

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

The screenshot shows the Cisco router's main menu with 'SECURITY' selected. Below the menu, there are tabs for 'MAC Filtering', 'Incoming IP Filtering', and 'Outgoing IP Filtering'. The 'MAC Filtering' tab is active, displaying the following content:

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

The screenshot shows the Cisco router's main menu with 'CERTIFICATE' selected. Below the menu, there are tabs for 'Local' and 'Trusted CA'. The 'Local' tab is active, displaying the following content:

**Local Certificates**

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
<a href="#">Create Certificate Request</a> <a href="#">Import Certificate</a>				

## Chapter 6 Security Configuration

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



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



- 5 In the Certificate Name field, enter the name of the certificate.
- 6 In the Certificate area, copy and paste the contents of the certificate file provided by the service provider.
- 7 Click **Apply** to save the CA certificate on the residential gateway.

# 7

## Advanced Configuration

The Advanced tab lets you to check the quality of service and IP traffic over your network and change the configuration.

Use this chapter to check the status of the more advanced features of your residential gateway, such as port mapping and DNS server configuration, and to change the configuration.

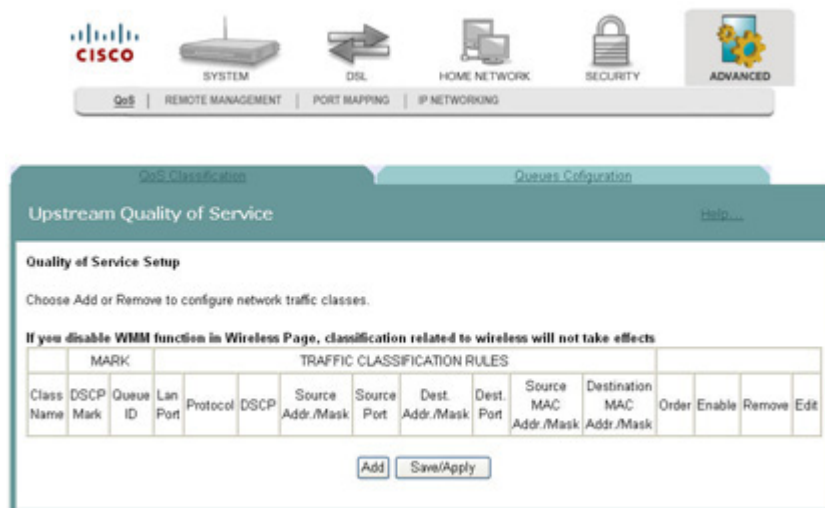
### In This Chapter

■ Upstream Quality of Service .....	182
■ Remote Management .....	186
■ Port Mapping .....	188
■ Virtual Servers Setup.....	191
■ Port Triggering Setup.....	195
■ DMZ Host Setup .....	199
■ DNS Server Configuration .....	200
■ DNS Entries .....	201
■ Dynamic DNS.....	202
■ Nslookup.....	205
■ Default Gateway Routing .....	206
■ Static Route .....	208
■ Ping .....	209
■ Internet Group Management Protocol.....	211
■ IPsec Settings.....	213

## Upstream Quality of Service

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

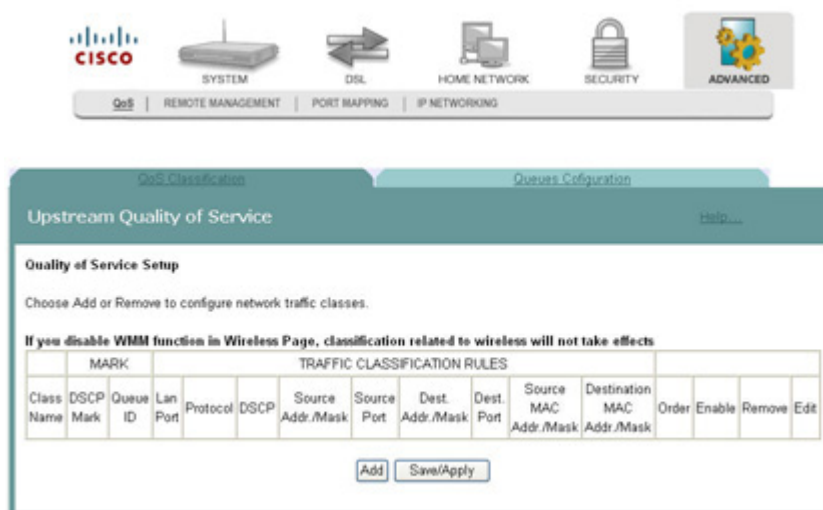
**Path:** Advanced > QoS > Upstream Quality of Service



## Adding Upstream Quality of Service Settings

To add upstream Quality of Service settings, complete the following steps.

- 1 Click **Advanced** on the main screen. The Upstream Quality of Service screen opens.



- 2 Click **Add**. The Add Upstream QoS Rule screen opens.

The screenshot shows the 'Add Upstream QoS Rule' configuration page. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below the navigation bar, the form is titled 'Add Upstream QoS Rule'. The form contains the following fields and options:

- Name:** A text input field.
- LAN Port:** A dropdown menu.
- Protocol:** A dropdown menu.
- Source:** A group of fields for source configuration:
  - IP Address : Text input
  - Subnet Mask : Text input
  - Port Number : Text input
  - MAC address: Text input
  - MAC Mask: Text input
- Destination:** A group of fields for destination configuration:
  - IP Address : Text input
  - Subnet Mask : Text input
  - Port Number : Text input
  - MAC address: Text input
  - MAC Mask: Text input
- DSCP Check :** A dropdown menu.
- Marker:**  checkbox
- Queue:**  checkbox
- SAVE:** A button at the bottom center.

- 3 In the Name field, enter the name of the QoS rule.
- 4 In the LAN Port field, select the LAN port for which you want to apply the rule.
- 5 In the Protocol field, select the protocol that you want to use from the following options:
  - TCP/UDP
  - TCP
  - UDP
  - ICMP
- 6 In the IP Address field, enter the source and destination addresses.
- 7 In the Subnet Mask field, enter the source and destination subnet masks.
- 8 In the Port Number field, enter the source and destination ports.
- 9 In the MAC address field, enter the MAC address for the source from which the packets are being sent and the MAC address for the destination. The MAC address should be in the form of 6 pairs of hex digits. For example, aa:ee:ff:11:03:24.

## Chapter 7 Advanced Configuration

- 10 In the MAC Mask field, enter the mask for the source MAC address from which the packets are being sent and the MAC Mask for the destination MAC address. A MAC mask of ff:ff:ff:00:00:00 matches all devices made by the same manufacturer (identified by the first three pairs of the MAC address). A MAC mask of ff:ff:ff:ff:ff:ff matches a single device.
- 11 In the DSCP Check field, select the matching DSCP value from the list of Diffserv code point.
- 12 Select the **Marker** field and choose from the list of Diffserv code point (DSCP) values to mark the specified data flow.
- 13 Select the **Queue** field and choose from the list of queues.
- 14 Click **Save**.

## Queues Configuration

Use Queues Configuration to configure QoS queues for each WAN connection type. By configuring the queues, you determine how the packets will be processed according to the assigned priorities. A queue with a higher priority has lower queue precedence.

**Path:** Advanced > QoS > Queues Configuration

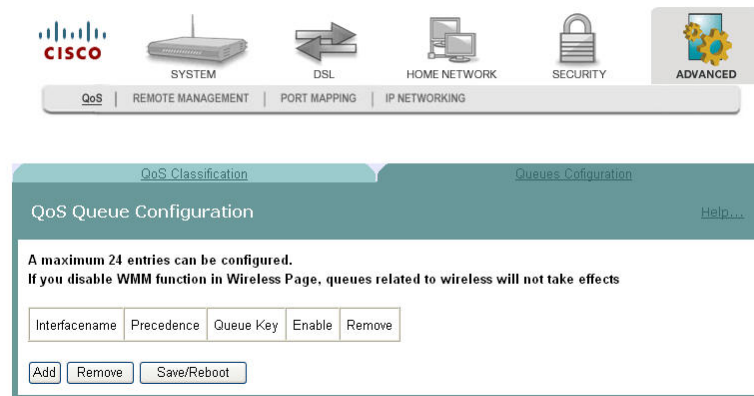
To set up your queues, complete the following steps.

- 1 Click **Advanced** on the main screen. The Upstream Quality of Service screen opens.

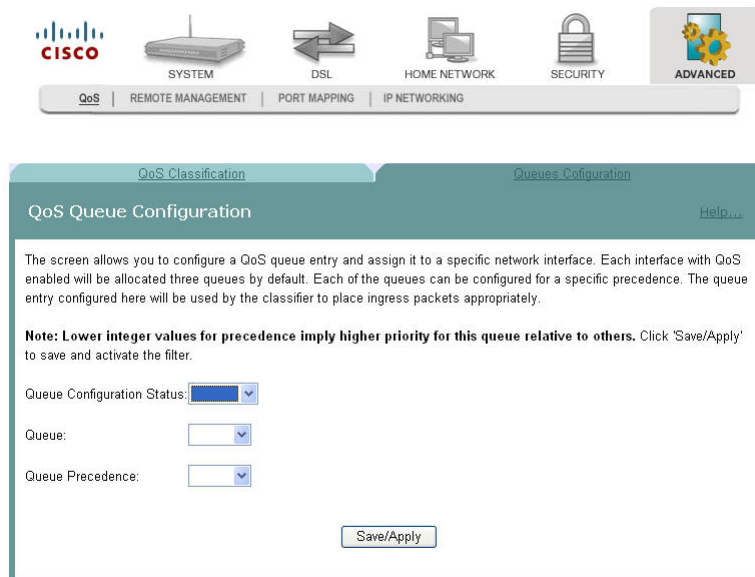
The screenshot shows the Cisco QoS configuration interface. At the top, there is a navigation bar with icons for QoS, REMOTE MANAGEMENT, PORT MAPPING, IP NETWORKING, SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. The 'ADVANCED' icon is highlighted. Below the navigation bar, the 'Upstream Quality of Service' screen is displayed. The screen has a teal header with 'Upstream Quality of Service' and a 'Help...' link. The main content area is titled 'Quality of Service Setup' and contains the following text: 'Choose Add or Remove to configure network traffic classes.' Below this, there is a warning: 'If you disable WMM function in Wireless Page, classification related to wireless will not take effects'. A table with 16 columns is shown, with the first two columns under 'MARK' and the remaining 14 under 'TRAFFIC CLASSIFICATION RULES'. The columns are: Class Name, DSCP Mark, Queue ID, Lan Port, Protocol, DSCP, Source Addr./Mask, Source Port, Dest. Addr./Mask, Dest. Port, Source MAC Addr./Mask, Destination MAC Addr./Mask, Order, Enable, Remove, and Edit. At the bottom of the table, there are two buttons: 'Add' and 'Save/Apply'.

MARK		TRAFFIC CLASSIFICATION RULES													
Class Name	DSCP Mark	Queue ID	Lan Port	Protocol	DSCP	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	Order	Enable	Remove	Edit

- 2 Click **Queues Configuration**. The Queues Configuration screen opens.



- 3 Click **Add** to add a queue.



- 4 For the Queue Configuration Status, select **Enable** or **Disable** to enable or disable your queue configuration.
- 5 Select from the Queue drop-down list for the associated WAN interface or connection type for Queue.
- 6 For the Queue Precedence field, select the Precedence as the relative priority for the queue. A smaller number indicates a higher priority.
- 7 Click **Save/Apply** to save the changes.

## Remote Management

The Remote Management -- TR-069 Client screen allows an auto-configuration server (ACS) to perform auto-configuration, provisioning, collection of statistics, and diagnostics for this residential gateway.

**Path:** Advanced > Remote Management



Remote Management -- TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provisioning, collection, and diagnostics to this device.

Select the desired values and click "Save/Apply" to configure the TR-069 client options.

Inform:  Disable  Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

### Configuring the TR-069 Client Options

To configure the TR-069 client options, complete the following steps.



- 1 Click **Advanced** on the main screen. The Remote Management -- TR-069 Client screen opens.



Remote Management -- TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provisioning, collection, and diagnostics to this device.

Select the desired values and click "Save/Apply" to configure the TR-069 client options.

Inform  Disable  Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

- 2 In the Inform field, choose one of the following options:
  - Click **Enable** to enable the periodic "inform" messages from the residential gateway.
  - Click **Disable** to disable the inform messages to the residential gateway.
- 3 In the Inform Interval field, enter the frequency that the inform messages are sent from the residential gateway to the auto-configuration server.
- 4 In the ACS URL field, enter the URL for the auto-configuration server.
- 5 In the ACS User Name field, enter the user name for auto-configuration server.
- 6 In the ACS Password field, enter the password for the auto-configuration server.
- 7 Check the **Connection Request Authentication** field.
- 8 In the Connection Request User Name field, enter the name of the connection request.
- 9 In the Connection Request Password field, enter the password for the connection request.
- 10 Click **GetRPCMethods** to obtain the list of remote procedural calls (RPC) supported by the auto-configuration server.
- 11 Click **Save/Apply** to save the configuration changes.

## Port Mapping

The Port Mapping screen allows you to specify which traffic will be transmitted over the WAN interface. Traffic is classified by ingress port, such as Ethernet port, or by DHCP option settings. Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces.

**Path:** Advanced > Port Mapping



Port Mapping

**Port Mapping -- A maximum 16 entries can be configured**

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has an IP interface.

Enable virtual ports on

Group Name	Enable/Disable	Remove	Edit	Interfaces	Enable/Disable
Default				USB	<input checked="" type="checkbox"/>
				eth0	<input checked="" type="checkbox"/>
				Wireless	<input checked="" type="checkbox"/>
				LAN3	<input checked="" type="checkbox"/>
				LAN1	<input checked="" type="checkbox"/>
				LAN4	<input checked="" type="checkbox"/>
IPTV	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/>	HPNA	<input checked="" type="checkbox"/>
				nas_0_8_35	<input checked="" type="checkbox"/>

(√LAN-ID only)

## Adding Port Mapping

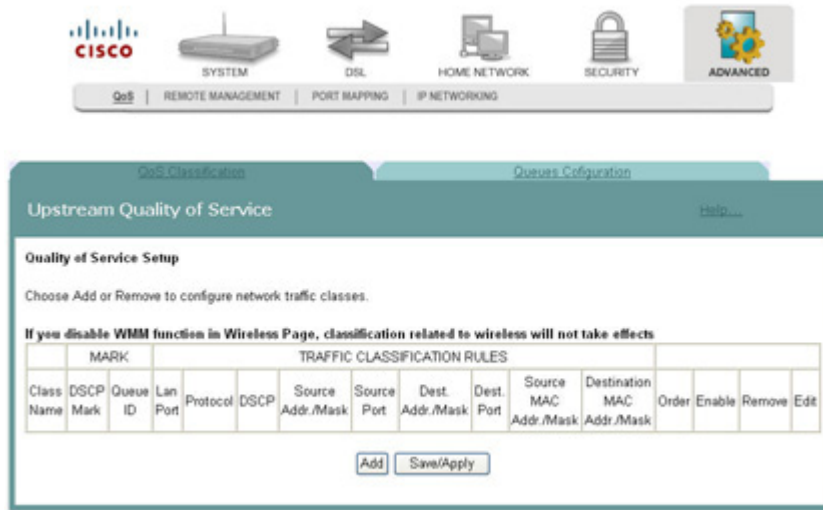
To add port mapping, complete the following steps.



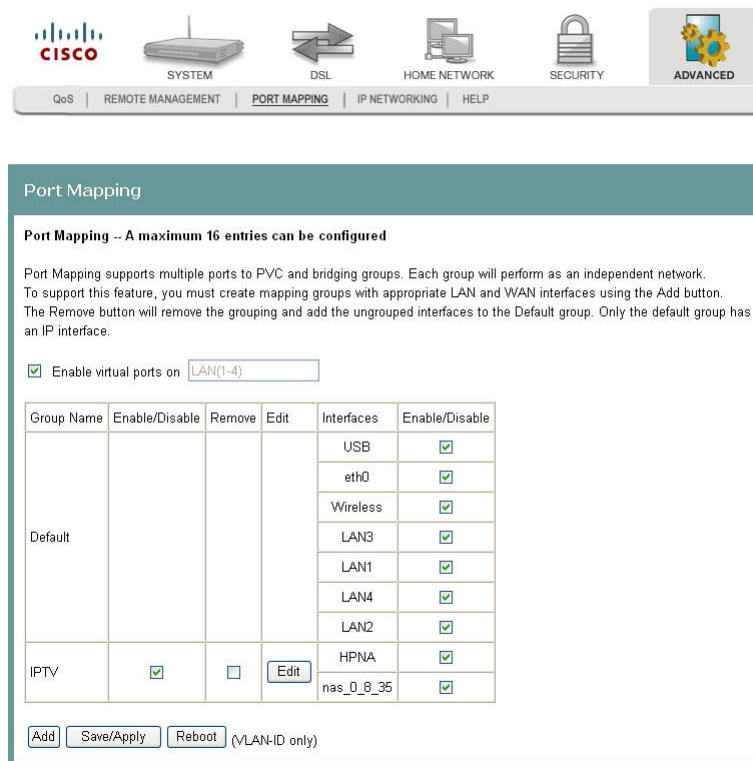
**CAUTION:**

**This procedure is for administrators only. Incorrectly using this function can adversely affect your system operation.**

- 1 Click **Advanced** on the main screen. The Upstream Quality of Service screen opens.



- 2 Click the **Port Mapping** tab. The Port Mapping screen opens.



- 3 Click **Add**. The Port Mapping Configuration screen opens.

**Port Mapping Configuration**

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.  
**Note that these clients may obtain public IP addresses**
3. Click Save/Apply button to make the changes effective immediately

**Note that the selected interfaces will be removed from their existing groups and added to the new group.**

**IMPORTANT** If a vendor ID is configured for a specific client device, please **REBOOT** the client device attached to the residential gateway to allow it to obtain an appropriate IP address.

Group Name:

Grouped Interfaces	Available Interfaces
<input type="text"/>	LAN3 LAN1 LAN4 LAN2 HPNA nes_0_8_35 Wireless USB

Automatically Add Clients With the following DHCP Vendor IDs

- 4 In the Group Name field, enter the name of the group. The group name must be unique. For example, enter IPTV.
- 5 For the Grouped Interfaces field, select interfaces from the Available Interfaces list and add them to the grouped interface list using the arrow buttons to create the required mapping of the ports.
- 6 In the Automatically Add Clients With the following DHCP Vendor IDs fields, add the DHCP option 60 [vendor ID option] string for the devices (typically IP set-tops) attached to the residential gateway.
- 7 Click **Save/Apply**.

## Virtual Servers Setup

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

**Path:** Advanced > IP Networking > NAT > Virtual Servers

**NAT -- Virtual Servers Setup**

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remote Host	Remove
Active Worlds	3000	3000	TCP	3000	3000	192.168.1.1		<input type="checkbox"/>
Active Worlds	5670	5670	TCP	5670	5670	192.168.1.1		<input type="checkbox"/>
Active Worlds	7777	7777	TCP	7777	7777	192.168.1.1		<input type="checkbox"/>
Active Worlds	7000	7000	TCP	7000	7000	192.168.1.1		<input type="checkbox"/>

## Adding a Virtual Server

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

- 1 Click **Advanced** on the main screen.
- 2 Click **IP Networking**. The NAT screen opens.

**NAT**

- [Virtual Servers](#)
- [Port Triggering](#)
- [DMZ Host](#)

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

**NAT -- Virtual Servers Setup**

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remote Host	Remove
Active Worlds	3000	3000	TCP	3000	3000	192.168.1.1		<input type="checkbox"/>
Active Worlds	5670	5670	TCP	5670	5670	192.168.1.1		<input type="checkbox"/>
Active Worlds	7777	7777	TCP	7777	7777	192.168.1.1		<input type="checkbox"/>
Active Worlds	7000	7000	TCP	7000	7000	192.168.1.1		<input type="checkbox"/>

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

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**  
Remaining number of entries that can be configured:28

Server Name:

Select a Service:

Custom Server:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

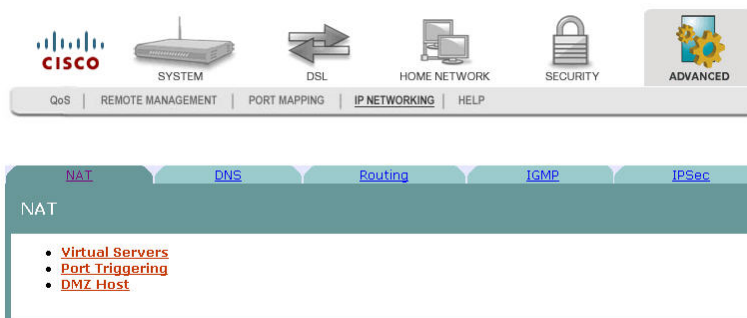
- 5 Under Server Name, choose one of the following:
- Click **Select a Service**, and choose a service from the drop-down list.
- OR
- Click **Custom Server**, and enter a server name and the Server IP Address.
- 6 In the Server IP Address field, enter the IP address for the server.
- 7 In the External Port Start/End fields, assign the external (Internet) port range of numbers that are associated with the service. These are the ports which will be used for receiving the service request from the WAN. If you have chosen to Select a Service from the above selection, the ports will be entered automatically for you.
- 8 Under Protocol, select TCP, UDP, or TCP/UDP.
- 9 In the Internet Port Start/End fields, assign the internal (LAN) port range of numbers that are associated with the service. These are the ports which the actual LAN server defines. If you have chosen to Select a Service from the above selection, the ports will be entered automatically for you.

- 10 In the Remote IP field, enter the service request (client) sender's IP address. Leave it blank to accept all incoming service requests regardless of the senders' IP address.
- 11 Click **Save/Apply** to add the virtual server.

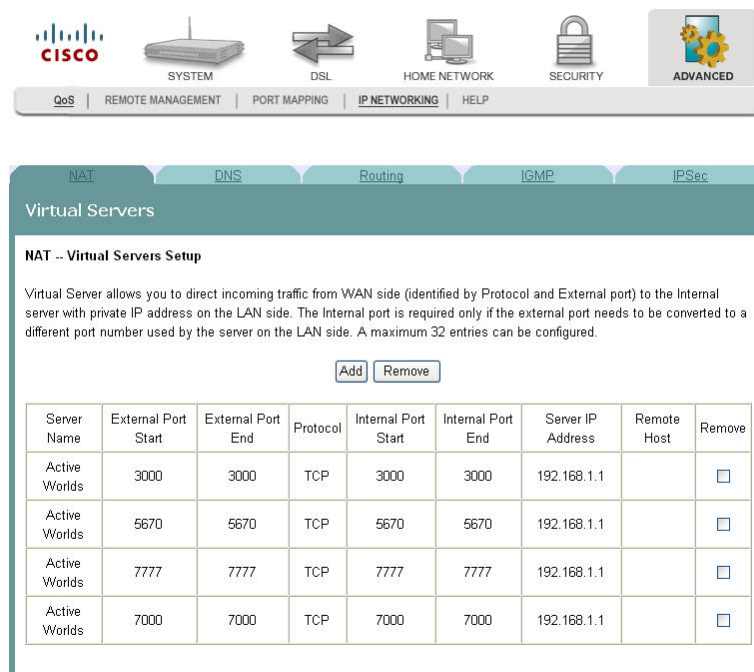
## Removing a Virtual Server

To remove a virtual server, complete the following steps.

- 1 Click **Advanced** on the main screen.
- 2 Click **IP Networking**. The NAT screen opens.



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



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

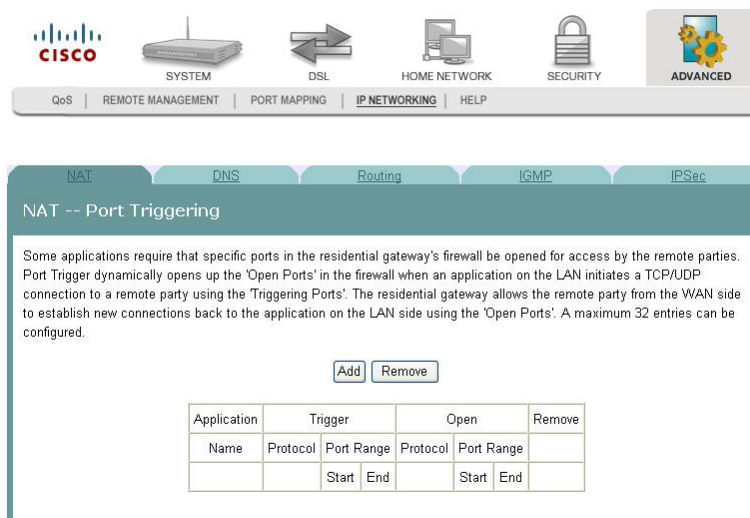


## Port Triggering Setup

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

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

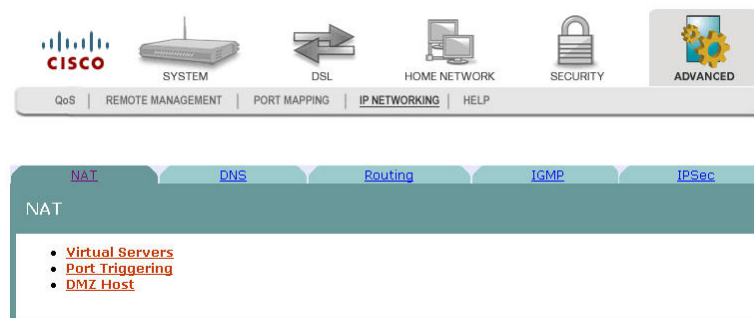
**Path:** Advanced > IP Networking > NAT > Port Triggering > NAT -- Port Triggering



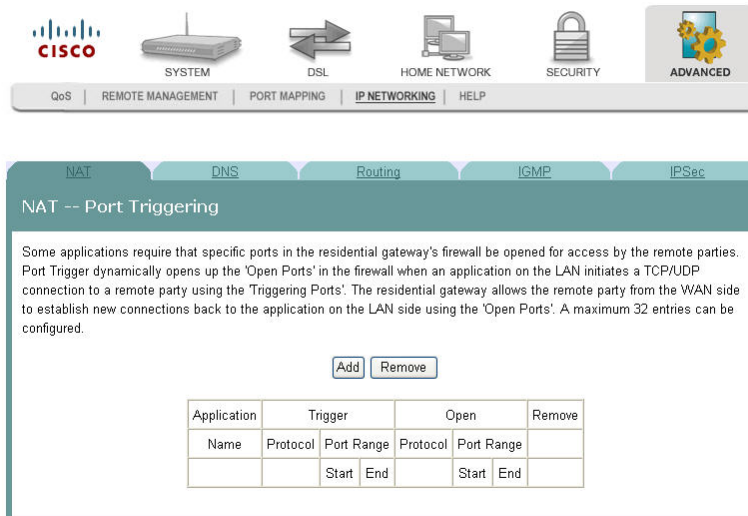
## Opening a Port on the Firewall

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

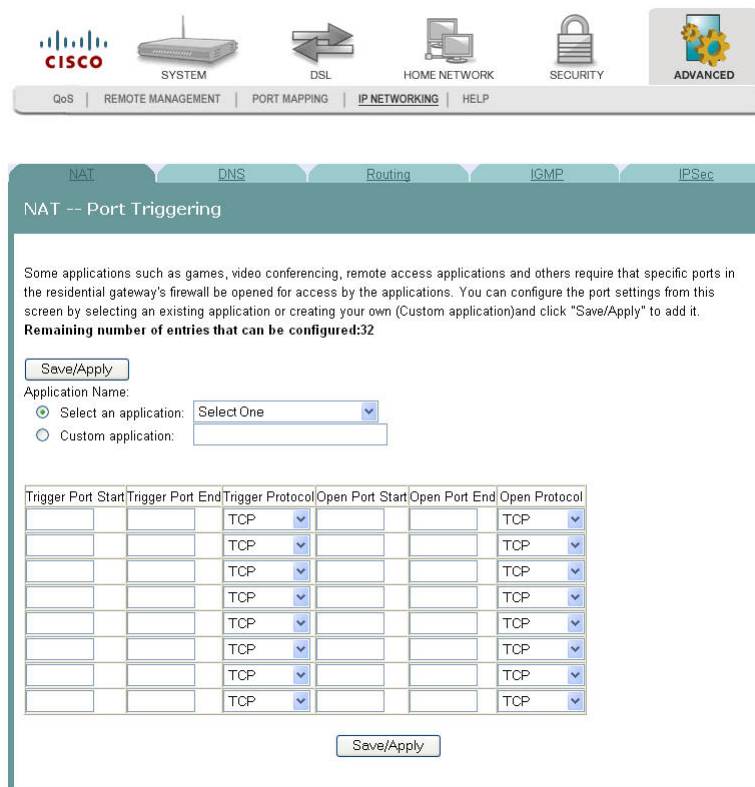
- 1 Click **Advanced** on the main screen.
- 2 Click **IP Networking**. The NAT screen opens.



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



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



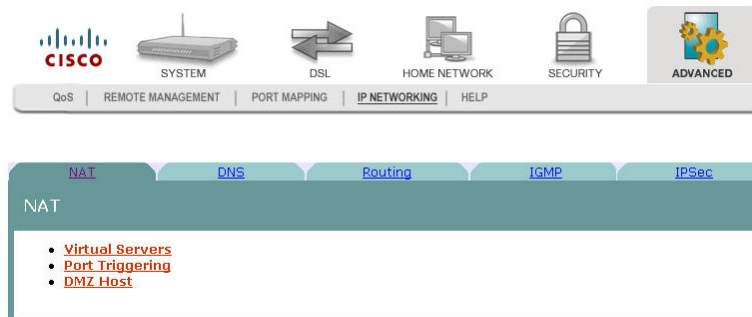
- 5 Under Application Name, choose one of the following:
  - Click **Select an Application** and choose an application from the drop-down list.
  - OR
  - Click **Custom Application**, and enter a name for the application.

- 6 Complete the fields on the screen as follows:
  - Under Trigger Port Start, enter the triggering port (start) that will cause the residential gateway to open up the incoming port for the particular LAN computer.
  - Under Trigger Port End, enter the triggering port (end) that will cause the residential gateway to open up the incoming port for the particular LAN computer.
  - Under Trigger Protocol, select **TCP/UDP**, **TCP** or **UDP**.
  - Under Open Port Start, enter the starting port number of the service you want to open on the firewall.
  - Under Open Port End, enter the ending port number of the service you want to open on the firewall.
  - Under Open Protocol, select **TCP/UDP**, **TCP** or **UDP**.
- 7 Click **Save/Apply** to open the ports on the firewall.

## Closing a Port on the Firewall

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

- 1 Click **Advanced** on the main screen.
- 2 Click **IP Networking**. The NAT screen opens.



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

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

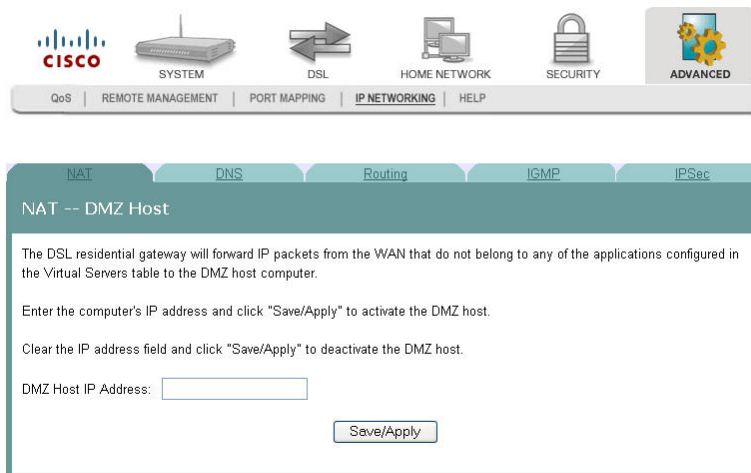
Application	Trigger		Open		Remove		
	Name	Protocol	Port Range	Protocol		Port Range	
			Start	End	Start	End	
Aim Talk	TCP	4099	4099	TCP	5191	5191	<input type="checkbox"/>

- 4 From the NAT -- Port Triggering screen, click **Remove** in the Remove column next to the port you wish to close.
- 5 Click **Remove**. The port you selected is closed.

## DMZ Host Setup

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

**Path:** Advanced > IP Networking > NAT > DMZ Host > NAT -- DMZ Host



### Activate the DMZ Host

In the DMZ Host IP Address field, enter the computer's IP address and click **Save/Apply** to activate the DMZ host.

### Deactivate the DMZ Host

Clear the DMZ Host IP Address field and click **Save/Apply** to deactivate the DMZ host.

## DNS Server Configuration

The DNS Server Configuration screen allows you to configure the Domain Name Server (DNS).

If the Enable Automatic Assigned DNS check box is checked, the residential gateway will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the check box is not checked, enter the primary and optional secondary IP address or domain name address of the DNS server to establish connection. Click **Save** to save the new configuration. You must reboot the residential gateway to make the new configuration effective.

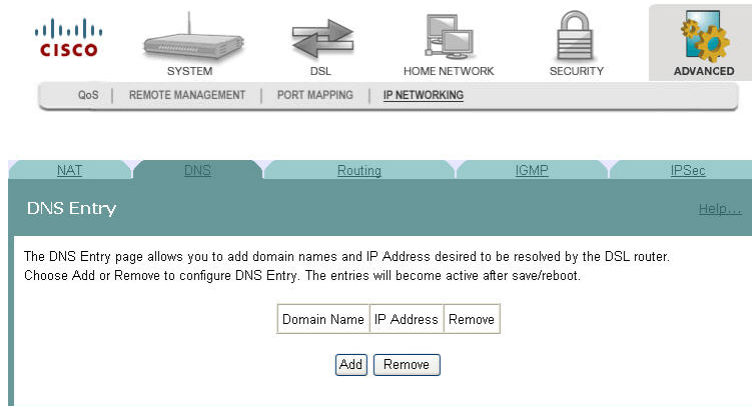
**Path:** Advanced > IP Networking > DNS > DNS Server

The screenshot shows the Cisco web interface for DNS Server Configuration. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below this is a menu bar with options: QoS, REMOTE MANAGEMENT, PORT MAPPING, IP NETWORKING (selected), and HELP. The main content area has tabs for NAT, DNS (selected), Routing, IGMP, and IPSec. The title is "DNS Server Configuration". Below the title is a paragraph of text explaining the "Enable Automatic Assigned DNS" checkbox. There is a checkbox labeled "Enable Automatic Assigned DNS" which is currently unchecked. Below this are two input fields: "Primary DNS server:" with the value "192.168.1.254" and "Secondary DNS server:" with the value "192.168.1.254". At the bottom center is a "Save" button.

## DNS Entries

The DNS Entries page allows you to add domain names and the IP addresses to be resolved by the Gateway. You could add a DNS entry by entering the Domain name and the corresponding IP address in the fields. Click **Save/Apply** to save your settings.

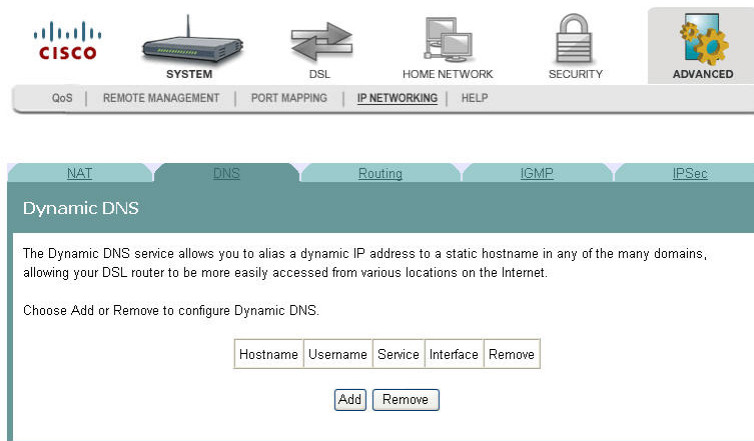
**Path:** Advanced > IP Networking > DNS > DNS Entries



## Dynamic DNS

The Dynamic DNS screen allows you to alias a dynamic IP address to a static hostname in any of the many domains. The alias allows your DSL router to be more easily accessed from various locations on the Internet.

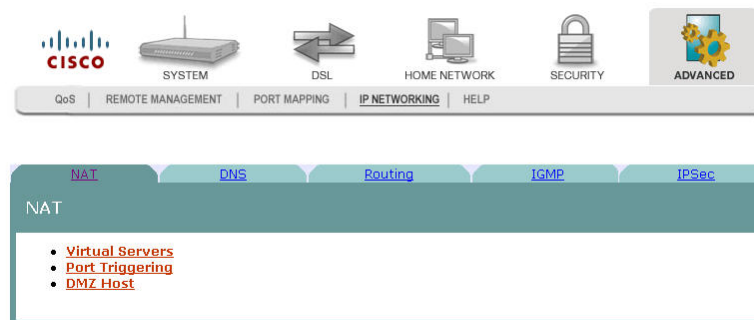
**Path:** Advanced > IP Networking > DNS > Dynamic DNS



## Adding an Alias for A Dynamic IP Address to a Static Host Name

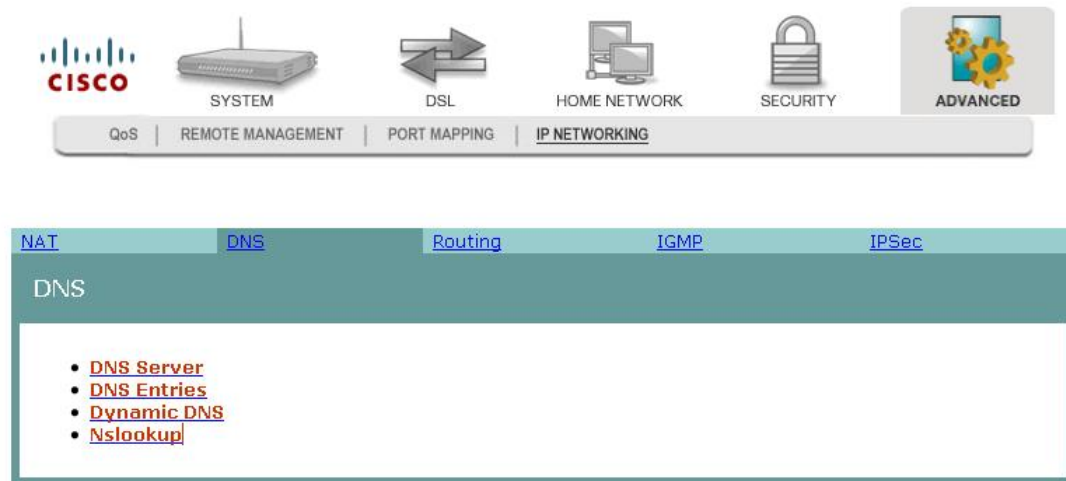
To alias a dynamic IP address to a static host name, complete the following steps.

- 1 Click **Advanced** on the main screen.
- 2 Click **IP Networking**. The NAT screen opens.

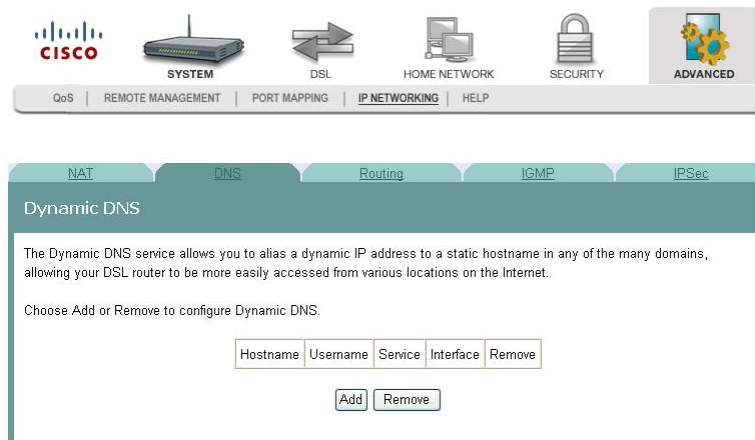




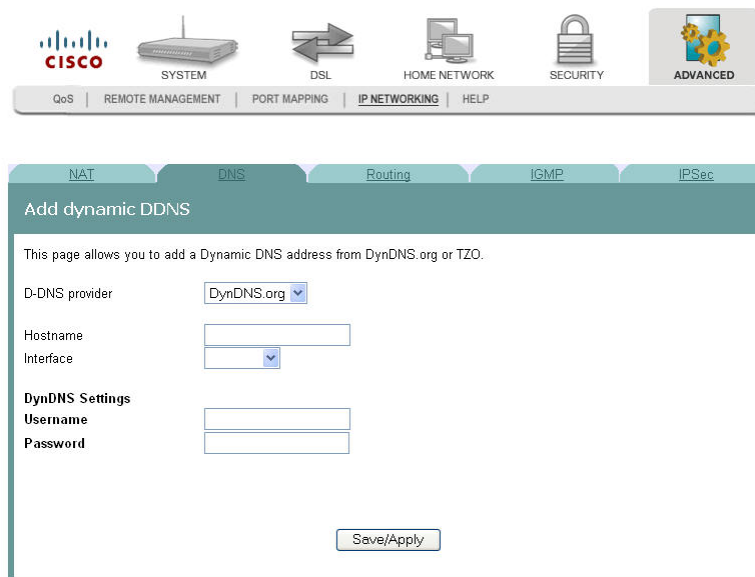
3 Click **DNS**. The DNS screen opens.



4 Click **Dynamic DNS**. The Dynamic DNS screen opens.



5 Click **Add** on the Dynamic DNS screen. The Add dynamic DDNS screen opens.



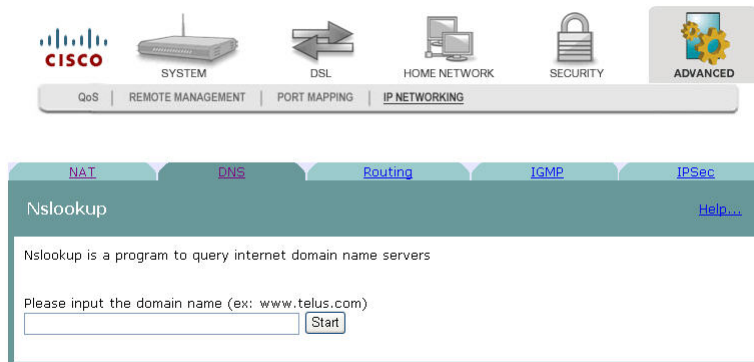
## Chapter 7 Advanced Configuration

- 6 In the D-DNS provider field, select the provider from the drop-down list.
- 7 In the Hostname field, enter the name of the host.
- 8 In the Interface field, select the interface from the drop-down list.
- 9 Under DynNDS Settings, enter your user name and password.
- 10 Click **Save/Apply**.

## Nslookup

The Nslookup tool is a utility to look up information in the DNS (Domain Name System). Basically, DNS maps domain names to IP addresses. Type in the domain name in the field, and press **Start** to look up the IP address.

**Path:** Advanced > IP Networking > DNS > Nslookup

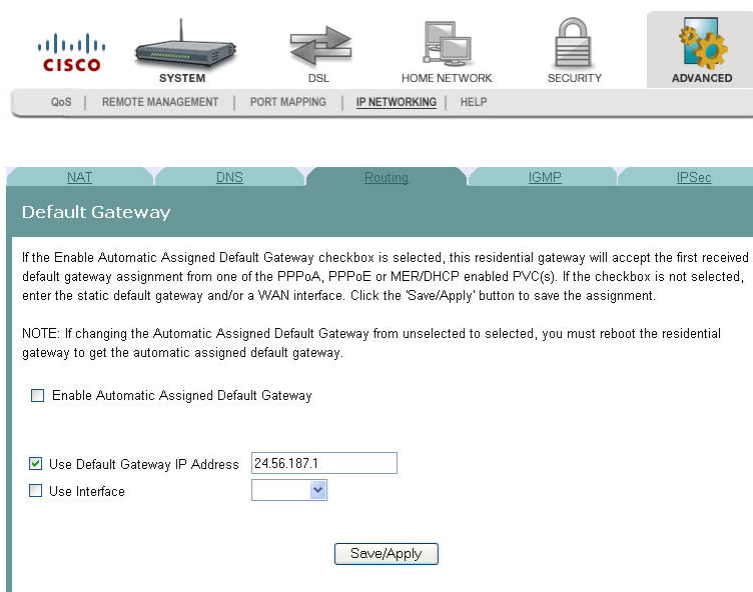


## Default Gateway Routing

The Default Gateway screen allows you to make gateway assignments for devices that are connected to the residential gateway.

**Note:** If you change the Enable Automatic Assigned Default Gateway check box from unselected to selected, you must reboot the router to get the automatic assigned default gateway.

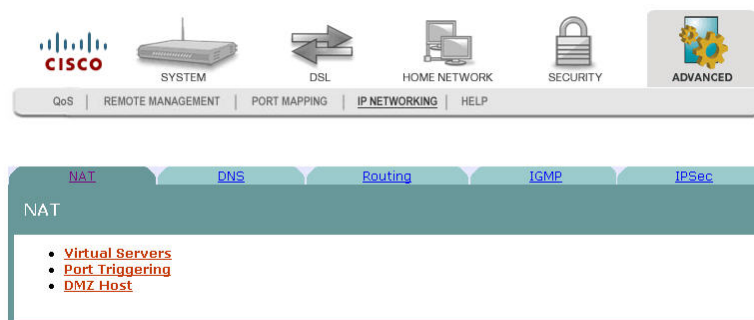
**Path:** Advanced > IP Networking > Routing > Default Gateway



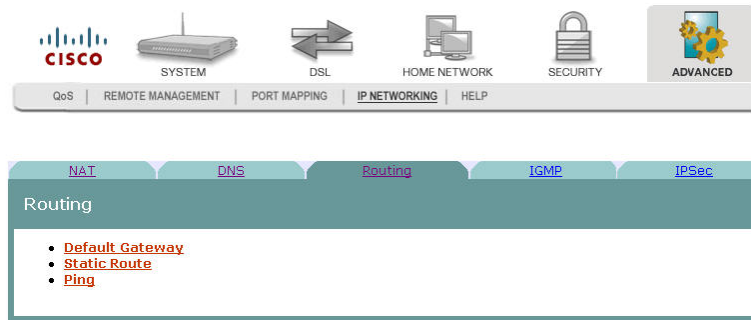
### Assigning Default Gateways

To assign a default gateway, complete the following steps.

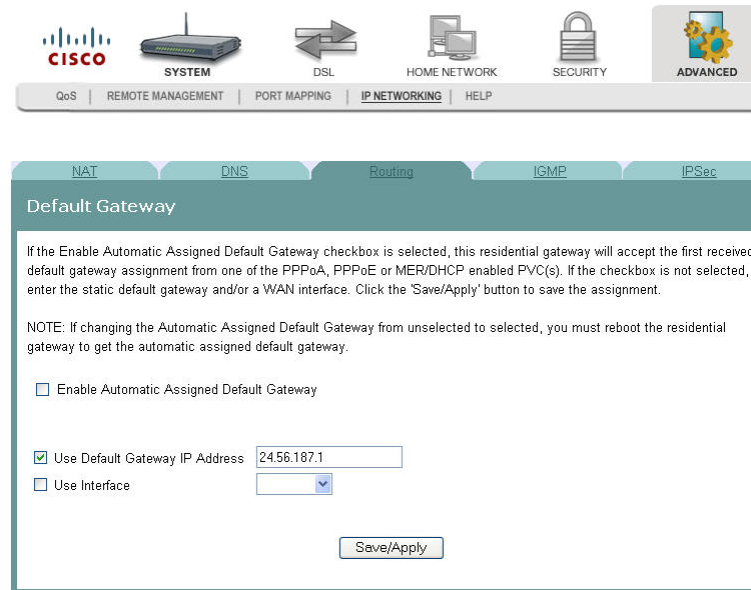
- 1 Click **Advanced** on the main screen.
- 2 Click **IP Networking**. The NAT screen opens.



- 3 Click **Routing**. The Routing screen opens.



- 4 Click **Default Gateway**. The Default Gateway screen opens.



- 5 Do you want to enable the automatic assigned default gateway?
  - If **yes**, be sure the Enable Automatic Assigned Default Gateway check box is checked. If this check box is checked, the residential gateway will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s).
  - If **no**, be sure the Enable Automatic Assigned Default Gateway check box is unchecked. If the check box is not checked, enter the default gateway IP address AND/OR a WAN interface from the drop-down list for the Use Interface field.
- 6 Click **Save/Apply** to save your selection.

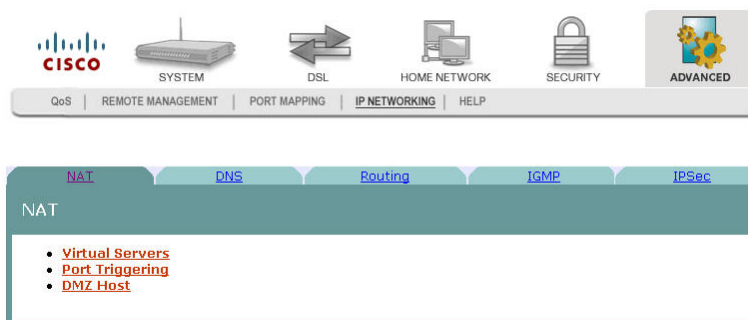
## Static Route

The Residential Gateway lets you set up static routes when routing packets from a specific network to another.

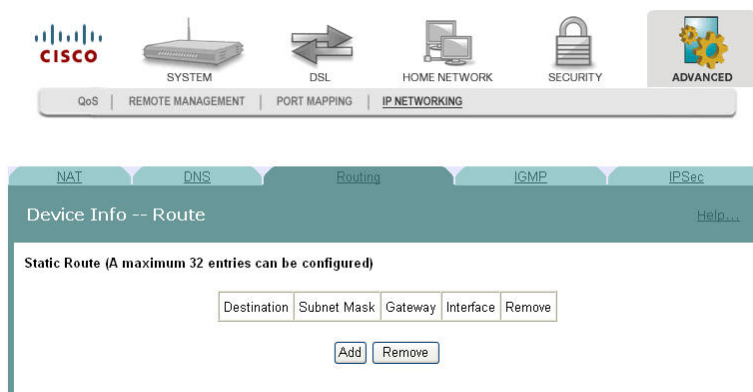
**Path:** Advanced > IP Networking > Routing > Static Route

To add a static routing entry, complete the following steps.

- 1 Click **Advanced** on the main screen.
- 2 Click **IP Networking**. The NAT screen opens.



- 3 Click **Routing**. The Routing screen opens.
- 4 Click **Static Route**. The Device Info -- Route screen opens.



- 5 Click **Add** to add a new entry.
- 6 Enter the Destination Network Address which should be a network ID for the destined network.
- 7 Enter the Subnet Mask for the destined network.
- 8 Select Use Gateway IP Address and identify the Gateway's IP Address to which the packet is forwarded.
- 9 Select Use Interface for the interface that is used to forward the packet from the drop-down menu.
- 10 Click **Save/Apply** at the bottom of the screen.

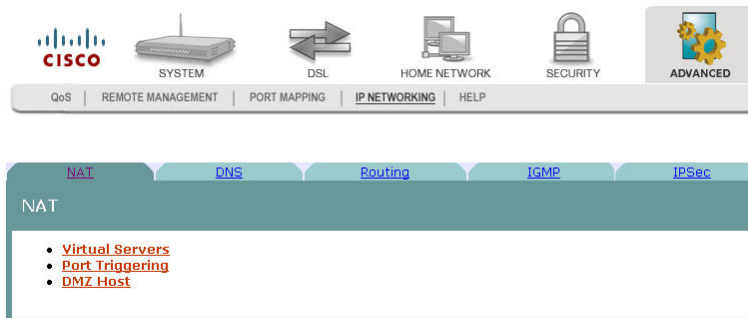
# Ping

The ping utility could be used to test the connectivity with other network devices.

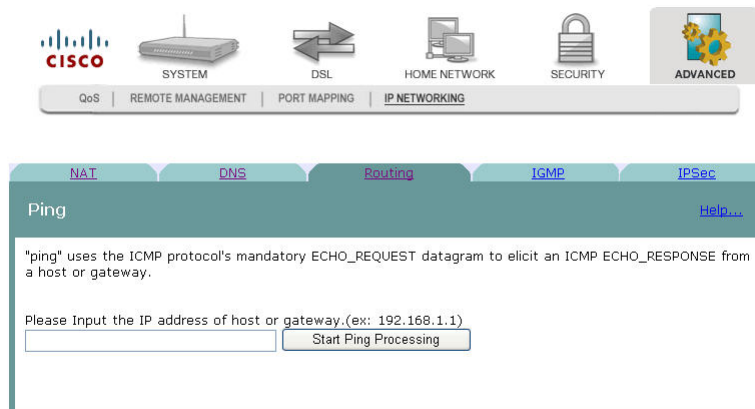
**Path:** Advanced > IP Networking > Routing > Ping

To test the connectivity with other devices (ping them), complete the following steps.

- 1 Click **Advanced** on the main screen.
- 2 Click **IP Networking**. The NAT screen opens.

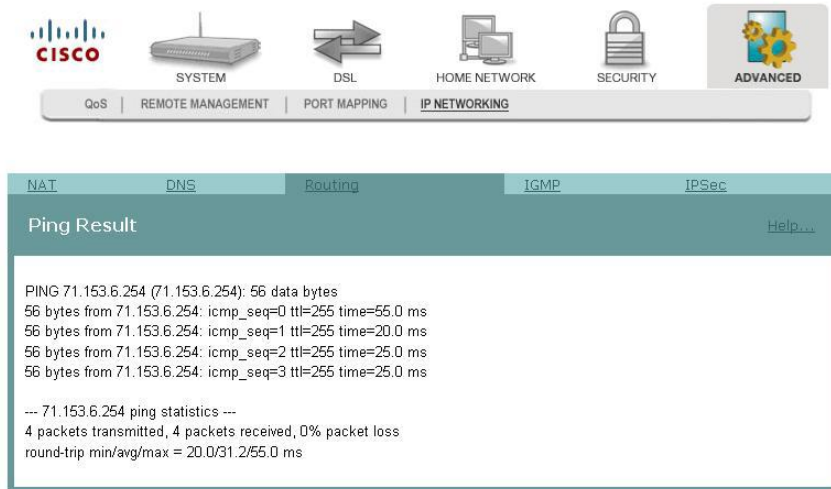


- 3 Click **Routing**. The Routing screen opens.
- 4 Click **Ping**. The Ping window opens.



## Chapter 7 Advanced Configuration

- 5 Enter the IP address of a remote host and click **Start Ping Processing**. The Ping result appears on the screen as shown below.



The screenshot displays the Cisco Advanced Configuration interface. At the top, there is a navigation bar with icons for CISCO, SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below this, a secondary navigation bar highlights the IP NETWORKING section, with sub-sections for QoS, REMOTE MANAGEMENT, PORT MAPPING, and IP NETWORKING. The main content area shows a 'Ping Result' window with the following output:

```
PING 71.153.6.254 (71.153.6.254): 56 data bytes
56 bytes from 71.153.6.254: icmp_seq=0 ttl=255 time=55.0 ms
56 bytes from 71.153.6.254: icmp_seq=1 ttl=255 time=20.0 ms
56 bytes from 71.153.6.254: icmp_seq=2 ttl=255 time=25.0 ms
56 bytes from 71.153.6.254: icmp_seq=3 ttl=255 time=25.0 ms

--- 71.153.6.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 20.0/31.2/55.0 ms
```



# Internet Group Management Protocol

The IGMP screen allows you to configure the Internet Group Management Protocol (IGMP) parameters. IGMP is a communications protocol that is used to manage the membership of Internet Protocol multicast groups. Routers use IGMP to manage multicasting. The IGMP messages are used to determine which host is part of which multicast group.

**Path:** Advanced > IP Networking > IGMP

The screenshot shows the IGMP configuration page in a Cisco router's web interface. The page is titled "IGMP" and has a "Help..." link. The "Enable IGMP snooping" checkbox is checked. Below it are two radio buttons: "Standard mode" and "Blocking", with "Blocking" selected. The "IGMP forward setting" section contains the following fields:

- Query Interval: 125 (30-127)sec
- Query Response Interval: 10 (5-10)sec
- Query Version: Version 3 (dropdown menu)
- Last member Query Interval: 1 (1-5)sec
- Last member Query Count: 2 (2-5)times

A "Save / Reboot" button is located at the bottom of the configuration area.

## Enabling IGMP Snooping

To enable IGMP snooping, complete the following steps.

- 1 Check the **Enable IGMP snooping** check box.
- 2 Select **Standard mode** to flood unknown multicast traffic. Select **Blocking** to discard unknown multicast traffic.
- 3 In the Query Interval field, enter the interval in seconds. The Query Interval is the amount of time in seconds between IGMP Host Query messages sent by the router.
- 4 In the Query Response Interval field, enter the interval in seconds. The Query Response Interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to an IGMP Query message.
- 5 In the Query Version field, choose the version from the drop-down list.

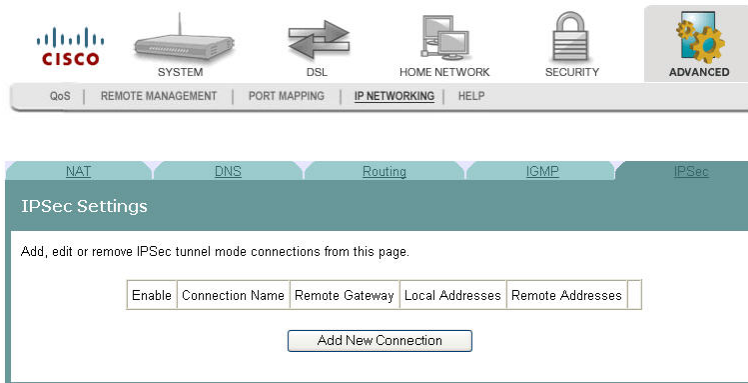
## Chapter 7 Advanced Configuration

- 6 In the Last member Query Interval field, enter the interval in seconds. It is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message.
- 7 In the Last member Query Count field, enter the value in numbers. It is the number of Group-Specific Query messages sent upon receipt of a message indicating a leave. (The default is 2.)
- 8 Click **Save/Reboot** to save your changes and reboot the system. enter the value in numbers. The default is 2. It is the number of Group-Specific Query messages sent upon receipt of a message indicating a leave.

## IPSec Settings

The IPSec Settings screen allows you to configure IP security settings for the residential gateway.

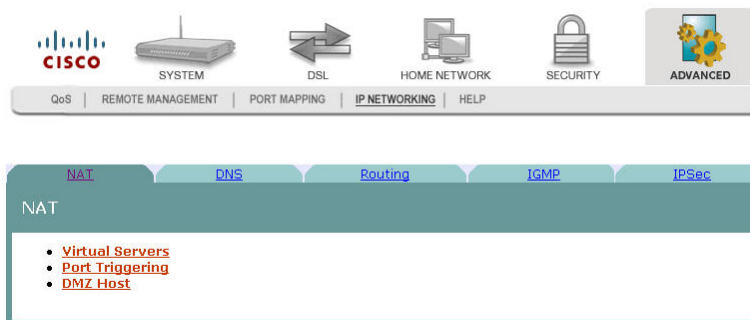
**Path:** Advanced > IP Networking > IPSec



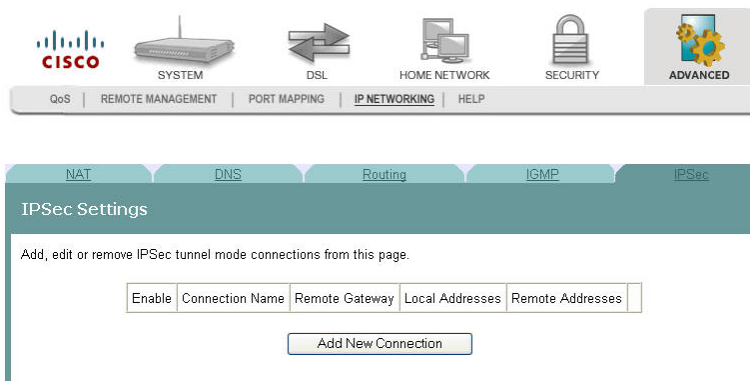
## Adding an IPSec Connection

To add an IPSec connection, complete the following steps.

- 1 Click **Advanced** on the main screen.
- 2 Click **IP Networking**. The NAT screen opens.



- 3 Click **IPSec**. The IPSec Settings screen opens.



- 4 Click **Add New Connection**. The IPSec Settings screen opens.

The screenshot shows the Scientific Atlanta Advanced Configuration interface. At the top, there is a navigation bar with icons for SYSTEM, DSL, HOME NETWORK, SECURITY, and ADVANCED. Below this, there are tabs for NAT, DNS, Routing, IGMP, and IPSec. The IPSec Settings screen is displayed, featuring the following fields and options:

- IPSec Connection Name: new connection
- Remote IPSec Gateway Address: 0.0.0.0
- Tunnel access from local IP addresses: Subnet
- IP Address for VPN: 0.0.0.0
- IP Subnetmask: 255.255.255.0
- Tunnel access from remote IP addresses: Subnet
- IP Address for VPN: 0.0.0.0
- IP Subnetmask: 255.255.255.0
- Key Exchange Method: Auto(IKE)
- Authentication Method: Pre-Shared Key
- Pre-Shared Key: key
- Perfect Forward Secrecy: Disable
- Show Advanced Settings button
- Save / Apply button

- 5 In the IPSec Connection Name field, enter the name of the connection.
- 6 In the Remote IPSec Gateway Address field, enter the gateway address for the remote IPSec gateway.
- 7 In the Tunnel access from local IP addresses field, select Subnet or Single Address.
- 8 In the IP Address for VPN, enter the IP address for the VPN connection.
- 9 In the IP Subnetmask field, enter the subnet mask for the VPN IP address.
- 10 In the Tunnel access from remote IP addresses field, select Subnet or Single Address.
- 11 In the IP Address for VPN, enter the IP address for the VPN connection.
- 12 In the IP Subnetmask field, enter the subnet mask for the VPN IP address.
- 13 In the Key Exchange Method field, select Auto(IKE) or manual.
- 14 In the Authentication Method field, select Pre-Shared Key or Certificate (X.509).
- 15 Depending upon the authentication method that you selected, do one of the following:
  - If you selected Pre-Shared Key, enter the name of the key in the Pre-Shared Key field.  
OR
  - If you selected Certificate (X.509), select a certificate from the drop-down list of certificates in the Certificate field.
- 16 In the Perfect Forward Secrecy field, select one of the following options:
  - If you select Enable, Perfect Forward Secrecy is enabled.  
OR
  - If you select Disable, Perfect Forward Secrecy is disabled.
- 17 Do you want to configure the advanced settings?

- If **yes**, in the Advanced IKE Settings field, click **Show Advanced Settings** to populate the screen with advanced settings.

- If **no**, go to step 20.

**18** Complete the advanced settings as follows:

- In the Phase 1 Mode field, select Main or Aggressive.
- In the Encryption Algorithm field, select one of the following encryption algorithms:
  - 3DES
  - AES -128
  - AES - 192
  - AES - 256
- In the Integrity Algorithm field, select MD5 or SHA1.
- In the Select Diffie-Hellman Group for Key Exchange field, select one of the following options:
  - 768 bit
  - 1024 bit
  - 1536 bit
  - 2048 bit
  - 3072 bit
  - 4096 bit
  - 6144 bit
  - 8192 bit
- In the Key Life Time, enter the life of the key in seconds.

**19** Repeat step 15 through 18 for each phase.

**20** Click **Save/Apply** to save your settings.



# 8

---

## Customer Information

### Introduction

This chapter provides contact information to obtain product support and return products for service.

### In This Chapter

- Customer Support ..... 218
- Return Products for Repair..... 220

## Customer Support

### If You Have Questions

If you have questions about this product, contact the representative who handles your account for information.

If you have technical questions, telephone your nearest technical support office at one of the following telephone numbers.

#### The Americas

---

United States	Cisco® Services Atlanta, Georgia	<b>Technical Support</b> <ul style="list-style-type: none"> <li>■ For <i>Digital Broadband Delivery System</i> products only, call:           <ul style="list-style-type: none"> <li>– Toll-free: 1-800-283-2636</li> <li>– Local: 770-236-2200</li> <li>– Fax: 770-236-2488</li> </ul> </li> <li>■ For all products <i>other than</i> Digital Broadband Delivery System, call:           <ul style="list-style-type: none"> <li>– Toll-free: 1-800-722-2009</li> <li>– Local: 678-277-1120</li> <li>– Fax: 770-236-2306</li> </ul> </li> </ul> <b>Customer Service</b> <ul style="list-style-type: none"> <li>■ Toll-free: 1-800-722-2009</li> <li>■ Local: 678-277-1120</li> <li>■ Fax: 770-236-5477</li> </ul>
---------------	-------------------------------------	---

---

#### The United Kingdom and Europe

---

Europe	European Technical Assistance Center (EuTAC), Belgium	<b>Product Information</b> <ul style="list-style-type: none"> <li>■ Telephone: 32-56-445-444</li> </ul> <b>Technical Support</b> <ul style="list-style-type: none"> <li>■ Telephone: 32-56-445-197 or 32-56-445-155</li> <li>■ Fax: 32-56-445-061</li> </ul>
--------	---	--

---

#### Asia-Pacific

---

China	Hong Kong	<b>Technical Support</b> <p>Telephone: 011-852-2588-4745</p> <p>Fax: 011-852-2588-3139</p>
-------	-----------	--

---



**Australia**

---

Australia      Sydney

**Technical Support**

Telephone: 011-61-2-8446-5374

Fax: 011-61-2-8446-8015

---

**Japan**

---

Japan            Tokyo

**Technical Support**

Telephone: 011-81-3-5322-2067

Fax: 011-81-3-5322-1311

---

**Additional Information**

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

## Return Products for Repair

You must obtain a return material authorization (RMA) number before you send products to us for repair or upgrade. To return a product for repair or upgrade, complete the following steps.

- 1 Obtain the following information about the product that you want to return for repair or upgrade:
  - The name and model number (if applicable) of the product and the quantity of returns
  - A reason for the return, such as upgrade or failure symptom
  - Your company name, contact, telephone number, email address, fax number, repair disposition authority, and any service contract details
  - A purchase order number

**Notes:**

- If you are unable to issue a purchase order at the time you request an RMA number, a proforma invoice will be sent to you at the completion of repair. This invoice lists all costs incurred.
- We must receive a purchase order within 15 days of receipt of proforma.

**Important:** In-warranty products can accrue costs through damage or misuse, or if no problem is found. Products incurring costs will not be returned to the customer without a valid purchase order.

- 2 Telephone or fax Factory Services at one of the following numbers to request an RMA number:
  - From North America, call:
    - Tel: 1-800-722-2009
    - Fax: 770-236-5477
  - From Europe, Middle East, or Africa, call:
    - Tel: 32-56-445-444
    - Fax: 32-56-445-051
  - From Latin America, call:
    - Tel: 1-770-236-5662
    - Fax: 1-770-236-5888
  - From Asia Pacific, call:
    - Tel: 852-2588-4746
    - Fax: 852-2588-3139

**Result:** The customer service representative will provide the RMA number and the shipping instructions to you.

**Note:** RMA numbers are only valid for 60 days. You must contact a customer service representative to revalidate your RMA numbers if the number is older than 60 days. After the RMA number is revalidated, you can return the product.

- 3 Pack the product in its original container and protective packing material.

**Important:**

- If the original container and packing material are no longer available, pack the product in a sturdy, corrugated box and cushion it with packing material that is appropriate for the method of shipping.
- You are responsible for delivering the returned goods to us safely and undamaged. Improperly packaged shipments, which may have caused additional damage, may be refused and returned to you at your expense.
- Do not return any power cords or accessories.

- 4 Write the following information on the outside of the container:

- Your name
- Your complete address
- Your Telephone number
- RMA number
- Problem description (for product failures)

**Important:** Absence of the RMA number may delay processing your product for repair. Include the RMA number in all correspondence.

- 5 Ship the product to the address you receive from the customer service representative.

**Important:** We do not accept freight collect. Be sure to prepay all shipments.



Cisco Systems, Inc.  
5030 Sugarloaf Parkway, Box 465447  
Lawrenceville, GA 30042

678.277.1000  
[www.cisco.com](http://www.cisco.com)

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc. trademarks used in this document.

Product and service availability are subject to change without notice.

© 2009 Cisco Systems, Inc. All rights reserved.

November 2009 Printed in United States of America

Part Number 4020210 Rev A