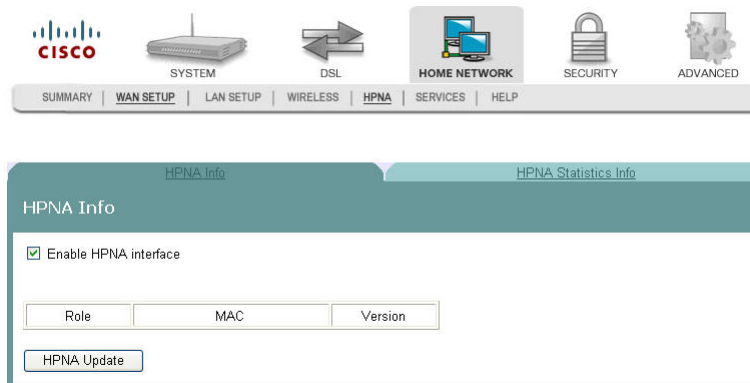


- Click **Show HPNA Client**. After processing, the HPNA Info screen opens. This screen shows the role, MAC Address, and the version of HPNA.



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



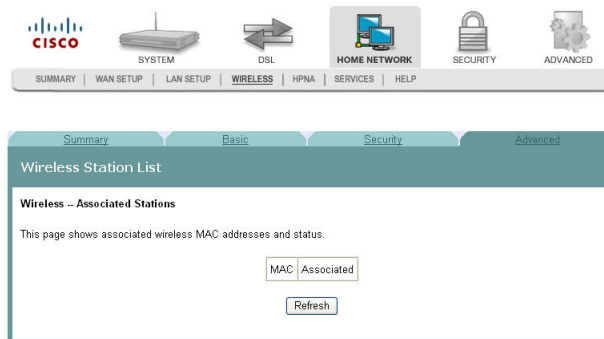
- In the Software File Name field, enter the name of the file that you want to use to update your system. You can click Browse to locate the file.
- Click **Next** and wait for the software for the attached HPNA devices to be updated.

Wireless Station List

This page shows the attached clients (also known as associated stations) to the wireless access point (AP) of the residential gateway. At this time, there is no limit to the number of simultaneously attached devices.

Chapter 5 Home Network Configuration

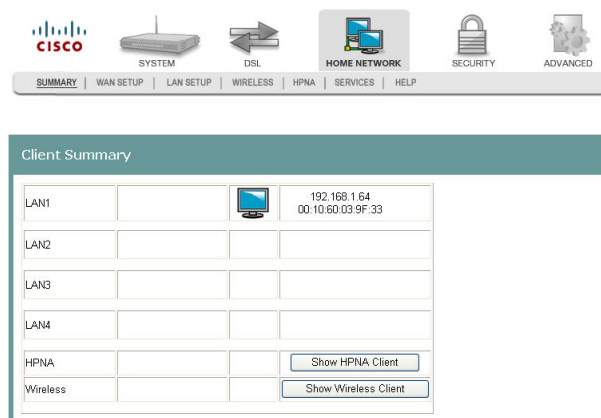
Path: Home Network > Summary > Show Wireless Client



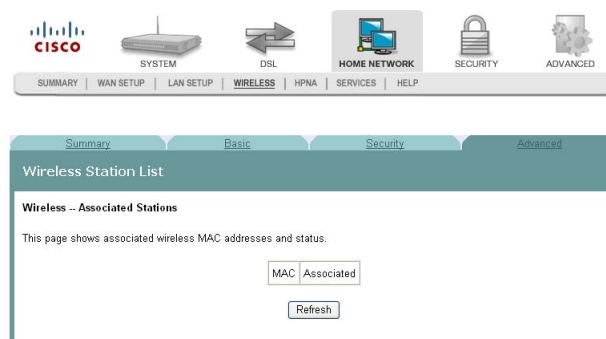
Showing Attached Clients

To show the attached clients to the wireless access point of the residential gateway, complete the following steps.

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



- 3 Click **Show Wireless Client**. The Wireless Station List screen opens. If you have a wireless client attached to the residential gateway, the screen displays the MAC Address of the client and whether the client is associated with the residential gateway.



- 4 Click **Refresh** to update the list of attached clients.

WAN Quick Setup

The WAN Quick Setup screen allows you to set up wide area network (WAN) connections and settings, such as virtual channel identifiers (VCI), virtual path identifiers (VPI), and quality of service (QoS).

Path: Home Network > WAN Setup > WAN Quick Setup



WAN Quick Setup

Wide Area Network (WAN) Setup

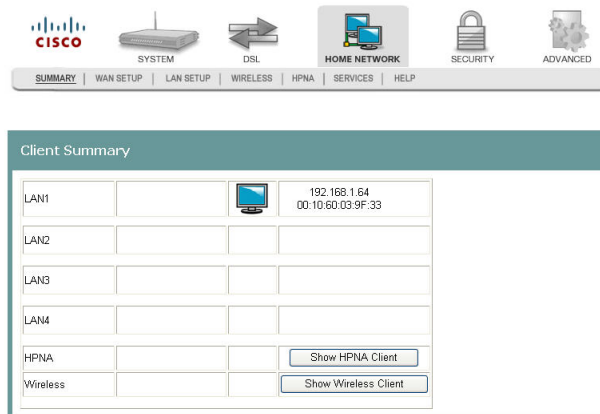
Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Category	Service	Interface	Protocol	IGMP	QoS	State	Remove	Edit
<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Reboot"/>										

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.



Chapter 5 Home Network Configuration

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

WAN Quick Setup

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Category	Service	Interface	Protocol	IGMP	QoS	State	Remove	Edit
--------------	----------	----------	---------	-----------	----------	------	-----	-------	--------	------

Add Remove Reboot

- 3 Click Add to configure a new WAN interface, or click Edit to edit an existing WAN interface.

The screenshot shows the WAN Setup configuration page. The navigation bar at the top includes: SUMMARY, WAN SETUP (selected), LAN SETUP, WIRELESS, and HPNA. The main content area is titled 'WAN Setup' and contains the following fields and options:

- Broadband Type: DSL (dropdown)
- DSL mode: ATM (dropdown)
- Broadband Connect Type: PPP over Ethernet (PPPoE) (dropdown)
- Encapsulation Mode: LLC/SNAP-BRIDGING (dropdown)
- VPI: 0, VCI: 36 (input fields)
- Service Category: UBR Without PCR (dropdown)
- VLAN Mux - Enable Multiple Protocols Over a Single PVC
- Enable Quality Of Service
- PPP Username: test (text input)
- PPP Password: •••• (password input)
- PPPoE Service Name: (text input)
- Authentication Method: AUTO (dropdown)
- Dial on demand (with idle timeout timer)
- PPP IP extension
- Use Static IP Address
- Retry PPP password on authentication error
- Enable PPP Debug Mode
- Bridge PPPoE Frames Between WAN and Local Ports
- Enable IGMP Multicast:
- Enable WAN Service:
- Save (button)

- 4 In the Broadband Type field, select **DSL**.
- 5 In the DSL Mode field, select **ATM**. More fields populate on the screen.
- 6 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.
- In the Broadband Connect Type field, select **PPP over Ethernet (PPPoE)**.
 - In the Encapsulation Mode field, select **LLC/SNAP - Bridging**.

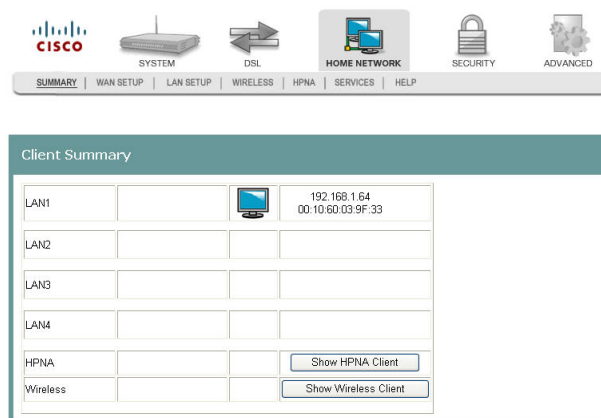
Chapter 5 Home Network Configuration

- c Check the **VLAN Mux - Enable Multiple Protocols Over a Single PVC** check box, if applicable.
 - d In the PPP Username: field, enter the user name for the point-to-point protocol.
 - e In the PPP Password: field, enter the password for the point-to-point protocol.
 - f In the PPPoE Service Name: field, enter the name for the point-to-point over Ethernet service.
 - g In the VPI field, enter the virtual path identifier (VPI). Values are: 0 to 65535.
 - h In the VCI field, enter the virtual channel identifier (VCI). Values are: 0 to 65535.
 - i In the Service Category field, select **ABRI Without PCR**.
 - j Check the 'Enable Quality of Service' check box if applicable
 - k In the Authentication Method field, select **AUTO**.
 - l Check **Enable NAT**.
 - m Check the **Enable IGMP Multicast** check box, if applicable
 - n Check the **Enable WAN Service** check box
- 7 Click **Save** to save your settings.
- 8 Click **Reboot**. This action reboots the residential gateway so that the WAN setup configuration takes effect.

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.

WAN Quick Setup

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Category	Service	Interface	Protocol	IGMP	QoS	State	Remove	Edit
--------------	----------	----------	---------	-----------	----------	------	-----	-------	--------	------

Add Remove Reboot

Chapter 5 Home Network Configuration

- Click **Add** to add a new WAN interface, or click **Edit** to modify an existing WAN interface.

The screenshot shows the WAN Setup configuration page in the Cisco Home Network Configuration Wizard. The navigation bar at the top includes: CISCO, SYSTEM, DSL, HOME NETWORK (selected), SECURITY, and ADVANCED. Below the navigation bar are tabs for SUMMARY, WAN SETUP (selected), LAN SETUP, WIRELESS, and HPNA. The main content area is titled "WAN Setup" and contains the following fields and options:

- Broadband Type: DSL (dropdown)
- DSL mode: ATM (dropdown)
- Broadband Connect Type: MAC Encapsulation Routing (MER) (dropdown)
- Encapsulation Mode: LLC/SNAP-BRIDGING (dropdown)
- VLAN Mux - Enable Multiple Protocols Over a Single PVC
- Service Category: UBR Without PCR (dropdown)
- VPI: 0 (text box)
- VC1: 35 (text box)
- Enable Quality Of Service
- Obtain IP address automatically
- Use the following IP address:
 - WAN IP Address: (text box)
 - WAN Subnet Mask: (text box)
- Obtain default gateway automatically
- Use the following default gateway:
 - Use IP Address: (text box)
 - Use WAN Interface: (dropdown)
- Obtain DNS server addresses automatically
- Use the following DNS server addresses:
 - Primary DNS server: (text box)
 - Secondary DNS server: (text box)
- Enable NAT
- Enable Fullcone NAT
- Enable IGMP Multicast
- Enable WAN Service
- Save (button)

- In the Broadband Type field, enter **DSL**.
- In the DSL Mode field, select **ATM**. More fields populate on the screen.
- 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 Select the **VLAN Mux - Enable Multiple Protocols Over a Single PVC** check box, if applicable.
 - d In the VLAN ID[0-4095]: field, enter an ID for the VLAN. Values are: 0 to 4095.
 - e In the VPI field, enter the virtual path identifier (VPI). Values are: 0 to 65535.
 - f In the VCI field, enter the virtual channel identifier (VCI). Values are: 0 to 65535.
 - g In the Service Category field, select **UBR Without PCR**.
 - h Select the **Enable Quality of Service** check box, if applicable.
 - i Select the **Obtain an IP address automatically** option.
 - j Select the **Obtain default gateway automatically** option.
 - k Select the **Obtain DNS server addresses automatically** option.
 - l Select **Enable NAT**.
 - m Select the **Enable IGMP Multicast** check box.
 - n Select the **Enable WAN Service** check box.
- 7 Click **Save**. The system returns to the previous screen.
- 8 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 Multicast Protocol (IGMP), and Universal Plug and Play (UPnP).

Path: Home Network > LAN Setup

The screenshot shows the 'LAN Setup' configuration page. At the top, there is a navigation bar with icons for CISCO, SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below this is a sub-menu with 'LAN SETUP' selected. The main content area is titled 'Local Area Network (LAN) Setup' and includes a 'Help...' link. The instructions state: 'Configure the DSL Residential Gateway IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the residential gateway to make the new configuration effective.'

Configuration fields include:

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0
- Enable UPnP
- Disable DHCP Server
- Enable DHCP Server
 - Start IP Address: 192.168.1.64
 - End IP Address: 192.168.1.253
 - Subnet Mask: 255.255.255.0
 - Leased Time (hour): 24

Buttons at the bottom are 'Save' and 'Save/Reboot'.

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.

The screenshot shows the 'Client Summary' screen. At the top, there is a navigation bar with icons for CISCO, SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below this is a sub-menu with 'LAN SETUP' selected and 'HOME NETWORK' highlighted. The main content area is titled 'Client Summary' and contains a table of network interfaces.

LAN1			192.168.1.64 00:10:60:03:9F:33
LAN2			
LAN3			
LAN4			
HPNA			Show HPNA Client
Wireless			Show Wireless Client

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

The screenshot shows the Cisco Home Network Setup interface. At the top, there are navigation tabs: SUMMARY, WAN SETUP, LAN SETUP (selected), WIRELESS, and HPNA. Above these tabs are icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. The main content area is titled 'Local Area Network (LAN) Setup' and includes a 'Help...' link. Below the title, there is a paragraph of instructions: 'Configure the DSL Residential Gateway IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the residential gateway to make the new configuration effective.' The form contains the following fields and options:

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0
- Enable UPnP
- Disable DHCP Server
- Enable DHCP Server
 - Start IP Address: 192.168.1.64
 - End IP Address: 192.168.1.253
 - Subnet Mask: 255.255.255.0
 - Leased Time (hour): 24

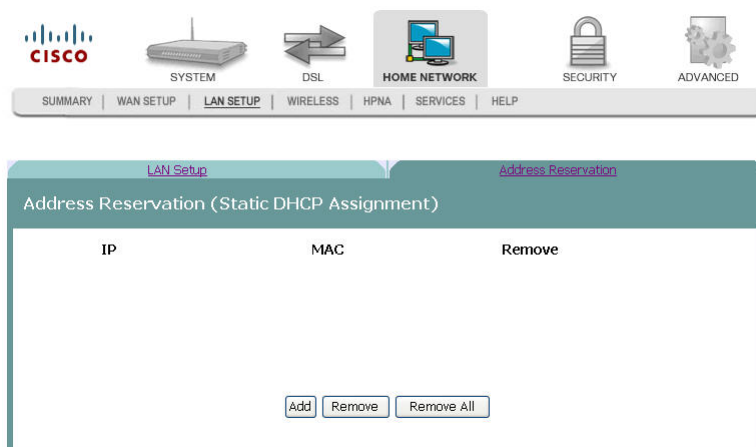
At the bottom of the form, there are two buttons: 'Save' and 'Save/Reboot'.

- 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 UpnP?
 - If **yes**, check the Enable UPnP check-box.
 - If **no**, clear the Enable UPnP check-box.
- 6 Do you want to Enable the DHCP server?
 - If **yes**, select Enable DHCP Server, and go to step 7.
 - If **no**, select Disable DHCP Server, and go to step 8.
- 7 Under Enable DHCP server, enter the following information:
 - a In the Start IP Address field, enter the first IP address in the range for the DHCP IP address lease pool.
 - b In the End IP Address field, enter the last IP address in the range for the DHCP IP address lease pool.
 - c In the Subnet Mask field, enter the subnet mask for the DHCP server.
 - d In the Leased Time (hour) field, enter the duration of the DHCP lease address.
- 8 Click **Save** to save the changes or click **Save/Reboot** to save the changes and reboot the residential gateway.

Reserving IP Addresses

The Address Reservation screen allows you to reserve IP addresses for specific devices. For example, you can reserve IP addresses for your laptop or PC in your home.

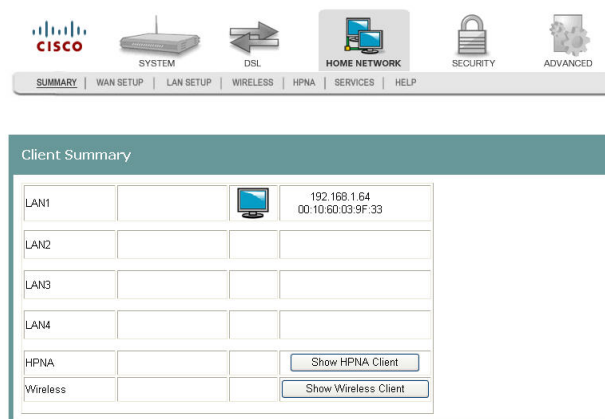
Path: Home Network > LAN Setup > Address Reservation



Reserving IP Addresses

To reserve a specific IP address for a specific MAC address, complete the following steps.

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



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

LAN Setup | Address Reservation

Local Area Network (LAN) Setup

Configure the DSL Residential Gateway IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the residential gateway to make the new configuration effective.

IP Address:
 Subnet Mask:

Enable UPnP

Disable DHCP Server

Enable DHCP Server

Start IP Address:
 End IP Address:
 Subnet Mask:
 Leased Time (hour):

- Click **Address Reservation**. The Reserve Specific IP Addresses for Specific MAC Addresses screen opens.

LAN Setup | Address Reservation

Reserve Specific IP Addresses for Specific MAC Addresses

Static DHCP Client List

Assign this IP : . . .

To this MAC : : : : : :

- In the Assign this IP field, enter the IP address you want to assign to the MAC address.
- In the To this MAC field, enter the MAC address to which you want to assign the IP address.
- Click **Save** to save your settings.

Wireless Summary

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

Path: Home Network > Wireless > Summary

Wireless Summary	
MAC Address	00:1E:6B:FA:9C:D8
SSID	Cisco
Authentication	open
Encryption	WEP Encryption:disabled

Wireless Basic

The Wireless -- Basic screen allows you to configure the basic features of the wireless LAN interface. You can enable or disable the LAN interface, hide the network from active scans, enter a name for the wireless network, and restrict the channel set based on country requirements.

Path: Home Network > Wireless > Basic

The screenshot shows the Cisco Wireless Basic configuration page. The navigation bar includes tabs for Summary, Basic, Security, Advanced, and Wi-Fi Protected Setup. The Basic tab is selected, showing the following configuration options:

- Enable Wireless
- Hide Access Point
- SSID: Cisco
- Channel: Auto
- BSSID: 00:18:68:FF:61:6B
- Wireless Mode: 802.11g & 802.11b
- 54g Protection: Auto
- Enable WMM

A Save/Apply button is located at the bottom right of the configuration area.

Enabling the Wireless Network

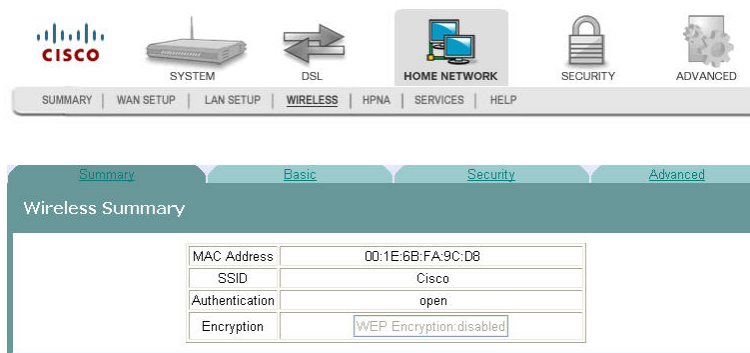
To enable the wireless network, complete the following steps.

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

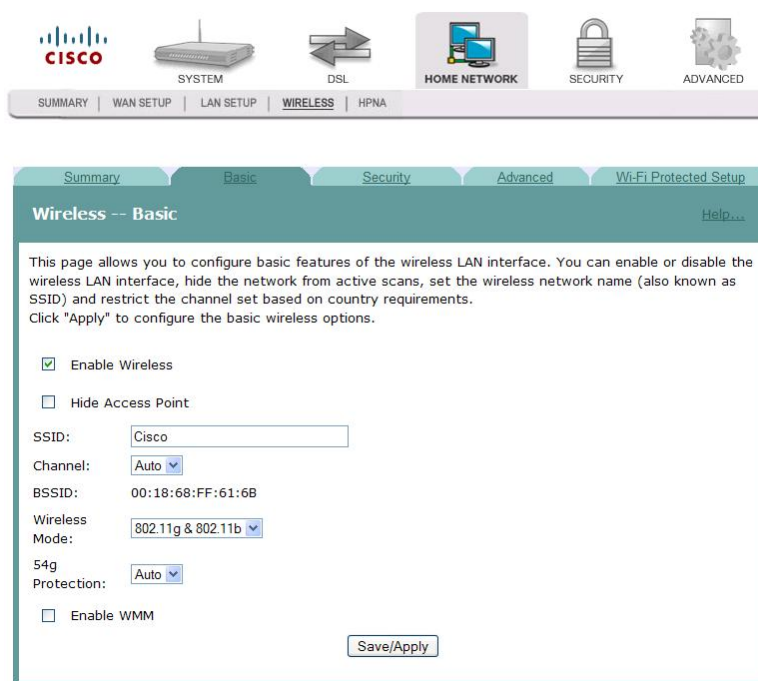
The screenshot shows the Client Summary screen. The navigation bar includes tabs for SUMMARY, WAN SETUP, LAN SETUP, WIRELESS, HPNA, SERVICES, and HELP. The WIRELESS tab is selected, showing the Client Summary screen. The screen displays a table of network interfaces and their status:

LAN1			192.168.1.64 00:10:60:03:9F:33
LAN2			
LAN3			
LAN4			
HPNA			Show HPNA Client
Wireless			Show Wireless Client

- Click **Wireless**. The Wireless Summary screen opens.



- Click **Basic**. The Wireless Basic screen opens.



- Check the **Enable Wireless** check box to enable the wireless network. The screen populates with additional fields.
- Do you want to prevent other wireless clients from communicating with the wireless access point (AP) of the residential gateway?
 - If **yes**, check the **Hide Access Point** check box. This feature prevents any other wireless client from communicating with the access point of the residential gateway (or disables the wireless connection).
 - If **no**, uncheck the **Hide Access Point** check box.
- In the SSID field, enter the Service Set Identifier (SSID).
- From the Channel drop-down list, select Auto or a channel from 1 to 11.
- In the Wireless Mode field, select the wireless mode from the drop-down list:
 - 802.11g & 802.11b - Allows you to mix Wireless-B with Wireless-G equipment, but you will lose the higher performance speeds of Wireless-G.

- 802.11g only - Features the same benefits as Wireless-B, but offers 5 times the speed at up to 54 Mbps. Wireless-G currently offers the best combination of performance and value. You can mix Wireless-B with Wireless-G equipment, but you will lose the higher performance speeds of Wireless-G.
 - 802.11b only - Operates on the 2.4GHz frequency band and can transmit data at speeds of up to 11 Mbps within a range of up to 100-150 feet. Wireless range can be affected by reflective or signal-blocking obstacles, such as mirrors, walls, devices and location, whether indoors or outdoors.
- 9 In the 54g Protection field, select Auto or Off. Do not disable 54g Protection if there is a possibility that an 802.11b device may need to use your wireless network.

Notes:

- 54g Protection allows 802.11g and 802.11b devices to co-exist in the same network without “speaking” at the same time. In Auto Mode, the wireless device will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
- You can enable Wi-Fi Multimedia (WMM) support to help improve the Quality of Service (QoS) for your wireless traffic. It is recommended that you leave these settings unchanged if you are not sure about your configuration. Changing these values may lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose.

- 10 Click **Save/Apply** to enable the wireless network.

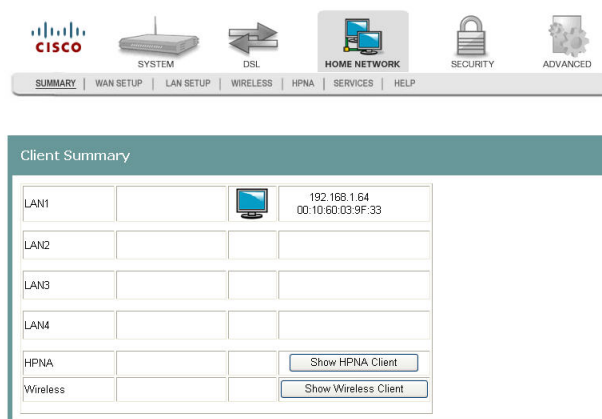
Securing Your Wireless Network with WEP

WEP is a security protocol for wireless networks. WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. A shared key (similar to a password) is used to allow communication between the computers and the residential gateway. WEP offers a basic, but satisfactory level of security for wireless data transmission.

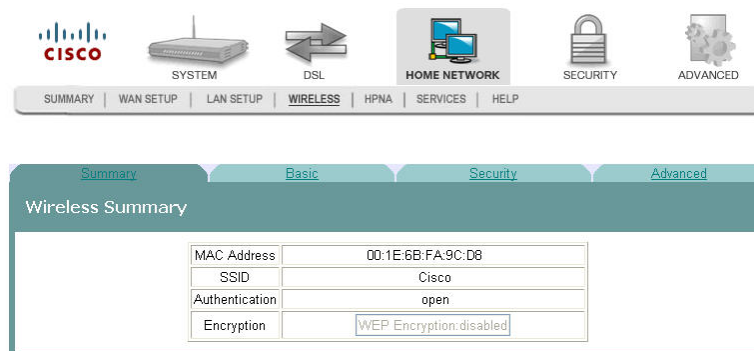
To secure your wireless network with Wired Equivalent Privacy (WEP), complete the following steps.

Chapter 5 Home Network Configuration

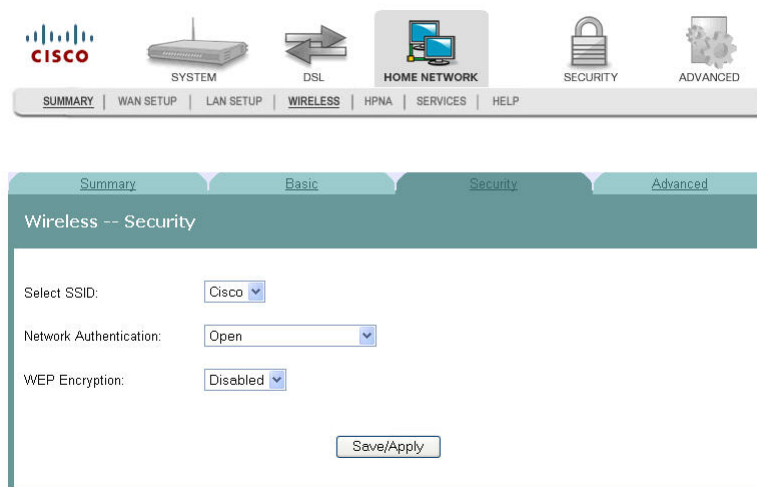
- 1 Click **Home Network** on the main screen. The Client Summary screen opens.



- 2 Click **Wireless**. The Wireless Summary screen opens.



- 3 Click **Security**. The Wireless -- Security screen opens.



- 4 In the **Select SSID** field, use the drop-down list to choose an option for the service set identifier (SSID).

Note: You can add options to this drop-down list on the Wireless -- Basic screen.

- 5 In the **Network Authentication** field, choose one of these two options for the authentication method.
 - **Open.** All devices may access the wireless network when WEP Encryption is disabled. When no authentication is required and if encryption is disabled, then the data that is passing between the access point and the client is also not encrypted. When WEP is enabled, the data is encrypted, but the client is not authenticated.
 - **WPA/WPA2.** See *Securing Your Wireless Network with Encryption Keys* (on page 120).
- 6 In the **WEP Encryption** field, select **Enabled**. The Wireless -- Security screen populates with more fields.

The screenshot shows the Cisco Wireless Security configuration page. The navigation bar at the top includes 'SUMMARY', 'WAN SETUP', 'LAN SETUP', 'WIRELESS', 'HPNA', 'SERVICES', and 'HELP'. The main content area is titled 'Wireless -- Security' and has tabs for 'Summary', 'Basic', 'Security', and 'Advanced'. The 'Security' tab is active. The configuration fields are as follows:

- Select SSID: Cisco
- Network Authentication: Open
- WEP Encryption: Enabled
- Encryption Strength: 128-bit
- Current Network Key: 1
- Network Key 1: [Input field]
- Network Key 2: [Input field]
- Network Key 3: [Input field]
- Network Key 4: [Input field]
- WEP Key Paraphrase: [Input field] [Generate]

Below the paraphrase field, there is a note: "*The encryption strength 128-bit generates 1 key. 64-bit generates 4 keys." At the bottom of the page is a 'Save/Apply' button.

- 7 In the **Encryption Strength** field, choose one of the following options:
 - **64-bit.** Secures your network by 64-bit (10 hex) encryption of all traffic using a static key.
 - **128-bit.** Secures your network by 128-bit (26 hex) encryption of all traffic using a static key.

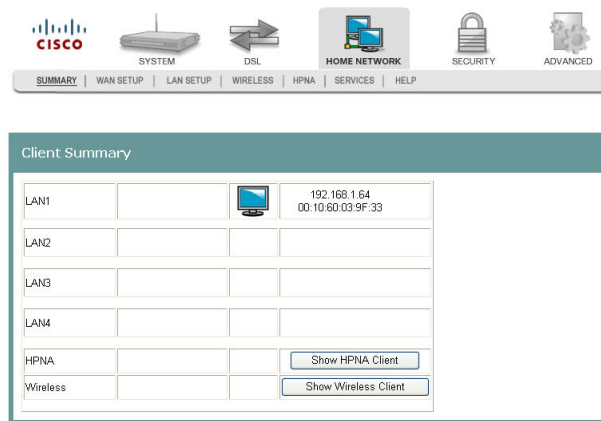
Important: These settings must be identical to your wireless client devices.

- 8 Do you want the system to generate the network key for you?
 - If **yes**, go to step 11.
 - If **no**, you must disable Serial Number Encryption and enter your own network key(s) in the field provided. Go to step 9.
- 9 In the Current Network Key field, select a network key from the drop-down list. Values are: 1, 2, 3, or 4.
- 10 In the Network Key 1 field, enter the network key you wish to use based on the encryption strength as discussed in step 7.
- 11 Based on the encryption strength you chose in step 7, do one of the following.
 - For 64-bit encryption, you can choose to enable Serial Number Encryption. When you enable Serial Number Encryption, the serial number of the gateway is preceded with a 0 (numeric zero) and is then used as the Network Key. Serial Number Encryption is not available for 128-bit encryption. If you don't want to use Serial Number Encryption (64 bit only), disable it by selecting Disabled from the drop-down list. Repeat steps 9 and 10 for keys 1 through 4 if you use 64-bit encryption. Go to step 12.
 - For 128-bit encryption, only one network key is used. Go to step 12.
- 12 In the WEP Key Paraphrase field, enter your information as follows based on 64-bit or 128-bit encryption strength:
 - For 64-bit encryption strength, enter a passphrase (1 to 31 characters) and click **Generate**. Four keys are generated based on the passphrase.
 - For 128-bit encryption, enter a passphrase (1 to 31 characters) and click **Generate**. Four keys are generated based on the passphrase.
- 13 Click **Save/Apply**.

Disabling the Wireless Network

To disable the wireless network, complete the following steps.

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



- 2 Click **Wireless**. The Wireless Summary screen opens.

MAC Address	00:1E:6B:FA:9C:D8
SSID	Cisco
Authentication	open
Encryption	WEP Encryption: disabled

- 3 Click **Basic**. The Wireless Basic screen opens.

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply" to configure the basic wireless options.

Enable Wireless

Hide Access Point

SSID:

Channel:

BSSID: 00:18:68:FF:61:6B

Wireless Mode:

54g Protection:

Enable WMM

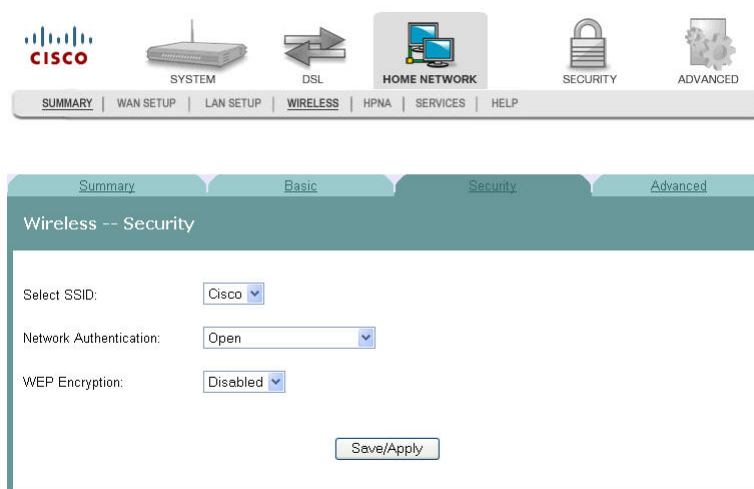
- 4 Uncheck the **Enable Wireless** check box. The wireless network fields are removed from the screen.
- 5 Click **Save/Apply** to disable the wireless network.

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 Disabled



Securing Your Wireless Network with Encryption Keys

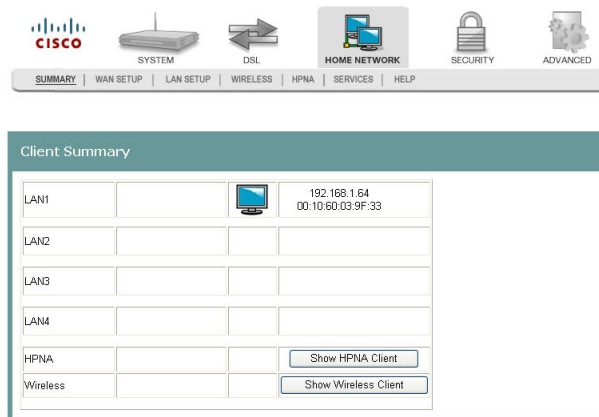
If you choose WPA Personal (also known as Wi-Fi Protected Access-PreShared Key) as the network authentication method, you can secure your network by encrypting all traffic using a pre-shared dynamic key. The following security methods are described:

- WPA Personal or WPA2 Personal
- Mixed WPA2 Personal/WPA Personal
- WPA/WPA2 Enterprise
- Mixed WPA/WPA2 Enterprise

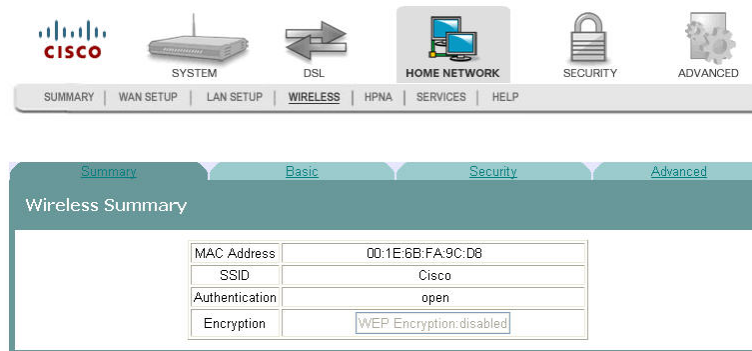
WPA Personal or WPA2 Personal

To secure your wireless network with a pre-shared dynamic key, complete the following steps.

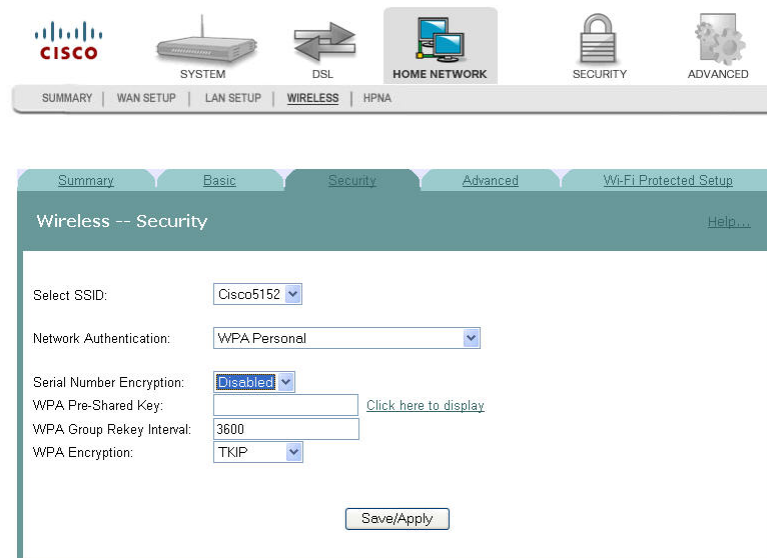
- 1 Click **Home Network** on the main screen. The Client Summary screen opens.



- 2 Click **Wireless**. The Wireless Summary screen opens.



- 3 Click **Security**. The Wireless -- Security screen opens.



- 4 In the Network Authentication field, select **WPA Personal** or **WPA2 Personal** from the drop-down list.

Chapter 5 Home Network Configuration

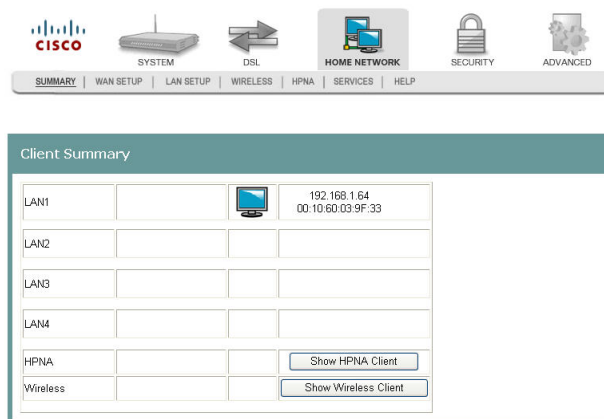
- 5 Select **Enabled or Disabled** to enable or disable your Serial Number Encryption function. Your serial number is printed on the back label of your device. If you enable this function, the system will automatically use your serial number as the pre-shared key for WPA Authentication.
- 6 In the WPA Pre-Shared Key field, enter a shared Key (8-63 characters). The system will periodically generate a dynamic key based on the shared key.
- 7 In the WPA Group Rekey Interval field, enter the group key renewal time period (in seconds). This time defines how often the dynamic key is regenerated
- 8 In the WPA Encryption field, select the encryption from the drop-down list. You have the option of choosing TKIP (Temporal Key Integrity Protocol), AES (Advanced Encryption System), or both. Typically AES is seen to be a more reliable form of encryption.
- 9 Click **Save/Apply** to save your settings.

Mixed WPA2 Personal/WPA Personal

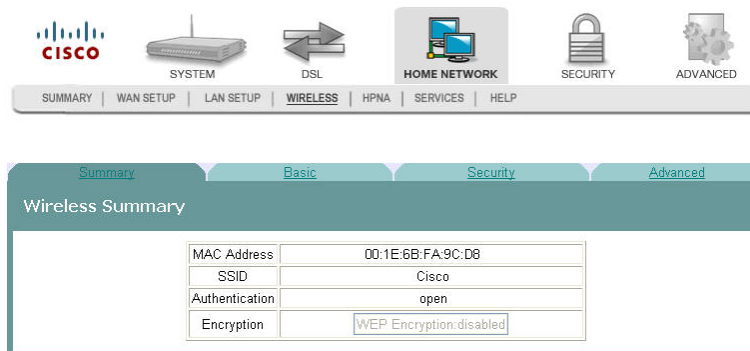
The security mode supports simultaneous WPA Personal and WPA2 Personal connections. You can have devices that use either WPA Personal or WPA2 Personal. The access point automatically chooses the encryption algorithm used by each client device.

To configure the Mixed WPA Personal and WPA2 Personal security settings for the access point, follow these steps:

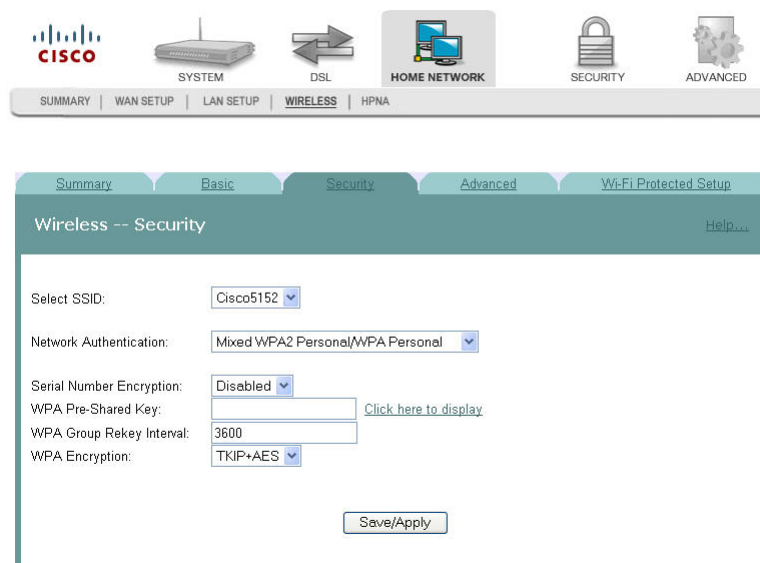
- 1 Click **Home Network** on the main screen. The Client Summary screen opens.



- 2 Click **Wireless**. The Wireless Summary screen opens.



- 3 Click **Security**. The Wireless -- Security screen opens.



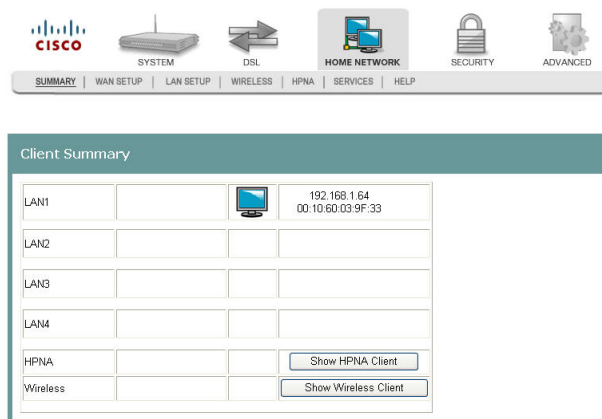
- 4 In the Network Authentication field, select Mixed WPA2 Personal/WPA Personal from the drop-down list.
- 5 Select **Enabled** or **Disabled** to enable or disable your Serial Number Encryption function. Your serial number will be printed on the back label of your device. If you enable this function, the system will automatically use your serial number as the network key for your WEP encryption.
- 6 In the WPA Pre-Shared Key field, enter a shared Key (8-63 characters). The system will periodically generate a dynamic key based on the shared key.
- 7 In the WPA Group Rekey Interval field, enter the group key renewal time period (in seconds). This time defines how often the dynamic key is regenerated
- 8 In the WPA Encryption field, select the encryption from the drop-down list.
- 9 Click **Save/Apply** to save your settings.

WPA/WPA2 Enterprise

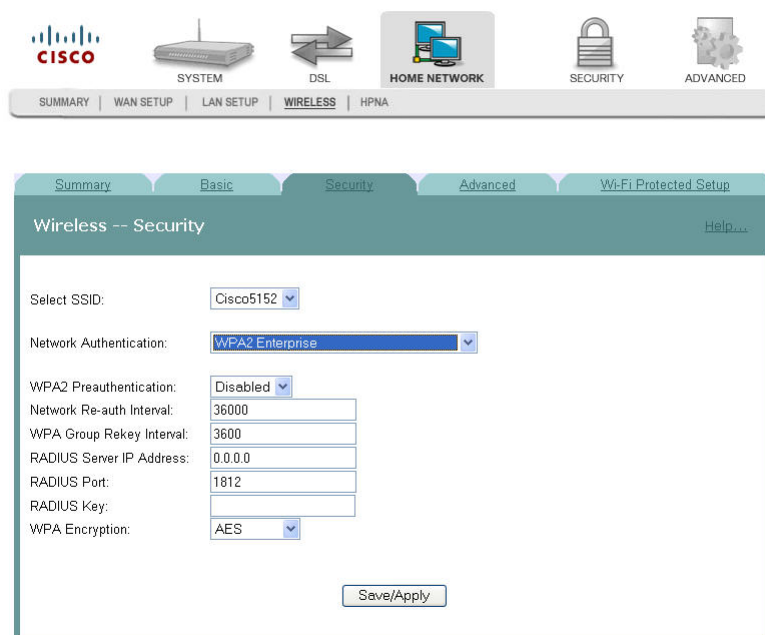
WPA/WPA2 Enterprise is used in coordination with a Remote Authentication Dial-In Use Service (RADIUS) server for client authentication.. If you choose this to be your authentication method, make sure that a RADIUS server is available in the network for authentication.

To configure the WPA/WPA2 Enterprise security settings for the access point, complete the following steps.

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



- 2 Click **Wireless**. The Wireless Summary screen opens.



- 3 In the Network Authentication field, select **WPA/WPA2 Enterprise** from the drop-down list.
- 4 Select **Enabled** or **Disabled** for your WPA2 Pre-authentication.

Note: In pre-authentication, a WPA2 wireless client can perform an 802.1X authentication with other wireless access points in its range when it is still connected to its current wireless access point.

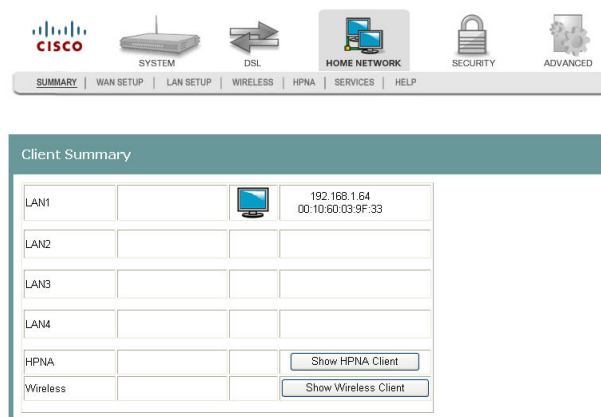
- 5 In the Network Re-auth Interval, enter the interval at which the re-authentication occurs.
- 6 In the WPA Group Rekey Interval field, enter the group key renewal time period (in seconds). This time defines how often the dynamic key will be regenerated.
- 7 In the RADIUS Server IP Address enter the IP address for your RADIUS server.
- 8 In the RADIUS Port field, enter the port number for your RADIUS server. The default port is 1812.
- 9 In the Radius Key field, please enter the secret key used by the access point and RADIUS server.
- 10 In the WPA Encryption field, please select your data encryption method from TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard).
- 11 Click **Save/Apply** to save your settings.

Mixed WPA/WPA2 Enterprise

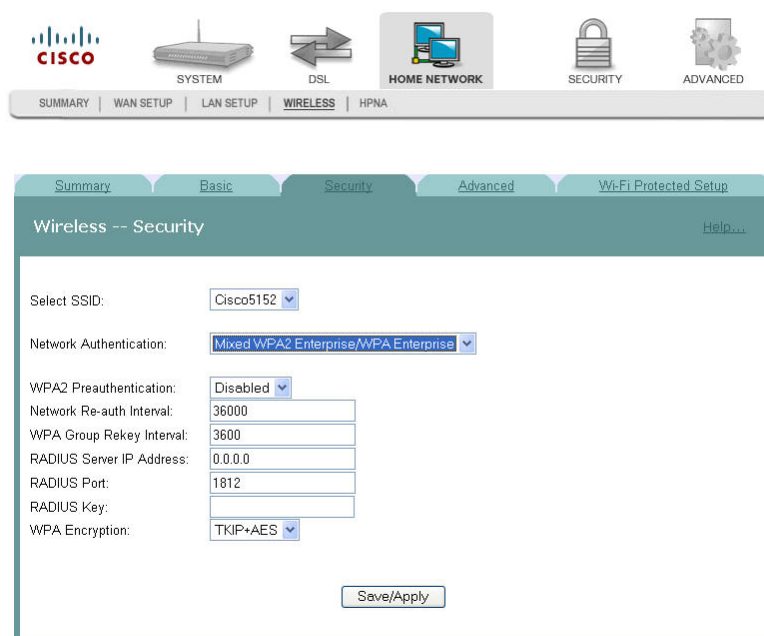
The security mode supports simultaneous WPA Enterprise and WPA2 Enterprise connections. You can have devices that use either WPA Enterprise or WPA2 Enterprise. The access point automatically chooses the encryption algorithm used by each client device.

To configure the Mixed WPA/WPA2 Enterprise security settings for the access point, complete the following steps.

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



- 2 Click **Wireless**. The Wireless Summary screen opens.

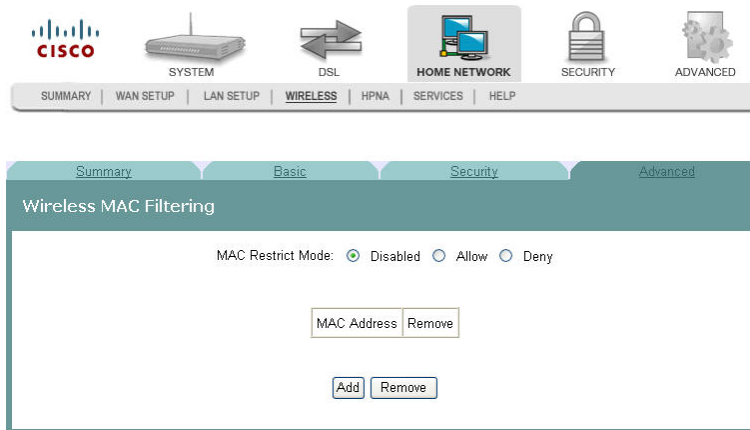


- 3 In the Network Authentication field, select **Mixed WPA2 Enterprise/WPA Enterprise** from the drop-down list.
- 4 Select **Enabled** or **Disabled** for your WPA2 Pre-authentication.
Note: In pre-authentication, a WPA2 wireless client can perform an 802.1X authentication with other wireless access points in its range when it is still connected to its current wireless access point.
- 5 In the Network Re-auth Interval, enter the interval at which the re-authentication occurs.
- 6 In the WPA Group Rekey Interval field, enter the group key renewal time period. This time defines how often the dynamic key will be regenerated.
- 7 In the RADIUS Server IP Address, enter the IP address for your RADIUS server.
- 8 In the RADIUS Port field, enter the port number for your RADIUS server. The default port is 1812.
- 9 In the Radius Key field, enter the secret key used by the access point and RADIUS server.
- 10 In the WPA Encryption field, select your data encryption method from TKIP (Temporal Key Integrity Protocol), AES (Advanced Encryption Standard), or TKIP+AES.
- 11 Click **Save/Apply** to save your settings.

Wireless MAC Filtering

The Wireless -- MAC Filtering screen allows you to allow or block certain wireless clients from accessing the residential gateway. If you know the MAC address of the client you want to block, you can use this screen to provide access to the residential gateway or block that client from accessing it.

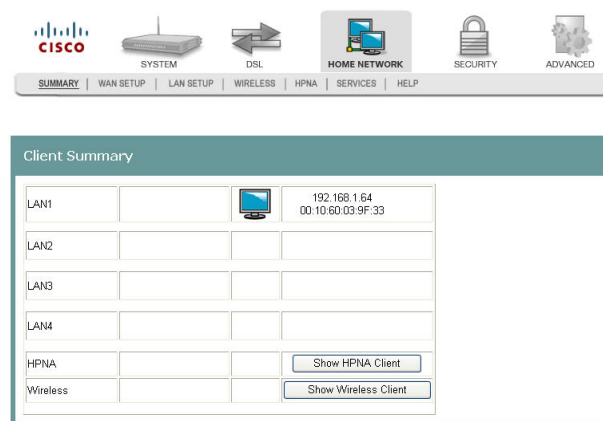
Path: Home Network > Wireless > Advanced > MAC Filter



Allowing Wireless Clients to Access the Residential Gateway

You can allow wireless clients to access the residential gateway if you know the client's MAC address. MAC restrict mode must be enabled. To allow wireless clients to access the residential gateway, complete the following steps.

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



Chapter 5 Home Network Configuration

- 2 Click **Wireless**. The Wireless Summary screen opens.

The screenshot shows the Cisco Home Network configuration interface. At the top, there are icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below these are navigation tabs: SUMMARY, WAN SETUP, LAN SETUP, WIRELESS, HPNA, SERVICES, and HELP. The main content area is titled "Wireless Summary" and contains a table with the following information:

MAC Address	00:1E:6B:FA:9C:D8
SSID	Cisco
Authentication	open
Encryption	WEP Encryption: disabled

- 3 Click **Advanced**. The Wireless Advanced Settings screen opens.

The screenshot shows the Cisco Home Network configuration interface. At the top, there are icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below these are navigation tabs: SUMMARY, WAN SETUP, LAN SETUP, WIRELESS, HPNA, SERVICES, and HELP. The main content area is titled "Wireless Advanced Settings" and contains a list of links:

- [MAC Filter](#)
- [Wireless Bridge](#)
- [Station Info](#)

- 4 Click **MAC Filter**. The Wireless MAC Filtering screen opens.

The screenshot shows the Cisco Home Network configuration interface. At the top, there are icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below these are navigation tabs: SUMMARY, WAN SETUP, LAN SETUP, WIRELESS, HPNA, SERVICES, and HELP. The main content area is titled "Wireless MAC Filtering" and contains the following information:

MAC Restrict Mode: Disabled Allow Deny

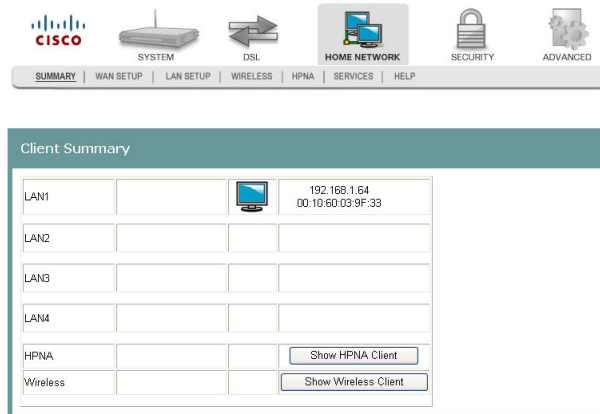
MAC Address	Remove
-------------	--------

- 5 In the MAC Restrict Mode field, click **Allow** to enable the MAC restrict mode.
- 6 Click **Add**. The Wireless -- MAC Filter screen opens.
- 7 In the MAC Address field, enter the MAC address of the client that you want to allow access to the residential gateway.
- 8 Click **Save/Apply** to allow this wireless client to access the residential gateway.

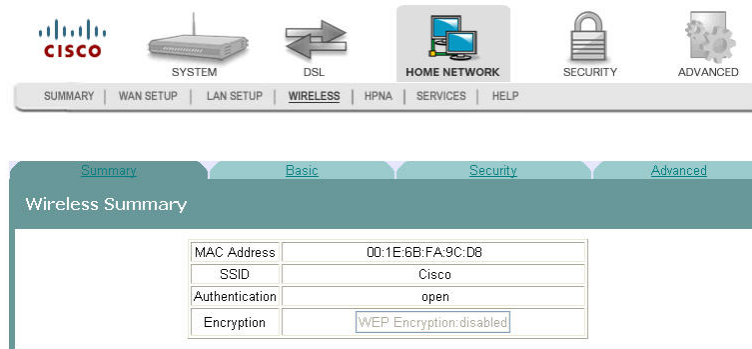
Blocking Wireless Clients

You can block wireless clients from accessing the residential gateway if you know the client's MAC address. MAC restrict mode must be enabled. To prevent wireless clients from accessing the residential gateway, complete the following steps.

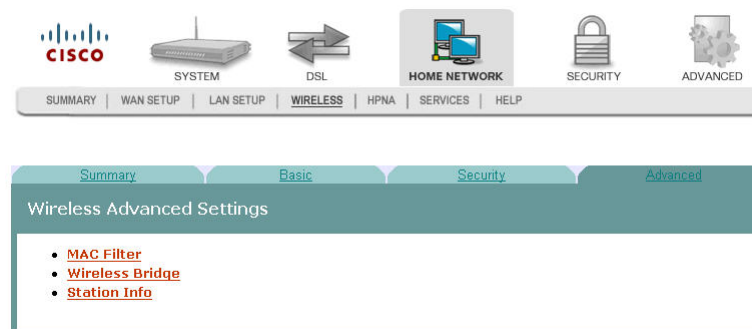
- 1 Click **Home Network** on the main screen. The Client Summary screen opens.



- 2 Click **Wireless**. The Wireless Summary screen opens.

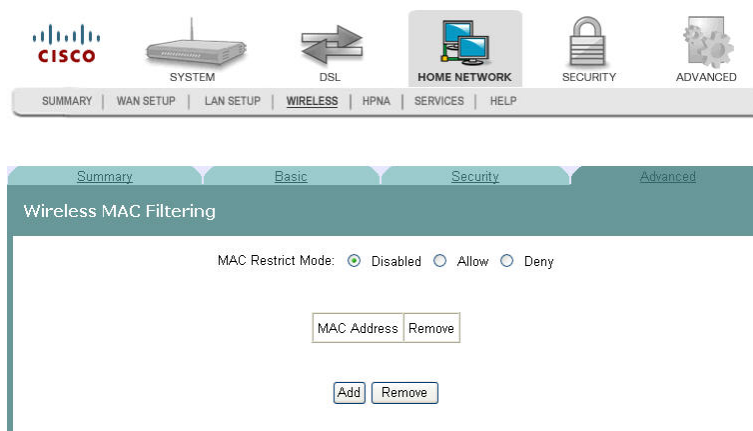


- 3 Click **Advanced**. The Wireless Advanced Settings screen opens.



Chapter 5 Home Network Configuration

- 4 Click **MAC Filter**. The Wireless MAC Filtering screen opens.



- 5 In the MAC Restrict Mode field, click **Deny** to enable the MAC restrict mode.
- 6 Click **Add**. The Wireless -- MAC Filter screen opens.
- 7 In the MAC Address field, enter the MAC address of the client that you want to prevent from accessing the residential gateway.
- 8 Click **Save/Apply** to prevent this wireless client from accessing the residential gateway.

Wireless Bridge

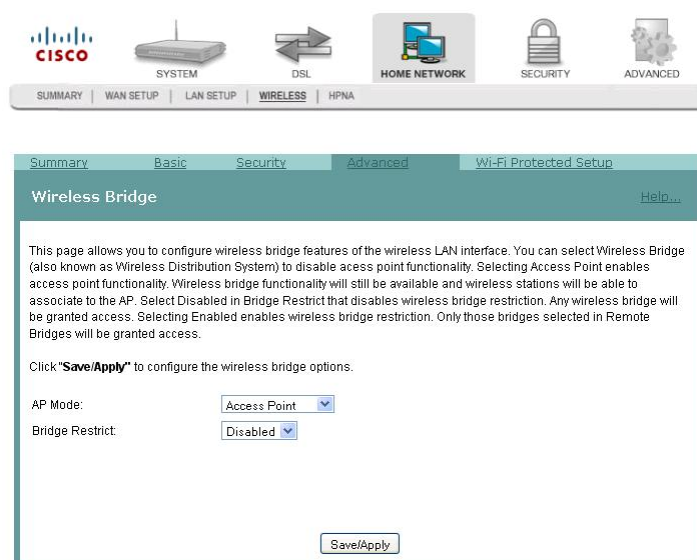
Wireless LAN Bridging (also referred to as a Wireless Distribution System, WDS) refers to two or more 802.11 access points that send traffic between them (from access point to access point) as opposed to between access point and a client computer.

The Wireless Bridge screen allows you to configure the wireless bridge features of the wireless LAN interface as follows:

- Select Wireless Bridge in the AP mode to disable access point functionality.
- Select Access Point in the AP mode to enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
- Select Disabled in the Bridge Restrict field to disable wireless bridge restriction so any device can communicate with the residential gateway over the wireless bridge.
- Select Enabled in the Bridge Restrict field to enable wireless bridge restriction to restrict the bridges that can communicate with the residential gateway over the wireless interface.
- Enter the MAC Address of the remote bridge in the Remote Bridges MAC Address field

Path: Home Network > Wireless > Advanced > Wireless Bridge

Bridge Restrict Disabled



Bridge Restrict Enabled

The screenshot shows the Cisco configuration interface for a wireless router. At the top, there are navigation icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below these is a breadcrumb trail: SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA. The main content area has tabs for Summary, Basic, Security, Advanced, and Wi-Fi Protected Setup. The 'Advanced' tab is selected, and the page title is 'Wireless Bridge'. A 'Hello...' link is in the top right corner. The main text explains the configuration options for the wireless LAN interface, including AP Mode, Bridge Restrict, and Remote Bridges MAC Address. The 'AP Mode' is set to 'Wireless Bridge' and 'Bridge Restrict' is set to 'Enabled'. There are two empty input fields for 'Remote Bridges MAC Address' and a 'Save/Apply' button at the bottom.

WIRELESS

SUMMARY | WAN SETUP | LAN SETUP | **WIRELESS** | HPNA

Summary Basic Security **Advanced** Wi-Fi Protected Setup

Wireless Bridge [Hello...](#)

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict that disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click **"Save/Apply"** to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Wireless Station List

This page shows associated wireless MAC addresses and status.

Path: Home Network > Wireless > Advanced > Station Info

The screenshot shows the Cisco Home Network configuration interface. The top navigation bar includes icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below the navigation bar, the 'WIRELESS' tab is selected. The main content area is titled 'Wireless Station List' and contains the following text:

Wireless -- Associated Stations

This page shows associated wireless MAC addresses and status.

Below the text, there are two columns labeled 'MAC' and 'Associated', and a 'Refresh' button.

Showing MAC Addresses and Clients

To show the wireless MAC Address and clients, complete the following steps.

- 1 Click **Home Network** on the main screen.
- 2 Click **Wireless**. The Wireless Summary screen opens.

The screenshot shows the Cisco Home Network configuration interface. The top navigation bar includes icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below the navigation bar, the 'WIRELESS' tab is selected. The main content area is titled 'Wireless Summary' and contains the following table:

MAC Address	00:1E:6B:FA:9C:D8
SSID	Cisco
Authentication	open
Encryption	WEP Encryption: disabled

- 3 Click **Advanced**. The Wireless Advanced Settings screen opens.

The screenshot shows the Cisco Home Network configuration interface. The top navigation bar includes icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below the navigation bar, the 'WIRELESS' tab is selected. The main content area is titled 'Wireless Advanced Settings' and contains the following list:

- [MAC Filter](#)
- [Wireless Bridge](#)
- [Station Info](#)

Chapter 5 Home Network Configuration

- 4 Click **Station Info**. The Wireless Station List opens.
- 5 Click **Refresh** to update the list of MAC addresses and associated status.

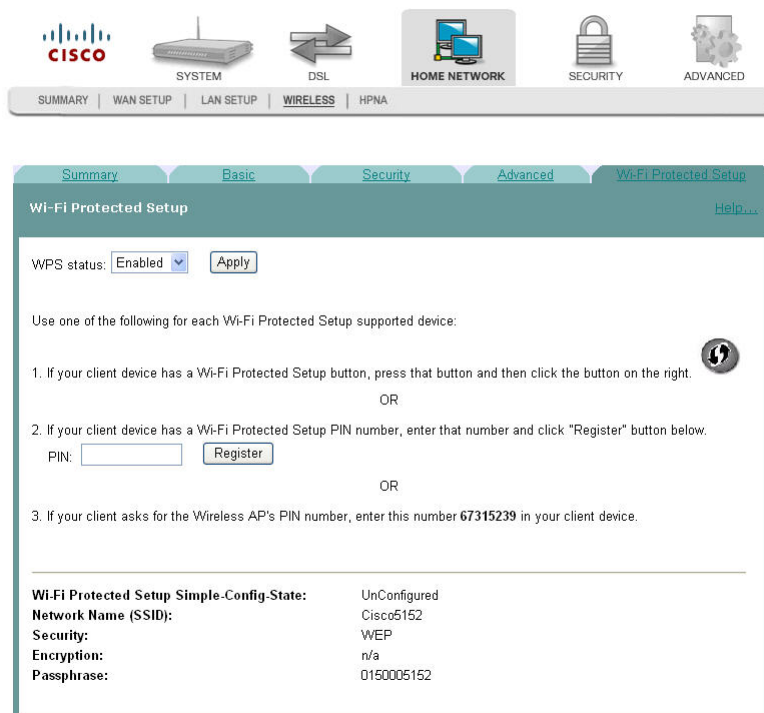
Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) is a standard for easy and secure establishment of a wireless home network.

You can choose to use either the PBC or PIN method for connecting the wireless networks using WPS. But first, you will still need to configure the appropriate authentication on your router. For more information, see *Security Configuration* (on page 141).

Note: Ensure that your wireless client supports WPS. If your wireless client does not support WPS, you cannot use this functionality.

Path: Home Network > Wireless > Wi-Fi Protected Setup



PBC Method

The PBC method requires the user to press a button (either actual or virtual) on both the DDR2200 and the new wireless client device to establish the wireless connection.

To set up your wireless network using the PBC method, complete the following steps.

- 1 Click **Home Network** on the main screen.
- 2 Click **Wi-Fi Protected Setup**. The Wi-Fi Protected Setup screen opens.
- 3 For the WPS status drop-down field, select **Enabled** to enable the WPS status.

Chapter 5 Home Network Configuration

- 4 Click the button at the right-hand-side on the page or the Wi-Fi-sec button on the device. Then, within 2 minutes, push another button on your client adapter's WPS setup screen. It should start the process of configuring the wireless security on your client station.

PIN Method

The PIN method requires the user to enter a personal identification number (PIN) from a label on the new device to establish the wireless connection.

To set up your wireless network using a PIN:

- 1 Click **Home Network** on the main screen.
- 2 Click **Wi-Fi Protected Setup**. The Wi-Fi Protected Setup screen opens.
- 3 For the WPS status drop-down field, select **Enabled** to enable the WPS status.
- 4 In the PIN field, enter the same PIN number (8-digit number, sometimes it will be shipped with your client's adapter if it supports WPS) for both of the wireless router and station. Then click **Register** to start the process of configuring the wireless security on your client station.

HPNA Information

The HPNA Info screen allows you to view the HPNA devices connected to the residential gateway.

Path: Home Network > HPNA > HPNA Info

The screenshot shows the Cisco Home Network configuration utility interface. The top navigation bar includes icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. The HPNA menu item is highlighted. Below the navigation bar, the HPNA Info screen is displayed. It features a checkbox for 'Enable HPNA interface' which is checked. Below this is a table with the following data:

Role	MAC	Version
MASTER	00:18:68:ff:4d:82	1.7.5

At the bottom of the HPNA Info screen, there is a button labeled 'HPNA Update'.

Updating HPNA Information

To update the HPNA information, complete the following steps.

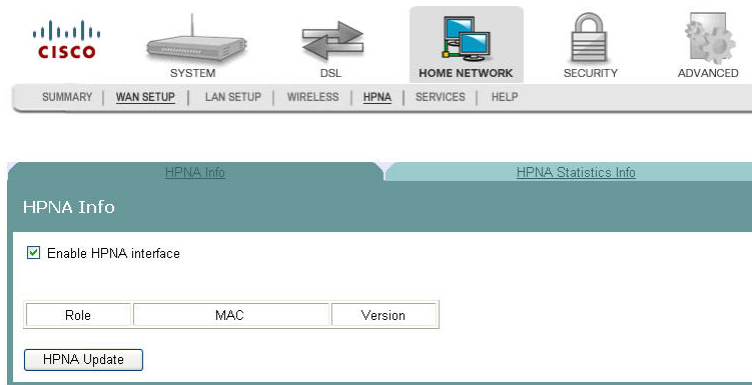
- 1 Click **Home Network** on the main screen. The Client Summary screen opens.

The screenshot shows the Client Summary screen in the Cisco Home Network configuration utility. The top navigation bar includes icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. The HPNA menu item is highlighted. Below the navigation bar, the Client Summary screen is displayed. It features a table with the following data:

LAN1			192.168.1.64 00:10:60:03:9F:33
LAN2			
LAN3			
LAN4			
HPNA			Show HPNA Client
Wireless			Show Wireless Client

Chapter 5 Home Network Configuration

- 2 Click **HPNA**. After a moment of processing, the HPNA Info screen opens.



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

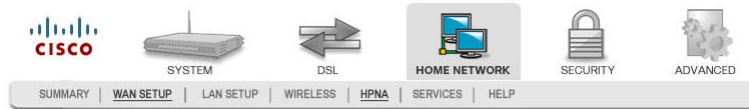


- 4 In the Software File Name field, enter the name of the file that you want to use to update your system. You can click Browse to locate the file.
- 5 Click **Next**. The software for the attached HPNA devices is updated.

HPNA Statistics Information

The HPNA Statistics Info screen displays the statistics for the HPNA devices connected to the residential gateway.

Path: Home Network > HPNA > HPNA Statistics Info



HPNA Info		HPNA Statistics Info	
HPNA Statistics Info			
0)	127.0.0.1:	(null)	packets
	Name:	lo	packets
1)	192.168.1.254:	(null)	bytes
	Name:	br0	bytes
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	packets
	Name:	(null)	clock ticks
	Name:	(null)	clock ticks
	Name:	(null)	clock ticks
	Name:	(null)	clock ticks
	Name:	(null)	clock ticks
	Name:	(null)	clock ticks
	Name:	(null)	clock ticks

6

Security Configuration

The Security tab allows you to check the security configuration and modify the configuration.

Use this chapter to help you check the status of the security configuration or make changes to the configuration.

In This Chapter

■ MAC Filtering Setup	142
■ Incoming IP Filtering.....	148
■ Outgoing IP Filtering	154
■ Parental Control Setup - Filtering Function.....	159
■ URL Filtering Function	165
■ Stateful Packet Inspection.....	170
■ Local Certificates.....	173
■ Trusted CA Certificates.....	178

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 MAC Filtering means that all MAC layer frames will be FORWARDED except those that match any of the specified rules in the following screen.

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

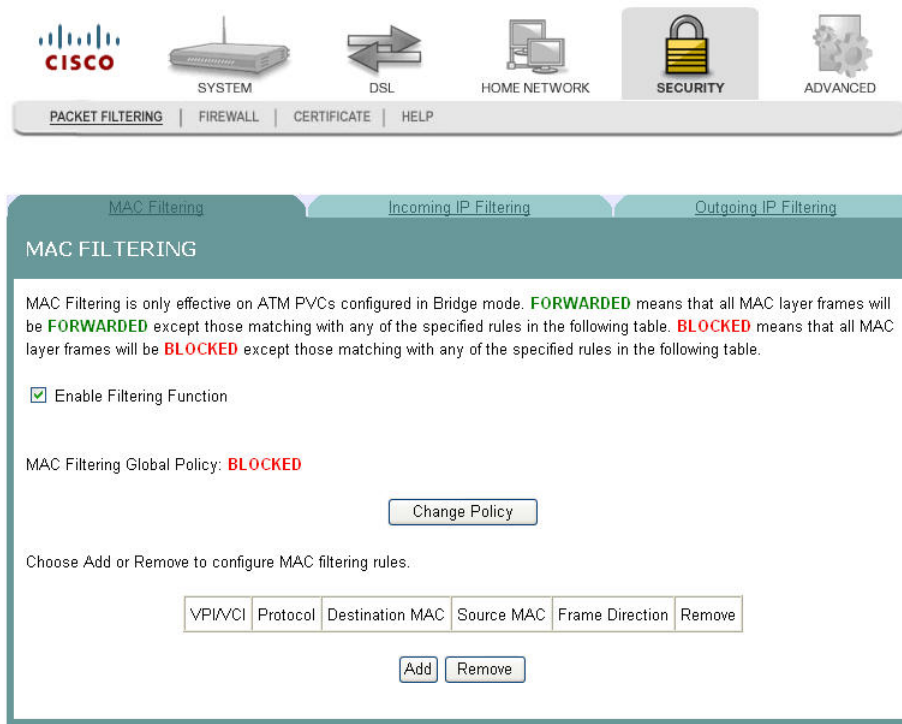
Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

[Add](#) [Remove](#)

Blocked MAC Filtering

Blocked MAC Filtering means that all MAC layer frames will be **BLOCKED** except those that match any of the specified rules in the following screen.



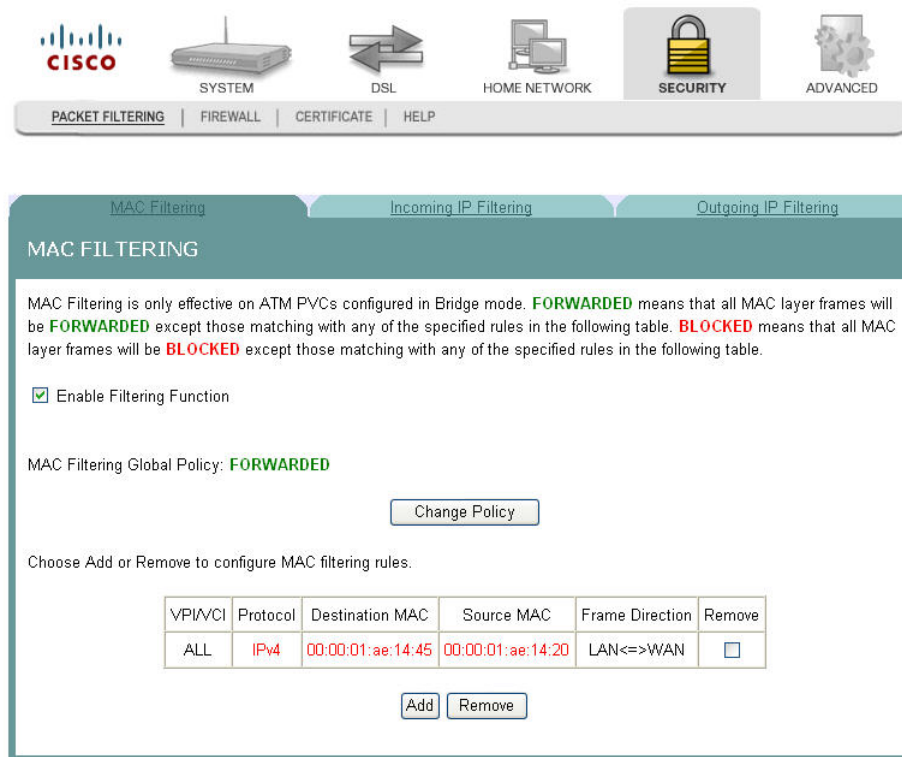
Adding MAC Filtering

To add MAC Filtering, complete the following steps.

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

Chapter 6 Security Configuration

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



The screenshot shows the Cisco router configuration interface. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below this is a sub-menu with PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area is titled "MAC FILTERING" and has three tabs: MAC Filtering, Incoming IP Filtering, and Outgoing IP Filtering. The text explains that MAC Filtering is only effective on ATM PVCs in Bridge mode and defines "FORWARDED" and "BLOCKED" states. A checkbox for "Enable Filtering Function" is checked. The global policy is set to "FORWARDED" with a "Change Policy" button. Below, a table shows a rule with Protocol "IPv4", Destination MAC "00:00:01:ae:14:45", Source MAC "00:00:01:ae:14:20", and Frame Direction "LAN<=>WAN". "Add" and "Remove" buttons are at the bottom.

MAC FILTERING

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

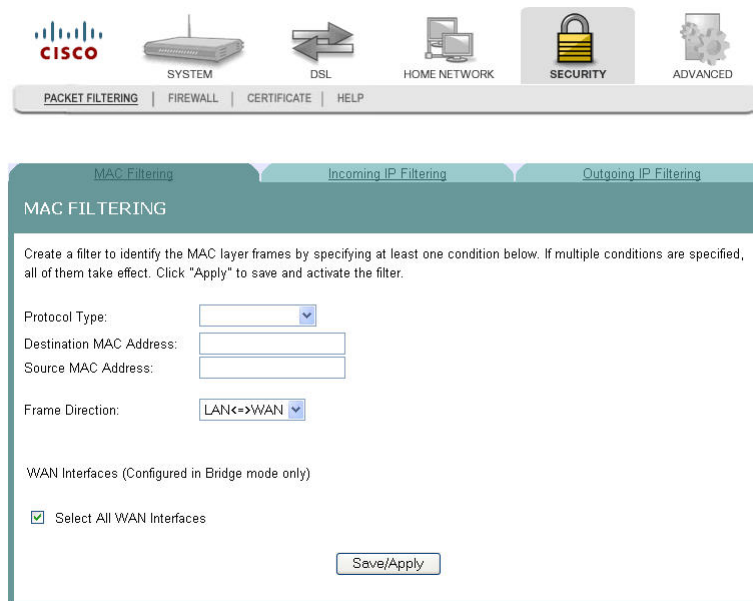
[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

[Add](#) [Remove](#)

- 3 Check the **Enable Filtering Function** check box.
- 4 Click **Add** to open a blank MAC Filtering screen.



The screenshot shows the Cisco router configuration interface, similar to the previous one. The "MAC FILTERING" tab is active. The text instructs the user to create a filter by specifying at least one condition. There are input fields for Protocol Type, Destination MAC Address, and Source MAC Address. The Frame Direction is set to "LAN<=>WAN". Under "WAN Interfaces (Configured in Bridge mode only)", the "Select All WAN Interfaces" checkbox is checked. A "Save/Apply" button is at the bottom.

MAC FILTERING

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Select All WAN Interfaces

[Save/Apply](#)

- 5 In the Protocol Type field, select one of the following protocols from the drop-down menu.
 - PPPoE
 - IPv4
 - IPv6
 - AppleTalk
 - IPX
 - NetBEUI
 - IGMP
- 6 In the Destination MAC Address field, enter the frame's destination MAC address.
- 7 In the Source MAC Address field, enter the frame's source MAC address.
- 8 In the Frame Direction field, select one of the following choices from the drop-down menu:
 - LAN<->WAN
 - WAN<->LAN
- 9 Do you want to select all WAN interfaces?
 - If **yes**, check the Select All WAN Interfaces check box under the WAN Interfaces (Configured in Bridge mode only) field.
 - If **no**, uncheck the Select All WAN Interfaces check box under the WAN Interfaces (Configured in Bridge mode only) field.
- 10 Click **Save/Apply** to add the MAC Filter.

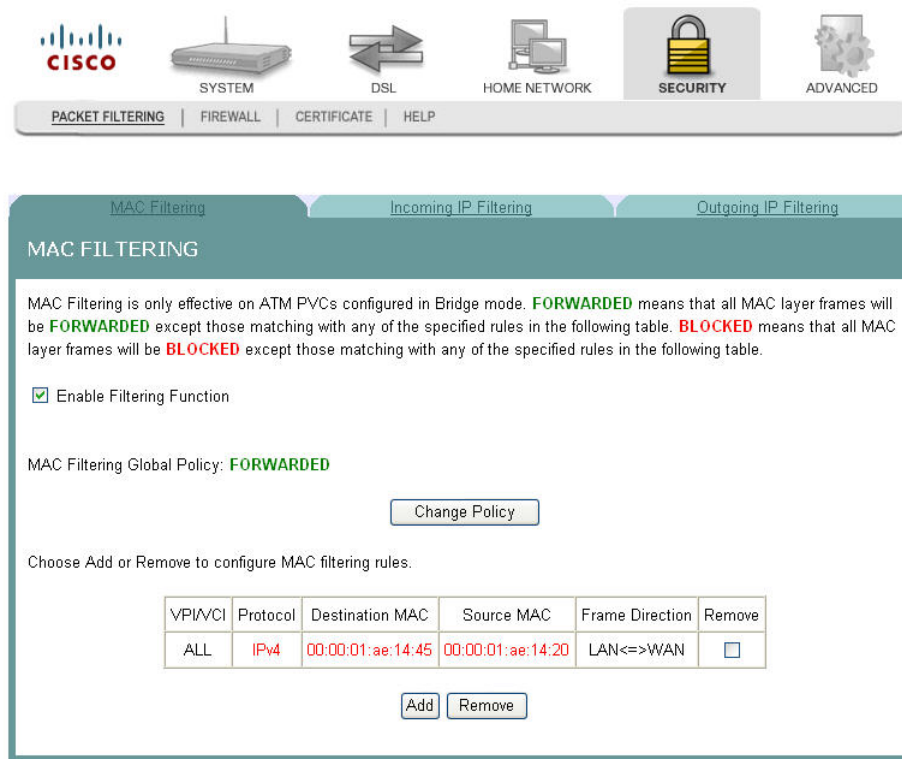
Forwarding or Blocking MAC Layer Frames

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.

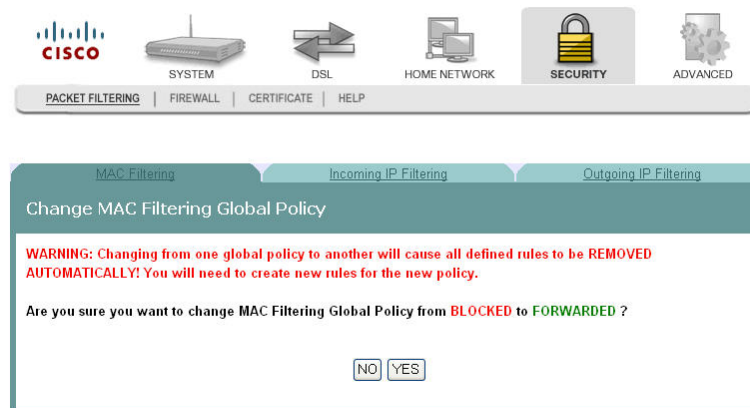
To change the policy on how MAC layer frames are forwarded or blocked, complete the following steps.

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

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



- Check the **Enable Filtering Function** check box.
- Click **Change Policy**. The Change MAC Filtering Global Policy screen opens. In this example, the global policy for MAC filtering is "Blocked."

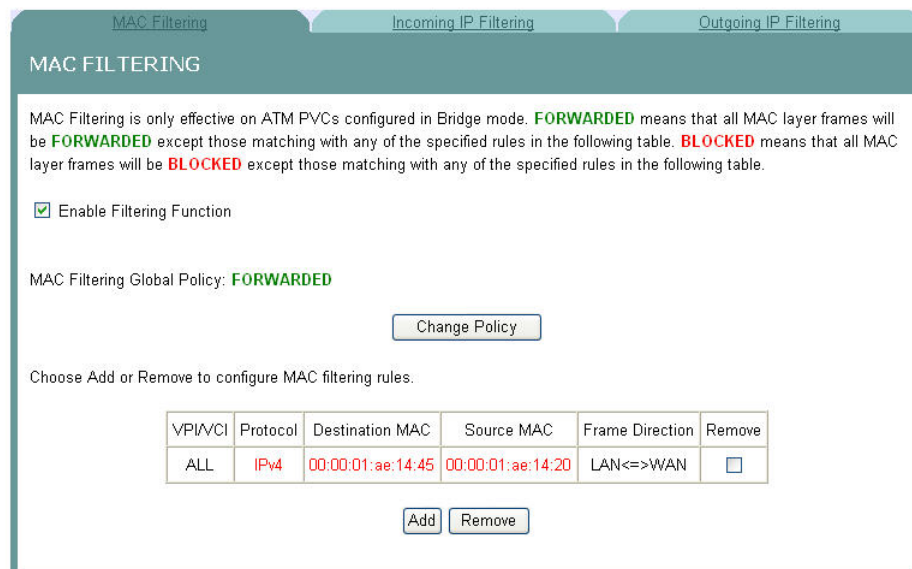


- Do you want to change the Global Policy?
 - If **yes**, click **Yes**. If the policy is forwarded, clicking Yes changes the policy to blocked and vice versa.
 - If **no**, click **No** and the policy remains unchanged.

Removing MAC Filtering

To remove a MAC 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.

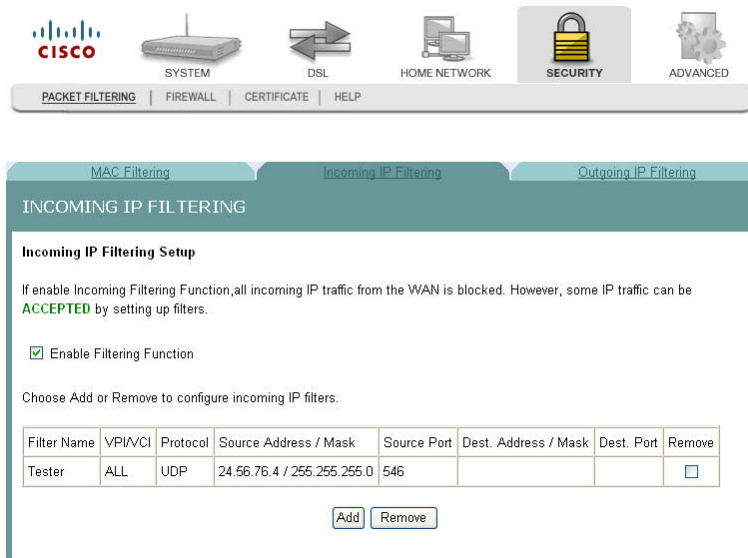


- 3 From the MAC Filtering screen, select **Remove** in the Remove column next to the MAC filtering rule you wish to remove.
- 4 Click **Remove** to remove the MAC filtering.

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 > Packet Filtering > 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.

MAC FILTERING

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

[Add](#) [Remove](#)

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

INCOMING IP FILTERING

Incoming IP Filtering Setup

If enable Incoming Filtering Function, all incoming IP traffic from the WAN is blocked. However, some IP traffic can be **ACCEPTED** by setting up filters.

Enable Filtering Function

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	ALL	UDP	24.56.76.4 / 255.255.255.0	546			<input type="checkbox"/>

[Add](#) [Remove](#)

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

The screenshot shows the Cisco configuration interface for adding an incoming IP filter. The navigation bar includes icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below the navigation bar are tabs for MAC Filtering, Incoming IP Filtering, and Outgoing IP Filtering. The main content area is titled "Add IP Filter -- Incoming" and contains the following text and form fields:

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.

Select All

- 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. You can enter one port or a range of ports using the following format: port or port:port.
Example: 0:5 indicates 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. You can enter one port or a range of ports using the following format: port or port:port.

Example: 0:5 indicates ports 0 through 5.

- 12 Do you want to select all of the WAN interfaces?
- If **yes**, check the **Select All** field under WAN Interfaces (Configured in Routing mode and with firewall enabled only).
 - If **no**, clear the **Select All** field under WAN Interfaces (Configured in Routing mode and with firewall enabled only).
- 13 Click **Save/Apply** to add the filter.

Enabling the Filtering Function

To enable the filtering function, complete the following steps.

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



MAC Filtering
Incoming IP Filtering
Outgoing IP Filtering

MAC FILTERING

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

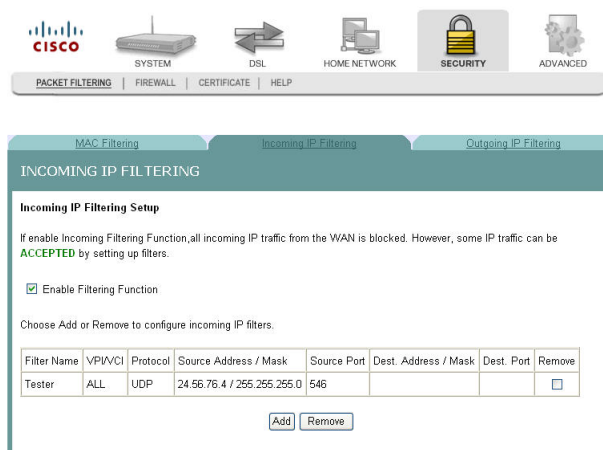
Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

[Add](#) [Remove](#)

Chapter 6 Security Configuration

- 2 Click **Incoming IP Filtering**. The Incoming IP Filtering screen opens.

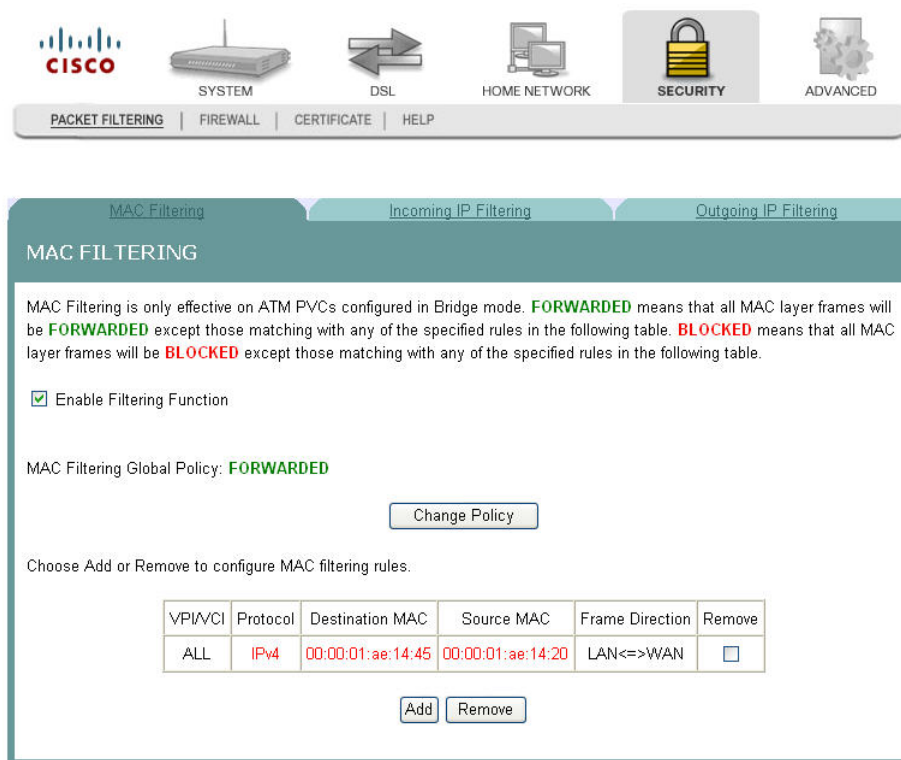


- 3 Check the **Enable Filtering Function** check box to enable the filtering function.

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.

The screenshot shows the Cisco router configuration interface. At the top, there are navigation tabs: PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. Below these are icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. The 'Incoming IP Filtering' tab is selected. The main content area is titled 'INCOMING IP FILTERING' and contains the following information:

Incoming IP Filtering Setup

If enable Incoming Filtering Function, all incoming IP traffic from the WAN is blocked. However, some IP traffic can be **ACCEPTED** by setting up filters.

Enable Filtering Function

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	ALL	UDP	24.56.76.4 / 255.255.255.0	546			<input type="checkbox"/>

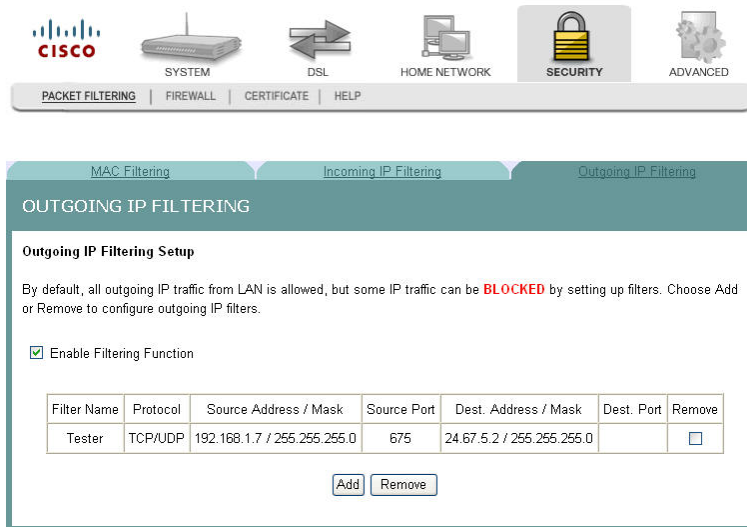
At the bottom of the table, there are 'Add' and 'Remove' buttons. The 'Remove' button is highlighted in the screenshot.

- 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.

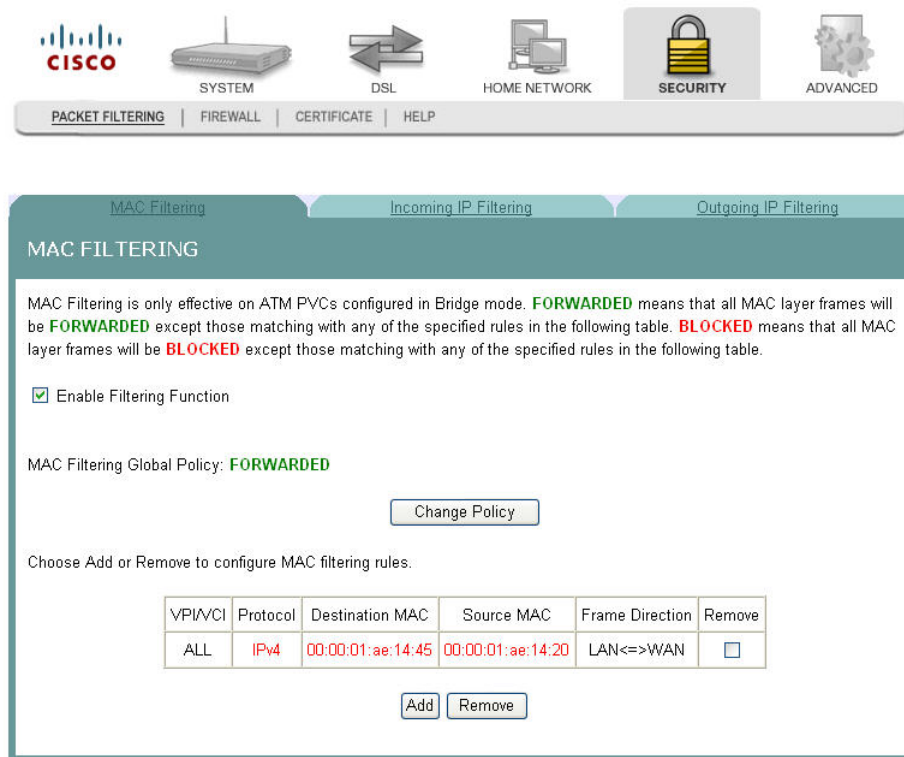
Path: Security > Packet Filtering > Outgoing IP Filtering



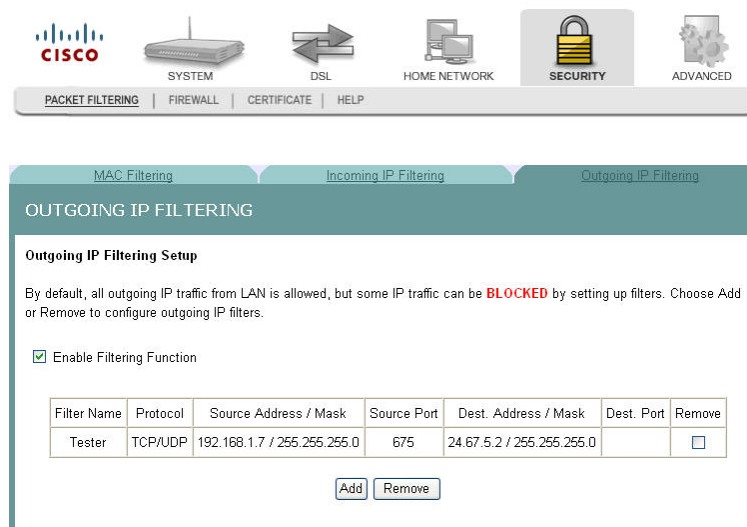
Enabling the Filtering Function

To enable the outgoing IP filtering function, complete the following steps.

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



- 2 Click **Outgoing IP Filtering**. The Outgoing IP Filtering screen opens.



- 3 Check the **Enable Filtering Function** check box to enable the filtering function.

Adding an Outgoing IP Filter

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

Chapter 6 Security Configuration

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

The screenshot shows the Cisco Security Configuration interface. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY (highlighted), and ADVANCED. Below this is a secondary navigation bar with links for PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area is titled "MAC FILTERING" and includes the following text:

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

[Add](#) [Remove](#)

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

The screenshot shows the Cisco Security Configuration interface with the "Outgoing IP Filtering" tab selected. The navigation bar and secondary navigation bar are the same as in the previous screenshot. The main content area is titled "OUTGOING IP FILTERING" and includes the following text:

Outgoing IP Filtering Setup

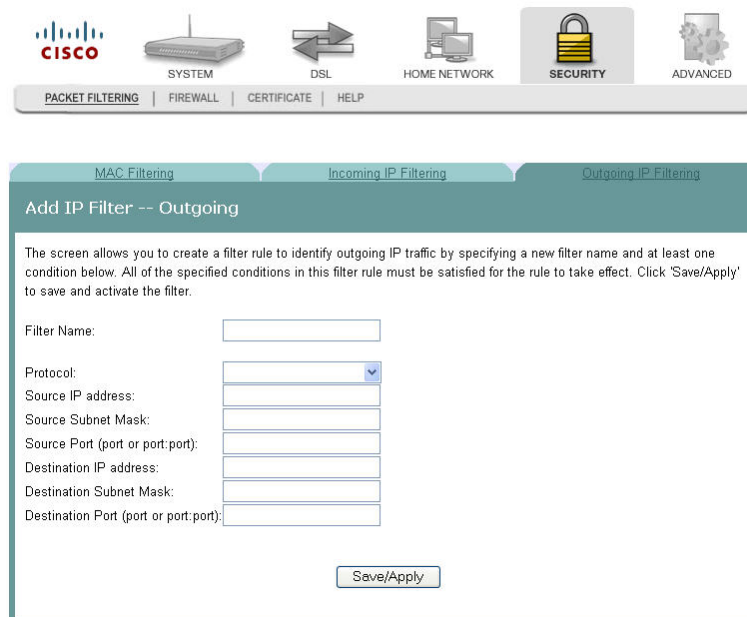
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters. Choose Add or Remove to configure outgoing IP filters.

Enable Filtering Function

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	TCP/UDP	192.168.1.7 / 255.255.255.0	675	24.67.5.2 / 255.255.255.0		<input type="checkbox"/>

[Add](#) [Remove](#)

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

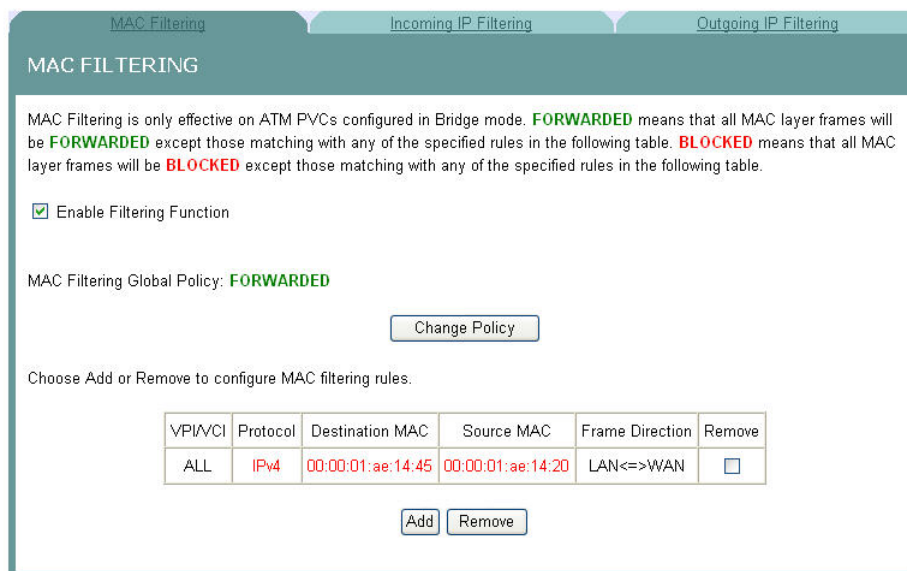


- 4 In the Filter Name field, enter the name of the filter.
Note: You cannot use blank spaces in the filter name.
- 5 In the Protocol field, select one of the following protocols:
 - TCP/UDP
 - TCP
 - UDP
 - ICMP
- 6 In the Source IP address field, enter the source IP address for the server sending the incoming packets.
- 7 In the Source Subnet Mask field, enter the subnet mask for the 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.

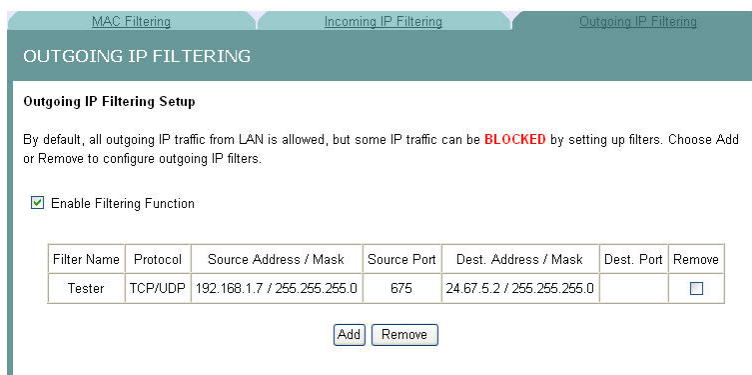
Removing an Outgoing IP Filter

To remove 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.

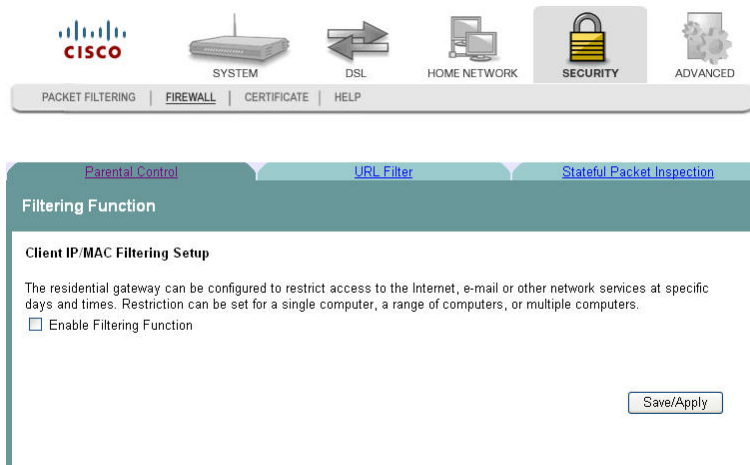


- 3 From the Outgoing IP Filtering screen, select **Remove** in the Remove column next to the filter you wish to remove.
- 4 Click **Remove** to remove the filter.

Parental Control Setup - Filtering Function

The Client IP/MAC Filtering Setup screen allows you to configure the residential gateway to restrict access to the Internet, email, or other network services at specific days and times. You can set time restrictions for a single computer, a range or computers, or multiple computers.

Path: Security > Firewall > Parental Control



Adding Time of Day Restrictions

The Filtering Function 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 residential 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, select the **Other MAC Address** option 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 > Firewall > Parental Control

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

Chapter 6 Security Configuration

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

The screenshot shows the Cisco router's configuration interface. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY (highlighted), and ADVANCED. Below this is a sub-menu with PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area is titled "MAC FILTERING" and has three tabs: MAC Filtering, Incoming IP Filtering, and Outgoing IP Filtering. The "MAC FILTERING" tab is active. The page contains the following text and controls:

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

[Add](#) [Remove](#)

- 2 Click the **Firewall** tab. The Filtering Function screen opens.

The screenshot shows the Cisco router's configuration interface. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below this is a sub-menu with PACKET FILTERING, FIREWALL (highlighted), CERTIFICATE, and HELP. The main content area is titled "Filtering Function" and has three tabs: Parental Control, URL Filter, and Stateful Packet Inspection. The "Filtering Function" tab is active. The page contains the following text and controls:

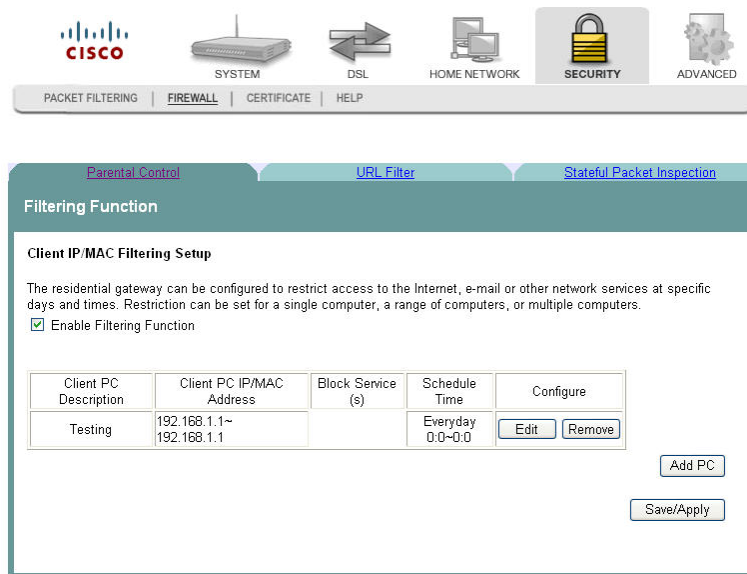
Client IP/MAC Filtering Setup

The residential gateway can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

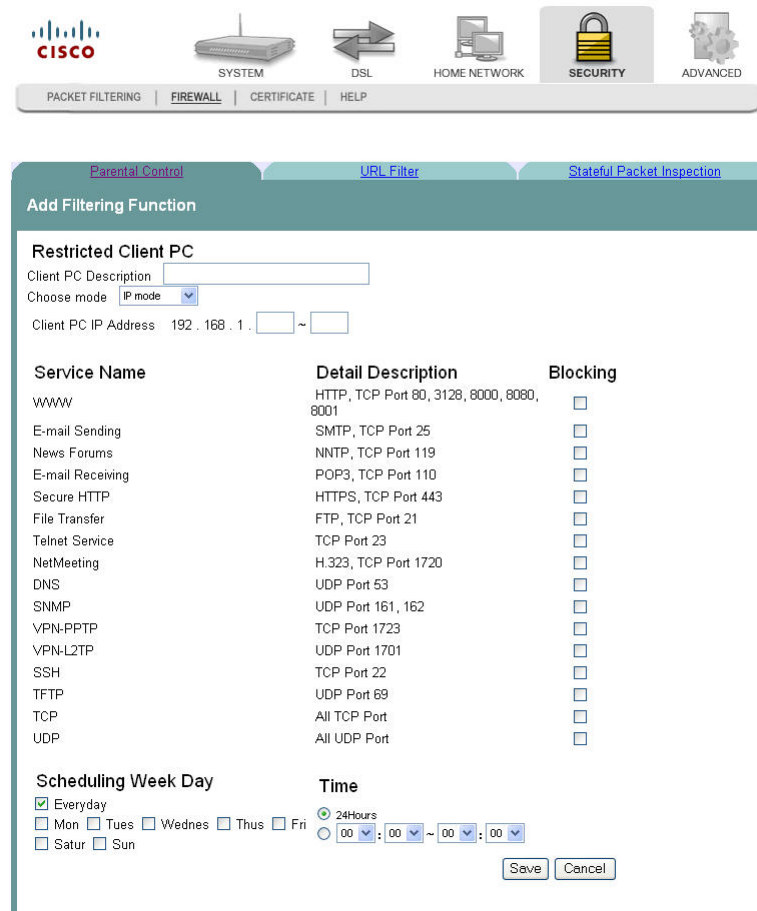
Enable Filtering Function

[Save/Apply](#)

- Check the **Enable Filtering Function** check box to enable the filtering function. The Client IP MAC Filtering screen populates with any time restrictions that are set.



- Click **Add PC**. The Add Filtering Function screen opens.



Chapter 6 Security Configuration

- 5 In the Client PC Description field, enter a description of the PC for which you want to block services.
- 6 In the Choose mode field, select IP mode or MAC mode from the drop-down menu.
- 7 Enter the IP address in the Client PC IP Address field, or enter the MAC address in the MAC address field depending upon the mode you selected in step 6.
- 8 Under Service Name area, check the **Blocking** check box for every service that you wish to filter.
- 9 In the Scheduling Week Day area, check the check boxes next to each day where you want to set up time of day restrictions. If you want to apply the time of day restrictions to everyday, check the Everyday check box. For example, check the F, Sa, and Su check boxes to apply time of day restrictions to Friday, Saturday, and Sunday.
- 10 In the Time area set the time as follows:
 - Click the 24Hours option to apply the restrictions 24 hours a day
 - Click the option where you select the time from the drop-down menus. Use the drop down menus to enter the time when you want the restriction to start and end.
- 11 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.

The screenshot shows the Cisco parental control interface. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY (highlighted), and ADVANCED. Below this is a sub-menu with PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area is titled 'MAC FILTERING' and includes the following text:

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

[Add](#) [Remove](#)

- 2 Click the **Firewall** tab. The Filtering Function screen opens.

The screenshot shows the Cisco parental control interface with the FIREWALL tab selected. The main content area is titled 'Filtering Function' and includes the following text:

Client IP/MAC Filtering Setup

The residential gateway can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

Enable Filtering Function

[Save/Apply](#)

Chapter 6 Security Configuration

- 3 Check the **Enable Filtering Function** check box to enable the filtering function. The Client IP/MAC Filtering Setup screen populates with any time restrictions that are set.

The screenshot shows the Cisco Firewall Configuration interface. At the top, there are navigation icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below these are tabs for PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area is titled "Filtering Function" and includes sub-tabs for Parental Control, URL Filter, and Stateful Packet Inspection. The "Client IP/MAC Filtering Setup" section contains a checkbox for "Enable Filtering Function" which is checked. Below this is a table with columns for Client PC Description, Client PC IP/MAC Address, Block Service (s), Schedule Time, and Configure. The table contains one entry: "Testing" with IP address "192.168.1.1~192.168.1.1" and schedule "Everyday 0:0~0:0". The Configure column for this entry has "Edit" and "Remove" buttons. There are also "Add PC" and "Save/Apply" buttons at the bottom right.

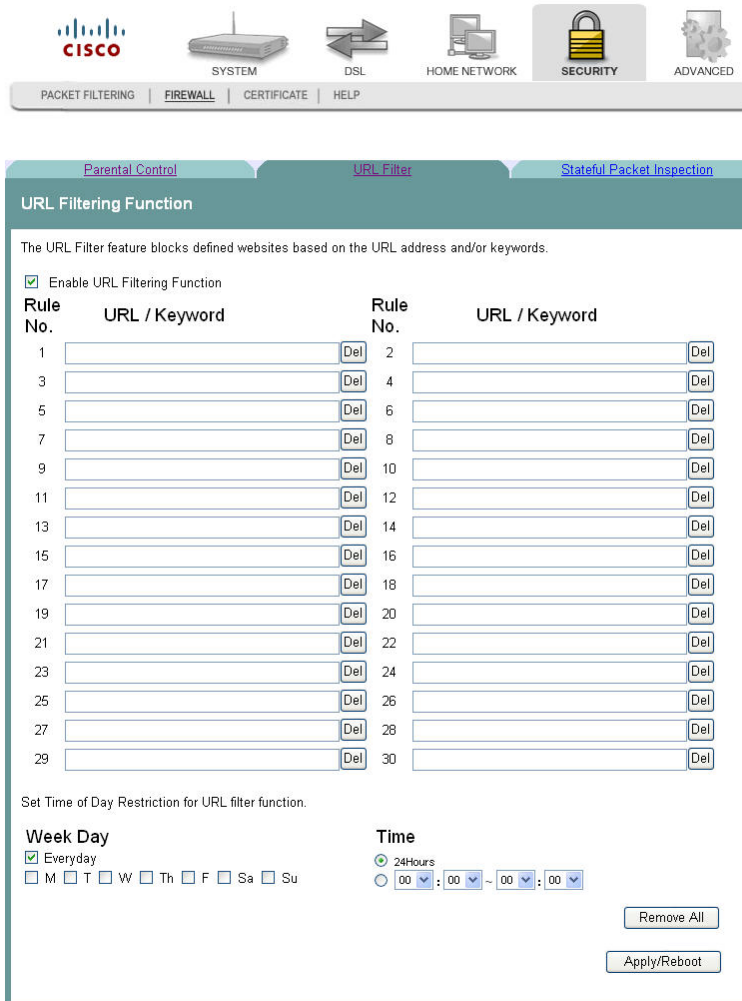
Client PC Description	Client PC IP/MAC Address	Block Service (s)	Schedule Time	Configure
Testing	192.168.1.1~192.168.1.1		Everyday 0:0~0:0	Edit Remove

- 4 From the Configure field select **Remove** in the Remove column next to the time of day restriction that you wish to remove.
- 5 Click **Remove** to remove the restriction.

URL Filtering Function

The URL Filtering Function screen allows you to block websites based on the URL address and/or key words used in the website. For example, if you have children in the home, you may want to block websites that are inappropriate for children by entering the URL or key words.

Path: Security > Firewall > URL Filter



Enabling URL Filtering

To enable URL filtering for the firewall, complete the following steps.

Chapter 6 Security Configuration

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

The screenshot shows the Cisco router's main menu with icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. The SECURITY icon is highlighted. Below the menu, the MAC Filtering configuration page is displayed. It includes a header with tabs for MAC Filtering, Incoming IP Filtering, and Outgoing IP Filtering. The main content area contains the following text:

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

[Add](#) [Remove](#)

- 2 Click the **Firewall** tab. The Filtering Function screen opens by default.

The screenshot shows the Cisco router's main menu with icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. The SECURITY icon is highlighted. Below the menu, the Firewall configuration page is displayed. It includes a header with tabs for Parental Control, URL Filter, and Stateful Packet Inspection. The main content area contains the following text:

Filtering Function

Client IP/MAC Filtering Setup

The residential gateway can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

Enable Filtering Function

[Save/Apply](#)

- 3 Click the **URL Filter** tab. The URL Filtering Function screen opens.
- 4 Click **Enable URL Filtering Function**. The URL Filtering Function screen updates with blank fields for entering the URLs that you want to block.

The URL Filter feature blocks defined websites based on the URL address and/or keywords.

Enable URL Filtering Function

Rule No.	URL / Keyword	Rule No.	URL / Keyword
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>
21	<input type="text"/>	22	<input type="text"/>
23	<input type="text"/>	24	<input type="text"/>
25	<input type="text"/>	26	<input type="text"/>
27	<input type="text"/>	28	<input type="text"/>
29	<input type="text"/>	30	<input type="text"/>

Set Time of Day Restriction for URL filter function.

Week Day
 Everyday
 M T W Th F Sa Su

Time
 24Hours
 00 : 00 - 00 : 00

Remove All
Apply/Reboot

- 5 For each rule, enter the URL or keyword that you want to block.
- 6 In the **Week Day** area, select Everyday or select the individual days on which you want the filter to take effect.
- 7 In the **Time** area, select 24Hours or select the individual times that you want the filter to take effect.
- 8 Click **Save**.

Removing a URL Filter

To remove a URL filter from the firewall, complete the following steps.

Chapter 6 Security Configuration

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

The screenshot shows the Cisco router's configuration interface. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY (highlighted), and ADVANCED. Below this is a sub-menu with PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area is titled "MAC FILTERING" and has three tabs: "MAC Filtering" (selected), "Incoming IP Filtering", and "Outgoing IP Filtering".

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

[Add](#) [Remove](#)

- 2 Click the **Firewall** tab. The Filtering Function screen opens by default.

The screenshot shows the Cisco router's configuration interface. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below this is a sub-menu with PACKET FILTERING, FIREWALL (highlighted), CERTIFICATE, and HELP. The main content area is titled "Filtering Function" and has three tabs: "Parental Control", "URL Filter", and "Stateful Packet Inspection".

Client IP/MAC Filtering Setup

The residential gateway can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

Enable Filtering Function

[Save/Apply](#)

- 3 Click the **URL Filter** tab. The URL Filtering Function screen opens.

- Click **Enable URL Filtering Function**. The URL Filtering Function screen updates with blank fields for entering the URLs that you want to block.

The URL Filter feature blocks defined websites based on the URL address and/or keywords.

Enable URL Filtering Function

Rule No.	URL / Keyword	Del	Rule No.	URL / Keyword	Del
1		Del	2		Del
3		Del	4		Del
5		Del	6		Del
7		Del	8		Del
9		Del	10		Del
11		Del	12		Del
13		Del	14		Del
15		Del	16		Del
17		Del	18		Del
19		Del	20		Del
21		Del	22		Del
23		Del	24		Del
25		Del	26		Del
27		Del	28		Del
29		Del	30		Del

Set Time of Day Restriction for URL filter function.

Week Day
 Everyday
 M T W Th F Sa Su

Time
 24Hours
 00 : 00 - 00 : 00

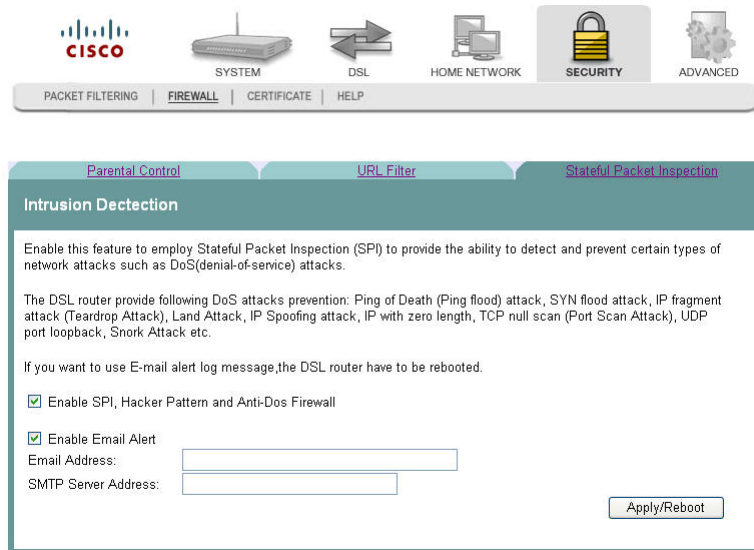
Remove All
 Apply/Reboot

- Click **Del** next to each rule that you want to delete. If you want to remove all the rules, click **Remove All**.
- Click **Save**.

Stateful Packet Inspection

The Stateful Packet Inspection screen allows the gateway to inspect packets passing through it to deny network attacks.

Path: Security > Firewall > Stateful Packet Inspection



Enabling Stateful Packet Inspection

To enable stateful packet inspection (SPI), complete the following steps.

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

The screenshot shows the Cisco router's main menu with the **SECURITY** tab selected. Below the menu, the **MAC FILTERING** configuration page is displayed. The page includes a header with tabs for **MAC Filtering**, **Incoming IP Filtering**, and **Outgoing IP Filtering**. The main content area explains that MAC Filtering is only effective on ATM PVCs in Bridge mode and defines **FORWARDED** and **BLOCKED** states. A checkbox for **Enable Filtering Function** is checked. The **MAC Filtering Global Policy** is set to **FORWARDED**, with a **Change Policy** button. Below this, a note says "Choose Add or Remove to configure MAC filtering rules." A table lists a single rule:

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

Buttons for **Add** and **Remove** are located below the table.

- 2 Click the **Firewall** tab. The Filtering Function screen opens by default.

The screenshot shows the Cisco router's main menu with the **FIREWALL** tab selected. Below the menu, the **Filtering Function** configuration page is displayed. The page has tabs for **Parental Control**, **URL Filter**, and **Stateful Packet Inspection**. The main content area is titled **Client IP/MAC Filtering Setup** and explains that the residential gateway can be configured to restrict access to the Internet, e-mail, or other network services. A checkbox for **Enable Filtering Function** is currently unchecked. A **Save/Apply** button is located at the bottom right of the configuration area.

Chapter 6 Security Configuration

- 3 Click the **Stateful Packet Inspection** tab. The Intrusion Detection screen opens.

The screenshot shows the Cisco DSL router configuration interface. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below this is a sub-menu with links for PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area is titled "Intrusion Detection" and contains the following text:

Enable this feature to employ Stateful Packet Inspection (SPI) to provide the ability to detect and prevent certain types of network attacks such as DoS(denial-of-service) attacks.

The DSL router provide following DoS attacks prevention: Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop Attack), Land Attack, IP Spoofing attack, IP with zero length, TCP null scan (Port Scan Attack), UDP port loopback, Snork Attack etc.

If you want to use E-mail alert log message,the DSL router have to be rebooted.

Enable SPI, Hacker Pattern and Anti-Dos Firewall

Enable Email Alert

Email Address:

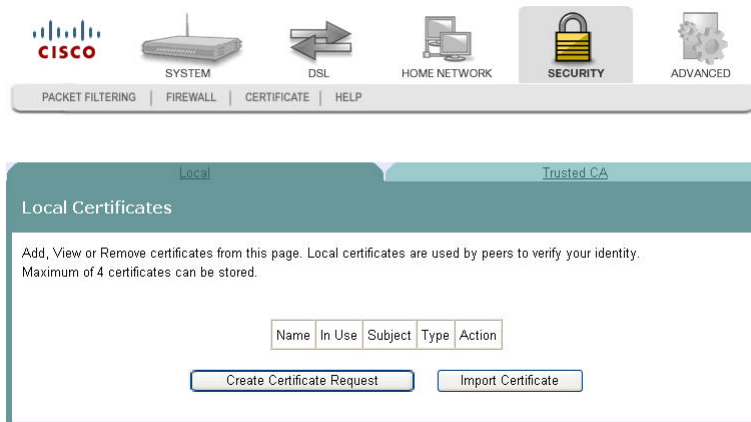
SMTP Server Address:

- 4 Select the **Enable SPI, Hacker Pattern and Anti-Dos Firewall** field.
- 5 Select the **Enable Email Alert** field and fill in the email address and SMTP server address that you want to notify when the DSL must be rebooted.
- 6 Click **Save/Apply** to enable stateful packet inspection.

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 on the residential gateway.

Path: Security > Certificate > Local > Local Certificates



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.

Chapter 6 Security Configuration

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

The screenshot shows the Cisco router's configuration interface. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY (highlighted), and ADVANCED. Below this is a sub-menu with PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area is titled 'MAC FILTERING' and includes tabs for 'MAC Filtering', 'Incoming IP Filtering', and 'Outgoing IP Filtering'. The text explains that MAC Filtering is only effective on ATM PVCs in Bridge mode and defines 'FORWARDED' and 'BLOCKED' states. A checkbox 'Enable Filtering Function' is checked. The global policy is set to 'FORWARDED', with a 'Change Policy' button. Below, a table shows a single rule with the following data:

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

Buttons for 'Add' and 'Remove' are located below the table.

- 2 Click **Add**. The Local Certificates screen opens.

The screenshot shows the 'Local Certificates' configuration page. The navigation bar is the same as in the previous screenshot, with 'SECURITY' highlighted. The sub-menu includes PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area has tabs for 'Local' (selected) and 'Trusted CA'. The text states: 'Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum of 4 certificates can be stored.' Below this is a table with the following headers: Name, In Use, Subject, Type, and Action. At the bottom, there are two buttons: 'Create Certificate Request' and 'Import Certificate'.

- Click **Create Certificate Request**. The Create New Certificate Request screen opens.

The screenshot shows the Cisco configuration interface for a residential gateway. The top navigation bar includes icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below this, the 'Create New Certificate Request' screen is active. The screen has two tabs: 'Local' and 'Trusted_CA'. The main content area contains the following text: 'To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.' Below this text are five input fields: 'Certificate Name:', 'Common Name:', 'Organization Name:', 'State/Province Name:', and 'Country/Region Name:'. The 'Country/Region Name' field is a dropdown menu currently showing 'US (United States)'. An 'Apply' button is centered at the bottom of the form.

- In the Certificate Name field, enter the name for the certificate.
- In the Common Name field, enter the common name of the certificate.
- In the Organization Name field, enter the name of the organization that owns the certificate.
- In the State/Province Name field, enter the state or province where you want to register the certificate.
- In the Country/Region Name field, use the drop-down list to select the country or region where you want to register the certificate.
- Click **Apply** to create the certificate. The certificate signing request screen opens.

The screenshot shows the 'Certificate signing request' screen. At the top, it says 'Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.' Below this is a table with the following data:

Name	Test
Type	request
Subject	CN=Test/O=Test/ST=Georgia/C=US

Below the table, the 'Signing Request' field contains the following base64-encoded text:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBEDCBgIBADAHQgoCvYVQDQDEwR0ZXRhbnQwCvYVQDQDEwR0ZXRhbnQw
YVQDQDEwR0ZXRhbnQwCvYVQDQDEwR0ZXRhbnQwYVQDQDEwR0ZXRhbnQw
gR0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEw
R0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEw
R0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEw
R0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEw
R0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEw
R0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEw
R0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEw
R0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEwR0ZXRhbnQwYVQDQDEw
-----END CERTIFICATE REQUEST-----
```

At the bottom of the screen, there are two buttons: 'Back' and 'Load Signed Certificate'.

- 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.

The screenshot shows the Cisco configuration interface. At the top, there are icons for SYSTEM, DSL, HOME NETWORK, SECURITY (highlighted), and ADVANCED. Below these are tabs for PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area is titled 'MAC FILTERING' and has sub-tabs for 'MAC Filtering', 'Incoming IP Filtering', and 'Outgoing IP Filtering'. The 'MAC Filtering' sub-tab is active. The page contains the following text and controls:

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	<input type="checkbox"/>

[Add](#) [Remove](#)

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

The screenshot shows the Cisco configuration interface. At the top, there are icons for SYSTEM, DSL, HOME NETWORK, SECURITY (highlighted), and ADVANCED. Below these are tabs for PACKET FILTERING, FIREWALL, CERTIFICATE, and HELP. The main content area is titled 'Local Certificates' and has sub-tabs for 'Local' and 'Trusted CA'. The 'Local' sub-tab is active. The page contains the following text and controls:

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum of 4 certificates can be stored.

Name	In Use	Subject	Type	Action
Create Certificate Request Import Certificate				

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

Local Trusted CA

Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

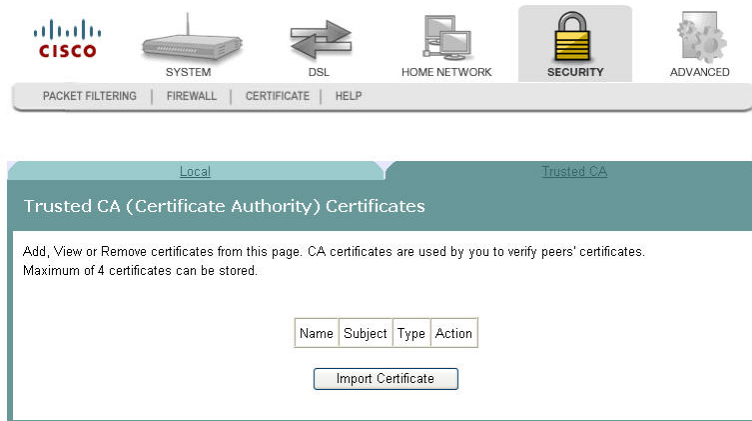
Apply

- 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 Trusted CA (Certificate Authority) Certificates screen 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 > Trusted CA (Certificate Authority) Certificates



Importing Trusted CA Certificates

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