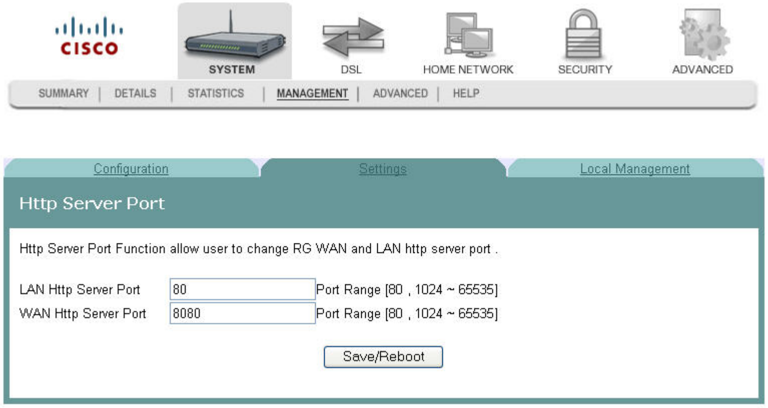
Http Server Port

The Http Server Port screen allows you to modify the

Q. to reviewers



Http Server Port

Http Server Port Function allow user to change RG WAN and LAN http server port .

LAN Http Server Port 80 Port Range [80 , 1024 ~ 65535]

WAN Http Server Port 8080 Port Range [80 , 1024 ~ 65535]

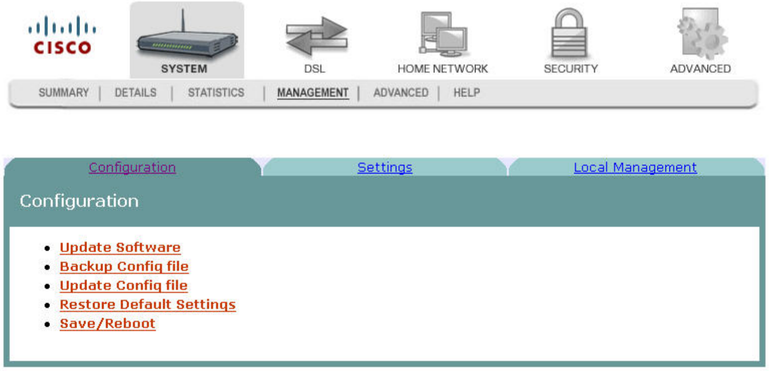
Modifying the Http Server Ports

Q. to reviewers: need help with procedure

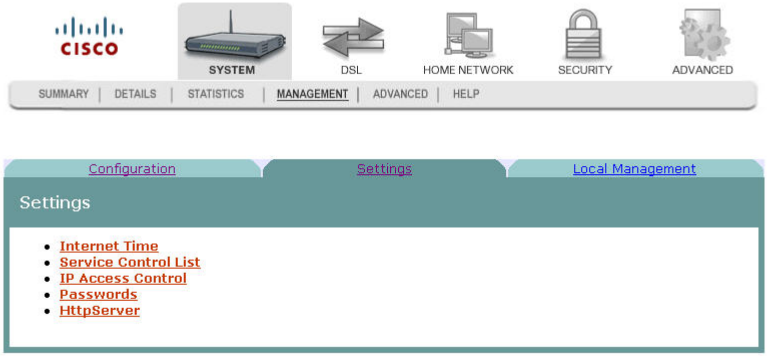
To modify the Http Server ports, complete the following steps.

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

2 Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



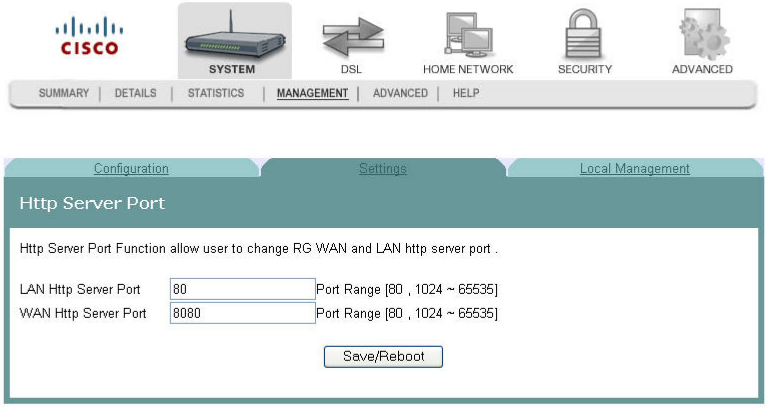
3 Click the **Settings** tab. The Settings screen opens.



Settings

- Internet Time
- Service Control List
- IP Access Control
- Passwords
- HttpServer

4 Click HttpServer. The Http Server Port opens.



Http Server Port

Http Server Port Function allow user to change RG WAN and LAN http server port .

LAN Http Server Port	80	Port Range [80 , 1024 ~ 65535]
WAN Http Server Port	8080	Port Range [80 , 1024 ~ 65535]

Save/Reboot

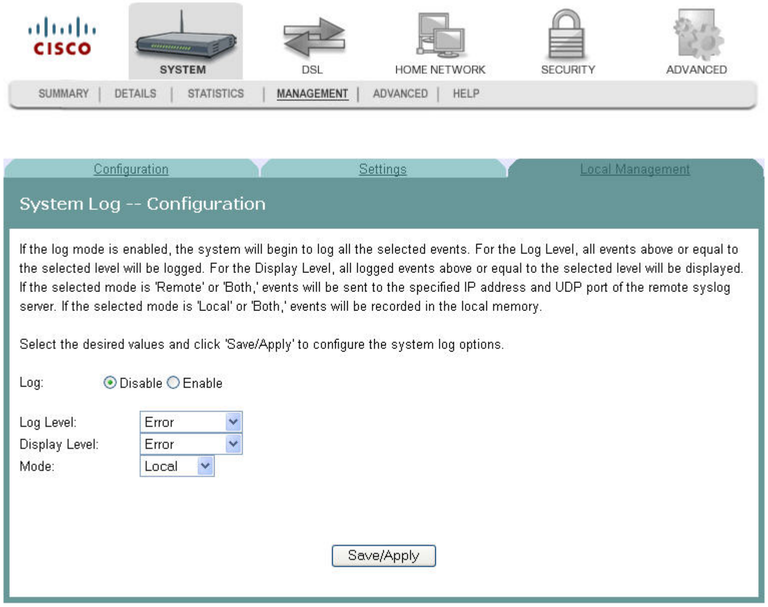
5 In the LAN Http Server Port field, enter the

6 In WAN Http Server Port field, enter the

System Log Configuration

The System Log -- Configuration screen allows you to log all the selected events on the residential gateway. For example, a failed login is an event that you can select.

Path: System > Management > Local Management > System Log Configuration



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log: ● Disable ○ Enable

Log Level: Error

Display Level: Error

Mode: Local

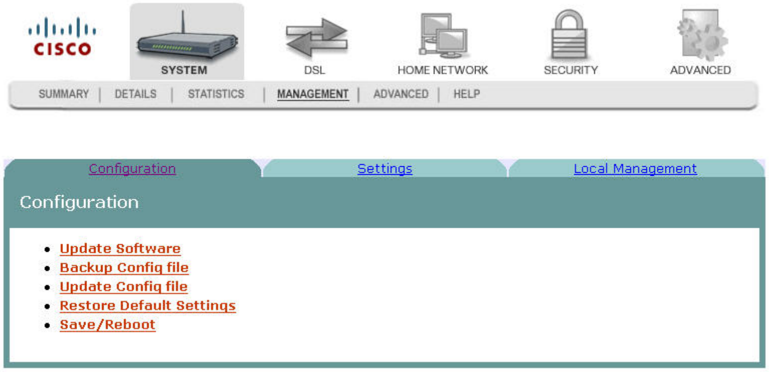
Save/Apply

Logging Events

To log selected events, complete the following steps.

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

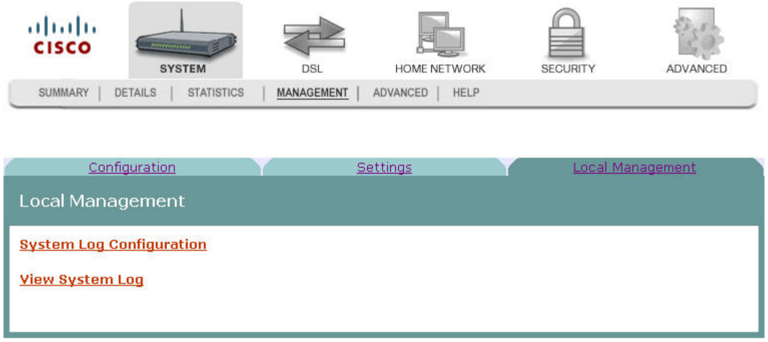
2 Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



Configuration

- Update Software
- Backup Config file
- Update Config file
- Restore Default Settings
- Save/Reboot

3 Click the **Local Management** tab. The Local Management screen opens.

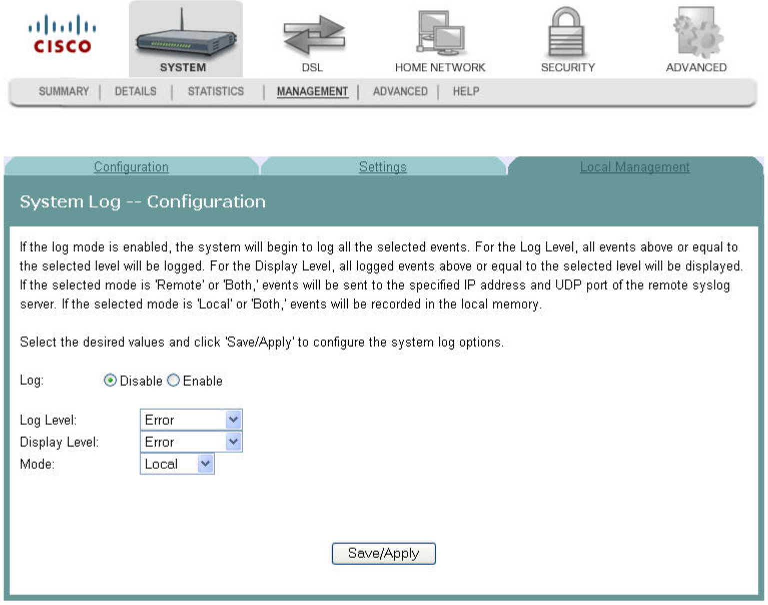


Local Management

System Log Configuration

View System Log

4 Click **System Log Configuration**. The System Log Configuration screen opens.



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log: ● Disable ○ Enable

Log Level: Error

Display Level: Error

Mode: Local

5 Do you want to enable the logging of events?

- If **yes**, in the Log field select **Enable** and go to step 6.
- If **no**, in the Log field, select **Disable** and click **Save/Apply** to turn off logging. You have completed this procedure.

6 In the Log Level field, select the level of events that you want to log from the following options. All events above or equal to the selected level will be logged.

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational

- Debugging

7 In the Display Level field, select the level of the logged events that you want to display from the following options. All logged events above or equal to the selected level will be displayed.

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debugging

8 Select the mode for the logging from the following options. If the selected mode is "remote" or "both," events are sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is "local" or "both," events are recorded in the local memory.

- Local. Events are logged in memory. You must log in to the device to display the events.
- Remote. Events log is sent to a remote server (syslog server).
- Both. Events are logged in memory and are sent to the remote server.

9 Click **Save/Apply** to start logging events.

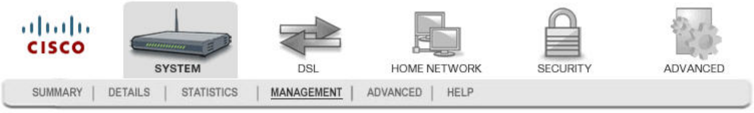
Disabling Logging

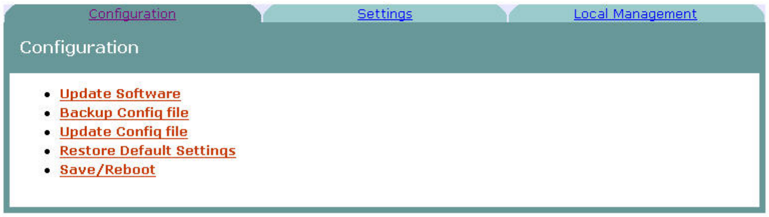
To disable the logging function, complete the following steps.

Q. to reviewer test this procedure against application

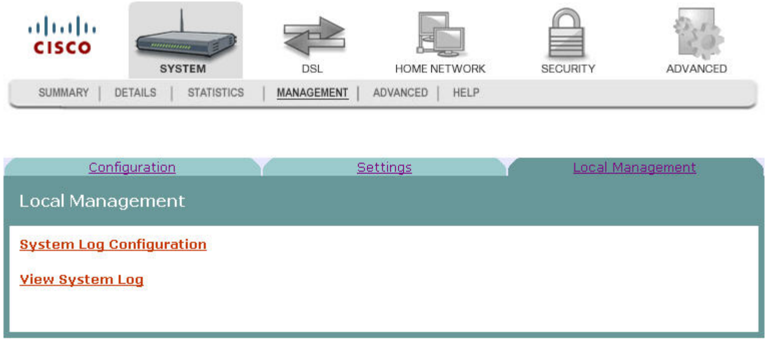
1 Click **System** on the main screen.

2 Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.





3 Click the **Local Management** tab. The Local Management screen opens.

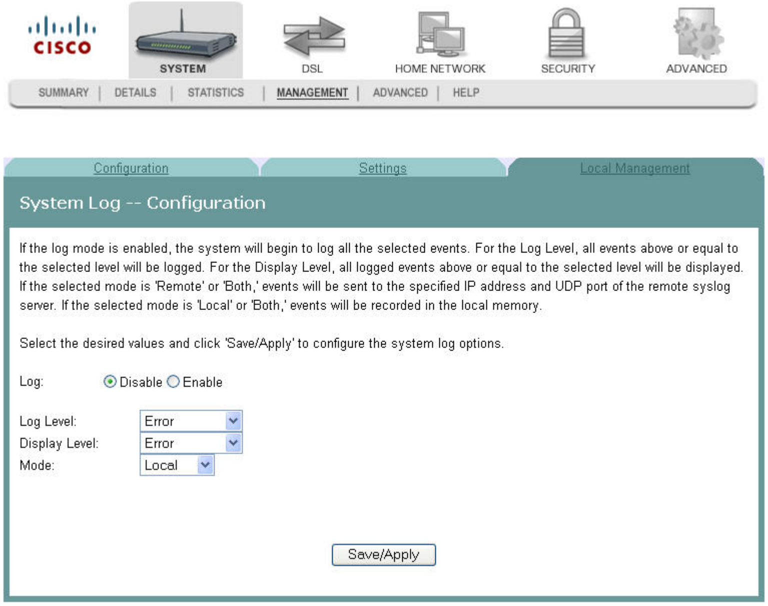


Local Management

System Log Configuration

View System Log

4 Click **System Log Configuration**. The System Log Configuration screen opens.



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log: ● Disable ○ Enable

Log Level: Error

Display Level: Error

Mode: Local

Save/Apply

5 In the Log field, click **Disable**.

6 In the Log Level field, select from the following options to indicate the level of alarms to be logged:

- Emergency
- Alert
- Optical
- Error
- Warning
- Notice
- Informational
- Debugging

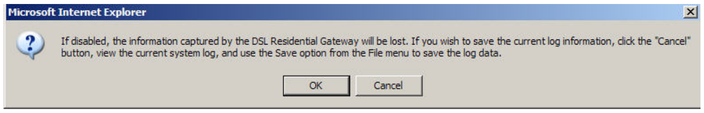
7 In the Display Level field, select from the following options to indicate the level of alarms that you want displayed:

- Emergency
- Alert
- Optical
- Error
- Warning
- Notice
- Informational
- Debugging

8 In the Mode field, select from the following options to indicate the location to store the logs.

- Local. Store on the residential gateway.
- Remote. Store on a remote log server.
- Both. Store on the residential gateway and on the remote log server.

9 Click **Save/Apply**. The following prompt appears alerting you that you will lose any information captured by the residential gateway:



If disabled, the information captured by the DSL Residential Gateway will be lost. If you wish to save the current log information, click the "Cancel" button, view the current system log, and use the Save option from the File menu to save the log data.

10 Are you sure you want to disable logging and lose the captured data?

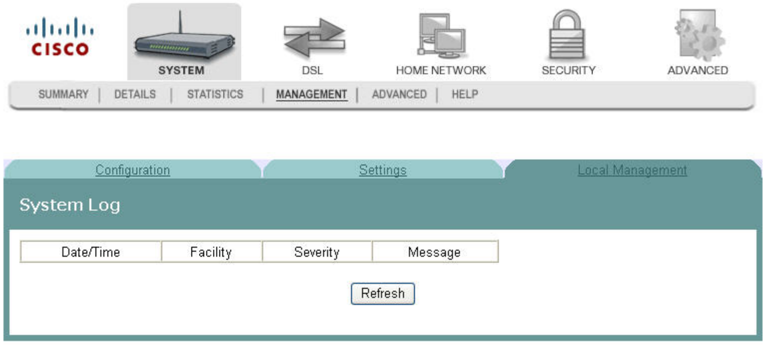
- If yes, click **OK** to turn off logging.
- If no, click **Cancel**.

System Logs

The System Log screen allows you to view the logs of activity for the residential gateway.

Q. to reviewers. How many or how big are events stored? How long are they stored? Will reset or power failure clear t hem? If this is a circular file, if so max size before roll over.

Path: System > Management > Local Management > View System Log



System Log

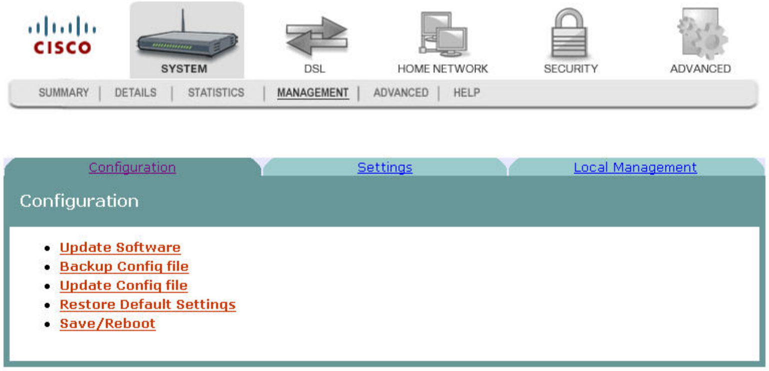
Date/Time	Facility	Severity	Message

Viewing System Logs

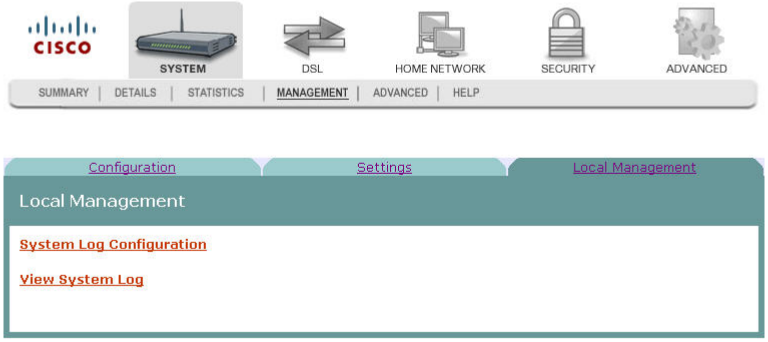
To view the system log for the residential gateway, complete the following steps.

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

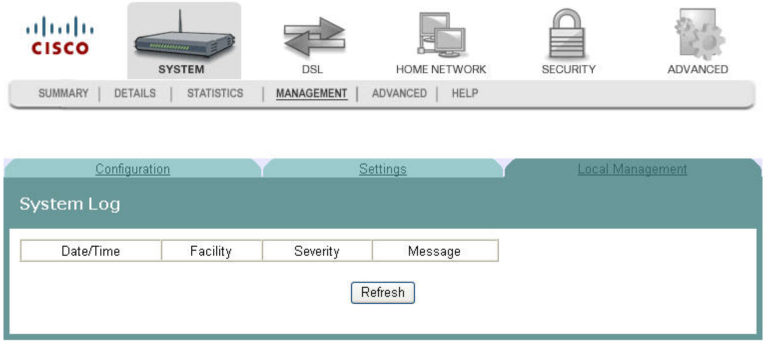
2 Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



3 Click the **Local Management** tab. The Local Management screen opens.



4 Click **View System Log**. The System Log screen opens.



Date/Time	Facility	Severity	Message

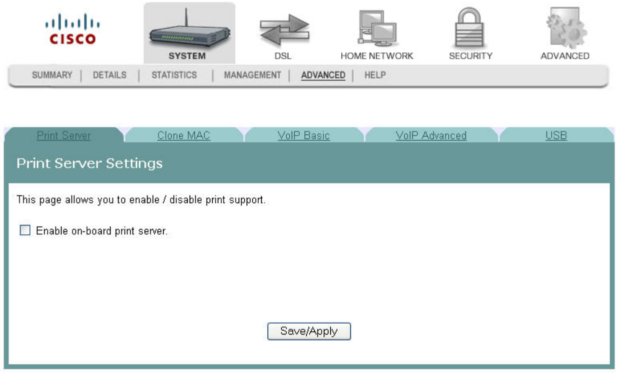
5 Review the log entries on the screen.

6 Click **Refresh** to refresh the system log.

Print Server Settings

The Print Server Setting screen allows you to enable or disable printer support from the USB connection.

Path: System > Advanced > Print Server



Print Server Settings

This page allows you to enable / disable print support.

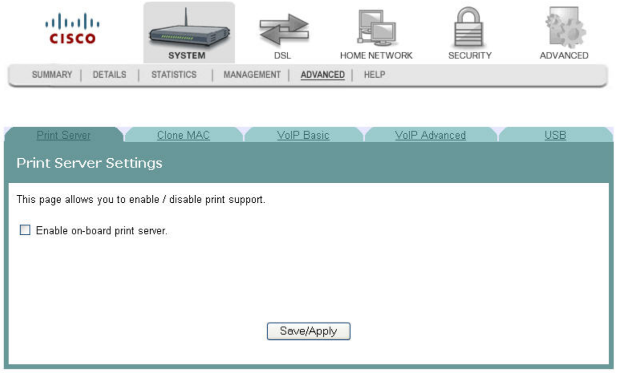
□ Enable on-board print server.

Enabling the Print Server

To enable the print server, complete the following steps.

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

2 Click the **Advanced** tab. The Print Server settings screen opens with the Print Server tab in the forefront.

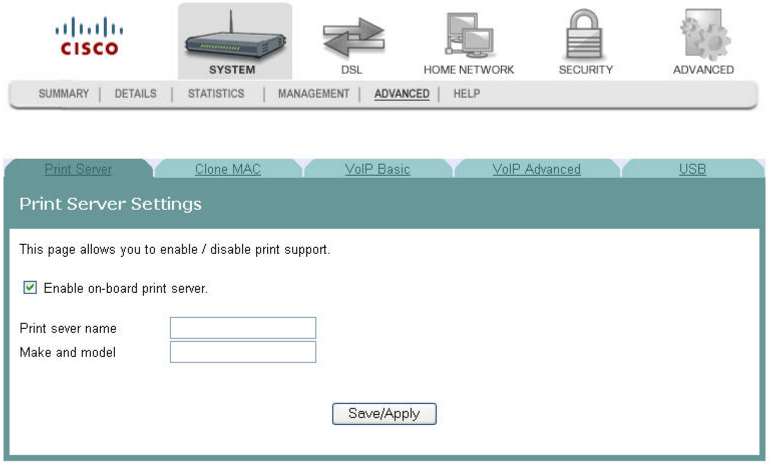


Print Server Settings

This page allows you to enable / disable print support.

□ Enable on-board print server.

3 Select the **Enable on-board print server** check box. The screen populates with more fields.



Print Server Settings

This page allows you to enable / disable print support.

☑ Enable on-board print server.

Print sever name

Make and model

4 In the Print server name field, enter the name of the print server you want to enable.

5 In the Make and model field, enter the make and model of the printer.

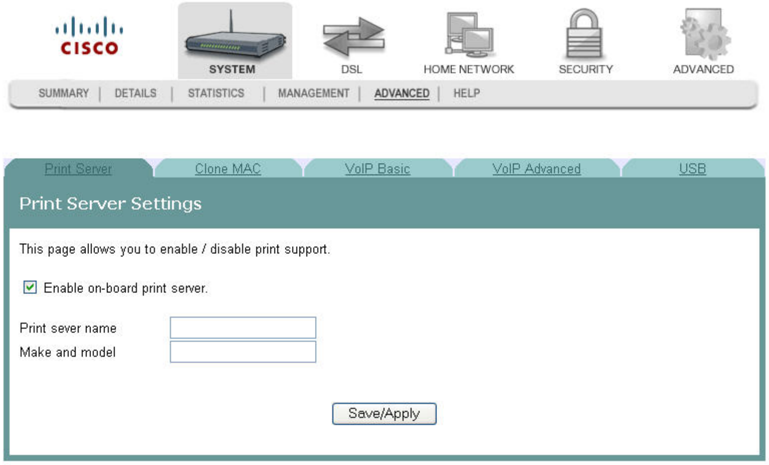
6 Click **Save/Apply** to enable the print server.

Disabling the Print Server

To disable the print server, complete the following steps.

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

2 Click the **Advanced** tab. The Print Server settings screen opens with the Print Server tab in the forefront.



Print Server Settings

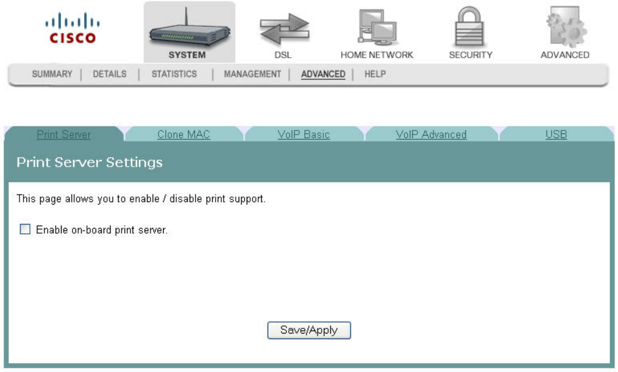
This page allows you to enable / disable print support.

☑ Enable on-board print server.

Print sever name

Make and model

3 Clear the Enable on-board print server check box. The screen refreshes and the fields for entering print server name, make, and mode are removed from the screen.



Print Server Settings

This page allows you to enable / disable print support.

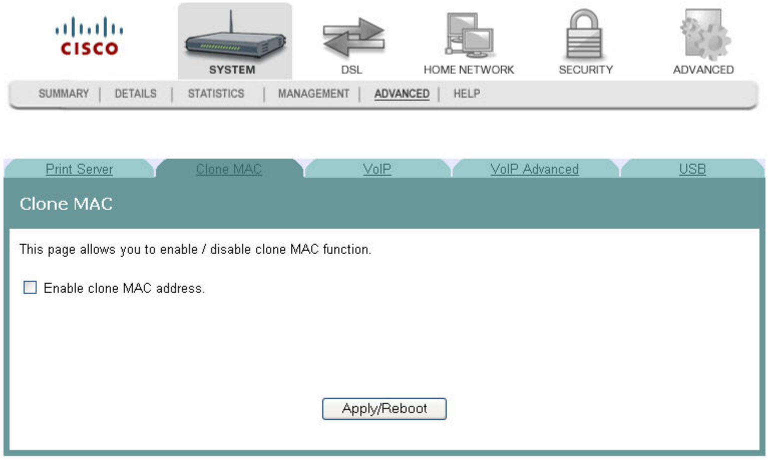
□ Enable on-board print server.

4 Click **Save/Apply** to disable the print server.

Clone MAC Addresses

The Clone MAC screen allows you to enable or disable the clone MAC function. The Clone MAC function allows you to clone MAC addresses so that the residential gateway assumes the MAC address of an attached device or a user-specified MAC address.

Path: System > Advanced > Clone MAC



Clone MAC

This page allows you to enable / disable clone MAC function.

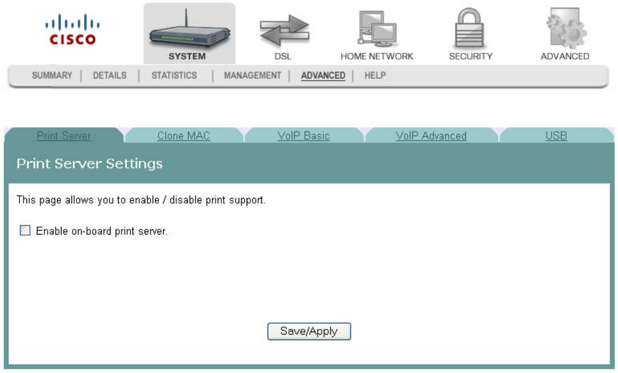
□ Enable clone MAC address.

Enabling the Clone MAC Function

To enable the Clone MAC function, complete the following steps.

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

2 Click the **Advanced** tab. The Print Server settings screen opens with the Print Server tab in the forefront.

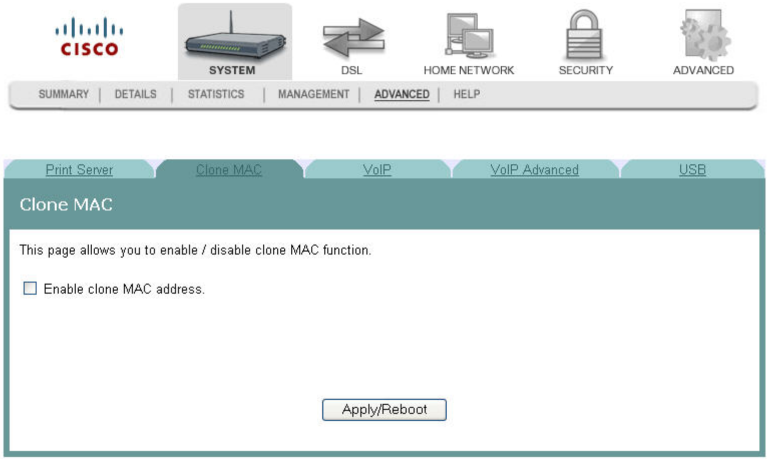


Print Server Settings

This page allows you to enable / disable print support.

□ Enable on-board print server.

3 Click the **Clone MAC** tab.

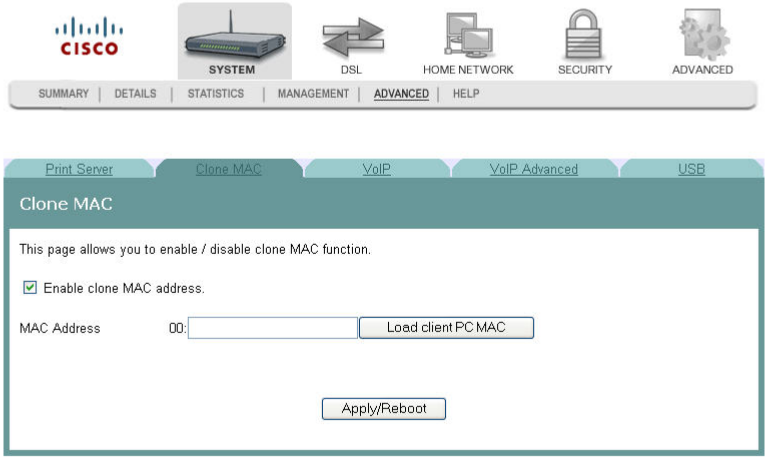


Clone MAC

This page allows you to enable / disable clone MAC function.

□ Enable clone MAC address.

4 Select the **Enable clone MAC address** check box. The screen populates with more fields.



Clone MAC

This page allows you to enable / disable clone MAC function.

☑ Enable clone MAC address.

MAC Address 00:

5 In the MAC Address field, enter the MAC address that you want to clone. You can also click **Load/client PC MAC** to locate an address you want to clone.

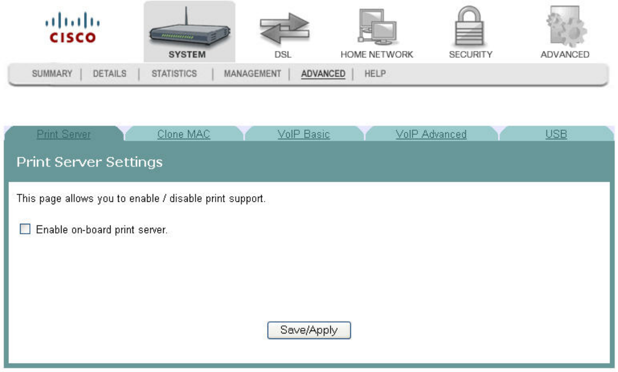
6 Click **Apply/Reboot** to clone the MAC address. The residential gateway reboots and assumes the MAC address you have specified.

Disabling the Clone MAC Function

To disable the Clone MAC function, complete the following steps.

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

2 Click the **Advanced** tab. The Print Server settings screen opens with the Print Server tab in the forefront.

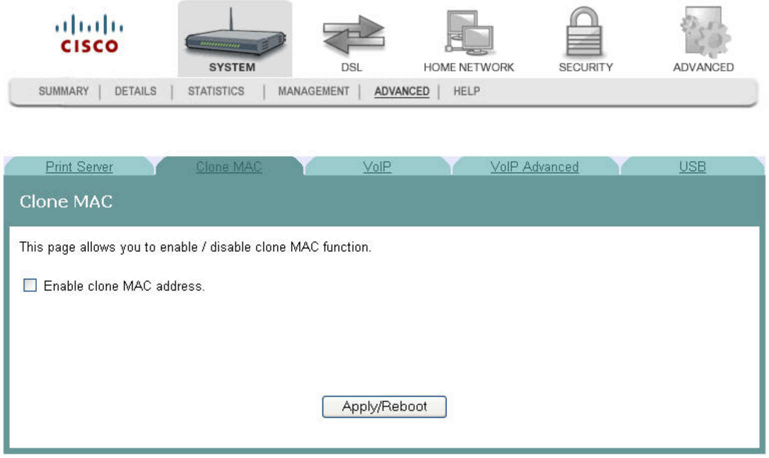


Print Server Settings

This page allows you to enable / disable print support.

□ Enable on-board print server.

3 Click the **Clone MAC** tab.



Clone MAC

This page allows you to enable / disable clone MAC function.

□ Enable clone MAC address.

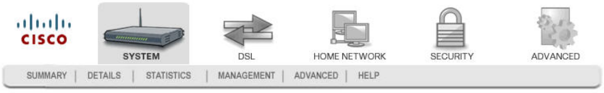
4 Uncheck the **Enable clone MAC address** check box. The screen refreshes and the field for entering the MAC address is removed from the screen.

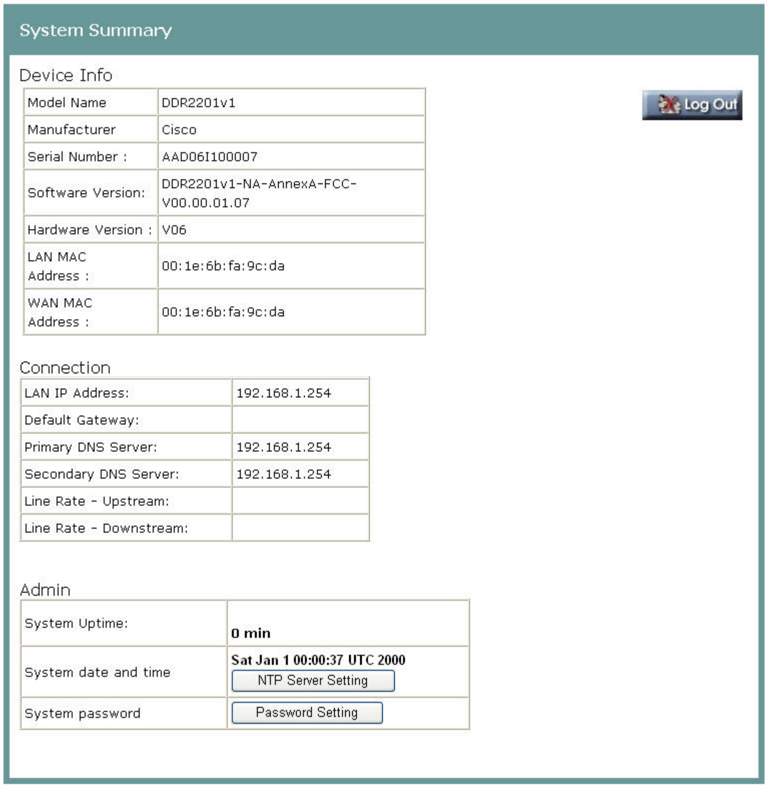
5 Click **Apply/Reboot** to disable the Clone MAC function.

Voice SIP Basic Configuration

The Voice ---- SIP screen allows you to enter and save the session initiation protocol (SIP) parameters and to start and stop the voice application.

Path: System > Advanced > VoIP Basic


cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | DETAILS | STATISTICS | MANAGEMENT | ADVANCED | HELP



System Summary

Device Info

Model Name	DDR2201v1
Manufacturer	Cisco
Serial Number :	AAD06I100007
Software Version:	DDR2201v1-NA-AnnexA-FCC-V00.00.01.07
Hardware Version :	V06
LAN MAC Address :	00:1e:6b:fa:9c:da
WAN MAC Address :	00:1e:6b:fa:9c:da

Connection

LAN IP Address:	192.168.1.254
Default Gateway:	
Primary DNS Server:	192.168.1.254
Secondary DNS Server:	192.168.1.254
Line Rate - Upstream:	
Line Rate - Downstream:	

Admin

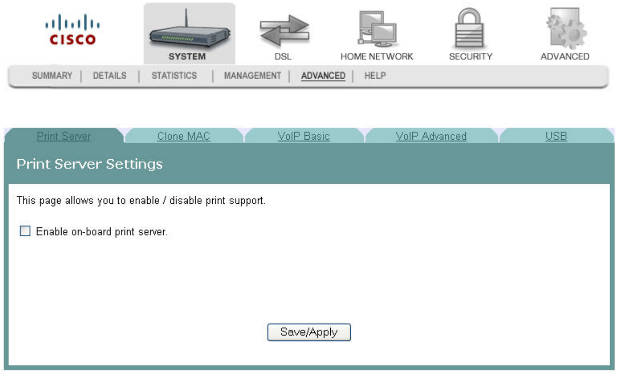
System Uptime:	**0 min**
System date and time	**Sat Jan 1 00:00:37 UTC 2000** NTP Server Setting
System password	Password Setting

Setting Up VoIP

To enter the VoIP parameters, complete the following steps.

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

2 Click **Advanced**. The Print Server Settings screen opens with the Print Server tab in the forefront.

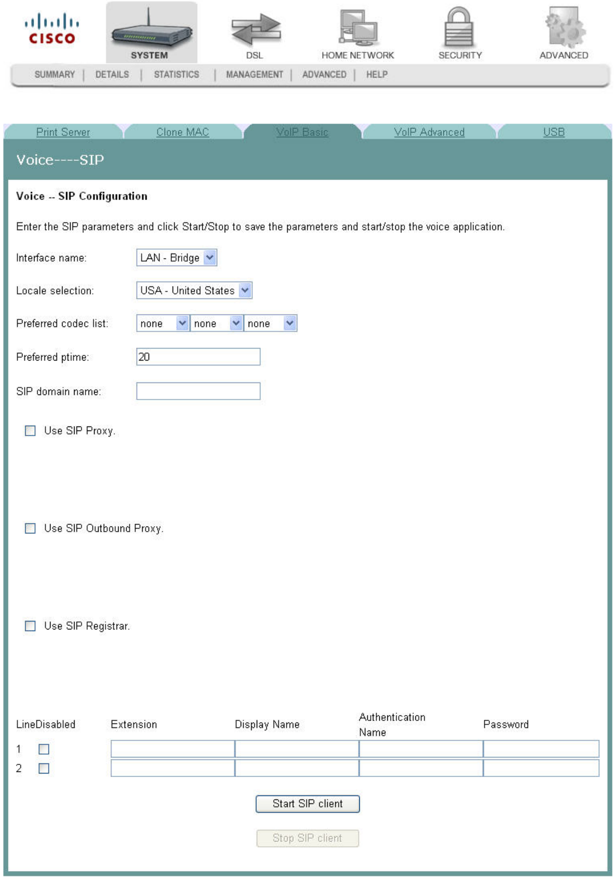


Print Server Settings

This page allows you to enable / disable print support.

□ Enable on-board print server.

3 Click the **VoIP Basic** tab. The Voice ---- SIP screen opens.



Voice----SIP

Voice -- SIP Configuration

Enter the SIP parameters and click Start/Stop to save the parameters and start/stop the voice application.

Interface name: LAN - Bridge

Locale selection: USA - United States

Preferred codec list: none none none

Preferred ptime: 20

SIP domain name:

□ Use SIP Proxy.

□ Use SIP Outbound Proxy.

□ Use SIP Registrar.

LineDisabled		Extension	Display Name	Authentication Name	Password
1	□				
2	□				

4 In the Interface name field, select the interface you want to use for VoIP.

5 In the Locale selection field, select the country where you are located.

6 In the Preferred codec field, select one of the following codec values:

Note: If you want to indicate an order of preference, enter a codec value for each column.

- G711U

- G711A
- G723
- G726
- G729
- BV16
- iLBC

7 In the Preferred ptime field, enter the time in seconds.

8 In the SIP domain name field, enter the domain name for the session initiation protocol (SIP) server.

9 Do you wish to use SIP Proxy?

- If **yes**, click in the Use SIP Proxy field to enter a check mark.
- If **no**, make sure the Use SIP Proxy field is deselected.

10 Do you wish to use an SIP Outbound proxy?

- If **yes**, select the Use SIP Outbound Proxy field.
- If **no**, make sure the Use SIP Outbound Proxy field is deselected.

11 Do you wish to use SIP Registrar?

- If **yes**, select the Use SIP Registrar field.
- If **no**, make sure the Use SIP Registrar field is deselected.

12 Do you wish to enable SIP tag matching?

- If **yes**, select the Enable SIP tag matching (clear for Vonage Interop) field.
- If **no**, make sure the Enable SIP tag matching (clear for Vonage Interop) field is deselected.

13 Do you wish to use a remote server for SIP log messages?

- If **yes**, select the Remote server for SIP log messages field.
- If **no**, make sure the Remote server for SIP log messages field is deselected.

14 In the Log IP Address field, enter the IP address for the log server.

15 In the Log port field, enter the port number for the log server.

16 In the Extension field, enter the phone number (extension) for the VoIP line.

17 In the Password field, enter the password for the extension. This allows you to authenticate the phone number.

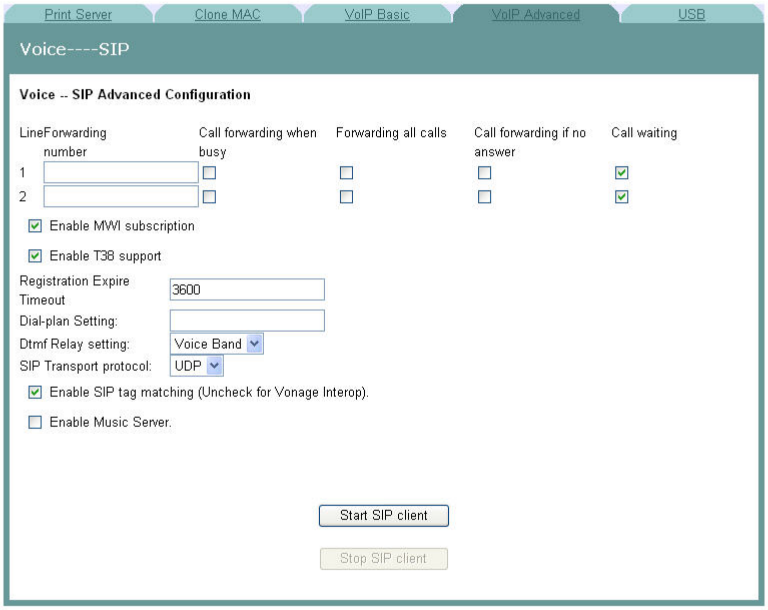
18 Do you want to activate the line?

- If **yes**, click **Start SIP client** to save your settings and to activate the line.
- If **no**, click **Stop SIP client** to deactivate the line.

Voice SIP Advanced Configuration

The Voice----SIP screen allows you to configure the more advanced VOIP features, such as call forwarding and ....

Path: System > Advanced > VoIP Advanced



Voice -- SIP Advanced Configuration

LineForwarding number		Call forwarding when busy	Forwarding all calls	Call forwarding if no answer	Call waiting
1		□	□	□	☑
2		□	□	□	☑

☑ Enable MWI subscription

☑ Enable T38 support

Registration Expire Timeout: 3600

Dial-plan Setting:

Dtmf Relay setting: Voice Band

SIP Transport protocol: UDP

☑ Enable SIP tag matching (Uncheck for Vonage Interop).

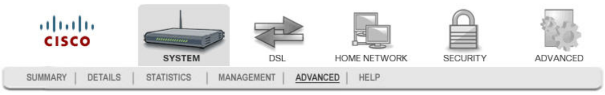
□ Enable Music Server.

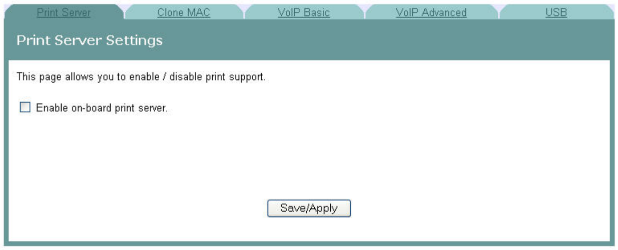
Setting Up Advanced VOIP Features

To set up the advanced VOIP features, complete the following steps.

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

2 Click **Advanced**. The Print Server Settings screen opens with the Print Server tab in the forefront.

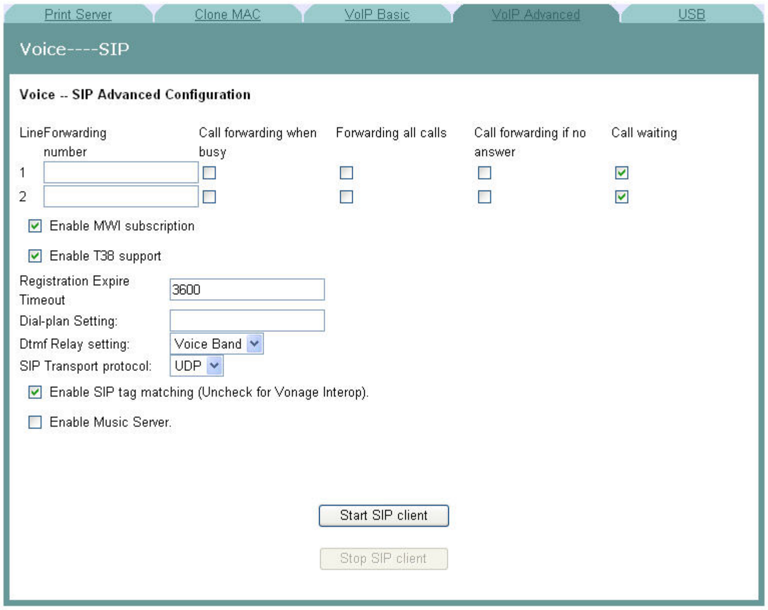




This page allows you to enable / disable print support.

□ Enable on-board print server.

3 Click the **VoIP Advanced** tab. The Voice ---- SIP screen opens.



Voice -- SIP Advanced Configuration

Line	Forwarding number	Call forwarding when busy	Forwarding all calls	Call forwarding if no answer	Call waiting
1		☐	☐	☐	☑
2		☐	☐	☐	☑

☑ Enable MWI subscription

☑ Enable T38 support

Registration Expire Timeout: 3600

Dial-plan Setting:

Dtmf Relay setting: Voice Band

SIP Transport protocol: UDP

☑ Enable SIP tag matching (Uncheck for Vonage Interop).

☐ Enable Music Server.

4 In the Forwarding Line number field, enter the number to which you want to forward calls. Configure how calls are forwarded to this line using the following options:

a Check the Call forwarding when busy check box if you want to forward this line to another number when this line is busy.

b Check the Forwarding all calls check box if you want to forward all calls to this line.

c Check the Call forwarding if no answer check box if you want to forward this line if the caller receives no answer.

d Check the Call waiting check box if you want to enable call waiting for this line.

5 Repeat step 4 for a second phone line for which you wish to forward incoming calls.

6 Check the Enable MWI subscription check box if you want to enable message waiting indicator.

7 Check the Enable T38 support check box if you want to enable T38 fax support.

8 In the Registration Expire Timeout field, enter the registration expiration time of the SIP client.

9 In the Dial-Plan Setting field, enter the dial plan for the line. For example, enter how many digits the user must enter before the call attempt is made.

10 In the Dtmf Relay setting field, select one of the following settings:

- Sip Info
- RFC2833
- Voice Band

11 In the SIP Transport protocol field, select the protocol you will support from the following options:

- All
- TCP
- UDP
- TLS

12 Check the Enable SIP tag matching (Uncheck for Vonage Interop) check box if you want to enable session initiation protocol.

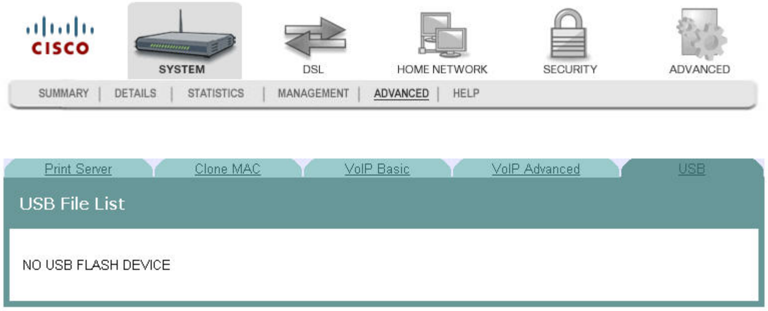
13 Check the Enable Music Server check box if you want to have music playing while callers wait.

14 Click Start SIP client or click Stop SIP client if you want to start or stop the SIP client.

USB File List

The USB File List screen allows you to view and download the content of a USB flash drive from any computer connected to the gateway. This feature allows your residential gateway to act like a shared network drive.

Path: System > Advanced > USB



USB File List

NO USB FLASH DEVICE

4

DSL Configuration

The DSL tab allows you to check the status of the DSL connection and to modify the configuration.

Use this chapter to help you check the status of the DSL connection, such as performance, and to modify the DSL configuration.

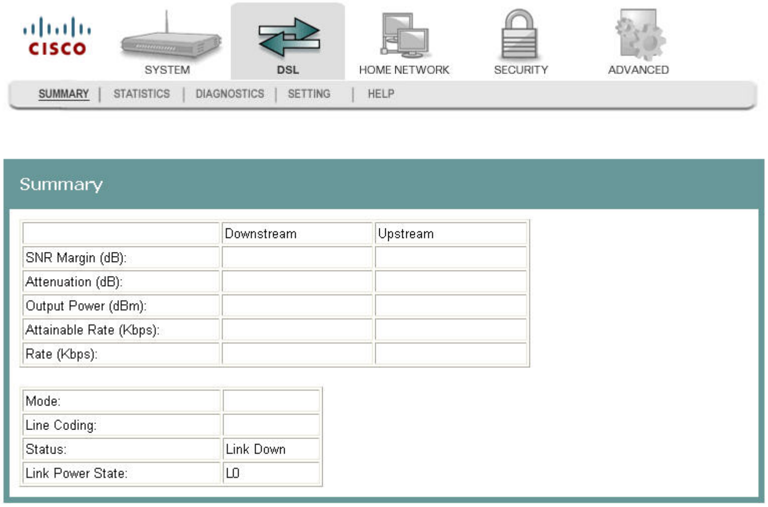
In This Chapter

- DSL Summary 82
- DSL Statistics 83
- DSL Diagnostics 85
- DSL Settings........ 87
- ADSL Tone Settings........ 89
- DSL Advanced Settings 91

DSL Summary

The DSL Summary screen shows the DSL performance and operational configuration of the DSL interface, such as signal to noise ratio and output power and line coding. The DSL chip on the residential gateway automatically detects the best method to use to communicate with the DSL access mutliplexer (DSLAM). This screen reports the results of that process.

Path: DSL > Summary



Summary

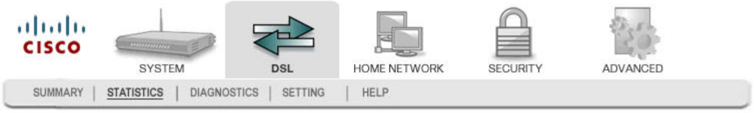
	Downstream	Upstream
SNR Margin (dB):		
Attenuation (dB):		
Output Power (dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		

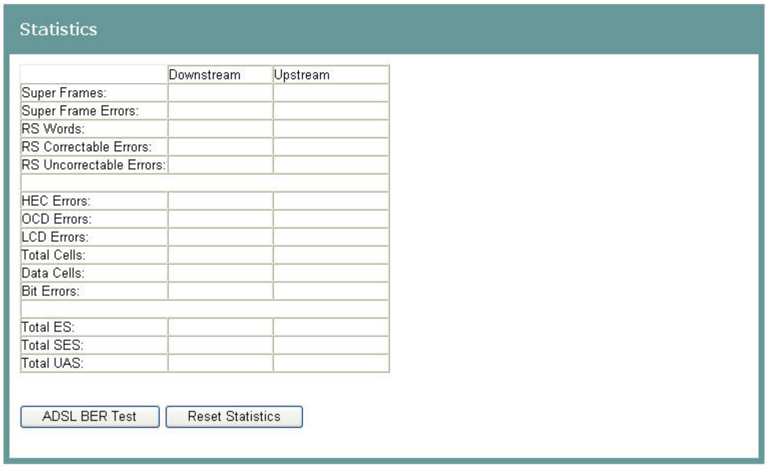
Mode:	
Line Coding:	
Status:	Link Down
Link Power State:	L0

DSL Statistics

The DSL Statistics screen displays statistics for devices and interfaces on the ADSL network. This screen shows the details of the physical layer of the DSL line such as the connection rate and signal to noise ratio.

Path: DSL > Statistics





Statistics

	Downstream	Upstream
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

Testing the Quality of the DSL Connection

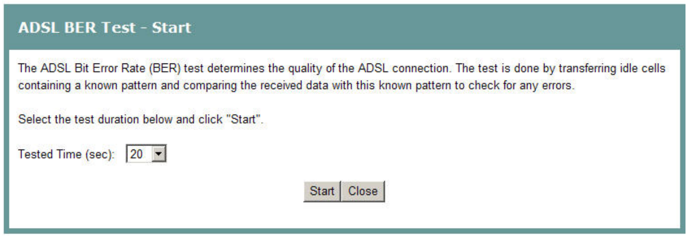
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

To test for quality of the DSL connection, complete the following steps.

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

2 Click the **Statistics** tab. The Statistics screen opens.

3 Click **ADSL BER Test**. The ADSL BER Test - Start screen opens.



ADSL BER Test - Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec): 20

4 In the Tested Time (sec) field, enter the duration of the test in seconds. Values are: 1, 5, 10, 20, 60, 120, 180, or 240 seconds.

5 Click **Start** on the ADSL BER Test - Start screen to start the test.

Reset Statistics

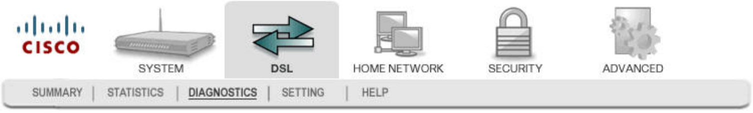
To reset the statistics, complete the following steps.

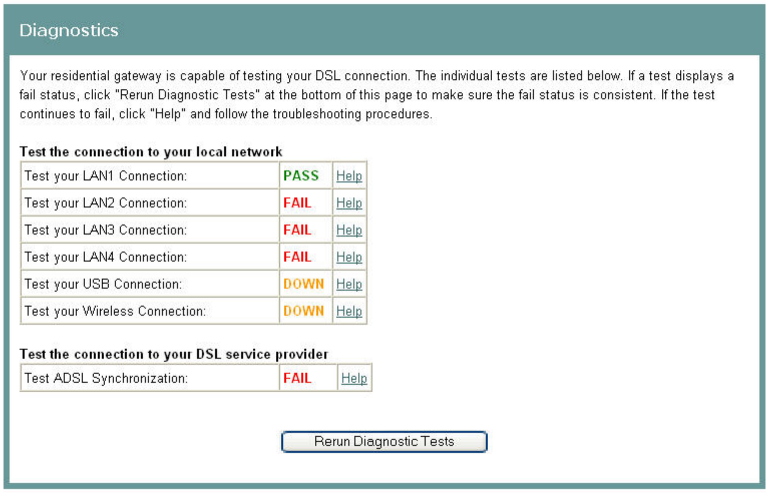
1. Click **DSL** on the main screen.
2. Click the **Statistics** tab. The Statistics screen opens.
3. Click **Reset Statistics** on the Statistics screen. This action clears the ADSL cell counters and sets them to zero.

DSL Diagnostics

The Diagnostics screen shows the results of diagnostics tests that the residential gateway performs while testing your DSL connection. The individual tests are listed on the Diagnostics screen.

Path: DSL > Diagnostics





Diagnostics

Your residential gateway is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your LAN1 Connection:	PASS	Help
Test your LAN2 Connection:	FAIL	Help
Test your LAN3 Connection:	FAIL	Help
Test your LAN4 Connection:	FAIL	Help
Test your USB Connection:	DOWN	Help
Test your Wireless Connection:	DOWN	Help

Test the connection to your DSL service provider

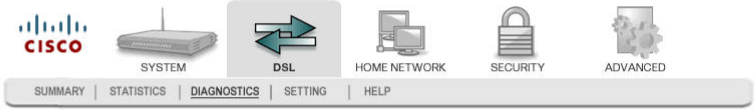
Test ADSL Synchronization:	FAIL	Help

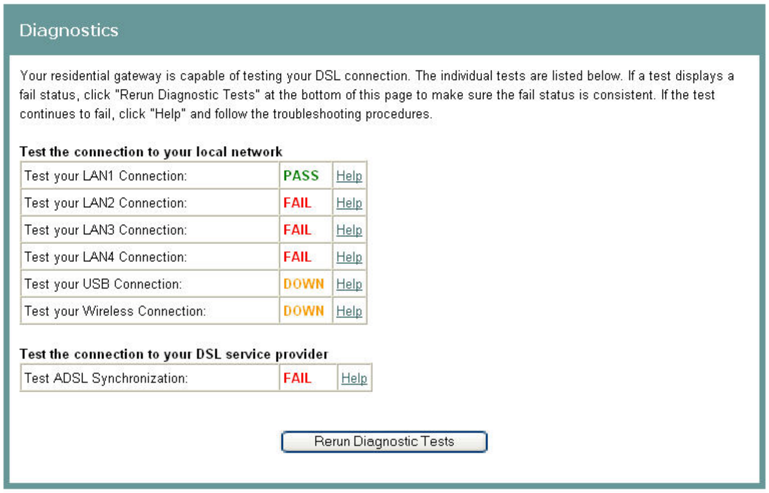
Running Diagnostic Tests

To run diagnostic tests for the residential gateway, complete the following steps.

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

2 Click the **Diagnostics** tab. The Diagnostics screen opens.





Diagnostics

Your residential gateway is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your LAN1 Connection:	PASS	Help
Test your LAN2 Connection:	FAIL	Help
Test your LAN3 Connection:	FAIL	Help
Test your LAN4 Connection:	FAIL	Help
Test your USB Connection:	DOWN	Help
Test your Wireless Connection:	DOWN	Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	FAIL	Help

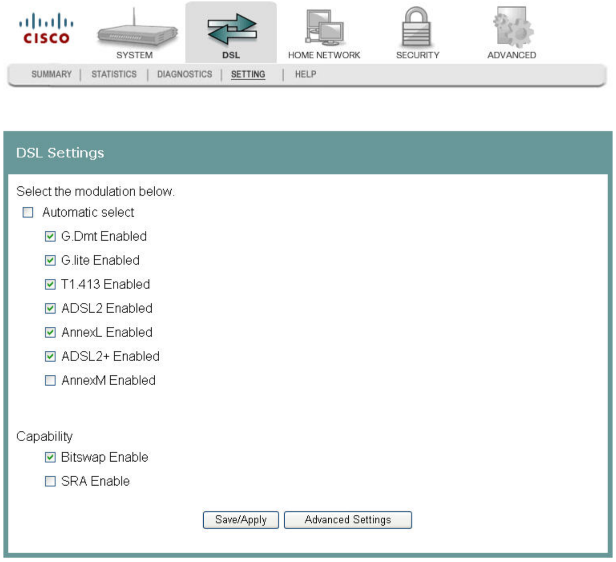
3 Click **Run Diagnostics Tests** to start the diagnostics test.

Q. to reviewers: How do they view the tests?

DSL Settings

The DSL Settings screen allows you to set the modulation for the residential gateway, select a phone line pair, and to select advanced capability of the chip set: seamless rate adaptation (SRA) and bitswap enable.

Path: DSL > Setting



DSL Settings

Select the modulation below.

☐ Automatic select

☑ G.Dmt Enabled

☑ G.lite Enabled

☑ T1.413 Enabled

☑ ADSL2 Enabled

☑ AnnexL Enabled

☑ ADSL2+ Enabled

☐ AnnexM Enabled

Capability

☑ Bitswap Enable

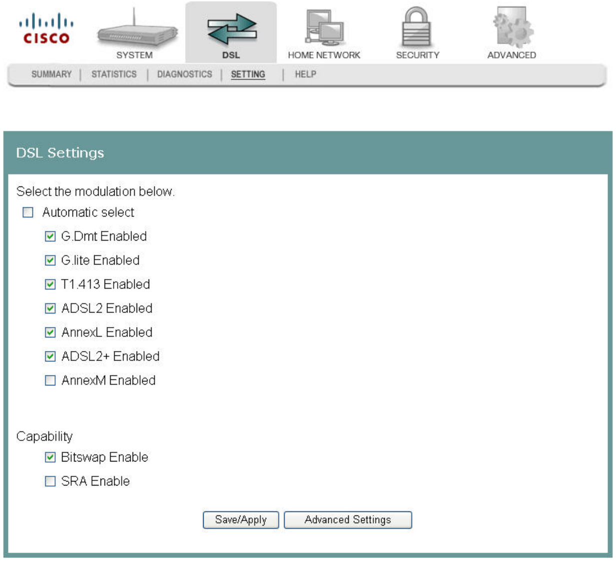
☐ SRA Enable

Configuring DSL Settings

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

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

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



DSL Settings

Select the modulation below.

☐ Automatic select

☑ G.Dmt Enabled

☑ G.lite Enabled

☑ T1.413 Enabled

☑ ADSL2 Enabled

☑ AnnexL Enabled

☑ ADSL2+ Enabled

☐ AnnexM Enabled

Capability

☑ Bitswap Enable

☐ SRA Enable

3 Do you want to automatically select the modulation?

- If **yes**, make sure the **Automatic select** check box is checked under Select the modulation below field. Go to step 5.
- If **no**, uncheck the **Automatic Select** check box. A list of modulation types appears.

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

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

5 Under the Capability field, select the capability that you want to use from the following options:

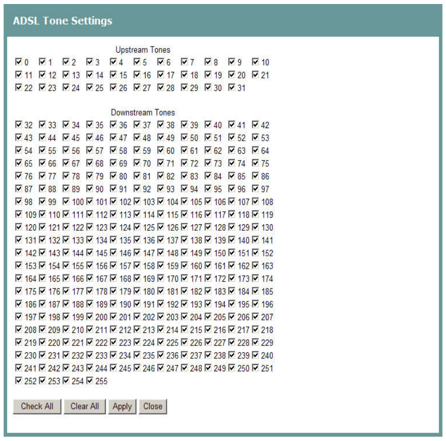
- Bitswap Enable
- SRA Enable

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

ADSL Tone Settings

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

Path: DSL > Setting > Advanced Settings > Tone Selection



ADSL Tone Settings

Upstream Tones

☑ 0 ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10
☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15 ☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21
☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31

Downstream Tones

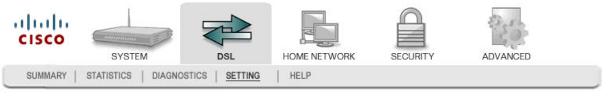
☑ 32 ☑ 33 ☑ 34 ☑ 35 ☑ 36 ☑ 37 ☑ 38 ☑ 39 ☑ 40 ☑ 41 ☑ 42
☑ 43 ☑ 44 ☑ 45 ☑ 46 ☑ 47 ☑ 48 ☑ 49 ☑ 50 ☑ 51 ☑ 52 ☑ 53
☑ 54 ☑ 55 ☑ 56 ☑ 57 ☑ 58 ☑ 59 ☑ 60 ☑ 61 ☑ 62 ☑ 63 ☑ 64
☑ 65 ☑ 66 ☑ 67 ☑ 68 ☑ 69 ☑ 70 ☑ 71 ☑ 72 ☑ 73 ☑ 74 ☑ 75
☑ 76 ☑ 77 ☑ 78 ☑ 79 ☑ 80 ☑ 81 ☑ 82 ☑ 83 ☑ 84 ☑ 85 ☑ 86
☑ 87 ☑ 88 ☑ 89 ☑ 90 ☑ 91 ☑ 92 ☑ 93 ☑ 94 ☑ 95 ☑ 96 ☑ 97
☑ 98 ☑ 99 ☑ 100 ☑ 101 ☑ 102 ☑ 103 ☑ 104 ☑ 105 ☑ 106 ☑ 107 ☑ 108
☑ 109 ☑ 110 ☑ 111 ☑ 112 ☑ 113 ☑ 114 ☑ 115 ☑ 116 ☑ 117 ☑ 118 ☑ 119
☑ 120 ☑ 121 ☑ 122 ☑ 123 ☑ 124 ☑ 125 ☑ 126 ☑ 127 ☑ 128 ☑ 129 ☑ 130
☑ 131 ☑ 132 ☑ 133 ☑ 134 ☑ 135 ☑ 136 ☑ 137 ☑ 138 ☑ 139 ☑ 140 ☑ 141
☑ 142 ☑ 143 ☑ 144 ☑ 145 ☑ 146 ☑ 147 ☑ 148 ☑ 149 ☑ 150 ☑ 151 ☑ 152
☑ 153 ☑ 154 ☑ 155 ☑ 156 ☑ 157 ☑ 158 ☑ 159 ☑ 160 ☑ 161 ☑ 162 ☑ 163
☑ 164 ☑ 165 ☑ 166 ☑ 167 ☑ 168 ☑ 169 ☑ 170 ☑ 171 ☑ 172 ☑ 173 ☑ 174
☑ 175 ☑ 176 ☑ 177 ☑ 178 ☑ 179 ☑ 180 ☑ 181 ☑ 182 ☑ 183 ☑ 184 ☑ 185
☑ 186 ☑ 187 ☑ 188 ☑ 189 ☑ 190 ☑ 191 ☑ 192 ☑ 193 ☑ 194 ☑ 195 ☑ 196
☑ 197 ☑ 198 ☑ 199 ☑ 200 ☑ 201 ☑ 202 ☑ 203 ☑ 204 ☑ 205 ☑ 206 ☑ 207
☑ 208 ☑ 209 ☑ 210 ☑ 211 ☑ 212 ☑ 213 ☑ 214 ☑ 215 ☑ 216 ☑ 217 ☑ 218
☑ 219 ☑ 220 ☑ 221 ☑ 222 ☑ 223 ☑ 224 ☑ 225 ☑ 226 ☑ 227 ☑ 228 ☑ 229
☑ 230 ☑ 231 ☑ 232 ☑ 233 ☑ 234 ☑ 235 ☑ 236 ☑ 237 ☑ 238 ☑ 239 ☑ 240
☑ 241 ☑ 242 ☑ 243 ☑ 244 ☑ 245 ☑ 246 ☑ 247 ☑ 248 ☑ 249 ☑ 250 ☑ 251
☑ 252 ☑ 253 ☑ 254 ☑ 255

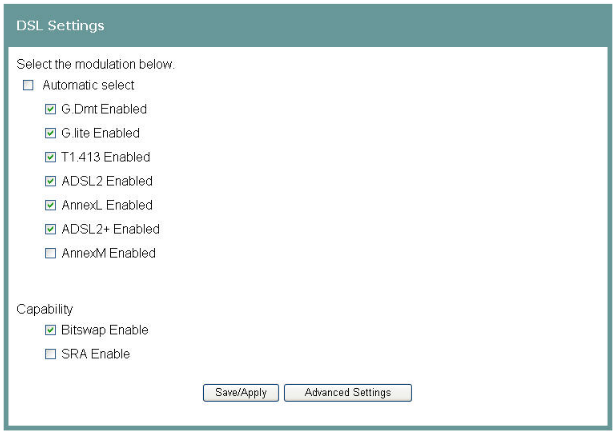
Setting DSL Tones or Frequencies

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

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

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





DSL Settings

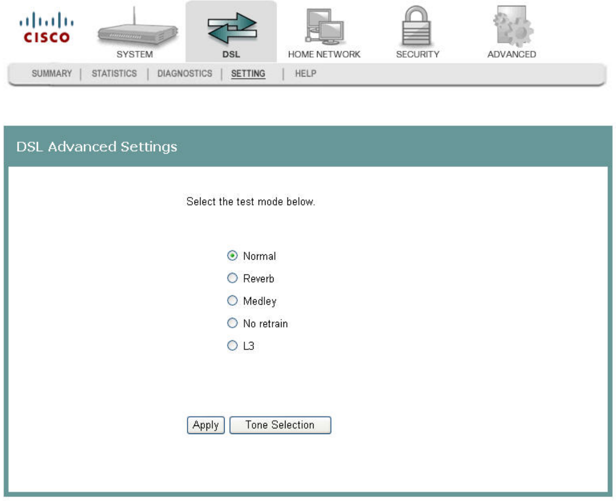
Select the modulation below.

☐ Automatic select
☑ G.Dmt Enabled
☑ G.lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☑ AnnexL Enabled
☑ ADSL2+ Enabled
☐ AnnexM Enabled

Capability

☑ Bitswap Enable
☐ SRA Enable

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

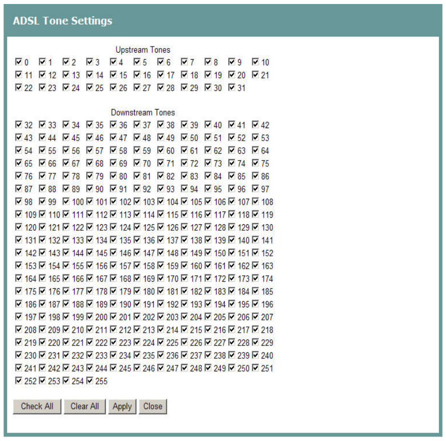


DSL Advanced Settings

Select the test mode below.

● Normal
○ Reverb
○ Medley
○ No retrain
○ L3

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



ADSL Tone Settings

Upstream Tones

☑ 0 ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10
☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15 ☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21
☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31

Downstream Tones

☑ 32 ☑ 33 ☑ 34 ☑ 35 ☑ 36 ☑ 37 ☑ 38 ☑ 39 ☑ 40 ☑ 41 ☑ 42
☑ 43 ☑ 44 ☑ 45 ☑ 46 ☑ 47 ☑ 48 ☑ 49 ☑ 50 ☑ 51 ☑ 52 ☑ 53
☑ 54 ☑ 55 ☑ 56 ☑ 57 ☑ 58 ☑ 59 ☑ 60 ☑ 61 ☑ 62 ☑ 63 ☑ 64
☑ 65 ☑ 66 ☑ 67 ☑ 68 ☑ 69 ☑ 70 ☑ 71 ☑ 72 ☑ 73 ☑ 74 ☑ 75
☑ 76 ☑ 77 ☑ 78 ☑ 79 ☑ 80 ☑ 81 ☑ 82 ☑ 83 ☑ 84 ☑ 85 ☑ 86
☑ 87 ☑ 88 ☑ 89 ☑ 90 ☑ 91 ☑ 92 ☑ 93 ☑ 94 ☑ 95 ☑ 96 ☑ 97
☑ 98 ☑ 99 ☑ 100 ☑ 101 ☑ 102 ☑ 103 ☑ 104 ☑ 105 ☑ 106 ☑ 107 ☑ 108
☑ 109 ☑ 110 ☑ 111 ☑ 112 ☑ 113 ☑ 114 ☑ 115 ☑ 116 ☑ 117 ☑ 118 ☑ 119
☑ 120 ☑ 121 ☑ 122 ☑ 123 ☑ 124 ☑ 125 ☑ 126 ☑ 127 ☑ 128 ☑ 129 ☑ 130
☑ 131 ☑ 132 ☑ 133 ☑ 134 ☑ 135 ☑ 136 ☑ 137 ☑ 138 ☑ 139 ☑ 140 ☑ 141
☑ 142 ☑ 143 ☑ 144 ☑ 145 ☑ 146 ☑ 147 ☑ 148 ☑ 149 ☑ 150 ☑ 151 ☑ 152
☑ 153 ☑ 154 ☑ 155 ☑ 156 ☑ 157 ☑ 158 ☑ 159 ☑ 160 ☑ 161 ☑ 162 ☑ 163
☑ 164 ☑ 165 ☑ 166 ☑ 167 ☑ 168 ☑ 169 ☑ 170 ☑ 171 ☑ 172 ☑ 173 ☑ 174
☑ 175 ☑ 176 ☑ 177 ☑ 178 ☑ 179 ☑ 180 ☑ 181 ☑ 182 ☑ 183 ☑ 184 ☑ 185
☑ 186 ☑ 187 ☑ 188 ☑ 189 ☑ 190 ☑ 191 ☑ 192 ☑ 193 ☑ 194 ☑ 195 ☑ 196
☑ 197 ☑ 198 ☑ 199 ☑ 200 ☑ 201 ☑ 202 ☑ 203 ☑ 204 ☑ 205 ☑ 206 ☑ 207
☑ 208 ☑ 209 ☑ 210 ☑ 211 ☑ 212 ☑ 213 ☑ 214 ☑ 215 ☑ 216 ☑ 217 ☑ 218
☑ 219 ☑ 220 ☑ 221 ☑ 222 ☑ 223 ☑ 224 ☑ 225 ☑ 226 ☑ 227 ☑ 228 ☑ 229
☑ 230 ☑ 231 ☑ 232 ☑ 233 ☑ 234 ☑ 235 ☑ 236 ☑ 237 ☑ 238 ☑ 239 ☑ 240
☑ 241 ☑ 242 ☑ 243 ☑ 244 ☑ 245 ☑ 246 ☑ 247 ☑ 248 ☑ 249 ☑ 250 ☑ 251
☑ 252 ☑ 253 ☑ 254 ☑ 255

5 Select the ADSL tone settings as follows.

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

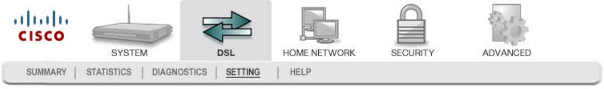
6 Click **Apply** to configure the tone settings.

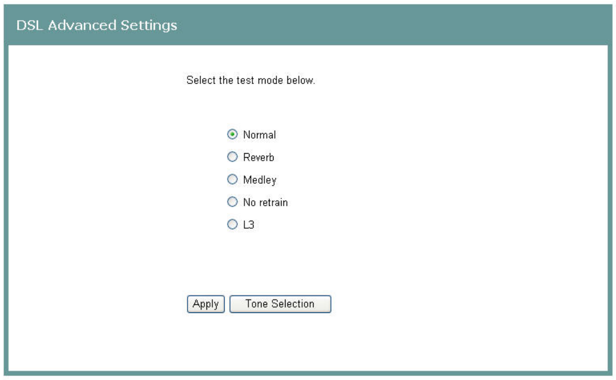
7 Click **Close** to return to the DSL Advanced Settings screen.

DSL Advanced Settings

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

Path: DSL > Setting > Advanced Settings




DSL Advanced Settings

Select the test mode below.

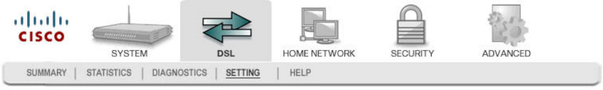
● Normal
○ Reverb
○ Medley
○ No retrain
○ L3

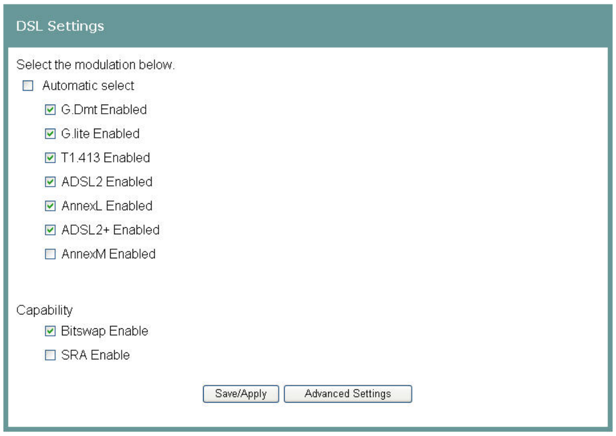
Configuring DSL Advanced Settings

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

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

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

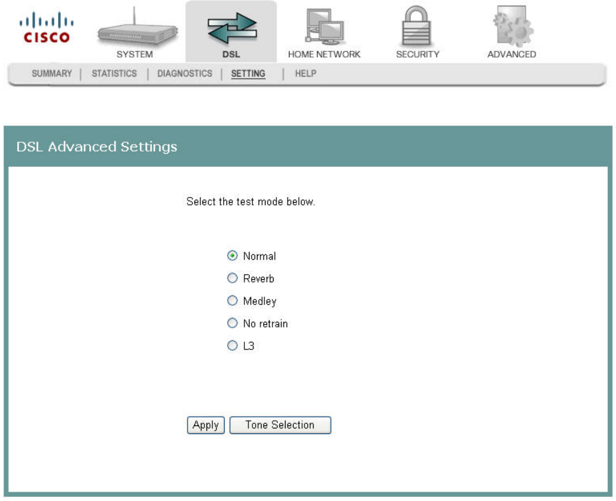



DSL Settings

Select the modulation below.
□ Automatic select
☑ G.Dmt Enabled
☑ G.lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☑ AnnexL Enabled
☑ ADSL2+ Enabled
□ AnnexM Enabled

Capability
☑ Bitswap Enable
□ SRA Enable

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



DSL Advanced Settings

Select the test mode below.

● Normal
○ Reverb
○ Medley
○ No retrain
○ L3

4 Select the test mode from the following options:

- Normal
- Reverb
- Medley
- No refrain
- L3

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

5

Home Network Configuration

The Home Network tab allows you to check the home network configuration. You use this tab to configure and check the status of the devices connected to your home network.

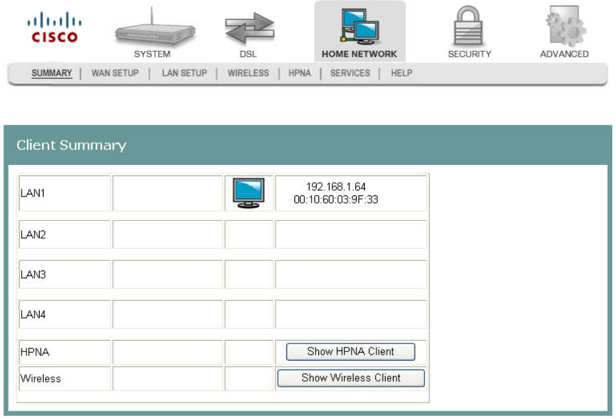
In This Chapter

- Client Summary 94
- WAN Quick Setup 97
- Set Top Box Quick Setup 101
- LAN Setup 103
- Wireless Summary 106
- Wireless Basic 107
- Wireless Security 111
- Wireless MAC Filtering 116
- Wireless Bridge 120
- Wireless Station List 121
- HPNA Information 123
- HPNA Statistics Information 125
- Home Monitoring 126

Client Summary

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

Path: Home Network > Summary


CISCO
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

Client Summary

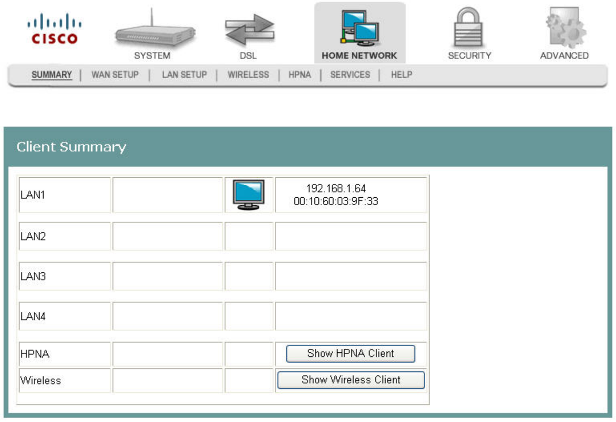
LAN1		🖥	192.168.1.64 00:10:60:03:9F:33
LAN2			
LAN3			
LAN4			
HPNA			Show HPNA Client
Wireless			Show Wireless Client

Updating HPNA Clients

To update the HPNA clients, complete the following steps.

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

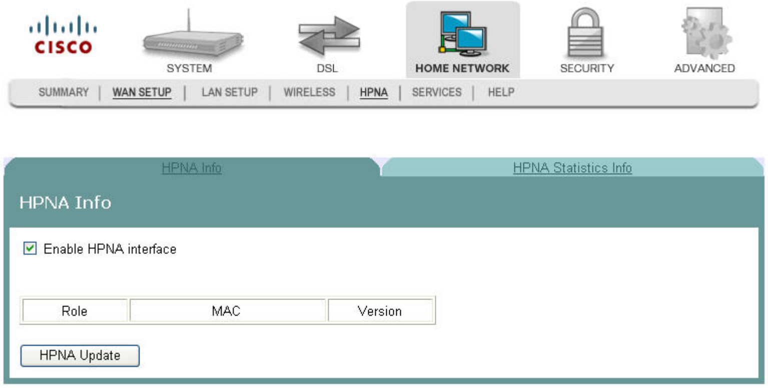
2 Click **Summary**. The Client Summary screen opens.


CISCO
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

Client Summary

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

3 Click **Show HPNA Client**. After processing, the HPNA Info screen opens.



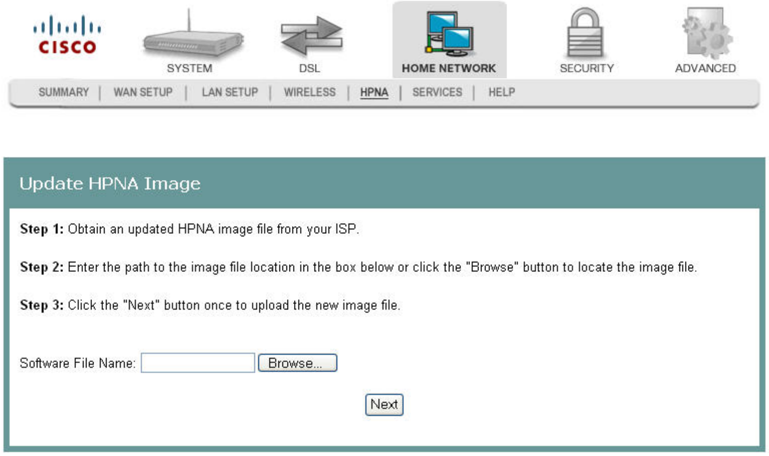
HPNA Info

☑ Enable HPNA interface

Role	MAC	Version

anji for rev B

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


CISCO
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP
Browse...
Next

Update HPNA Image

Step 1: Obtain an updated HPNA image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Next" button once to upload the new image file.

Software File Name:

Da

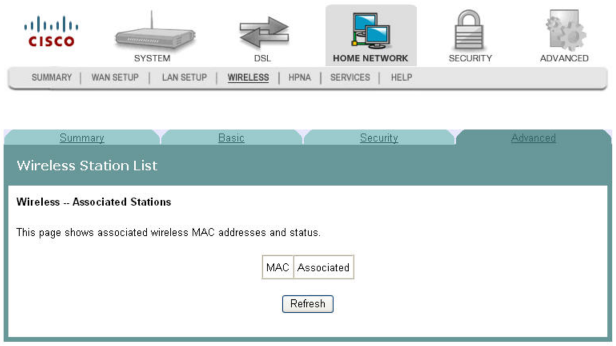
5 In the Software File Name field, enter the name of the file that you want to use to update your system. You can click Browse to locate the file.

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

Wireless Station List

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

Path: Home Network > Summary > Show Wireless Client



Wireless Station List

Wireless -- Associated Stations

This page shows associated wireless MAC addresses and status.

MAC	Associated

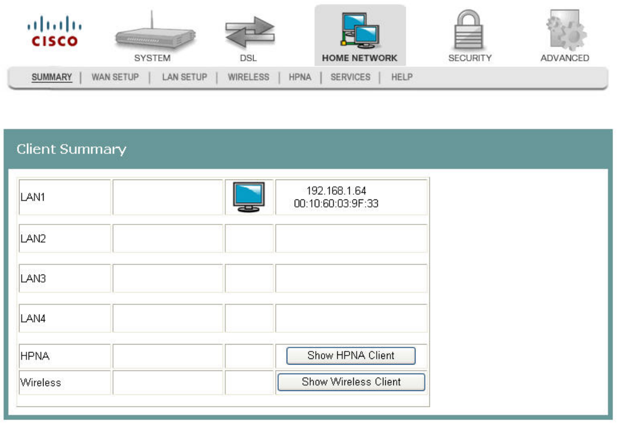
Refresh

Showing Attached Clients

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

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

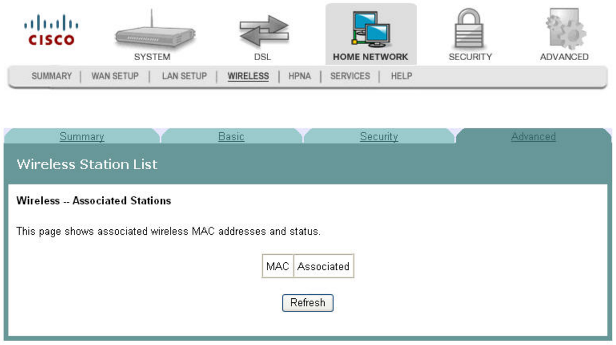
2 Click **Summary**. The Client Summary screen opens.


cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

Client Summary

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

3 Click **Show Wireless Client**. The Wireless Station List screen opens.



Wireless Station List

Wireless -- Associated Stations

This page shows associated wireless MAC addresses and status.

MAC	Associated

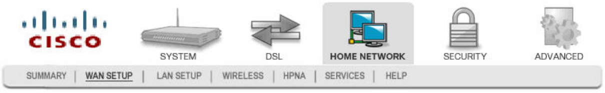
Refresh

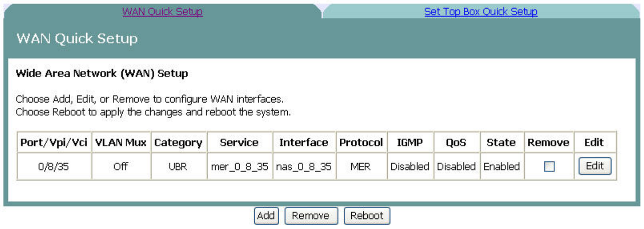
4 Click **Refresh** to update the list of attached clients.

WAN Quick Setup

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

Path: Home Network > WAN Setup > WAN Quick Setup


CISCO
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP



WAN Quick Setup

Wide Area Network (WAN) Setup

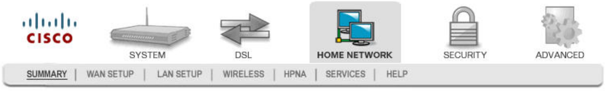
Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Reboot to apply the changes and reboot the system.

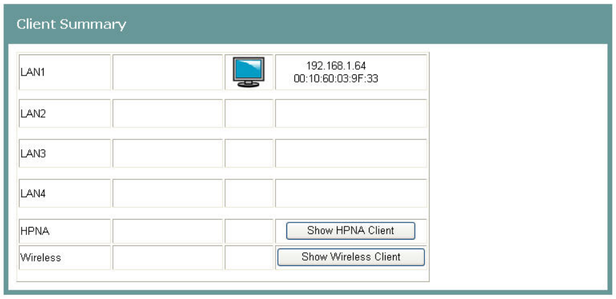
Port/Vpi/Vci	VLAN Mux	Category	Service	Interface	Protocol	IGMP	QoS	State	Remove	Edit
0/8/35	Off	UBR	mer_0_8_35	nas_0_8_35	MER	Disabled	Disabled	Enabled	□	Edit

Configuring the WAN Interface (PPPoE Broadband Type)

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

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

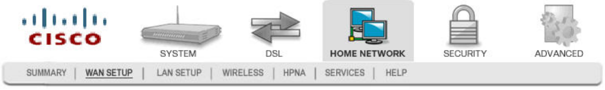

CISCO
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

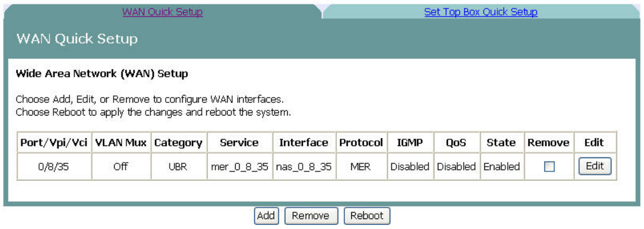


Client Summary

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

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


SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP



WAN Quick Setup

Wide Area Network (WAN) Setup

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

Port/Vpi/Vci	VLAN Mux	Category	Service	Interface	Protocol	IGMP	QoS	State	Remove	Edit
0/8/35	Off	UBR	mer_0_8_35	nas_0_8_35	MER	Disabled	Disabled	Enabled	□	Edit

Q. to reviewers click edit or add to see the next fields.

3 In the Broadband Type field, select **DSL**.

4 In the DSL Mode field, select **ATM**. More fields populate on the screen.

5 Complete the following fields on the screen as follows:

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

- **a** In the Broadband Connect Type field, select **PPP over Ethernet (PPPoE)**.
- **b** In the Encapsulation Mode field, select **LLC/SNAP - Bridging**.
- **c** Check the **VLAN Mux - Enable Multiple Protocols Over a Single PVC** check box.
- **d** In the **PPP Username:** field, enter the user name for the point-to-point protocol.
- **e** In the **PPP Password:** field, enter the pasword for the point-to-point protocol.
- **f** In the **PPPoE Service Name:** field, enter the name for the point-to-point over Ethernet service.
- **g** In the Authentication Method field, select auto from the drop-down list. Auto turns on authentication automatically.
- **h** In the **VPI** field, enter the virtual path identifier (VPI). Values are: 0 to 65535
- **i** In the **VCI** field, enter the virtual channel identifier (VCI). Values are: 0 to 65535
- **j** In the **Service Category** field, select **UBR Without PCR**.
- **k** In the **Authentication Method** field, select **AUTO**.
- **l** Select the **Enable IGMP Multicast** check box.
- **m** Select the **Enable WAN Service** check box.

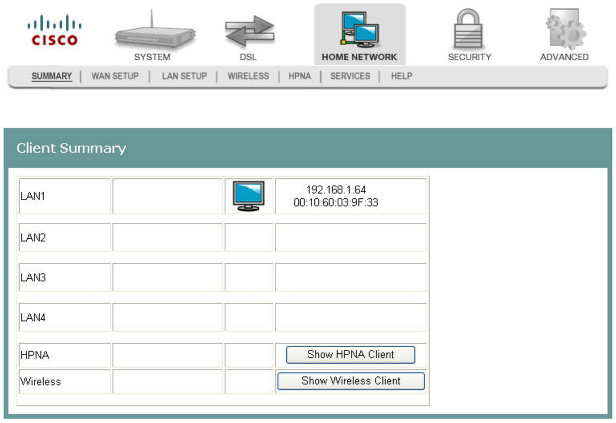
6 Click **Add**.

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

Configuring the WAN Interface (MER Broadband Type)

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

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


cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

Client Summary

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

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

Q. to reviewers: Need to click Add or Edit to see this screen.

3 Click Add or Edit.

<Need populated screen screen>

4 In the Broadband Type field, enter **DSL**.

5 In the DSL Mode field, select **ATM**. More fields populate on the screen.

6 Complete the following fields on the screen as follows:

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

a In the Broadband Connect Type field, select **MAC Encapsulation Routing (MER)**.

b In the Encapsulation Mode field, select **LLC/SNAP - Bridging**.

c Select the **VLAN Mux - Enable Multiple Protocols Over a Single PVC** check box.

d In the **VLAN ID[0-4095]:** field, enter an ID for the VLAN. Values are 0-4095.

e In the VPI field, enter the virtual path identifier (VPI). Values are: 0 to 65535

f In the VCI field, enter the virtual channel identifier (VCI). Values are: 0 to 65535

g In the the Service Category field, select **UBR Without PCR**.

h Select the **Enable Quality of Service** check box.

i Select the **Obtain an IP address automatically** option.

j Select the **Obtain default gateway automatically** option.

k Select the **Obtain DNS server addresses automatically** option.

- **l** Select the **Enable IGMP Multicast** check box.
- **m** Select the **Enable WAN Service** check box.

7 Click **Add**.

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

Set Top Box Quick Setup

The Set Top Box Quick Setup screen allows you to quickly configure set-top box permanent virtual circuits (PVCs) and DHCP option 60 parameters.

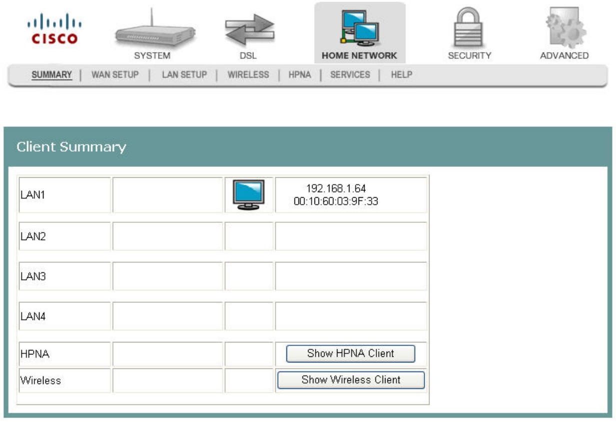
Path: Home Network > WAN Setup > Set Top Box Quick Setup

Q. to reviewers Need populated screen

Configuring a Quick Set Up for a Set-Top

To quickly configure set-top box permanent virtual circuits (PVCs) and DHCP option 60 parameters, complete the following steps.

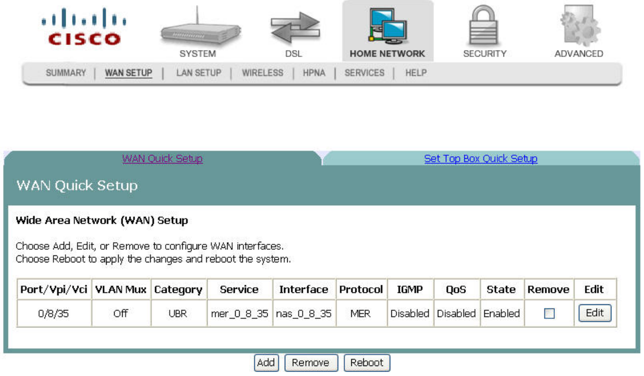
1 Click **Home Network** on the main screen. The Client Summary screen opens.



Client Summary

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

2 Click **WAN Setup.** The WAN Quick Setup screen opens with the WAN Quick Setup tab in the forefront.



WAN Quick Setup

Wide Area Network (WAN) Setup

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

Port/Vpi/Vci	VLAN Mux	Category	Service	Interface	Protocol	IGMP	QoS	State	Remove	Edit
0/8/35	Off	UBR	mer_0_8_35	nas_0_8_35	MER	Disabled	Disabled	Enabled	□	Edit

3 Click the **Set Top Box Quick Setup** tab.

Q. to reviewers: Need populated screen

4 Complete the fields on the screen as follows.

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

a In the Broadband Type field, select **DSL**.

b In the DSL mode field, select **ATM**.

c In the Broadband Connect Type filed, select **MAC Encapsulation Routing (MER)**.

d In the Encapsulation Mode field, select **LLC/SNAP - BRIDGING**.

e In the VPI field, enter the virtual path identifier (VPI). Values are: 0 to 65535

f In the VCI field, enter the virtual channel identifier (VCI). Values are: 0 to 65535

g In the Service Category field, select **UBR Without PCR**.

h In the Enable Virtual Port Function (Configure following parameter if the Set Top Box has been installed) field, enable the check box.

i In the Group Name field, enter a descriptive name for the virtual port group.

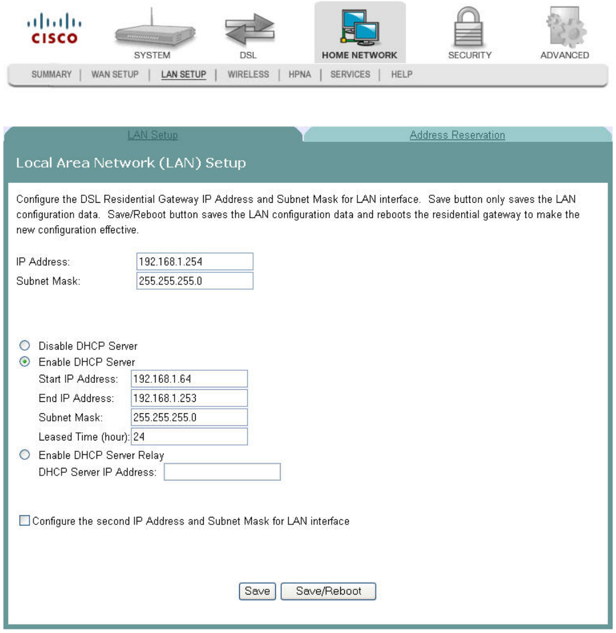
j In the Automatically Add Clients With the following DHCP Vendor IDs field, enter the DHCP option 60 string of the attached set-top boxes.

5 Click **Save/Reboot** to save your changes.

LAN Setup

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

Path: Home Network > LAN Setup



Local Area Network (LAN) Setup

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

IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0

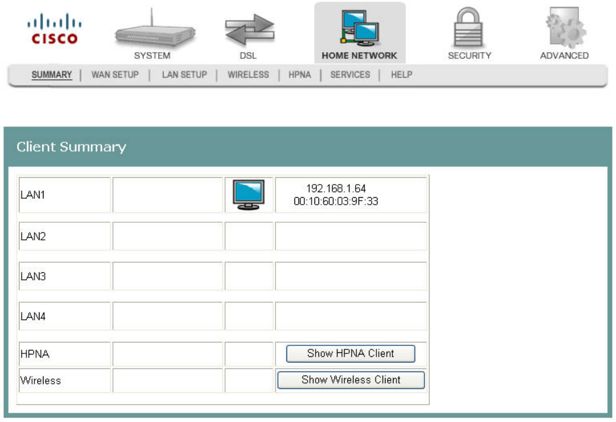
○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.64
End IP Address: 192.168.1.253
Subnet Mask: 255.255.255.0
Leased Time (hour): 24
○ Enable DHCP Server Relay
DHCP Server IP Address:

□ Configure the second IP Address and Subnet Mask for LAN interface

Configuring the LAN Interface

To configure the LAN interface, complete the following steps.

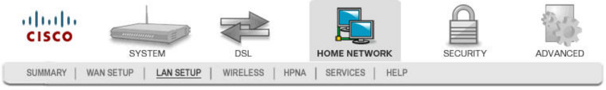
1 Click **Home Network** on the main screen. The Client Summary screen opens.

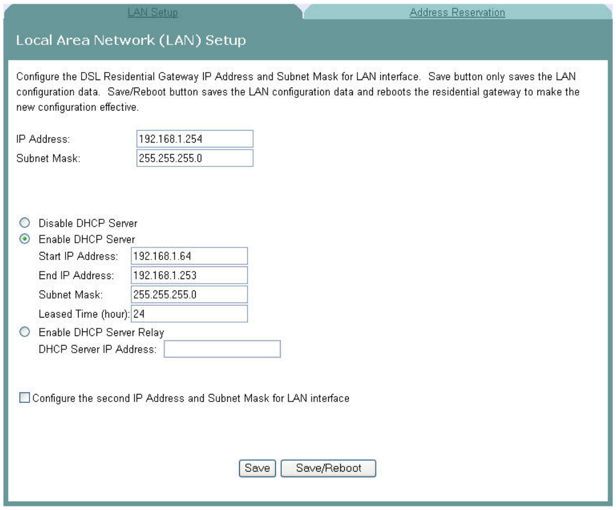

CISCO
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

Client Summary

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

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


cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP



Local Area Network (LAN) Setup

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

IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.64
End IP Address: 192.168.1.253
Subnet Mask: 255.255.255.0
Leased Time (hour): 24
○ Enable DHCP Server Relay
DHCP Server IP Address:

□ Configure the second IP Address and Subnet Mask for LAN interface

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

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

5 Do you want to enable UPnP?

- If **yes**, check the Enable UPnP check box.
- If **no**, uncheck the Enable UPnP check box.

6 Do you want to Enable the DHCP server?

- If **yes**, select **Enable DHCP Server**, and go to step 7.
- If **no**, select **Disable DHCP Server**, and go to step 8.

7 Under Enable DHCP server, enter the following information:

a In the Start IP Address field, enter the first IP address in the range for the DHCP IP address lease pool.

b In the End IP Address field, enter the last IP address in the range for the DHCP IP address lease pool.

c In the Subnet Mask field, enter the subnet mask for the DCHP server.

d In the Leased Time (hour) field, enter the duration of the DHCP lease address.

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

- If **yes**, check the **Configure the second IP Address and Subnet Mask for LAN interface** check box. The screen populates with another IP address and subnet mask field. Go to step 9.
- If **no**, uncheck the **Configure the second IP Address and Subnet Mask for LAN interface** check box. Go to step 10.

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

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

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

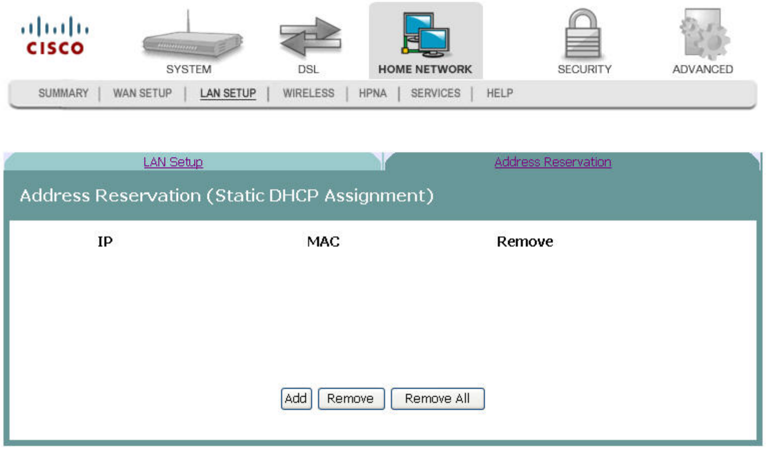
10 Click **Save** to save the changes or click **Save/Reboot** to save the changes and reboot the residential gateway.

Address Reservation

The Address Reservation screen..

Q. to reviewers: Need info

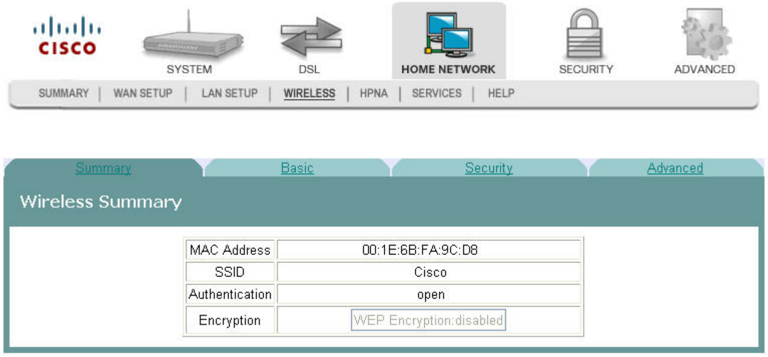
Path: Home Network > LAN Setup > Address Reservation


CISCO
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP
LAN Setup
Address Reservation
Address Reservation (Static DHCP Assignment)
IP
MAC
Remove
Add
Remove
Remove All

Wireless Summary

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

Path: Home Network > Wireless>Summary



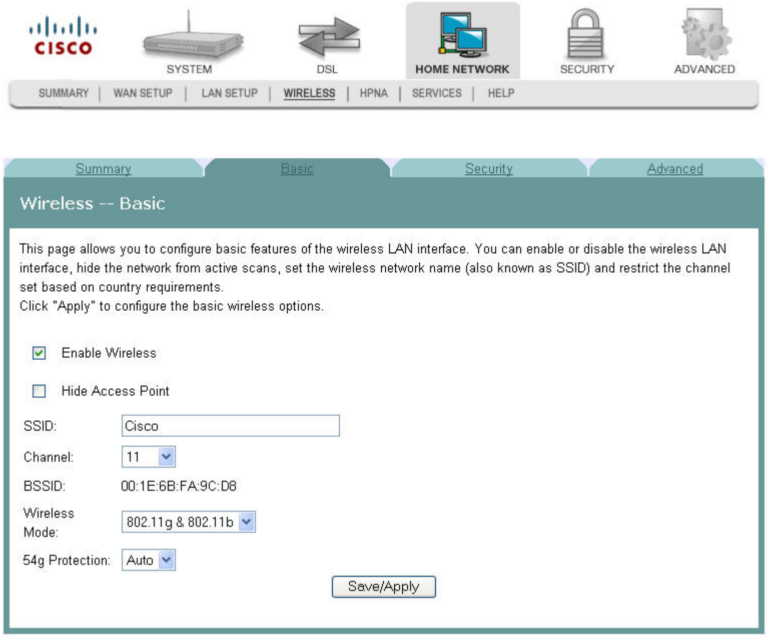
Wireless Summary

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

Wireless Basic

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

Path: Home Network > Wireless > Basic



Wireless -- Basic

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

☑ Enable Wireless

□ Hide Access Point

SSID: Cisco

Channel: 11

BSSID: 00:1E:6B:FA:9C:D8

Wireless Mode: 802.11g & 802.11b

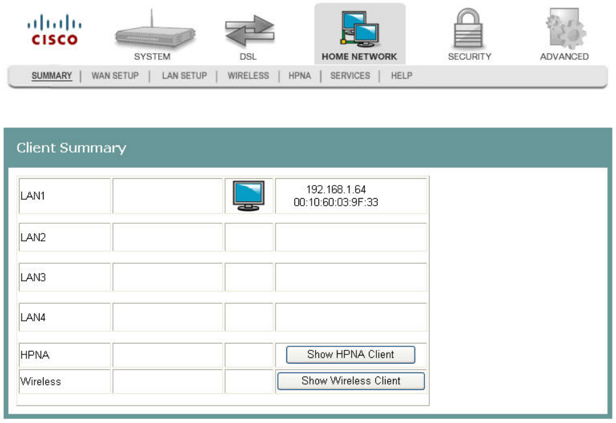
54g Protection: Auto

Save/Apply

Enabling the Wireless Network

To enable the wireless network, complete the following steps.

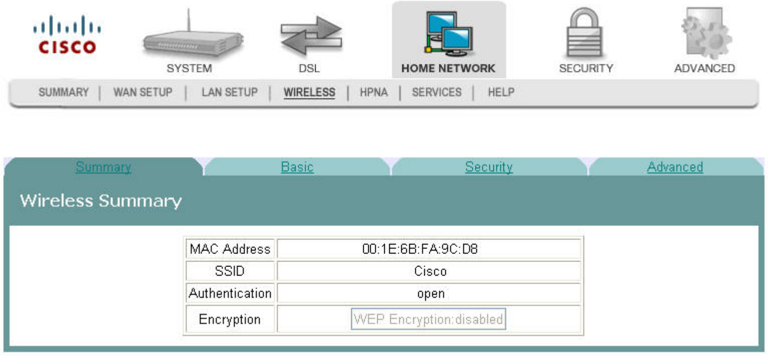
1 Click lick **Home Network** on the main screen. The Client Summary screen opens.


cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

Client Summary

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

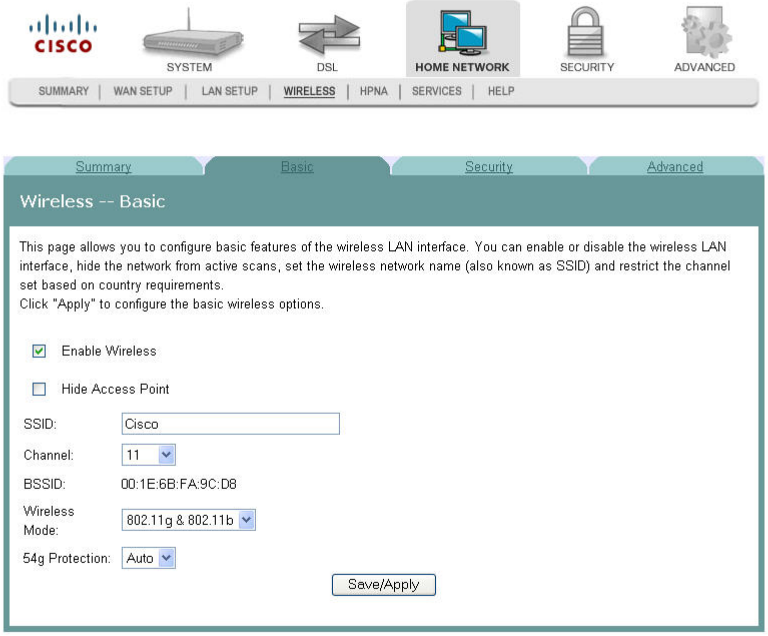
2 Click **Wireless.** The Wireless Summary screen opens.



Wireless Summary

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

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



Wireless -- Basic

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

☑ Enable Wireless

☐ Hide Access Point

SSID: Cisco

Channel: 11

BSSID: 00:1E:6B:FA:9C:D8

Wireless Mode: 802.11g & 802.11b

54g Protection: Auto

4 Check the **Enable Wireless** check box to enable the wireless network. The screen populates with additional fields.

5 Do you want to prevent other wireless clients from communicating with the wireless access point (AP) of the residential gateway?

- If **yes**, check the **Hide Access Point** check box. This feature prevents any other wireless client from communicating with the access point of the residential gateway (or disables the wireless connection).
- If **no**, uncheck the **Hide Access Point** check box.

6 In the SSID field, enter the service set identifier (SSID).

7 From the Channel drop-down list, select Auto or a channel from 1 to 11.

8 In the Wireless Mode field, select the wireless mode from the drop-down list:

- 802.11g & 802.11b - Allows you to mix Wireless-B with Wireless-G equipment, but you will lose the higher performance speeds of Wireless-G.

- 802.11g only - Features the same benefits as Wireless-B, but offers 5 times the speed at up to 54 Mbps. Wireless-G currently offers the best combination of performance and value. You can mix Wireless-B with Wireless-G equipment, but you will lose the higher performance speeds of Wireless-G.
- 802.11b only - Operates on the 2.4GHz frequency band and can transmit data at speeds of up to 11 Mbps within a range of up to 100-150 feet. Wireless range can be affected by reflective or signal-blocking obstacles, such as mirrors, walls, devices and location, whether indoors or outdoors.

9 In the 54g Protection field, select Auto or Off. Do not disable 54g Protection if there is a possibility that a 802.11b device may need to use your wireless network.

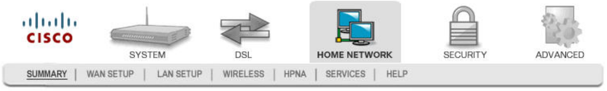
Note: 54g Protection allows 802.11g and 802.11b devices to co-exist in the same network without "speaking" at the same time. In Auto Mode, the wireless device will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.

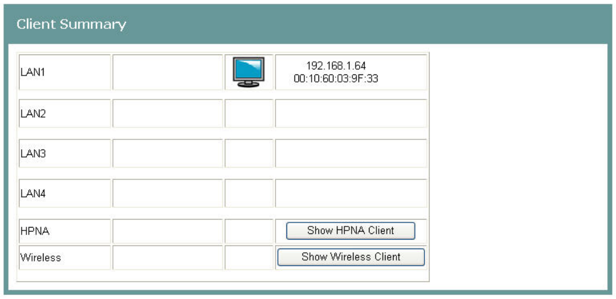
10 Click **Save/Apply** to enable the wireless network.

Disabling the Wireless Network

To disable the wireless network, complete the following steps.

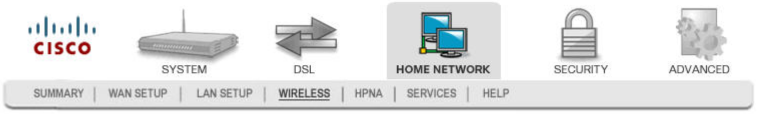
1 Click lick **Home Network** on the main screen. The Client Summary screen opens.

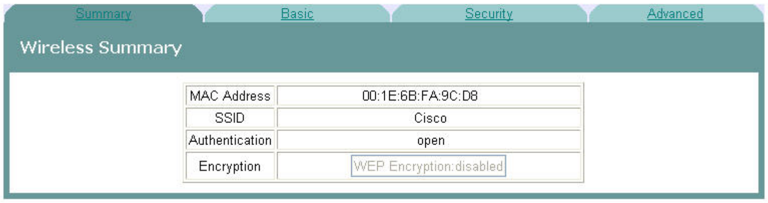

cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP


Client Summary

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

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

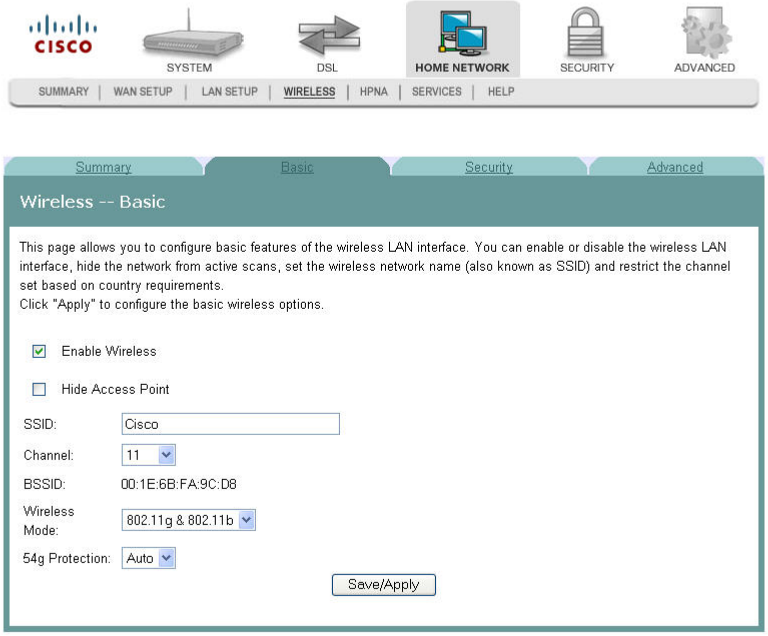

cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP



Wireless Summary

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

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



Wireless -- Basic

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

☑ Enable Wireless

□ Hide Access Point

SSID: Cisco

Channel: 11

BSSID: 00:1E:6B:FA:9C:D8

Wireless Mode: 802.11g & 802.11b

54g Protection: Auto

4 Uncheck the **Enable Wireless** check box. The wireless network fields are removed from the screen.

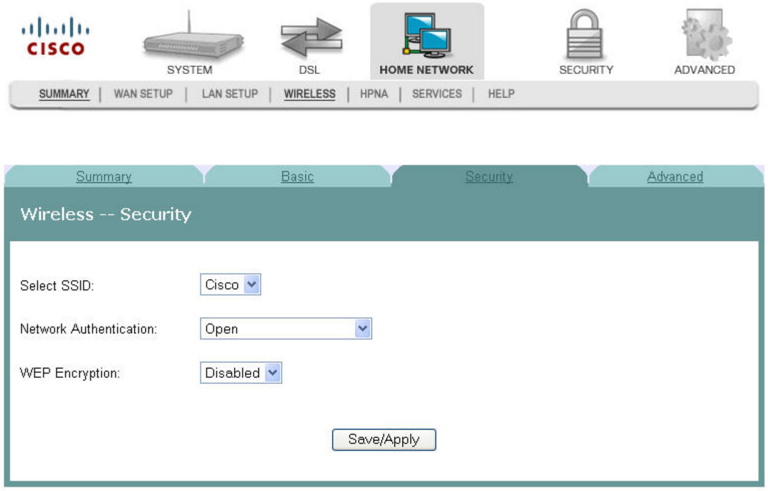
5 Click **Save/Apply** to disable the wireless network.

Wireless Security

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

Path: Home Network > Wireless > Security

WEP Encryption Disabled



Select SSID: Cisco

Network Authentication: Open

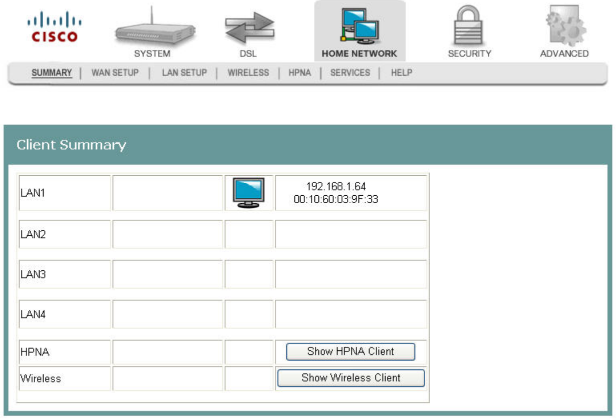
WEP Encryption: Disabled

Securing Your Wireless Network with WEP

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

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

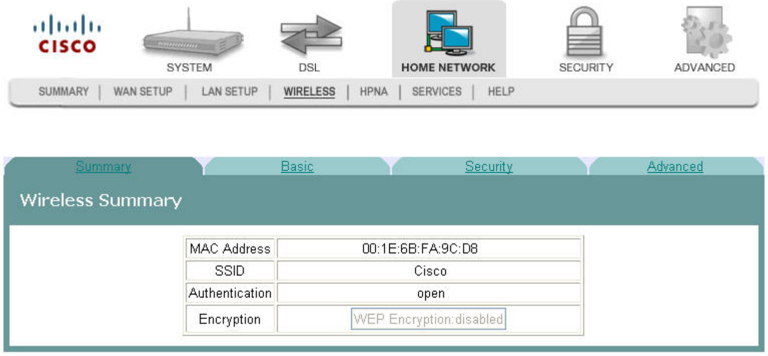
1 Click **Home Network** on the main screen. The Client Summary screen opens.


SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

Client Summary

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

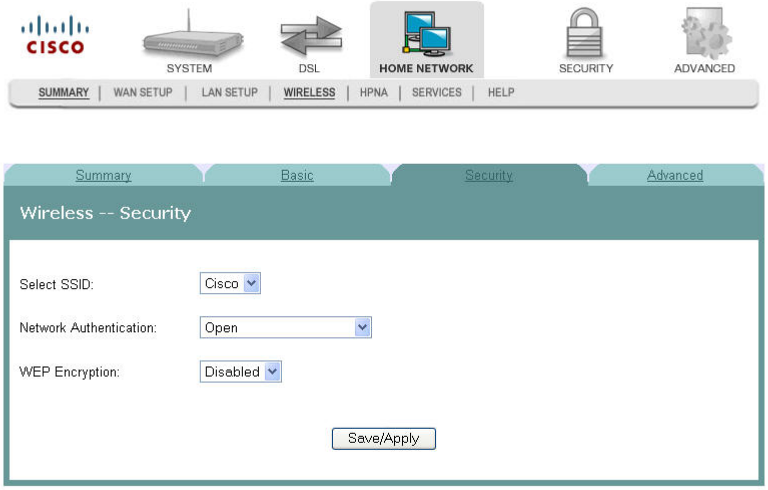
2 Click **Wireless.** The Wireless Summary screen opens.


SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP
Summary
Basic
Security
Advanced

Wireless Summary

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

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



Wireless -- Security

Select SSID: Cisco

Network Authentication: Open

WEP Encryption: Disabled

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

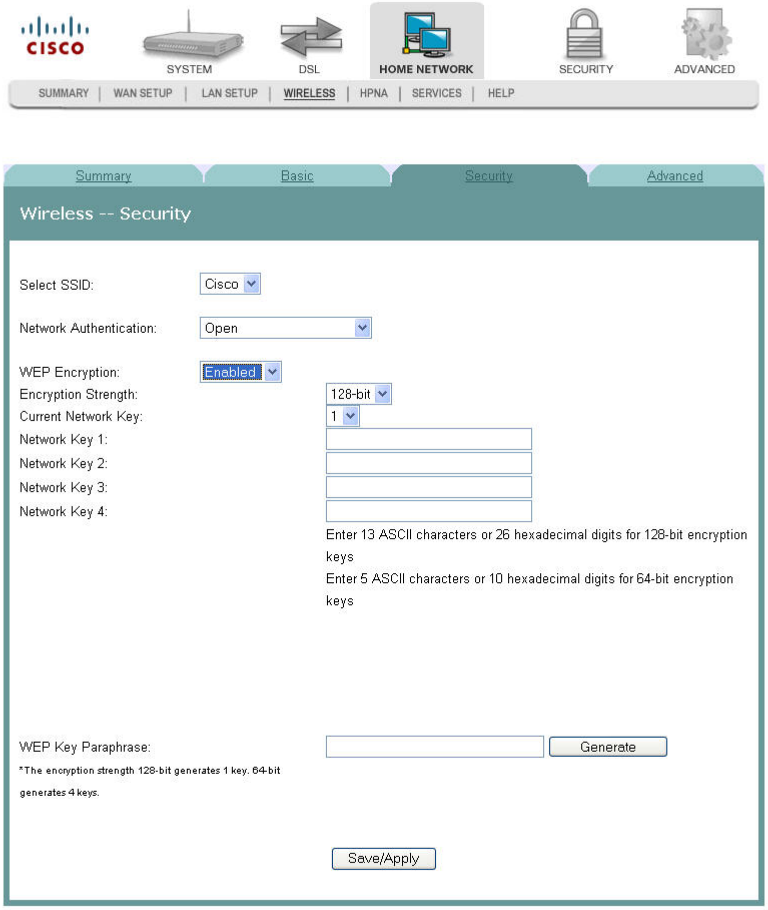
Note: You can add options to this drop-down list on the Wireless -- Basic screen.

5 In the **Network Authentication field**, choose one of these two options for the authentication method.

- Open. All devices may access the wireless network. (Preferred Option).

- Shared. Only devices configured with the 64 bit or 128 Bit Key may access the wireless network.

6 In the WEP Encryption field, select **Enabled**. The Wireless -- Security screen populates with more fields.



Wireless -- Security

Select SSID: Cisco

Network Authentication: Open

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 1

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys

Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

WEP Key Paraphrase:

*The encryption strength 128-bit generates 1 key. 64-bit generates 4 keys.

7 In the Encryption strength field, choose one of the following options:

- 64-bit. Secures your network by 64-bit (10 hex digit) encryption of all traffic using a static key.
- 128-bit. Secures your network by 128-bit (26 hex digit) encryption of all traffic using a static key.

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

8 Do you want the system to generate the network key for you?

- If **yes**, go to step 11.
- If **no**, you must enter your own network key(s) in the field provided. Go to step 9.

9 In the Current Network Key field, select a network key from the drop-down list. Values are: 1, 2, 3, or 4.

10 In the Network Key 1 field, enter the network key you wish to you use.

11 Based on the encryption strength you chose in step 7, do one of the following.

- For 64-bit encryption, repeat steps 9 and 10 for keys 2 through 4 if you use 64-bit encryption. If you use 128-bit encryption, only one network key is required. Go to step 14.
- For 128-bit encryption, only one network key is used. Go to step 13.

12 In the WEP Key Paraphrase field, enter your information as follows based on 64-bit or 128-bit encryption strength:

- For 64-bit encryption strength, enter a passphrase (1 to 31 characters) and click **Generate**. Four keys are generated based on the passprhase.
- For 1280bit encryption, enter a passphrase (1 to 31 characters) and click Generate. A single key is generated based on the passprhase.

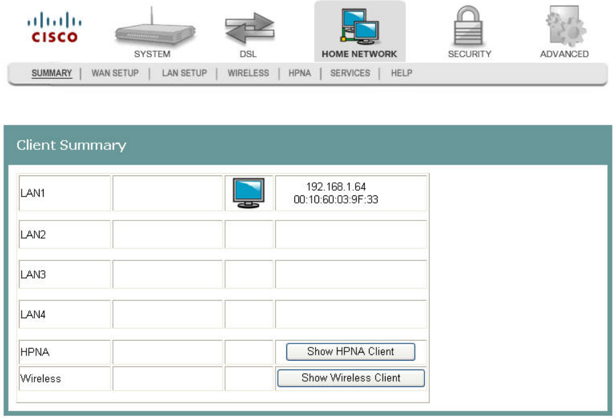
13 Click **Save/Apply**.

Securing Your Wireless Network with Encryption Keys

If you choose WPA-PSK (Wi-Fi Protected Access-PreShared Key) as the network authentication method, you can secure your network by encrypting all traffic using a pre-shared dynamic key.

To secure your wireless network with a preshared dynamic key, complete the following steps.

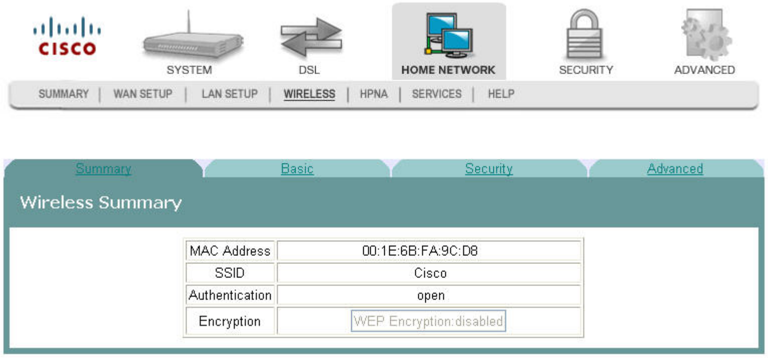
1 Click **Home Network** on the main screen. The Client Summary screen opens.



Client Summary

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

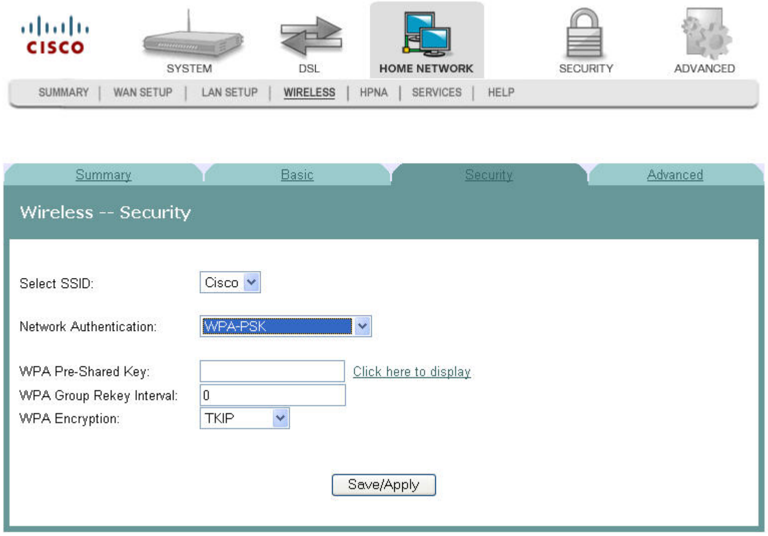
2 Click **Wireless.** The Wireless Summary screen opens.


SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP
Summary
Basic
Security
Advanced

Wireless Summary

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

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



Wireless -- Security

Select SSID: Cisco

Network Authentication: WPA-PSK

WPA Pre-Shared Key: Click here to display

WPA Group Rekey Interval: 0

WPA Encryption: TKIP

Cli

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

5 In the **WPA Pre-Shared Key** field, enter a shared Key (8-63 characters). The system will periodically generate a dynamic key based on the shared key.

6 In the **WPA Group Rekey Interval** field, enter the group key renewal time period. This time defines how often the dynamic key is regenerated

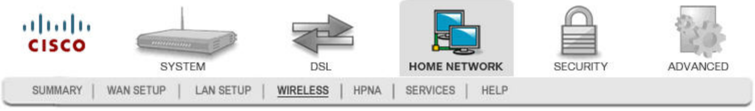
7 In the **WPA Encryption** field, select the encryption from the drop-down list.

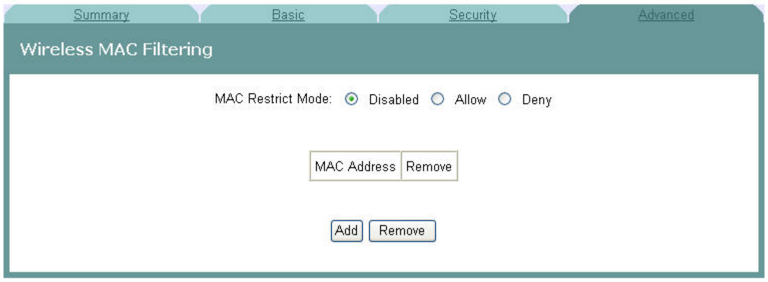
8 Click **Save/Apply** to save your settings.

Wireless MAC Filtering

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

Path: Home Network > Wireless > Advanced > MAC Filter


cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP



Wireless MAC Filtering

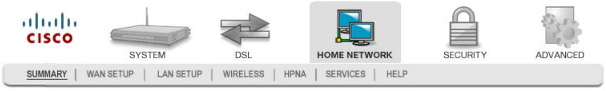
MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

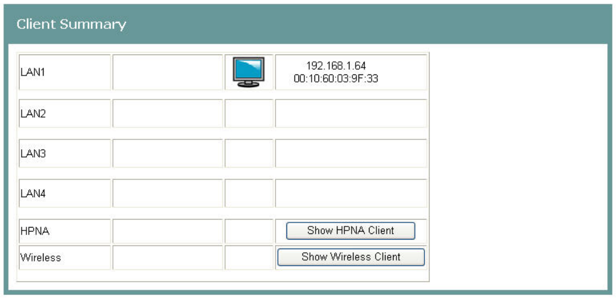
MAC Address	Remove

Allowing Wireless Clients to Access the Residential Gateway

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

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

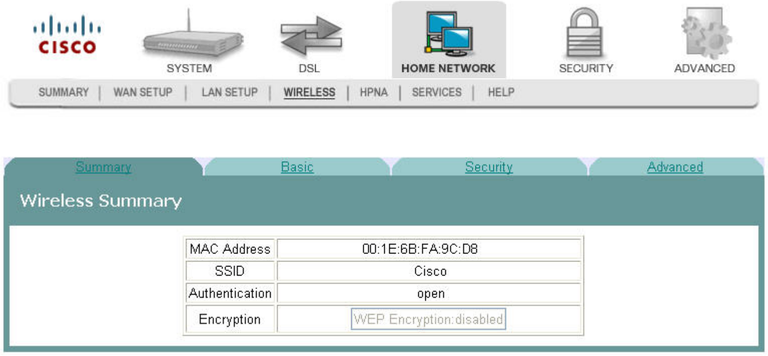

cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP



Client Summary

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

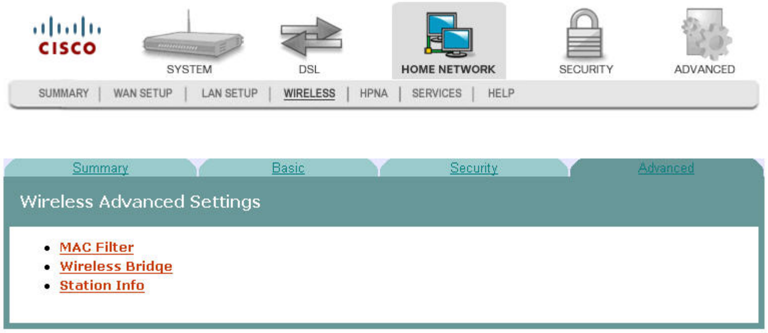
2 Click **Wireless.** The Wireless Summary screen opens.



Wireless Summary

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

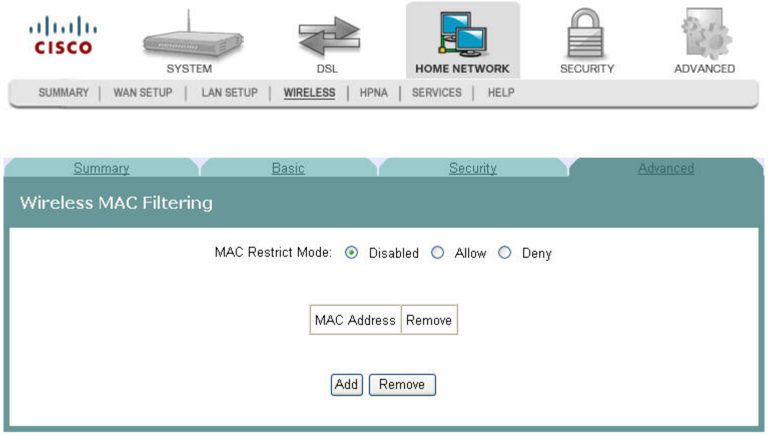
3 Click **Advanced**. The Wireless Advanced Settings screen opens.



Wireless Advanced Settings

- MAC Filter
- Wireless Bridge
- Station Info

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



Wireless MAC Filtering

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

5 In the MAC Restrict Mode field, click **Allow** to enable the MAC restrict mode.

6 Click **Add**. The Wireless -- MAC Filter screen opens.

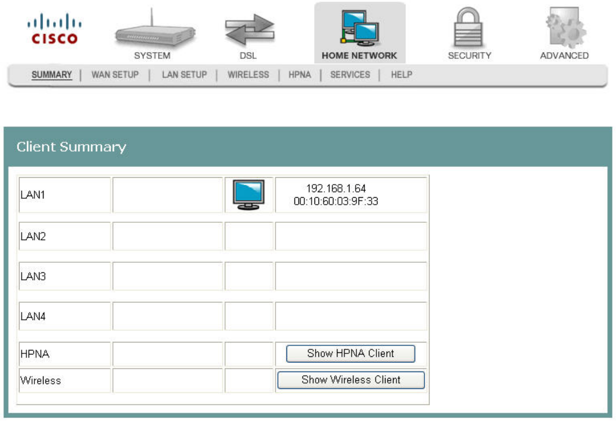
7 In the MAC Address field, enter the MAC address of the client that you want to allow access to the residential gateway.

8 Click **Save/Apply** to allow this wireless client to access the residential gateway.

Blocking Wireless Clients

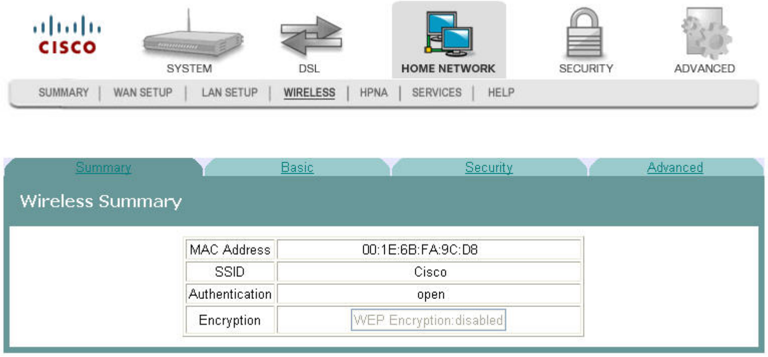
You can block wireless clients from accessing the residential gateway if you know the client's MAC address. MAC restrict mode must be enabled. To prevent wireless clients from accessing the residential gateway, complete the following steps.

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



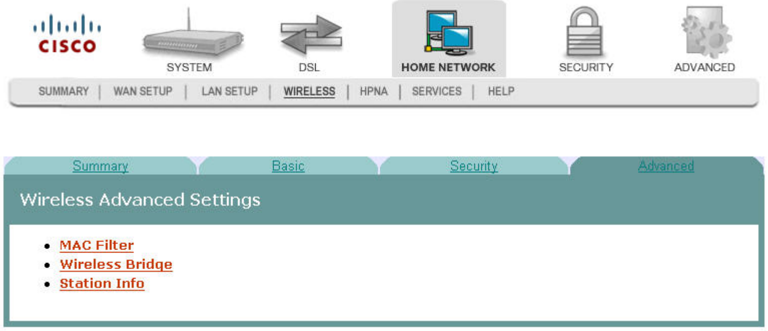
LAN1			192.168.1.64 00:10:60:03:9F:33
LAN2			
LAN3			
LAN4			
HPNA			Show HPNA Client
Wireless			Show Wireless Client

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



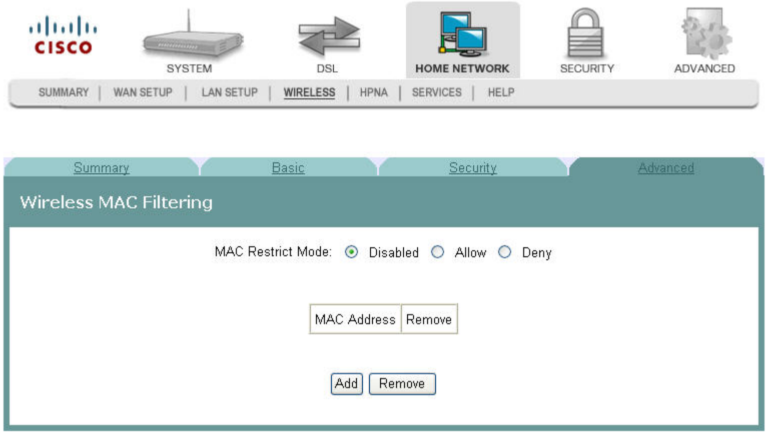
MAC Address	00:1E:6B:FA:9C:D8
SSID	Cisco
Authentication	open
Encryption	WEP Encryption:disabled

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


CISCO
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP
Summary
Basic
Security
Advanced
Wireless Advanced Settings

- MAC Filter
- Wireless Bridge
- Station Info

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



Wireless MAC Filtering

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

5 In the MAC Restrict Mode field, click **Deny** to enable the MAC restrict mode.

6 Click **Add**. The Wireless -- MAC Filter screen opens.

7 In the MAC Address field, enter the MAC address of the client that you want to prevent from accessing the residential gateway.

8 Click **Save/Apply** to prevent this wireless client from accessing the residential gateway.

Wireless Bridge

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

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

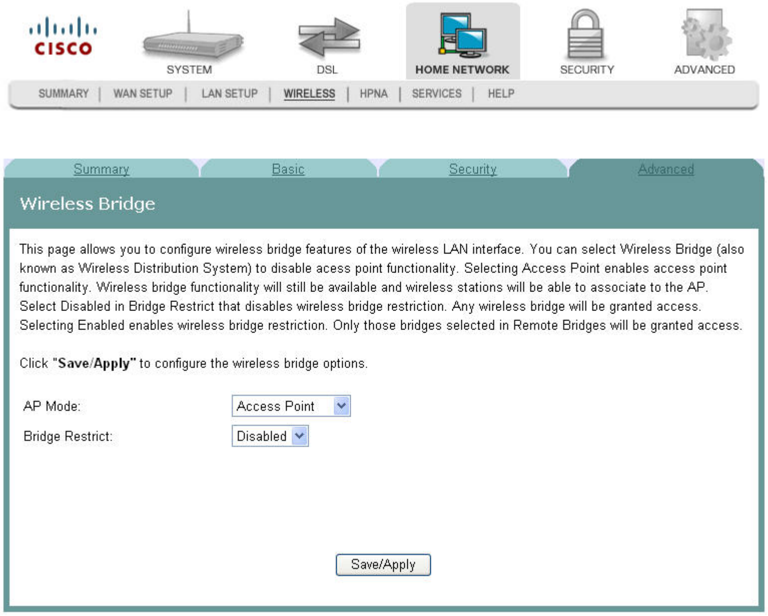
Select Wireless Bridge for the AP mode to disable access point functionality.

Select Access Point for the AP mode to enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.

Select Disabled for the Bridge Restrict field to disable wireless bridge restriction and any device can communicate with the residential gateway over the wireless bridge.

Select Enabled for the Bridge Restrict field to enable wireless bridge restriction to restrict the bridges that can communicate with the residential gateway over the wireless interface.

Path: Home Network > Wireless > Advanced > Wireless Bridge



Wireless Bridge

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

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

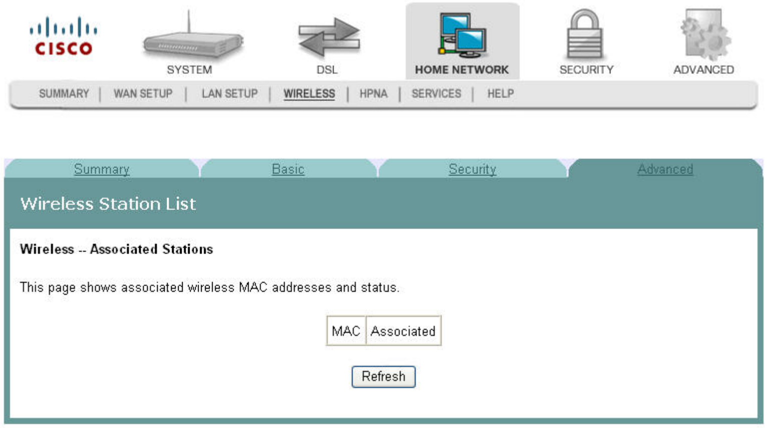
AP Mode: Access Point

Bridge Restrict: Disabled

Wireless Station List

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

Path: Home Network > Summary > Show Wireless Client



Wireless Station List

Wireless -- Associated Stations

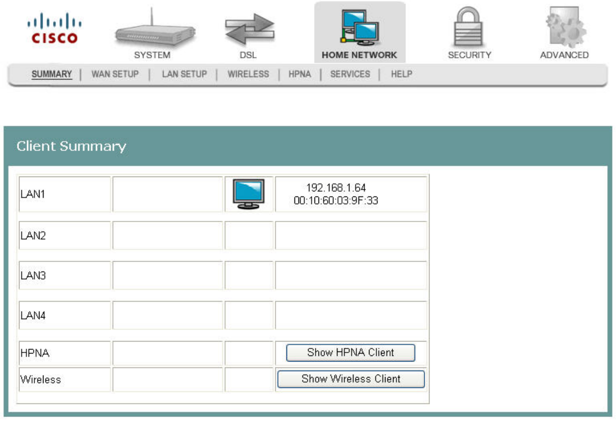
This page shows associated wireless MAC addresses and status.

MAC	Associated

Showing Attached Clients

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

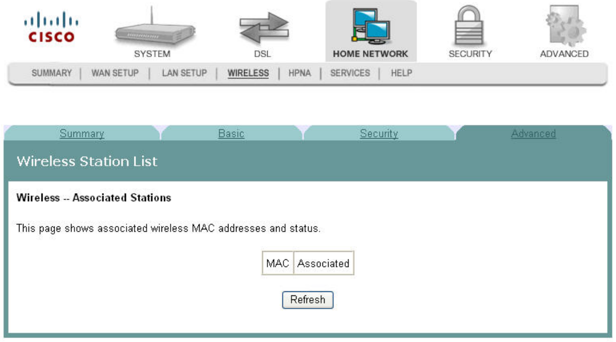
1. Click **Home Network** on the main screen.
2. Click **Summary**. The Client Summary screen opens.


SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

Client Summary

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

3 Click **Show Wireless Client**. The Wireless Station List screen opens.



Wireless Station List

Wireless -- Associated Stations

This page shows associated wireless MAC addresses and status.

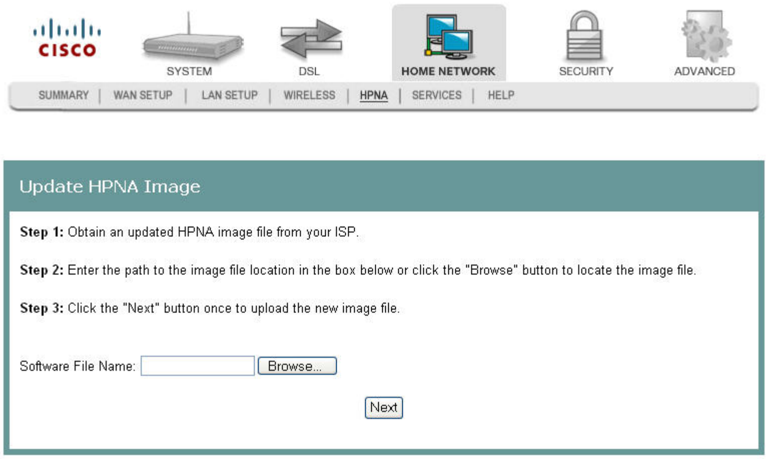
MAC	Associated

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

HPNA Information

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

Path: Home Network > HPNA > HPNA Info


cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP
Browse...
Next

Update HPNA Image

Step 1: Obtain an updated HPNA image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

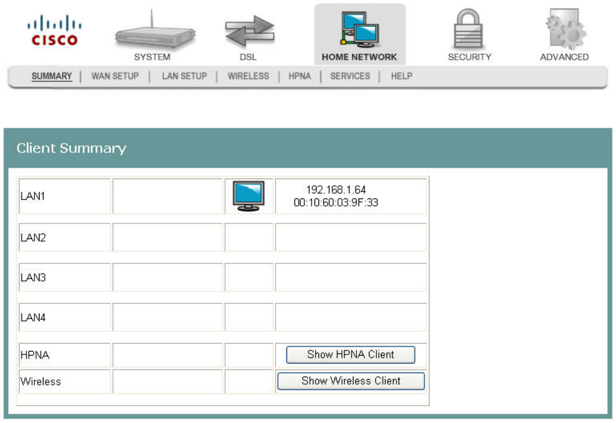
Step 3: Click the "Next" button once to upload the new image file.

Software File Name:

Updating HPNA Information

To update the HPNA information, complete the following steps.

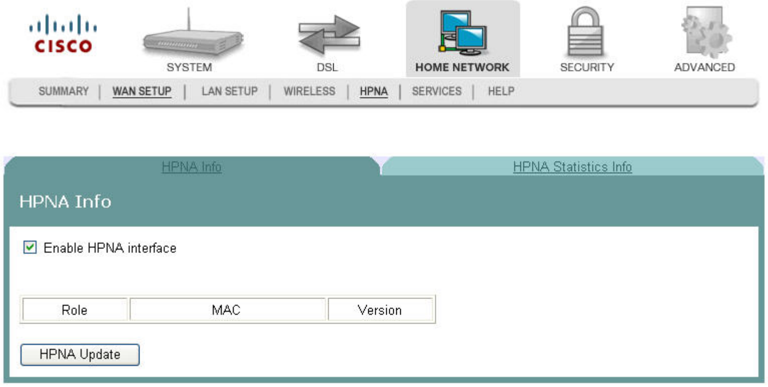
1 Click **Home Network** on the main screen. The Client Summary screen opens.


cisco
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

Client Summary

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

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



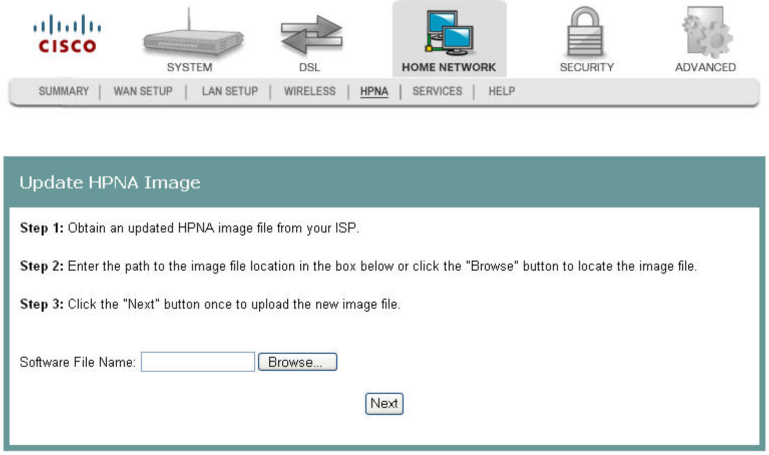
HPNA Info

☑ Enable HPNA interface

Role	MAC	Version

HPNA Update

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


CISCO
SYSTEM
DSL
HOME NETWORK
SECURITY
ADVANCED
SUMMARY | WAN SETUP | LAN SETUP | WIRELESS | HPNA | SERVICES | HELP

Update HPNA Image

Step 1: Obtain an updated HPNA image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Next" button once to upload the new image file.

Software File Name: Browse...

Next

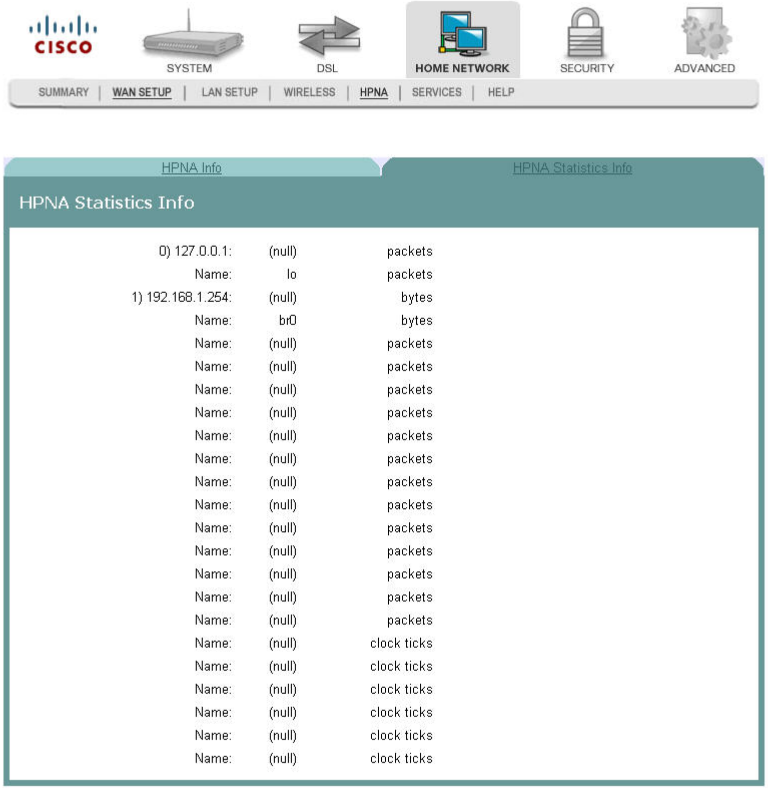
4 In the Software File Name field, enter the name of the file that you want to use to update your system. You can click Browse to locate the file.

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

HPNA Statistics Information

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

Path: Home Network > HPNA > HPNA Statistics Info



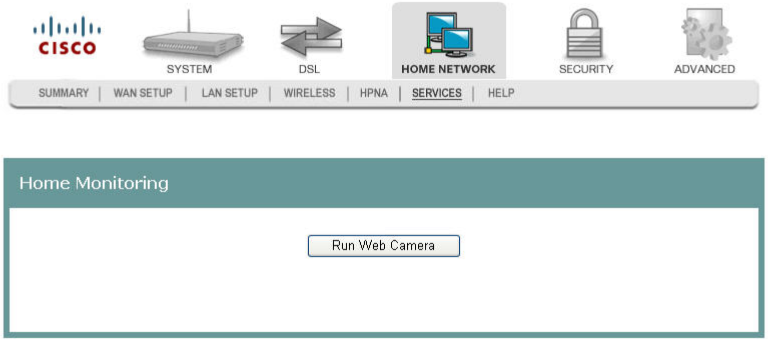
HPNA Statistics Info

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

Home Monitoring

The Home Monitoring screen allows you to monitor your surroundings by attaching a web camera to the USB port of the residential gateway. After you connect your camera, click **Run Web Camera**. A popup window appears showing the camera video output. The home monitoring feature is for local use only.

Path: Home Network > Services > Home Monitoring



6

Security Configuration

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

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

In This Chapter

- MAC Filtering Setup 128
- Incoming IP Filtering 134
- Outgoing IP Filtering 141
- Parental Control Setup - Filtering Function 146
- URL Filtering Function 151
- Stateful Packet Inspection 156
- Local Certificates 158
- Trusted CA Certificates 163

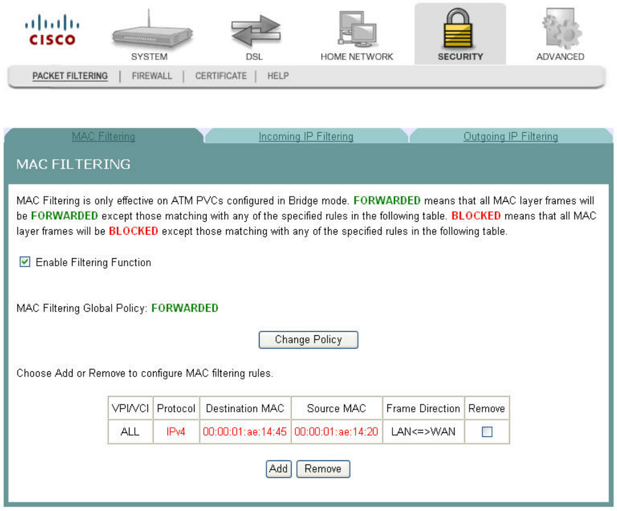
MAC Filtering Setup

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

Path: Security > Packet Filtering > MAC Filtering

Forwarded MAC Filtering

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



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

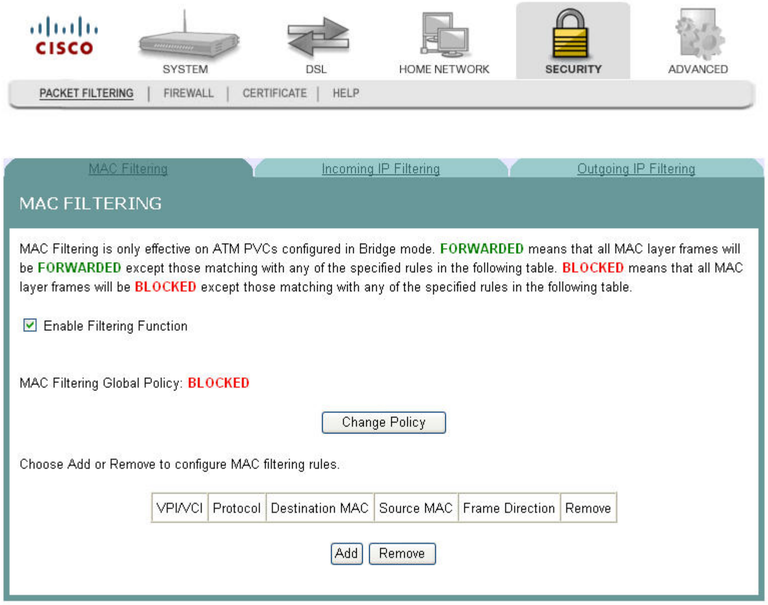
MAC Filtering Global Policy: **FORWARDED**

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	□

Blocked MAC Filtering

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



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: BLOCKED

Change Policy

Choose Add or Remove to configure MAC filtering rules.

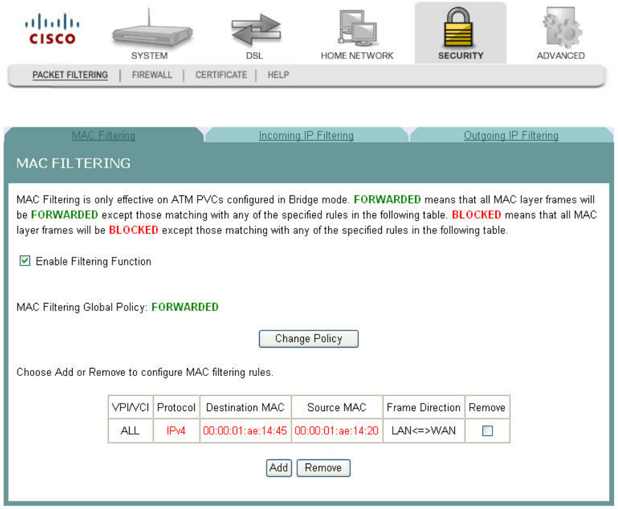
VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

Add Remove

Adding MAC Filtering

To add MAC Filtering, complete the following steps.

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



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

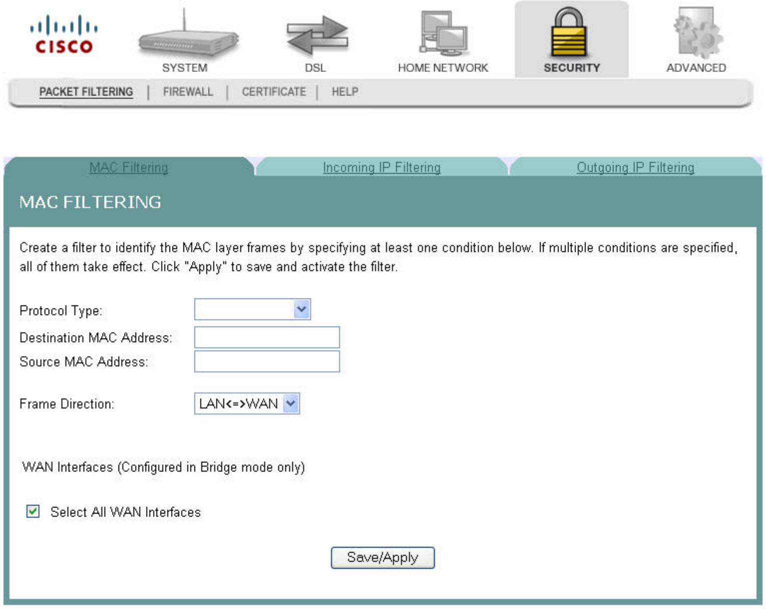
Change Policy

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	□

Add Remove

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



MAC FILTERING

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

Protocol Type:	
Destination MAC Address:	
Source MAC Address:	
Frame Direction:	LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

☑ Select All WAN Interfaces

Cl

5 In the Protocol Type field, select one of the following protocols from the drop-down menu.

- PPPoE
- IPv4
- IPv6
- AppleTalk
- IPX
- NetBEUI
- IGMP

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

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

8 In the Frame Direction field, select one of the following choices from the drop-down menu:

- LAN<->WAN
- WAN<->LAN

9 Do you want to select all WAN interfaces?

- If **yes**, check the Select All WAN Interfaces check box under the WAN Interfaces (Configured in Bridge mode only) field.
- If **no**, uncheck the Select All WAN Interfaces check box under the WAN Interfaces (Configured in Bridge mode only) field.

10 Click **Save/Apply** to add the MAC Filter.

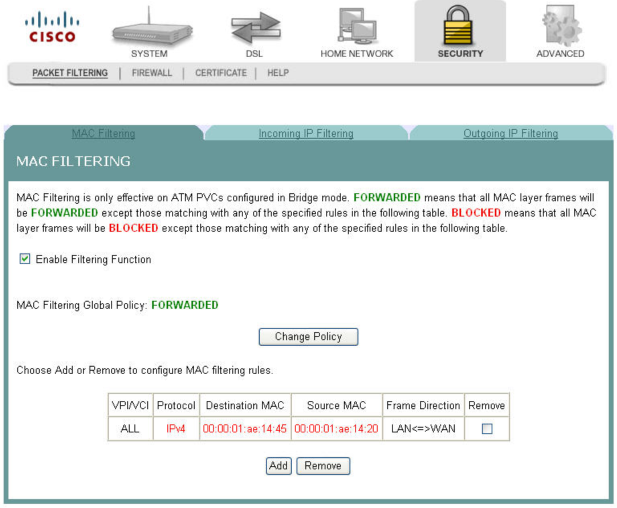
Forwarding or Blocking MAC Layer Frames

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

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

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

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



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

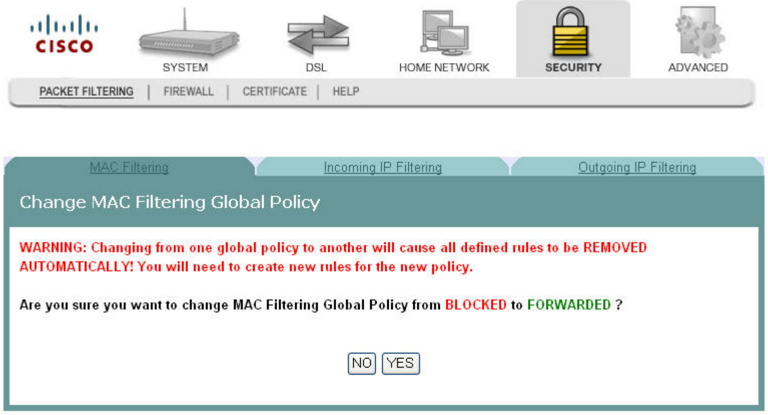
MAC Filtering Global Policy: FORWARDED

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	□

3 Check the **Enable Filtering Function** check box.

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



Change MAC Filtering Global Policy

WARNING: Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Are you sure you want to change MAC Filtering Global Policy from BLOCKED to FORWARDED ?

5 Do you want to change the Global Policy?

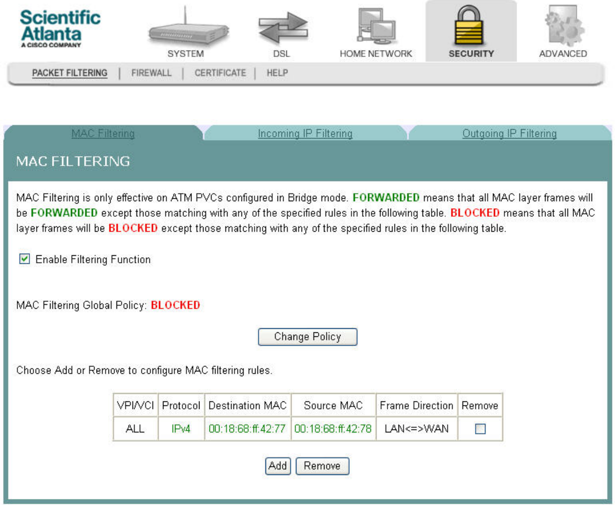
- If **yes**, click **Yes**. If the policy is forwarded, clicking Yes changes the policy to blocked and vise versa.
- If **no**, click **No** and the policy remains unchanged.

Removing MAC Filtering

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

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

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



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: BLOCKED

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	IPv4	00:18:68:ff:42:77	00:18:68:ff:42:78	LAN<=>WAN	□

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

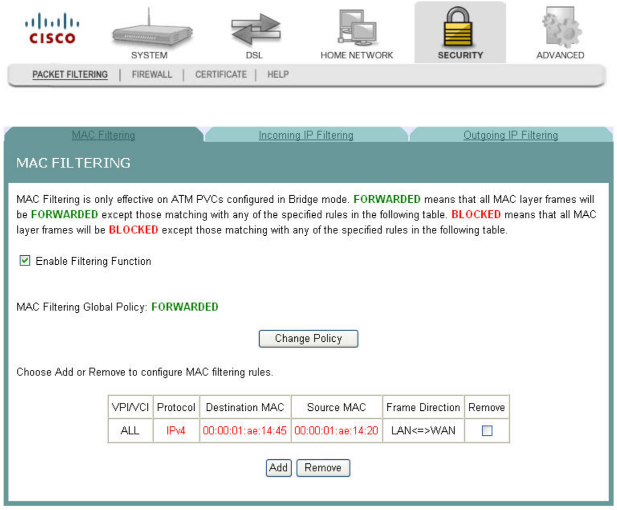
4 Click **Remove** to remove the MAC filtering.

Removing MAC Filtering

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

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

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



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

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	□

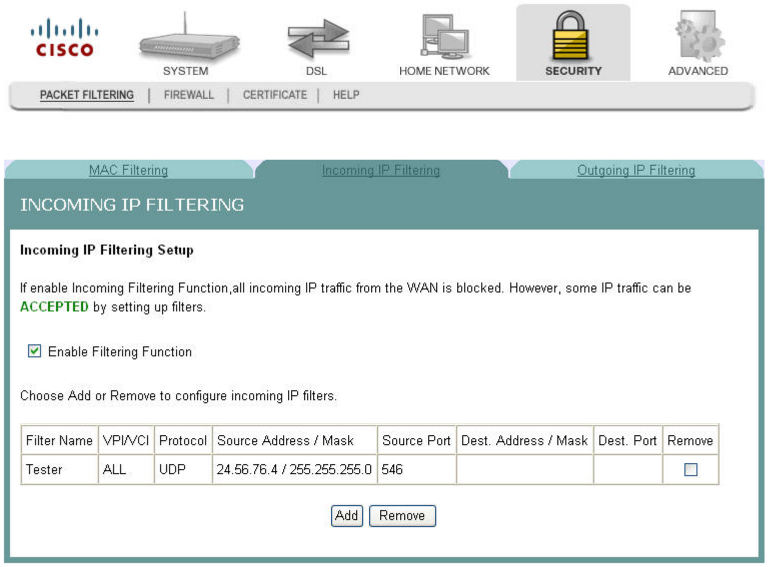
3 From the MAC Filtering screen, select **Remove** in the Remove column next to the MAC filtering rule you wish to remove.

4 Click **Remove** to remove the MAC filtering.

Incoming IP Filtering

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

Path: Security > Packet Filtering > Incoming IP Filtering



INCOMING IP FILTERING

Incoming IP Filtering Setup

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

☑ Enable Filtering Function

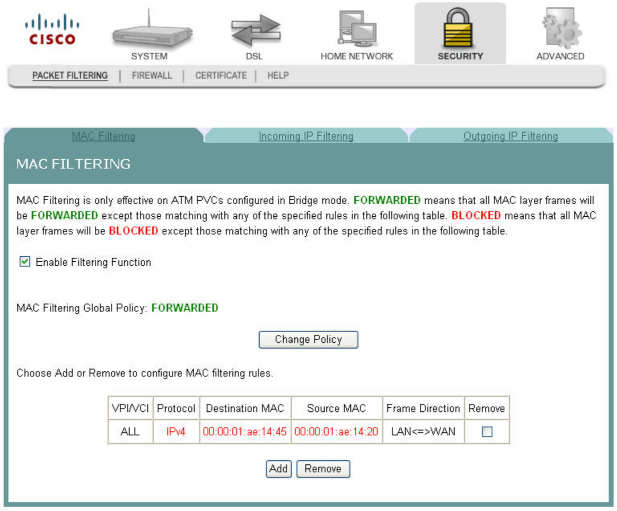
Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	ALL	UDP	24.56.76.4 / 255.255.255.0	546			□

Enabling the Filtering Function

To enable the filtering function, complete the following steps.

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



MAC FILTERING

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.

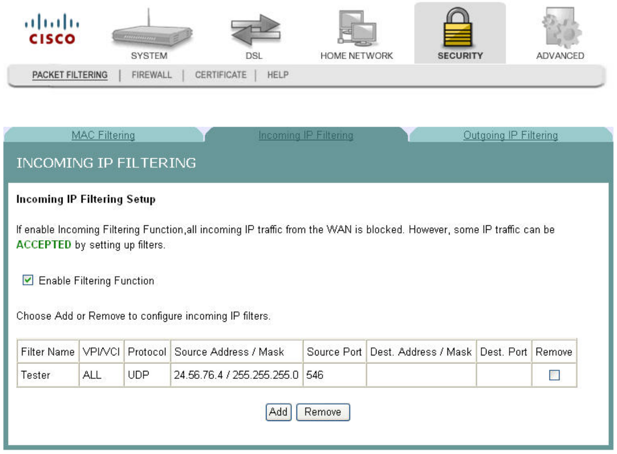
☑ Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

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	□

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



INCOMING IP FILTERING

Incoming IP Filtering Setup

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

☑ Enable Filtering Function

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	ALL	UDP	24.56.76.4 / 255.255.255.0	546			□

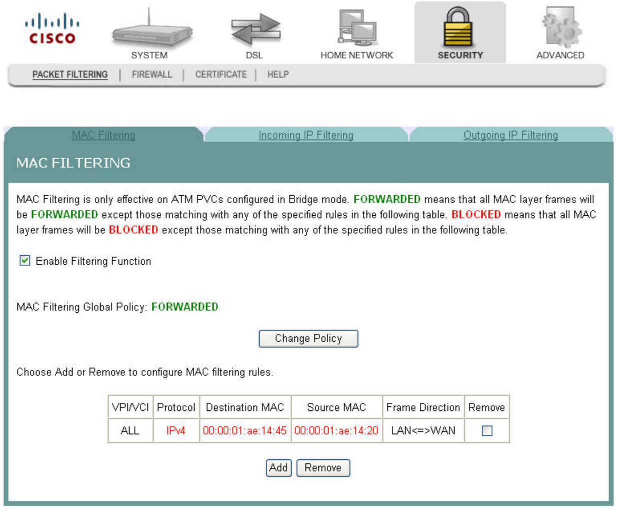
3 Check the **Enable Filtering Function** check box to enable the filtering function.

Adding an Incoming IP Filter

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

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

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



MAC FILTERING

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

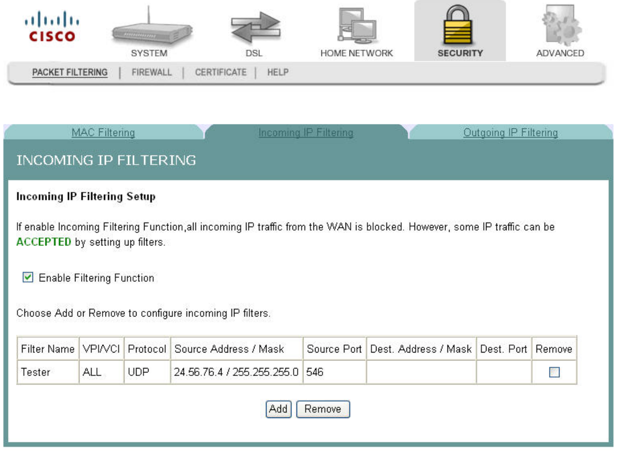
☑ Enable Filtering Function

MAC Filtering Global Policy: FORWARDED

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	□

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



INCOMING IP FILTERING

Incoming IP Filtering Setup

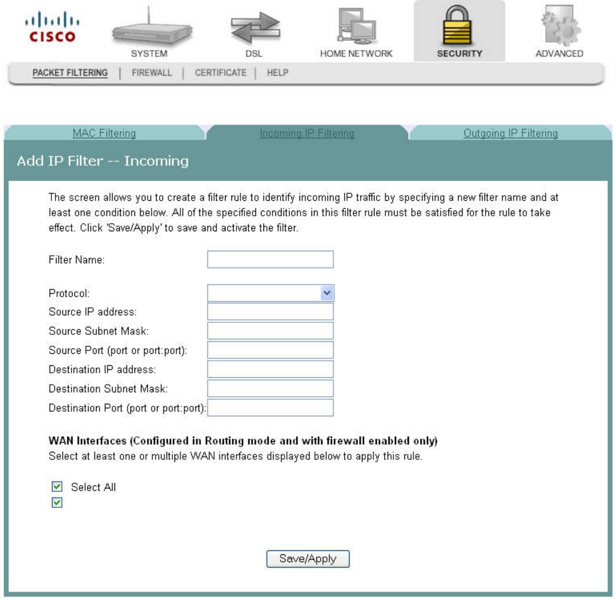
If enable Incoming Filtering Function,all incoming IP traffic from the WAN is blocked. However, some IP traffic can be **ACCEPTED** by setting up filters.

☑ Enable Filtering Function

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	ALL	UDP	24.56.76.4 / 255.255.255.0	546			□

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



Add IP Filter -- Incoming

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled only)

Select at least one or multiple WAN interfaces displayed below to apply this rule.

☑ Select All

☑

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

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

- TCP/UDP
- TCP
- UDP
- ICMP

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

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

8 In the Source Port field, enter the port number of the server sending the incoming packets. You can enter one port or a range of ports using the following format: port or port:port.

Example: 0:5 indicates ports 0 through 5.

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

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

11 In the Destination Port field, enter the port number for the server receiving the packets. You can enter one port or a range of ports using the following format: port or port:port.

Example: 0:5 to indicates ports 0 through 5.

12 Do you want to select all of the WAN interfaces?

- If **yes**, check the **Select All** field under WAN Interfaces (Configured in Routing mode and with firewall enabled only).
- If **no**, clear the **Select All** field under WAN Interfaces (Configured in Routing mode and with firewall enabled only).

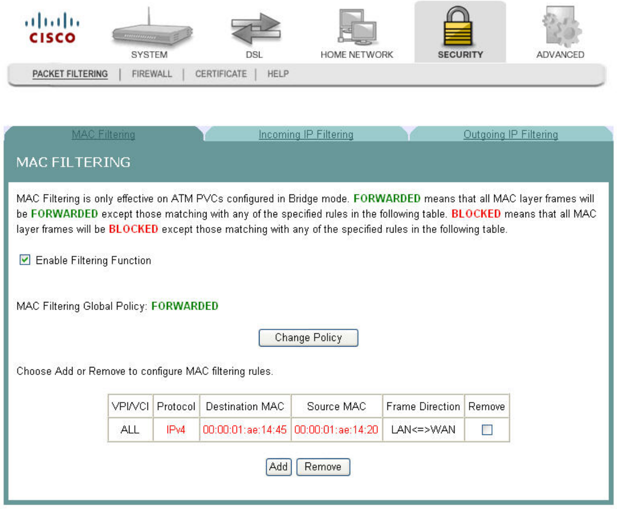
13 Click **Save/Apply** to add the filter.

Adding an Incoming IP Filter

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

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

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



MAC FILTERING

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

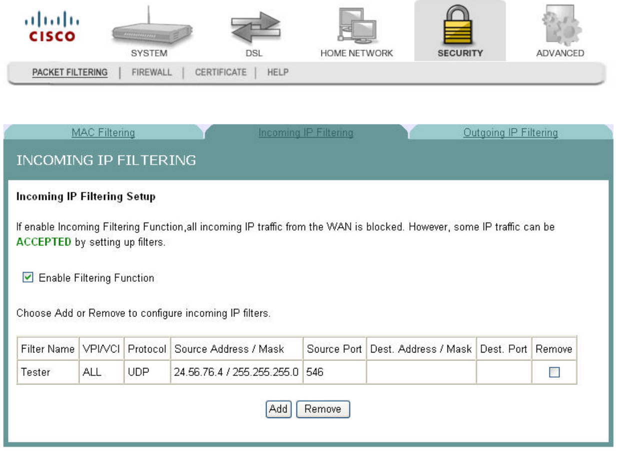
☑ Enable Filtering Function

MAC Filtering Global Policy: FORWARDED

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	□

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



INCOMING IP FILTERING

Incoming IP Filtering Setup

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

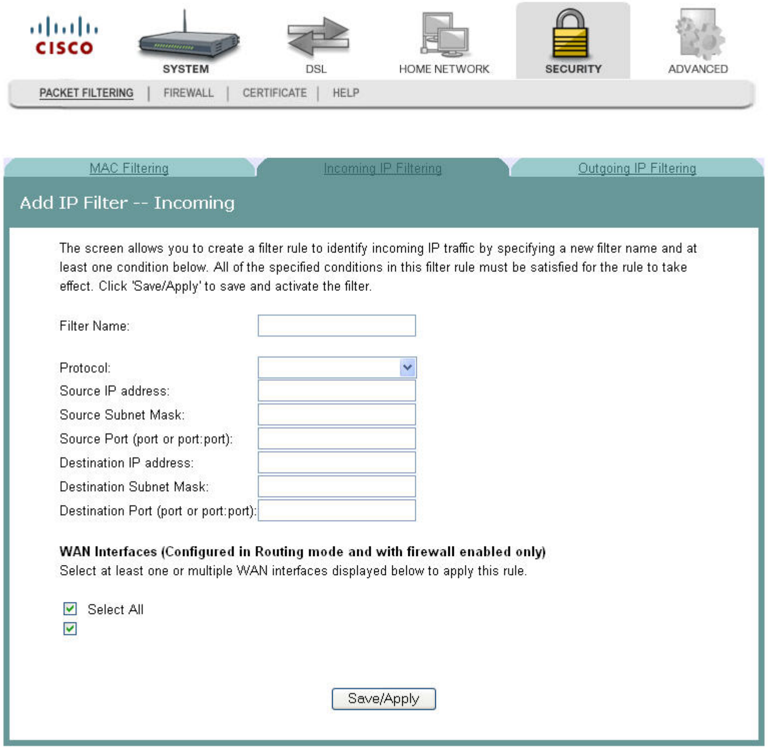
☑ Enable Filtering Function

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	ALL	UDP	24.56.76.4 / 255.255.255.0	546			□

Add Remove

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



Add IP Filter -- Incoming

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled only)

Select at least one or multiple WAN interfaces displayed below to apply this rule.

☑ Select All

☑

Save/Apply

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

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

- TCP/UDP
- TCP
- UDP
- ICMP

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

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

8 In the Source Port field, enter the port number of the server sending the incoming packets. You can enter one port or a range of ports using the following format: port or port:port.

Example: 0:5 indicates ports 0 through 5.

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

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

11 In the Destination Port field, enter the port number for the server receiving the packets. You can enter one port or a range of ports using the following format: port or port:port.

Example: 0:5 to indicates ports 0 through 5.

12 Do you want to select all of the WAN interfaces?

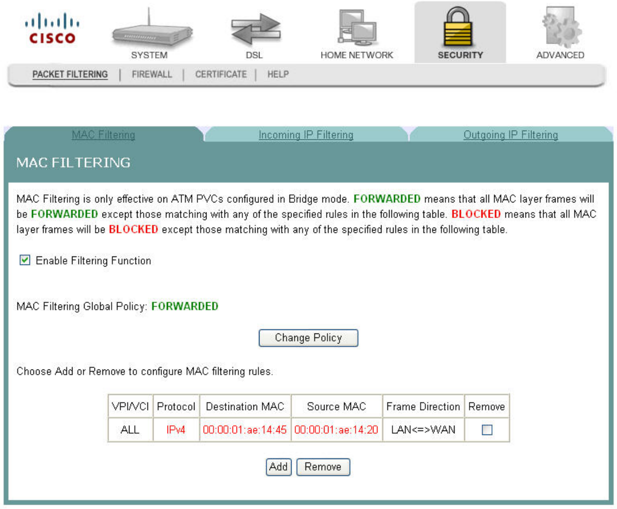
- If **yes**, check the **Select All** field under WAN Interfaces (Configured in Routing mode and with firewall enabled only).
- If **no**, clear the **Select All** field under WAN Interfaces (Configured in Routing mode and with firewall enabled only).

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

Removing an Incoming IP Filter

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

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



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.

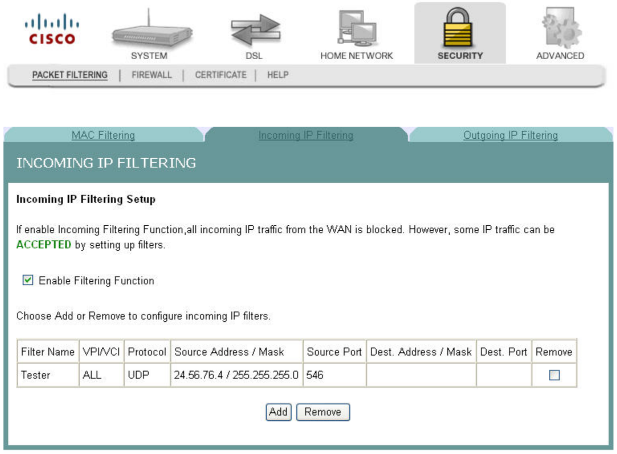
☑ Enable Filtering Function

MAC Filtering Global Policy: FORWARDED

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	□

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



INCOMING IP FILTERING

Incoming IP Filtering Setup

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

☑ Enable Filtering Function

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	ALL	UDP	24.56.76.4 / 255.255.255.0	546			☐

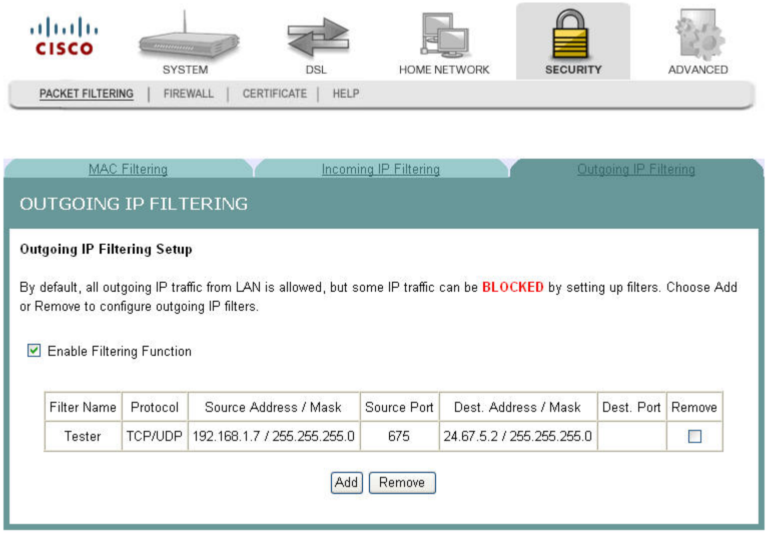
3 From the Incoming IP Filtering screen, select **Remove** in the Remove column next to the filter you wish to remove.

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

Outgoing IP Filtering

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

Path: Security > Packet Filtering > Outgoing IP Filtering



Outgoing IP Filtering Setup

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

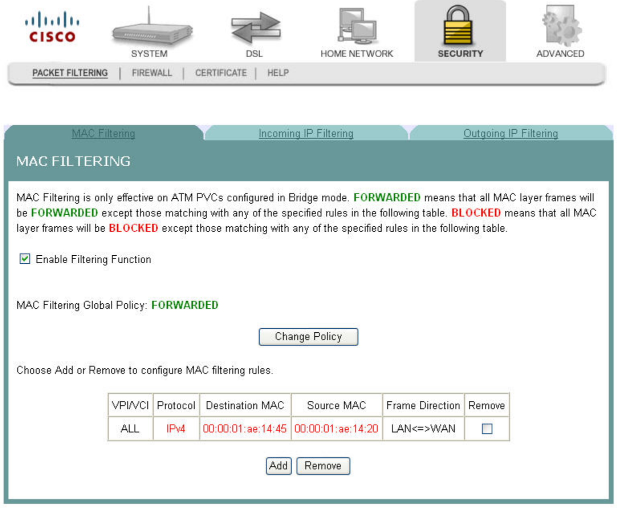
☑ Enable Filtering Function

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	TCP/UDP	192.168.1.7 / 255.255.255.0	675	24.67.5.2 / 255.255.255.0		□

Enabling the Filtering Function

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

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



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.

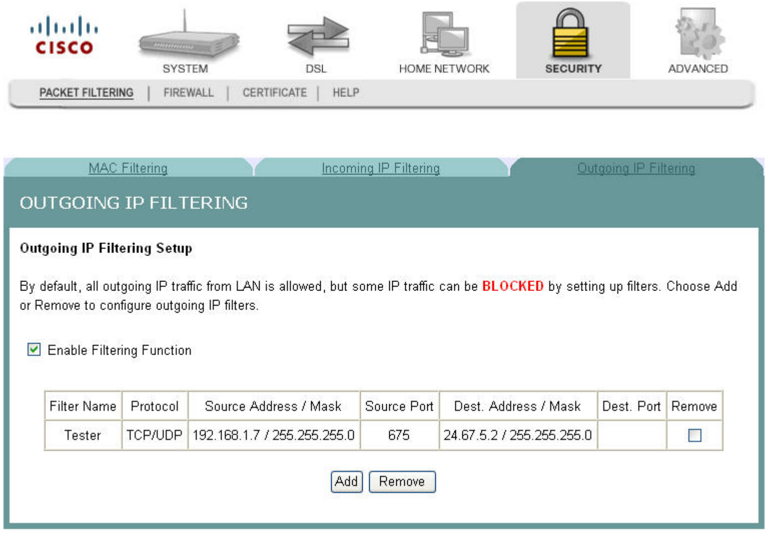
☑ Enable Filtering Function

MAC Filtering Global Policy: FORWARDED

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	□

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



OUTGOING IP FILTERING

Outgoing IP Filtering Setup

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

☑ Enable Filtering Function

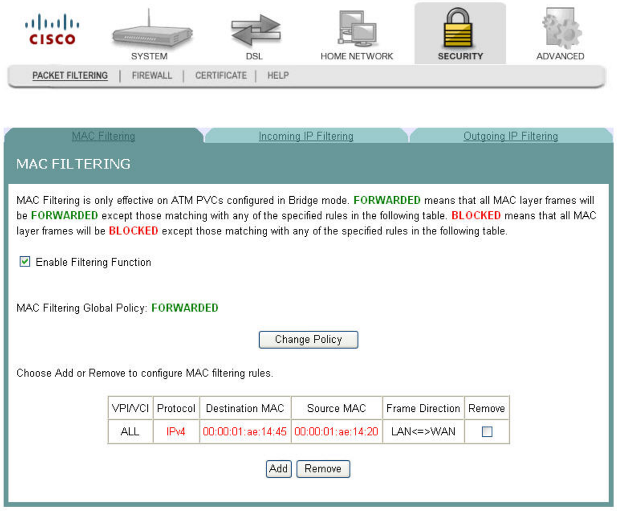
Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	TCP/UDP	192.168.1.7 / 255.255.255.0	675	24.67.5.2 / 255.255.255.0		□

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

Adding an Outgoing IP Filter

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

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



MAC FILTERING

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

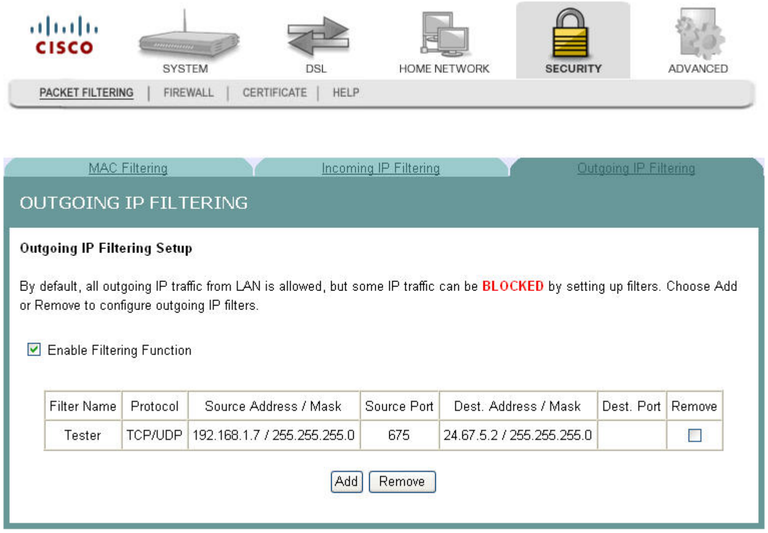
☑ Enable Filtering Function

MAC Filtering Global Policy: **FORWARDED**

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	□

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



OUTGOING IP FILTERING

Outgoing IP Filtering Setup

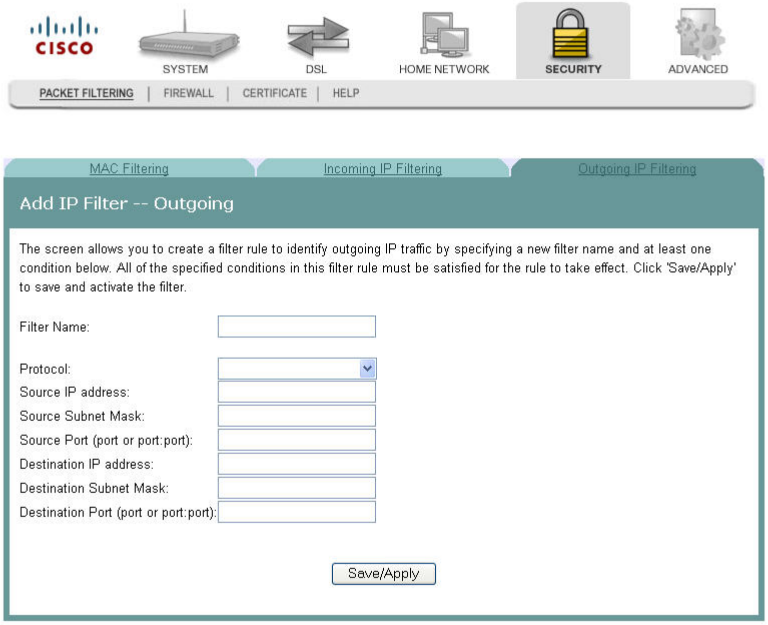
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters. Choose Add or Remove to configure outgoing IP filters.

☑ Enable Filtering Function

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	TCP/UDP	192.168.1.7 / 255.255.255.0	675	24.67.5.2 / 255.255.255.0		□

Add Remove

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



Add IP Filter -- Outgoing

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Save/Apply

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

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

- TCP/UDP
- TCP
- UDP
- ICMP

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

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

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

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

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

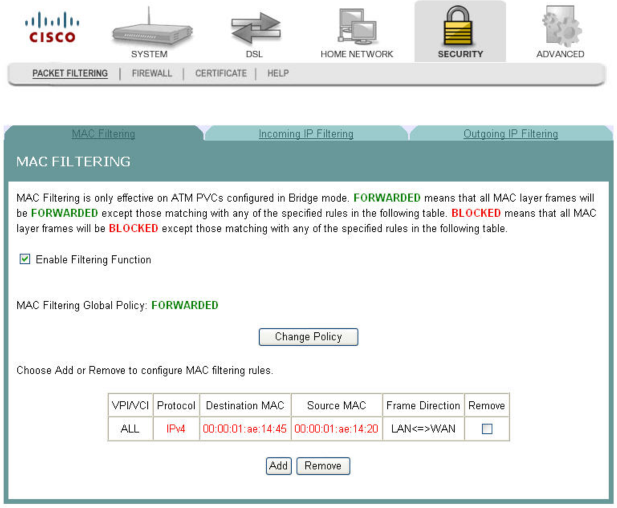
11 In the Destination Port field, enter the port number for the server receiving the packets. Use the following format: port or port:port.

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

Removing an Outgoing IP Filter

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

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



MAC FILTERING

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

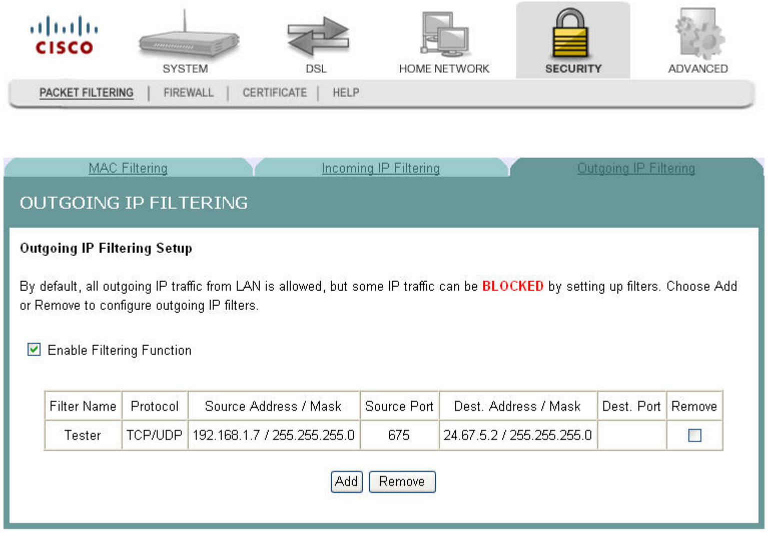
☑ Enable Filtering Function

MAC Filtering Global Policy: FORWARDED

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	□

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



OUTGOING IP FILTERING

Outgoing IP Filtering Setup

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

☑ Enable Filtering Function

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Tester	TCP/UDP	192.168.1.7 / 255.255.255.0	675	24.67.5.2 / 255.255.255.0		□

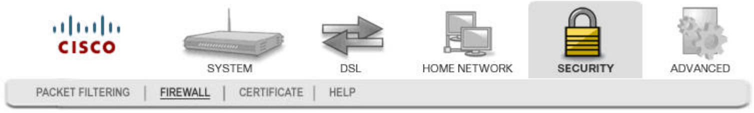
3 From the Outgoing IP Filtering screen, select **Remove** in the Remove column next to the filter you wish to remove.

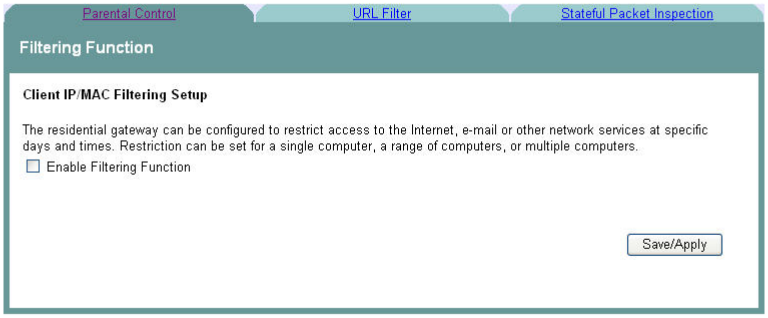
4 Click **Remove** to remove the filter.

Parental Control Setup - Filtering Function

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

Path: Security >Firewall > Parental Control





Filtering Function

Client IP/MAC Filtering Setup

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

□ Enable Filtering Function

Adding Time of Day Restrictions

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

Path: Security > Firewall > Parental Control

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