Z0105001-L00-01

RGW series
Setup manual

For Version 1.4.1

ROOT Inc.

1. Setup Method

1.1 Connections

First, it is required to login in order to set up this unit. There are two methods to login; one is through serial line, and two, through telnet or Secure Shell (SSH) from a host on LAN.

When setting up with serial line, we suggest using terminal software such as Hyperterminal for personal computers.

Setup configurations for terminal software are as follows:

Data Transfer Rate: 19200 bps

Character Bit Length: 8

Parity Check: None

Stop Bit Length: 1

Flow Control: RGW 2400/OD - hardware flow←Isn’t it “None”?, as Japanese manual says

To connect with SSH, prior setup by serial line or telnet is required. Refer to "Generating Host key of SSH" (Section 1.7.50).

1.2 Setup

There are two methods for setup:

One is to use command-line shell by command input from console; the other is to directly rewrite configuration file from internal OS shell.

Setup through internal OS shell requires knowledge of both OS and network. Please contact us regarding specific setup method.

1.3 User Mode and Privileged Mode

The command-line shell has two modes which are privileged mode and user mode.

Mode	Description	Prompt
Privileged Mode	A mode that can execute all commands	"$"
User Mode	A mode that can execute only basic commands and display commands	">"

1.4 Setting by Command Line Shell

A login prompt is displayed when connected with telnet:

```
login:
```

Enter user name "admin":

```
login: admin<CR>
```

Proceed to enter password:

Password:xxxxxxxx<CR> (Note: Entered password is not displayed. See Section 3 for factory default user mode password setting.)

When login is accomplished, prompt > is displayed.

When changing the setup, it is required to move to privileged mode.

To move to privileged mode, enter command:

```
>administrator<CR>
```

Proceed to enter password for privileged mode:

password:xxxxxxxx<CR> (Note: Entered password is not displayed. See Section 3 for factory default privileged mode password setting.)

Prompt $ is displayed.

To connect with SSH, please refer to "Generating Host key of SSH" (Section 1.7.50).

1.4.1 List of Command Line Shell Functions

<table>
<tr><th>Function</th><th>Description</th></tr>
<tr><td>Supplement to Command</td><td>By pressing [TAB] key, command string is inserted to the supplemental part possible</td></tr>
<tr><td>Help on Commands</td><td>By pressing [?] key, displays list of available command or description of each command.
Example:
$ip?
*ip address
*ip route add
*ip route delete
Since no command is formed in ip, commands starting with ip are displayed.
$ ip address ?
usage: ip address"Interface Ipaddress Netmask"
e.g. : $ ip address ep0 192.168.0.100 255.255.255.0
Since the command "ip address" is unique, usage and examples are displayed.</td></tr>
<tr><td>Editing Command Line</td><td>This function supports editing of command line.
The key bind of each is as follows:
<table>
<tr><th>Key</th><th>Description</th></tr>
<tr><td>Back Space</td><td>Deletes one character before cursor</td></tr>
<tr><td>Ctrl-A</td><td>Moves cursor to the head of command line</td></tr>
<tr><td>Ctrl-E</td><td>Moves cursor to the end of command line</td></tr>
<tr><td>Ctrl-D</td><td>Deletes the character on cursor</td></tr>
<tr><td>Ctrl-U</td><td>Deletes the entire command line</td></tr>
<tr><td>Ctrl-F (->)</td><td>Moves cursor to the right</td></tr>
<tr><td>Ctrl-B (<-)</td><td>Moves cursor to the left</td></tr>
<tr><td>Ctrl-K</td><td>Deletes the character after cursor</td></tr>
</table></td></tr>
<tr><td>Record of Entered Commands</td><td>Retains records of inputted command
<table>
<tr><th>Key</th><th>Description</th></tr>
<tr><td>Ctrl-P</td><td>Calls previous recorded entry</td></tr>
<tr><td>Ctrl-N</td><td>Calls next recorded entry</td></tr>
</table></td></tr>
</table>

1.5 List of Commands

Setup Item	**Command**
Setting password	passwd
Setting host name	hostname
Setting IP address	ip address
Setting static route	ip route add
Deleting static route	ip route delete
Setting ICMP Redirect send out	ip icmp redirect
Setting wireless frequency	wireless channel
Setting wireless transmission rate	wireless tx rate
Setting wireless WEP function	wireless wep encryption
Setting wireless WEP key number	wireless wep key use
Setting wireless WEP key value	wireless wep key value
Setting wireless port type	wireless port
Setting wireless network name	wireless network
Setting wireless station name	wireless station
Switching infrastructure mode to Access Point	wireless BSS AP mode
Setting wireless SSID	wireless ssid
Adding wireless MAC address filter	wireless macfilter add
Deleting wireless MAC address filter	wireless macfilter delete
Setting static ARP entry	arp add
Deleting ARP entry	arp delete
Setting to choose the use of RIP	rip
Setting to choose to send static route with rip	rip static-supply
Setting RIP action	rip action
Setting RIP version	rip version
Setting to choose the use of filter	filter
Setting Filter	filter add
Deleting Filter	filter delete
Setting to choose the use of NAT	nat
Setting map action of NAT	nat add map
Setting bimap action of nat	nat add bimap

Setting map-block action of nat	nat add map-block
Setting rdr action of nat	nat add rdr
Deleting nat	nat delete
Setting to choose the use of DHCP server	dhcp
Setting IP address to be distributed by DHCP server	dhcp pool
Setting validity period of IP address to be distributed by DHCP server	dhcp expire
Setting DNS server to be distributed by DHCP server	dhcp dns add
Deleting DNS server to be distributed by DHCP server	dhcp dns delete
Setting domain name to be distributed by DHCP server	dhcp domain
Setting default route to be distributed by DHCP server	dhcp defaultroute
Setting DHCP relay agent	dhcp relay
Setting to choose the use of SNMP function	snmp
Setting SNMP community name	snmp community
Setting location of SNMP	snmp location
Setting contact of SNMP	snmp contact
Setting access of SNMP	snmp access
Setting TRAP of SNMP	snmp trap
Setting of syslog	syslog
Setting of host to transfer syslog	syslog host
Setting facility to transfer syslog	syslog add
Deleting facility to transfer syslog	syslog delete
Generating SSH host key	ssh keygen
Setting SSH authenticate method	ssh authentication
Downloading SSH public key	ssh keyget
Setting telnet access	access telnet
Setting monitor access	access monitor
Setting ssh access	access ssh
Save	save
Loading setting contents	load

Cold start	cold start
Updating firmware	update
Setting date and time	date
Displaying software version	show version
Clearing ARP cache	clear arp
Confirming saved contents	show setup
Displaying host name	show hostname
Displaying IP address	show ip address
Displaying static route	show ip route
Displaying date and time	show date
Displaying lease status of DHCP server	show dhcp
Displaying filtering status	show filtering
Displaying status of NAT	show nat
Displaying status of SSH	show ssh
Displaying ARP cache table	show arp
Displaying elapsed time from start	show uptime
Displaying wireless signal strength	show wireless signal strength
Displaying wireless setting	show wireless status
Displaying status of MAC address filter	show wireless macfilter
Displaying wireless infrastructure mode of Access Point	show wireless ap
Displaying SNMP setting	show snmp
Restart	restart
Ping	ping
Log out	quit
Moving to privileged mode	administrator
Displaying command help	help
Referring to command history	history
Close	exit

1.6 Typographical Conventions

Typographical conventions used in the command list are shown below.

Convention	Description	Example(s)
Courier new, regular style	Command	ip address
italics	Indicates a variable which must be replaced with a real value.	ip address *Interface IPaddress Netmask*
square brackets [ ]	The argument within the brackets may be omitted. Do not enter the brackets in the command line.	ssh keygen version [overwrite]
Quotation marks " "	Enclosed expression must be entered exactly as shown (hard coded). Do not enter the quotation marks in the command line.	"all"
| bar (exclusive OR)	You must enter one, and only one, of the items separated by the bar. Do not enter the bar in the command line.	ne0| wi0| lo0
Braces { }	List of arguments from which you must choose an item in syntax descriptions, or an enclosed phrase. Do not enter the braces in the command line.	Port { = | ! | <= | >= } *portNo*

1.7 Explanation of Each Command

Each item is set without the need to restart.

1.7.1 Setting Password

Input format	passwd *user*
Parameter	user - user : Password of user mode - administrator : Password of privileged mode
Description	Sets password
Note	Password for privilege mode executes in only the privilege mode. To discontinue entry, enter Ctrl-D. Only alphabet characters and numerals can be entered in character string. Number of characters is up to 8 characters. To refer or to change the setting will be unable due to loss of password. Also, method to initialize the password (cold start) will be unable due to loss of password.

1.7.2 Setting Host Name

Input format	hostname *hostname*
Parameter	hostname - Hostname with domain name
Description	Sets hostname
Note	Executes only in privileged mode.
Example	$ hostname mypc.mydomain.co.jp

1.7.3 Setting IP Address

Input format	ip address *Interface IPaddress Netmask*
Parameter	-Interface Interface name Ethernet: ne0 Wireless: wi0 -IP address ip address -Netmask netmask

Description	Sets IP address to specified interface.
Example	$ip address wi0 192.168.0.100 255.255.255.0

1.7.4 Setting Static Route

Input format	ip route add *Destination Netmask Gateway*
Parameter	Destination - Destination IP address Netmask - Destination netmask Gateway - IP address of gateway
Description	Sets static route. When Netmask is omitted, host route is set.
Note	Executes only in privileged mode.

Examples	$ ip route add 10.0.0.0 255.0.0.0 192.168.0.1
	$ ip route add default 192.168.0.254 (In case of default mode)
	$ ip route add 192.168.32.3 192.168.33.2 (In case of host route)

1.7.5 Deleting Static Route

Input format	ip route delete *Destination Netmask Gateway*
Parameter	Destination - Destination IP address Netmask -Destination netmask Gateway - IP address of gateway
Description	Deletes static route
Note	Executes only in privilege mode.

Examples	$ ip route delete 10.10.0.0 255.255.0.0
	$ ip route delete default (In case of default route)
	$ ip route delete 192.168.32.3 (In case of host route)

1.7.6 Setting ICMP Redirect Send Out

Input format	ip icmp redirect *flags*
Parameter	flags

	- enable In use - disable Not in use
Description	Chooses use of ICMP Redirect send out function or not.
Example	$ icmp redirect enable

1.7.7 Setting Wireless Frequency

<table>
<tr><td>Input format</td><td>wireless channel <i>Channel</i></td></tr>
<tr><td>Parameter</td><td>Channel</td></tr>
<tr><td>Description</td><td>Sets wireless frequency
<table>
<tr><th>Channel</th><th>Frequency(MHz)</th><th>Channel</th><th>Frequency(MHz)</th></tr>
<tr><td>1</td><td>2412</td><td>8</td><td>2447</td></tr>
<tr><td>2</td><td>2417</td><td>9</td><td>2452</td></tr>
<tr><td>3</td><td>2422</td><td>10</td><td>2457</td></tr>
<tr><td>4</td><td>2427</td><td>11</td><td>2462</td></tr>
<tr><td>5</td><td>2432</td><td>12</td><td>2467</td></tr>
<tr><td>6</td><td>2437</td><td>13</td><td>2472</td></tr>
<tr><td>7</td><td>2442</td><td>14</td><td>2484</td></tr>
</table></td></tr>
<tr><td>Note</td><td>Executes only in privileged mode.</td></tr>
<tr><td>Example</td><td>$ wireless channel 3</td></tr>
</table>

1.7.8 Setting Wireless Transmission Rate

<table>
<tr><td>Input format</td><td>wireless txrate <i>Rate</i></td></tr>
<tr><td>Parameter</td><td>Rate
-Wireless transmission rate 1 – 15
<table>
<tr><th>Value</th><th>Rate</th><th>Value</th><th>Rate</th></tr>
<tr><td>1</td><td>1Mbps fixed</td><td>9</td><td>11 -> 1Mbps</td></tr>
<tr><td>2</td><td>2Mbps fixed</td><td>10</td><td>11 -> 2Mbps</td></tr>
<tr><td>3</td><td>2 -> 1Mbps</td><td>11</td><td>11 -> 2 -> 1Mbps</td></tr>
<tr><td>4</td><td>5.5Mbps fixed</td><td>12</td><td>11 -> 5.5Mbps</td></tr>
<tr><td>5</td><td>5.5 -> 1Mbps</td><td>13</td><td>11 -> 5.5 -> 1Mbps</td></tr>
<tr><td>6</td><td>5.5 -> 2Mbps</td><td>14</td><td>11 -> 5.5 -> 2Mbps</td></tr>
<tr><td>7</td><td>5.5 -> 2 ->1Mbps</td><td>15</td><td>11 -> 5.5 ->2 -> 1Mbps</td></tr>
<tr><td>8</td><td>11Mbps fixed</td><td></td><td></td></tr>
</table></td></tr>
</table>

Description	Sets wireless transmission rate
Note	Executes only in privileged mode in case of infrastructure mode on Access Point, it is not possible to set wireless transmission rate.
Example	$ wireless txrate 8

1.7.9 Setting Wireless WEP Function

Input format	wireless wep encryption *flag*
Parameter	Flag - enable : In use - disable : Not in use
Description	Chooses the use of WEP in case of packet transmission.
Note	Executes only in privileged mode. In case setting of transmission rate is 5.5M or 11Mbps, actual transmission rate may be lowered when WEP is used.
Example	$ wireless wep encryption enable

1.7.10 Setting Wireless WEP Key Number

Input format	wireless wep key use *flag*
Parameter	flag - flag 1 - 4
Description	Sets WEP key number to be used in transmission.
Note	Executes only in privileged mode
Example	$ wireless wep key use 1

1.7.11 Setting WEP Key Value

Input format	wireless wep key value *flag value*
Parameter	flag - key number (1 - 4) value - ASCII (5 characters), or HEX (10 character hexadecimal number starting with 0x.)
Description	Sets WEP key value.
Note	Key length is automatically decided according to length of value.

Example	$ wireless wep key value My Key←the “key number” is missing and 2 ASCII wording (“My” and “Key”). Is this example correct?

1.7.12 Setting Wireless Port Type

Input format	wireless port *value*
Parameter	Value -1: BSS mode (client station in infrastructure mode) -3: Ad-hoc mode (factory set value)
Description	Sets RGW to act as a client station in infrastructure (BSS) or ad hoc mode.
Note	Executes only in privileged mode. This command allows the RGW to function as a wireless client station in an 802.11b basic service set (BSS). To set up the RGW as an Access Point, use the ***wireless BSS AP mode*** command (section 1.7.15). The ***wireless port*** command cannot be used while ***wireless BSS AP mode*** is enabled.
Example	$ wireless port 3

1.7.13 Setting Wireless Network Name

Input format	wireless network *value*
Parameter	value - Network name (SSID) in BSS mode (max. 30 characters)
Description	Sets network name during BSS mode.
Notes	Executes only in privileged mode. Enables communication with an Access Point having the same network name (SSID) when RGW is functioning as a wireless client station in infrastructure mode. To set the network name (SSID) when RGW is functioning as an Access Point, use the ***wireless ssid*** command (section 1.7.16) instead.

Example	$ wireless network NetBSD_IBSS

1.7.14 Setting Wireless Station

Input format	wireless station *value*
Parameter	Value - Station name of BSS mode (max. 30 characters)
Description	Sets station name during BSS mode
Notes	Executes only in privileged mode. Sets a distinguishing name and is valid in wireless port 1 during BSS mode. Some monitoring programs poll the station name of each wireless client in the BSS for identification purposes.
Example	$ wireless station NetBSD_Wave LAN/IEEE_node

1.7.15 Switching to Wireless Infrastructure Mode of Access Point

Input format	wireless BSS AP mode *flag*
Parameter	flag - enable: Set infrastructure mode of Access Point - disable: Delete infrastructure mode of Access Point
Description	Sets RGW to function as the Access Point in an 802.11b BSS.
Notes	Executes only in privileged mode. Access Point is enabled [disabled] after the following commands are entered: 1. wireless BSS AP mode enable [disable] 2. save 3. restart 4. save When flag is set to disable, RGW operates in ad-hoc mode. Important note: The SSID cannot be modified after wireless BSS AP mode is enabled. SSID parameter should be set using ***wireless ssid*** command (section 1.7.16) prior to enabling wireless BSS AP mode.
Example	$ wireless BSS AP mode enable

1.7.16 Setting Wireless SSID

Input format	wireless ssid *value*
Parameter	value -SSID of infrastructure mode (max. 30 characters)
Description	Specifies SSID during infrastructure mode of Access Point.
Notes	Executes only in privileged mode. Enables communication with station of BSS mode having same network name. This command can only be used when Access Point mode of infrastructure is in operation.
Example	$ wireless ssid NetBSD_IBSS

1.7.17 MAC Address Filter

Input format	wireless macfilter add *param*
Parameter	Param - Specify MAC address
Description	Sets MAC address that permits wireless LAN communication.
Notes	Executes only in privileged mode. Permits communication with all wireless terminal, when MAC address is not set. Maximum number of entries of MAC address filter is 50.
Example	$wireless macfilter add 11:22:33:44:55:66

1.7.18 Deleting MAC Address Filter

Input format	wireless macfilter delete *param*
Parameter	param - Specify MAC address
Description	Deletes MAC address that registered into MAC address filter.
Note	Executes only in privileged mode. Permits communication with all wireless terminal when MAC address is not set.
Example	$ wireless macfilter delete 11:22:33:44:55:66

1.7.19 Setting Use or Non Use of RIP

Input format	rip *flag*
Parameter	flag - enable : use - disable : Not in use
Description	Chooses to use RIP or not.
Note	Executes only in privileged mode
Example	$ rip enable

1.7.20 Setting to Announce Static Route in RIP

Input format	rip static-supply *flag*
Parameter	flag - enable : Announce static route - disable : Do not Announce static route
Description	Sets to announce static route in RIP
Note	Executes only in privileged mode.
Example	$ rip static-supply enable

1.7.21 Setting Rip Action

Input format	rip action *interface action*
Parameter	interface - interface name action - supply : Send and receive route - listen : Receives route only

	- disable : Neither send nor receive route
Description	Sets RIP action
Note	Executes only in privileged mode.
Example	rip action wi0 supply

1.7.22 Setting RIP Version

Input format	rip version *interface version*
Parameter	interface -interface name version - ripv2:Uses RIPv2 (multicast) - ripv12:Uses RIPv2 (multicast) and RIPv1 (broadcast). - ripv1:Uses RIPv1 (broadcast).
Description	Sets RIP version.
Notes	Executes only in privileged mode.
Example	$ rip version wi0 ripv2

1.7.23 Setting to Use Filter

Input format	Filter *flag*
Parameter	flag - enable : In use - disable : Not in use
Description	Chooses to use IP filter or not
Note	Executes only in privileged mode.
Example	$ filter enable

1.7.24 Setting IP Filter

Input format	filter add *number action inout* [*log level facility.level*][quick] [on *interface*] [proto *proto*] [from [!] *address* [port] to [!] *address* [port]] [*flags*] [with] [keep] [*group*]
Parameter	number -0-655335 : Filter No. action

	- block: puts mark on the packet to be cancelled. - pass: Puts mark on the packet to be passed. inout - in: A rule for a packet which enters from interface and enters RGW. - out: A rule for a packet which exits from RGW to interface. log - log: Specifies “log” keyword to log IP filtering - level: Specifies syslog facility and level preceded by “level” keyword - facility: facility of syslog (auth, user, daemon) - level: level of syslog (info, notice, warning, err...) Transfer to host specified by syslog command mentioned in later quick - quick: adapts immediately to rule on interface - on ne0| wi0| lo0 : Specifies interface proto - tcp/udp | udp | tcp | icmp address - any | 1.2.3.4/24 format | 1.2.3.4 mask 255.255.255.0 format port - port{= | ! | <|> | <= | > = | eq | ne | lt | gt | le | ge} portNo flags - Combination of TCP flag, FSRPAU. Can be specified during proto tcp(F=FIN, S=SYN, R=RST, P=PUSH, A=ACK, U=URG) with - with ipopts : with IP option - with short : extremely short packet - with frag : fragmented packet keep - keep state : implements filtering by keep state controlling condition of session group - head N : makes new group N

	- group N : sets rule in group N
Description	Sets filtering for IP packet
Note	Executes only in privileged mode. Sorted according to filter No. and set in ascending order.
Example	$ filter add 100 block out proto tcp from 100.100.0.0/16 to any port = 80

1.7.25 Deleting IP Filter

Input format	filter delete *number*
Parameter	number - 0-65535 : filter No.
Description	Deletes filtering for IP packet
Note	Executes only in privileged mode.
Example	$ filter delete 100

1.7.26 Setting the Use of NAT

Input format	nat *flag*
Parameter	flag - enable : Use - disable : No use
Description	Chooses use or no use of NAT.
Note	Executes only in privileged mode. NAT function in Ethernet side will be valid when switched to enable , factory set (wireless side: global and Ethernet side: private).
Example	$ nat enable

1.7.27 Setting map Action of NAT

Input format	nat add map *number interface address1* -> *address2* [portmap *Proto ports*| proxy port *portname tag/protocol*]
Parameter	Number - 0-255 : NAT No. (common at nat add * command) interface - name of interface address1

	- IP address on local side - 1.2.3.4/xx format address2 - IP address on global side - 1.2.3.4/xx format proto - tcp/udp|udp|tcp ports - auto|{lower limit of port No.}:{upper limit of port No.} format portname - name of port (eg: ftp) tag - tag protocol - protocol
Description	Sets map action of NAT
Notes	Executes only in privileged mode. Sorted according to nat No. common to nat setup and set in ascending order
Examples	$ nat add map 10 ne0 10.0.0/8-> 210.100.100.101/32 portmap tcp/udp 1025:65000 $ nat add map 15 ne0 10.0.0/8-> 0/32 proxy port ftp ftp/tcp

1.7.28 Setting bimap Action of NAT

Input format	nat add bimap *number interface address1* -> *address2*
Parameter	number - 0-255 : NAT No. (common at nat add command) interface - name of interface address1 - IP address on local side - 1.2.3.4/xx format address2 - IP address on global side - 1.2.3.4/xx format

Description	Sets bimap action of NAT
Notes	Executes only in privileged mode. Sorted according to nat No. common to nat setup and set in ascending order.
Example	$ nat add bimap 3 ne 10.0.0.5/32 -> 210.100.100.101/32

1.7.29 Setting map-block Action of NAT

Input format	nat add map-block *number interface address1* -> *address2* [ports *port*]
Parameter	number - 0-255 : NAT No.(common at nat add*command) interface - name of interface address1 - IP address on local side - 1.2.3.4/xx format adderss2 - IP address on global side - 1.2.3.4/xx format port - auto|port No.
Description	Sets mapblock action of NAT
Note	Executes only in privileged mode. Sorted according to nat No. common to nat setup and set in ascending order.
Example	$ nat add map-block 2 ne 10.0.0.5/8 -> 210.100.100.101/24 ports auto

1.7.30 Setting rdr Action of NAT

Input format	nat add rdr *number interface address1* port *port ->address2* port *port proto*
Parameter	number - 0-255 : NAT No. (common at nat add* command) interface - name of interface address1 - IP address on local side - 1.2.3.4/24 format address2 - IP address on global side port - Port No. proto - tcp/udp|tcp|udp (default value: tcp)
Description	Sets rdr action of NAT
Notes	Executes only in privileged mode. Sorted according to nat No. common to nat setup and set in ascending order.
Example	$ nat add rdr 5 ne0 10.0.0.5/32 port 7777 -> 210.100.100.101 port 20

1.7.31 Deleting NAT

Input format	nat delete *number*
Parameter	number - 0-255 : NAT No.
Description	Deletes NAT entry
Note	Executes only in privileged mode
Example	$ nat delete 3

1.7.32 Setting to Choose the Use of DHCP server

Input format	nat *flag* [*interface*]
Parameter	flag - enable : Use - disable : Not in Use interface - name of interface using DHCP server function. It assumes ne0 when omitted. Not required during disable.
Description	Chooses between use and no use of DHCP server function.
Notes	Executes only in privileged mode. Distribute IP address must be in the interface network. Refer to limitation for details.
Example	$ dhcp enable

1.7.33 Setting IP Address Range to be Distributed through DHCP server

Input format	dhcp pool *ipaddress1 ipaddress2*
Parameter	ipaddress 1 - Head of IP address ipaddress2 - End of IP address Description Sets range of IP address to be distributed through DHCP server.
Note	Executes only in privileged mode.
Example	$ dhcp pool 192.168.0.1 192.168.0.254

1.7.34 Setting Expiration of IP Address to be distributed through DHCP server

Input format	dhcp expire *period*
Parameter	period - Expiration of IP address (Second)
Description	Sets expiration of IP address to be distributed through DHCP server.
Note	Executes only in privileged mode.
Example	$ dhcp expire 7200

1.7.35 Setting DNS Server to be distributed through DHCP server

Input format	dhcp dns add *ipaddress*
Parameter	ipaddress * IP address of DNS server
Description	Sets DNS server to be distributed through DHCP server.
Note	Executes only in privileged mode. Maximum of 2 can be registered.
Example	$ dhcp dns add 210.100.100.101

1.7.36 Deleting DNS Server to be distributed through DHCP server

Input format	dhcp dns delete *ipaddress*
Parameter	ip address -iP address of DNS server
Description	Deletes DNS server to be distributed through DHCP server.
Note	Executes only in privileged mode.
Example	$ dhcp dns delete 210.100.100.101

1.7.37 Setting Domain Name to be distributed through DHCP server

Input format	dhcp domain *domainname*
Parameter	domainname - Domain name
Description	Sets domain name to be distributed through DHCP server. When domainname is omitted, domain name is not distributed.
Note	Executes only in privileged mode.
Example	$ dhcp domain root-hq.com

1.7.38 Setting Default Route to be distributed through DHCP server

Input format	dhcp defaultroute [*defaultroute*]
Parameter	defaultroute -IP address of default route
Description	Sets default route to be distributed through DHCP server. When defaultroute is omitted, default route is not distributed.
Note	Executes only in privileged mode.
Example	$ dhcp defaultroute 172.30.100.2

1.7.39 Setting DHCP Relay Agent

Input format	dhcp relay *flag*
Parameter	flag - IP address : IP address of DHCP server - disable : Not in use
Description	Sets DHCP relay agent.
Note	Executes only in privileged mode.
Example	$ dhcp relay 172.10.0.1

1.7.40 Setting to Choose the Use of SNMP Server Function

Input format	snmp *flag*
Parameter	flag - enable : Use - disable : Not in use
Description	Chooses use and no use of SNMP server.
Note	Executes only in privileged mode.
Example	$ snmp enable

1.7.41 Setting SNMP Community Name

Input format	snmp community ***name***
Parameter	name - community name
Description	Sets SNMP community name. Up to maximum of 31 characters.
Note	Executes only in privileged mode.
Example	$ snmp community secret

1.7.42 Setting Location of SNMP

Input format	snmp location *str*
Parameter	str - Character string
Description	Sets location of SNMP. Up to maximum of 255 characters.
Note	Executes only in privileged mode.

Example	$ snmp location 1-17-8 Nishikata Bunkyo-ku Tokyo Japan

1.7.43 Setting Contact of SNMP

Input format	snmp contact *str*
Parameter	str - Character string
Description	Sets contact of SNMP. Up To maximum of 255 characters.
Note	Executes only in privileged mode.
Example	$ snmp contact Tarou Yamada <taro@root-hq.com>

1.7.44 Setting Access of SNMP

Input format	snmp access [*ipaddress*|*network*]
Parameter	ipaddress -ip address | "all" network -network address with netmask 255.255.255.0 format
Description	Specifies accessible host range to RGW with SNMP .
Notes	Executes only in privileged mode. Checking of IP filter is implemented prior to checking the setting of this access.
Example	$ snmp access 192.168.0.0 255.255.255.0

1.7.45 Setting SNMP TRAP

Input format	snmp trap *mode flag* [*community* [*port*]]
Parameter	mode - v1|v2|inform v1:snmp v1 v2:snmp v2 inform:NOTIFICATION flag

	- IP address : host of IP address sending the trap - disable : not in use community name of community used for sending trap and not required during disable port - port No. (use 162 during omission) not required during disable
Description	Specifies type of trap and host sending snmp trap when restarted and/or detected invalid access.
Note	Executes only in privileged mode.
Example	$ snmp trap v2 210.100.100.101 root

1.7.46 Setting to Choose the Use of syslog Function

Input format	syslog *flag*
Parameter	flag - enable : use - disable : not in use
Description	Chooses use and no use of syslog function.
Note	Executes only in privileged mode.
Example	$ syslog enable

1.7.47 Setting Host to Transfer syslog

Input format	syslog host *ipaddress*
Parameter	ipaddress - IP address : IP address of host to transfer syslog
Description	Sets IP address of host to transfer syslog.
Note	Executes only in privileged mode.
Example	$ syslog host 172.10.0.1

1.7.48 Setting Facility to Transfer syslog

Input format	syslog add *facility level*

Parameter	facility kern | user | auth | authpriv | syslog | cron | ftp | uucp | local0-7 | daemon |* level emerg | alert | crit | err | warning | notice | info | debug | none | *
Description	Sets facility and its level to transfer syslog.
Note	Executes only in privileged mode.
Example	$ syslog add * info

1.7.49 Deleting Facility to Transfer syslog

Input format	syslog delete *facility level*
Parameter	facility kern | user | auth authpriv| syslog | cron | ftp | uucp | local0-7| daemon |* level emerg | alert | crit | err | warning | notice | info | debug | none | *
Description	Sets facility and its level to delete syslog.
Note	Executes only in privileged mode.
Example	$ syslog delete kern crit

1.7.50 Generating Host Key of SSH

Input format	ssh keygen *version* [overwrite←Isn't it better to enclose it with " "? because it is hard coding]
Parameter	version - v1 : generate host key of SSHv1 - v2 : generate host key of SSHv2 - v12 : generate host key of both SSHv1 and SSHv2

	overwrite Specified when overwriting host key already generated
Description	Generates host key of RGW
Notes	Executes only in privileged mode. It takes a while to complete this command. To specify v2 and v12, Ver 1.4.0 and latter only can be used.
Example	$ ssh keygen v1

1.7.51 Setting Authentication Method of SSH

Input format	ssh authentication *way*
Parameter	way - passwd: password authentication is valid - key: public key authentication is valid - both: both password and public key authentications are valid
Description	Specifies authentication method of SSH.
Notes	Executes only in privileged mode. Factory set default: both.
Example	$ ssh authentication key

1.7.52 Downloading Public Key of SSH

Input format	ssh keyget *version URL*
Parameter	version - v1 : download public key of SSHv1 - v2 : download public key of SSHv2 URL - URL with open key
Description	Downloads public key to RGW.
Notes	An access will be valid with public key downloaded by this command. Executes only in privileged mode. To specify v2, Ver 1.4.0 and later only can be used.

Example	$ ssh keyget v1 http://192.168.0.12/~rgw/identity.pub

1.7.53 Switching Version of SSH

Input format	ssh version *version*
Parameter	version - v1: SSHv1 - v2: SSHv2 - v12: both
Description	Switches Version of SSH
Notes	An access will be valid with specified SSH version by this command. Executes only in privileged mode. Ver 1.4.0 and later only can be used on this command.
Example	$ ssh version v12

1.7.54 Setting telnet Access

Input format	access telnet [*ipaddress*|*network*]
Parameter	ipaddress - IP address | "all" network - network address having netmask 255.255.255.0 format
Description	Specifies host range possible to access to RGW with telnet.
Notes	Executes only in privileged mode. Checking IP filter is implemented prior to checking setup access
Example	

1.7.55 Setting http Access

Input format	access http [*ipaddress*|*network*]
Parameter	
Description	
Notes	
Example	

↑This command explanation is missing.

1.7.56 Setting monitor Access

Input format	access monitor [*ipaddress*|*network*]
Parameter	ipaddress - IP address | "all" network - network address having netmask 255.255.255.0 format
Description	Specifies host range possible to access to RGW with monitor.
Notes	Executes only in privileged mode. Checking IP filter is implemented prior to checking setup access. The monitor is an application which displays wireless condition of RGW that operates on Windows. It can be downloaded from ROOT Inc. home page.
Example	

1.7.57 Setting SSH Access

Input format	access ssh [*ipaddress*|*network*]
Parameter	ipaddress - IP address | "all" network - network address having netmask 255.255.255.0 format
Description	Specifies host range possible to access to RGW with ssh.
Notes	Executes only in privileged mode. Checking IP filter is implemented prior to checking setup access.
Example	

1.7.58 Save

Input format	save
Parameter	None
Description	Saves setup contents.
Notes	Executes only in privileged mode. Reflected on system file and setup file is saved in command format.

1.7.59 Setting Static ARP

Input format	arp add *ipaddress macaddress*
Parameter	ipaddress - IP address macaddress - MAC address
Description	Sets entry of static ARP
Example	$ arp add 10.0.0.1 11:22:33:44:55:66

1.7.60 Deleting ARP

Input format	arp delete *ipaddress*
Parameter	ipaddress - IP address
Description	Deletes ARP entry set to IP address.
Note	Executes only in privileged mode.
Example	$ arp delete 10.0.0.1

1.7.61 Loading Setup with tftp

Input format	load tftp *ipaddress file*
Parameter	ipaddress -IP address | disable file -load specified file (not required during disable)
Description	Loads contents of file.
Notes	Executes only in privileged mode. When save is implemented after specifying tftp server with this command, load of setup file with tftp is implemented during restart. To get with tftp during start, implement after setup of default route, and overwrite parameters that were already set.
Example	

1.7.62 Cold Start

Input format	cold start

Parameter	None
Description	Returns equipment to factory default setting.
Note	Executes only in privileged mode. Restarts after returning to factory default setting.

1.7.63 Updating Firmware

Input format	update *url*
Parameter	url - URL of file to be downloaded
Description	Downloads file and update firmware.
Note	Executes only in privileged mode.
Example	

1.7.64 Setting Date and Time

Input format	date *yyyy/mm/dd HH:MM*
Parameter	yyyy - Year mm - Month dd - Day HH - Hour MM - Minute
Description	Sets date and time.
Note	When this command is set, it is reflected on system.
Example	$ date 2000/12/24 12:30

1.7.65 Restart

Input format	restart
Parameter	None
Description	Restarts system.

Notes	Executes only in privileged mode. This function is possible by reboot.

1.7.66 Clearing ARP Cache

Input format	clear arp
Parameter	None
Description	Clears ARP cache table.
Note	Executes only in privileged mode.

1.7.67 Displaying Host Name

Input format	show hostname
Parameter	None
Description	Displays host name registered in system.
Note	

1.7.68 Displaying IP Address

Input format	show ip address
Parameter	None
Description	Displays IP address registered in system.
Note	Displays IP address allocated to wireless and ethernet

1.7.69 Displaying Static Route

Input format	show ip route
Parameter	None
Description	Displays static route registered in system.
Note	Does not display route that is automatically generated by kernel (route to directly connected network etc.).

1.7.70 Displaying Lease Status of DHCP server

Input format	show dhcp
Parameter	None

Description	Displays lease status of DHCP server
Note	None

1.7.71 Displaying Filtering

Input format	show filtering
Parameter	None
Description	Displays status of filtering (Number of packet that matches rule).
Note	Head number of each rule is number of packet that matches rule and is not a filter number. To display filter number, use show setup command.

1.7.72 Displaying ARP Cache Table

Input format	show arp
Parameter	None
Description	Displays ARP cache table.
Note	

1.7.73 Displaying Elapsed Time from Start

Input format	show uptime
Parameter	None
Description	Displays elapsed time from start.
Note	

1.7.74 Displaying Firmware Version

Input format	show version
Parameter	None
Description	Displays this command line shell and information on OS version.

1.7.75 Displaying Date and Time

Input format	show date
Parameter	None
Description	Displays present date and time.

1.7.76 Displaying Wireless Signal Strength

Input format	Show wireless signal strength
Parameter	None
Description	Displays wireless signal strength.
Note	

1.7.77 Displaying Wireless Setting

Input format	Show wireless status
Parameter	None
Description	Displays wireless status
Note	This command is intended to display status of internal driver as maintenance purpose. To confirm setting value use show setup command.

1.7.78 Displaying Access Point Mode on Wireless Infrastructure

Input format	show wireless AP
Parameter	None
Description	Displays Access Point mode on wireless infrastructure.
Note	This command displays to confirm Access Point mode on infrastructure.

1.7.79 Displaying SNMP Setting

Input format	show snmp
Parameter	None
Description	Displays SNMP setting.

Note	

1.7.80 Displaying SSH Setting

Input format	show ssh
Parameter	None
Description	Displays SSH status.
Note	

1.7.81 Checking Contents of Setting

Input format	show setup
Parameter	None
Description	Checks contents of setting.

1.7.82 Checking Saved Contents of Command Format

Input format	show config
Parameter	None
Description	Checks saved contents of command format.
Note	

1.7.83 ping

Input format	ping *Ipaddress*
Parameter	Ipaddress - IP address of remote side
Description	Issues ICMP Echo to IP address of remote side.
Note	

1.7.84 Log Out

Input format	quit or exit
Parameter	None
Description	Logs out from command line shell.

Note	

1.7.85 Moving to Privileged Mode

Input format	administrator
Parameter	None
Description	Moves to privileged mode.
Note	

1.7.86 Displaying Command Help

Input format	help *command*
Parameter	None
Description	Displays help of commands.

1.7.87 Referring to History

Input format	history
Parameter	None
Description	Displays present history.
Note	

Note

The command line shell can be implemented through serial line, telnet, or SSH, but following message is displayed when multiple numbers of command line shells are operated simultaneously.

WARNING: another administrator is still alive (Detected when command line shell is already in operation)

ATTENTION: Two or more administrator are active now!!! (Displayed to all command line shell in operation)

When a separate setting is implemented simultaneously a setting which can not be anticipated may occur. In such case, it is recommended to implement minimum amount of settings then restart.

The command line shell observes non-communication time when there is no input for approximately 300 seconds, the session is shutdown automatically.
However, non-communication observation is not implemented during operation of each command.

1.8 Limitations

The command line shell has following limitations:

1.8.1 DHCP

To start DHCP it is required to set each item of DHCP and press command
"$ dhcp enable."

1.8.2 Others

Please refer to "4. Tips and Hints for Setup."

3. Factory Default Settings

The settings when leaving our factory are as follows:

Data Settings	Contents
User Mode user name	"admin"
User Mode Password	"admin"
Privileged Mode Password	"admin"
Host Name	rgw
IP Address and Netmask	Ethernet Side: 172.30.100.2/24 Wireless Side: 10.12.1.2/24
Static Route	None
Default Route	10.12.1.1
Access Control	None
RIP	Not Used
SNMP	Used. No trap.
DHCP	Not Used
IP Filter	Not Used
MAC Address Filter	Not Used
NAT	Not Used
SYSLOG	Not Used
Load Tftp	Not Used
SSH: Version implemented	SSHv1
SSH: Generating Host Key	Not Generated
SSH: Public Key Download	Not Set
SSH: Authentication Method	Password Authentication/public key Authentication
Wireless Communication Mode	Ad-Hoc Mode

4. Tips and Hints for Setting Up

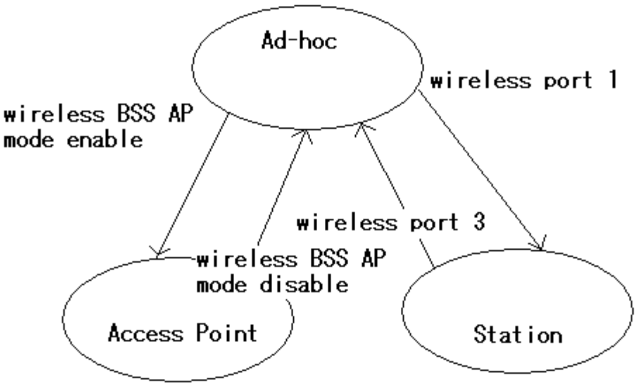
A various knacks for setting up RGW are described in this chapter:

4.1 Wireless

4.1.1 Communication Mode

In wireless communication of RGW, there are 2 modes: Ad infrastructure.

The switching for these are implemented by using wireless setup of command line shell. The factory default setting is in Ad-hoc, and to change to infrastructure mode an Ad-hoc mode is implemented.



In order to make RGW to Access Point of infrastructure mode, it is implemented by wireless BSS AP mode enable command from Ad-hoc mode. However, you must save & reboot after that. After restart, it operates as Access Point of infrastructure mode, so that make required settings, and save. This enables to keep the setting of RGW as Access Point of infrastructure mode.

Following is summary of switch over to infrastructure mode:

-1. Various settings

-2. wireless BSS AP mode enable
-3. save (store setting)
-4. reboot (restart RGW)
-5. After restart, other settings
-6. save (store setting)

(Note: Even if no change is made in "5. other settings", please make sure to implement "6. save.")

It is not possible to directly switch Access Point of infrastructure mode to Station of infrastructure mode.
It is necessary once to switch Access Point to Ad-hoc mode from wireless BSS AP mode disable.
The following steps are made to switch from Access Point of infrastructure mode to Ad-hoc mode:

-1. wireless BSS AP mode disable
-2. save (store setting)
-3. reboot (restart RGW)
-4. After restart, save (store setting)
(Note: Please make sure to "4. save" after restart.)

The wireless port command is used to switch Ad-hoc mode and Station of infrastructure mode. Use of this command immediately switches the mode of RGW , and there is no need to restart.

Please note that when above switching of modes are made with wireless links•Athe link will be disconnected when operation switch over.

On Access Point of infrastructure mode, there are following limitations:

- * On wireless relay, MAC address filter and IP filter do not work.
- * There is no roaming function. The RGW does not support an Extended Service

Set (ESS).

- * The wireless transfer rate depends on the settings on the client station side. That is why it is not possible to set the wireless txrate command in AP mode. Also, when Access Point is observed by monitor program, the transfer rate does not indicate a valid value. (does this mean that the transfer rate observed by the monitor program is inaccurate, or that the invalid value ‘0’ is shown?)
- * The possible link of Station is 200 maximum.

Since, on infrastructure mode flow of beacon and control data, general, an the actual rate is lower than Ad-hoc mode.

4.1.2 WEP

It is possible to encrypt the data (MPDU) that RGW transmits on air. In order to code this, WEP (Wired Equivalent Privacy), a secret key method can be used. Up to 4 keys can be registered for each RGW. Since WEP require coding and compounding processes, an actual transfer rate may be lowered in comparison without using the WEP. For details, please refer to our home page.

4.1.3 Wireless Relay

A single unit of RGW enables wireless packet relay.
There are 2 methods for relaying:

When wireless port type is Ad-hoc, relay is in IP layer.
On infrastructure mode, Access Point implements relay in MAC layer.

However, relay with a single unit becomes a transfer using a same wireless channel as actual rate is lowered to below 1/2.
On relay in IP layer, the station implemented must set in an order as not to send out ICMP redirect.
Depending upon its condition, host routing becomes required. For details, please refer to our home page.
On relay in MAC layer, please note that IP filter and MAC address filter do not work at the station implementing relay.

By using 2 units of RGW linked both with Ethernet, each RGW is enable to be used with different wireless channels, so that generally an actual rate increases than relaying with a single RGW.

4.2 Fire Wall

4.2.1 IP Filter

The syntax of IP filter rule is explained in the previous chapter, but terms of each parameter with examples are mentioned here:

Once more, syntax of filter rule is indicated:

```
filter add  number action inout [log level facility.level] [quick] [on interface]
[proto proto] [from[!] address [port] to [!] address [port]][flags][with]
[keep][group]
```

Each filter rule has a number, and IP packet received by RGW is assessed in order by all rules. And, it is processed accordingly to finally matched rule (There are exceptions which is mentioned later).
The IP filter of RGW is set to default permit (pass). In other words, a packet do not matches to any rule is permitted.
In addition, filter number having order and rule sequence to set RGW is an independent one.

* For action, set "pass" or "block", and when it matches the rule specify action of either pass or cancel.

* For inout, set "in" or "out", and specify either packet going in RGW or going out of RGW.

```
filter add 10 block in from any to any
filter add 11 pass in from any to any
```

When these 2 rules are specified, all packets received by RGW initially checks rule No.10. All packet matches and becomes action of block(cancel). Furthermore, rule No.11 is checked next. All packet matches at No.11 and becomes action of pass (pass). From above results, operation (pass) of rule No.11 which finally matched is implemented. After all, in case of above 2 rules all packet passes.

* For quick, it is possible to specify "quick." When a packet matches rule specified "quick", this packet is not assessed in later filter rule.
  For example, in order to RGW to un-pass packet from host 192.168.1.2, when received packet from this address, block it, and there is no longer a need to check the rule. In such a case, by specifying quick keyword an action is immediately applied in case it matches it.

```
filter add 15 block in quick from 192.168.1.2 to any
filter add 16 pass in from any to any
```

In this setting, the packet from 192.168.1.2 is blocked (block) by rule No.15 specified by quick.
In the next rule No.16, it is intended to pass all packets, but packet matched to rule No.15 is specified as quick, checking of next rule is not applied.

* On "on interface", it is possible to specify wi0 (wireless side) and ne0 (ethernet side). Also, lo0 (loopback device) can be specified too. On internal RGW, it possesses IP address 127.0.0.1 in device lo0, and it is used for internal process.
  It is not possible to access externally to this address. On the contrary, please note that an trouble may occur to operation of RGW when any access is blocked (block) to 127.0.0.1 of device lo0. When this "on interface" keyword does not exist, all interface, ne0, wi0 and lo0, become the target.

```
filter add 20 pass in quick on lo0 from any to 127.0.0.1
filter add 21 block in from 192.168.0.0/16 to any
filter add 22 pass in on wi0 from 192.168.0.0/24 to any
filter add 23 block out on ne0 from 172.16.0.0/12 to any
```

On rule No.20, an access of loop back device is immediately permitted.

On rule No.21, the packet is blocked (block) from address for private network 192.168.0.0/16 that is already reserved.

The wireless side (wi0), however, is linked to network of 192.168.0.0/24 so that on No.22, pass is specified only in 192.168.0.0/24.

Since it follows finally matched rule, the rule up to this point, for example, when packet from 192.168.0.3 comes from wireless side becomes pass, but packet from Ethernet side and/or 192.168.1.2 is blocked (block).
The rule No.23 is to prevent packet from address 172.16.0.0/12 for reserved private network to going to Ethernet side.

On proto, is possible to specify "tcp/udp", "tcp", "udp", or "icmp", and based on these protocol classifications the filter rule can be set. When there is no proto, it matches all classifications. In the example below, packets tcp and udp from Ethernet side passes (pass), but icmp from Ethernet side is blocked (block).

```
filter add 40 pass in on ne0 proto tcp/udp from any to any
filter add 41 block in on ne0 proto icmp from any to any
```

* As you understand already, the rule can be set on packet by specifying IP address and/or network such as from and to.
Also, "any" which expresses all hosts can be specified.

On port, port number for TCP/UDP can be specified, and filter rule specified with specific port can be set. The port is valid in TCP and UDP packets. Also, when port is not specified all ports becomes the target of rule. In the following example, TCP packet directed to port No.80 from wireless side passes (pass).

```
filter add 50 pass in on wi0 proto tcp from any to any port = 80
```

On flags, it is possible to specify F(FIN),S(SYN),R(RST),P(PUSH),(ACK), U(URG) of TCP flag, and it is also possible to set filter rule according to type of flags. The packet of TCP flag which do not match specified in flags do not match filter rule.

On with, it is possible to specify "ipopts","short",or "frag." ipopt can detect packet having IP option on IP header. short can improperly detect
packet with short IP header. frag can detect fragmented IP header.

```
filter add 60 block in quick from any to any with short
```

In this filter rule, packet with improperly short IP header is immediately blocked (block).

When keep state is specified, it is possible to set filter rule controlling the status. When keep state is specified, a new TCP session is settled and information of this session is stored internally. And the packet after this session which is stored in RGW can implement to pass without having to check with separate filter in both directions. Even in case of UDP packet when keep state is specified, IP address and port No. of UDP packet is stored in memory for 600 seconds, and can pass only UDP packet of reverse direction with same IP address and port No. On icmp, when keep state is specified, the reply in respect to this icmp can pass for 600 seconds.

```
filter add 70 pass out quick on ne0 proto udp from any to any keep state
filter add 71 pass out quick on ne0 proto tcp from any to any flags S keep state
filter add 72 block in quick on ne0 proto tcp from any to any flags FUP
```

On rule No.70, it passes (pass) udp packet going out to Ethernet side,
and passes (pass) udp packet of this response for 600 seconds.
On rule No.71, it passes (pass) tcp packet with S flag going out to Ethernet side, and after that passes (pass) packet of session input/output wise.
On rule No.72 when a packet of flag F(FIN),U(URG),P(PSH) comes from Ethernet side, it is immediately blocked (block). However, it does not reach this rule when the status is controlled in rule from previous checking of No.70 and 71.

The head is an indicator to give discrimination number to the packet that matches filter rule. The packet which matched this rule checks discrimination number by filter rule in the group. With these head and group, group of filter rule can be generated. In addition, by specifying quick on filter rule with this head, after checking the rule with same group of that discrimination number, checking of other rules is not applied.

```
filter add 100 pass in on ne0 from any to any
filter add 101 block in quick on ne0 from 192.168.0.0/24 to any
filter add 102 block in quick on ne0 from 172.16.0.0/12 to any
filter add 110 block out on wi0 from any to any
filter add 111 pass out quick on wi0 proto tcp/udp from any to any flags S keep state
filter add 112 pass out quick on wi0 proto icmp from any to any keep state
```

When above set of rule is optimized by head and group, it becomes as follows:

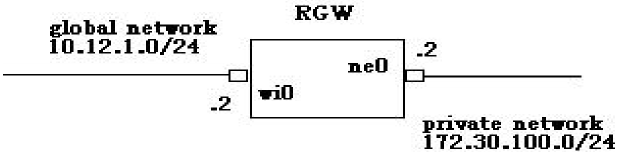
```
filter add 100 pass in on ne0 from any to any head 1
filter add 101 block in quick on ne0 from 192.168.0.0/24 to any group 1
filter add 102 block in quick on ne0 from 172.16.0.0/12 to any group1
filter add 110 block out on wi0 from any to any head 2
filter add 111 pass out quick on wi0 proto tcp/udp from any to any flags  S keep state
group 2
filter add 112 pass out quick on wi0 proto icmp from any to any keep state group 2
```

On set of rule optimized by head and group when rule No.100 matches first, rules No.101 to 102 are checked in order. The rules No.101 to 102 are specified by quick so that it is immediately blocked (block) when matched. When it does not match the rules from No. 101 to 102, it is immediately passed (pass) from rule of No.100.

The packet going out to wireless side (wi0) do not match rule of No.100, so that the next rule to be assessed becomes No.110. When it matches rule of No.110, rules of No.111 and 112 are checked in order. When it matches each an action appropriate to each rule is applied. When it does not match rules of No.111 and 112, the block of action of No.110 is applied.

As you can see grouping of filter rule by use of head and group enables better comprehension of complex set of rules as well as improvement of filtering performance.
In addition, the values specified in head and/or group is not relevant to filter number.

4.2.2 NAT



In the above network configuration, in order to access to global side from client linked to network of private side, it is made possible with following command:

```
nat add map nnn wi0 172.30.100.0/24 -> 10.12.1.2/32
```

On this command, the internal dispatch IP address (172.30.100.0/24)
is rewritten to 10.12.1.2 in RGW and goes out to the global side.
However, the port number of dispatch packet of TCP/UDP do not change.
In order to avoid overlap dispatch port number, it is changed by specifying keyword, portmap.

```
   nat add map nnn wi0 172.30.100.0/24 -> 10.12.1.2/32 portmap tcp/udp 20000:30000
```

On this command, on top of change of IP address of TCP and UDP packets, the dispatch port number enables to change in the range of 20000 to 30000.
As for range of port number for portmap keyword, it is possible to specify in auto.

This command works similarly to the following:

```
    nat add map nnn wi0 172.30.100.0/24 ->0/32 portmap tcp/udp 20000:30000
```

Also, it is known that several application protocols do not work within NAT. The NAT in RGW corresponds with proxy to ftp, and access is possible for client without the need to change to passive mode by using following command:

```
nat add map nnn wi0 172.30.100.0/24->0/32 proxy port ftp ftp/tcp
```

To summarize above the rule for NAT in general is as follows:

```
nat add map 10 wi0 172.30.100.0/24 -> 0/32 proxy port ftp ftp/tcp
nat add map 11 wi0 172.30.100.0/24 -> 0/32 portmap tcp/udp auto
nat add map 12 wi0 172.30.100.0/24 -> 0/32
```

Each rule of NAT is assessed in numerical order. For example, when command No.12 is specified before No.10, all packet going out to global side from 172.30.100.0/24 changes only IP address so that expected operation of NAT will not be obtained.

The packet of icmp changes only the IP address so that for example, the ping in contrary from multiple clients to same host at global side is responded only to initially demanded client.

It is possible to reach from global side by setting server on inner side of NAT.

```
nat add bimap 100 wi0 172.30.100.3/32 -> 10.12.0.2/32
```

From this command an access to 10.12.0.2 from outside of NAT corresponds to access of host 172.30.100.3 of inside NAT.

On bimap, spoof to host is possible, but on rdr, spoof of service becomes possible. For example:

```
nat add rdr 101 wi0 10.12.0.2/32 port 80 -> 172.30.100.4/32 port 8000
```

With this command, an access to port No.80 of 10.12.0.2 from outside of NAT becomes access to host port No.8000 of 172.30.100.4 of inside NAT. With this rdr, it is possible during each port (each service) to distribute packet to separate port of separate host.

Note: The packet entering RGW implements address change of NAT before process of IP filter. On the other hand, packet going out of RGW implements process of IP filter before address change of NAT.