Chapter 4 Operating **SecuwayGate 100**

『Chapter4. Operating **SecuwayGate 100**』 covers various system maintenance features, including how to check the LED displays, how to replace the whole or a part of **SecuwayGate 100**, and how to change IP addresses in **SecuwayCenter 2000**, and how to change security policies in **SecuwayGate 100**.

The LED displays of **SecuwayGate 100** help you identify the current status of **SecuwayGate 100** with regard to connection, operation, and hardware failure. Depending on the status of the device you identified, you may need to take appropriate actions, such as editing the properties of the **SecuwayGate 100** or replacing the device with a new one.

NOTE

The **SecuwayGate 100** log is stored in RAM and **SecuwayCenter 2000** log is stored in the Center Log MSSQL database. The **SecuwayGate 100** sends its log in response to regular requests by **SecuwayCenter 2000**, ever minute. **SecuwayCenter 2000** stores the received **SecuwayGate 100** logs in the Gate Log MSSQL database. There is separation between the Center Logs and the Gate Logs

4.1 LED Status

When **SecuwayGate 100** is in a normal state, the Power LED and Secure LED are 'ON'. The Net LED, which represents the transmission state of the rear-panel network interface, blinks in a normal state.

- **When SecuwayGate 100 is a in normal state**

LED Display	Initial State (Factory-Default)
Power LED ON Alarm LED ON Secure LED OFF	It represents the initial factory default for installing **SecuwayGate 100**.

LED Display	Normal State (After Setup)
Power LED ON Alarm LED OFF Secure LED ON	It indicates that the initial setup has been completed with the Smart card issued from **SecuwayCenter 2000** and **SecuwayCenter 2000** has been found. The normal state of each LED is as shown in the left pane.

NOTE The Net LED on the front panel keeps blinking according to the transmission state of the network interface port located on the rear side of the device. If the port is not physically connected to a line or a device, the Net LED is 'OFF', not blinking.

- **When an error occurred in SecuwayGate 100**

LED	Error & Troubleshooting
Secure LED blinks	Indicates that the **SecuwayGate 100** failed to receive a set of security settings from **SecuwayCenter 2000** when it attempted to initiate a communication with **Secuway Center 2000** as soon as it completed the configuration setup. Check the cable connection to the Net port of **SecuwayGate 100** and the service status of **SecuwayCenter 2000**.

LED	Error & Troubleshooting
Secure LED is OFF	Indicates that no security policy is applied to **SecuwayGate 100**. If the Secure LED is turned off during the normal service mode, it implies that **SecuwayGate 100** is incapable of acting in accordance with the security policies set in **SecuwayCenter 2000**. It means you need to create a new Smart card (or file) in **SecuwayCenter 2000** and initialize **SecuwayGate 100** with a new Smart card. The Secure LED is often turned off automatically when the **SecuwayGate 100** administrator presses the Emergency Erase button by mistake, or when the security policies were not stored in **SecuwayGate 100**, due to a hardware problem. If there is a problem with the hardware, please contact our service center and request for a hardware checkup and maintenance service.
Net LED is OFF	If the Net LED is not blinking, it means that the network interface is not in service. Check the cable connection to the Net port of **SecuwayGate 100**.
Alarm LED is ON	Indicates **SecuwayGate 100** is in factory-default settings or **SecuwayGate 100** configuration settings were erased by the act of pressing the Emergency Erase button. Issue a new Smart card (or file) from **SecuwayCenter 2000** to initialize **SecuwayGate 100**.

4.2 SecuwayGate 100 Replacement Procedures

If the current **SecuwayGate 100** system is defective and needs a replacement, follow the replacement procedures below.

Step 1

To replace **SecuwayGate 100** with a new one, turn on the new system, and insert the existing smart card for initial configuration. If the new **SecuwayGate 100** system has been used in other place, it has to be initialized using the emergency erase switch before inserting the smart card.

Be sure to press the emergency erase switch while the system is turned off to initialize the system.

Step 2

Insert the existing smart card for initial configuration issued by **SecuwayCenter 2000**, which has been used to initialize the previous **SecuwayGate 100** system, and turn on the system. Check cable connectivity for communication between **SecuwayCenter 2000** and **SecuwayGate 100** at this time, and check that the LED for cable connection on rear side is lit.

When the new **SecuwayGate 100** system is turned on, the system will read and save the information on the smart card automatically.

NOTE

If **SecuwayGate 100** does not read the smart card automatically, turn off the system, press the emergency erase switch, and turn on the system again, as the system may not have been properly initilized.

Step 3

Check that smart card is successfully read through that the LED status is normal.

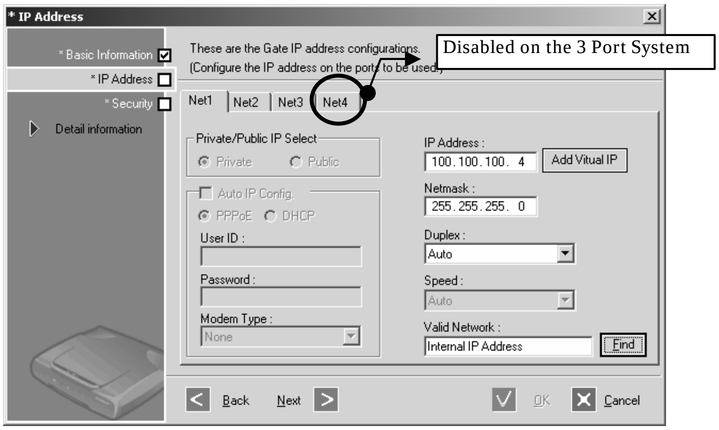
4.3 SecuwayGate 100 IP Address Change Procedures

No **SecuwayGate 100** console command can change the current IP address of **SecuwayGate 100**. Only the administrator of **SecuwayCenter 2000** is authorized to change the IP address of **SecuwayGate 100**.

The **SecuwayCenter 2000** administrator can change the IP address of **SecuwayGate 100** in the following ways.

1. Start the **SecuwayCenter 2000** (run **SecuwayCenter 2000 Server → Secuway Center 2000 Client**.) and select **SecuwayGate 100** of which IP address you want to change.

2. Double-click the selected **SecuwayGate 100** and move to the 'IP Address' step. The 'IP Address' window appears.



Disabled on the 3 Port System

* IP Address

These are the Gate IP address configurations.
(Configure the IP address on the ports to be used.)

IP Address : 100. 100. 100. 4

Netmask : 255. 255. 255. 0

Duplex : Auto

Speed : Auto

Valid Network : Internal IP Address

Select the tab (Net1, Net2, Net3, and Net4) for the port. Enter the new IP address in the 'IP Address' field, and click [Next]. Click [OK] in the window that appears after you click [Next].

Note that you have just edited the database information, and now you need to send the new IP information to **SecuwayGate 100**.

3. To send the new IP information to **SecuwayGate 100**, right-click **SecuwayGate 100** in which you have changed the IP address

from the **SecuwayCenter 2000** menu and ‘Resend Information’ from the popup menu list.

4. Before you can use the changed IP address in **SecuwayGate 100**, you need to restart **SecuwayGate 100**.

4.4 Security Policy Change Procedures

To apply a changed security policy to **SecuwayGate 100** after changing the security policy in **SecuwayCenter 2000**, select <Security Policy> → <Apply> from the menu of **SecuwayCenter 2000** while the communication between **SecuwayCenter 2000** and **SecuwayGate 100** is working properly.

For more detailed procedures, refer to the **SecuwayCenter 2000** Guide.

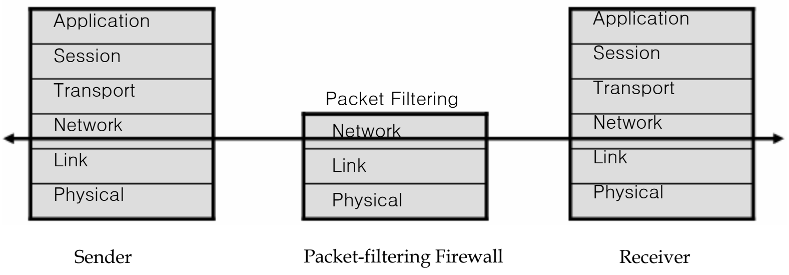
4.5 Content Security

Content security applies the state analysis method to the application-level to analyze and control the contents of the packet. It refers to a function to prevent or convert the access by analyzing the inbound packets and outbound packets. Among various content security schemes, **SecuwayGate 100** supports FTP filtering, HTTP content filtering, and SMTP filtering. The packet filters implemented in a firewall examine and control the incoming packets with the user-specified filtering rules. SecuwayGate 100 filters all the incoming and outgoing packets, except a few types of special packets including broadcasting packet and Non-IP packet.

In general, three types of content security measures are widely used: Packet Filtering, Application-level Proxy, and State analysis. **SecuwayGate 100** employs the State analysis method. These three types of filtering methods are briefly explained below.

- Packet Filtering

Packet filtering refers to the technology that collects the IP header (which usually contains source IP, destination IP, and port number) and protocol (e.g. TCP, UDP, ICMP, etc.) header and determines which network packets to allow through the firewall in accordance with the predefined security policies. Most routers have packet filtering as a built-in feature, and most firewall solutions provide this feature as well.



- Strengths

Because of its simplicity, packet filtering is easy to implement. Since a few basic rules need to be applied to check packets, packet filtering is also very fast. Its transparent operation presents another strength to users.

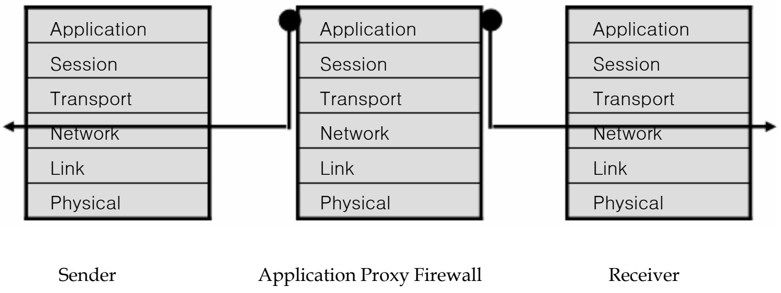
- Weaknesses

With packet filtering, it is impossible to implement a sophisticated filtering rule for complicated network or service. Since it passes or drops according to the limited number of simple access control rules, packet filtering is too simple to act as a firewall and to protect the internal resources effectively from the external intrusions.

- Application-level Proxy

Application-level Proxy acts as a link between an external network (the client) and a specific internal resource (the application server).

Acting as an application server to the client and as a client to the application server, the application-level proxy intermediates the communication between the two entities, as if the client directly communicates with the application server. The application server only recognizes that it is communicating with a client of the proxy server , and does not have further information about the specific client.



- Strengths

In an application-level proxy firewall environment, only the proxy server is known to the external network, which enables complete non-disclosure of the internal computer network system (e. g. IP address).

- Weaknesses

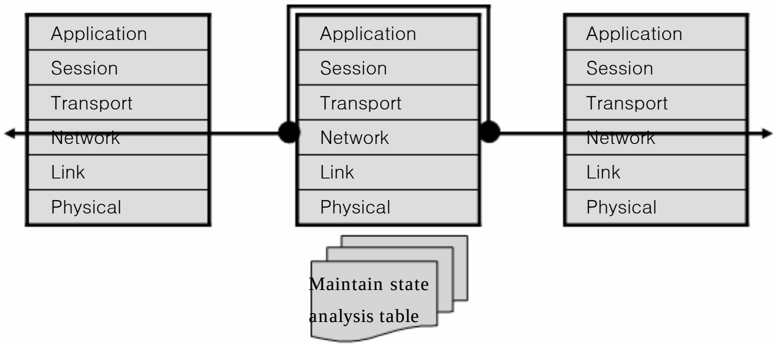
Since a separate proxy server is required for each application service (e.g. FTP proxy server, TELNET proxy server, HTTP proxy server), it is required to implement a proxy server for each internet service provided by your organization.

If your organization decides to introduce a new internet service, it may be impossible or may take a long time to implement the relevant proxy server, especially when the internet service your organization implements is not made of an industry-standard protocol or unknown source codes.

It is also disadvantageous that each application requires a separate user authentication process. In addition, the client software or user module needs to be modified in most cases.

- **State analysis**

State analysis does more than simply filter packets with the information within the packet headers. It interprets and examines the whole contents of a packet, from the network layer to the application layer. It keeps track of incoming packets over a period of time and determines whether to allow the packets to pass through the firewall.



For example, the first packet received in a session is compared with the pre-configured set of access rules and the packet information is added to the state analysis table. Once it is determined whether to pass the first packet through the firewall, and the following packets are automatically passed or dropped according to the results of the state analysis. When the session is closed, the state information entry in the state analysis table is deleted, but a set of derivative access rules from the analysis results is reflected the state to enable dynamic packet filtering.

You can also gather similar state information from the application data of a stateless protocol(e.g. UDP or RPC) packet. If an application service requires inspection against all application data, it is also possible to apply additional application-level processing to each packet for inspection.

In short, state analysis basically adopts the packet filtering technique and imitates application-level proxy technique to interpret and filter application data with far less overload than the application-level proxy. In comparison with the application-level proxy, a state analysis-based firewall offers a similar filtering capability but with much more enhanced performance. The transparent packet filtering feature for user applications is also a good reason to choose state analysis.

Based on this state analysis technique, **SecuwayGate 100** offers you highly efficient filtering mechanism and powerful content security.

Chapter 5 Console Commands

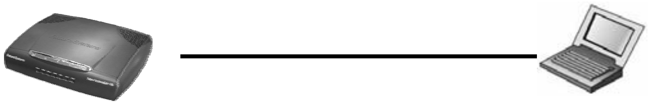
In order to use the console commands in **SecuwayGate 100**, you must connect the PC to the Console port at the rear of the **SecuwayGate 100**.

『Chapter 5 Console Commands』 describes how to log in to **SecuwayGate 100** and use console commands with the Hyper Terminal program.

5.1 Connecting SecuwayGate 100

- Step 1. Running Hyper Terminal Program

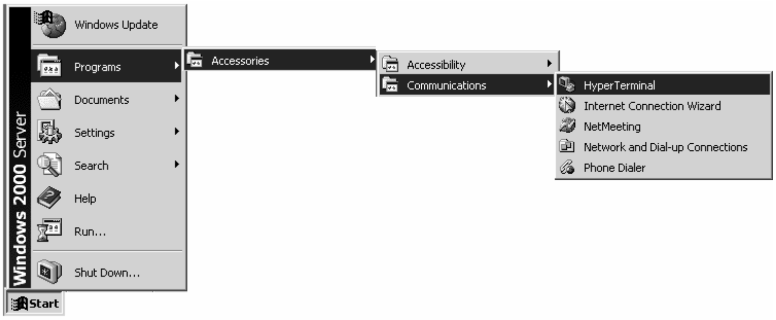
Connect the console port of **SecuwayGate 100** and the connector linked to the serial port of a laptop or PC.



SecuwayGate 100 PC used to execute console commands

A Administrators connect to **SecuwayGate 100** from a host in the protected network or form a PC installed with **SecuwayClient 2000**

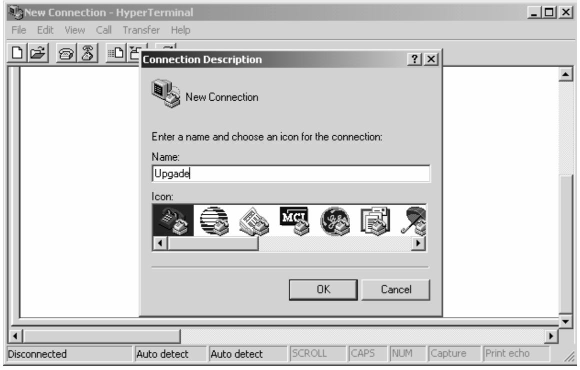
Once you have established the connection, execute the Hyper Terminal program by selecting <Start>→ <Programs>→ <Accessories>→ <Communications>→ <Hyper Terminal> in the PC, which you will use as a console window.



- Step 2. Configuring Hyper Terminal Environment

Once the Hyper Terminal is executed, select an icon and configure the connection environment in the order of 'Connection name' → 'COM port' → 'Port properties'

- Connection name entry



New Connection

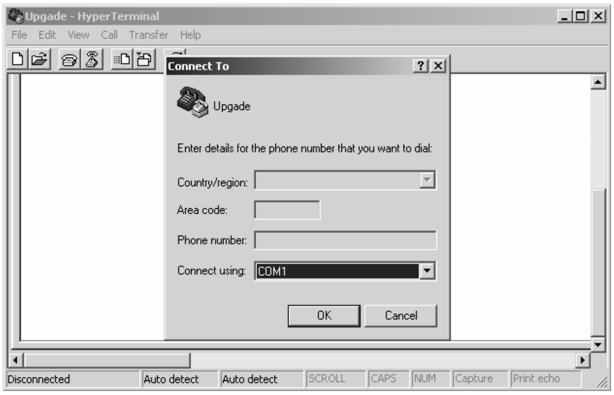
Enter a name and choose an icon for the connection:

Name: Upgade

Icon:

In this example, we entered “Upgrade” for the connection name. You may choose any name you want. Then click OK. The following dialogue box for setting the port to use for the connection will appear.

- Com port setting



Upgade

Enter details for the phone number that you want to dial:

Country/region:

Area code:

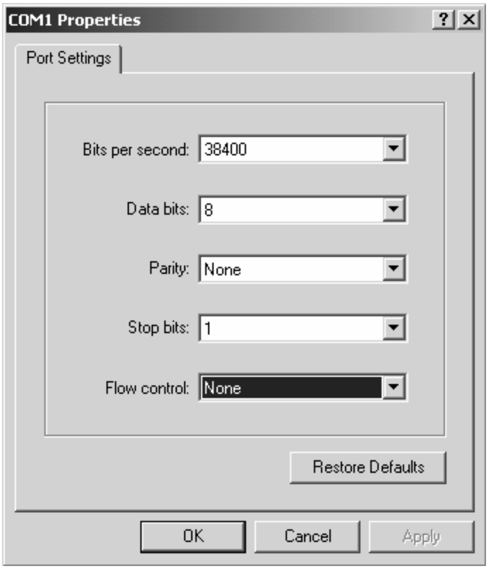
Phone number:

Connect using: COM1

Select the port to connect. For connecting to the console port, direct connection to COM1 or COM2 is usually selected. After checking the actually connected port, click OK. Then the environment for the port to connect will be set as follows.

- Setting environment for the connection port

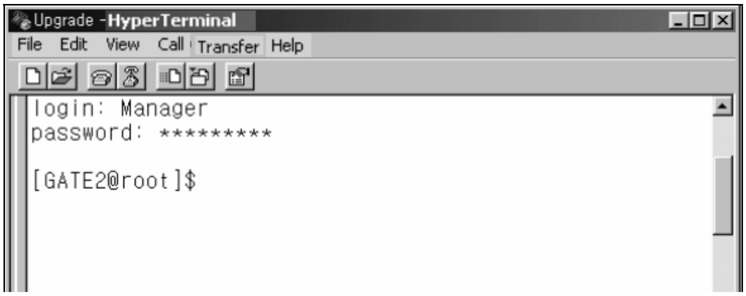
When you select the port, the following dialogue box for setting environment for the port will appear. Configure it as shown in the figure. Be sure to set the bit per second to 38400 and select None for the Flow control. Otherwise normal connection is disabled for some cases. Therefore you should set it just as indicated in the following figure.



Bits per second: 38400
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

- Confirming Correct Connection

After finishing the hyper-terminal settings, you will be able to log on as shown below. For login ID and password, you may enter the ones that have been previously issued from the master token issuer in **SecuwayCenter 2000**.



```
login: Manager
password: *********

[GATE2@root]$
```

The **SecuwayGate 100** will only accept 3 failed login attempts for the Security Administrator account, and will the deny login attempts for a period of five minutes. This functionality can be disabled by the Security Administrator for that **SecuwayGate 100,** if required.(see "sv command” in chapter 5 Console Commands)

CAUTION When the **SecuwayGate 100** Security Administrator account is inactive for 2 minutes, then it will logoff automatically.

5.2 How to Use Commands

You can use console commands when your PC is connected to the console port of **SecuwayGate 100** or when a remote PC is enabled to connect to a Telnet program from the outside.

A Administrators connect to **SecuwayGate 100** from a host in the protected network or from a PC installed with **SecuwayClient 2000**

The term '**SecuwayGate**' mentioned in this document is a common designation of **SecuwayGate 2000, SecuwayGate 1000, SecuwayGate 100** and **RenoGate**.

The List of Commands

Command	Purpose
addlog	**SecuwayGate** forcibly generates a dummy log, and transmits the log to **SecuwayCenter 2000**. The log is used for verifying normal operation of log transmission.
advanced	When functions are executed such as input, correction and deletion of routing scripts, the routing scripts stored in **SecuwayCenter 2000** or Flash are executed upon system restarting or receiving the policies, and control operation of different services (daemons).
arp	The command is similar to Linux arp command. The command displays arp table, and adds or deletes arp entries.
arp_hash	Caches arp to determine use of arp, and searches for the current arp cache.
authinfo	Displays the job list under user authentication (e.g., IP address, processing status, error number, timestamp, retrial count and message length) and the information list of user authentication in the active session (i.e., session list of each user ID).

autoup	Automatically upgrades firmware or harmful databases.
bypass	Ignores the security policies applied to **SecuwayGate**, and changes communication between specific networks to bypass. This command is available before communication with **SecuwayCenter 2000** after entering **SecuwayGate** setup information.
capture	Displays brief header information of IP and TCP for packets entered/displayed in/on specific IP or port. Executing this command may degrade performance of the system, and is only recommended for simple packet inspection. The function is released with 'capture 0.'
center	Displays or changes IP address of **SecuwayCenter 2000** currently stored in **SecuwayGate**.
change_ip	Changes **SecuwayGate** IP and **SecuwayCenter 2000** IP set on **SecuwayGate** objects.
chk_gateway	Searches for a gateway for specific IP on specific interface.
cpuinfo	Displays information of CPU and system of **SecuwayGate**.
crypto	Tests the boards upon acceleration of encryption/decryption. Devices available of testing include FSC2002, Bud-F(FACE), and CAFE. Algorithm test is available for FSC2002 only, and stress test for FACE or cafe only. Every 5000th testing indicates success or failure of encryption/decryption.
date	Converts the time currently set on the gate into UTC and RTC type, or sets the time.
debug	Converts the time currently set on the gate into UTC and RTC type, or sets the time.
del	Erases and initializes the details including IPSec-relevant tables. The table initialized for respective option is as follows:
delses	Erases the session information.

dev	It is possible to show information of devices and systems, and change attributes (e.g., duplex and speed) of the interface.
dhcp	dhcp ip Shows or changes allocation information.
entry	Shows items in the session table.
eraseobj	Erases the objects containing the security information of **SecuwayGate**, and initializes **SecuwayGate**.
failover	Displays the failover operation mode of the current **SecuwayGate** on the screen.
findcenter	Searches for the location (interface number) of **SecuwayCenter 2000** communicating with **SecuwayGate**, or stops searching.
get_arp	Transmits ARP Request of concerned IP to the specified interface.
help	Displays a list of available commands.
history	Shows the commands used on the shell so far.
icmp	Defines whether allowing ICMP communication or not. The command is only available before communication with **SecuwayCenter 2000** after entering the initial setup information.
ipconfig	Same as existing Linux command. The command is used when showing configuration information of the whole interfaces, setting IP of specific interface or stopping operation.
import	Initializes **SecuwayGate** with the initial files of **SecuwayGate** issued from **SecuwayCenter 2000**, or enters the certificate.
ip_hash	Displays device (interface) information of a certain IP on the screen, which is kept for a certain period (as a hash table format). This command is mainly used for verifying IP validity of the concerned device.
ip_verify	Inspects valid network belonging to IP address.
lb	Shows the Line Load Balancing status. Inspects the status of the leased line/VPN line/router backup when using the line option.
lbinfo	Displays user ID and password of a line where Line Load Balancing is set to..
lineinfo	Same as lb line command.

log	It is possible to check logs accumulated on **SecuwayGate**, which have not been transmitted to the log server.
lookup	The function finds IP address and MAC address corresponding with the host name, and displays the results on the screen.
ls	Same as the help command.
mainfo	The function controls starting or aborting MA, and checks the system status information managed by MA.
netstat	Displays the socket information of **SecuwayGate**.
nvram_info	Displays the nvram information.
obj	Shows the objects of Gate.
ping	Operates in a manner same as normal ping. Ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams (“pings”) have an IP and ICMP header, followed by a “struct timeval” and then an arbitrary number of “pad” bytes used to fill out the packet.
pppoe	Verify the status of PPPoE.
proxy_arp	Adds or deletes concerned entries to or from Arp Proxy Table, or searches for the entries from the table and displays the results.
proxy_ip	Displays the Proxy IP information of the concerned IP on the screen.
reset	Reboots **SecuwayGate**.
rhosttab	The command is relevant to the hash table to seach for SA of the remote host.
romc	Displays the **SecuwayGate** flash memory information.
route	Shows the routing table registered on the system, and adds or deletes routing information.
session	Shows the session table.
set_mac	Changes the MAC address of **SecuwayGate**.

status	Displays the system information of **SecuwayGate**, statistical information of packets for each protocol, and the packet filtering status. Dependent upon the options, it is possible to verify the detail statistical data, the interface status and the processing rate about transmitted and received packets of the IP/TCP/UDP/ICMP protocols.
sv	The command controls each flag value.
sysbg	Displays the system log messages stored in the backup SRAM of **SecuwayGate 1000/2000** on the screen.
syslog	Displays information of IP/port, number of **SecuwayCenter 2000** logs and the log types of the server relevant to Syslog.
task	Viewing the kernel task list
ted	**SecuwayGate** performs TED for the gate set on the IPSec gate list based on the IPSec gate list set to **SecuwayCenter 2000** or GateAdmin, and manages information of the counterpart gate in the table. The ted command verifies the TED table (or the VPN table) status, or manually performs TED.
timereq	Tests **SecuwayCenter 2000** and the time service. Upon system booting, **SecuwayGate** first transmits the TimeRequest packets to **SecuwayCenter 2000** to synchronize the time with **SecuwayCenter 2000**.
traceroute	Plays a role same as the traceroute command on Linux. The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route one's packets follow (or finding the miscreant gateway that's discarding your packets) can be difficult. Traceroute utilizes the IP protocol `time to l' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

trap_buf	Once a trap takes place such as memory violation, the command stores the monitor message in the consoles as well as the flash memory in object id 14. Therefore, it is possible to obtain various information by analyzing the dump message.
upgrade	The command upgrades the firmware. The command first runs the upgrade daemon to the gate, and receives and processes images when firmware files are transmitted to the network. UDP protocol port 9876 is used for upgrade. Please note that data relevant to upgrade is not affected by the security policies.
version	Displays the firmware version information, the compiling date and the compiling option information of **SecuwayGate**.
view_traffic	It is possible to verify the current CPU utilization, memory utilization, number of sessions, and traffics of **SecuwayGate**.
xurl	Checks the harmful site database provided from SafeNet for any URL, or inspects the autonomy grade of the concerned URL. The harmful site database contains overseas sites, not domestic sites.
xurl_db	Manages the harmful site database.
ldap	Gains access to the LDAP server to search for CRL.
p1info	Shows the detail information of SA in step 1.
pki	Shows the PKI information.
pic	Shows information of PIC operation and SA. PIC is used for authentication of Remote Access Client in GateAdmin environments.
sainfo	Shows the SA-relevant table.
secinfo	Shows the IPSec-relevant table.
view_tid	Displays the TID table on the screen.

Detailed Description of each Commands

NOTE

Please refer to “SecuwayGate Console Commads” maual for futher information on how to use **SecuwayGate 100** console commands

Chapter 6 Upgrading Firmware

The firmware of **SecuwayGate 100** can be upgraded, if necessary. The following section describes the firmware upgrading procedures.

The administrator can load new firmware to upgrade functions provided by **SecuwayGate 100**.

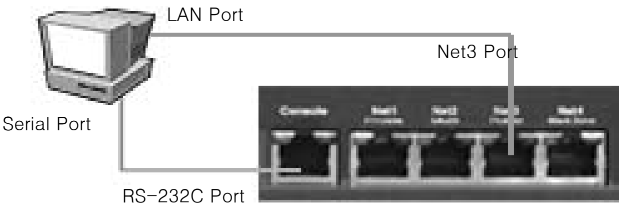
6.1 Preparations for upgrade

Prepare PC with the HyperTerminal program and **SecuwayGate 100** firmware loading program Lanload.exe which is included in the installation CD.

Cable Connection

1. Connect the serial port of the PC and RS-232C port of **SecuwayGate 100** with the console connector as shown in the following figure. (Use normal LAN cable as the connector).

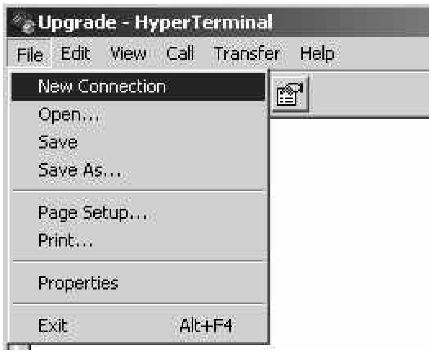
2. Connect any one of the ports Net1, Net2, Net3, and Net4 of **SecuwayGate 100** with the LAN port of PC. For explanation purposes, port Net3 is chosen in the figure.

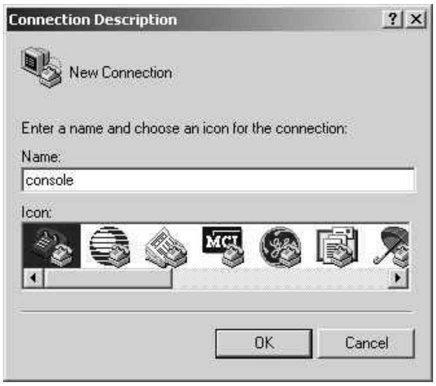


6.2 Loading Firmware

Configuring HyperTerminal

1. Select [New Connection], input the name for the connection, and click OK.

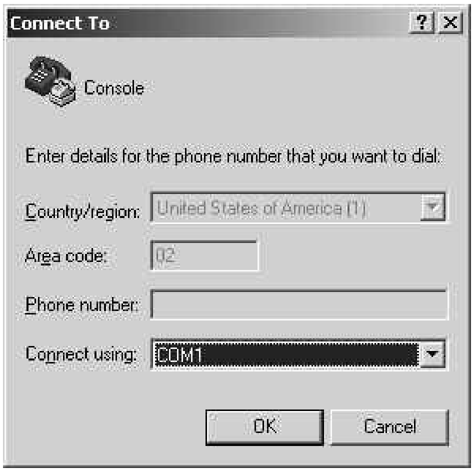




Enter a name and choose an icon for the connection:

Name: console

2. Configure Modem to Connect to COM1. (This may vary depending on your PC configuration.)



Console

Enter details for the phone number that you want to dial:

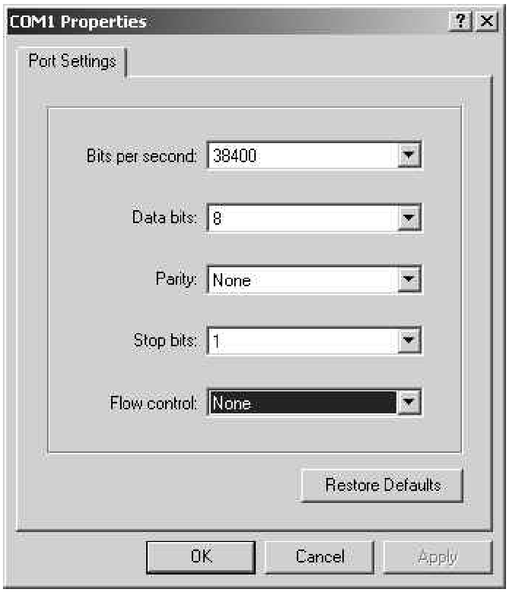
Country/region: United States of America (1)

Area code: 02

Phone number:

Connect using: COM1

Setup port Net3onfiguration as shown in the following figure.



COM1 Properties

Port Settings

Bits per second: 38400

Data bits: 8

Parity: None

Stop bits: 1

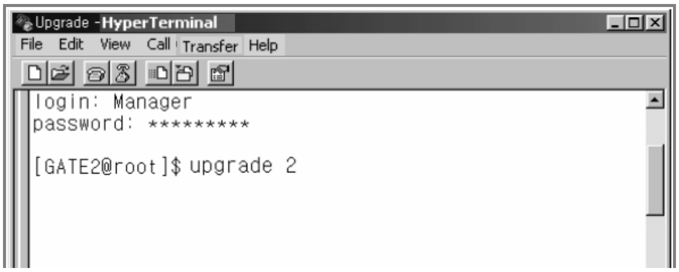
Flow control: None

3. Click OK, and the HyperTerminal window will be displayed. In the window, press <Enter> key to connect to **SecuwayGate 100**, and a screen will be displayed allowing ID and password input.

6.3 Logon SecuwayGate 100

1. In the Hyper Terminal window, enter the registered login ID and password.

2. Specify the port number of **SecuwayGate 100** used to upgrade the program in the following format ('upgrade 2', in this case). Here '0' means the port Net1 on the rear side, and '1', '2', and '3' refer to Net2, Net3, and Net4, respectively. In this case, the Net3 is connected to the internal LAN, therefore you need to type "upgrade 2" when prompted.

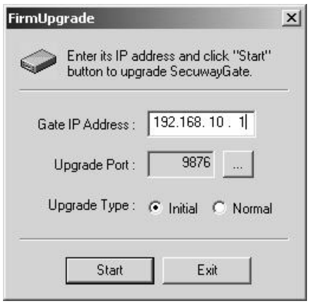


```
login: Manager
password: *********

[GATE2@root]$ upgrade 2
```

6.4 Executing ‘Upgrade’ File

The ‘upgrade’ file is used to upgrade the existing firmware of **SecuwayGate 100**.

Two firmware upgrade methods are supported in **SecuwayGate 100**: Initial and Normal. You can select either upgrade type in the ‘FirmUpgrade’ window, which appears when you execute FirmUpgarde.exe.


FirmUpgrade

Enter its IP address and click "Start" button to upgrade SecuwayGate.

Gate IP Address : 192.168. 10 . 1

Upgrade Port : 9876

Upgrade Type : ● Initial ○ Normal

Initial	Refers to upgrading in debug mode. Debug mode is a pre-operation phase in which **SecuwayGate 100** is completely reset. If you upgrade a firmware in debug mode, the new firmware is automatically reloaded and adopted in **SecuwayGate 100**.
Normal	Refers to upgrading the firmware to **SecuwayGate 100** currently in operation. T upgraded firmware is adopted only when the admionistrator resets **SecuwayGate 100** manually.

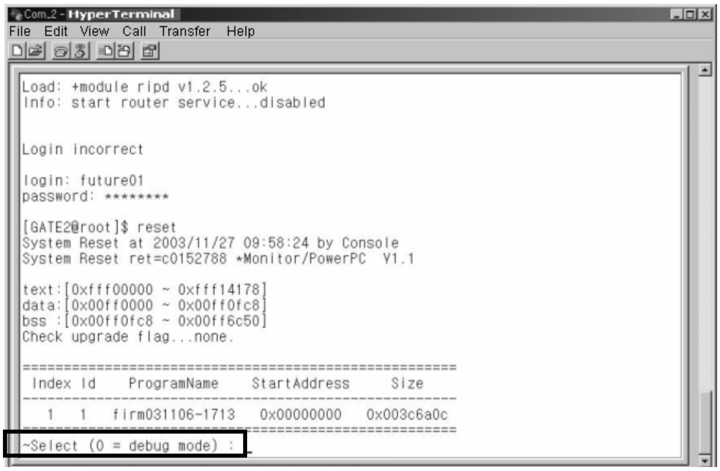
NOTE

“Normal(N)” firmware upgrade type is widely used for its convenience.

6.4.1 Upgrading Firmware

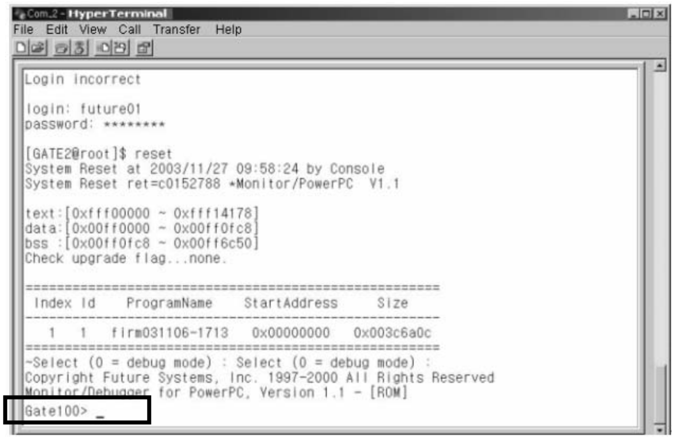
Initial (I) Upgrade Type

1. Reset **SecuwayGate 100**. When you reboot **SecuwayGate 100**, press “~” key in the Hyper Terminal window and enter the debug mode. The following figure is displayed:



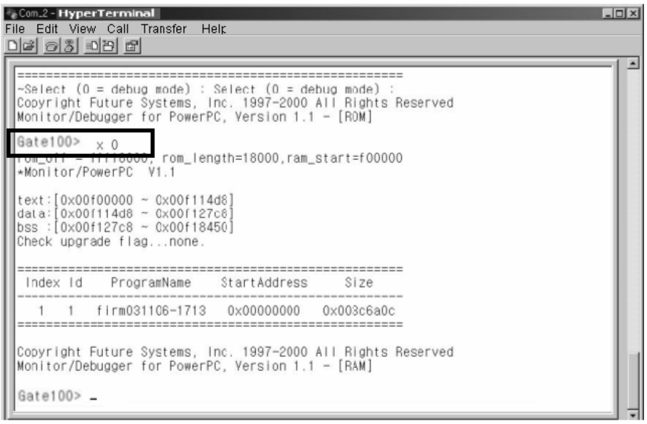
```
Load: +module ripd v1.2.5...ok
Info: start router service...disabled


Login incorrect

login: future01
password: ********

[GATE2@root]$ reset
System Reset at 2003/11/27 09:58:24 by Console
System Reset ret=c0152788 *Monitor/PowerPC  V1.1

text:[0xfff00000 ~ 0xfff14178]
data:[0x00ff0000 ~ 0x00ff0fc8]
bss :[0x00ff0fc8 ~ 0x00ff6c50]
Check upgrade flag...none.

=====================================================
 Index Id    ProgramName    StartAddress     Size
-----------------------------------------------------
   1   1   firm031106-1713   0x00000000   0x003c6a0c
=====================================================
~Select (0 = debug mode) : _
```

2.Type “0” to enter the debug mode, and type “0” again. The Gate 100 prompt appears.



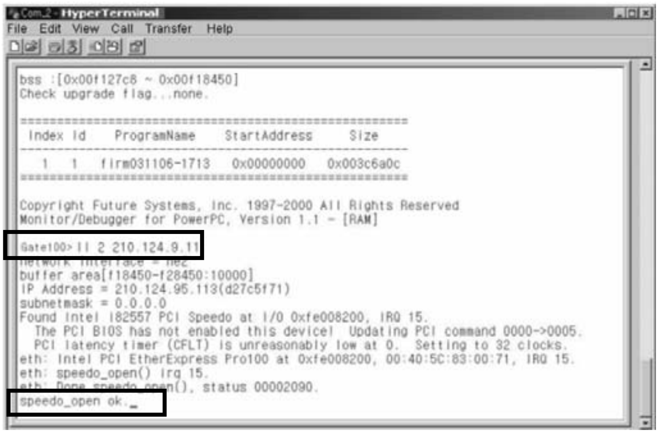
```
Login incorrect

login: future01
password: ********

[GATE2@root]$ reset
System Reset at 2003/11/27 09:58:24 by Console
System Reset ret=c0152788 *Monitor/PowerPC  V1.1

text:[0xfff00000 ~ 0xfff14178]
data:[0x00ff0000 ~ 0x00ff0fc8]
bss :[0x00ff0fc8 ~ 0x00ff6c50]
Check upgrade flag...none.

=====================================================
 Index Id    ProgramName    StartAddress     Size
-----------------------------------------------------
   1   1   firm031106-1713   0x00000000   0x003c6a0c
=====================================================
~Select (0 = debug mode) : Select (0 = debug mode) :
Copyright Future Systems, Inc. 1997-2000 All Rights Reserved
Monitor/Debugger for PowerPC, Version 1.1 - [ROM]
Gate100> _
```

3. Type “x 0” and press ‘Enter’.



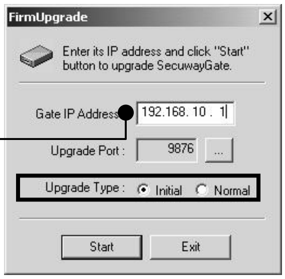
```
=======================================================
~Select (0 = debug mode) : Select (0 = debug mode) :
Copyright Future Systems, Inc. 1997-2000 All Rights Reserved
Monitor/Debugger for PowerPC, Version 1.1 - [ROM]

Gate100>  x 0
rom_off = fff18000, rom_length=18000,ram_start=f00000
*Monitor/PowerPC  V1.1

text:[0x00f00000 ~ 0x00f114d8]
data:[0x00f114d8 ~ 0x00f127c8]
bss :[0x00f127c8 ~ 0x00f18450]
Check upgrade flag...none.

=======================================================
 Index Id    ProgramName    StartAddress     Size
-------------------------------------------------------
   1   1   firm031106-1713   0x00000000   0x003c6a0c
=======================================================

Copyright Future Systems, Inc. 1997-2000 All Rights Reserved
Monitor/Debugger for PowerPC, Version 1.1 - [RAM]

Gate100> _
```

4. Type “ll 2 *IP address of SecuwayGate 100*” and press ‘Enter’. The “speedo_open ok.” message is displayed.



```
bss :[0x00f127c8 ~ 0x00f18450]
Check upgrade flag...none.

=======================================================
 Index Id    ProgramName    StartAddress     Size
-------------------------------------------------------
   1   1   firm031106-1713   0x00000000   0x003c6a0c
=======================================================

Copyright Future Systems, Inc. 1997-2000 All Rights Reserved
Monitor/Debugger for PowerPC, Version 1.1 - [RAM]

Gate100> ll 2 210.124.9.11
network interface = ne2
buffer area[f18450-f28450:10000]
IP Address = 210.124.95.113(d27c5f71)
subnetmask = 0.0.0.0
Found Intel i82557 PCI Speedo at I/O 0xfe008200, IRQ 15.
  The PCI BIOS has not enabled this device!  Updating PCI command 0000->0005.
  PCI latency timer (CFLT) is unreasonably low at 0.  Setting to 32 clocks.
eth: Intel PCI EtherExpress Pro100 at 0xfe008200, 00:40:5C:83:00:71, IRQ 15.
eth: speedo_open() irq 15.
eth: Done speedo_open(), status 00002090.
speedo_open ok._
```

5. Execute FirmUpgarde.exe in a PC to which **SecuwayGate 100** is connected. The ‘FirmUpgrade’ window appears. In the ‘Gate IP Address’ field, enter the IP address of the Net3 port. Select ‘Initial’ for the ‘Upgrade Type’ field. The ‘Upgrade Port’ is already set to ‘9876’. If you edit this value, the system may not work properly. Click [Start].



FirmUpgrade

Enter its IP address and click "Start" button to upgrade SecuwayGate.

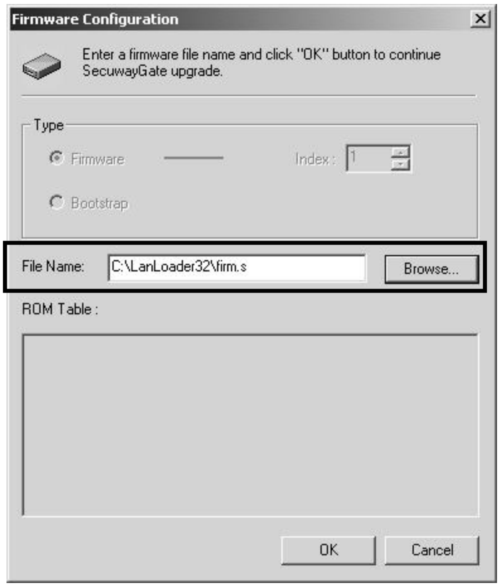
Gate IP Address: 192.168. 10 . 1

Upgrade Port : 9876

Upgrade Type : ● Initial ○ Normal

Enter the IP address of Net3 port

6. The ‘ FirmUpgarde Configuration’ window appears. Specify the location of the firmware upgrade file in ‘ File Name’ by clicking [Browse] and selecting the file. Click [OK].



Firmware Configuration

Enter a firmware file name and click "OK" button to continue SecuwayGate upgrade.

Type

● Firmware Index : 1

○ Bootstrap

File Name: C:\LanLoader32\firm.s

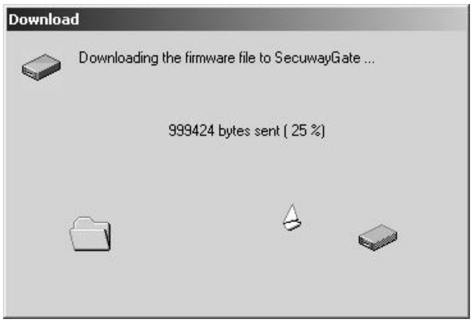
ROM Table :

Firmware	Transfers the firmware as well as the DB that blocks harmful sites to **SecuwayGate 100**.
Index	Indicates the memory allotment index of **SecuwayGate 100**. While the index No. 1~8 are pre-assigned to store the firmware, the index No. 9 is assigned to the DB for blocking harmful sites. Usually, No. 1 is used to store the firmware. It is because **SecuwayGate 100** starts to check the availability of the firmware with the index No. 1 and loads the first one available in the index. If no

	firmware is available in the index No. 1, it checks the index in the order of No.2, 3, 4, ... 8 to load the first available firmware.

NOTE The name of a firmware file is either ‘first’ or ‘firm’. If you are updating the firware in initial mode, you must select the firmware named as ‘first’.

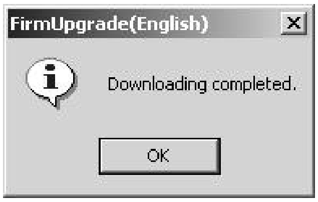
Click [OK]. The ‘Download’ window appears to show you the process of transmitting the firmware file to **SecuwayGate 100** as shown below.


Download

Downloading the firmware file to SecuwayGate ...

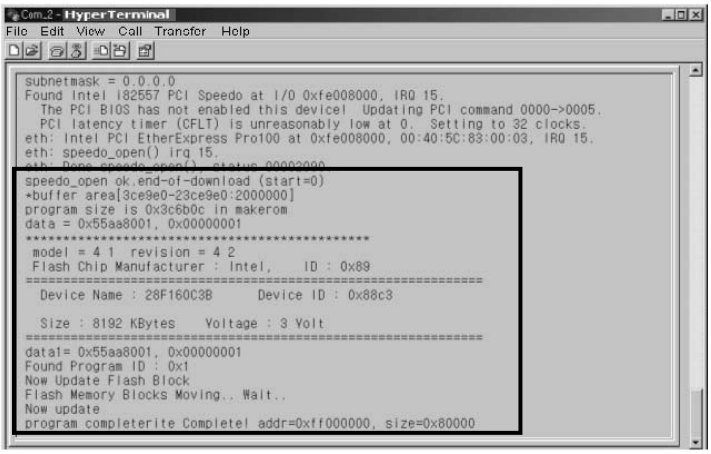
999424 bytes sent (25 %)

Once the file transmission is completed, “Download completed” message appears.


FirmUpgrade(English)

Downloading completed.

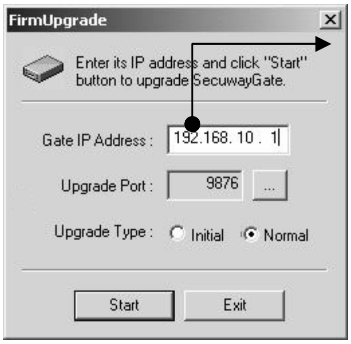
If the firmware transmission is completed, you will see the following messages in the Hyper Terminal window, and **SecuwayGate 100** is automatically reset.



```
subnetmask = 0.0.0.0
Found Intel i82557 PCI Speedo at I/O 0xfe008000, IRQ 15.
  The PCI BIOS has not enabled this device!  Updating PCI command 0000->0005.
  PCI latency timer (CFLT) is unreasonably low at 0.  Setting to 32 clocks.
eth: Intel PCI EtherExpress Pro100 at 0xfe008000, 00:40:5C:83:00:03, IRQ 15.
eth: speedo_open() irq 15.
eth: Done speedo_open(), status 00002090.
speedo_open ok.end-of-download (start=0)
*buffer area[3ce9e0-23ce9e0:2000000]
program size is 0x3c6b0c in makerom
data = 0x55aa8001, 0x00000001
**********************************************
 model = 4 1  revision = 4 2
 Flash Chip Manufacturer : Intel,    ID : 0x89
==============================================================
  Device Name : 28F160C3B      Device ID : 0x88c3

  Size : 8192 KBytes    Voltage : 3 Volt
==============================================================
data1= 0x55aa8001, 0x00000001
Found Program ID : 0x1
Now Update Flash Block
Flash Memory Blocks Moving.. Wait..
Now update
program completerite Complete! addr=0xff000000, size=0x80000
```

Normal (N) Upgrade Type

1. Execute FirmUpgarde.exe in a PC to which **SecuwayGate 100** is connected. The ‘FirmUpgrade’ window appears. In the ‘Gate IP Address’ field, enter the IP address of the Net3 port. Select the ‘Initial’ for ‘Upgrade Type’ field. The ‘Upgrade Port’ is already set to ‘9876’. If you edit this value, the system may not work properly. Click [Start].



Enter its IP address and click "Start" button to upgrade SecuwayGate.

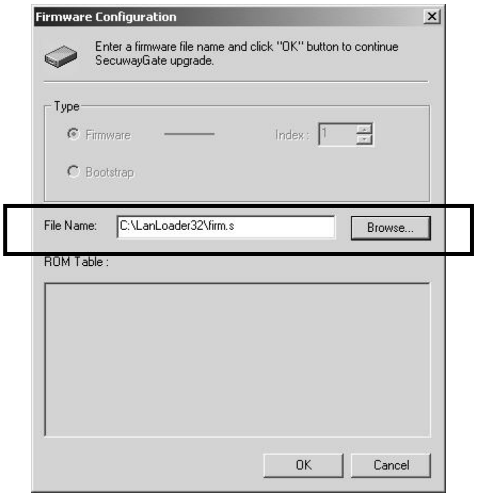
Gate IP Address : 192.168. 10 . 1

Upgrade Port : 9876

Upgrade Type : ○ Initial ● Normal

Enter the IP address of Net3 port.

2. The ‘ FirmUpgarde Configuration’ window appears. Specify the location of the firmware upgrade file in ‘ File Name’ by clicking [Browse] and selecting the file. Click [OK]



Enter a firmware file name and click "OK" button to continue SecuwayGate upgrade.

Type

● Firmware Index : 1

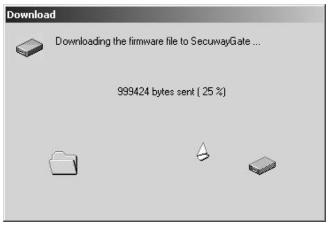
○ Bootstrap

File Name: C:\LanLoader32\firm.s

ROM Table :

The name of a firmware file is either ‘first’ or ‘firm’. If you are updating the firware in normal mode, you must select the firmware named as ‘firm’.

Click [Transmit]. The ‘Download’ window appears to show you the process of transmitting the firmware file to **SecuwayGate 100** as shown below

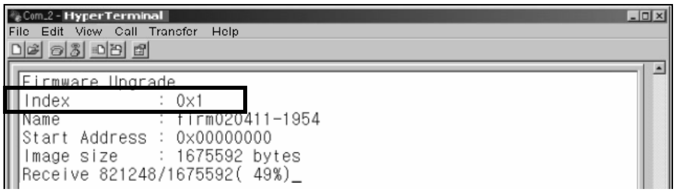


Download

Downloading the firmware file to SecuwayGate ...

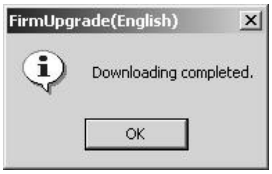
999424 bytes sent (25 %)

You can also verify the firmware downloading process in the “Index: 0x1” section of the Hyper Terminal.



```
Firmware Upgrade
Index          : 0x1
Name           : firm020411-1954
Start Address  : 0x00000000
Image size     : 1675592 bytes
Receive 821248/1675592( 49%)_
```

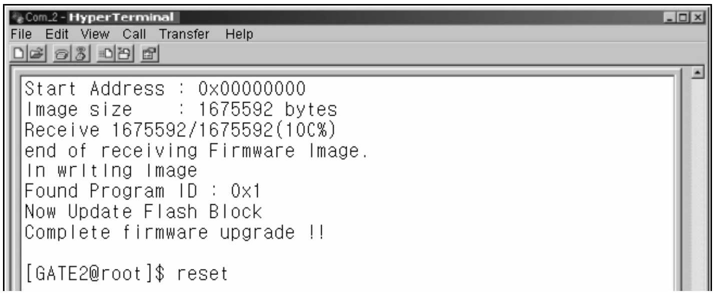
Once the file transmission is completed, “Download completed” message.



FirmUpgrade(English)

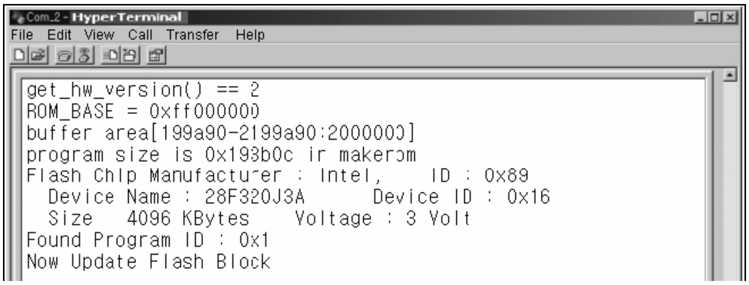
Downloading completed.

3. If the firmware transmission is completed, execute “reset” in the Hyper Terminal. To apply the ungraded firmware, you must execute “reset”command.



```
Start Address : 0x00000000
Image size    : 1675592 bytes
Receive 1675592/1675592(100%)
end of receiving Firmware Image.
In writing Image
Found Program ID : 0x1
Now Update Flash Block
Complete firmware upgrade !!

[GATE2@root]$ reset
```

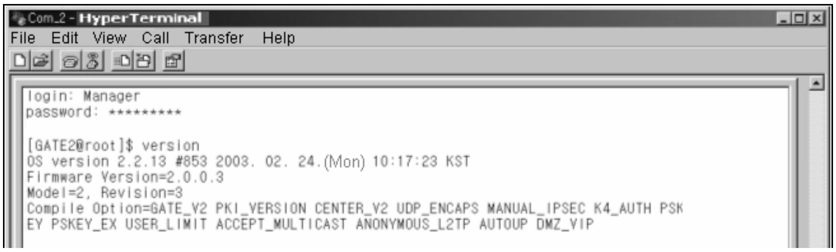
4. **SecuwayGate 100** is restarted once the firmware has been upgraded.



```
get_hw_version() == 2
ROM_BASE = 0xff000000
buffer area[199a90-2199a90:2000000]
program size is 0x193b0c in makerom
Flash Chip Manufacturer : Intel,    ID : 0x89
  Device Name : 28F320J3A      Device ID : 0x16
  Size   4096 KBytes    Voltage : 3 Volt
Found Program ID : 0x1
Now Update Flash Block
```

6.5 Checking Firmware Loading

The version of the firmware can be checked through HyperTerminal on the PC connected to the **SecuwayGate 100** console. To check the version of the firmware, type the “version” command.



```
login: Manager
password: *********

[GATE2@root]$ version
OS version 2.2.13 #853 2003. 02. 24.(Mon) 10:17:23 KST
Firmware Version=2.0.0.3
Model=2, Revision=3
Compile Option=GATE_V2 PKI_VERSION CENTER_V2 UDP_ENCAPS MANUAL_IPSEC K4_AUTH PSK
EY PSKEY_EX USER_LIMIT ACCEPT_MULTICAST ANONYMOUS_L2TP AUTOUP DMZ_VIP
```

Appendix A

Q&A About **SecuwayGate 100**

1) I want to change the IP address of the SecuwayGate 100 which is in use. What should I do?

In order to change the IP address of the **SecuwayGate 100** which is in use, select the [Modification] feature in the [Gate Management (G)] in **SecuwayCenter 2000**. After changing features, you must send the changed features using [Resend (R)], and in particular when you have changed the IP address, you must run [Gate Restart (T)].

2) Is it mandatory to use the four ports, i.e., Private, Multi, Public, and Black Zone ports at the rear for their specified purposes?

The four ports Net1 (Private), Net2 (Multi), Net3 (Public), Net 4 (Black Zone) are specified for user convenience, and you don't have to use them for their specified uses. In actual application, the administrator may use the four ports in his/her discretion for operational convenience.

Because the four ports at the rear are controlled by valid network setting and security policy in **SecuwayCenter 2000**, they may not be used for Private, Multi, Public, and Black Zone as specified, but for separating the network into four networks to control each network individually.

3) How can I change the security policy of SecuwayGate 100?

After changing the security policy in **SecuwayCenter 2000**, send it to **SecuwayGate 100** on-line. Then the changed security policy will be applied immediately. The **SecuwayGate 2000** administrator cannot insert or delete a security policy by accessing through the Console port or Telnet. If the security policy needs to be changed, you must ask the administrator of **SecuwayCenter 2000** to do it.

4) When moving the SecuwayGate 100 to another place, what settings should be changed?

You must consider the following two cases when moving the system to another place. If the TCP/IP related information is changed, you must change and transmit the IP address or other network information, before moving the **SecuwayGate 100** or you must have the initial setting smart card reissued from **SecuwayCenter 2000** and then import it into **SecuwayGate 100** after moving.

5) How can I stop the use of SecuwayGate 100 in emergency?

In order to stop it, you must first discuss with the administrator of **SecuwayCenter 2000** or Gate Admin, and then run the [Stop Service] in the [Gate (G)] menu in **SecuwayCenter 2000**

6) is the meaning of the “Valid network” and the reason of setting it with the issuance of SecuwayGate 100?

Valid network is a set of valid IPs of the hosts connected to each interface, i.e., Net1, Net2 and Net3. Valid network must be set in order to decide the paths through which received packets are sent. By setting the valid network, you can also prevent IP Spoofing by verifying the validity of the starting IP address. If the valid network is incorrectly configured, the IP spoofing error message will appear in **SecuwayCenter 2000**, and it may cause such problems as the data accepted on security policy are transferred to other interfaces and do not arrive at the destination. For details on setting valid network, please refer to the User’s Guide for **SecuwayCenter 2000** .

7) **It is said that SecuwayGate 100 processes the send/receive packets through the conditional analysis method. How does it manage sessions? In other words, when is the time that the session is registered and deleted?**

For TCP, the session is registered when the Syn packet is received, and for UDP, it is registered when the Data packet enters. In both cases, the session can be registered only when the security policy is in the “Accept” state in **SecuwayGate 100**.

The time when the session is deleted is different with Firmware versions for TCP. In version 1.5, 2.0 and higher, the session is deleted when the Timeout value of the security policy is exceeded in **SecuwayCenter 2000**, or FIN or Reset Packet is received. On the other hand, in hardware of versions lower than 1.5,2.0, the session is deleted only when the FIN or Reset Packet is received. Therefore, when the session finishes abnormally in the PC or server, the sessions will be accumulated. For UDP, because the session timeout value is set to 30 seconds regardless of firmware versions, the session will be canceled when packet transmission time exceeds 30 seconds for the session.

8) **What types of L4 switches support load balancing by interoperation with SecuwayGate 100 (VPN) equipment?**

1) Radware: FireProof 2) Piolink: Pinkbox1016

3) Alton: AD3, 180e

9) **When should we reboot SecuwayGate 100 due to modification of information in SecuwayGate 100?**

1) When the IP of **SecuwayGate 100** is changed.

2) When upgrading firmware.

3) You don’t have to reboot when the valid network is changed.

10) **Does the SecuwayGate 100 equipment support line/server load-balancing feature?**

SecuwayGate 100 supports both line load-balancing (LLB) and server load-balancing (SLB).

LLB enables the duplication of the Internet lines with two ADSL lines, or with one ADSL line and one dedicated line, enhancing availability of the Internet. LLB decides its line by combination of the starting IP address and destination IP address, and make it possible that all communication will be processed through the remaining line even if one line fails.

SLB checks the availability of the homogeneous servers, enabling continuous service. The methods of supporting SLB include: server inspection by using PING to check the activation of the server, server inspection by checking the use of the service, round-robin method for service distribution to servers and the number of sessions method.

11) Does the firewall features of SecuwayGate 100 include blocking of harmful websites?

SecuwayGate 100 supports the feature to block harmful websites through HTTP Content filtering function. You can block the access to the hosts containing specific character strings, or to specific directories or files. In addition, the feature of filtering various dangerous scripts (JavaScript, VBScript, etc.) is provided.

12) Can SecuwayGate 100 be operated on other vendors' NMS program?

SecuwayGate 100 supports SNMP V1.0 to enable its operation on other vendor's NMS's. However, due to various security problems, not all SNMP functions are supported. Only viewing is allowed for most functions.

13) What should be checked, if file upload fails after going through SecuwayGate 100 using a fixed IP?

For ADSL modems, there is a limit in MTU size. It is typical that the size is limited for floating IPs, but not for fixed IPs. Samsung ADSL modems generally fall in this case, but Hyundai ADSL modems are usually configured to limit the MTU size for fixed IPs by default. If file upload fails on the Internet or into tunnels after installing **SecuwayGate 100**, the ADSL modem must be checked. You can determine that this is the problem if a file of 1 Kbytes is uploaded but a file of over 2 Kbytes is not uploaded.

14) Which ports are used for various messengers?

ICQ / AOL: 5190 MSN: 1863

Chollian (CQM) : 1421 Soft Messenger: 5004

Bluebird: 3300 Netsgo (Minigo): 5004

Yahoo: since Yahoo cannot be controlled by port, you should block cs.yahoo.com or scsa.yahoo.com. However, you must be careful because if you block these two sites, it may not be possible to access yahoo.com itself.

For some of the above ports, only the login ports are listed. (If you block only the login port, access is disabled.)

15) Can ADSL fixed and floating lines and the ADSL lines of different vendors be used together?

With KT’s ADSL line, line load balancing and fail-over are normally operated for all situations such as fixed/fixed, floating/ floating, and fixed/ floating, as well as with Hanaro Telecom and Thrunet.

<Note>

- When setting ADSL LLB: For [fixed/fixed] or [fixed/ floating] configuration, the NAT Rule is applied (in fixed IP) to allow access to external Web. However, for floating [/floating] configuration, no extra NAT Rule is required.
- When setting ADSL fail-over: it correctly operates for all situations such as modem’ s power off, line cut-off of modem or gate, and serial line cut-off of the modem.

16) What is the PIN arrangement of the SecuwayGate 100's console cable?

Numbers marked in the console connector	Line color
2	Yellow
3	Green
5	Red
8	Brown

15.Jan. 2004 Future Systems, Inc.

7,8F, Koland Bldg, 1009-1, Daechi-dong, Knagnam-gu, Seoul, 135-851 Korea
Tel : +82-2-3468-7777 , Fax : +82-2-3468-7700
Homepage : http://www.future.co.kr