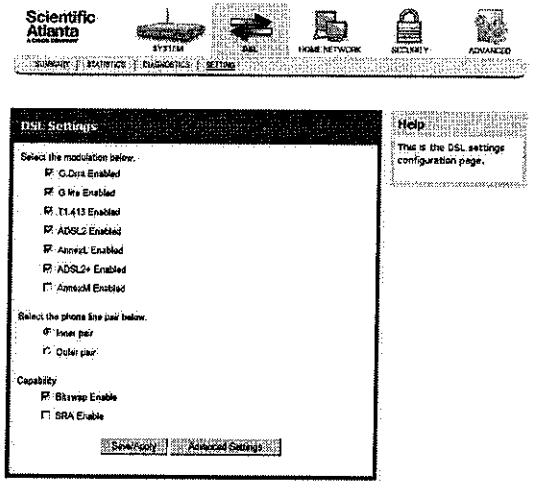
Configuring DSL Settings

To configure the DSL settings for the residential gateway, complete the following steps.

1 Click **System** on the main screen. The Summary screen opens by default.

2 Click the **Setting** tab. The DSL Settings screen opens.



3 Under the Select the modulation below area on the screen, select the modulation that you want to use. You can select one or all of the following modulations:

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

4 Select the phone line pair that you want to use from the following options: ?? what is this????

- Inner pair
- Outer pair

5 Select the capability that you want to use from the following options:

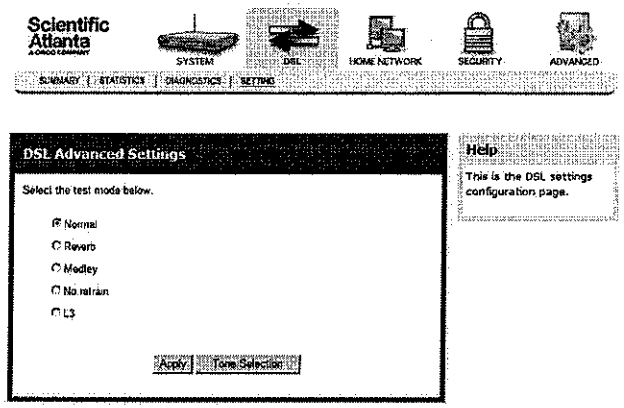
- Bitswap Enable
- SRA Enable

6 Click **Save/Apply** to save the configuration.

DSL Advanced Settings

The DSL Advanced Settings screen allows you to select a test mode.

Path: DSL>Setting>Advanced Settings

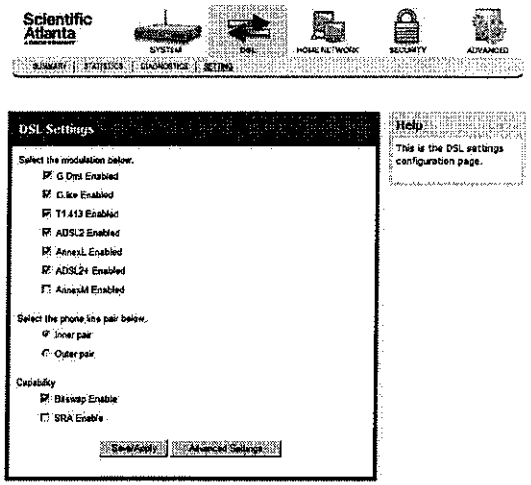


Configuring DSL Advanced Settings

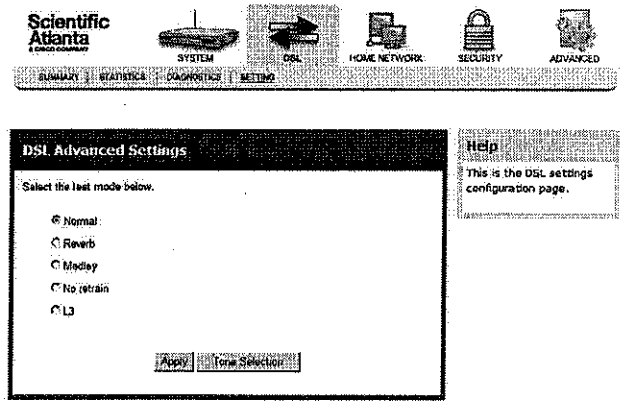
To configure the DSL advanced settings, complete the following steps.

1 Click **DSL** on the main screen. The Summary screen opens by default.

2 Click the **Setting** tab. The DSL Settings screen opens.



3 Click **Advanced Settings**. The DSL Advanced Settings screen opens.



4 Select the test mode from the following options:

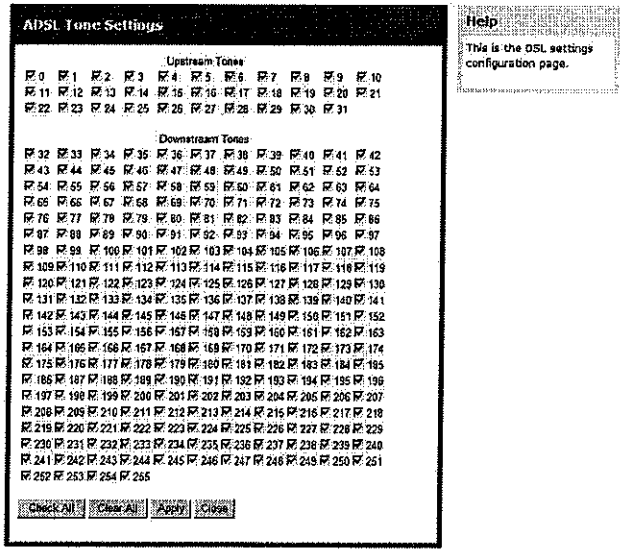
- Normal
- Reverb
- Medley
- No refrain
- L3

5 Click **Apply** to configure the advanced settings.

Tone Settings

The ADSL Tone Settings screen allows you to select active DSL tones or frequencies used by the DSL transceiver.

Path: DSL>Setting>Advanced Settings>Tone Selection

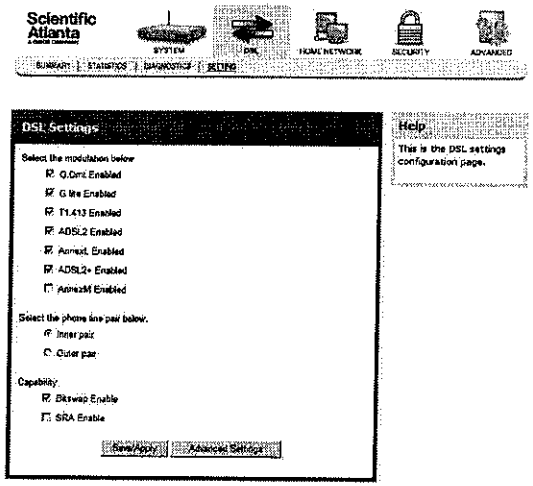


Setting DSL Tones or Frequencies

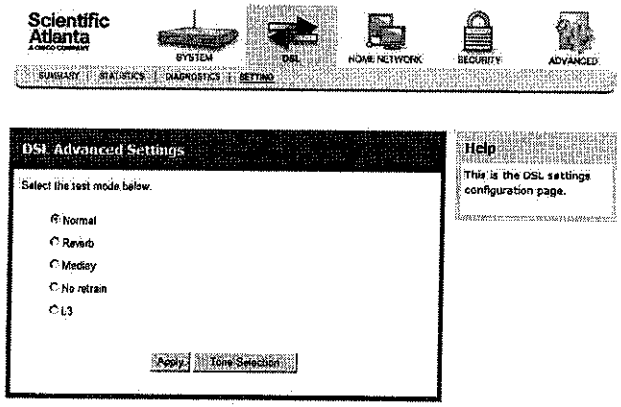
To set DSL tones or frequencies, complete the following steps.

1 Click **DSL** on the main screen. The Summary screen opens by default.

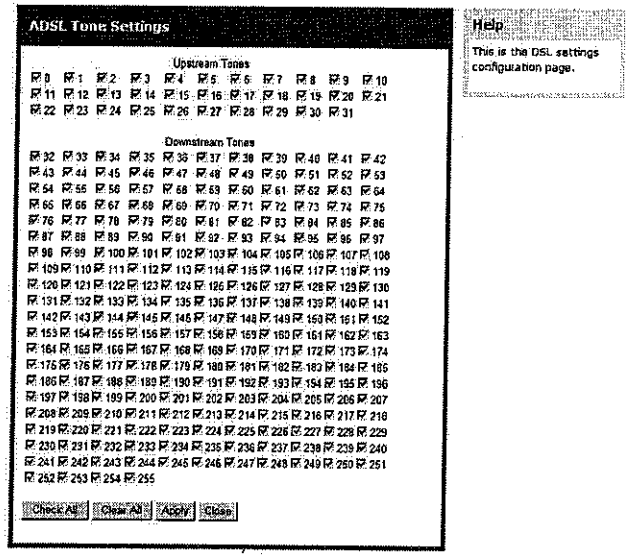
2 Click the **Setting** tab. The DSL Settings screen opens.



3 Click **Advanced Settings**. The DSL Advanced Settings screen opens.



4 Click **Tone Selection**. The ADSL Tone Settings screen opens.



5 Select the ADSL tone settings as follows.

- To select all the tones, click **Check All**.
- To select individual tones, click **Clear All** and then select the tones you want.

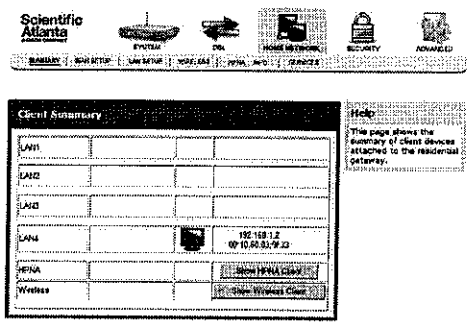
6 Click **Apply** to configure the tone settings.

7 Click **Close** to return to the DSL Advanced Settings screen.

Client Summary

The Client Summary screen shows all the client devices attached to the residential gateway. You can click Show HPNA Client to display the HPNA devices attached to the HPNA RF interface of the residnential gateway.

Path: Home Network>Summary

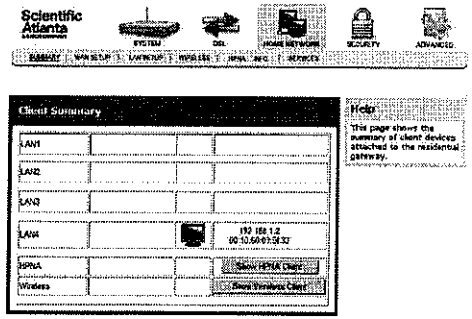


Updating HPNA Clients

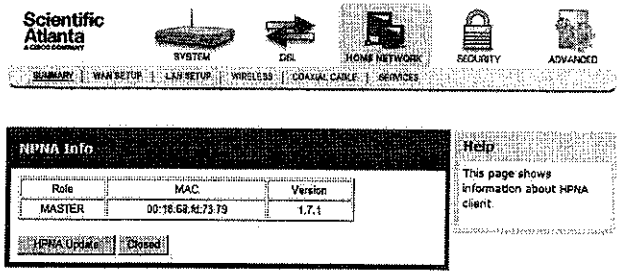
To update the HPNA clients, complete the following steps.

1 Click **Home Network** on the main screen.

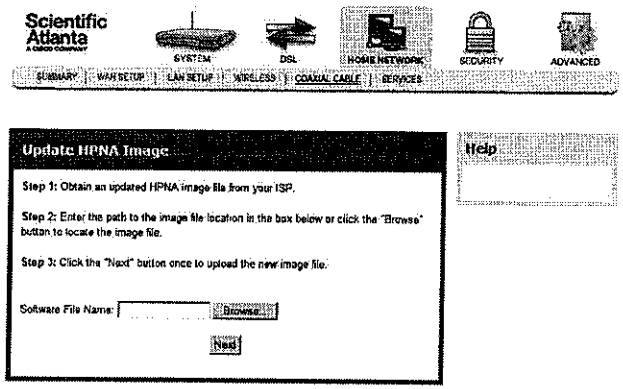
2 Click **Summary**. The Client Summary screen opens.



3 Click **Show HPNA Client**. The HPNA Info screen opens.



4 Click **HPNA Update** to update the HPNA software of HPNA devices attached to the residential gateway The Update HPNA window opens.



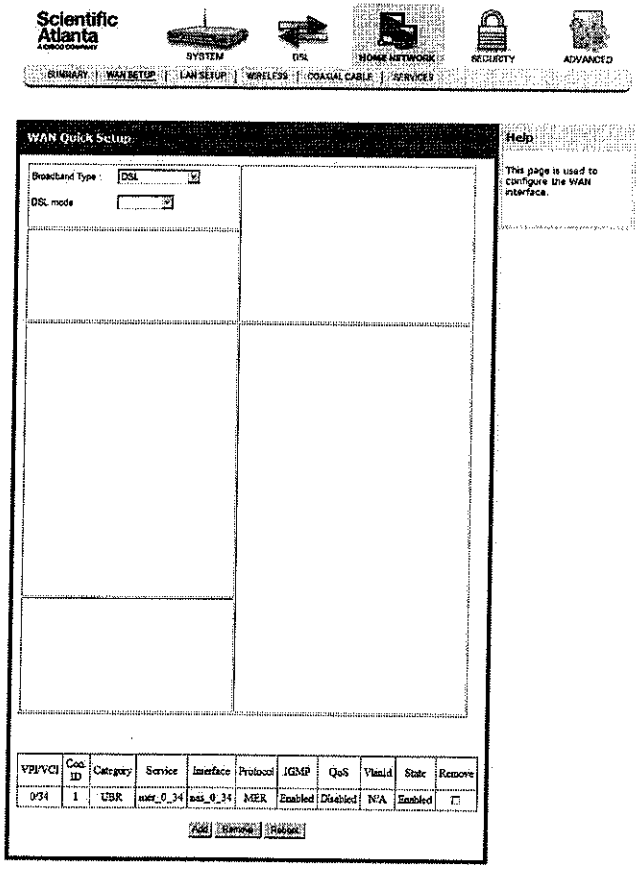
5 In the Software File Name field, enter the name of the file that you want to use to update your system. You can click Browse to locate the file.

6 Click **Next**. The software for the attached HPNA devices is updated.

WAN Setup

The Wide Area Network (WAN) Setup screen allows users to set up WAN connections and settings, such as virtual channel identifiers (VCi), virtual path identifiers (VPI), and quality of service (QoS).

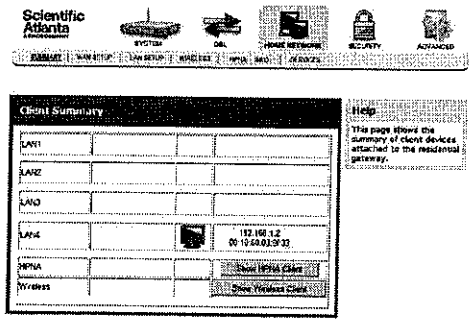
Path: Home Network>WAN Setup



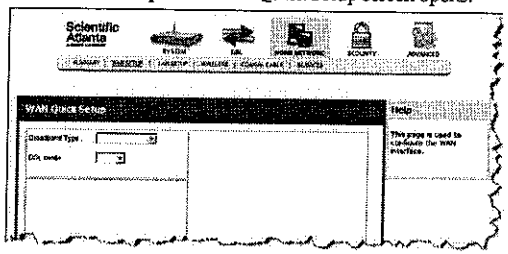
Configuring the WAN Interface (MER Broadband Type)

To configure a WAN interface for MAC Encapsulation Routing (MER) broadband type, complete the following steps.

1 Click **Home Network** on the main screen. The Client Summary screen opens.

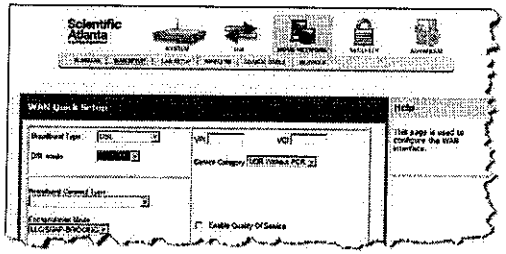


2 Click **WAN Setup**. The WAN Quick Setup screen opens.



3 In the Broadband type field, enter DSL.

4 In the DSL Mode field, enter ATM. More fields populate on the screen as shown here.



5 Complete the following fields on the screen as follows:

Note: This configuration is an example of a specific setting for the residential gateway. Your values may differ depending upon your service provider.

- **a** In the Broadband Connect Type field, select **MAC Encapsulation Routing (MER)**.
- **b** In the Encapsulation Mode field, select **LLC/SNAP - Bridging**.
- **c** In the VPI field, enter the virtual path identifier (VPI). Values are: 0 to 65535
- **d** In the VCI field, enter the virtual channel identifier (VCI). Values are: 0 to 65535
- **e** In the the Service Category field, select **UBR Without PCR**.
- **f** Select the Enable Quality of Service check box.
- **g** Select the Obtain an IP address automatically option.
- **h** Select the Obtain default gateway automatically option.
- **i** Select the Obtain DNS server addresses automatically option.
- **j** Select the Enable IGMP Multicast check box.
- **k** Select the Enable WAN Service check box.

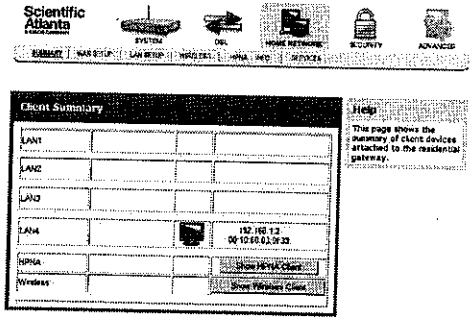
6 Click **Add**.

7 Click **Reboot**. This action reboots the residential gateway so that the WAN setup configuration takes effect.

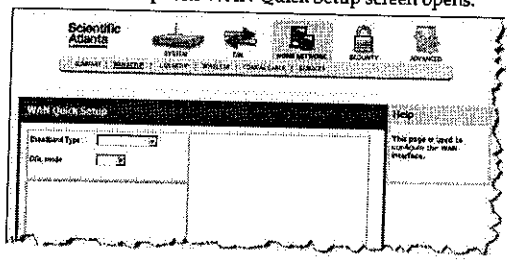
Configuring the WAN Interface (PPPoE Broadband Type)

To configure a WAN interface with the PPP over Ethernet (PPPoE) broadband type, complete the following steps.

1 Click **Home Network** on the main screen. The Client Summary screen opens.

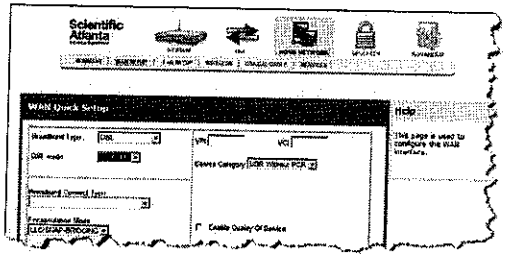


2 Click **WAN Setup**. The WAN Quick Setup screen opens.



3 In the Broadband type field, enter DSL.

4 In the DSL Mode field, enter ATM. More fields populate on the screen as shown here.



5 Complete the following fields on the screen as follows:

- **a** In the Broadband Connect Type field, select **PPP over Ethernet (PPPoE).**
- **b** In the Encapsulation Mode field, select **LLC/SNAP - Bridging.**
- **c** In the VPI field, enter the virtual path identifier (VPI). Values are: 0 to 65535
- **d** In the VCI field, enter the virtual channel identifier (VCI). Values are: 0 to 65535
- **e** In the the Service Category field, select **UBR Without PCR.**
- **f** In the Authentication Method field, select **AUTO.**
- **g** Select the Enable IGMP Multicast check box.
- **h** Select the Enable WAN Service check box.

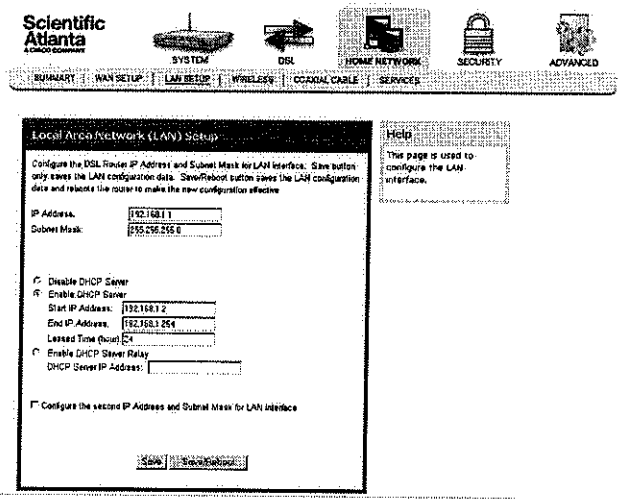
6 Click **Add.**

7 Click **Reboot.** This action reboots the residential gateway so that the WAN setup configuration takes effect.

LAN Setup

The Local Area Network (LAN) Setup screen allows users to set up LAN settings such as dynamic host configuration protocol (DHCP), Internet gateway multi-cast protocol (IGMP), and universal plug and play (UPnP).

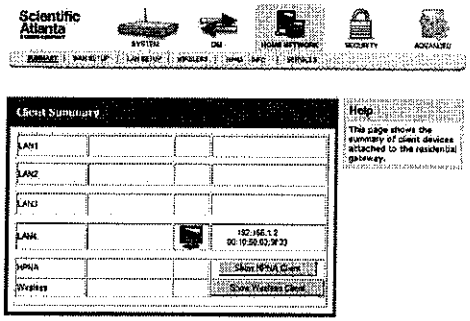
Path: Home Network>LAN Setup



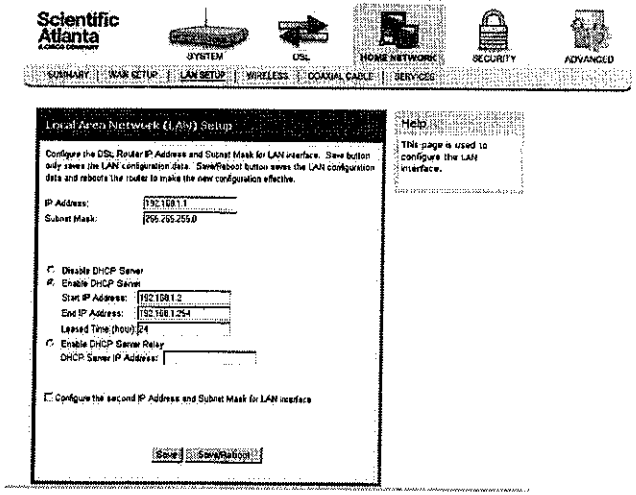
Configuring the LAN Interface

To configure the LAN interface, complete the following steps.

1 Click **Home Network** on the main screen. The Client Summary screen opens.



2 Click **LAN Setup.** The Local Area Network (LAN) setup screen opens.



3 In the IP Address field, enter the IP address for the residential gateway.

4 In the Subnet Mask field, enter the subnet mask for the residential gateway.

5 Do you want to Enable the DHCP server?

- If **yes**, select **Enable DHCP Server**, and go to step 6.
- If **no**, select **Disable DHCP Server**, and go to step 7.

6 Under Enable DHCP server, enter the following information:

- In the Start IP Address, enter the first IP address in the range for...
- In the End IP Address, enter the last IP address in the range for...
- In the Leased Time (hour) field, enter the...

7 Do you want to enable the DHCP server relay?

- If **yes**, select **Enable DHCP Server Relay**. The DHCP Server address field populates with the address for the ...
- If **no**, do not select **Enable DHCP Server Relay**.

8 Do you want to configure a second IP address and subnet mask for the LAN interface?

- If **yes**, select **Configure the second IP Address and Subnet Mask for LAN interface**. The screen populates with another IP address and subnet mask field.
- If **no**, do no select **Configure the second IP Address and Subnet Mask for LAN interface**. Go to step 10.

9 Under Configure the second IP Address and Subnet Mask for LAN interface, enter the following information.

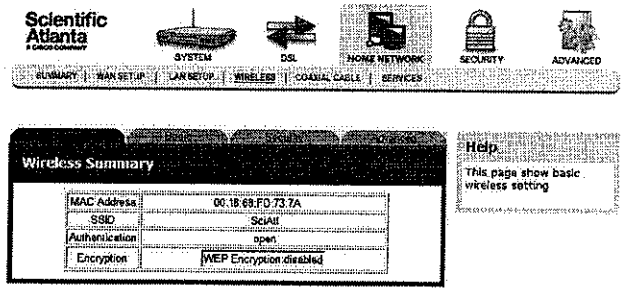
- In the IP Address field, enter the IP address for the residential gateway.
- In the Subnet Mask field, enter the subnet mask for the residential gateway.

10 Click **Save to save the changes** or click **Save/Reboot** to save the changes and reboot the residential gateway.

Wireless Summary

The Wireless Summary screen shows the MAC address and security information for the wireless connection.

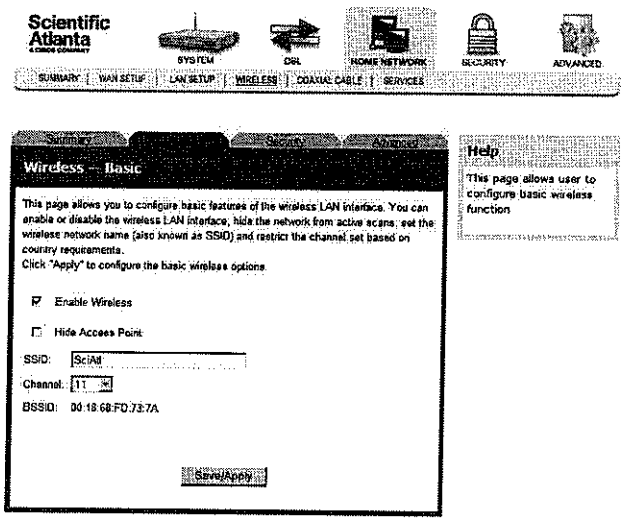
Path: Home Network>Wireless>Summary



Wireless Basic

The Wireless Basic screen shows the basic wireless access point (AP) parameters.

Path: Home Network>Wireless>Basic

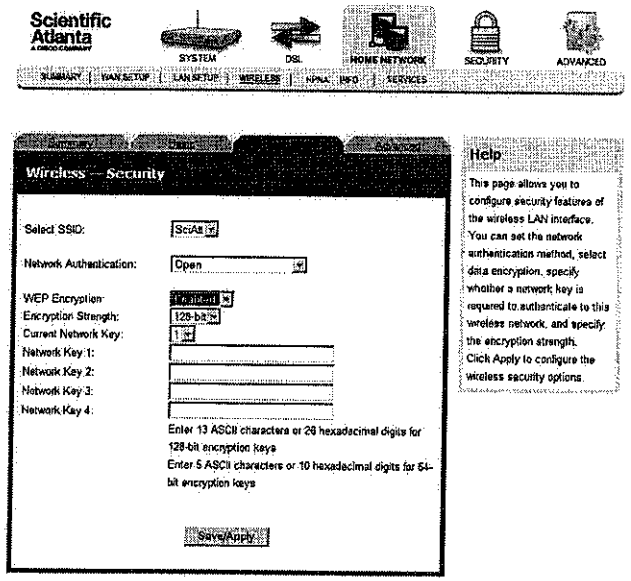


Wireless Security

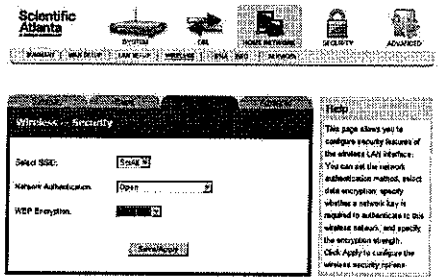
The Wireless Security screen allows you to configure security features of the wireless LAN interface. You can set the network authentication method, select data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Path: Home Network>Wireless>Security

WEP Encryption Enabled



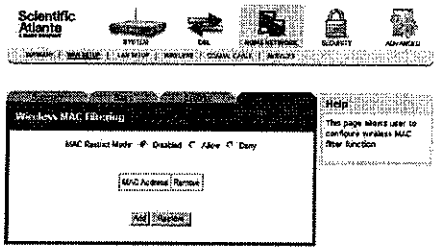
WEP Encryption Disabled



Wireless MAC Filter

The Wireless – MAC Filter screen allows you set filter schemes for the wireless access points.

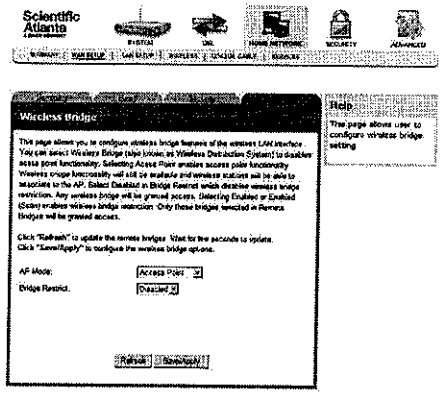
Path: Home Network>Wireless>Advanced>MAC Filter



Wireless Bridge

The Wireless – Bridge screen allows you to configure the wireless access point as a bridge.

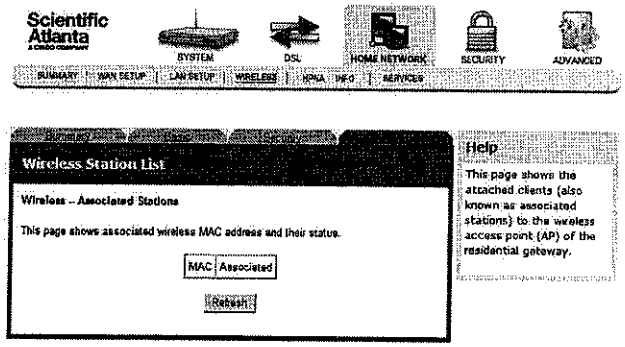
Path: Home Network>Wireless>Advanced>Wireless Bridge



Wireless Station List

This page shows the attached clients (also known as associated stations) to the wireless access point (AP) of the residential gateway.

Path: Home Network>Wireless>Advanced>Station Info

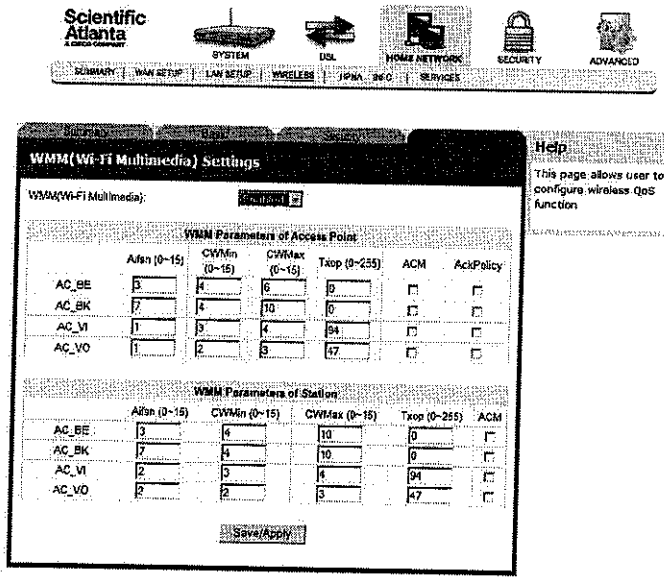


Wi-Fi Multimedia Settings

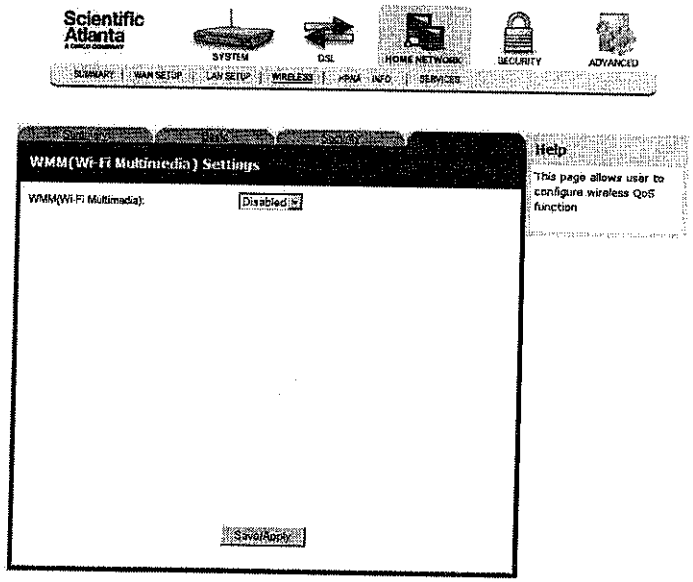
The WMM (Wi-Fi Multimedia) Settings screen allows you to congiure the WMM Parameters access point.

Path: Home Network>Wireless>Advanced>Wi-Fi Multimedia Settings

WMM (Wi-Fi Multimedia) Settings Enabled



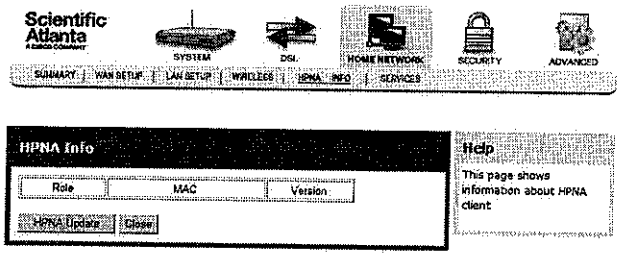
WMM (Wi-Fi Multimedia) Settings Disabled



HPNA Information

The HPNA Info screen allows you to...

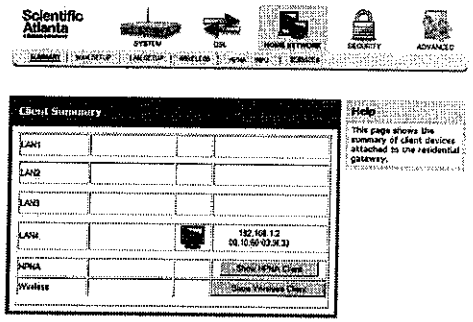
Path: Home Network>HPNA Info



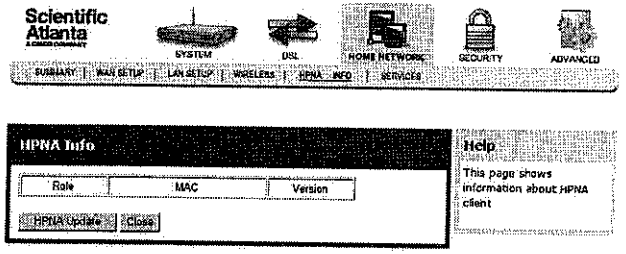
Updating HPNA Information

To update the HPNA information, complete the following steps.

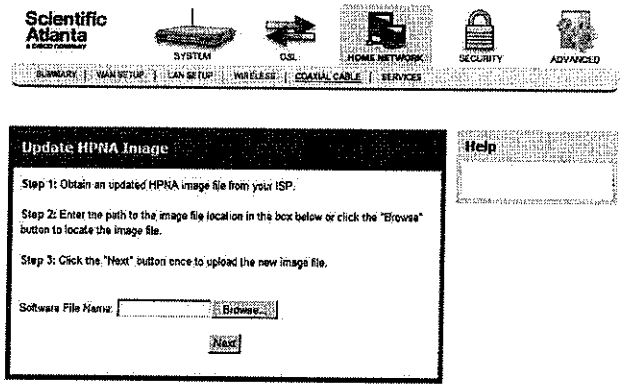
1 Click **Home Network** on the main screen. The Client Summary screen opens.



2 Click **HPNA Info**. The HPNA Info screen opens.

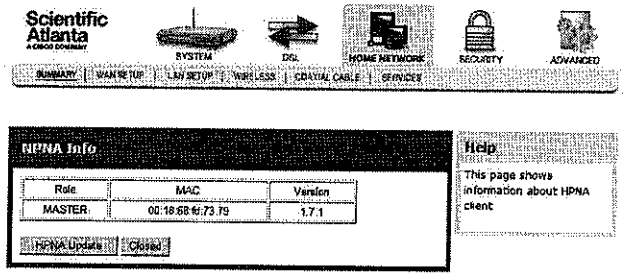


3 Click **HPNA Update** to to update the HPNA software of HPNA devices attached to the residential gateway The Update HPNA window opens.



4 In the Software File Name field, enter the name of the file that you want to use to update your system. You can click Browse to locate the file.

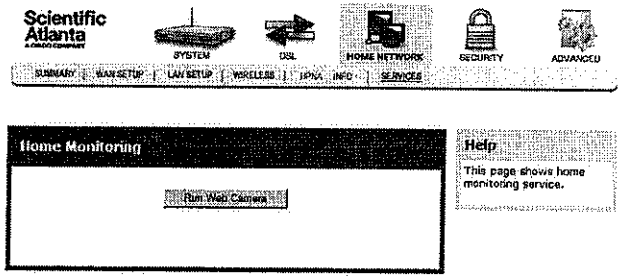
5 Click **Next**. The software for the attached HPNA devices is updated.



Home Monitoring

The Home Monitoring screen allows you to run a web camera to watch...

Path: Home Network>Services>



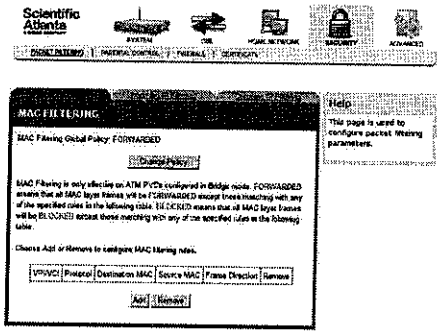
MAC Filtering Setup

The MAC Filtering Setup screen allows you to set up filters for packets containing configured MAC addresses. With the MAC Filtering feature you can restrict access to certain servers based on their MAC address. MAC Filtering is only effective on ATM PVCs configured in Bridge mode.

Path: Security>Packet Filtering>MAC Filtering

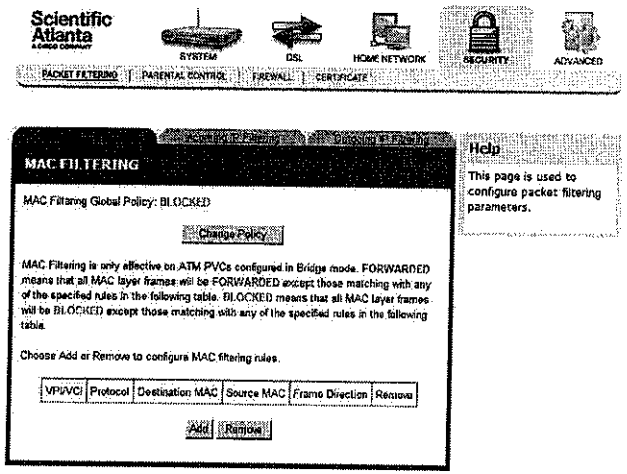
Forwarded MAC Filtering

FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table.



Blocked MAC Filtering

BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

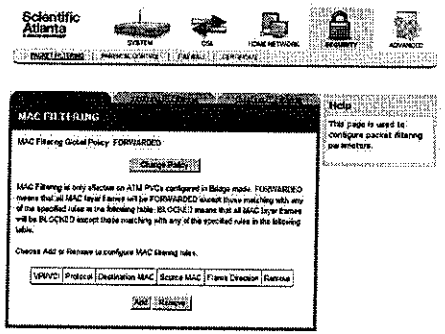


Adding MAC Filtering

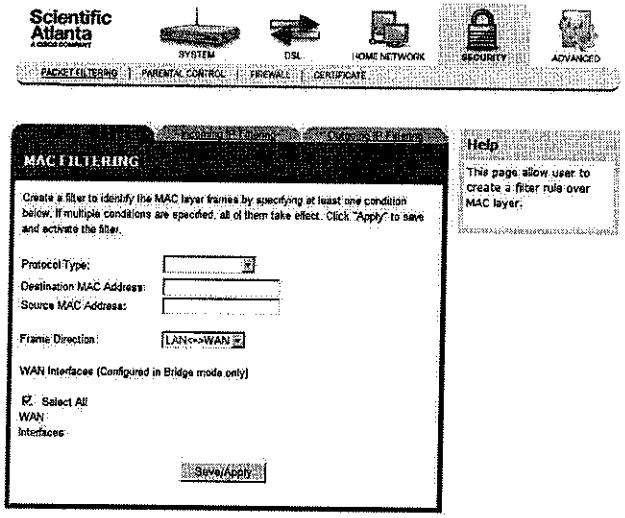
To add MAC Filtering, complete the following steps.

1 Click **Security** on the main screen. The Packet Filtering tab opens by default.

2 Click **MAC Filtering**. The MAC Filtering screen opens.



3 Click **Add** to open a blank MAC Filtering screen.



4 In the Protocol Type field, select one of the following protocols from the drop-down menu.
- PPPoE
- IPv4
- IPv6
- AppleTalk
- IPX
- NetBEUI
- IGMP

5 In the Destination MAC Address field, enter the frame's destination MAC address.

6 In the Source MAC Address field, enter the frame's source MAC address.

7 In the Frame Direction field, select one of the following choices from the drop-down menu:
- LAN<->WAN
- WAN<->LAN

8 Click Save/Apply to add the MAC Filter.

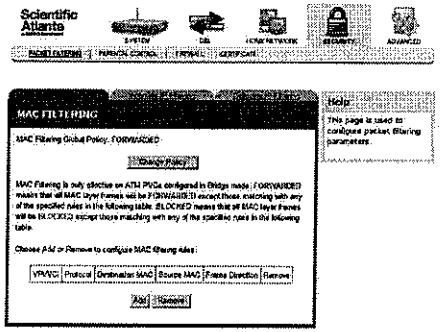
Forwarding or Blocking MAC Layer Frames

You can change the policy on how MAC layer frames are forwarded or blocked. FORWARDED means that all MAC layer frames will be forwarded except those matching with any of the specified rules in the table on the screen. BLOCKED means that all MAC layer frames will be blocked except those matching with any of the specified rules in the table on the screen.

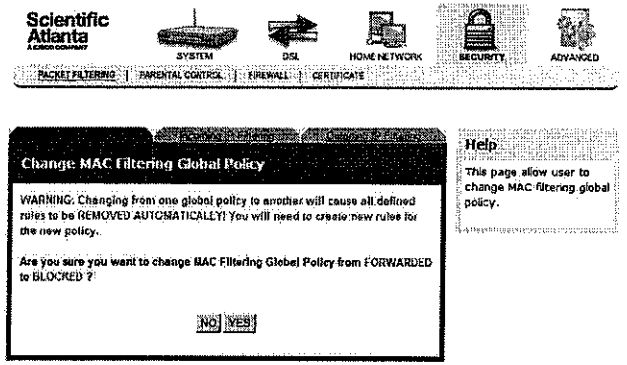
To change the policy on how MAC layer frames are forwarded or blocked, complete the following steps.

1 Click **Security** on the main screen. The Packet Filtering tab opens by default.

2 Click **MAC Filtering**. The MAC Filtering screen opens.



3 Click **Change Policy**. The Change MAC Filtering Global Policy screen opens. In this example, the global policy for MAC filtering is "Forwarded."



4 Do you want to change the Global Policy?

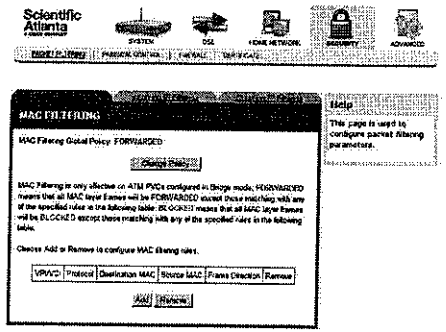
- If **yes**, click Yes. If the policy is forwarded, clicking Yes will change it to blocked and vise versa.
- If **no**, clock No and the policy will remain unchanged.

Removing MAC Filtering

To remove aMAC filtering rule you have set up, complete the following steps.

1 Click **Security** on the main screen. The Packet Filtering tab opens by default.

2 Click **MAC Filtering**. The MAC Filtering screen opens.



3 From the MAC Filtering screen, select **Remove** in the Remove column next to the MAC filtering rule you wish to remove.

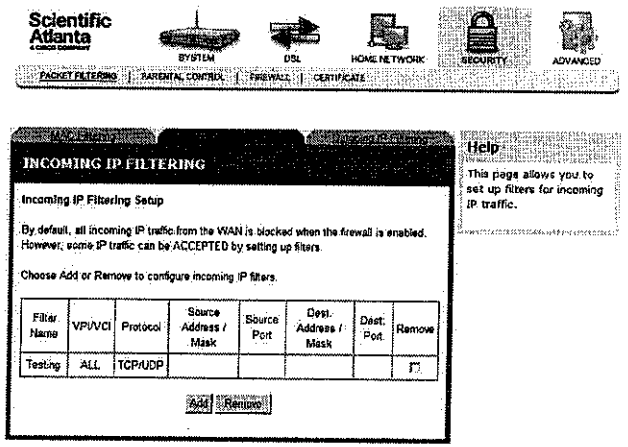
4 Click **Remove**.

5 Click **Change Policy**. The MAC filtering rule is removed.

Incoming IP Filtering

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be accepted by setting up filters.

Path: SECURITY>Incoming IP Filtering

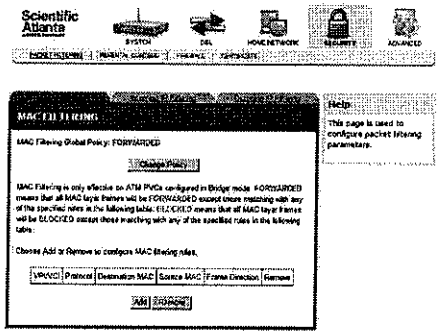


Adding an Incoming IP Filter

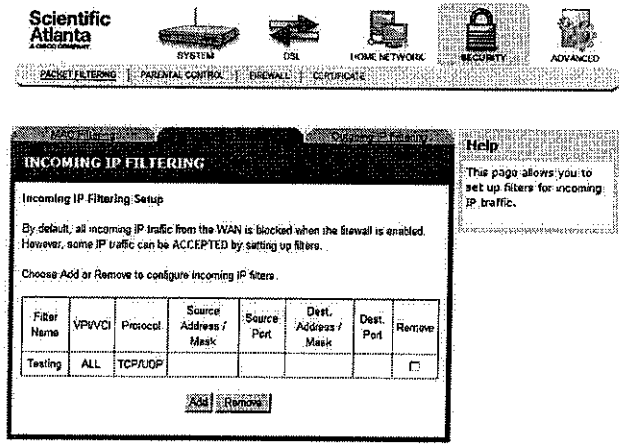
You can create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition for the filter. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.

To add an incoming IP filter, complete the following steps.

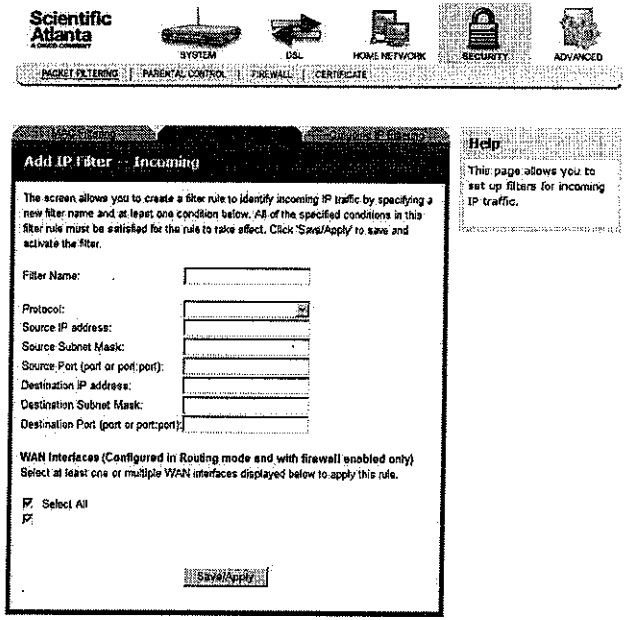
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



2 Select the Incoming IP Filtering tab. The Incoming IP Filtering screen opens.



3 Click **Add**. The Add IP Filter Incoming screen opens.



4 In the Filter Name field, enter the name of the filter.

5 In the Protocol field, select one of the following protocols:

- TCP/UDP
- TCP
- UDP
- ICMP

6 In the Source IP address field, enter the source IP address of the server sending the incoming packets.

7 In the Source Subnet Mask field, enter the subnet mask of the server sending the incoming packets.

8 In the Source Port field, enter the port number of the server sending the incoming packets. Use the following format: port or port:port You can enter one port or a range of ports (for example, 0:5 to indicate ports 0 through 5).

9 In the Destination IP address field, enter the destination IP address for the server receiving the packets.

10 In the Destination Subnet Mask field, enter the subnet mask for the server receiving the packets.

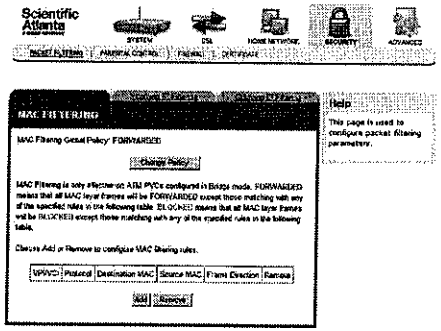
11 In the Destination Port field, enter the port number for the server receiving the packets. Use the following format: port or port:port You can enter one port or a range of ports (for example, 0:5 to indicate ports 0 through 5).

12 Click **Save/Apply** to add the filter.

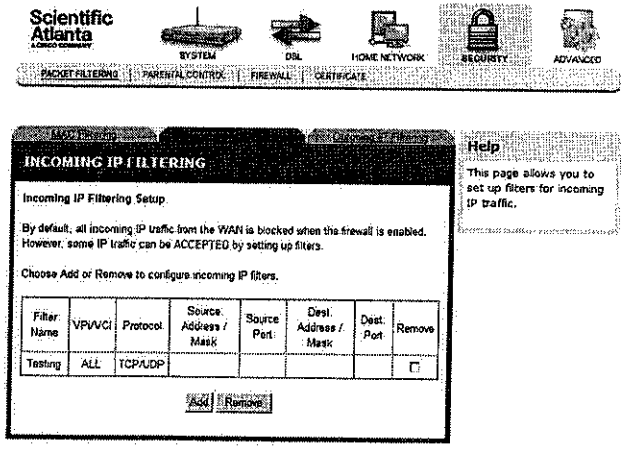
Removing an Incoming IP Filter

To remove an incoming IP filter, complete the following steps.

1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



2 Select the Incoming IP Filtering tab. The Incoming IP Filtering screen opens.



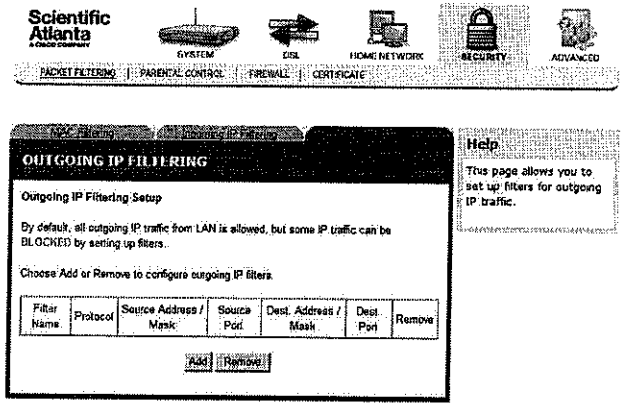
3 From the Incoming IP Filtering screen, select **Remove** in the Remove column next to the filter you wish to remove.

4 Click **Remove** to remove the filter.

Outgoing IP Filtering

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

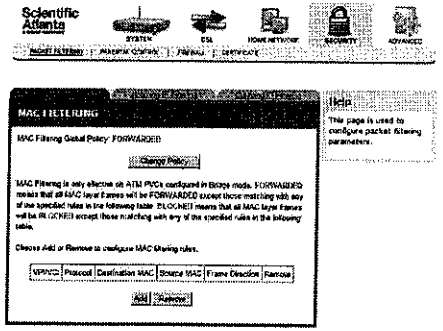
Path: SECURITY>Outcoming IP Filtering



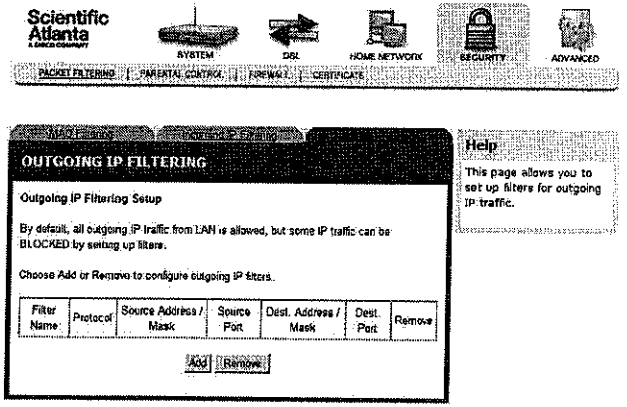
Adding an Outgoing IP Filter

To add an outgoing IP filter, complete the following steps.

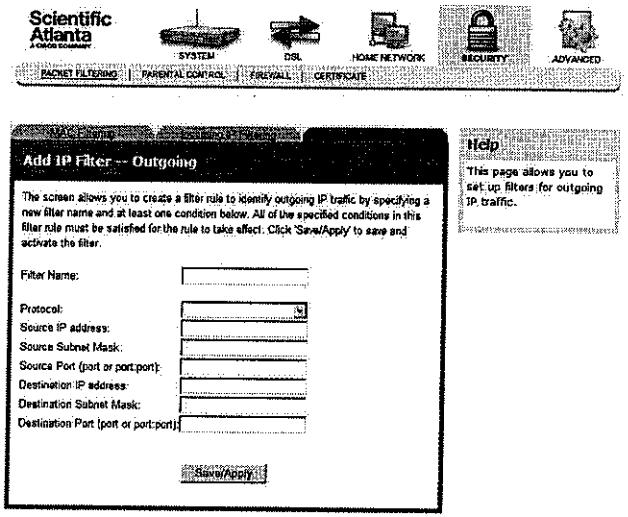
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



2 Select the Outgoing IP Filtering tab. The Outgoing IP Filtering screen opens.



3 Click **Add**. The Add IP Filter Outgoing screen opens.



4 In the Filter Name field, enter the name of the filter. The maximum character length is... You cannot use blank spaces in the filter name.

5 In the Protocol field, select one of the following protocols:

- TCP/UDP
- TCP
- UDP
- ICMP

6 In the Source IP address field, enter the source IP address for the server sending the incoming packets.

7 In the Source Subnet Mask field, enter the subnet mask for the for the server sending the incoming packets.

8 In the Source Port field, enter the port number for the server sending the incoming packets. Use the following format port or port:port.

9 In the Destination IP address field, enter the destination IP address for the server receiving the packets.

10 In the Destination Subnet Mask field, enter the subnet mask for the server receiving the packets.

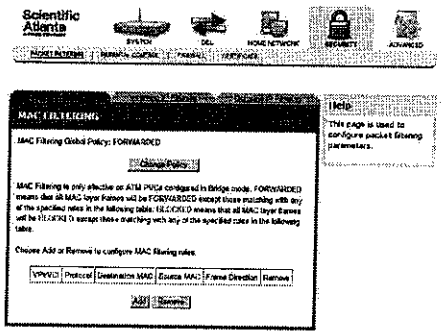
11 In the Destination Port field, enter the port number for the server receiving the packets. Use the following format port or port:port ????

12 Click **Save/Apply** to add the filter.

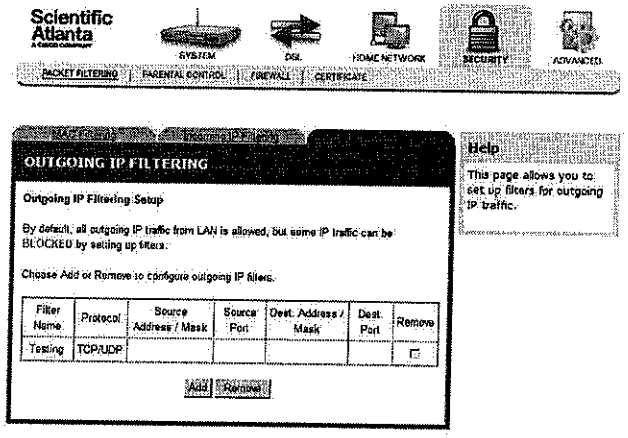
Removing an Outgoing IP Filter

To rmove an outgoing IP filter, complete the following steps.

1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



2 Select the Outgoing IP Filtering tab. The Outgoing IP Filtering screen opens.



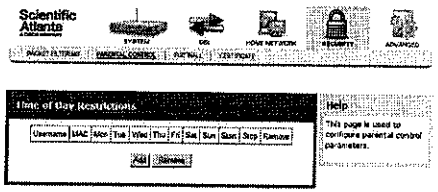
3 From the Outgoing IP Filtering screen, select **Remove** in the Remove column next to the filter you wish to remove.

4 Click **Remove** to remove the filter.

Parental Control Setup - Time of Day Restrictions

The Time of Day Restrictions screen allows you to block access to the Internet for certain times of the day. This screen adds time of day restriction to a special LAN device connected to the resiential gateway. The browser's MAC Address automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN devices, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to a command window and type ipconfig /all.

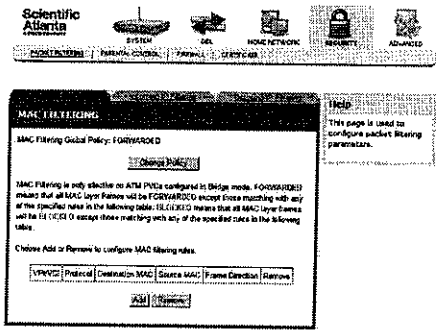
Path: Security>Parental Control



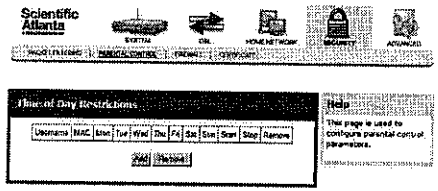
Adding Time of Day Restrictions

To add time of day restrictions, complete the following steps.

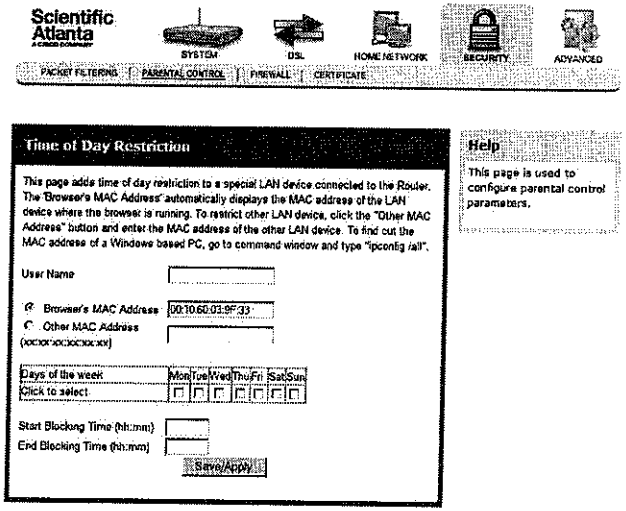
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



2 Click the Parental Control tab. The Time of Day Restrictions screen opens.



3 Click **Add**. The Time of Day Restriction screen opens.



4 In the User Name filed, enter the name for the time restriction.

5 Do you want to use the MAC address for the browser?

- If **yes**, click the Browser's MAC Address field and enter the MAC address of the LAN device where the browser is running.
- If **no**, click the Other MAC Address field and enter the MAC address of any other LAN device that you want to which you want to apply the time restrictions.

6 In the Days of the week area, click in the check boxes under each day where you want to set up time of day restrictions. For example, click in the Fri, Sat, and Sun check boxes.

7 In the Start Blocking Time field, enter the time when you want the time restriction to start. Use an hh:mm format.

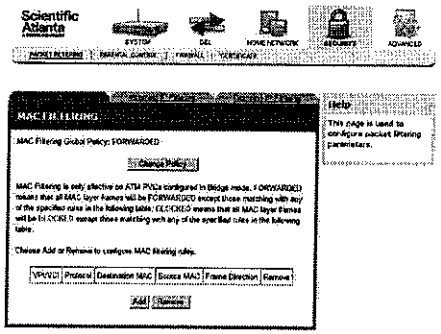
8 In the End Blocking Time field, enter the time when you want the time restriction to end. Use an hh:mm format.

9 Click **Save/Apply** to enable the time of day restrictions.

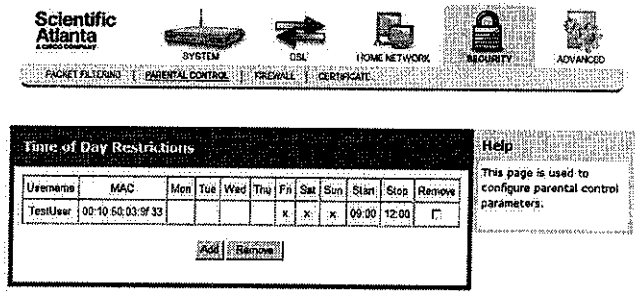
Removing Time of Day Restrictions

To remove time of day restrictions, complete the following steps.

1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



2 Click the Parental Control tab. The Time of Day Restrictions screen opens.



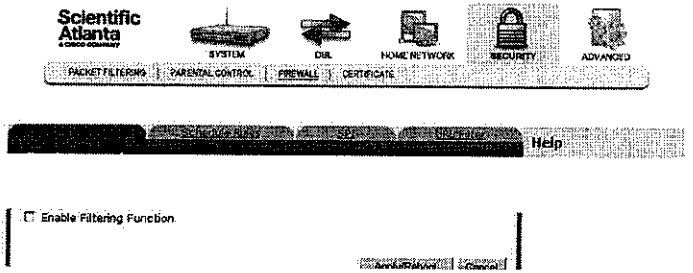
3 From the Time of Day Restrictions screen, select **Remove** in the Remove column next to the time of day restriction that you wish to remove.

4 Click **Remove** to remove the restriction.

Firewall Filtering Function

The Filterng Function sceen allwos you enable the filtering function for the firewall

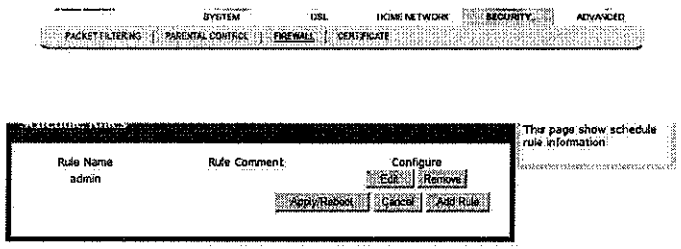
Path: Security>Firewall>PC Privileges



Schedule Rules

The Schedule Rules screen shows you the current rules set up for the firewall.

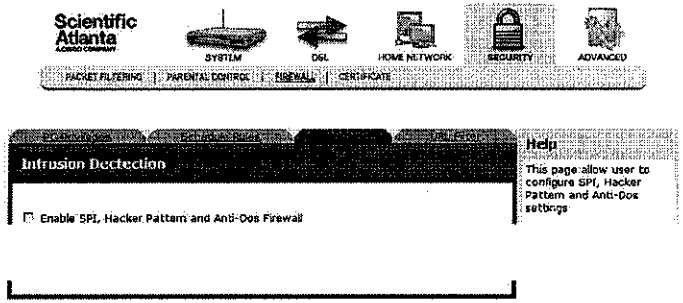
Path: Security>Firewall>Schedule Rules



Intrusion Detection

The Intrusion Detection screen allows you to configure the settings for detecting intruders to your residential gateway.

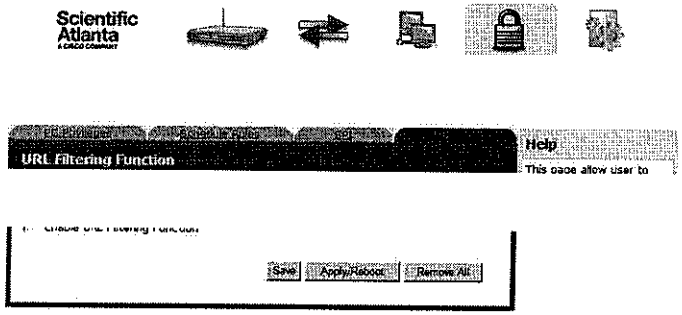
Path: Security>Firewall>SPI



URL Filtering Function

The URL Filtering Function screen allows you to configure the features for filtering URLs.

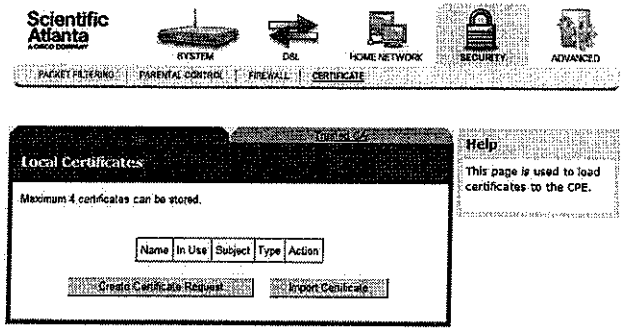
Path: Security>Firewall>URL Filter



Local Certificates

The Local Certificates screen allows you to load certificates onto the residential gateway. Local certificates are used by peers to verify your identity. A maximum of four certificates can be stored.

Path: Security>Certificate>Local

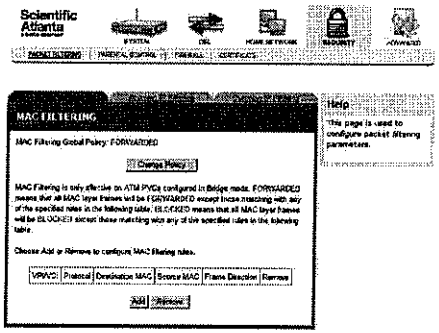


Creating Certificates

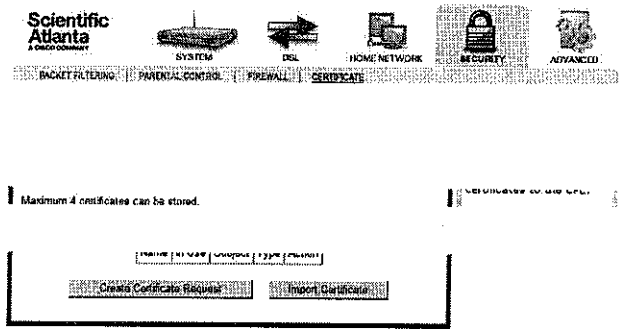
The Create Certificate screen allows you to generate a certificate by specifying certificate parameters shown in this screen.

To create a certificate, complete the following steps.

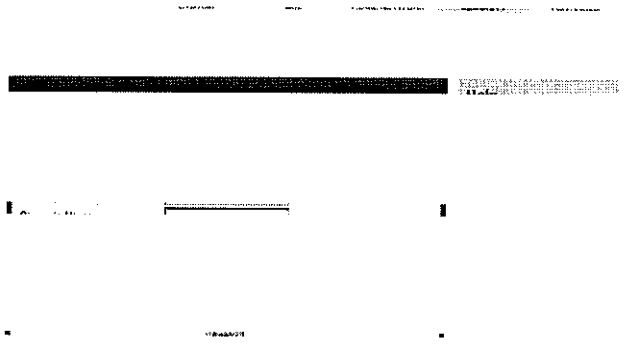
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



2 Click **Certificate.** The Local Certificates screen opens.



3 Click **Create Certificate Request.** The Create new certificate request screen opens.



4 In the Certificate Name field, enter the name for the certificate.

5 In the Common name field, enter the common name of certificate.

6 In the Organization field, enter the name of the organization that owns the certificate.

7 In the State/Province field, enter the state or province where you want to register the certificate.

8 In the Country/Region Name, use the drop-down list to select the country or region where you want to register the certificate.

9 Click **Apply** to create the certificate. The certificate signing request screen opens.

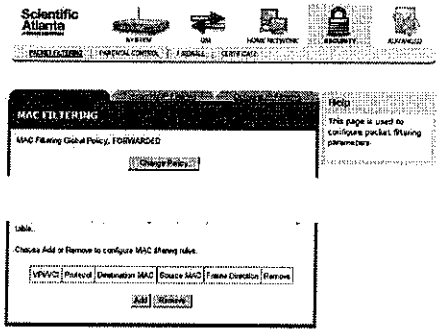
10 Click **Load Signed Certificate** to save the certificate on the residential gateway.

Importing Local Certificates

The Import Certificate screen allows you to import a pre-existing certificate to the residential gateway.

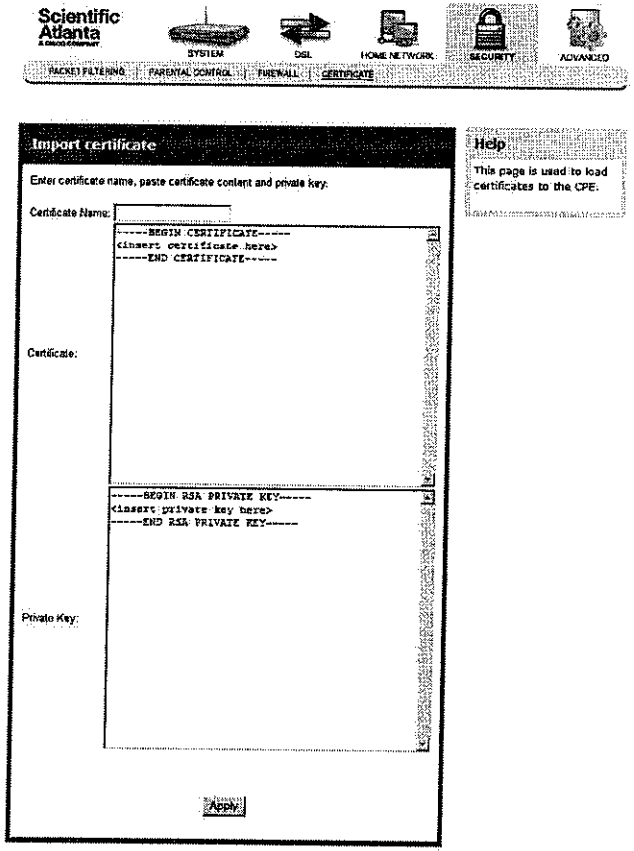
To import a certificate, complete the following steps.

1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



2 Click **Certificate.** The Local Certificates screen opens.

3 Click **Import Certificate.** The Import certificate screen opens.



4 In the Certificate Name field, enter the name of the certificate.

5 In the Certificate area, copy and paste the contents of the certificate file provided by the service provider.

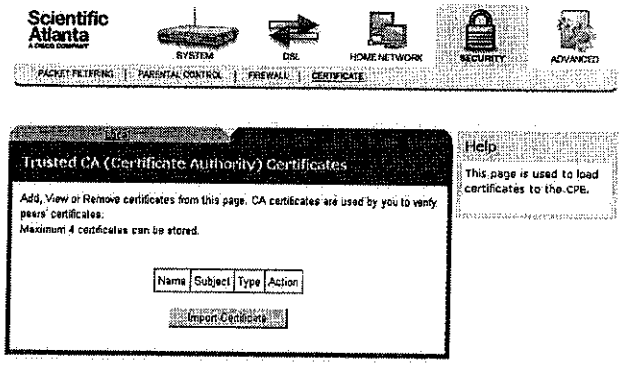
6 In the Private Key area, copy and paste the private key from the certificate file provided by the service provider.

7 Click **Apply** to save the certificate on the residential gateway.

Trusted CA Certificates

The allows you to load certificates onto the residential gateway. You can use CA certificates to verify peers' certificates. A maximum of four certificates can be stored.

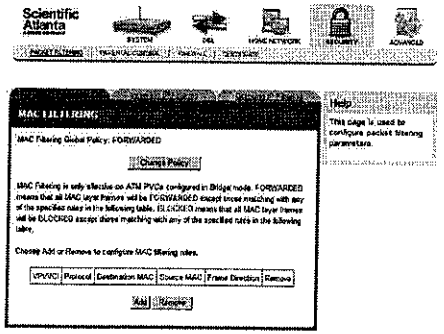
Path: Security>Certificate>Trusted CA



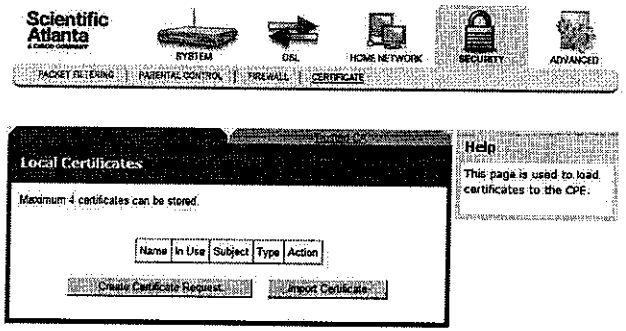
Importing Trusted CA Certificates

The Import CA certificate screen allows you to import a pre-existing trusted CA certificate to the residential gateway..

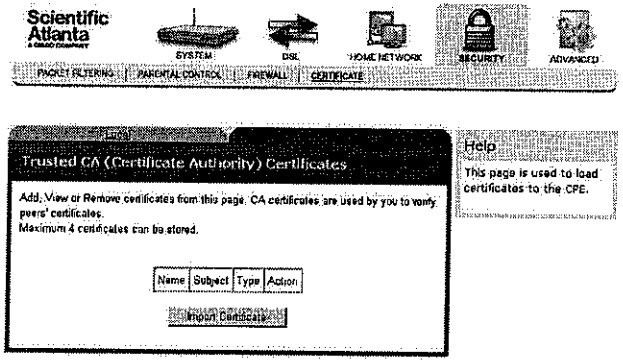
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



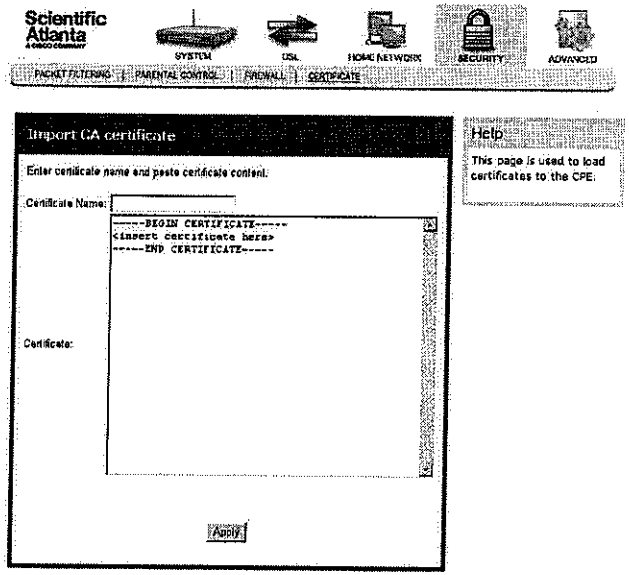
2 Click **Certificate**. The Local Certificates screen opens.



3 Click **Trusted CA**. The Trusted CA (Certificate Authority) Certificates screen opens.

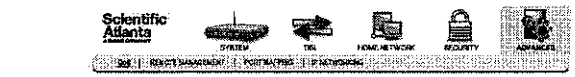


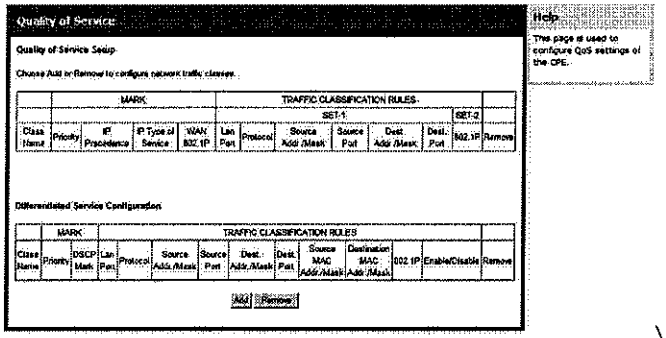
4 Click **Import Certificate**. The Import CA Certificate screen opens.



Quality of Service

The Quality of Service screen allows you to configure the Quality of Service (QoS) settings for the residential gateway.

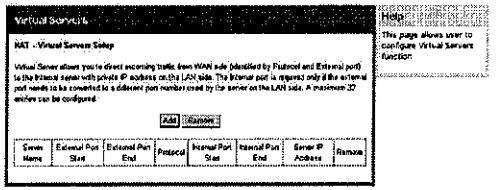




Virtual Servers Setup

The NAT -- Virtual Servers Setup screen allows you to configure servers to which you want to forward IP packets that belong to a specific service.

Path: Home Network>Services>Virtual Servers

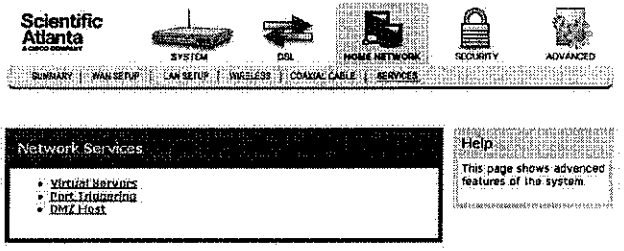


Adding a Virtual Server

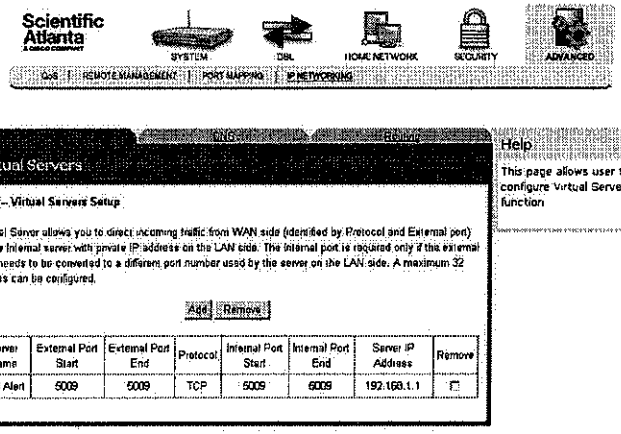
To add and configure a virtual server, complete the following steps.

1 Click **Home Network** on the main screen.

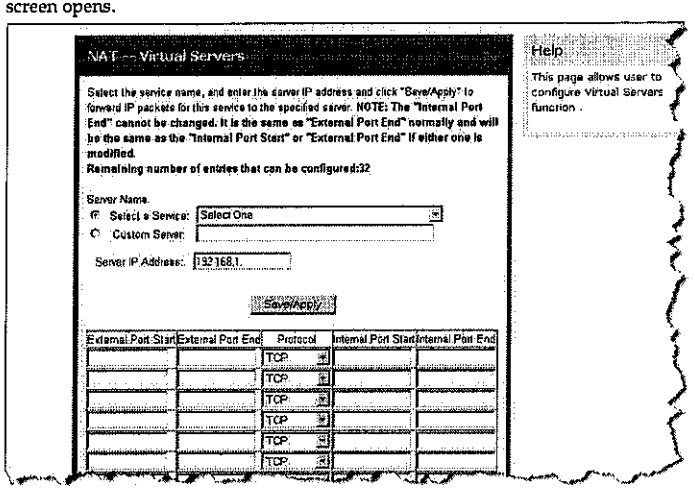
2 Click **Services**. The Network Services screen opens.



3 Click **Virtual Servers**.The Virtual Servers Setup screen opens.



4 From the Virtual Servers Setup screen, click **Add**. The NAT Virtual Servers screen opens.



5 Under Server Name, do one of the following:

- Click Select a Service, and choose a service from the drop-down list.
- Click Custom Server, and enter a name and the Server IP Address.

6 Under Protocol, select **TCP** or **UDP**.

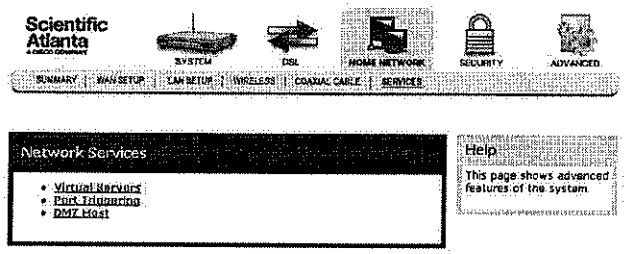
7 Click **Save/Apply** to add the virtual server.

Removing a Virtual Server

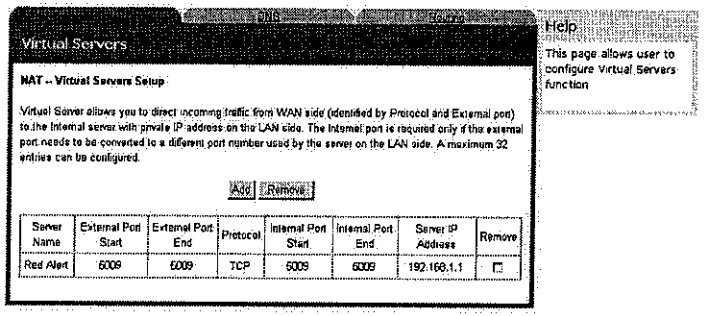
To remove a virtual server, complete the following steps.

1 Click **Home Network** on the main screen.

2 Click **Services**. The Network Services screen opens.



3 Click **Virtual Servers**.The Virtual Servers Setup screen opens.



4 From the NAT Virtual Servers Setup screen, select **Remove** in the Remove column next to the server you wish to remove.

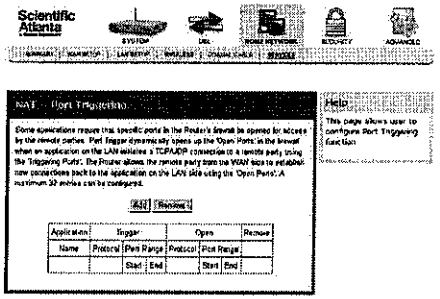
5 Click **Remove** to remove the NAT Virtual Server.

Port Triggering Setup

Some applications require that specific ports in the router's firewall be opened for access by the remote parties. The Port Triggering feature dynamically opens up the "Open Ports" in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the Triggering Ports feature. The router allows the remote party from the WAN side to establish new connections with the application on the LAN side using the open ports. A maximum 32 entries can be configured.

The NAT -- Virtual Servers Setup screen allows you to configure servers to which you want to forward IP packets that belong to a specific service.

Path: Home Network>Services>Port Triggering

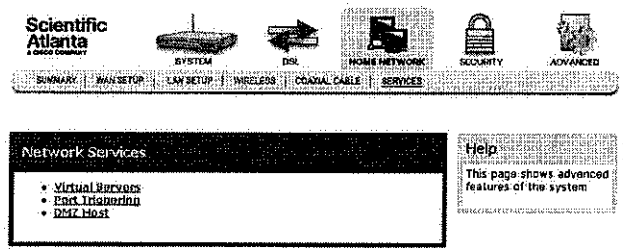


Opening a Port on the Firewall

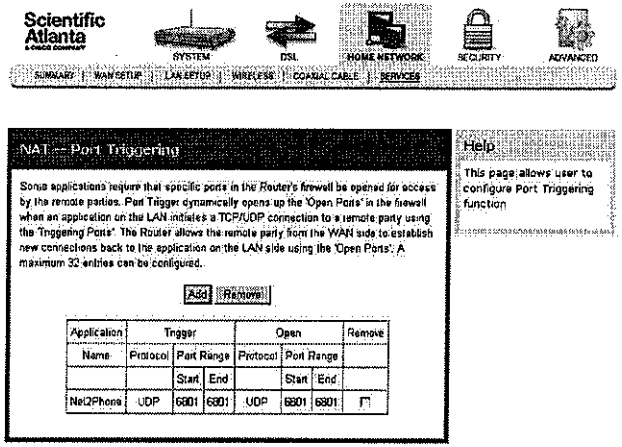
To open a port on the firewall, complete the following steps.

1 Click **Home Network** on the main screen.

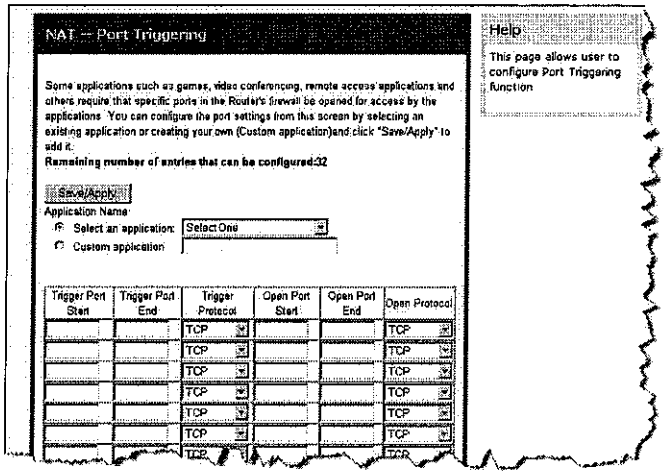
2 Click **Services.** The Network Services screen opens.



3 Click **Port Triggering.** The NAT Port Triggering screen opens.



4 From the NAT Port Triggering screen, click **Add.** The NAT Port Triggering screen opens with a list of available protocols.



5 Under Application Name, do one of the following:

- Click Select an Application and choose an application from the drop-down list.

  OR

- Click Custom Application, and enter a name for the application.

6 Complete the fields on the screen as follows:

- Under Trigger Port Start, enter the time that you want to open the trigger port on the firewall.
- Under Trigger Port End, enter the time that you want to close the trigger port on the firewall.
- Under Trigger Protocol, select **TCP/UDP, TCP** or **UDP.**
- Under Open Port Start, enter the starting port number for the ports that you want to open on the firewall.
- Under Open Port End, enter the ending port number for the ports that you want to open on the firewall.
- Under Open Protocol, select **TCP/UDP, TCP** or **UDP.**

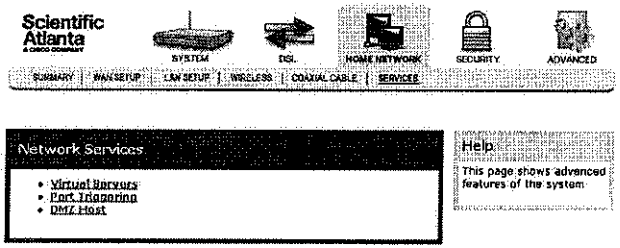
7 Click **Save/Apply** to open the ports on the firewall.

Closing a Port on the Firewall

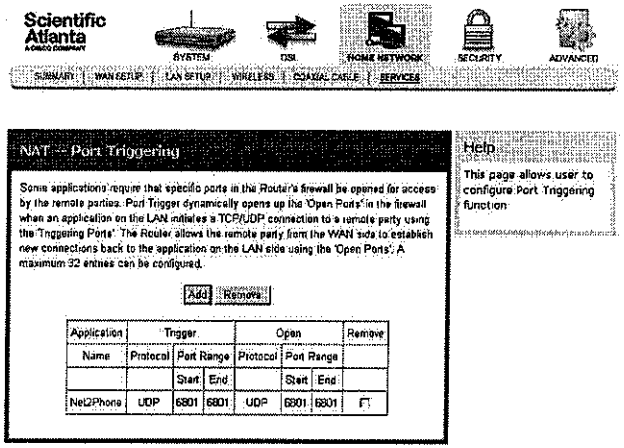
To close a port on the firewall, complete the following steps.

1 Click **Home Network** on the main screen.

2 Click **Services**. The Network Services screen opens.



3 Click **Port Triggering**. The NAT Port Triggering screen opens.



4 From the NAT Port Triggering screen, click **Remove** in the Remove column next to the port you wish to close.

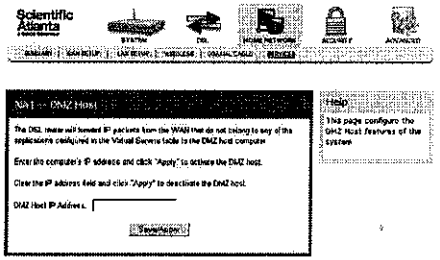
5 Click **Remove**. The port you selected is closed.

DMZ Host Setup

The NAT -- DMZ Host screen allows the IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to be forwarded to the DMZ (demilitarized zone) host computer.

Path: Home Network>Services>DMZ Host

Q. to reviewers: Need to clarify the information for this screen.



Activate the DMZ Host

Enter the computer's IP address and click Apply to activate the DMZ host.

Deactivate the DMZ Host

Clear the IP address field and click Apply to deactivate the DMZ host.

Scientific Atlanta
A CISCO COMPANY

Scientific Atlanta, A Cisco Company
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

770.236.5000
www.scientificatlanta.com

Printed in United States of America
April 2007
Part Number 4002550 Rev A