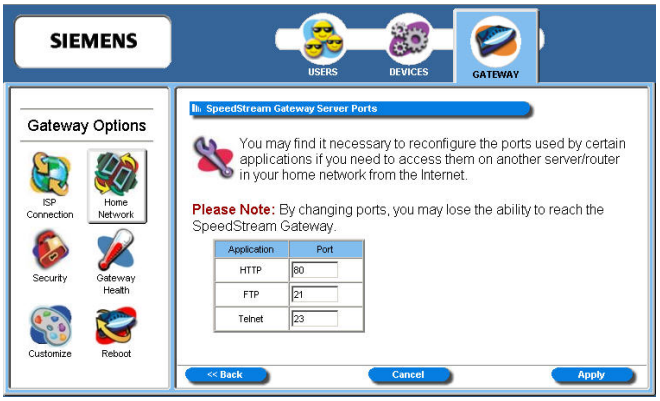
Server Ports

Common applications such as HTTP (Web site traffic), FTP, and Telnet use pre-defined incoming port numbers for compatibility with other services. If you wish to change the ports used by these applications you may do so using this option. This feature is recommended for use by advanced users only.

To configure the server port option:

1. Click the **Configure the Local SpeedStream Gateway Server Ports** hyperlink. This displays the "SpeedStream Gateway Server Ports" window.



2. Optionally, type a port number in **HTTP**. The default port for this field is 80.
3. Optionally, type a port number in **FTP**. The default port for this field is 21.
4. Optionally, type a port number in **Telnet**. The default port for this field is 23.
5. Click **Apply**. This displays the "Your settings have been saved" window.
6. Optionally, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your Gateway.

LAN/WAN Port

If your Gateway contains four Ethernet ports, Ethernet port #4 can be used as either a LAN (network) port or as a WAN (Internet connection) port. Select the appropriate option to define whether the port is used as a fourth local network port or as a connection for another broadband device.

Note: For configuration of the port as a WAN port, you may be required to consult your Internet Service Provider for the appropriate settings.

To configure the LAN/WAN port:

1. Click the **Configure the Local SpeedStream Gateway LAN/WAN Port** hyperlink. This displays the "SpeedStream Gateway LAN/WAN Port" window.

2. Select one of the following options:

   - **LAN** (Local Area Network)
     Use the port as a connection to the network located in your home or premises.
   - **WAN** (Wide Area Network)
     Use the port as a connection to a large connected network such as the Internet that is spread over a large geographic area. If you select the WAN option, please contact your ISP for instructions on how to configure this option.

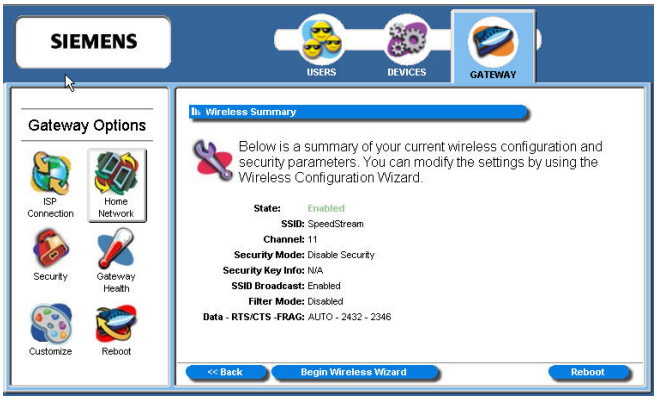
3. Click **Apply**.

Wireless Network

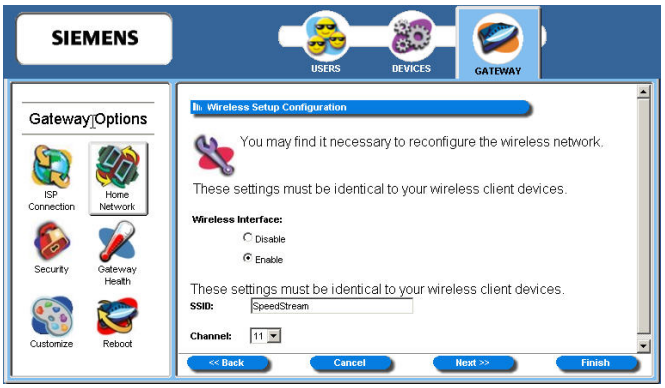
Configure the wireless network using this option. The wireless settings on the Gateway must match those of any wireless clients on your network.

To configure the wireless network:

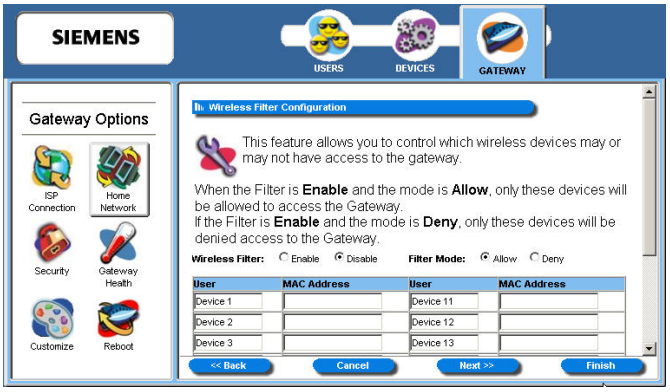
1. Click the **Configure the Local SpeedStream Gateway Wireless Network** hyperlink. This displays the "Wireless Summary" window.



2. Click **Begin Wireless Wizard**. This displays the "Wireless Setup Configuration" window.



3. Select **Enable** to enable the **Wireless Interface**.
4. Type your wireless network ID in **SSID** (Service Set Identifier).
5. Optionally, select a channel ID from the **Channel** drop-down menu. This is typically done if you experience any interference with your wireless Gateway.
6. Click **Next**. This displays the "Wireless Security Configuration" window.



Set the wireless security level from the "Wireless Security Configuration" window. All wireless devices attached to the Gateway **MUST** have the same wireless security settings for your network to have proper communications and security.

7. From the **Security Mode** drop-down menu, select one of the following options:

   - **WEP 64-bits**
     Wireless Equivalency Privacy. WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 64-bit encryption, which is the least secure WEP option. Please see the section in this document titled Wireless Setup WEP 64-Bit Option (Advanced Home Networking) for more information.

   - **WEP 128-bits**
     Wireless Equivalency Privacy. WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is a most secure WEP option. Please see the section in this document titled Wireless Setup WEP 128-Bit Option (Advanced Home Networking) for more information.

   - **WPA PSK**
     Wi-Fi Protected Access. WPA security changes encryption keys after a specified amount of time. This is the most secure option for wireless networks. Please see the section in this document titled Wireless Setup WPA PSK Option (Advanced Home Networking) for more information.

8. Optionally, select the **Enable SSID Broadcast** option so wireless users can see the existence of the wireless Gateway with the associated SSID.

Wireless Setup WEP 64-Bit Option (Advanced Home Network)

WEP security offers the same security offered by a wired LAN with encrypted packets. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer.

To use the WEP 64-bit option:

1. From the "Wireless Security Configuration" window, select **WEP 64-bits** from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless 64-bit WEP Configuration" window.

3. Select one of the following **Authentication** options:
   - **Open System**
     Open system keys are always authenticated at the device level. After authentication, data is encrypted between the Gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
   - **Shared Key**
     Shared keys accept a string of unencrypted data from a device. The Gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
4. Type a phrase in **Passphrase**. The passphrase is used to generate the 64-bit keys. The passphrase can be between 1 and 32 characters.
5. Click **Generate Keys**. The system responds by generating keys that display in the boxes under **Passphrase**. Four different keys are generated.
6. Select one of the four keys to use for encryption.
7. Click **Next**. This displays the "Wireless Filter Configuration" window.

Wireless Setup WEP 128-Bit Option (Advanced Home Network)

WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is the most secure WEP option. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer.

To use the WEP 128-bit option:

1. From the "Wireless Security Configuration" window, select **WEP 128-bits** from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless 128-bit WEP Configuration" window.

3. Select one of the following **Authentication** options:
   - **Open System**
     Open system keys are always authenticated at the device level. After authentication, data is encrypted between the Gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
   - **Shared Key**
     Shared keys accept a string of unencrypted data from a device. The Gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
4. Type a phrase in **Passphrase**. The passphrase is used to generate the 128-bit key. The passphrase can be between 1 and 32 characters.
5. Click **Generate Keys**. The system responds by generating keys that display in the boxes under **Passphrase**.
6. Select one of the keys to use for encryption.
7. Click **Next**. This displays the "Wireless Filter Configuration" window.

Wireless Setup WPA PSK Option (Advanced Home Network)

WPA security changes encryption keys after a specified amount of time. This is the most secure option for wireless networks. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer.

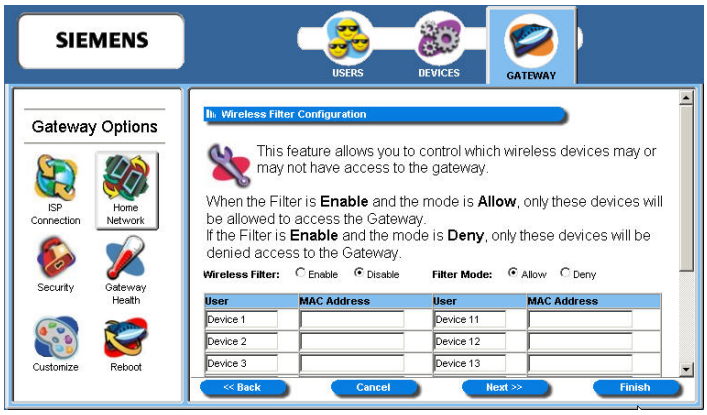
To use the WPA option:

1. From the "Wireless Security Configuration" window, select **WPA PSK** from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless WPA Configuration" window.

3. Select one of the following from the **Algorithms** drop-down menu:
   - **TKIP**
     Temporal Key Integrity Protocol is a more powerful security protocol than WEP. This option verifies the security configuration after encryption keys are determined, synchronizes changing of the unicast encryption key for each frame, and determines a unique starting unicast encryption key for each pre-shared key authentication.
   - **AES**
     Advanced Encryption Standard) supports a private key algorithm that ranges from 128 to 256 bits.
4. Type a key in **Shared Key**. The shared key is used to generate a dynamic encryption key for Gateway security.
5. Type a numeric value (in seconds) in **Group Key Renewal** to specify time to lapse between changing the key. The minimum time value is 30.
6. Click **Next**. This displays the "Wireless Filter Configuration" window.

Wireless Filter and Options Configuration

Control access to the Gateway of wireless devices based on the MAC address of the device using the "Wireless Filter Configuration" window. A MAC (Media Access Control) address refers to a hardware address that uniquely identifies each device of a network. Refer to the user documentation for each device you wish to deny or allow access for a particular MAC address.



To configure the wireless filter:

1. Select one of the following **Wireless Filter** options:
   - **Enable**
     Enable wireless filtering.
   - **Disable**
     Disable wireless filtering. If wireless filtering is disabled, all devices have access to the Gateway.
2. If wireless filtering is enabled, select one of the following **Filter Mode** options:
   - **Allow**
     Permits access to all the MAC addresses entered in the table.
   - **Deny**
     Restricts Gateway access to all the MAC addresses entered in the table.
3. Type the MAC address in the **MAC Address** column next to each device you either want to permit or restrict access.
4. Click **Next**. This displays the "Wireless Options Configuration" window.

5. Optionally, configure the following items:

   - **Data Transfer Rate**
     If a particular wireless client is unable to auto-negotiate a connection to the Gateway, the data transfer rate may be set to a specific data rate such as 11 Mbps for 802.11b wireless clients.
   - **RTS/CTS Threshold**
     A group of wireless clients may experience difficulty communicating with the Gateway without interrupting each other's communications. If this occurs, the RTS/CTS threshold may be set to a higher number to allow them each a longer period in which to communicate with the Gateway before the priority is switched to another wireless client wishing to transmit data.
   - **Fragmentation Threshold**
     The fragmentation threshold may be lowered to improve reliability in an excessively "noisy" wireless environment if changing channels does not provide significant enough improvement.

If you wish to reset the options in the "Wireless Options Configuration" window, click **Restore Default Values**. The system responds by restoring all the advanced features on this page.

6. Click **Next**. This displays the "Wireless Wizard" finish window.
7. Click **Finish** to save the settings.
8. Click **Reboot** for your wireless configuration to take effect.

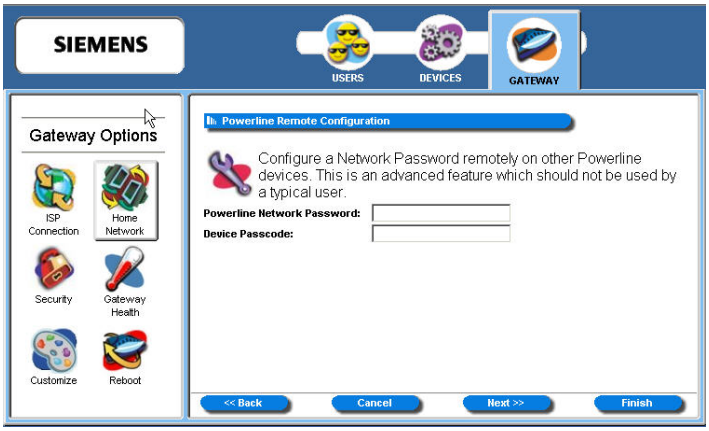
Powerline Security Configuration

If you have a Powerline enabled Gateway, you have the option of configuring security for the Powerline connection.

To configure powerline security:

1. Select one of the following **Powerline Interface** options:
   - **Enable**
     Enables a powerline connection.
   - **Disable**
     Disables a powerline connection. Click **Next**. This displays the "Finish" window.
2. If you selected **Enable**, enter a password to secure your powerline connection. This password must be identical on all powerline client devices.
3. Select one the following from the **Security Level** drop-down menu.
   - **Off**
     Powerline encryption is turned off.
   - **Minimum**
     Data transmitted is encrypted. Receives all data: unencrypted and encrypted.
   - **Standard**
     Data transmitted is encrypted. Data received must be encrypted.
   - **Maximum**
     Same as standard. Data transmitted is encrypted. Data received must be encrypted.
4. Click **Next**. This displays the "Powerline Filter Configuration" window.

5. Select one of the following **Powerline Filter** options:
   - **Enable**
     Enables powerline filtering.
   - **Disable**
     Disables powerline filtering. If powerline filtering is disabled, all devices have access to the Gateway.
6. If powerline filtering is enabled, select one of the following **Filter Mode** options:
   - **Allow**
     Permits access to all the MAC addresses entered in the table.
   - **Deny**
     Restricts access to all the MAC addresses entered in the table.
7. Type the MAC address in the **MAC Address** column next to each device you either want to permit or restrict access.
8. Click **Next**. This displays the "Powerline Remote Configuration" window.



Optionally configure a network password remotely on other powerline devices. To do this:

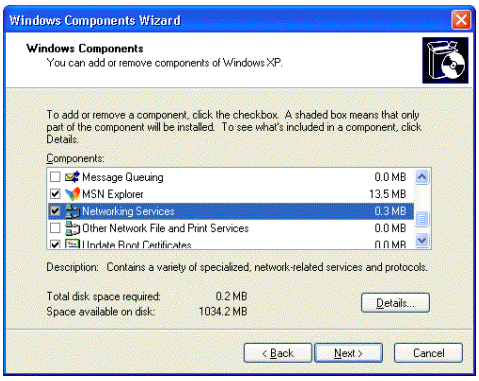
9. Enter the password you want to assign to all powerline devices in **Powerline Network Password**.
10. Enter the current password in **Device Password** for the powerline devices you want to change.
11. Click **Next**. This displays the Wizard "Finish" window.
12. Click **Reboot** to save the settings.

UPnP (Universal Plug and Play)

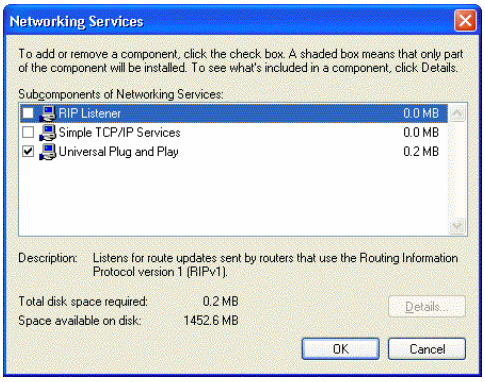
Microsoft UPnP allows the Gateway to communicate directly with certain Windows operating systems to trade information about the special needs of certain applications (such as messaging programs and interactive games) as well as provide information about other devices on the network. This communication between the operating system and Gateway greatly reduces the amount of manual configuration required to use new applications and devices.

Only certain versions of Windows XP and computer support the UPnP (Universal Plug and Play) function. Before configuring this option, make sure that UPnP is installed on your computer and enabled. Follow the steps below for installing UPnP components.

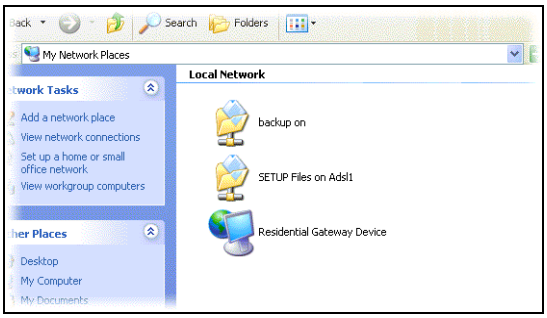
1. Select **Start>Control Panel**.
2. Select **Add or Remove Programs>Add/Remove Windows Components** to open the "Windows Components Wizard" window**.**



3. Select **Network Services** and click **Details**. This displays the "Networking Services" window.



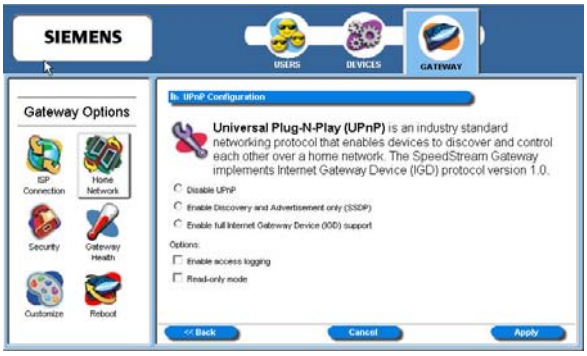
4. Select **Universal Plug and Play**.
5. Click **OK**. The system installs the UPnP components automatically.
6. After finishing the installation, go to **My Network Places**. You will find an icon for the UPnP function called Residential Gateway Device.



7. Double-click the icon. The Gateway will open another Web page for UPnP functions. Now, NAT functionality is available. The Gateway will create virtual servers automatically when it detects the computer running Internet applications that require this configuration.

Now you can configure the Gateway for UPnP. To configure UPnP on the Gateway:

1. Click **Configure the Universal Plug and Play Settings** link to display the "UPnP Configuration" window:



2. Select one of the following operating modes to enable or disable UPnP.

   - **Disable UPnP**
     Prevents the Gateway from using the UPnP feature to communicate with other devices or your operating system. Also may be disabled if your operating system does not support UPnP.
   - **Enable Discovery and Advertisement only (SSDP)**
     Sends information about new devices (hardware) detected only. No information concerning software applications or services is transmitted.
   - **Enable full Internet Gateway Device (IGD) support**
     Allows the Gateway to communicate freely with computers on the network about new devices, software applications, and services as needed to ensure they are working with minimal manual configuration required.

3. Select one of the following control options.

   - **Enable Access Logging**
     Logs UPnP transactions to the system log.
   - **Read Only Mode**
     Can read configuration information from a device; cannot modify the device configuration.

4. Click **Apply** to accept the settings. This displays the UPnP finish window.
5. Click **Reboot**.

Security

Your Gateway provides broad security measures against unwanted users. Security also allows for the configuration of the Gateway firewall, administrator password, (NAT) Network Address Translation, and DMZ (Demilitarized Zone) configuration.

To use the security option, click the **Security** button on the **Gateway Options** pane. This displays the "Security Options" window containing icons to access the security features.

This section is organized into parts that correspond to the following buttons shown in the **Gateway Option**s pane.

Firewall Settings

Configure the network firewall. A firewall is a system designed to prevent unauthorized access to or from a private network.

Admin Password

Change administrative password.

Address Translation

Configure address translation. Address translation hides individual users/computers behind a single outward-facing address. Hiding internal addresses allows greater security for your network.

Firewall Settings

A firewall is a system designed to prevent unauthorized access to or from a private network. The firewall window provides a listing of options to be enabled or disabled as well as links to configure the more complex details of each feature.

To configure the firewall:

1. From the "Security Options" window, click **Firewall Settings**. This displays the "Firewall Settings" window.

2. Select the checkboxes for all **Security** options you wish to enable. This can be any of the following:

   - **Level**
     Enable security level access is from the Gateway to the Internet or other networks. Click **Configure** to configure Security Level feature. This displays the "Firewall Level Configuration" window.

   - **Attack Detection**
     Enable protection from common hacker attacks to your computer/network from the Internet. Click **Configure** to configure the Attack Detection feature. This displays the "Attack Detection Configuration" window.

   - **IP Filtering**
     Configure inbound and outbound filter rules if your firewall Level setting is Custom. Click **Configure** to configure IP filter rules. This displays the "Firewall IP Filter Configuration Wizard" window.

3. Select **DMZ** for the **Gaming** option if you want to enable DMZ. Click **Configure** to configure firewall DMZ option. This displays the "Firewall DMZ Configuration" window.

4. Select the checkboxes for all **Support** options you wish to enable. This can be any of the following:

   - **Firewall Snooze Control**
     Bypass the firewall for a set amount of time so outside support personnel can access your Gateway or network or so you can run an application that conflicts with the firewall. Click Configure to configure the snooze control. This displays the "Firewall Snooze Control" window.

Security Level

Security level refers to how much access is permitted from your Gateway to the Internet or other networks.

To enable and configure the security level feature:

1. Select **Level** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **Level**. This displays the "Firewall Level Configuration" window.

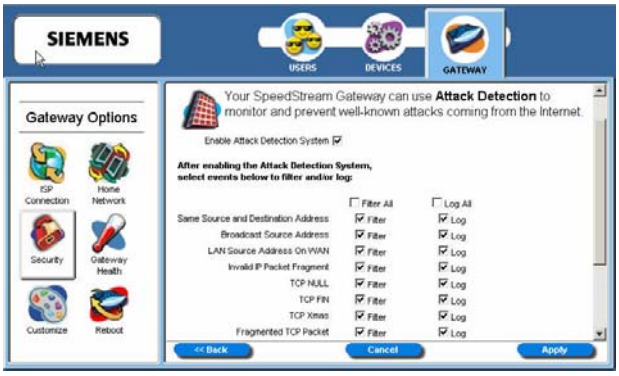
3. Select the firewall security level from the **Select Firewall Level** drop-down menu. This can be one of the following:
   - **Off**
     No firewall protection. Data can move freely both in and out of the Gateway.
   - **Low**
     Provides basic firewall protection. Attack detection is enabled and only ports well known to the Gateway can allow the flow of data.
   - **High**
     Provides maximum firewall protection. Only certain applications are allowed through the firewall or traffic that is already "in conversation" with an application from the host PC and host application. (ICSA 3.0a Compliant.)
   - **Custom**
     Set your own rules for firewall protection. This option should be used by advanced users only. If you select this option, you must set customized rules for both inbound and outbound traffic using the IP Filtering option.
4. Click **Apply**.

Attack Detection

If the Attack Detection System is enabled, the Gateway provides protection against the most common hacker attacks that attempt to access your computer/network from the Internet. Intrusion attempts can also be logged to provide a record of attempts and their source (when available).

To enable and configure the attack detection feature:

1. Select **Attack Detection** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **Attack Detection** option. This displays the "Attack Detection Configuration" window.



3. Select **Enable Attack Detection**.
4. Select **Filter** for each event in the list you want to filter or, if you want to filter all events, select **Filter All**. This provides maximum protection against malicious intrusion from outside your network.
5. Select **Log** for each event in the list you want to log or, if you want to log all events, select **Log All**.
6. Click **Apply**.

Below is a description of each event that can be monitored.

- **Same Source and Destination Address**
  An outside device can send a SYN (synchronize) packet to a host with the same source and destination address (including port) causing the system to hang. When the receiving host tries to respond to the source address in the packet, it ends up just sending it back to itself. This packet could ping-pong back and forth over 200 times (consuming CPU resources) before being discarded.
- **Broadcast Source Address**
  An outside device can send a ping to your Gateway broadcast address using a forged source address. When your system responds to these pings, it is brought down by echo replies.
- **LAN Source Address on LAN**
  An outside device can send a forged source address in an incoming IP packet to block trace back.
- **Invalid IP Packet Fragment**
  An outside device can send fragmented data packets that can bring down your system. IP packets can be fairly large in size. If a link between two hosts transporting a packet can only handle smaller packets, the large packet may be split (or fragmented) into smaller ones. When the packet fragments get to the destination host, they must be reassembled into the original large packet like pieces of a puzzle. A specially crafted invalid fragment can cause the host to crash
- **TCP NULL**
  An outside device can send an IP packet with the protocol field set to TCP but with an all null TCP header and data section. If your Gateway responds to this attack, it will bring down your system.

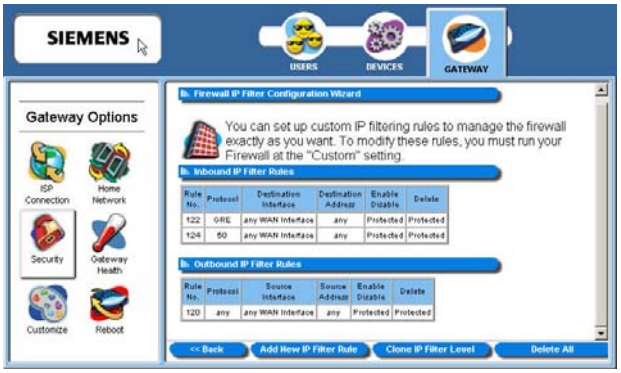
- **TCP FIN**
  An outside device can send an attack using TCP FIN. This attack never allows a data packet to finish transmitting and brings down your system.
- **TCP XMAS**
  An outside device can send an attack using TCP packets with all the flags set. This causes your system to slow to a halt.
- **Fragmented TCP Packet**
  An outside device can send an attack using fragmented packets to allow an outside user Telnet access to a device on your network.
- **Fragmented TCP Header**
  An outside device can send an attack using TCP packets with only a header and no payload. When numerous packets are sent through the Gateway in this manner, your system slows and halts.
- **Fragmented UDP Header**
  An outside device can send an attack using fragmented UDP headers to bring down a device on your network.
- **Fragmented ICMP Header**
  An outside device can send an attack using fragmented ICMP headers to bring down a device on your network.
- **Inconsistent UDP/IP header lengths**
  An outside device can send an attack using inconsistent UDP/IP headers to bring down a device on your network.
- **Inconsistent IP header lengths**
  An outside device can send an attack using changes in the IP header to zero the fragment offset field. This will be treated as a complete packet when received and cause your system to halt.

IP Filtering

Define inbound and outbound IP filter rules using this procedure. IP filtering rules can only be defined if the **Firewall Level** setting is **Custom**. This method of firewall protection is recommended for advanced users only.

To define IP filtering rules:

1. Click the **Configuration** hyperlink next to the **IP Filter** option on the "Firewall Settings" window. This displays the "Firewall IP Filter Configuration Wizard" window.



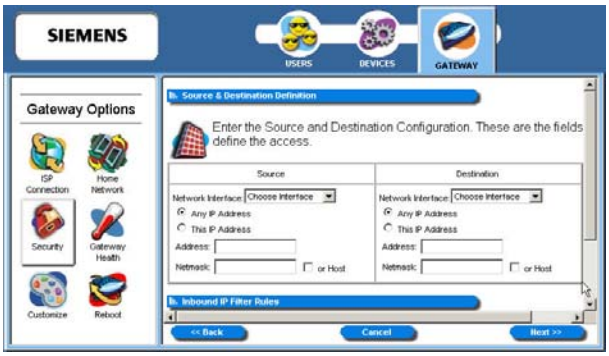
2. Do one of the following:
   - Click **Add New IP Filter Rule** to add new IP filter rules. This displays the "Basic Rule Definition" window.
   - Click **Clone IP Filter Level** to clone IP filter rules already defined. This displays the "Clone Rule Definition" window. Once cloned, you can modify the existing rules.

Add New IP Filter Rules

The "Basic Rule Definition" window is displayed when you select **Add New IP Filter Rule** from the "Firewall IP Configuration Wizard" window. Using this option, you can define both inbound and outbound rules. Each rule defined is added to the Rule Definition table.

To add a new rule:

1. Type up to a five digit numeric value in **Rule No** to uniquely identify the rule.
2. Select either **Permit** or **Deny** from the **Access** drop-down menu. Select **Permit** to allow the rule and **Deny** to prohibit the rule.
3. Select either **Inbound** or **Outbound** from the **Direction** drop-down menu. **Inbound** refers to data coming into the Gateway, while **Outbound** refers to data transmitted from the Gateway.
4. Optionally, select **Disable stateful inspection for packets matching this rule**.
5. Optionally, select **Create a log entry for packets matching this rule**. When selected, an entry is placed in the log file when packets match this rule.
6. Click **Next**. This displays the "Source and Destination Definition" window.



7. Under the **Source** heading, select a network connection from the **Network Interface** drop-down menu.
8. Select one of the following options:
   - **Any IP Address**
     Select this option if this rule applies to any IP address from the source.
   - **This IP Address**
     Select this option if a rule applies to a specific IP address from the source.

9. If you selected **This IP Address**, enter an IP address in the **IP Address** field and do one of the following:
   - Enter a netmask in the **Netmask** field.
   - Select **or Host** to use your Gateway netmask as the source netmask.
10. Under the **Destination** heading, select a network connection from the **Network Interface** drop-down menu.
11. Select one of the following options:
   - **Any IP Address**
     Select this option if this rule applies to any IP address of the destination.
   - **This IP Address**
     Select this option if a rule applies to a specific IP address of the destination.
12. If you selected **This IP Address**, enter an IP address in the **IP Address** field and do one of the following:
   - Enter a netmask in the **Netmask** field.
   - Select **or Host** to use your Gateway netmask as the destination netmask.
13. Click **Next**. This displays the "Protocol Definition" window.

14. Do one of the following:
   - Select one of the following protocol options from the **Select by Name** drop-down menu. This defines the types of packets filtered.
     - Any Protocol
     - TCP (Transmission Control Protocol):
       Provides reliable, sequenced, and unduplicated delivery of bytes to remote or local users. Click Next to display the "TCP/UDP Options" window.
     - UDP (User Datagram Protocol):
       Provides for the exchange of datagrams without acknowledgement or guaranteed delivery. Click Next to display the "TCP/UDP Options" window.
     - **ICMP** (Internet Control Message Protocol):
       A mechanism that provides for peer communication. The most commonly used application for this protocol is the PING command. Click **Next** to display the "ICMP Options" window.
     - **GRE** (Generic Routing Encapsulation):
       A tunneling protocol that is used primarily for VPN (Virtual Private Networks).
   - Type a protocol number in the **Select by Number** field.
15. Click **Finish**.

TCP/UDP Options Window

The "TCP/UDP Options" window is displayed if you select TCP or UDP protocol from the "Protocol Definition" window. If you selected either of these protocol types, you must identify the source and destination ports.

1. Select one of the following options from the **Source Port Operator** drop-down menu and the **Destination Port Operator** drop-down menu:

   - **any**
     Any port is acceptable as the source/destination port.
   - **less than or equal to**
     A port less than or equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **equal to**
     A port equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **greater than or equal to**
     a port greater than or equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **range**
     Any port between the value of the entry in the **Port 1** field and the value in the **Port 2** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** and **Port 2** fields.

2. Optionally, select **Check TCP syn packets** if you wish this rule to prevent the blocking of synchronization packets for pre-existing sessions.
3. Click **Next**.
4. Click **Finish**.

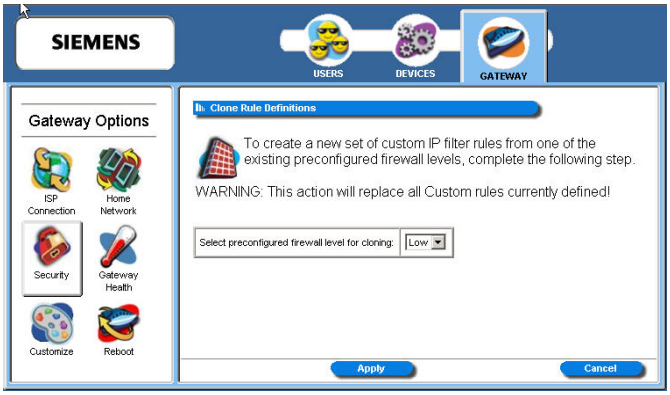
ICMP Options Window

The "ICMP Options" window is displayed if you select ICMP protocol from the "Protocol Definition" window.

1. Do one of the following:
   - Select any of the ICMP options you wish to filter.
   - Select **All Types** to filter all options.
2. Click **Next**.
3. Click **Finish**.

Clone IP Filter Rules

The "Clone Rule Definitions" window is displayed when you select **Clone IP Filter Level** from the "Firewall IP Configuration Wizard" window. Using this option, you can clone either high or low level rules and modify them according to your needs. If you choose to clone IP filter rules, the rules already defined in the Rule Definition table are discarded.



To clone IP filter rules:

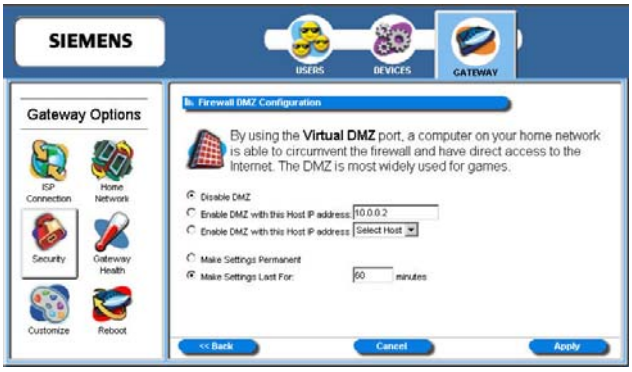
1. Select one of the following from the **Select preconfigured firewall level for cloning** drop-down menu.
   - **Low**
     Clones low-level IP filter rules.
   - **High**
     Clones high-level IP filter rules.
2. Click **Apply**. This displays the "Firewall IP Filter Configuration Wizard" window with the selected rule set showing in the Rule Definition table.
3. Disable or delete any rule as desired.

DMZ

The DMZ feature allows a computer on your home network to circumvent the firewall and have direct access to the internet. This feature is primarily used for gaming. The Gateway allows you to configure a temporary or permanent DMZ (Demilitarized Zone) to bypass the firewall for network or Internet gaming. If the DMZ feature is enabled, you must select the computer to be used as the DMZ computer/host. This function is recommended for use only when you require this special level of unrestricted access as it leaves your Gateway and network exposed to the Internet with no firewall protection.

To enable and configure the DMZ:

1. Select **DMZ** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **DMZ**. This displays the "Firewall DMZ Configuration" window.



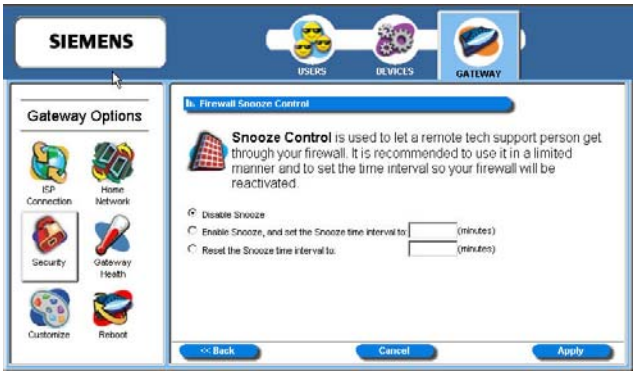
3. Select one of the following DMZ enable options:
   - **Disable DMZ**
     The firewall is not bypassed.
   - **Enable DMZ with this Host IP address**
     The firewall is bypassed through an IP address typed in the box next to this field.
   - **Enable DMZ with this Host IP address**
     The firewall is bypassed through an IP address that is selected from the **Select Host** drop-down menu next to this field. Select the desired host from the drop down.
4. Select one of the following time element options:
   - **Make Settings Permanent**
     DMZ settings are permanent unless changed by the administrator.
   - **Make Settings Last for**
     DMZ settings last for only the time (in minutes) entered in the box next to this option.
5. Click **Apply**.

Firewall Snooze Control

The snooze feature allows you to bypass the firewall for a set amount of time so outside support personnel can access your Gateway or network, or so you can run an application that conflicts with the firewall. This function is recommended for use only when you require this special level of unrestricted access as it leaves your Gateway and network exposed to the Internet with no firewall protection.

To enable and configure snooze control:

1. Select **Firewall Snooze Control** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **Firewall Snooze Control**. This displays the "Firewall Snooze Control" window.



3. Select one of the following options:
   - **Disable Snooze**
     Disables all snooze control. In this mode, the firewall is not bypassed.
   - **Enable Snooze, and set the Snooze time interval to**
     Enables snooze for a specified time period. Be sure to enter the number of minutes to define how long the firewall should be disabled.
   - **Reset the Snooze time interval to**
     Reset the snooze control time period. Use this option if you need a time extension for an open snooze session. Be sure to specify the additional amount of time (minutes) the firewall should be disabled.
4. Click **Apply**.

Administrator Password

You may change the Gateway administrator password at any time if you have administrative rights to the Gateway. To change the administrator password:

1. From the "Security Options" window, click the **Admin Password** button. This displays the "Enter Network Password" window.
2. Provide the administrator log on ID and password, then click **OK**. This displays the Gateway Administrator Setup window.

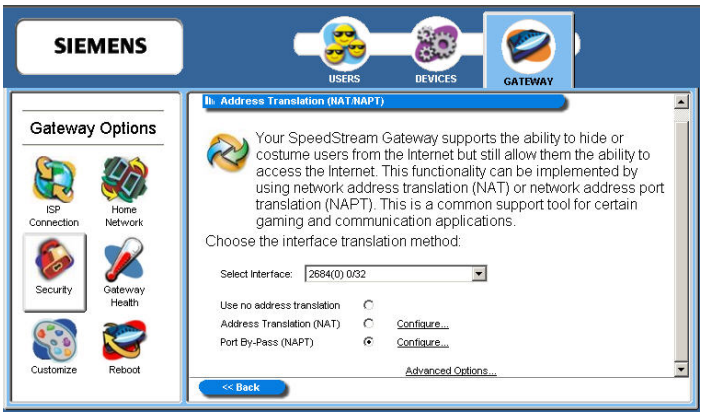
3. Make any desired changes to the **User Name**, **New Password**, and **Confirm Password**.
4. Click **Save Settings**.

Address Translation

The Address Translation feature provides different methods of keeping individual users/computers hidden behind a single outward-facing address, while still allowing them to access the Internet and related applications. If you have more than one available Internet connection interface, they will all be displayed in the drop-down menu for ease of selection.

To enable and configure the address translation feature:

1. From the "Security Options" window, select the **Address Translation** button. This displays the "Address Translation (NAT/NAPT)" window.



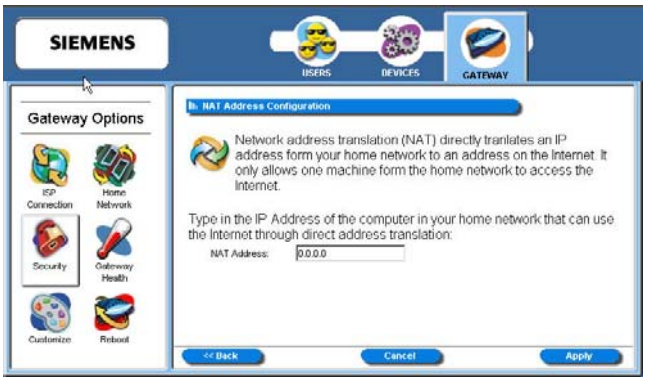
2. Select an interface from the **Select Interface** drop-down menu.
3. Select one of the following options:
   - **Use no address translation**
     Disables address translation.
   - **Address Translation (NAT)**
     Uses NAT for address translation. NAT is an Internet standard that allows a LAN to use one set of IP addresses for internal traffic and a second set for external traffic. This displays the "NAT Address Configuration" window.
   - **Port By-Pass (NAPT)**
     Uses NAPT for address translation. Only TCP, UDP, and ICMP protocols support NAPT. NAPT allows many devices connected to the Gateway access to the Internet while masking the identification of the internal IP addresses. This displays the "Port By-Bass Configuration" window.

Address Translation With NAT

Network Address Translation (NAT) translates an IP address from your home network to an address on the Internet. It allows only one machine to access the Internet.

To enable and configure NAT address translation:

1. Select **Address Translation (NAT)** from the "Address Translation (NAT/NAPT)" window.
2. Click the **Configure** hyperlink next to **Address Translation (NAT)**. This displays the "NAT Address Configuration" window.



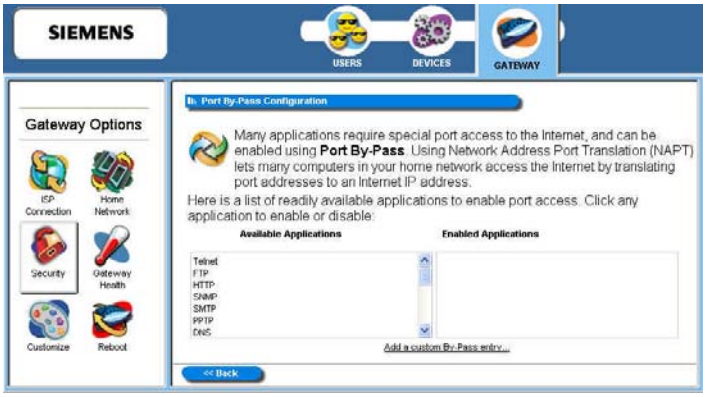
3. Type the IP address of the one computer in your network that you wish to have access to the Internet.
4. Click **Apply**.

Address Translation With NAPT

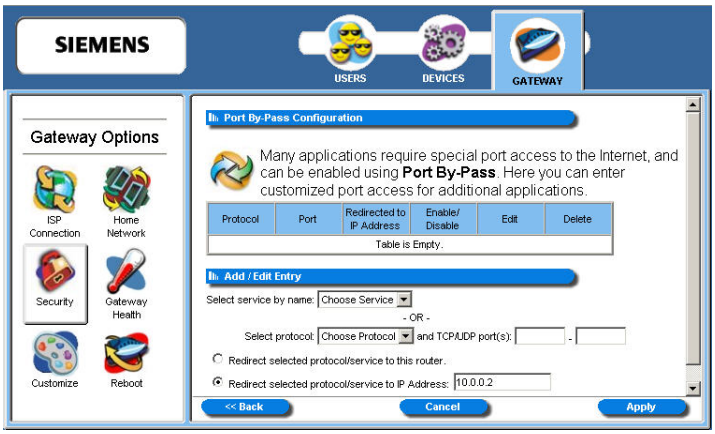
Many applications require special port access to the Internet in order to function. By enabling Network Address Port Translation (NAPT), multiple computers in your home network have access to the Internet by translating port addresses to an Internet IP address while masking their IP addresses from outside users. Only TCP, UDP, and ICMP protocols support NAPT.

To enable and configure NAPT address translation:

1. Select **Port By-Pass (NAPT)** from the "Address Translation (NAT/NAPT)" window.
2. Click the **Configure** hyperlink next to **Port By-Pass (NAPT)**. This displays the "Port-By-Pass Configuration" window.



3. To enable an application for NAPT, click the desired application from the **Available Applications** list. The application is moved to the **Enabled Applications** list.
4. Optionally, click the **Add a custom bypass entry** hyperlink. This displays the advanced features on the Port By-Pass Configuration" window. The advanced option allows you to configure special port access to the Internet.



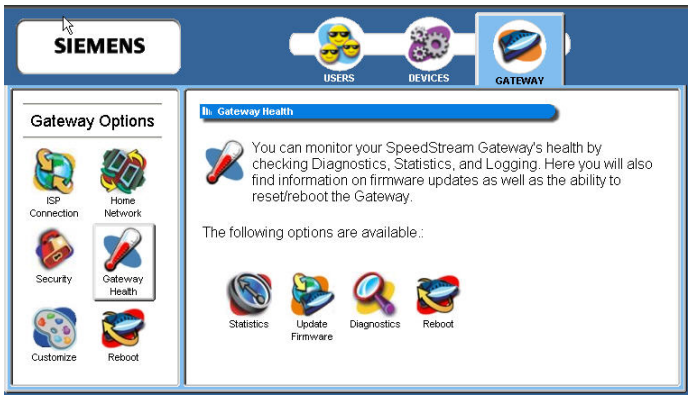
5. Do one of the following:
   - Select one of the following services from the **Select service by name** drop-down menu.
     - **Telnet**
       Telnet is a program that allows you to connect to other computers over the Internet. This options uses port 23.
     - **FTP** (File Transfer Protocol)
       FTP is used to transfer files in both ASCI and Binary format between local and remote devices. This option uses port 21.
     - **HTTP** (Hyper Text Transfer Protocol)
       HTTP is the standard method of transferring all types of information over the Internet. This option uses port 80.
     - **SNMP** (Signaling Network Management Protocol)
       SNMP is a protocol used by network management applications to help manage a network. This option uses port 161.
     - **SMTP** (Simple Mail Transfer Protocol)
       SMTP is used for sending email between servers. This port uses port 25.
     - **PPTP** (Point-to-Point Tunneling Protocol)
       PPTP is a protocol that allows VPN (Virtual Private Network) applications. This option uses port 1723.
     - **Domain**
       Domain is used for DNS options. This option uses port 53.
   - Select a protocol from the **Select Protocol** drop-down menu. This can be one of the following:
     - **TCP** (Transmission Control Protocol)
       Provides reliable, sequenced, and unduplicated delivery of bytes to a remote or local user.
     - **UDP** (User Datagram Protocol)
       A connectionless mode protocol that provides the delivery of packets to a remote or local user.
     - **ICMP** (Internet Control Message Protocol)
       A method by which IP software on a host or Gateway can communicate to pass information to other machines.
     - **GRE** (Generic Routing Encapsulation)
       This protocol is used to provide tunneling for a VPN connection.
6. If you selected a protocol, type the range of UDP or TCP ports in the appropriate boxes
7. Select one of the following options:
   - **Redirect selected protocol/service to this router**
     The protocol or service that you select is directed to your Gateway.
   - **Redirect selected protocol/service to IP Address**
     The protocol or service that you select is directed to an IP address on your LAN that you type in the box next to this field.
8. Click **Apply**.

Chapter 7

Monitoring Gateway Health

This chapter explains how to monitor the health of the Gateway.

This chapter describes how to monitor the health of the Gateway. The Gateway health options are used to gauge the various measures of Gateway's health. To use the Gateway health options, click the **Gateway Health** button from the **Gateway Options** pane. This displays the "Gateway Health" window.



Gateway Health options discussed in this chapter:

This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Health** pane.

Statistics

Used to measure the Internet stats, home networking stats, security stats, and the different Gateway log files.

Update Firmware

Updates the firmware of your Gateway through the Internet or from a device connected to your Gateway. (Not all Gateways will have this option.)

Diagnostics

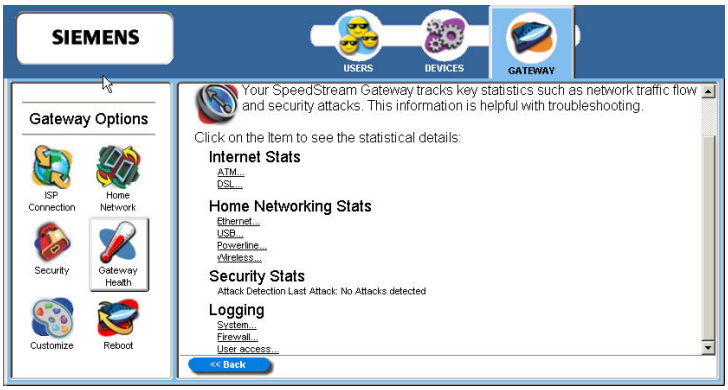
Runs a diagnostic program against a selected connection on your Gateway.

Reboot

Reboots the system or resets all settings to Gateway factory defaults.

Statistics

You can display statistics for the Internet, Home Networking, Security, and Logging. To display any of these statistics, click the **Statistics** button from the "Gateway Health" window. This displays the "SpeedStream Gateway Statistics" window.



Click the hyperlink for the type of statistics you wish to view. These fall into four categories:

- **Internet Stats**
  Internet statistics are commonly used by your Internet Service provider to diagnose service-related issues. Internet statistics include either ATM or DSL statistics.
- **Home Networking Stats**
  Home Networking statistics are helpful for troubleshooting issues on your home network. These statistics are displayed for each physical interface connected to the Gateway. They are separated into Ethernet, USB, Powerline, or Wireless statistics.
- **Security Stats**
  Security breach attempts are shown for any firewall rules or attack detection services you have defined on the Firewall customization window.
- **Logging**
  Extensive activity logs are provided for advanced troubleshooting and administrative use. The following types of logs are available: System, Firewall, and User Access.

Internet Stats

Internet statistics are commonly used by your Internet Service provider to diagnose service-related issues. Internet statistics include either ATM or DSL statistics.

ATM Statistics

View status and statistical information for the WAN-side Asynchronous Transfer Mode (ATM) network connection. WAN-side connection to the service provider is based on an Asynchronous Transfer Mode (ATM) network connection. In addition, statistical information is provided for each Virtual Circuit (VC) configured under the ATM Adaptation Layer (AAL).

To view ATM statistics, click the **ATM** hyperlink under **Internet Stats**.

DSL Statistics

View status and statistical information for the Digital Subscriber Line (DSL) when the physical WAN-side connection to the service provider is achieved through a DSL line. Statistical information is accumulated over periodic intervals and may be displayed for up to a 24 hour period.

To view DSL statistics, click the **DSL** hyperlink under **Internet Stats**

Home Networking Stats

Home Networking statistics are helpful for troubleshooting issues on your home network. These statistics are displayed for each physical interface connected to the Gateway. They are separated into Ethernet, USB, Powerline, or Wireless statistics.

Ethernet Statistics

View status and statistical information for LAN-side Ethernet connectivity.

Pay special attention to the status (up or down) reported for each Ethernet port to verify that each cable is connected properly and detected by the Gateway.

USB Statistics

View status and statistical information for LAN-side USB connectivity.

Pay special attention to the status (up or down) reported for each USB port to verify that each cable is connected properly and detected by the Gateway.

Powerline Statistics

View status and statistical information for Powerline connectivity.

Pay special attention to the status (up or down) reported for the Powerline connection to verify that powerline is connected properly and detected by the Gateway.

Wireless Statistics

View status and statistical information for Wireless connectivity.

Pay special attention to the status (up or down) reported for the wireless connection to verify that the wireless connection is properly configured and detected by the Gateway.

Logging

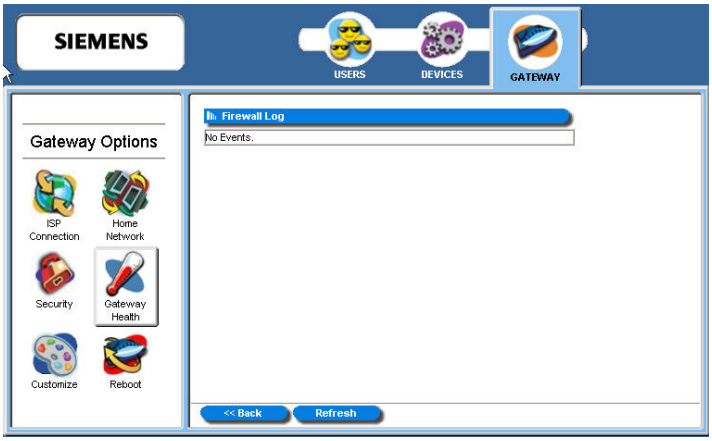
Extensive activity logs are provided for advanced troubleshooting and administrative use. The following types of logs are available: System, Firewall, and User Access.

System Logging

System logging displays Gateway status, user login, interfaces accessed, etc. Activity displayed in the system log is defined using the checkboxes provided at the bottom of the window. Click Apply after making any changes. The system log can be cleared or saved to a text file using the appropriate buttons, Clear Log or Save Log.

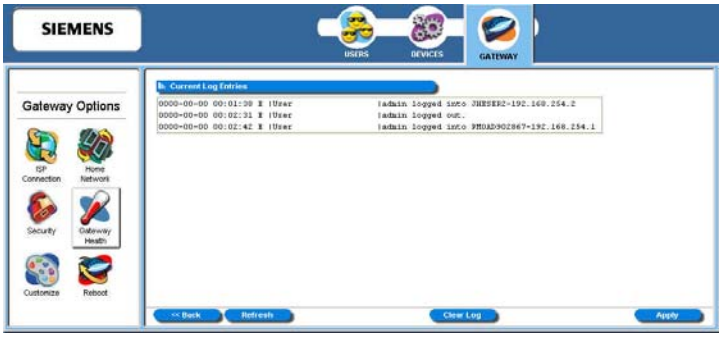
Firewall Logging

Firewall Logging displays attempts (both failures and successes) to access data through the firewall. Firewall log entries are defined on the **Firewall Settings Configuration** window found under the **Security** menu.



User Access

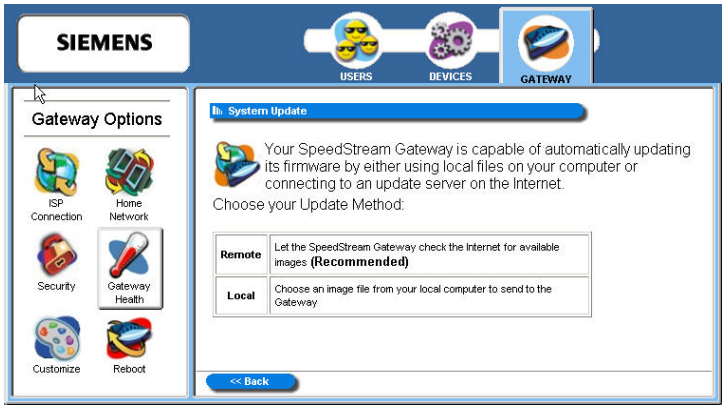
User Access logging displays activity related to users logging in or out of the Gateway. Both successful and unsuccessful attempts by username are recorded.



Update Firmware

This feature updates the firmware of your Gateway through the Internet or from a device connected to your Gateway. This option may not be available on your Gateway configuration. If available, you must be logged in as the Gateway Administrator to access the utility.

To access this feature, click the **Update Firmware** button from your "Gateway Health" window. This displays the "System Update" window.



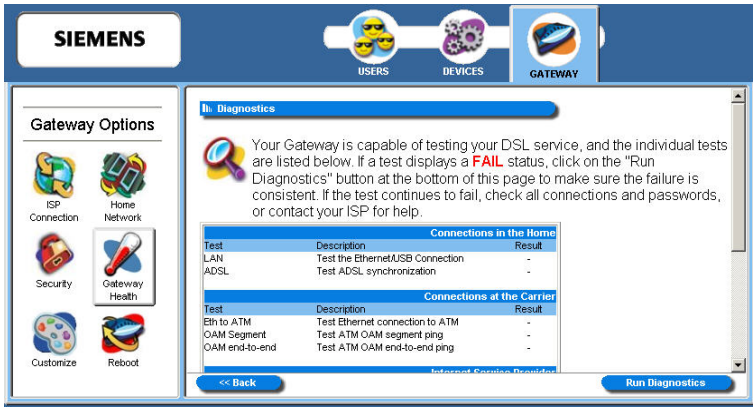
Select one of the following download options to start the download process.

- **Remote**
  Checks the Internet for the appropriate upgrade file. This is the recommended method.
- **Local**
  Download the firmware update from a location on your network and select the upgrade file. Before doing this, you must download the upgrade file to your computer.

Important: Do not turn off or interrupt the Gateway during a firmware upgrade session. The Gateway could be rendered inoperable!

Diagnostics

The Gateway provides diagnostic tests and data for each interface. This data is commonly requested by technical support to assist in troubleshooting. To access this feature, click the **Diagnostics** button from your "Gateway Health" window. This displays the "Diagnostics" window.



To use the diagnostic option:

1. Select a connection to test from the **Connection to Test** drop-down menu. You must move all the way to the bottom of this window to display this drop-down menu.
2. Click **Run Diagnostics**. The system responds by displaying the results in the different tables. Pay special attention to any tests that report a failing condition and check the connections for these interfaces before running the diagnostics again.
3. Click **Apply**.

Chapter 8

Miscellaneous Gateway Options

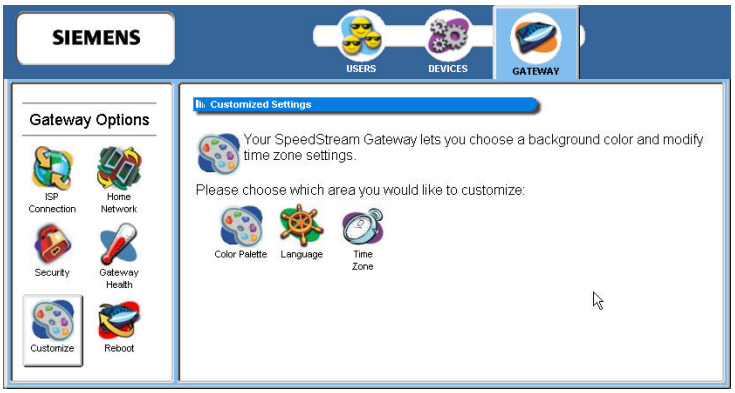
This chapter explains how to customize the appearance of the configuration program and to reboot the Gateway. This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Options** pane.

Customize the Gateway's display.

Reboot the Gateway.

Customize

You are able to control the background color, language, and time zone settings of your Gateway using customization options. To access the customization options, click the **Customization** button from the **Gateway Options** pane. This displays the "Customized Settings" window.



Customization options discussed in this chapter:

Customize the appearance of the configuration interface/program.

Select language to display in text. (Not all Gateways will have this option.)

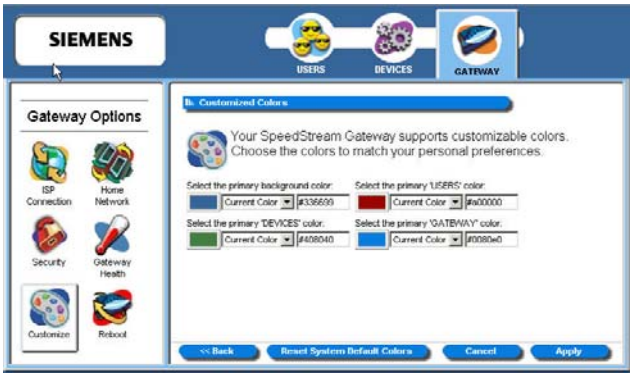
Configure time parameters to automatically synchronize the Gateway's internal date and time settings with those of your selected time zone.

Color Palette

Multiple color selections are available to customize the appearance of the configuration interface/program.

To configure the color palette:

1. From the "Customized Settings" window, click the **Color Palette** button. This displays the "Customized Colors" window.



2. Using the color drop-down menus from the different display options, select the colors you wish to use in the system.
3. Optionally, type a numeric color value in the box next to the particular color drop-down menu. The number is based on RGB (Red Green Blue) values. For example, the color red is represented by a value of ff0000, green is represented by a value of 00ff00, and blue is represented by a value of 0000ff. If you are entering a numeric value for the color, ensure that the "#" is in front of your numeric value.

   Click **Reset System Default Colors** if you want to reset all system color schemes to the factory settings.
4. Click **Apply**.

Language

Multiple languages may be available for displaying text in the configuration interface/program. This option may not be available on your Gateway configuration.

To set the language used on the Gateway windows:

1. From the "Customized Settings" window, click the **Language** button. This displays the "Customized Language" window.

2. Select your desired language.
3. Click **Apply**.

Time Zone

Using this option, you can configure the time parameters to automatically synchronize the Gateway's internal date and time settings with those of your selected time zone. This time will be used to control time restrictions you may set for users as well as in entries in the system log.

To enable and configure the time zone feature:

1. From the "Customized Settings" window, click the **Time Zone** button. This displays the "Configure Time Zone" window.

2. Select **Yes** for **Enable Time Client**.
3. Select a time zone from the **Select Time Zone** drop-down menu.

   Note: The Gateway's time server is unable to determine whether your time zone is currently observing daylight savings time. If you are currently observing daylight savings time, select an alternate time zone that matches your time settings during daylight savings time observation periods.
4. Click **Apply**.

Reboot

You can reboot the Gateway using the Reboot option, or you can reset the Gateway to factory defaults using the reset option. Reboot should be used when the Gateway needs to be restarted. The Gateway can also be rebooted using the power switch on the rear panel of the Gateway. This option can be used at either the user or administrator level.

To reboot or reset factory defaults on the Gateway:

1. Click the **Reboot** button from the **Gateway Options** pane. This displays the "System Reboot" window.

2. If you want the factory default settings to be reset, click **Reset to Factory Defaults**. Reset should be used when you find it necessary to recover the factory default settings. This may be necessary when a custom configuration did not go as planned, when a new configuration is desired, or when the Gateway does not appear to be working properly. This option resets all custom settings, users, and passwords on your Gateway. You must be logged on as the administrator to use this option.

3. Click **Reboot**.

Appendix A

Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the Wireless DSL Gateway and some possible solutions to them. If you follow the suggested steps and the Gateway still does not function properly, contact your Internet Service Provider or Technical Support for assistance.

General Issues

Problem: **Can't connect to the Gateway to configure it.**

Solution: Check the following:

- The Gateway is properly installed, connections are OK, and it is powered ON. Check the LEDs for Ethernet or USB port status.
- Ensure that your computer and the Gateway are on the same network segment.
- If your computer is set to "Obtain an IP Address automatically" (DHCP client), restart your computer.

Internet Access

Problem : **When I enter a Web site address or IP address I get a time out error.**

Solution: A number of things could be causing this. Try the following troubleshooting steps.

- Verify that other computers work. If they do, ensure that your computer's IP settings are correct. *Refer to Chapter 3- Operating System Configuration.* If using a fixed (static) IP address, check the network mask, default Gateway and DNS settings as well as the IP address.
- If the computers are configured correctly, but still not working, check the Gateway. Ensure that it is connected and on. Connect to it and check its settings. (If you cannot connect to it, check the Ethernet and power connections.)

Problem: **Some applications do not run properly when using the Gateway.**

Solution: The Gateway processes the data passing through it, so it is not transparent.

- If you are running a supported Windows operating system, ensure that the UPnP feature is enabled. Refer to *UPnP (Universal Plug and Play)* in Chapter 5 for more information on this feature.
- If this does not solve the problem or your operating system does not support UPnP you can use the *DMZ* function. This should work with almost every application, but:

  - It is a security risk, since the firewall is disabled for the DMZ computer.

  - Only one (1) computer can use this feature.
- A third option is to use the Firewall Snooze Control feature to temporarily disable the

firewall to allow the application to function unimpeded.

Contacting Technical Support

Before contacting technical support, please refer to the previous troubleshooting information. For issues concerning DSL service or connectivity, contact your Internet Service Provider (ISP) directly. If you are still unable to resolve the problem, be prepared to provide the following information:

- Internet Service Provider and service type (DSL, cable)
- Product model number (SpeedStream SS6000 Series)
- Date of purchase or installation
- Description of problem

Technical Support services are available via the Internet, e-mail and telephone:

Telephone: (972) 852-1000
Fax: (972) 852-1001
Email: infor.ssn@siemens.com
Internet: http://www.icn.siemens.com/subscriber

Appendix B

Specifications

Media Interface:	RJ-11 DSL WAN connection (5) 10/100Base-T RJ-45 Ethernet LAN connections (Auto-MDI/MDI-X) USB Type B connection DB-9 RS-232 Serial console port
Diagnostic LEDs:	Power, Status, Link and Activity for DSL, Ethernet, USB (optional), and Wireless
Management:	Intuitive, Web-based management Comprehensive hardware diagnostics SNMPv1 support UPnP IGD-NAT traversal support XML Management Scheme, DSL Forum 2002-281
Security:	PAP (RFC 1334), CHAP (RFC 1994) Password Authentication Access Control list Stateful Inspection Firewall with Denial of Service (DoS) protection Pre-configured firewall levels for ease of use with "Custom" level for advanced users Filter on source and/or destination IP address Filter on transport protocol and/or port number Firewall logging with Network Time Protocol support and Syslog support DMZ support and Firewall "Snooze" feature Content filtering ICSA compliancy mode
Standards Compliance:	IEEE 802.1d, 802.11g, 802.3, and 802.3u USB 1.1 (optional) T1.413 issue 2 G.992.1 (G.DMT) G.992.2 (G.Lite)

Routing:	DHCP server and DNS agent Network Address Port Translation (NAPT) Network Address Translation (NAT) Packet filtering RFC 2364 Point-to-Point Protocol over ATM PVCs (PPPoA) RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE) RFC 2684 (formerly 1483) Bridged Ethernet and routed encapsulation RFC 2225 (formerly 1577) Classical IP over ATM PPPoE Relay/Bridging Configurable PAP and CHAP authentication TCP/IP with RIP1 and RIP2 or static routing on the LAN and/or WAN Dynamic DNS Support IP QoS (depending on configuration)
Bridging:	IEEE 802.1.d Transparent Learning Bridge (dynamic learning of up to 255 addresses) RFC 2684 (formerly 1483) Bridged Ethernet over ATM PVCs Spanning Tree support
AAL and ATM Support:	Up to 8 active VCCs across VPI 0-255, VCI 0-65535 address range ATM Forum UNI3.1/4.0 PVC ATM Traffic class: UBR, CBR, VBRnrt, VBRrt OAM F5
Power:	12V power supply included 1000mA max. output
Certifications:	FCC Part 15, Class B FCC Part 68 UL Listed CE certification CSA Industry Canada WHQL

Siemens Subscriber Network
4849 Alpha Road
Dallas, TX 75244 USA
(972) 852-1000 Tel
(972) 852-1001 Fax
info.ssn@siemens.com
http://www.icn.siemens.com/subscriber