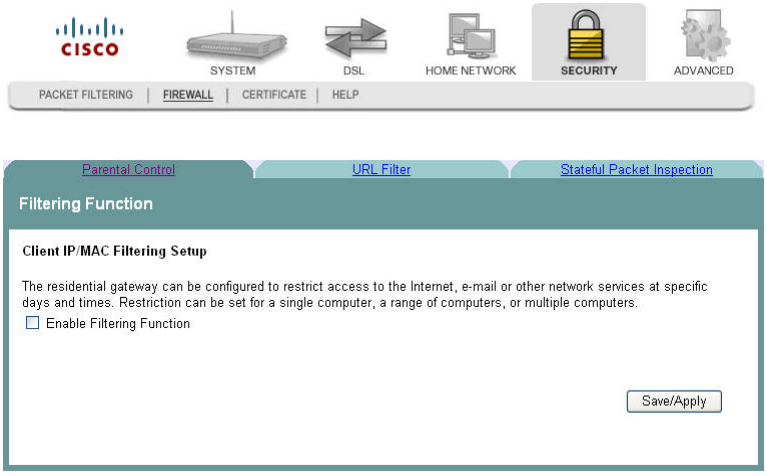
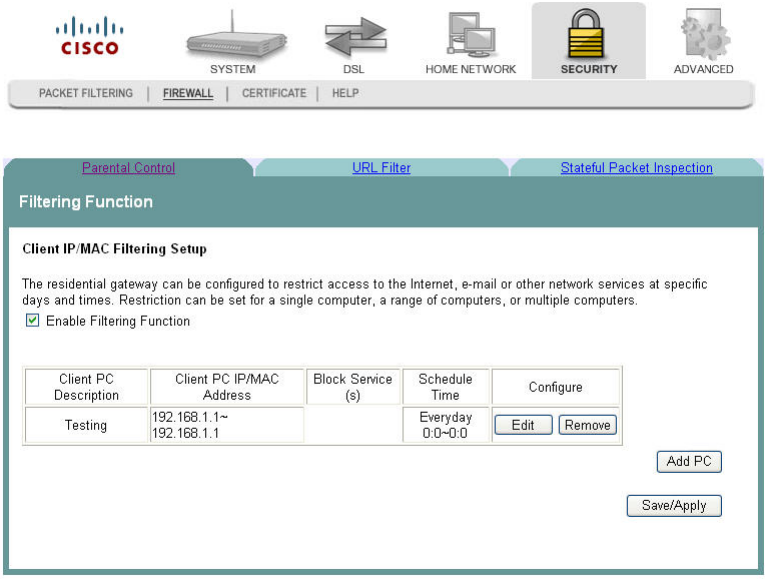
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.

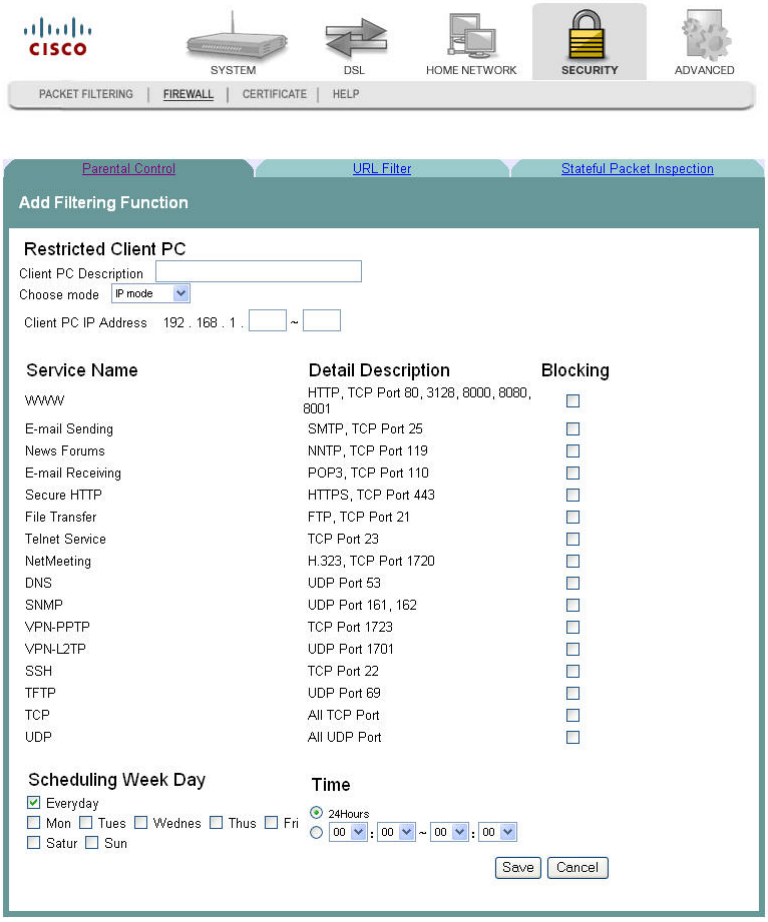
2 Click the **Firewall** tab. The Filtering Function screen opens.



3 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.



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



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, Click **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 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.

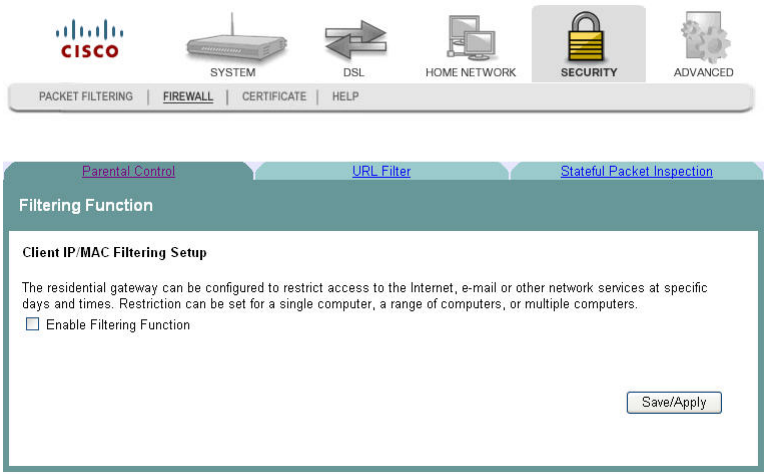
11 Click **Save/Apply** to enable the time of day restrictions.

Removing Time of Day Restrictions

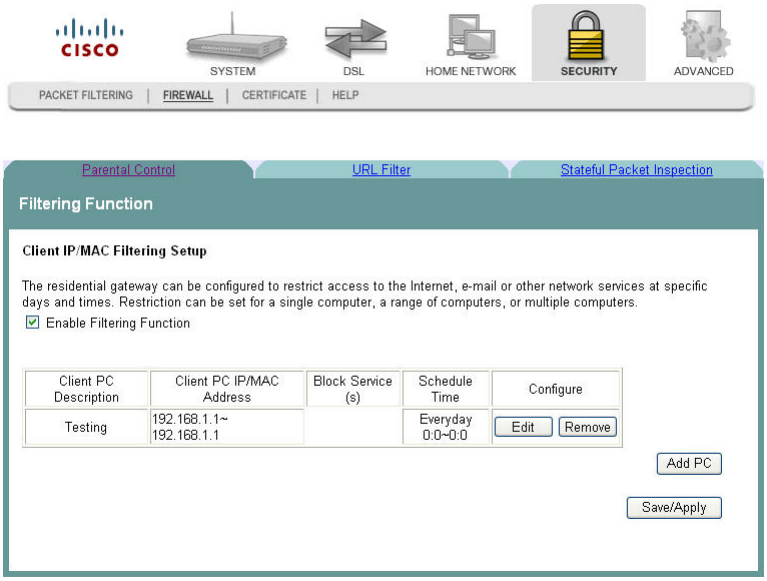
To remove time of day restrictions, complete the following steps.

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

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



3 Check the **Enable Filtering Function** check box to enable the filtering function. The Mac Filtering screen populates with any time restrictions that are set.



Q. to reviewers. screen changed test steps.

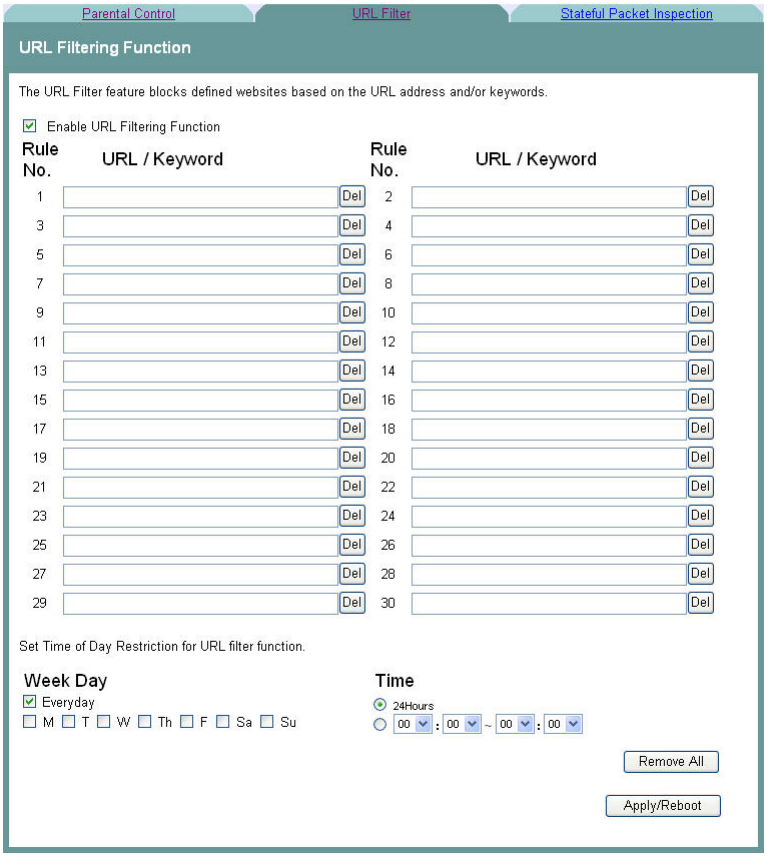
4 From the Configure field select **Remove** in the Remove column next to the time of day restriction that you wish to remove.

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.

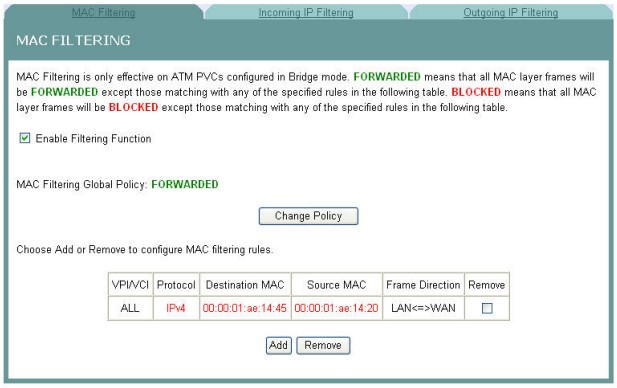
Path: Security > Firewall > URL Filter



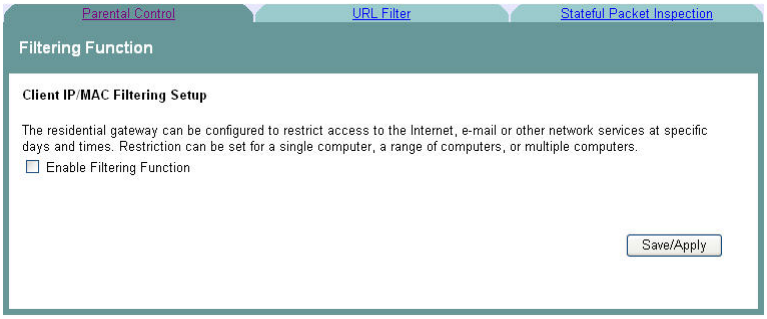
Enabling URL Filtering

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

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

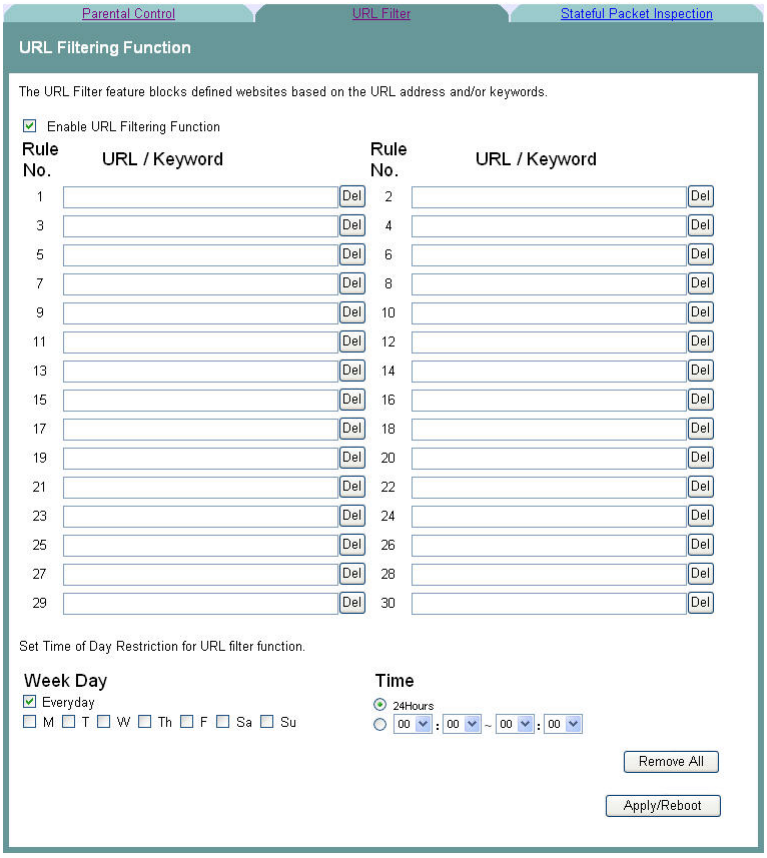


2 Click the **Firewall** tab. The Filtering Function screen opens by default.



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.



5 For each rule, enter the URL or keyword that you want to block.

6 Under **Week Day**, select Everyday or select the individual days on which you want the filter to take effect.

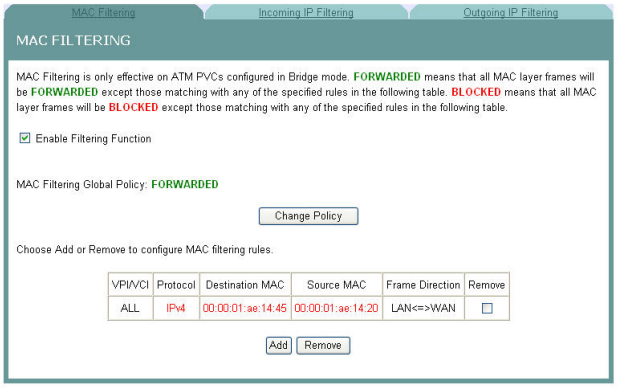
7 Under **Time**, select 24Hours or select the individual times that you want the filter to take effect.

8 Click **Save**.

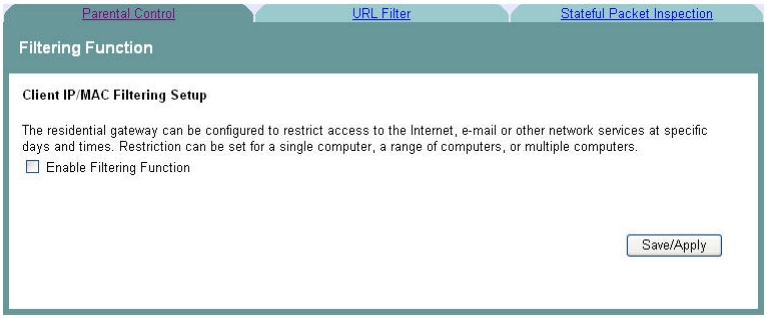
Removing a URL Filter

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

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

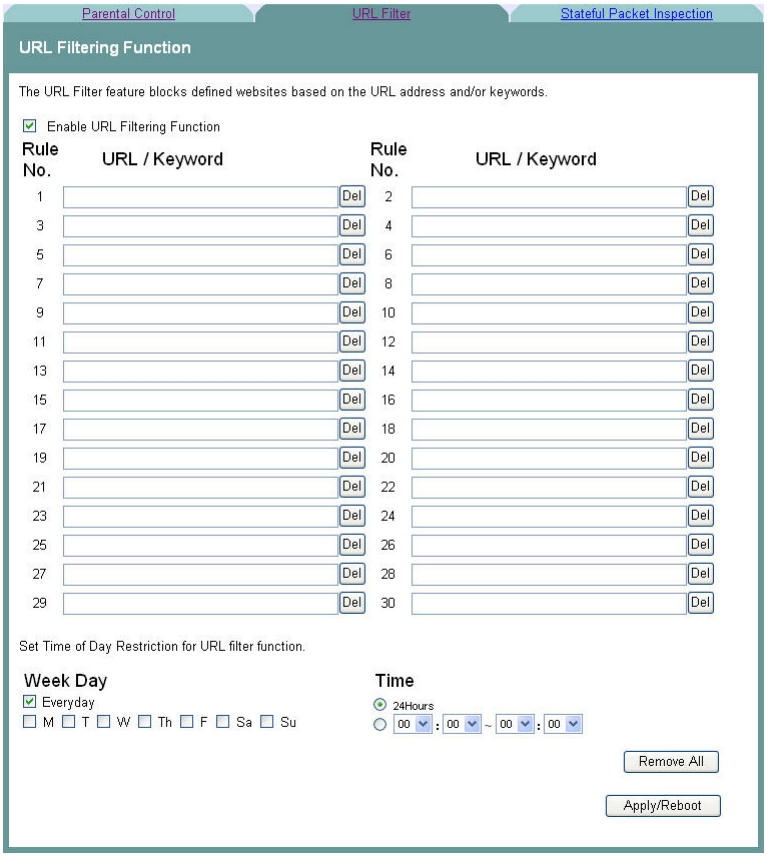


2 Click the **Firewall** tab. The Filtering Function screen opens by default.



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.



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

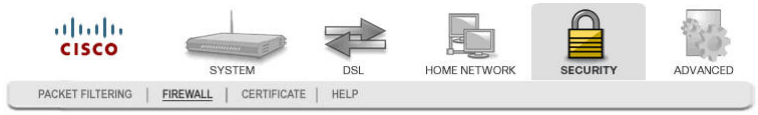
6 Click **Save**.

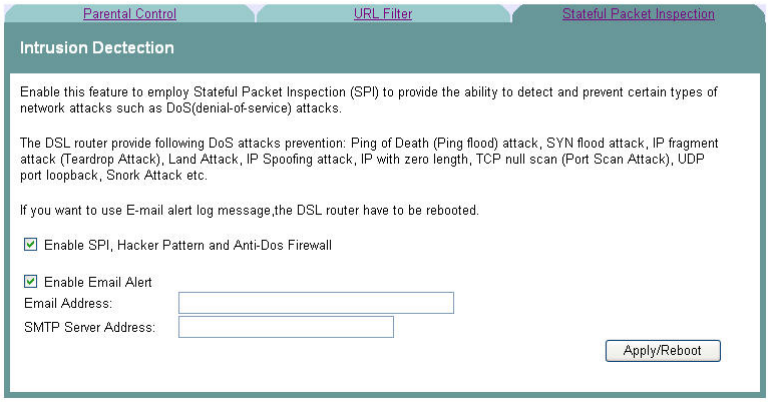
Stateful Packet Inspection

The Stateful Packet Inspection screen allows you to use stateful packet inspection (SPI) to detect and prevent certain types of network attacks such as DoS (denial-of-service) attacks.

Q. to reviewers provide more detail.

Path: Security > Firewall > Stateful Packet Inspection

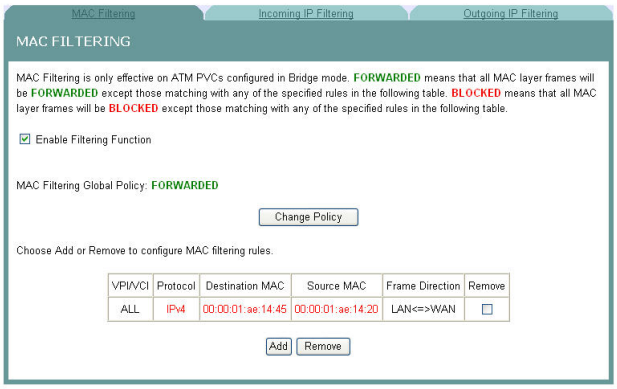




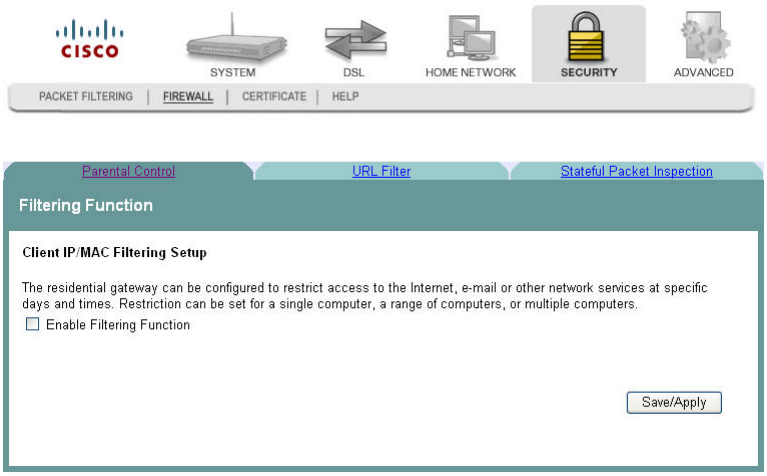
Enabling Stateful Packet Inspection

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

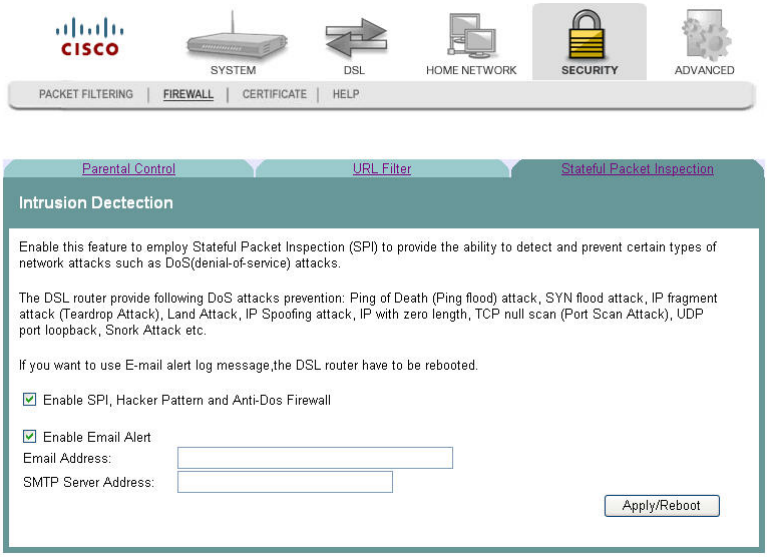
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



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



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



4 Select the **Enable SPI, Hacker Pattern and Anti-Dos Firewall** field.

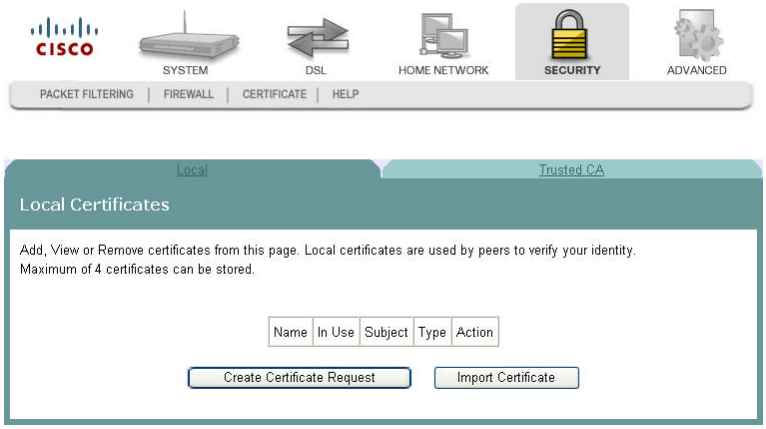
Q. to reviewers: What about the Enable Email ALert field?

5 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

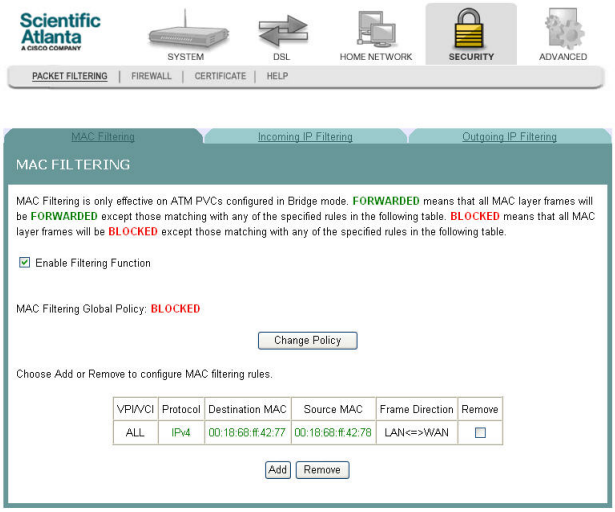


Creating Certificates

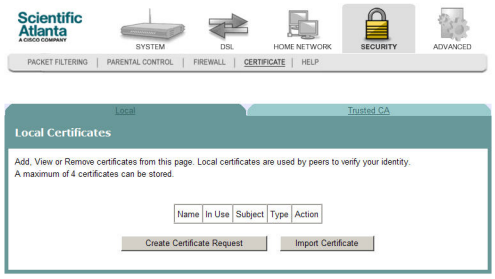
The Create Certificate screen allows you to generate a certificate by specifying certificate parameters shown in this screen.

To create a certificate, complete the following steps.

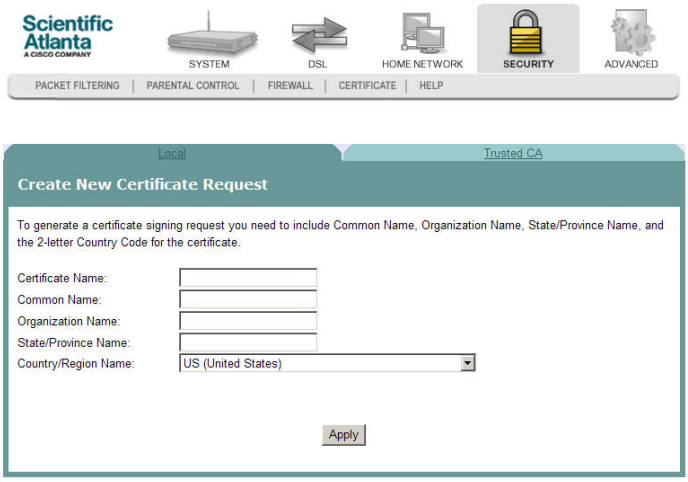
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



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



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



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

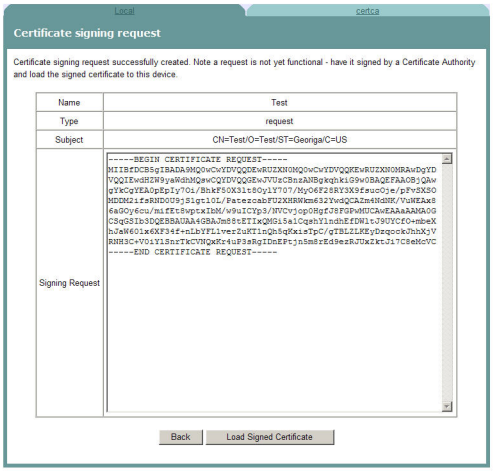
5 In the Common Name field, enter the common name of the certificate.

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

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

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

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



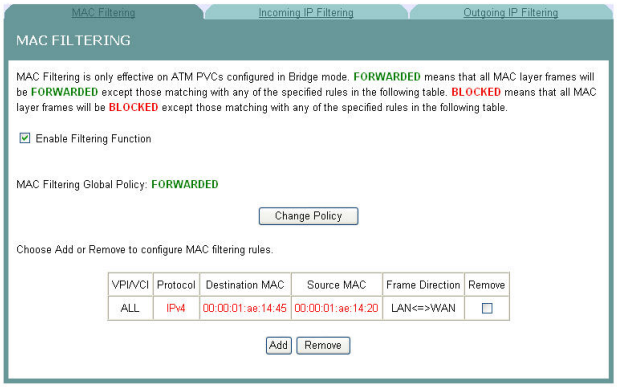
10 Click **Load Signed Certificate** to save the certificate on the residential gateway.

Importing Local Certificates

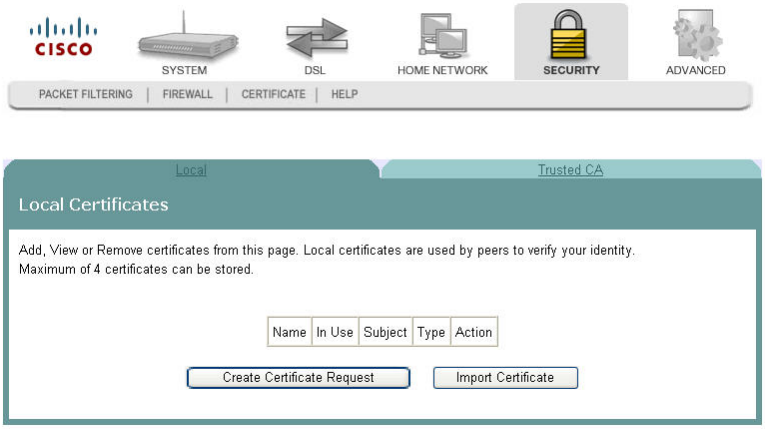
The Import Certificate screen allows you to import a pre-existing certificate to the residential gateway.

To import a certificate, complete the following steps.

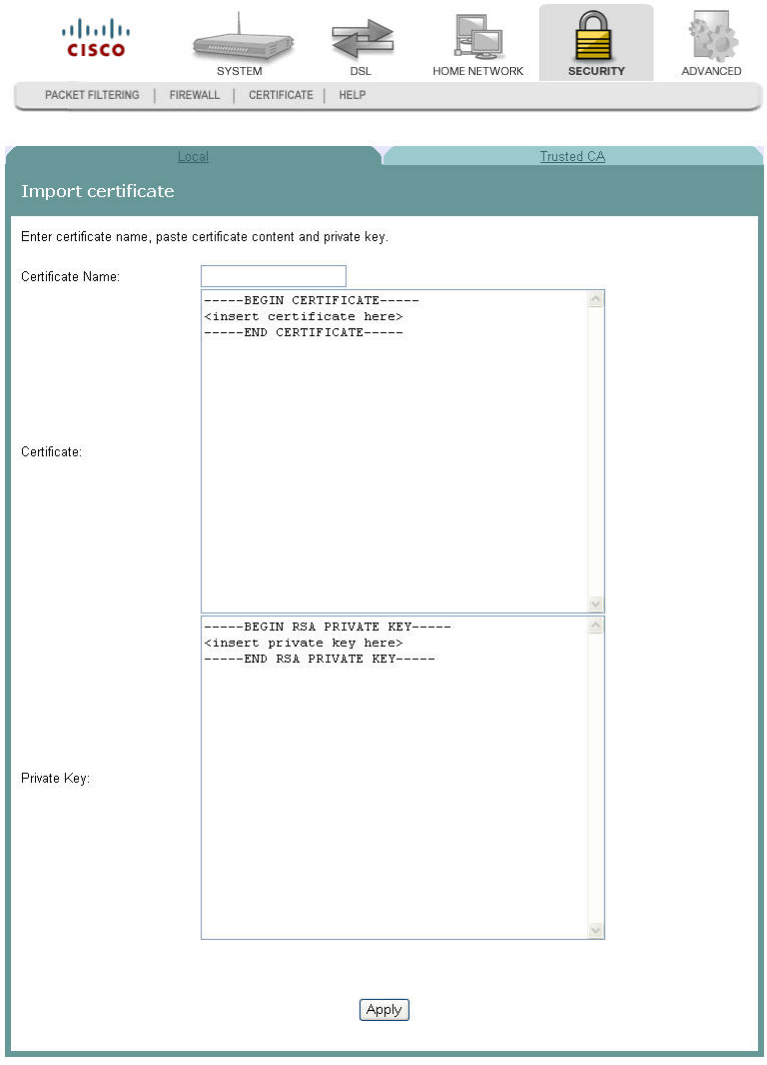
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



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



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



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

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

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

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

Trusted CA Certificates

The 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.

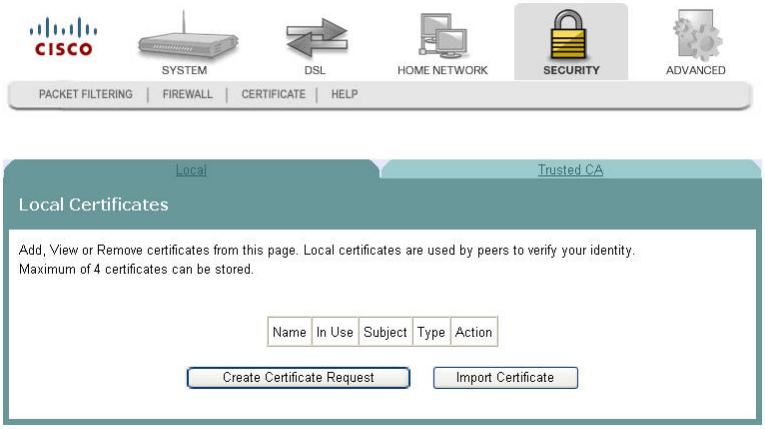
Path: Security > Certificate > Trusted CA > Trusted CA (Certificate Authority) Certificates

Importing Trusted CA Certificates

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

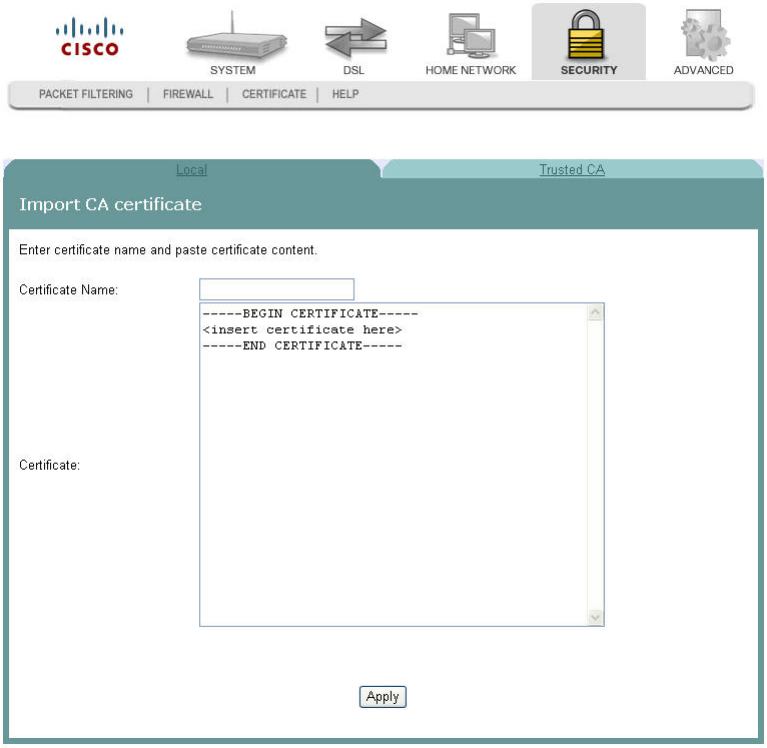
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.

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



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 to 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.

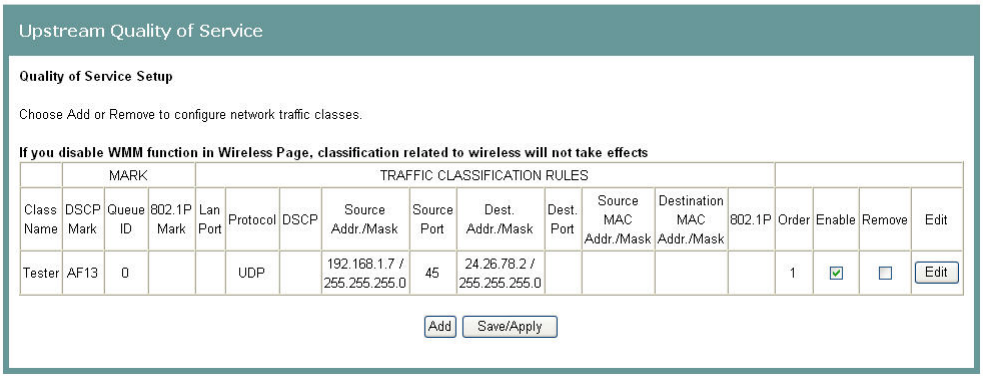
In This Chapter

Upstream Quality of Service

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

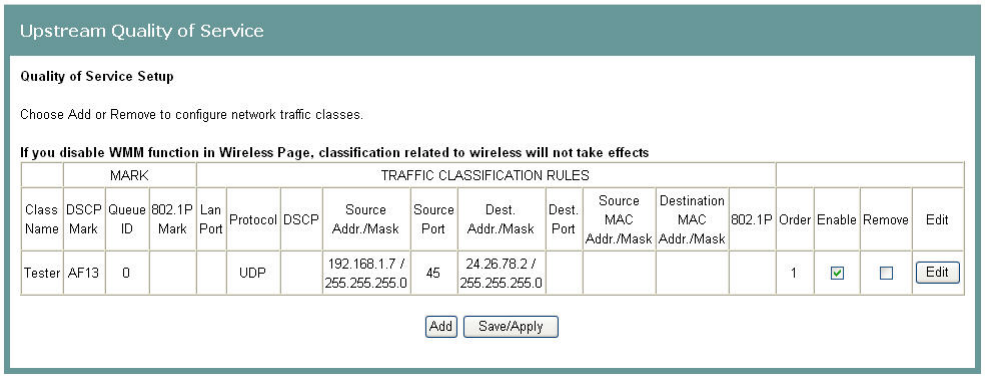
Q. to reviewers: Screen alignment is off.



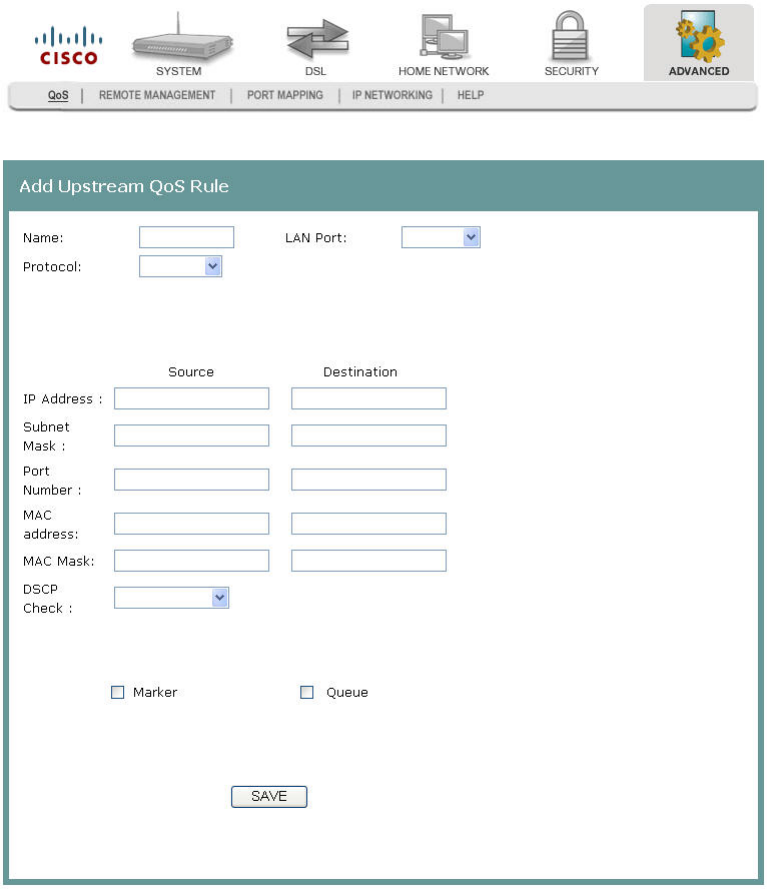
Adding Upstream Quality of Service Settings

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.



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.

10 In the MAC Mask field, enter the mask for the source from which the packets are being sent.

Q. to reviewers Fields changed update

11 Select the Marker field and choose from the list of Diffserv code point (DSCP) values.

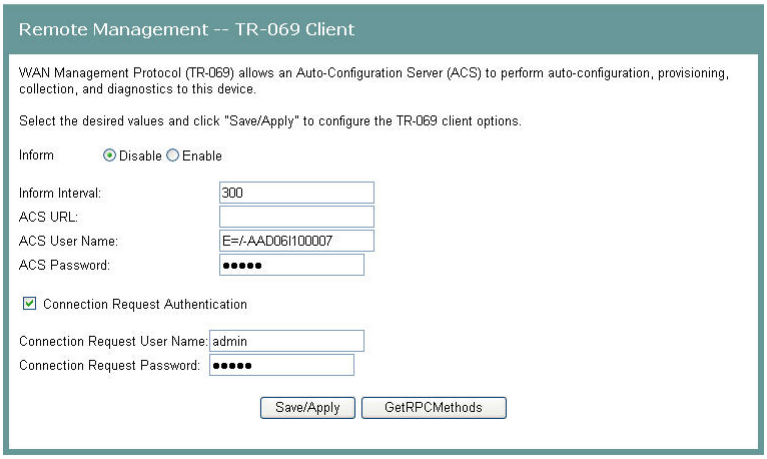
12 Select the Queue field and choose from the list of queues.

13 Click **Save**.

Remote Management

The Remote Management -- TR-O69 Client screen allows an autoconfiguration server (ACS) to perform autoconfiguration, provisioning, collection of statistics, and diagnostics for this residential gateway.

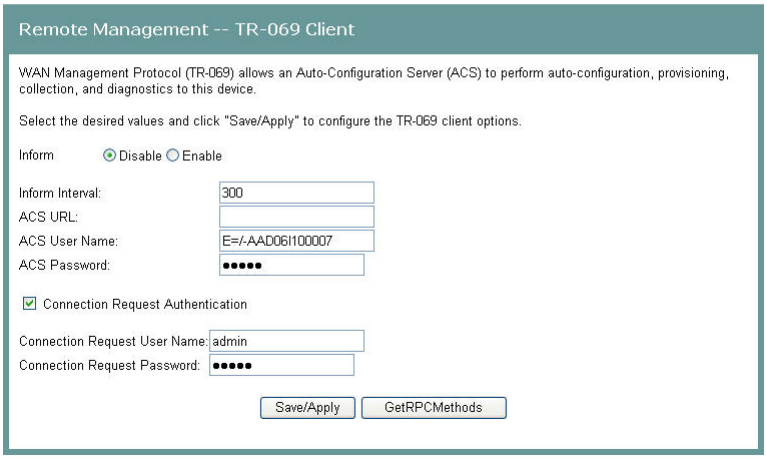
Path: Advanced > Remote Management



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.



2 In the Inform field, choose one of the following options:

- Click **Enable** to 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 frequency that the inform messages are sent from the residential gateway to the autoconfiguration server.

4 In the ACS URL field, enter the URL for the autoconfiguration server.

5 In the ACS User Name field, enter the user name for autoconfiguration server.

6 In the ACS Password field, enter the password for the autoconfiguration server.

7 Select 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.

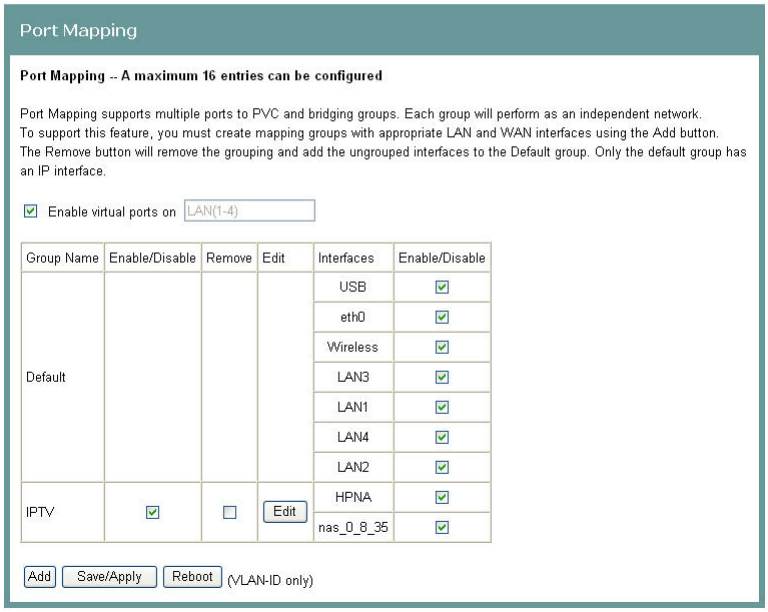
10 Click **GetRPCMethods** to obtain the list of remote procedural calls (RPC) supported by the autoconfiguration server.

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



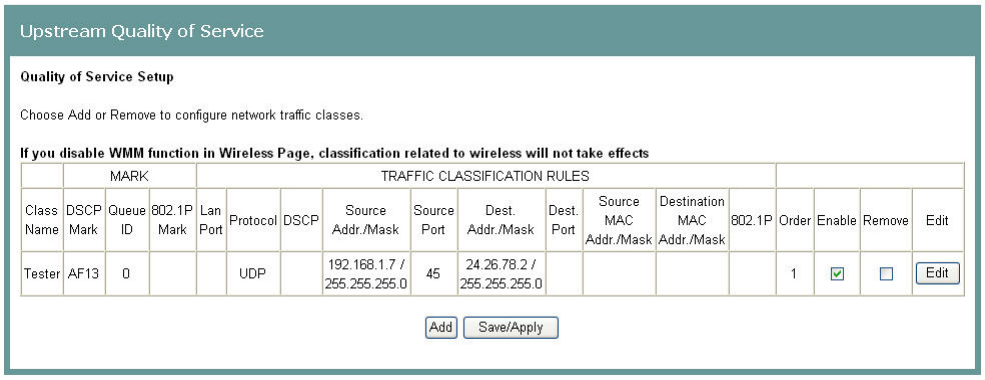
Adding Port Mapping

To add port mapping, complete the following steps.

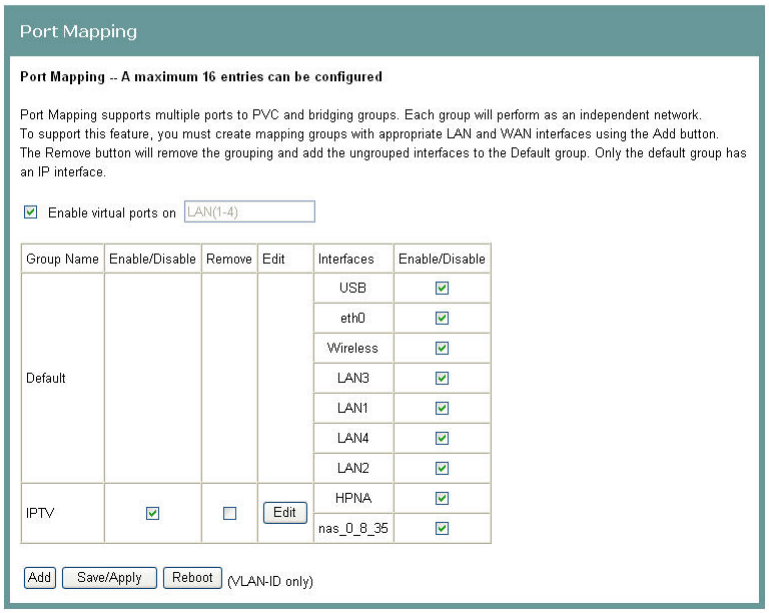
CAUTION:

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.



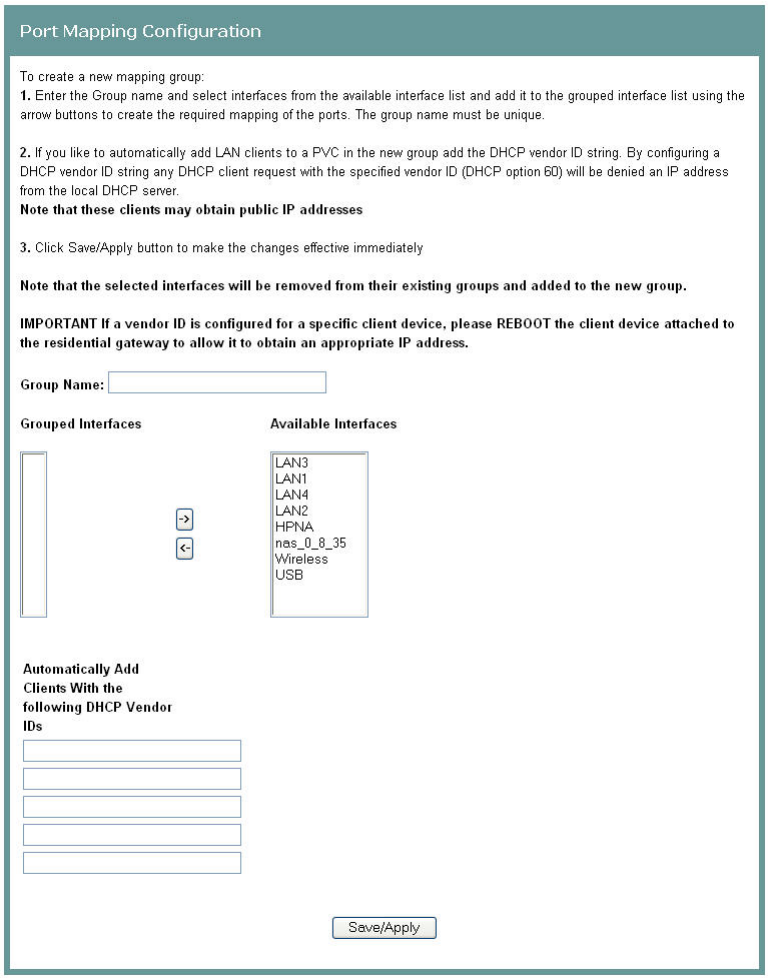
2 Click the **Port Mapping** tab. The Port Mapping screen opens.



3 Select the Enable virtual ports on field if you want to use the port mapping feature.

4 Select Enable Diffserv to 802.1p conversion if you want to convert diffserv code points to 802.1p tags.

5 Click **Add**. The Port Mapping Configuration screen opens.



6 In the Group Name field, enter the name of the group. The group name must be unique. For example, enter IPTV.

7 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.

8 In the Automatically Add Clients With the following DHCP Vendor IDs, add the DHCP option 60 [vendor ID option] string for the devices (typically IP set-tops) attached to the residential gateway.

9 Click **Save/Apply**.

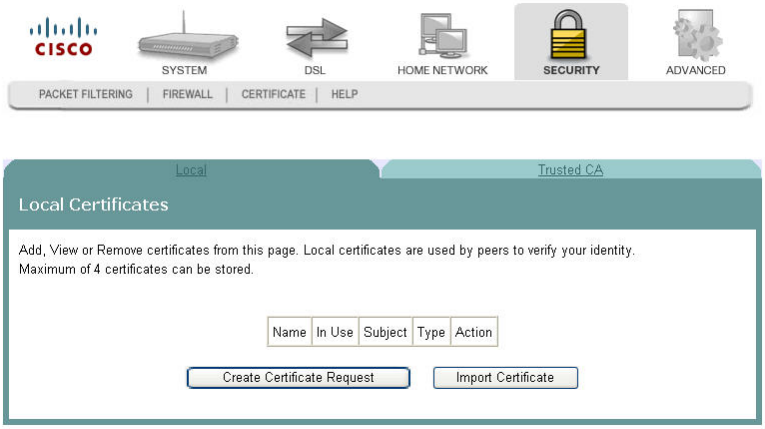
Creating Certificates

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

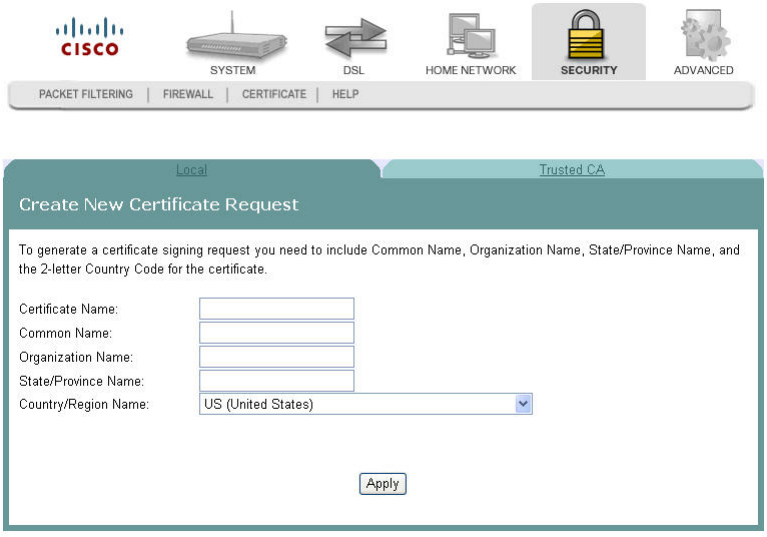
To create a certificate, complete the following steps.

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

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



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



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

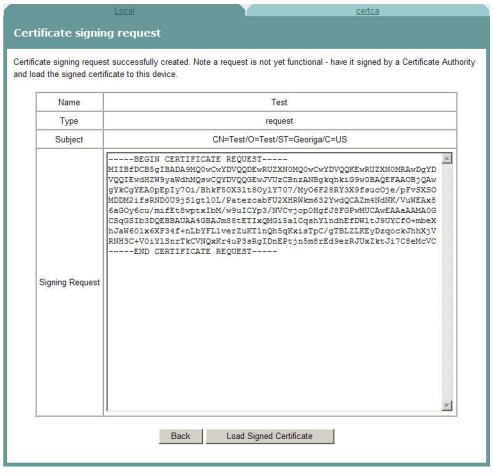
5 In the Common Name field, enter the common name of the certificate.

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

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

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

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

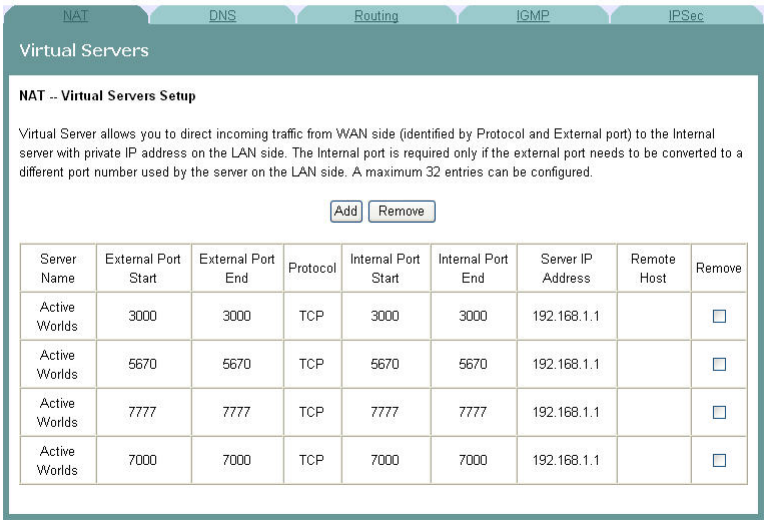


10 Click **Load Signed Certificate** to save the certificate on the residential gateway.

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



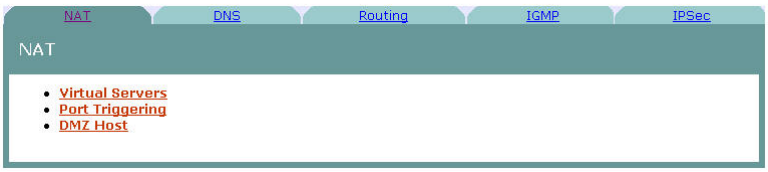
Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remote Host	Remove
Active Worlds	3000	3000	TCP	3000	3000	192.168.1.1		☐
Active Worlds	5670	5670	TCP	5670	5670	192.168.1.1		☐
Active Worlds	7777	7777	TCP	7777	7777	192.168.1.1		☐
Active Worlds	7000	7000	TCP	7000	7000	192.168.1.1		☐

Adding a Virtual Server

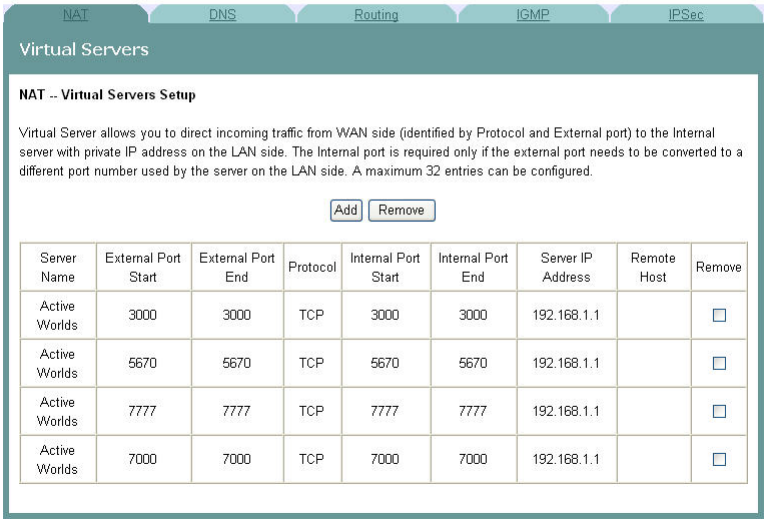
To add and configure a virtual server, complete the following steps.

1 Click **Advanced** on the main screen.

2 Click **IP Networking**. The NAT screen opens.

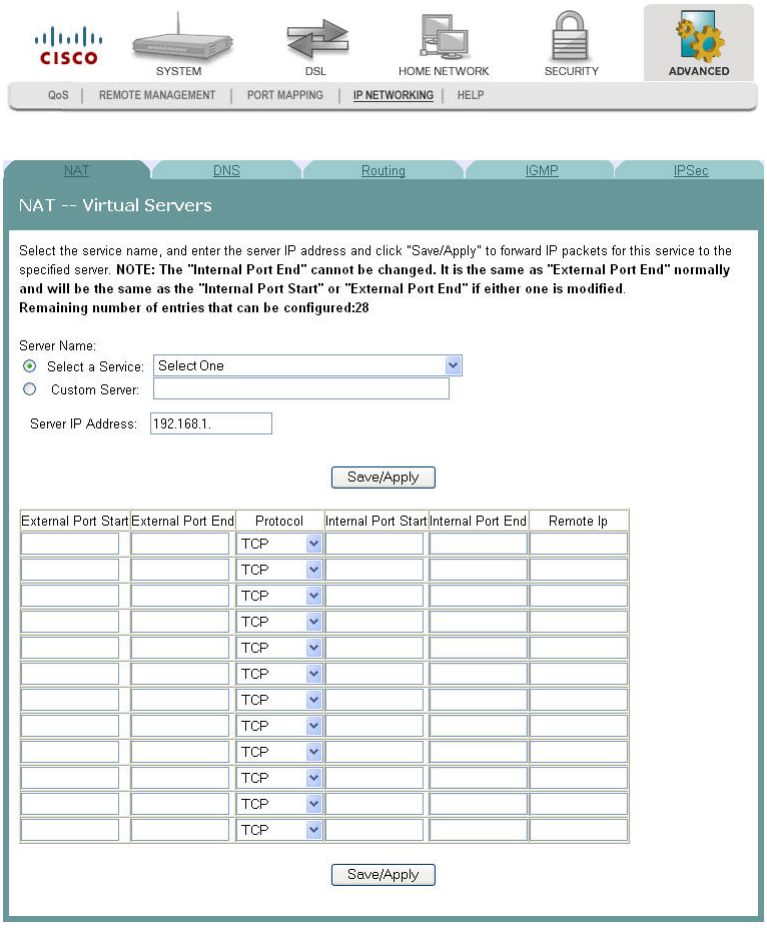


3 Click **Virtual Servers**.The Virtual Servers screen opens.



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		☐
Active Worlds	5670	5670	TCP	5670	5670	192.168.1.1		☐
Active Worlds	7777	7777	TCP	7777	7777	192.168.1.1		☐
Active Worlds	7000	7000	TCP	7000	7000	192.168.1.1		☐

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



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 Under Protocol, select **TCP, UDP, TCP/UDP**.

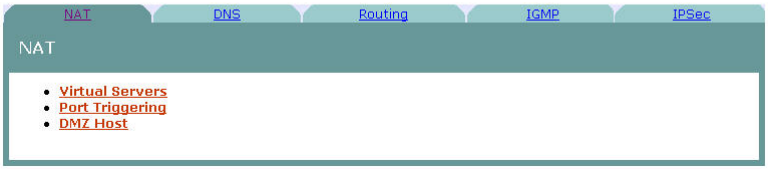
8 Click **Save/Apply** to add the virtual server.

Removing a Virtual Server

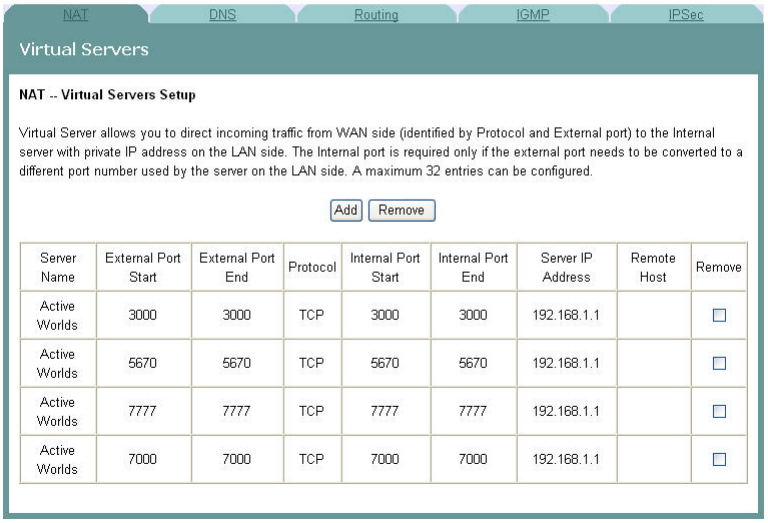
To remove a virtual server, complete the following steps.

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.

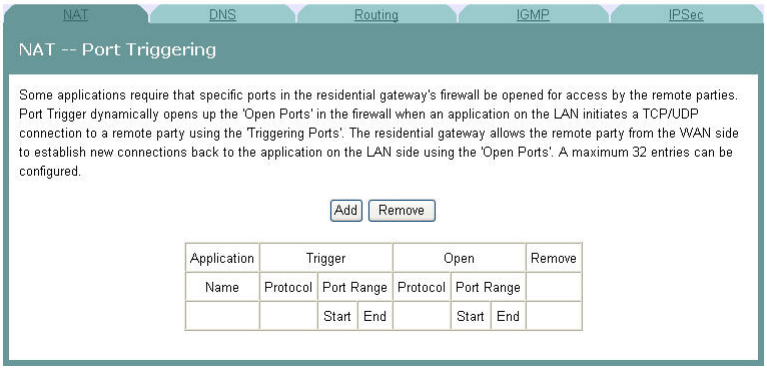
5 Click **Remove** to remove the NAT Virtual Server.

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

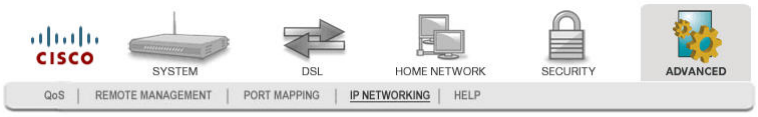


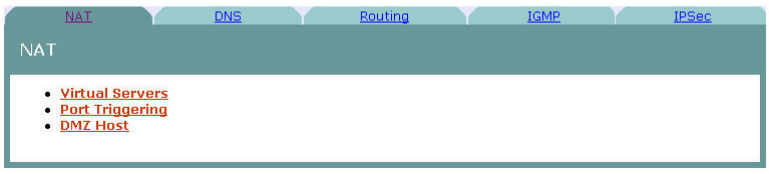
Opening a Port on the Firewall

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

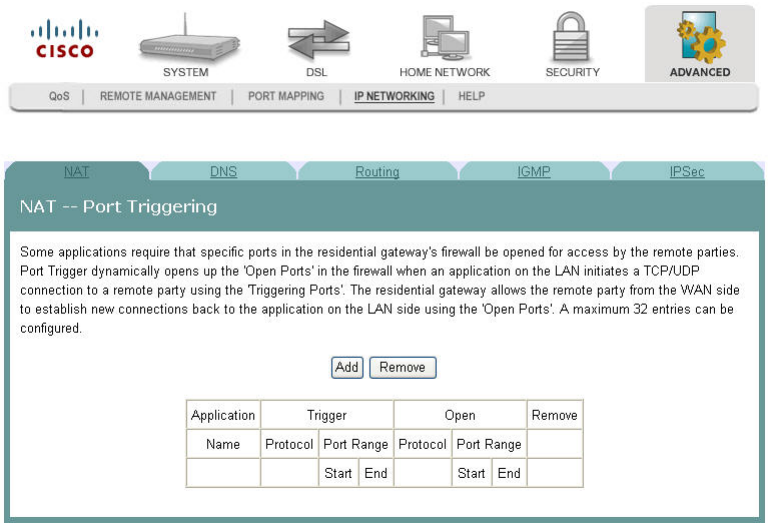
1 CClick **Advanced** on the main screen.

2 Click **IP Networking**. The NAT screen opens.

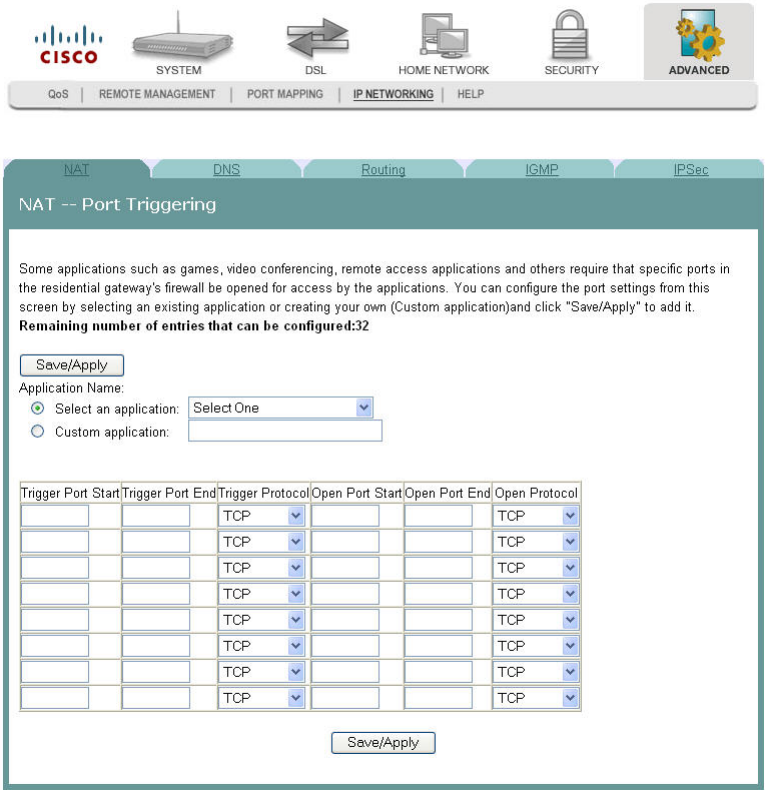




3 Click **Port Triggering**. The NAT -- Port Triggering screen opens.



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

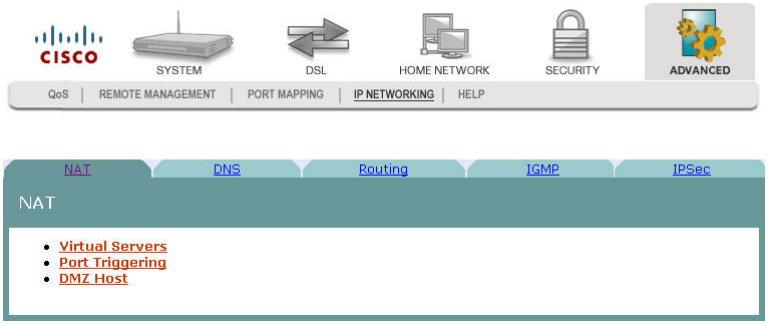
7 Click **Save/Apply** to open the ports on the firewall.

Closing a Port on the Firewall

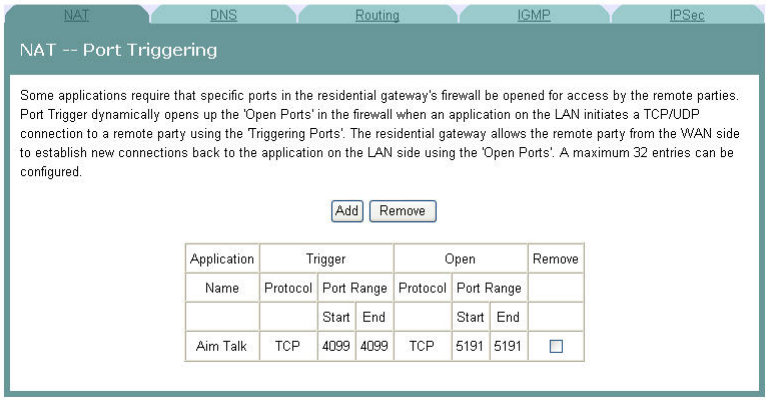
To close a port on the firewall, complete the following steps.

1 Click **Advanced** on the main screen.

2 Click **IP Networking**. The NAT screen opens.



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



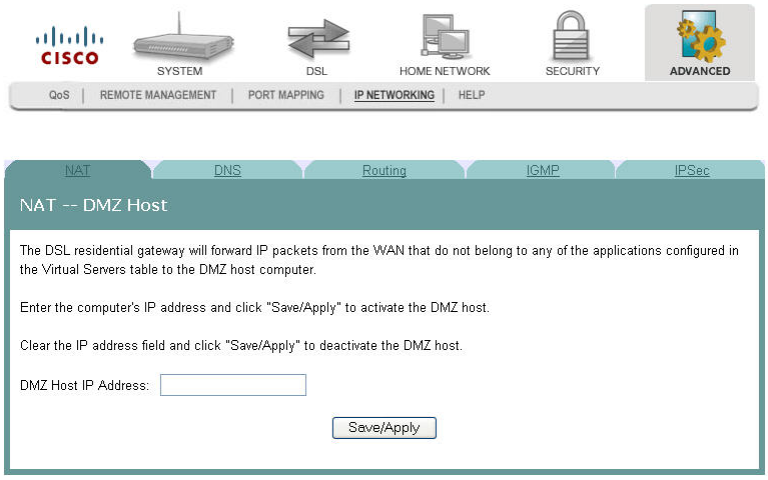
4 From the NAT -- Port Triggering screen, click **Remove** in the Remove column next to the port you wish to close.

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

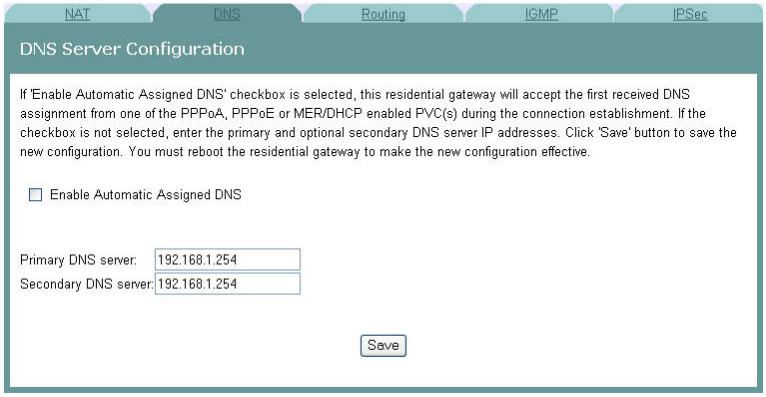
Clear the DMZ Host IP Address field and click **Save/Apply** to deactivate the DMZ host.

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 selected, this router 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 router to make the new configuration effective.

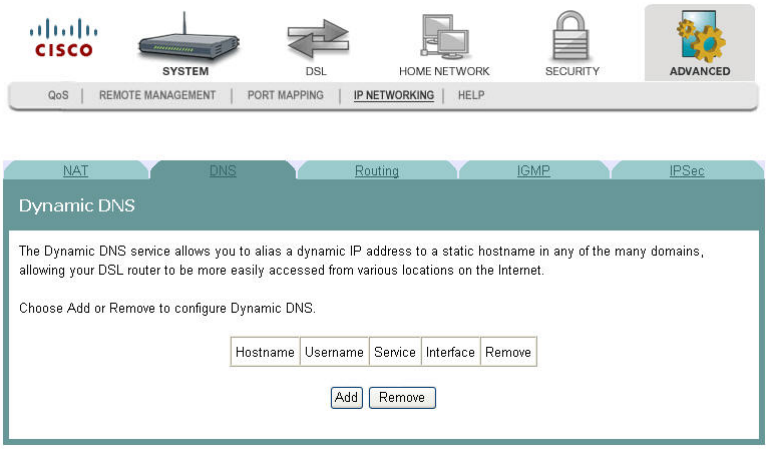
Path: Advanced > IP Networking > DNS > DNS Server



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.

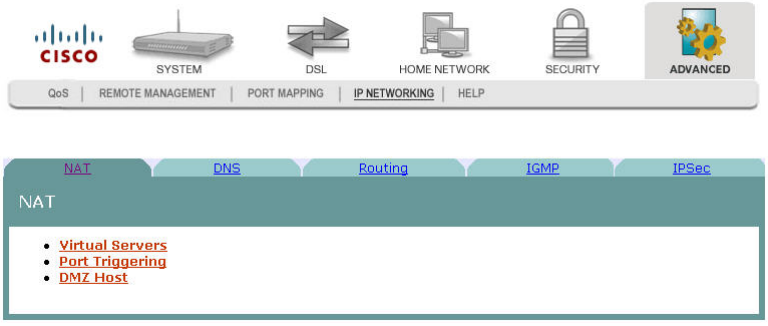
Path: Advanced > IP Networking > DNS > Dynamic DNS



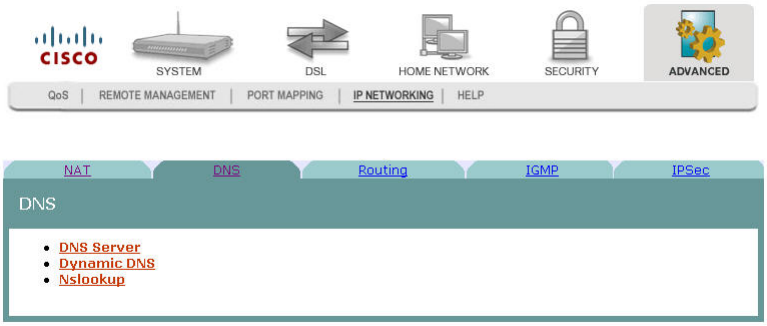
Adding an Alias for A Dynamic IP Address to a Static Host Name

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

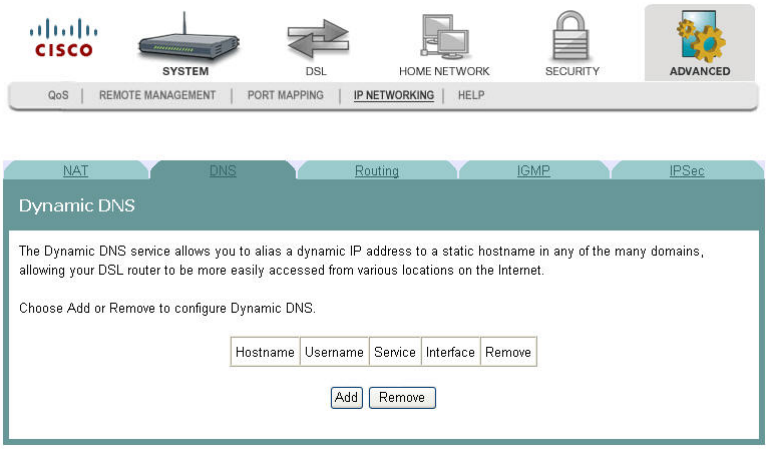
1. Click **Advanced** on the main screen.
2. Click **IP Networking.** The NAT screen opens.



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

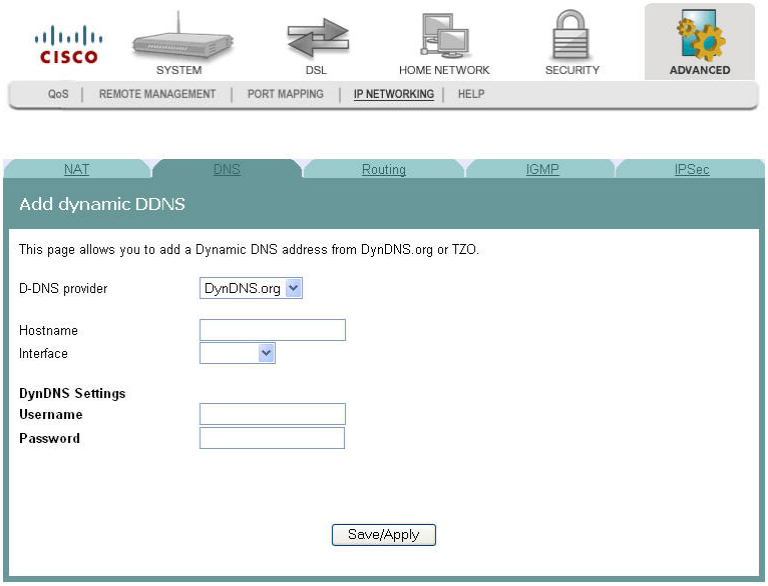


4 Click **Dynamic DNS**. The Dynamic DNS screen opens.



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

Q. to reviewers Dynamic should be a capital D on screen.



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.

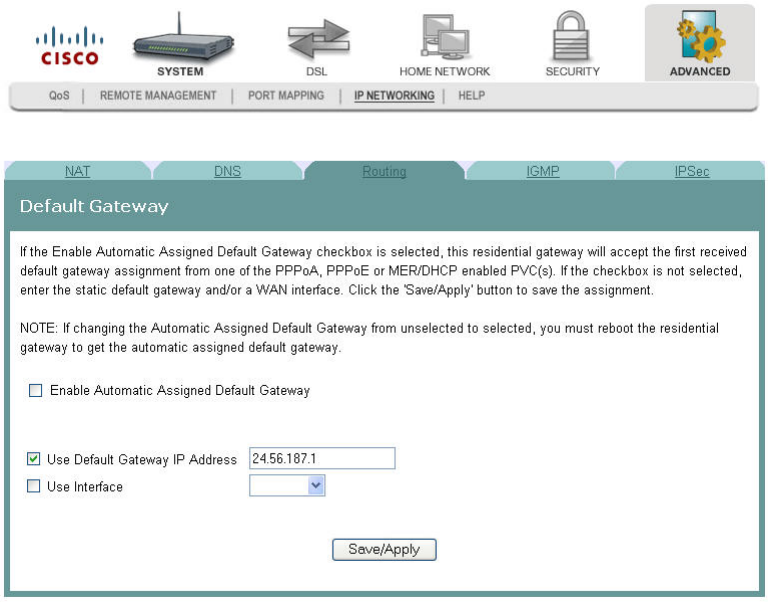
10 Click **Save/Apply**.

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

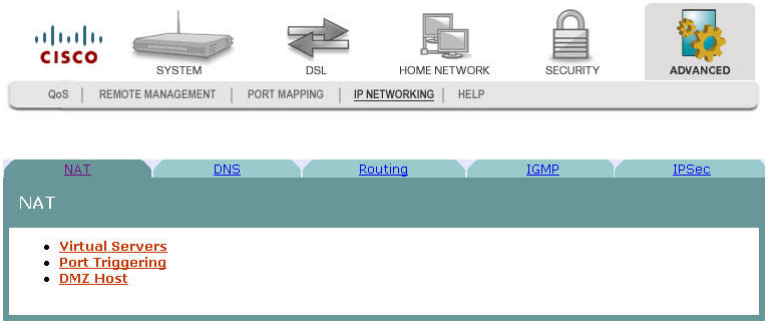


Assigning Default Gateways

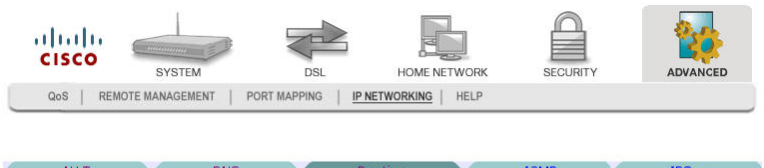
To assign a default gateway, complete the following steps.

1 Click **Advanced** on the main screen.

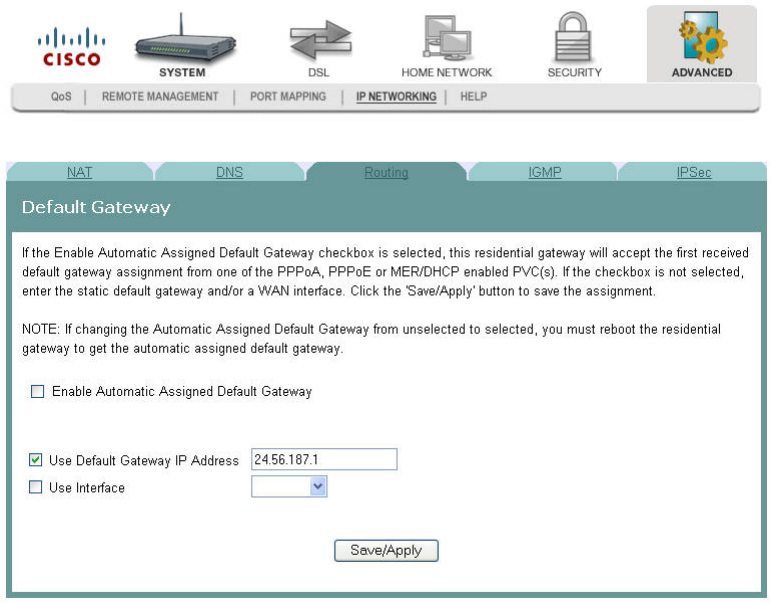
2 Click **IP Networking.** The NAT screen opens.



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 defautl gateway?

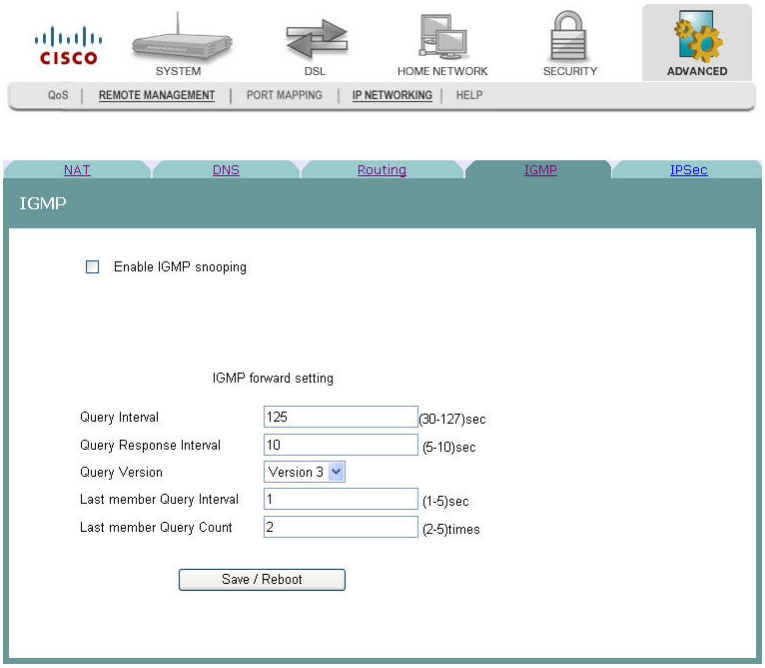
- If **yes**, be sure the Enable Automatic Assigned Default Gateway check box is checked. If this check box is checked, the residential gateway will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s).
- If **no**, be sure the Enable Automatic Assigned Default Gateway check box is not checked. If the check box is not checked, enter the static default gateway AND/OR a WAN interface.

6 Click **Save/Apply** to save your selection.

Internet Group Management Protocol

IGMP screen allows you to configure the Internet group management protocol (IGMP) parameters. The Internet Group Management Protocol 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 hosts are part of which multicast groups.

Path: Advanced > IP Networking > IGMP



The

Enabling IGMP Snooping

IGMP snooping is???? Reviewer question

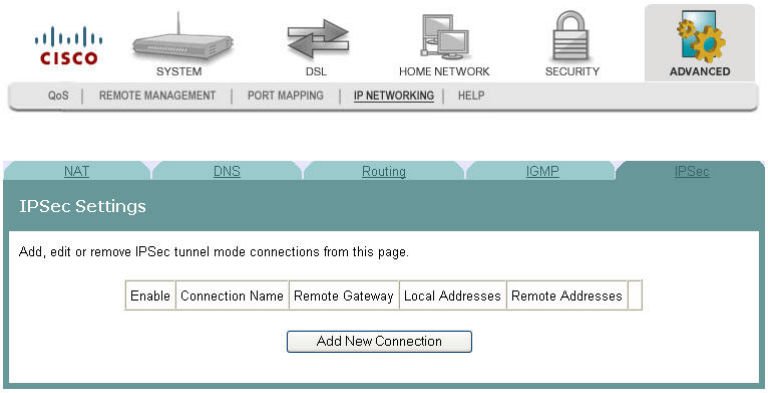
To enable IGMP snooping, complete the following steps.

1. Select the **Enable IGMP snooping** field.
2. In the Query Interval field, enter the interval in seconds.
3. In the Query Response Interval field, enter the interval in seconds.
4. In the Query Version field, choose the version from the drop-down list.
5. In the Last member Query Interval field, enter the interval in seconds.
6. In the Last member Query Count field, enter the number of times you want the system to query.
7. Click **Save/Reboot** to save your changes and reboot the system.

IPSec Settings

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

Path: Advanced > IP Networking > IPSec

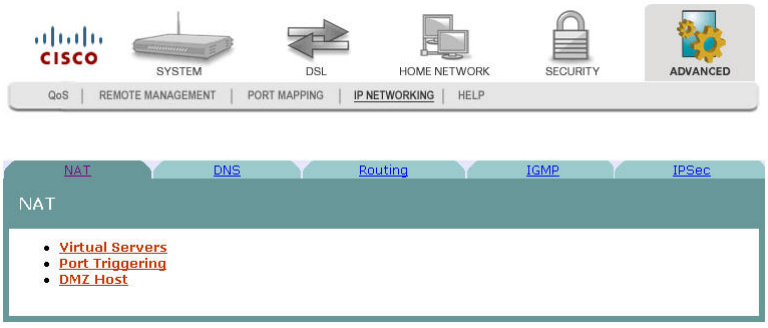


Adding an IPSec Connection

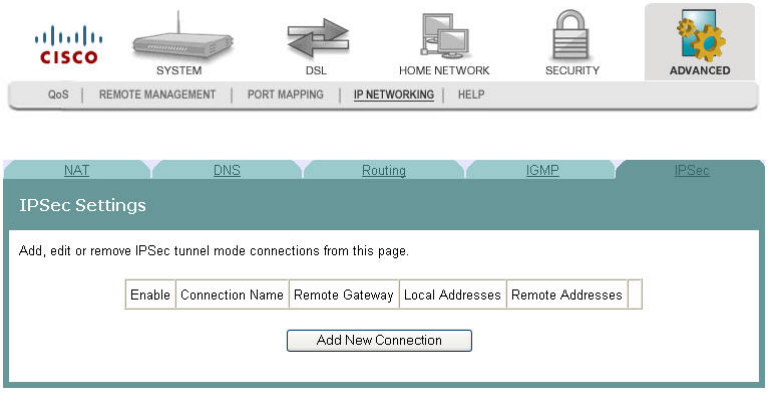
To add an IPSec connection, complete the following steps.

1 Click **Advanced** on the main screen.

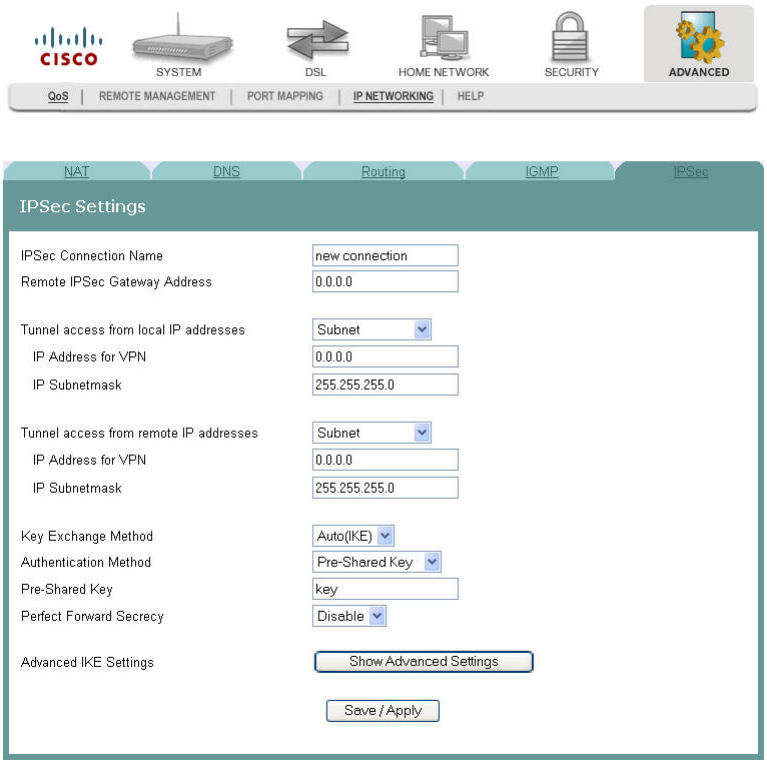
2 Click **IP Networking.** The NAT screen opens.



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



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



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 Key Exchange Method field, select Auto(IKE) or manual.

11 In the Authentication Method field, select Pre-Shared Key or Certificate (X.509).

12 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.

13 In the Perfect Forward Secrecy field, select one of the following options:

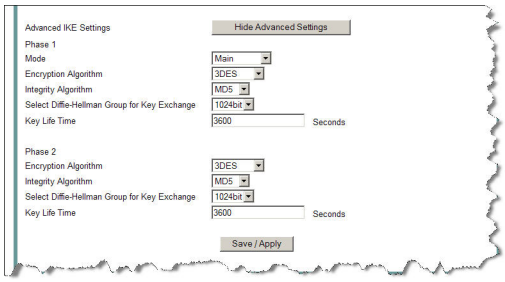
- If you select Enable, Perfect Forward Secrecy is enabled.

  OR

- If you select Disable, Perfect Forward Secrecy is disabled.

14 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 17.

15 Complete the advanced settings as follows:

a In the Phase 1 Mode field, select Main or Aggressive.

b In the Encryption Algorithm field, select one of the following encryption algorithms:

- 3DES
- AES -128
- AES - 192
- AES - 256

c In the Integrity Algorithm field, select MD5 or SHA1.

d 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

e In the Key Life Time, enter the life of the key in seconds.

16 Repeat step 15 for each phase.

17 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

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	**Technical Support** ■ For *Digital Broadband Delivery System* products only, call: – Toll-free: 1-800-283-2636 – Local: 770-236-2200 – Fax: 770-236-2488 ■ For all products *other than* Digital Broadband Delivery System, call: – Toll-free: 1-800-722-2009 – Local: 678-277-1120 – Fax: 770-236-2306 **Customer Service** ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 ■ Fax: 770-236-5477

The United Kingdom and Europe

Europe	European Technical Assistance Center (EuTAC), Belgium	**Product Information** ■ Telephone: 32-56-445-444 **Technical Support** ■ Telephone: 32-56-445-197 or 32-56-445-155 ■ Fax: 32-56-445-061

Asia-Pacific

China	Hong Kong	**Technical Support** Telephone: 011-852-2588-4745 Fax: 011-852-2588-3139

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.

Service Provider Video Technology Group
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678.277.1000
www.scientificatlanta.com

March 2009 Printed in United States of America Part Number 4030765 Rev 01