not outputted.

 If you do not execute this command, the value "1" is specified.

Usage example In the case of changing the output level of the console messages the ipsec object outputs as "2".

loglevel ipsec 2

6.5 Terminal output control commands

terminal timeout

[Normal user][Administrator]

Function Set the terminal automatic logout time.

Format **terminal timeout { on *time* | off }**

Parameters **{ on *time* | off }**

Specify the time for automatic logout timeout of the user that executed the command on the terminal. This setting applies to normal users and device management users who log in to the NS-2250.

The corresponding user is automatically log out if no operation, such as entering a command, is performed during the specified time.

Specify the timeout time from 1 through 60 minutes if you have specified "on". The unit one minute.

Specify "off" to disable automatic logout.

The default parameter is set according to the "set terminal default timeout" command setting. When the "set terminal default timeout" command has not been executed, the default parameter is "on" and "10" minutes.

Usage example To set the timeout time for automatic logout to 30 minutes.

terminal timeout on 30

terminal editing**[Normal user][Administrator]**

Function	Enable or disable the terminal line editing function.
Format	terminal editing { enable disable }
Parameters	{ enable disable } Set to enable or disable the editing of command lines using the terminal delete and arrow keys. Specify "enable" to enable the line editing function. Specify "disable" to disable the line editing function. The default parameter is set according to the "set terminal default editing" command setting. When the "set terminal default editing" command has not been executed, the default parameter is "enable".
Usage example	To disable line editing on the terminal. terminal editing disable

terminal page**[Normal user][Administrator]****Function** Enable or disable the terminal paging function.**Format** **terminal page { enable | disable }****Parameters** **{ enable | disable }**

With this command you can enable the paging function that separates the output text into a different page when the text exceeds the specified number of lines per page. Disable the paging function to display the output text continuously.

Specify "enable" to enable the paging function.

Specify "disable" to disable the paging function.

The default parameter is set according to the "set terminal default page" command setting. When the "set terminal default page" command has not been executed, the default parameter is "enable".

Usage example To disable the paging function on the terminal.**terminal page disable**

terminal height**[Normal user][Administrator]****Function** Specify the number of lines per page of the terminal.**Format** **terminal height** *rows***Parameters** *rows*

Specify the number of lines per page from 10 through 256.

The default parameter is set according to the "set terminal default height" command setting. When the "set terminal default height" command has not been executed, the default parameter is "23".

Usage example To set to 32 the number of lines on one page.**terminal height 32**

terminal width**[Normal user][Administrator]****Function** Specify the number of characters per line of the terminal.**Format** **terminal width** *columns***Parameters** *columns*

Specify the number of characters per line from 40 through 256.

The default parameter is set according to the "set terminal default width" command setting. When the "set terminal default width" command has not been executed, the default parameter is "80".

Usage example To set to 120 the number of characters on one line.**terminal width 120**

terminal prompt	[Normal user][Administrator]
Function	Specify the display format of the terminal prompt.
Format	terminal prompt { device { on off } hostname { on off } time { on off } }
Parameters	<p>{ device { on off } hostname { on off } time { on off } } Specify the display format of the terminal prompt.</p> <p>device { on off } Specify the identification information of the terminal. The default parameter is set according to the "set terminal default prompt" command setting. When the "set terminal default prompt" command has not been executed, the default parameter is "on".</p> <p>on Display the identification information (terminal number, etc.) of the terminal used on the prompt.</p> <p>off No display the identification information (terminal number, etc.) of the terminal used on the prompt.</p> <p>hostname { on off } Specify the NS-2250 host name of the terminal. The default parameter is set according to the "set terminal default prompt" command setting. When the "set terminal default prompt" command has not been executed, the default parameter is "on".</p> <p>on Display the NS-2250 host name on the prompt.</p> <p>off No display the NS-2250 host name on the prompt.</p> <p>time { on off } Specify the current time of the terminal. The default parameter is set according to the "set terminal default prompt" command setting. When the "set terminal default prompt" command has not been executed, the default parameter is "off".</p> <p>on Display the current time on the prompt.</p> <p>off No display the current time on the prompt.</p>
Usage example	To include the current time in the items displayed on the prompt.
Explanation	<p>terminal prompt time on</p> <p>The prompt display is as follows when the host name, terminal identification number, and current time are displayed.</p> <p>(c) [12:30:10]NS-2250 ></p> <p>(c) indicates that the terminal used is connected to the CONSOLE port. When a number is shown in the parentheses (), it means that the terminal used is a Telnet/SSH terminal connected to the NS-2250. The number in parentheses is the terminal number. [12:30:10] in the middle shows the current time in the following format: [hours:minutes:seconds]. "NS-2250" on the right is the NS-2250 host name.</p>

terminal redisp**[Normal user][Administrator]**

Function Specify whether or not to redisplay the previously entered command string on the next prompt screen after a command input error has occurred.

Format **terminal redisp { on | off }**

Parameters **{ on | off }**

Specify "on" to redisplay the command string that caused the error.

Specify "off" not to redisplay the command string that caused the error.

The default parameter is set according to the "set terminal default redisp" command setting. When the "set terminal default redisp" command has not been executed, the default parameter is "on".

Usage example To set not to redisplay the command string.

terminal redisp off

Chapter7

Other commands

Chapter 7 describes the other setting commands that can be used on the NS-2250.

7.1 Port server menu commands

Commands used to operate sessions and logs displayed in the port server.

- 0 (return Port Select Menu)
- 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)

When you access a serial port with the port log function enabled, the following port log menu is displayed.

```
-- RW1 -----
Host : "NS-2250-1"
Label : L3SW-1
-----
0 : return Port Select Menu
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>
```

0 (return Port Select Menu)

Function Return to port selection menu.

Explanation This menu appears only when Select mode is selected. It does not appear when Direct mode is selected.

Execution example

```
connect tty 1 RW mode
-- RW1 -----
Host : "NS-2250-1"
Label : L3SW-1
-----
0 : return Port Select Menu
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> 0
return Port Select Menu
Host : "NS-2250-1 "
login from 192.168.1.1
user (user1) Access TTY List
=====
tty : Label RW R0
-----
1 : EXAtrax-Tokyo-6F-00001 1 0
2 : EXAtrax-II 2 1
3 : BlueBrick-Makuhari-7F-00001 0 N/A
4 : BlueBrick-Makuhari-7F-00002 0 N/A
5 : Switch-1 1 0
: (Omitted)
-----
Enter tty number to access serial port
<ttyno> : connect to serial port RW session ( 1 - 32 )
<ttyno>r : connect to serial port R0 session ( 1r - 32r )
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 (display Port Log)

Function Display the port log of the currently connected serial port.

Execution example

```
tty-1:rw>1
Sep 8 11:16:15 ether: port 1 LINK DOWN.
Sep 8 11:16:15 ether: port 2 LINK DOWN.
           (Display the log of monitored equipment)
:
:
:
```

2 (display Port Log (LAST))

Function Display the most recent part of the ports log of the currently connected serial port.

Explanation Displays approximately the 5000 most recent characters of the port log.

Execution example

```
tty-1:rw>2
:
:
:
Sep 8 11:30:15 ether: port 1 LINK UP.
Sep 8 11:30:25 ether: port 2 LINK UP.
```

3 (start tty connection)

Function Access the monitored equipment.

Execution example

```
tty-1:rw>3
Press "CTRL-A" to return this MENU.
Start tty connection
Welcome to xxxx
XXXXX login:
```

Note See the description of the "set portd tty cmdchar" command for details on how to set "cmdchar".

4 (close telnet/ssh session)

Function Close the session of the currently connected serial port.

Note Only the session in which the command has been entered is closed. The other connected sessions do not change.

5 (show all commands)

Function Display a list of port server menu commands.

Execution example

```
tty-1:rw>5
-- RW1 -----
Host : "NS-2250-1"
Label : L3SW-1
-----
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>
```

Note You can also press "?" or "TAB" to display the port server menu list.

6 (display & erase Port Log)

Function Display and delete the port log of the currently connected serial port.

Note When this command is executed, port logs saved in the USB memory or NS-2250 internal memory are not actually deleted. It simply hides the log displayed with "1: display Port Log".

7 (erase Port Log)

Function Delete the port log of the currently connected serial port.

Note When this command is executed, port logs saved in the USB memory or NS-2250 internal memory are not actually deleted. It simply hides the log displayed with "1: display Port Log".

8 (send Port Log)

Function Forcibly send the port log of the currently connected serial port to the external FTP/email server that has been set.

Note

- If no destination server (FTP or email) has been set for the port logs, nothing happens when you execute this command.
- Only a prompt is displayed when you execute this command.
- The transmission result (success/failure) is not displayed. Check the result on the destination server (FTP or email server).

9 (show Port Log configuration)

Function Display setting information, such as the save space, transfer interval, and transfer destination server of the port log of the currently connected serial port.

Execution example

```
tty-1:rw>9
tty : 1
  Log : on, size : 500KB
  Syslog output: on
  NFS output : on
  loginstamp : on
  Trigger : Interval : 60 min
           : Ratio : 80 %
  SendLog : mail
           : Mail addr : mgr@example.co.jp SMTP server : 192.168.1.251
           : Mail addr : - SMTP server : -
tty-1:rw>
```

10 (send break to tty)

Function Send a break signal to the currently connected serial port.

Note To send a break signal to a serial port with this command, you must first use the "set portd tty brk_char brk" command to make the settings to enable the sending of NTV break characters.

If the above command has not been set ("set portd tty brk_char" setting), no break signal is sent when you execute this command.

7.2 Port selection menu commands

Commands of the port selection menu displayed in the port server when in Select mode.

- *ttyno*
- *ttynor*
- *l*
- *l ttyno-ttyno*
- *d*
- *d ttyno-ttyno*
- *h*
- *e*

When you log in as a port user to the NS-2250 from a Telnet/SSH client, and when the port server connection mode is Select mode, the following port selection menu is displayed.

```
Host : "NS-2250-1 "
login from 192.168.1.1
user (user1) Access TTY List
=====
tty : Label                                RW      RO
-----
  1 : EXAtrax-Tokyo-6F-00001                1        0
  2 : EXAtrax-II                          2        1
  3 : BlueBrick-Makuhari-7F-00001           0       N/A
  4 : BlueBrick-Makuhari-7F-00002           0       N/A
  5 : Switch-1                             1        0
  : (Omitted)
-----
Enter tty number to access serial port
<ttyno>          : connect to serial port RW session ( 1 - 32 )
<ttyno>r         : connect to serial port RO session ( 1r - 32r )
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>
```

ttyno

Function Connect to the specified serial ports in Normal mode.

Execution example

To connect to the serial port 7 in Normal mode.

7

ttynor

Function Connect to the specified serial ports in Normal mode.

Execution example

To connect to the serial port 7 in Monitoring mode.

7r

1

Function Refresh the list of ports to which connection is possible.

ltytno-ttytno

Function Refresh the specified range of ports from list of ports to which connection is possible.

Execution example

To redisplay serial ports 2 to 8.

```
12-8
```

To redisplay serial ports 10 and higher numbers.

```
110-
```

To redisplay serial ports 15 and lower numbers.

```
1-15
```

d

Function Refresh detailed information of the user connected to the serial port (port number, user name, and IP address of Telnet/SSH client).

dttyno-ttyno

Function Refresh detailed information of the users connected to a range serial ports (port number, user name, and IP address of Telnet/SSH client).

Execution example

To redisplay serial ports 2 to 8.

```
d2-8
```

To redisplay serial ports 10 and higher numbers.

```
d10-
```

To redisplay serial ports 15 and lower numbers.

```
d-15
```

h

Function Display a list of port selection menu commands.

Note You can also press "?" or "TAB" to display the port server menu list.

e

Function Close the port selection menu and disconnect the Telnet/SSH session.

Index

Symbols

<i>ttyno</i>	408
<i>ttynor</i>	409
0 (return Port Select Menu)	396
1 (display Port Log)	398
10 (send break to tty)	407
2 (display Port Log (LAST))	399
3 (start tty connection)	400
4 (close telnet/ssh session)	401
5 (show all commands)	402
6 (display & erase Port Log)	403
7 (erase Port Log)	404
8 (send Port Log)	405
9 (show Port Log configuration)	406

A

add logd tty ftp	143
add logd tty mail	142

B

backup system-image	382
---------------------------	-----

C

clear arp	365
clear startup	375
clear system-image	384
console	386
copy startup	377
copy system	379
create allowhost	189
create auth access_group	192
create ip host	46
create ip route	48
create ip6	42
create ip6route	50
create ipfilter	52
create ipsec secret psk	60
create user	97

D

d	412
<i>dttno-ttno</i>	413
date	348
default startup	376
delete allowhost	191
delete auth access_group	220
delete ip host	47
delete ip route	49
delete ip6	45

delete ip6route	51
delete ipfilter	54
delete ipfilter allentry	57
delete ipfilter line	56
delete ipsec secret psk	62
delete user	104
disable bonding	40
disable ftpd	188
disable ipfilter	59
disable ipsec conn	91
disable nfs	130
disable snmp	116
disable sntp	135
disable sshd	186
disable syslog	124
disable telnetd	181
disconnect	367

E

e	415
echo	378
enable bonding	39
enable ftpd	187
enable ipfilter	58
enable ipsec conn	90
enable nfs	129
enable snmp	115
enable sntp	134
enable sshd	185
enable syslog	123
enable telnetd	180
engineering	349
exit	350

F

ftp	372
-----------	-----

H

h	414
hangup	361
history	362

L

l	410
<i>lttno-ttno</i>	411
loginfo	364
loglevel	387
logout	351
logsave	363

P

ping 352
ping6 353

R

reboot 354
remove logd tty ftp 159
remove logd tty mail 158
restore system-image 383

S

set acct mode 222
set acct radius auth_deny_stop 224
set acct radius retry 223
set acct radius server addr 225
set acct radius server key 227
set acct radius server nas_id 229
set acct radius server port 226
set acct radius server timeout 228
set acct tacacs auth_deny_stop 230
set acct tacacs server addr 231
set acct tacacs server key 232
set acct tacacs server timeout 233
set auth mode 195
set auth radius retry 197
set auth radius server addr 198
set auth radius server def_user 209
set auth radius server key 200
set auth radius server nas_id 208
set auth radius server normal 204
set auth radius server port 199
set auth radius server portusr 202
set auth radius server root 206
set auth radius server timeout 201
set auth su_cmd username 196
set auth tacacs def_user 213
set auth tacacs server addr 210
set auth tacacs server key 211
set auth tacacs server timeout 212
set bonding up_delay 38
set community 119
set console 177
set dns 92
set dns localdomain 93
set ether nego 96
set hostname 34
set ip6addr 43
set ipaddr 35
set ipinterface mtu 41
set ipsec conn auto 63
set ipsec conn dpdaction 78
set ipsec conn esp 74
set ipsec conn forceencaps 77
set ipsec conn ike 73
set ipsec conn ikelifetime 75
set ipsec conn keyexchange 72
set ipsec conn left 65

set ipsec conn leftid 64
set ipsec conn leftsourceip 67
set ipsec conn leftsubnet 66
set ipsec conn lifetime 76
set ipsec conn right 69
set ipsec conn rightid 68
set ipsec conn rightsourceip 71
set ipsec conn rightsubnet 70
set logd output 145
set logd tstamp 146
set logd tty log 147
set logd tty lstamp 148
set logd tty mail auth 156
set logd tty mail port 152
set logd tty mail sender 155
set logd tty mail subject 154
set logd tty mail type 153
set logd tty nfs 150
set logd tty sendlog 151
set logd tty syslog 149
set nfs rotate 127
set nfs server addr 125
set nfs server proto 126
set portd auth 162
set portd connect 160
set portd idle_timeout 167
set portd menu 161
set portd ro_timeout 168
set portd sshro 166
set portd sshrw 165
set portd telro 164
set portd telrw 163
set portd tty brk_char 171
set portd tty cmdchar 173
set portd tty label 174
set portd tty limit 170
set portd tty nl 172
set portd tty session 169
set portd tty timeout 175
set snmp authenrap 107
set snmp bondingactswtrap 112
set snmp coldstarttrap 110
set snmp contact 106
set snmp dsrtrap 109
set snmp linktrap 108
set snmp location 105
set snmp powertrap 111
set snmp polltime 132
set snmp server 131
set sshd auth 182
set sshd host_key 184
set sshd port 183
set syslog host 121
set tcpkeepalive 37
set telnet cmdchar 178
set telnetd port 179
set temperature adjust 245

set terminal default editing 237
 set terminal default height 238
 set terminal default page 240
 set terminal default prompt 241
 set terminal default redisp 242
 set terminal default timeout 243
 set terminal default width 239
 set timezone 244
 set trap manager 117
 set tty baud 136
 set tty bichar 137
 set tty detect_dsr 141
 set tty flow 140
 set tty parity 138
 set tty stop 139
 set user password 99
 set user port 100
 set user sshkey 101
 show acct 340
 show acct radius 341
 show acct tacacs 342
 show allowhost 321
 show arp 278
 show auth 327
 show auth access_group 331
 show auth radius 328
 show auth tacacs 330
 show bonding 257
 show config 322
 show config info 325
 show config startup 324
 show console 318
 show cpu 251
 show dns 282
 show environment 249
 show ether 259
 show ip 265
 show ip host 267
 show ip route 268
 show ip6 266
 show ip6route 269
 show ipfilter 283
 show ipinterface 264
 show ipsec conn 288
 show ipsec sad 294
 show ipsec secret 287
 show ipsec spd 293
 show ipsec status 291
 show log 253
 show logd 313
 show memory 252
 show ndp 279
 show nfs 301
 show portd 303
 show portd session 307
 show portd tty 305
 show service 320

show slot 250
 show snmp 297
 show sntp 299
 show stats acct radius 343
 show stats acct tacacs 344
 show stats auth radius 335
 show stats auth tacacs 336
 show stats console 319
 show stats ether 262
 show stats icmp6 276
 show stats ip 272
 show stats ip6 274
 show stats ipfilter 285
 show stats logd tty 316
 show stats tcp 280
 show stats tty 311
 show stats udp 281
 show support 254
 show syslog 300
 show system-image 385
 show tcp 270
 show terminal 326
 show timezone 346
 show tty 309
 show udp 271
 show user 295
 show user login 296
 show version 247
 shutdown 355
 su 356
 switch bonding 360

T

telnet 357
 terminal editing 389
 terminal height 391
 terminal page 390
 terminal prompt 393
 terminal redisp 394
 terminal timeout 388
 terminal width 392
 tftp log 370
 tftp setup 368
 tftp support 371
 tftp verup 369
 trace 366
 traceroute 358
 traceroute6 359

U

unset acct radius server addr 234
 unset acct radius server nas_id 235
 unset acct tacacs server addr 236
 unset auth radius server addr 214
 unset auth radius server nas_id 218
 unset auth radius server normal 216
 unset auth radius server portusr 215

unset auth radius server root.....	217
unset auth tacacs server addr	219
unset community	120
unset dns	94
unset dns localdomain	95
unset ip6addr	44
unset ipaddr	36
unset ipsec conn	79
unset ipsec conn esp	89
unset ipsec conn ike.....	88
unset ipsec conn left	81
unset ipsec conn leftid	80
unset ipsec conn leftsourceip	83
unset ipsec conn leftsubnet	82
unset ipsec conn right.....	85
unset ipsec conn rightid.....	84
unset ipsec conn rightsourceip.....	87
unset ipsec conn rightsubnet	86
unset logd tty mail auth	157
unset nfs server addr.....	128
unset portd tty label.....	176
unset snmp contact	114
unset snmp location	113
unset snmp server.....	133
unset syslog host.....	122
unset trap manager.....	118
unset user sshkey	103
V	
verup cleanup.....	381
verup execute.....	380
W	
write	374

SEIKO

SEIKO SOLUTIONS INC.

8, Nakase 1-chome, Mihama-ku, Chiba-shi, Chiba 261-8507, Japan
tel (+81)43-273-3184
<http://www.seiko-sol.co.jp>