## **Http Server Port**

The Http Server Port screen allows you to modify the

2. to reviewers						
uluulu cisco						
	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED	
SUMMARY   DETAILS	STATISTICS   MAN	AGEMENT ADVANC	ED   HELP			
Configuration Http Server Port		<u>Settings</u>		Local Man	agement	
Http Server Port Function	allow user to change F	G WAN and LAN ht	ttp server port .			
LAN Http Server Port	80	Port Range [80 ,	1024 ~ 65535]			
WAN Http Server Port	8080	Port Range (80 ,	1024 ~ 65535]			
		Save/Rebo	ot			

## Modifying the Http Server Ports



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.



4 Click HttpServer. The Http Server Port opens.

cisco	SYSTEM			SECURITY	ADVANCED
SUMMARY   DETAILS	STATISTICS   MA	NAGEMENT   ADVANCED   HE	LP		
Configuratio	n	Settings		l ocal Man	anement
Ittp Server Por	t			Looarman	
ttn Sener Port Functio	n allow user to change	RG WAN and I AN httn server	nort		
		Det Barry 100, 1034 C	55051		
ANT LIAM CONTRACTOR	00	FULL Rarige JOU , 1024 ~ 0	2272]		
AN Http Server Port VAN Http Server Port	8080	Port Range (80 , 1024 ~ 6	5535]		
LAN Http Server Port WAN Http Server Port	8080	Port Range (80 , 1024 ~ 6	5535]		

- 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

cisco	SYSTEM	DSL	HOME NETWOR	K SECUR	ITY ADVANCED	
SUMMARY   DET	TAILS   STATISTICS	MANAGEMENT	ADVANCED   HELP	2		
Config	uration	1	<u>Settings</u>		Local Management	
System Log -	- Configuratior					
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: <ul> <li>Disable</li> <li>Error</li> </ul>						
Display Level:	Error 💙					
wode:	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.



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



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

alialia cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED	
SUMMARY   D	ETAILS   STATISTICS	MANAGEMENT	ADVANCED   HELP			
Conf	iguration	Y	Settings	Local Ma	inagement	
System Log	Configuratio					
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: <ul> <li>Disable</li> <li>Error</li> </ul>						
Display Level:	Error 🗸					
Mode:	Local 💌					
		Se	we/Apply			

- 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.



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

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED	
SUMMARY   D	ETAILS   STATISTICS	MANAGEMENT	ADVANCED   HELP			
Confi	guration	S S	Settings	Local Ma	inagement	
System Log	Configuratio					
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 event 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: <ul> <li>O Disable</li> <li>Denable</li> </ul>						
Display Level:	Error 🖌					
Mode:	Local 💙					
		Sa	we/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:

and the second se			
?	If disabled, the information captured by the DSL Residential Gatewa button, view the current system log, and use the Save option from	iy will be lost. If the File menu to	you wish to save the current log information, click the "Cancel" o save the log data.
	OK	Cancel	]

- 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

cisco	SYSTEM	DSL		SECURITY	ADVANCED
SUMMARY   DET.	AILS   STATISTICS	MANAGEMENT	ADVANCED   HELP		
<u>Config</u> System Log	uration	<u><u> </u></u>	ettings	Local Ma	inagement
Date/Time	Facility	Severity	Message		
		٦	lefresh		

#### **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.

CISCO SUMMARY   D	SYSTEM ETAILS   STATISTICS	DSL MANAGEMENT	HOME NETWORK	SECURITY	ADVANCED
<u>Com</u> System Log	iguration	Y	Settings	Local Ma	nagement
Date/Time	Facility	Severity	Message Refresh		

- 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



## **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.



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

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
SUMMARY   DETAILS	STATISTICS   MANAG	EMENT ADVANCE	<u>p</u>   HELP		
Print Server	Clone MAC	VolP Basic	VolP A	dvanced	USB
Print Server Setti	ngs				
This page allows you to en	able / disable print supp	ort.			
Enable on-board print	server.				
Print sever name					
Wate and model					
		Save/Apply			
7					

- 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.

cisco	SYSTEM	DSL		SECURITY	ADVANCED
SUMMARY   DETAILS	STATISTICS   MA	NAGEMENT   ADVANCE	D HELP		
Print Server	Clone MAC	VolP Basic	VolP	Advanced	USB
Print Server Setti	ngs				ularikalik.
This page allows you to en	able / disable print s	upport.			
☑ Enable on-board print :	server.				
Print sever name					
Make and model					
		Save/Apply			

**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.

cod LICB						
555						
Seve/Apply						

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



## **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.

cisco	SYSTEM	DSL		SECURIT	Y ADVANCED	
SUMMARY   DETAILS	STATISTICS   MANAG	BEMENT   ADVANCE	D   HELP			
Print Server	Clone MAC	VolP Basic	VolP A	Advanced	USB	
Print Server Setti	ngs					
This page allows you to er	nable / disable print supp	ort.				
🔲 Enable on-board print	server.					
Save/Apply						

3 Click the Clone MAC tab.



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

cisco	SYSTEM	DSL		SECURITY	ADVANCED
SUMMARY   DETAILS	STATISTICS   MA	NAGEMENT   ADVAN	CED   HELP		
Print Server Clone MAC	Clone MAC	VolP	<u>VolP A</u>	dvanced	USB
This page allows you to en	nable / disable clone   dress.	MAC function.			
MAC Address	00:	Loa	d client PC MAC	]	
		Apply/Reb	oot		

- **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.



3 Click the Clone MAC tab.

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
SUMMARY   DETAILS	STATISTICS   MA	NAGEMENT ADVAN	ICED   HELP		
Print Server		VolP	VolP A	<u>dvanced</u>	USB
Clone MAC					
This page allows you to en	able / disable clone N	MAC function.			
🔲 Enable clone MAC add	iress.				
		Apply/Reb	oot		

- **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

	EM	DSL	HOME NETWORK	SECURITY	ADVANCED	
SUMMARY   DETAILS	STATISTICS	MANAGEMENT	ADVANCED   HELP			
Custom Cummo						
System Summa	ý					
Device Info						
Model Name	DDR2201	v1				Log Out
Manufacturer	Cisco					
Serial Number :	AAD06I1	00007				
Software Version:	DDR2201 V00.00.0	v1-NA-Ann 1.07	exA-FCC-			
Hardware Version :	V06					
LAN MAC Address :	00:1e:6b	:fa:9c:da				
WAN MAC Address :	00:1e:6b	:fa:9c:da				
-						
Connection			trans capitols			
LAN IP Address:		192.168.	1.254			
Default Gateway:						
Primary DNS Server:		192.168.	1.254			
Secondary DNS Ser	ver:	192.168.	1.254			
Line Rate - Upstrea	m:					
Line Rate - Downstr	eam:					
Admin						
Admin						
System Uptime:		0 min				
System date and tir	ne	Sat Jan 1 NTP S	00:00:37 UTC 2000 erver Setting			
System password		Passw	ord 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.



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

cisco	SYSTEM	DSL	HOME NETWO		ADVANCED
SUMMARY DE	TAILS STATISTICS	MANAGEMENT	ADVANCED   HELI	2	
				0005000-0012	
Print Server	Clone MAC	VolP.1	<u>Basic</u>	VolP Advanced	USB
VoiceSIP					
Voice SIP Confi	guration				
Enter the SIP para	meters and click Start/S	top to save the para	meters and start/	stop the voice applic	ation.
Interface name:	LAN - Bridge 💙	]			
Locale selection:	USA - United St	ates 💌			
Preferred codec list	none 💌 none	e 💙 none 💙			
Preferred ptime	20				
0.0.1					
SIP domain name:					
Use SIP Prop	cy.				
Use SIP Out	aaund Proxy.				
🔲 Use SIP Reg	istrar.				
LineDisabled	Extension	Display Name	Authe Name	entication	Password
1					
4					
		Start S	IP client		
		Stop S	IP client		

- 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

Print Server	Clone MAC	VolP Basic	VolP Advanced	USB
VoiceSIP				
Voice SIP Advanced	Configuration			
LineForwarding number 1 2 2 Enable MWI subsc 2 Enable T38 support Registration Expire Timeout Dial-plan Setting: Dtmf Relay setting: SIP Transport protocol:	Call forwarding when busy ription t 3600 Voice Band V UDP V	Forwarding all calls	Call forwarding if no answer 	Call waiting
✓ Enable SIP tag mat ☐ Enable Music Serve Enable Music Serve	tching (Uncheck for ∨onag	Start SIP client		

## 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.

cisco	SYSTEM	DSL		SECURITY	ADVANCED
SUMMARY   DETAILS	STATISTICS   MAN	AGEMENT   ADVANC	ED   HELP		
Print Server	Clone MAC		VolP A	volvanced	
Print Server Setti					
This page allows you to er	able / disable print sup	iport.			
Enable on-board print	server.				
		Save/Appl	/		
		-			

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

Print Server	Clone MAC	VolP Basic	VoIP Advanced	USB
VoiceSIP				
Vaica SIP Advanced	Configuration			
voice Sir Auvanceu	Configuration			
LineForwarding	Call forwarding when	Forwarding all calls	Call forwarding if no	Call waiting
number	busy	_	answer	_
1 870				
2				
💟 Enable MVVI subscr	ription			
🗹 Enable T38 support				
Registration Expire	2600	í		
Timeout	3000			
Dial-plan Setting:				
Dtmf Relay setting:	Voice Band 💙			
SIP Transport protocol:	UDP 💙			
🗹 Enable SIP tag mat	ching (Uncheck for Vonage	Interop).		
Enable Music Serve	ar			
	ſ	Start SIP client		
	l	oran on chefit		
		Stop SIP client		

- **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

cisco	SYSTEM	DSL	HOME NETWOR	K SECURITY	ADVANCED
SUMMARY   DE	TAILS   STATISTICS	MANAGEMENT	ADVANCED   HELP		
<u>Print Server</u> USB File List	Clone MAC	<u>. Vol</u>	P Basic	VolP Advanced	USB
NO USB FLASH [	DEVICE				

3-6-2009 Draft

# 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
<u> </u>	

## **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 multiplexer (DSLAM). This screen reports the results of that process.

**Path**: DSL > Summary

CISCO SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
SUMMARY   STATISTICS	DIAGNOSTICS   SETTING	HELP		
Summary				
		1000	1	
	Downstream	Upstream		
SNR Margin (dB):				
Attenuation (dB):				
Output Power (dBm):				
Attainable Rate (Kbps):				
Rate (Kbps):				
La de arra				
Mode:				
Line Coding:				
Status:	Link Down			
	Entre Down			

## **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

cisco sy	STEM	DSL	HOME NETWORK	SECURITY	ADVANCED
SUMMARY   STATISTIC	S   DIAGNOSTIC	S SETTING	HELP		
	-				
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:					
	<u></u>				
ADSL BER Test	Reset Stati	stics			

#### 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.

The ADSL Bit Error R	ate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cel
containing a known p	attent and comparing the received data with this known pattern to check for any errors.
Select the test duration	on 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.

#### Chapter 4 DSL Configuration

#### **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

CISCO SYSTEM		HOME NETWORK	SECURITY	ADVANCED
SUMMARY   STATISTICS   DIAGNOS	TICS   SETTING	HELP		
Diagnostics				
Your residential gateway is capable of	testing your DS	L connection. The indivi	dual tests are liste	d below. If a test displays a
fail status, click "Rerun Diagnostic Tes	ts" at the botto	m of this page to make	sure the fail status	is consistent. If the test
continues to fail, click "Help" and follov	v the troublesho	ooting procedures.		
Test the connection to your local ne	etwork			
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		
ter an province				
Test the connection to your DSL se	rvice provider			
Test ADSL Synchronization:	FAIL	Help		
	[ Re	erun Diagnostic Tests		

#### **Running Diagnostic Tests**

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

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

#### Chapter 4 DSL Configuration

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

cisco	SYSTEM	DSL	HOME NETWOR	SECURITY	ADVANCED
SUMMARY	STATISTICS   DIAGNO	STICS   SETTING	HELP		
Diagnostic	s				
Your residential fail status, click continues to fail Test the conne	gateway is capable o "Rerun Diagnostic Te click "Help" and folle ction to your local i	oftesting your DS ests" at the botto ow the troublesho network	GL connection. The in m of this page to ma poting procedures.	ndividual tests are list ake sure the fail statu	ed below. If a test displays a s is consistent. If the test
Test your LAN	1 Connection:	PASS	Help		
Test your LAN	2 Connection:	FAIL	Help		
Test your LAN	3 Connection:	FAIL	Help		
Test your LAN	4 Connection:	FAIL	Help		
Test your USB	Connection:	DOWN	Help		
Test your Wire	less Connection:	DOWN	Help		
Test the conne	ection to your DSL s	ervice provider			
Test ADSL Sy	nchronization:	FAIL	Help		
		Re	erun Diagnostic Tes	s	

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



#### **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.

cisco 🧉	SYSTEM	DSL		SECURITY	ADVANCED
SUMMARY   STA	TISTICS   DIAGNOST	ICS   <u>SETTING</u>	HELP		
DSL Settings					
Select the modu	ation below.				
Automatic s	elect				
🗹 G.Dmt E	nabled				
🗹 G.lite Er	abled				
🗹 T1.413 E	Enabled				
ADSL2	Enabled				
🗹 AnnexL	Enabled				
ADSL2+	Enabled				
🗖 AnnexM	Enabled				
Capability					
Bitswap	Enable				
SRA En	able				
		Save/Apply	Advanced Setti	ngs	

#### Chapter 4 DSL Configuration

- **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

										Upst	rea	m T	on	35								
F	1		7	1	V	2	V	3	V	4	V	5	7	6	7	7	F	8	V	9	7	10
F	1	11	7	12	V	13	P	14	7	15	V	16	7	17	7	18	V	19	P	20	7	21
P	1	22	7	23	7	24	2	25	P	26	7	27	7	28	7	29	P	30	2	31		
									D	own	stre	am	То	nes								
F	1	32	4	33	V	34	2	35	P	36	V	37	7	38	7	39	V	40	V	41	7	42
P	1	43	7	44	V	45	7	46	P	47	7	48	7	49	V	50	V	51	7	52	7	53
P	1	54	V	55	7	56	4	57	V	58	2	59	7	60	V	61	2	62	V	63	7	64
P	1	55	V	66	V	67	V	68	V	69	V	70	7	71	V	72	V	73	V	74	V	75
F	1	76	7	77	V	78	2	79	V	80	V	81	7	82	7	83	V	84	2	85	7	86
F	1	87	7	88	V	89	F	90	7	91	7	92	7	93	7	94	R	95	7	96	7	97
P	1	86	4	99	V	100	P	101	P	102	7	103	7	104	V	105	P	106	P	107	7	108
2	,	109	7	11	7	111	P	112	V	113	V	114	7	115	7	116	R	117	2	118	7	119
P	7	120	V	12	1 🖓	122	P	123	V	124	V	125	7	126	7	127	F	128	V	129	7	130
P	,	131	7	13	21	133	P	134	V	135	V	136	7	137	7	138	V	139	V	140	7	141
F	1	142	V	14	3 🔽	144	P	145	P	146	V	147	P	148	7	149	R	150	P	151	7	152
P	1	153	V	15	١V	155	P	156	V	157	7	158	7	159	7	160	P	161	2	162	7	163
P	2	164	7	16	51	166	P	167	P	168	2	169	7	170	V	171	V	172	V	173	7	174
P		175	V	17	5₽	177	P	178	V	179	V	180	7	181	V	182	¥	183	V	184	7	185
P	7	186	V	18	7	188	P	189	V	190	V	191	7	192	7	193	P	194	P	195	7	196
F	1	197	P	19	5	195	P	200		201	7	202	7	203	7	204	R	205	P	206	V	207
P	1	208	V	20	9 🔽	210	P	211	P	212	V	213	2	214	V	215	P	216	P	217	7	218
P	1	219	7	22	7	221	P	222	V	223	V	224	7	225	7	226	R	227	2	228	7	229
P	1	230	V	23	1 🔽	232	P	233	V	234	V	235	7	236	7	237	F	238	V	239	7	240
P	1	241	7	24	2	243	P	244	V	245	V	246	7	247	7	248	F	249	V	250	7	251
	1	252	V	25	317	254	P	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.

				SECURITY	ADVANCED
SUMMARY   STATISTICS	DIAGNOSTICS	SETTING   HEL	Р		
DSL Settings					
Select the modulation	below.				
Automatic select					
🗹 G.Dmt Enable	ed				
🗹 Gilite Enabled	ł				
T1.413 Enabl	ed				
🗹 ADSL2 Enab	led				
🗹 AnnexL Enab	led				
🗹 ADSL2+ Ena	bled				
🔲 AnnexM Enab	oled				
Capability					
🗹 Bitswap Enab	le				
SRA Enable					
	Sa	ve/Apply A	dvanced Settings		

#### Chapter 4 DSL Configuration

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

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
SUMMARY	STATISTICS   DIAGNOST	ICS   <u>Setting</u>	HELP		
- 	100 MD				
DSL Advar	nced Settings				
	Se	lect the test mod	ie below.		
		<ol> <li>Norma</li> </ol>			
		O Reverb			
		Ne sets	e in		
		0.13	am		
		0.00			
		nnly Tone 9	Selection		
	Ľ	Tone c			

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

								-0	Upst	rea	m T	one	s									
7	0	7	1	7	2	V	3	7	4	V	5	V	6	7	7	V	8	7	9	7	10	
7	11	7	12	7	13	R	14	7	15	V	16	7	17	7	18	V	19	7	20	7	21	
7	22	7	23	7	24	2	25	7	26	7	27	7	28	7	29	V	30	7	31			
_		-		_		_		2	own	stre	am	101	182	_		-		_		_		
<u> </u>	32	2	33	2	34	2	35	2	36	2	37	2	38	4	39	2	40	2	41	2	42	
<u> </u>	43	2	44	2	45	2	46	2	47	2	48	2	49	2	50	M	51	2	52	2	53	
ľ	54		55		56	ž	51	Ľ	58	2	59	2	60	ľ	61	M	62	2	63	Ľ	64	
<u> </u>	66	2	00	2	0/	2	66	2	69	2	70	2	1	2	12	Ľ	13	2	14	2	/5	
<u> </u>	16	2	"	M	18	2	79	2	80	2	81	2	82	2	83	M	84	2	85	2	86	
ž	8/	M	88	M	89		90	M	91	N N	92		93	M	94	N	95		96	M M	97	
1	30	EZ.	33		100	E C	440	IN IN	102	1	105	E C	104	IN IN	105	1	100	E I	107		100	
-	100	E C	100		100	17	112	IN IN	113	1	100	10	110	IN IN	107	12	100	1	110		113	
-	120		121		122	-	120	E C	124	-	120	-	120	E C	120	-	120	Ē	140		130	
÷	142	-	142		133	-	146	E I	133	17	147	-	140	E I	140	-	100	Ē	140		160	
÷	162	Ē	164		100		160	E I	167		100	Ē	140	E I	100		100	Ē	101	1	102	
÷	164	2	165	2	166	2	167	V	168	17	169	2	170	V	171	1	172	R	173	2	174	
-	175	1	176	2	177	R	178	7	179	R	180	R	181	7	182	1	183	V	184	1	185	
-	186	Ā	187	2	188	R	189	7	190	R	191	R	192	7	193	R	194	R	195	V	196	
7	197	7	198	7	199	7	200	7	201	2	202	7	203	7	204	7	205	7	206	V	207	
v	208	7	209	7	210	7	211	V	212	7	213	7	214	7	215	7	216	7	217	V	218	
~	219	7	220	7	221	7	222	V	223	7	224	7	225	V	226	4	227	4	228	7	229	
7	230	7	231	7	232	7	233	7	234	2	235	7	236	7	237	F	238	7	239	7	240	
7	241	7	242	7	243	F	244	7	245	V	246	7	247	7	248	F	249	7	250	7	251	
7	252	7	253	7	254	7	255															
(	Chec	k/	M		Clea	H A	II	A	pph		Clo	se										

- 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

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED	
SUMMARY	STATISTICS   DIAGNO	STICS   <u>SETTING</u>	HELP			
DSL Adva	nced Settings					
	ä	Select the test mo	de below.			
		<ol> <li>Norma</li> </ol>	ıl			
		O Rever	1			
		🔘 Medle	У			
		🔘 No ret	rain			- 1
		O L3				
		Apply Tone	Selection			

#### **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.

SUMMARY   STATISTICS   DIAGNOS	HELP	
	Theor	
SL Settings		
elect the medulation below		
Automatic select		
G Dmt Enabled		
G lite Enabled		
T1 413 Enabled		
ADSI 2 Enabled		
Apport Enabled		
Annext Enabled		
ADSL2+ Enabled		
apability		
Bitswap Enable		
SRA Enable		

#### Chapter 4 DSL Configuration

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

cisco 🧃	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
SUMMARY   STA	ATISTICS   DIAGNOST	ICS   <u>SETTING</u>	HELP		
DSL Advance	ed Settings				
6 <u>.</u>					
	Se	lect the test mod	le below.		
		<ul> <li>Normal</li> <li>Deveda</li> </ul>			
		Modlov			
		<ul> <li>Ne rotr</li> </ul>	ain		
		012	an		
		Vω			
	A	pply Tone S	Selection		

- **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	
WAN Quick Setup	
Set Top Box Quick Setup	
LAN Setup	
Wireless Summary	
Wireless Basic	
Wireless Security	
Wireless MAC Filtering	
Wireless Bridge	
Wireless Station List	
HPNA Information	
HPNA Statistics Information	
Home Monitoring	

## **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		SECURITY	ADVANCED
SUMMARY   WA	N SETUP   LAN SETUP	WIRELESS   HF	NA   SERVICES   HELP		
Client Summ	ary				
	ſ			-	
LAN1			192.168.1.64 0:10:60:03:9F:33		
	1				
LAN2				-	
LAN3					
00000					
LAN4					
			Show HDNA Client		
				1	
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		SECURITY	ADVANCED
SUMMARY	WAN SETUP   LAN SETUP	WIRELESS   HF	PNA   SERVICES   HELP		
Client Sum	mary				
olicite o diff					
LAN1			192.168.1.64 10:10:60:03:9F:33		
		3			
LAN2					
LAN3					
LANA					
L COLMA					
HPNA			Show HPNA Client		

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

cisco	SYSTEM	DSL		SECURITY	ADVANCED	
SUMMARY   W	AN SETUP   LAN SETUP	WIRELESS   HPNA	SERVICES   HELP			
	HPNA Info	Y	HP	NA Statistics Info		
IPNA Info						
Chable HPNA	A Intenace					
Role	MAC	Version				
HPNA Update						
						anji toj

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   H	PNA   SERVICES   HELP			
Update HPNA Image					
Step 1: Obtain an updated HPNA image f	le from your ISP.				
Step 2: Enter the path to the image file lo	cation in the box b	elow or click the "Browse" b	outton to locate the i	mage file.	
Step 3: Click the "Next" button once to up	load the new imag	e file.			
Software File Name:	Browse				
	[	Next			
					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

CISCO	SYSTEM	DSL	н		SECURITY	ADVANCED
SUMMARY   WA	N SETUP   LAN SETUP	WIRELESS	HPNA   SE	RVICES   HELP		
Summary	4 Y	Basic	Y	Security	Y	Advanced
Mirolono Stol	atom a ton					
wireless sta	uon List					
Vireless Associ	iated Stations					
Wireless - Associ	iated Stations	C addresses an	nd status			
Wireless Sta Wireless Associ This page shows a	iated Stations	C addresses an	nd status.			
Wireless Associ This page shows a	iated Stations	C addresses an	nd status. AC Associati	əd		
Wireless - Associ	iated Stations	C addresses an MA	nd status. AC Associate Refresh	ad		

#### **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 SET	JP   LAN SETUP   WIRELES	S   HPNA   SERVICES   HELP		
Client Summary				
LAN1		192.168.1.64 00:10:60:03:9F:33		
LAN2				
LAN3				
LAN4				
HPNA		Show HPNA Client		
A Containe		Show Wireless Client	1	

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



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

		SYST	EM	DSL	HOME N	ETWORK	SEC	URITY	ADV.	ANCED
SUMMARY	WAN SETUR	2   LAN SE	TUP   WIRELE	ESS   HPNA	SERVICES	HELP				
							at Low Boar	COURSE DO	the second se	
	WAN	Ouick Setup			_	2		COLC SE	ωp	_
N Quick	WAN: Setup	<u>Ouick Setup</u>		T.		2	Sterep box	COLC: SE	ωp	
N Quick	WAN	) Satur				2	30.100.800	Currese	<u>wp</u>	
NN Quick e Area Net	WAN Setup work (WAN	) Setup		1		2	st rop box	COLCEDE	<u>0</u> 2	
AN Quick le Area Net ose Add, Edi	WAN Setup work (WAN t, or Remove	) Setup ) Setup	e WAN interfac	es. tem		2	211001004	CULCE	up	
AN Quick le Area Net ose Add, Edi ose Reboot t	WAN: Setup work (WAN t, or Remove p apply the c	) Setup ) Setup to configure hanges and	e WAN interfac	es. tem.		2				
AN Quick e Area Net ose Add, Edi ose Reboot t rt/Vpi/Vci	WAN: Setup work (WAN t, or Remove p apply the c	) Setup ) Setup to configure hanges and Category	WAN interface reboot the sys	es, tem. Interface	Protocol	IGMP	QoS	State	Remove	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	Commune				253
SUMMARY   W	SYSTEM VAN SETUP   LAN SETUP	DSL   WIRELESS   HI	PNA   SERVICES   HELP	SECURITY	ADVANCED
liont Summ					
lient <del>sum</del> n	nary				
LAN1			192.168.1.64 00:10:60:03:9F:33		
LAN2					
LAN3					
				-	
LAN4	-				
HPNA			Show HPNA Client		
DAT 1			Show Wireless Client		

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



#### 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.
- 1 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.



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.

- 1 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.

cisco	SYSTEM	DSL		SECURITY	ADVANCED
SUMMARY   WAN	SETUP   LAN SETUP	WIRELESS   HF	NA SERVICES HELP		
Client Summa	iry				
				-1	
LAN1			192.168.1.64 I0:10:60:03:9F:33		
	-				
LANZ					
LAN3					
LAN4					
1.112.00.02					
HPNA			Show HPNA Client		

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



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

SUMMARY     WAN SETUP     LAK       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 and reboots the residential gateway to make mew configuration effective.       IP Address:     192.168.1.254       Subnet Mask:     255.255.255.0       © Disable DHCP Server     Statil P Address:       IP Configure the Second IP Address and Subnet Mask for LAN interface	25						ululu cisco ∈
LAN Seture         Address Reservation           Local Area Network (LAN) Setup         Configure the DSL Residential Gateway IP Address and Subnet Mask for LAN interface. Save button only saves the Locanfiguration data. SaveReboot button saves the LAN configuration data and reboots the residential gateway to make new configuration effective.           IP Address:         192.1881.254           Subnet Mask:         255.255.255.0           Image: DHCP Server         Enable DHCP Server           Image: DHCP Server         Enable DHCP Server      <	ANGED	URITY ADVANC	HELP	SERVICES   H	WIRELESS   HPNA	TUP   LAN SETUP	SUMMARY   WAN SET
Local Area Network (LAN) Setup       Configure the DSL Residential Gateway IP Address and Subnet Mask for LAN interface. Save button only saves the Loconfiguration data. Save/Reboot button saves the LAN configuration data and reboots the residential gateway to make new configuration effective.       IP Address:     192.168.1.254       Subnet Mask:     255.255.255.0       Image: DHCP Server     Image: DhCP Server       Image: DhCP Server     Image: DhCP Serv							
		constion	Address Resenta			LAN Setup	
Configure the DSL Residencial Gateway IP Address and Subnet Mask for LAN interface. Save button only saves the L configuration data. Save/Reboot button saves the LAN configuration data and reboots the residential gateway to make mew configuration effective.  IP Address: 192.168.1.254 Subnet Mask: 255.255.255.0  Disable DHCP Server Start IP Address: 192.168.1.64 End IP Address: 192.168.1.64 End IP Address: 192.168.1.253 Subnet Mask: 255.255.255.0 Leased Time (how);24 Configure the second IP Address and Subnet Mask for LAN interface Configure the second IP Address and Subnet Mask for LAN interface							
Configure the DSL Residential Gateway IP Address and Subnet Mask for LAN interface. Save button only saves the L configuration data. Save/Reboot button saves the LAN configuration data and reboots the residential gateway to make new configuration effective. IP Address: 192.1681.254 Subnet Mask: 255.255.0 © Disable DHCP Server © Enable DHCP Server Start IP Address: 192.1681.64 End IP Address: 192.1681.253 Subnet Mask: 255.255.255.0 Leased Time (hour) [24 © Enable DHCP Server IP Address:					etup	WOFK (LAIN) SE	Local Area Netw
new configuration effective.  IP Address: IP Address: 255 255 255 0  Disable DHCP Server Enable DHCP Server Tart IP Address: IP 211881.64 Enable DHCP Server Lessed Time (hour);[24 Enable DHCP Server DHCP Server IP Address: DHCP Server IP Address: Configure the second IP Address and Subnet Mask for LAN interface	LAN e the	tton only saves the LAN tial gateway to make th	erface. Save button on the second s	Mask for LAN inte	Address and Subnet Market Address and Subnet Market	idential Gateway IP A w/Reboot button save	Configure the DSL Resid
IP Address:       192.168.1254         Submet Mask:       255.255.0         © Disable DHCP Server         Start IP Address:       192.168.164         Enable DHCP Server         Start IP Address:       192.168.164         Enable DHCP Server         Submet Mask:       255.255.255.0         Leased Time (hour); 24         O Enable DHCP Server IP Address:         DHCP Server IP Address:         Configure the second IP Address and Subnet Mask for LAN interface	0 1110	tial gateway to make the	soto the residential g	.ion data and repo	so the D-ix conliguial	ive.	new configuration effecti
Subnet Mask: 255.255.0 Disable DHCP Server Start IP Address: 192.168.1.64 End IP Address: 192.168.1.253 Subnet Mask: 255.255.0 Leased Time (hour);24 Configure the second IP Address:						192.168.1.254	IP Address:
Disable DHCP Server     Enable DHCP Server     Start IP Address: 192.168.1.64     End IP Address: 192.168.1.253     Subnet Mask: 255.255.0     Leased Time (hour) 24     Enable DHCP Server IP Address:     DHCP Server IP Address:     Configure the second IP Address and Subnet Mask for LAN interface						255.255.255.0	Subnet Mask:
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 (hout) 24     C     Enable DHCP Server Relay     DHCP Server IP Address:     Configure the second IP Address and Subnet Mask for LAN interface							
O Isable DHCP Server     Enable DHCP Server     Start IP Address: 192.168.1.64     End IP Address: 192.168.1.253     Subnet Mask: 255.255.20     Leased Time (nout) 24     O Enable DHCP Server Relay     DHCP Server IP Address:     Configure the second IP Address and Subnet Mask for LAN interface							
Start IP Address:       192.168.1.64         End IP Address:       192.168.1.253         Subnet Mask:       255.255.255.0         Leased Time (hout)       24         O Enable DHCP Server Relay       DHCP Server IP Address:						ver	O Disable DHCP Serv
End IP Address: 192168.1253 Subnet Mask: 255255255.0 Leased Time (hout) 24 © Enable DHCP Server Relay DHCP Server IP Address:						ver 192.168.1.64	<ul> <li>Enable DHCP Service</li> <li>Start IP Address:</li> </ul>
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						192.168.1.253	End IP Address:
Lessed Time (hour) [24 © Enable DHCP Server Relay DHCP Server IP Address:						255.255.255.0	Subnet Mask:
Enable DHCP Server Relay DHCP Server IP Address: Configure the second IP Address and Subnet Mask for LAN interface						): 24	Leased Time (hour)
DHCP Server IP Address:						ver Relay	C Enable DHCP Server
Configure the second IP Address and Subnet Mask for LAN interface						ddress:	DHCP Server IP Ad
Configure the second IP Address and Subnet Mask for LAN interface							
				nterface	bnet Mask for LAN ir	d IP Address and Su	Configure the second
Save SaveRebort				e/Rehoot	Sava Sav		
				et level (	0000 000		

#### **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		SECURITY	ADVANCED
SUMMARY   V	VAN SETUP   LAN SETUP	WIRELESS   HP	NA SERVICES HELP		
Client Sumr	nany				
Glieffe Salffi					
LAN1			192.168.1.64 0.10.60.03.9F:33		
		3			
LAN2					
LAN3					
I ANIA					
	_				
			Show HPNA Client		
HPNA					

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

cisco	SYSTEM			RK	SECURITY	ADVANCED
SUMMARY   WAN SE	TUP   LAN SETUP	WIRELESS   HP	A SERVICES	HELP		
	LAN Setup			Addre	ess Reservation	
Local Area Net	work (LAN) S					
Configure the DSL Res	idential Gateway IP	Address and Subn	et Mask for LAN ir	nterface. S	ave button only s	aves the LAN
configuration data. Sav	e/Reboot button sa	wes the LAN configu	uration data and re	boots the r	residential gatewa	ay to make the
new configuration effec	ive.					
IP Address	192 168 1 254					
Subnot Maek:	255 255 255 0					
Odbitet Wask.	233.233.233.0					
O Disable DHCP Se	ver					
Enable DHCP Ser	rer					
Start IP Address:	192.168.1.64					
End IP Address:	192.168.1.253					
Subnet Mask:	255.255.255.0					
Leased Time (hou	): 24					
O Enable DHCP Ser	ver Relay					
DHCP Server IP A	ddress:					
Configure the secor	d IP Address and S	Subnet Mask for LAI	N interface			
		Save S	eve/Rehoot			
			aventeboot			

- 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..

th: Home No	etwork > LAN	Setup > Address R	eservation	
cisco syst			ADVANCED	
SUMMARY   WAN SETUP	LAN SETUP   WIRELESS   HPNA	SERVICES   HELP		
LAN Setu	P	Address Reservation		
	(Static DHCD Assignm	ient)		
ddress Reservatior	T (Stude Diller Assignin			

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

cisco	SYSTEM	DSL		SECURITY	ADVANCED
SUMMARY	NAN SETUP   LAN SETUP	WIRELESS   HPM	NA   SERVICES   HELP		
Summ	ary.	Basic	Security	Y	Advanced
<u>Summ</u> /ireless St	immary	<u>Basic</u>	Security	Y.	<u>Advanced</u>
Summ Vireless Su	immary	Basic	Security		<u>Advanced</u>
Summ Vireless Su	immary MAC Address	Basic 00	Security :1E:6B:FA:9C:D8		<u>Advanced</u>
Summ /ireless Su	Immary MAC Address SSID	Basic 00	Security :1E:6B:FA:9C:D8 Cisco		<u>Advanced</u>
Summ Vireless Su	Immary MAC Address SSID Authentication	Basic 00	Security 1E:68:FA:9C:D8 Cisco open		<u>Advanced</u>

## **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

cisco	SYSTEM	DSL	н		SECURITY	ADVANCED
SUMMARY   Y	VAN SETUP   LAN	SETUP   WIRELESS	HPNA   SE	RVICES   HELP		
Summ	ary.			<u>Security</u>		Advanced
Wireless	Basic					
This page allows interface, hide th set based on cor Click "Apply" to Enable W Hide Acc SSID: Channel: BSSID: Wireless Mode: 54g Protection:	you to configure b e network from act thruty requirements configure the basic fireless ess Point Cisco 00:1E:6B:FA:9C: 802:11g & 802:11 Auto	asic features of the wi ive scans, set the wir wireless options.	rireless LAN in reless network	terface. You can er	lable or disable th	e wireless LAN trict the channel

#### **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		SECURITY	ADVANCED
SUMMARY   V	VAN SETUP   LAN SETUP	WIRELESS   HP	A SERVICES HELP		
Client Sumr	nary				
				-	
LAN1		<b>1</b>	192.168.1.64 ):10:60:03:9F:33		
LANZ					
LANZ					
LAN3					
LANIA					
LAN4					
HPNA			Show HPNA Client		
Wireless			Show Wireless Client	]	

2 Click Wireless. The Wireless Summary screen opens.

cisco	SYSTEM	DSL		SECURITY	ADVANCED
SUMMARY   W	AN SETUP   LAN SETUP	WIRELESS   HPNA	SERVICES   HELP		
19-10					212
Summa	ty Y	Basic	<u>Security</u>	Y	<u>Advanced</u>
<u>Summa</u> Wireless Su	¤ Y mmary	Basic	<u>Security</u>	1	<u>Advanced</u>
<u>Summa</u> Wireless Su	mmary MAC Address	Basic 00:1	Security E:6B:FA:9C:D8		<u>Advanced</u>
Summa Wireless Su	mmary MAC Address SSID	Basic 00:1	Security E:6B:FA:9C:D8 Cisco		<u>Advanced</u>
Summa Wireless Su	MAC Address SSID Authentication	Basic 00:1	Security E:6B:FA:9C:D8 Cisco open		<u>Advanced</u>

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

aludu cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
SUMMARY   V	VAN SETUP   LAN SETUP	WIRELESS   HP!	NA   SERVICES   HELP		
Summa	ary	Basic	Security	Y	Advanced
Wireless	Basic				
This page allows interface, hide the set based on cou Click "Apply" to c Enable W Hide Acce SSID: Channel: BSSID: Wireless Mode: 54g Protection:	you to configure basic fe a network from active sca nthy requirements. configure the basic wirele ireless ass Point Cisco 11 v 00:1E:6B:FA:9C:D8 802.11g & 802.11b v Auto v	atures of the wireles ans, set the wireless ass options.	s LAN interface. You can e network name (also knowr e/Apply	nable or disable th	he wireless LAN strict the channel

- 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.

SUMMARY         WAN SETUP         LAN SETUP         WIRELESS         HPHA         SERVICES         HELP           Client Summary         Image: Image	ADVANCED
Client Summary           LAN1           Image: Client Summary           LAN1           Image: Client Summary           LAN2           LAN3           LAN4	
Client Summary           LANI         Image: 192,168,1.64 00:10:60:03:9F:33           LANZ         Image: 192,168,1.64 00:10:10:00:03:9F:33           LANZ         Image: 192,168,1.64 00:10:10:00:03:9F:33           LANZ         Image: 192,168,1.64 00:10:10:00:03:9F:33	
LANI IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	
LAN2	
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   N	WAN SETUP   LAN SETUP	WIRELESS   HPN	A   SERVICES   HELP		

	шу	Basic	<u>Security</u>	Advanced
reless Su	immary			
	MAC Address	00:1E:68	-FA-9C-D8	
	SSID	00.12.00	Cisco	
	Authentication		open	
	E	WED Epor	votion: disabled	

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

cisco	SYSTEM	DSL	но		SECURITY	ADVANCED
SUMMARY   V	VAN SETUP   LAN SETUP	<u>WIRELESS</u>	HPNA   SERV	/ICES   HELP		
Summa	ary	Basic		<u>Security</u>	Y	Advanced
Wireless	Basic					
This page allows interface, hide th set based on co. Click "Apply" to i Enable W Hide Acco SSID: Channel: BSSID: Wireless Mode: 54g Protection:	you to configure basic fe e network from active sca intry requirements. configure the basic wirele fireless ess Point Cisco 11 00:1E:6B:FA:9C:D8 802.11g & 802.11b Auto	vatures of the wirele ans, set the wirele ass options.	eless LAN inter ess network n sve/Apply	erface. You can er	hable or disable t	he wireless LAN strict the channel

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

## **Wireless Security**

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

**Path**: Home Network > Wireless > Security

#### WEP Encryption Disabled



#### Securing Your Wireless Network with 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.



2 Click Wireless. The Wireless Summary screen opens.

cisco	SYSTEM	DSL		SECURITY	ADVANCED
SUMMARY   V	VAN SETUP   LAN SETUP	WIRELESS   H	IPNA   SERVICES   HELP		
Summa	arv/	Basic	Security	_	Advanced
Summa	ary	Basic	Security	Y	<u>Advanced</u>
<u>Summ</u> Vireless Su	immary	Basic	Security		<u>Advanced</u>
Summa Vireless Su	immary MAC Address	Basic	Security		<u>Advanced</u>
<u>Summ</u> : Vireless Su	Immary MAC Address SSID	Basic	Security 0:1E:6B:FA:9C:D8 Cisco		<u>Advanced</u>
Summ: Vireless Su	Immary MAC Address SSID Authentication	Basic C	Security 00:1E:6B:FA:9C:D8 Cisco open		Advanced

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



Summary	Basic		<u>Security</u>	Advanced
Wireless Securit	Y			
Select SSID:	Cisco 💌			
Network Authentication:	Open	*		
WEP Encryption:	Disabled 💌			
		Save/Apply		

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.

cisco			NETWORK	SECURITY	ADVANCED
SUMMARY   WAN SETUP	LAN SETUP	RELESS   HPNA   S	ERVICES   HELP		
Summary	Ba	sic	<u>Security</u>		Advanced
Wireless Securit	v				
Select SSID:	Cisco 💌				
Network Authentication:	Open	~			
WEP Encryption: Encryption Strength: Current Network Key: Network Key 1: Network Key 2: Network Key 3: Network Key 4:	Enebled V	128-bit V 1 V Enter 13 ASCII	characters or 26 her haracters or 10 hexa	kadecimal digits for	or 128-bit encryption 64-bit encryption
WEP Key Paraphrase: *The encryption strength 128-bit g generates 4 keys.	enerates 1 key. 64 bit			Generate	
		Save/Apply	,		

- 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 64bit 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.

cisco			SECURITY	ADVANCED
SUMMARY   WAN SETUP	LAN SETUP   WIRELESS	HPNA   SERVICES   HELF	0.00000000	ABTATOLD
lient Summary				
LAN1		192.168.1.64 00:10:60:03:9F:33		
LAN2				
LAN3				
LAN4				
HPNA		Show HPNA Client		

2 Click Wireless. The Wireless Summary screen opens.

cisco	Cumum D				250
	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
SUMMARY   \	WAN SETUP   LAN SETUP	WIRELESS   HPNA	SERVICES   HELP		

	ty Y	Basic		Security	Y	<u>Advanced</u>
ireless Su	mmary					
	P					
	MAC Address		00:1E:6B:FA:9C:	D8		
	SSID		Cisco			
	Authentication		open			

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

cisco sy	STEM			SECURITY	ADVANCED
SUMMARY   WAN SETUP	LAN SETUP	WIRELESS   HPNA	SERVICES HELP		
Summary	<b>_</b>	Bacin	Security		Advanced
Wireless Securit	,	<u></u>	<u>uccani</u>		
Select SSID:	Cisco 👻				
Network Authentication:	WPA-PSK	~			
WPA Pre-Shared Key:		Click he	ere to display		
WPA Group Rekey Interval: WPA Encryption:	U TKIP	~			
		Save/Ap	pply		

- 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 SETUR	WIRELESS   HPNA	A SERVICES HELP		
Summ	ary	Basic	Security		Advanced
Wireless M	IAC Filtering				
	MAC F	lestrict Mode: 💿 Dis	abled 🔿 Allow 🔿 De	eny	
		MAC Addres	s Remove		
		[Add] [F	lemove		

#### 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   W	AN SETUP   LAN SETUP	WIRELESS   HF	NA SERVICES HELP		
Client Summ	าลเร				
cherre Samin	icii y				
LAN1			192.168.1.64 I0:10:60:03:9F:33		
LAN2					
LAN3					
LAN4					
HPNA			Show HPNA Client		
				1	

2 Click Wireless. The Wireless Summary screen opens.

cisco	SYSTEM	DSL		SECURITY	ADVANCED
SUMMARY   W	AN SETUP   LAN SETUP	WIRELESS   HPNA	SERVICES   HELP		NUM Storestations and an
Summa	ry (	Basic	Security	Y	Advanced
<u>Summa</u> Wireless Su	mmary	Basic	<u>Security</u>		<u>Advanced</u>
<u>Summa</u> Wireless Su	mmary	Basic	<u>Security</u>		<u>Advanced</u>
<u>Summa</u> Wireless Su	mmary MAC Address	Basic 00:1	Security E:6B:FA:9C:D8		Advanced
Summa Wireless Su	MAC Address SSID	Basic 00:1	Security E:6B:FA:9C:D8 Cisco		<u>Advanced</u>
Summa Wireless Su	MAC Address SSID Authentication	Basic 00:1	Security E:6B:FA:9C:D8 Cisco open		<u>Advanced</u>

3 Click Advanced. The Wireless Advanced Settings screen opens.

CISCO SUMMARY W	SYSTEM AN SETUP   LAN SETU	DSL UP   WIRELESS	HPNA	DME NETWORK SERVICES   HELP	SECURITY	ADVANCED
Summar Wireless Adv	vanced Setting	<u>Basic</u> JS		<u>Security</u>		Advanced
<ul> <li>MAC Filte</li> <li>Wireless</li> <li>Station In</li> </ul>	rr Bridge nfo					

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

cisco	SYSTEM		HOME NETWORK	SECURITY	ADVANCED
SUMMARY   WA	N SETUP   LAN SE	TUP   <u>WIRELESS</u>   I	HPNA   SERVICES   HELP		
Summary	۲.	Basic	Security	Y	Advanced
Wireless MA	C Filtering				
	MA	C Restrict Mode: 💿	Disabled 🔘 Allow 🔘	Deny	
		MAC Ad	Idress Remove		
		Add	Remove		

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

#### **Blocking Wireless Clients**

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

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



2 Click Wireless. The Wireless Summary screen opens.

cisco	Cumumi 3				200
SUMMARY	WAN SETUP   LAN SETUP	WIRELESS   HPNA	SERVICES   HELP	SECORITY	ADVANCED

Summ	ary	Basic	<u>Security</u>	Advanced
/ireless Su	ummary			
	MAC Address	00:1E:6	iB:FA:9C:D8	
	SSID		Cisco	
	Authentication		open	

3 Click Advanced. The Wireless Advanced Settings screen opens.



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

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
SUMMARY   WAI	N SETUP   LAN SETUP	WIRELESS   HPNA	SERVICES   HELP		
Summary	Y	Basic	<u>Security</u>		Advanced
Wireless MA(	C Filtering				
	ç				
	MAC Re	estrict Mode: 💿 Disa	abled 🔿 Allow 🔿 De	eny	
		MAC Addres	s Remove		
		Add Re	emove		

- 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

cisco	SYSTEM	DSL		HOME NETWORK	SECURITY	ADVANCED
SUMMARY   WA	N SETUP   LAN SETU	P   WIRELESS	HPNA	SERVICES   HELP		
Summary	Y	Basic	Y	<u>Security</u>		Advanced
Wireless Brid	lge					
This page allows yo known as Wireless functionality. Wirel Select Disabled in Selecting Enabled Click <b>"Save/Apply</b> AP Mode: Bridge Restrict:	bu to configure wirele Distribution System ses bridge (nuctionali Bridge Restrict that of enables wireless brid " to configure the wir " to configure the wir [ A. Di	ss bridge feature to disable aces ty will still be avri- disables wireless ge restriction. O eless bridge opti ccess Point sabled	es of the wire s point funct ailable and w bridge restri- tions.	iless LAN interface. 1 itonality. Selecting Ar irreless stations will b iction. Any wireless t idges selected in Ren	′ou can select ¼ ccess Point ensat e able to assi ridge will be grar note Bridges will	/ireless Bridge (also les access point ate to the AP, ited access. be granted access.

## **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

cisco	SYSTEM	DSL		HOME NETWORK	SECURITY	ADVANCED
SUMMARY   1	WAN SETUP   LAN SET	TUP   <u>WIRELESS</u>	HPNA	SERVICES   HELP		
Summs	ary	Basic	Y	<u>Security</u>		Advanced
Wireless St	ation List					
Wireless Asso	ociated Stations					
This page shows	associated wireless	MAC addresses a	nd status.			
		M	AC Associa	ated		
			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   HI	PNA   SERVICES   HELP		
Client Sum	mary				
LAN1			192.168.1.64 J0:10:60:03:9F:33		
LAN2					
LAN3					
LAN4					
HPNA			Show HPNA Client		

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



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

	neo
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 "l	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	

### **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		SECURITY	ADVANCED
SUMMARY	WAN SETUP   LAN SETUP	WIRELESS   HPM	IA   SERVICES   HELP		
Client Sum	mary				
LANM			192.168.1.64	1	
LAN			: 10:60:03:9F:33		
LAN2					
LAN3					
I AN4					
HPNA			Show HPNA Client		

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

cisco	SYSTEM	DSL HO		SECURITY	ADVANCED
SUMMARY   WA	N SETUP   LAN SETUP	WIRELESS   HPNA   SER	VICES   HELP		
	HPNA Info	The second se	HP	NA Statistics Info	
HPNA Info					
🗹 Enable HPNA i	nterface				
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			SECUENTY	
SUMMARY   WA	N SETUP   LAN SETUP	WIRELESS   H	PNA   SERVICES   HELP	SECONT	ADVANGED
1400 M R. 4000000					
Update HPN	A Image				
Step 1: Obtain an	updated HPNA image fi	le from your ISP.			
Step 2: Enter the p	oath to the image file loo	cation in the box b	elow or click the "Browse" b	utton to locate the i	mage file.
Step 3: Click the "I	Next" button once to up	load the new imag	je file.		
Software File Name	e:(	Browse			
		(	Next		
			2		

- 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

cisco d	SYSTEM			TWOPK	SECURITY	
SUMMARY   WAN S	ETUP   LAN SETUP	WIRELESS	HPNA   SERVICES	HELP		
	HPNA Info			HEN	A Statistics Info	
	- Tofo					
HPINA Statistic	s mo					
	0) 127.0.0.1:	ínullì	packets			
	Name:	lo	packets			
1)	192.168.1.254:	(null)	bytes			
	Name:	brO	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

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
SUMMARY		WIRFLESS   HPNA	I SERVICES   HELP	SECORITY	ADVANCED
Home Moni	itoring				
		Run Web	Camera		

# 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.

cisco	SYS	EM	DSL	HOME NETWO		RITY	ADVANCED
PACKET FILTERIN	<u>G</u>   FIRE	VALL   C	CERTIFICATE   HELF	2			
MAC Filtering			Incom	Incoming IP Filtering		Outgoing IP Filtering	
MAC FILTER							
Enable Filterin     MAC Filtering Glob	g Function pal Policy:	FORWAR	DED CH	ange Policy			
		Destand		Course MAC	Former Dispetieur	Demons	
	ALL	IPv4	00:00:01:ae:14:45	00:00:01:ae:14:20	LAN<=>WAN	rcerniove	
			Add	Remove			
#### **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.

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
PACKET FILTERIN	<u>G</u>   FIREWALL   CEF	RTIFICATE   HELP		đ fa	
MAC F	Filtering	Incoming	IP Filtering	Outgoing I	P Filtering
MAC FILTER	ING				
MAC Filtering is or be FORWARDED layer frames will br I Enable Filterin MAC Filtering Glob	nly effective on ATM P∿ except those matching e <b>BLOCKED</b> except the g Function bal Policy: <b>BLOCKED</b>	/Cs configured in Bri with any of the spec se matching with ar Chani	dge mode. FORWARDE ified rules in the followin y of the specified rules ge Policy	D means that all MA og table. BLOCKED n in the following table.	C layer frames will neans that all MAC
Choose Add or Re	move to configure MAC	filtering rules.			
	VPI/VCI Protocol	Destination MAC	Source MAC Frame D	irection 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.

cisco	SYS	TEM	DSL	HOME NETWO		RITY	ADVANCED
PACKET FILTERING	<u>G</u>   FIRE	WALL   C	CERTIFICATE   HELP				
MAC F	iltering		Incomi	ng IP Filtering		Outgoing I	IP Filtering
MAC FILTER	ING						
Enable Filtering MAC Filtering Glob	g Function al Policy:	FORWAR	DED				
			Ch	ange Policy			
Choose Add or Rer	move to co	nfigure M4	AC 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.

#### 3-6-2009 Draft

#### Chapter 6 Security Configuration

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
PACKET FILTERING	FIREWALL   C	ERTIFICATE   HELP			
MAC Fi	Itering	Incoming	g IP Filtering	Outgoing	IP Filtering
MAC FILTERI	NG				
Protocol Type: Destination MAC Ad Source MAC Addre: Frame Direction:	Idress:	WAN V			
WAN Interfaces (Co	onfigured in Bridge m	node only)			
🗹 Select All WA	N Interfaces				
		Sav	e/Apply		

- 5 In the Protocol Type field, select one of the following protocols from the dropdown 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 dropdown 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.

cisco		The lot of					620
	SYS	TEM	DSL	HOME NETWO	RK SECU	RITY	ADVANCED
PACKET FILTERIN	G   FIRE	WALL   C	SERTIFICATE   HELP				
MAC F	iltering		Incom	ing IP Filtering		Outaoina I	P Filtering
MAC FILTER	ING						
Enable Filterin     MAC Filtering Glob	g Function	FORWAR	DED	any of the specified	roles in the follow	ving table.	
			Ch	ange Policy			
Choose Add or Re	move to co	nfigure M4	AC 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 Click **Change Policy**. The Change MAC Filtering Global Policy screen opens. In this example, the global policy for MAC filtering is "Blocked."

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED				
PACKET FILTERIN	NG   FIREWALL   CER	TIFICATE   HELP							
MAC	Filtering	Incoming	IP Filtering	Outgoing	IP Filtering				
Change MA	C Filtering Global	Policy							
WARNING: Chan AUTOMATICALL	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	Are you sure you want to change MAC Filtering Global Policy from BLOCKED to FORWARDED ?								
		NO	YES						

- 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.

L   CERTIFICATE   HELI	> Bridge mode. FOR pecified rules in the n any of the specifie	WARDED means i following table. Bi ad rules in the follow	Outgoing IP F that all MAC la LOCKED mear wing table.	iltering yer frames will is that all MAC
ATM PVCs configured in matching with any of the s xcept those matching with	ing IP Filtering Bridge mode. FOR pecified rules in the n any of the specifie	WARDED means 1 e following table. <mark>B</mark> i ad rules in the follor	Outgoing IP F that all MAC la LOCKED mear wing table.	<u>iltering</u> yer frames will is that all MAC
ATM PVCs configured in natching with any of the s xcept those matching with	Bridge mode. FOR pecified rules in the n any of the specifie	WARDED means t e following table. <mark>B</mark> ed rules in the follo	that all MAC la LOCKED mear wing table.	yer frames will is that all MAC
DCKED				
CH ure MAC filtering rules.	ange Policy			
Protocol Destination MAC	Source MAC	Frame Direction	Remove	
IPv4 00:18:68:ff:42:77	00:18:68:ff:42:78	LAN<=>WAN		
1	CH ire MAC filtering rules. rotocol Destination MAC IPv4 00:18:68:ff:42:77 [Add	Change Policy           ure MAC filtering rules.           rotocol         Destination MAC         Source MAC           IPv4         00:18:68:ff:42:77         00:18:68:ff:42:78           [Artid]         Remove	Change Policy           ure MAC filtering rules.           rotocol         Destination MAC         Source MAC         Frame Direction           IPv4         00:18:68:ff42:77         D0:18:68:ff42:78         LAN<<>>WAN           Add         Remove         Add         Remove	Change Policy are MAC filtering rules. Totocol Destination MAC Source MAC Frame Direction Remove IPv4 00:16:66:ff.42:77 00:16:66:ff.42:78 LAN<

- **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.

cisco	SYS	TEM	DSL	HOME NETWO		RITY	ADVANCED
PACKET FILTERING	FIRE	WALL   C	ERTIFICATE   HELP				
MAC F	Itering		Incomi	ng IP Filtering		Outgoing I	P Filtering
MAC FILTER	ING						
MAC Filtering is on be FORWARDED e layer frames will be I Enable Filtering	ly effective xcept tho BLOCKE Function	on AIM H se matchir Dexcept t	"VUs configured in ig with any of the sy hose matching with	Bridge mode, FORV secified rules in the any of the specified	VARDED means t following table. <mark>BL</mark> I rules in the follow	hat all MAV .OCKED m ving table.	C layer frames will leans that all MAC
MAC Filtering Glob	al Policy:	FORWAR	DED				
			Ch	ange Policy			
Choose Add or Rer	nove to co	nfigure M4	AC 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			S

- **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

aliali cisco	¢	SYSTEM	DSL	HOME NET	WORK SECURIT	TY	ADVANCED			
PACKET FIL	TERING	FIREWALI	L   CERTIFICATE   HELP							
N	MAC Filtering Incoming IP Filtering Outgoing IP Filtering									
INCOMIN	NG IP F	ILTER	ING							
Incoming IP	Filtering	Setup								
If enable Inco ACCEPTED I	ming Filte by setting	ring Funct up filters.	ion,all incoming IP traffic fro	m the WAN is	blocked. However, som	e IP traffic ca	an be			
🗹 Enable f	Filtering Fu	unction								
Choose Add	or Remove	e to config	ure 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						

# **Enabling the Filtering Function**

To enable the filtering function, complete the following steps.

cisco	SYS	IFM	DSI			BITY	ADVANCED
PACKET FILTERI	NG   FIRE	WALL   C	CERTIFICATE   HELP				
MAC	Filtering		Incomi	ng IP Filtering		Outgoing I	P Filtering
MAC FILTER							
🔽 Enable Filteri	na Eunction						
MAC Filtering Glo	ibal Policy:	FORWAR	DED				
MAC Filtering Glo	ibal Policy:	FORWAR	DED	ange Policy			
MAC Filtering Glo Choose Add or R	ibal Policy: emove to co	FORWAR	DED Chi	ange Policy			
MAC Filtering Glo	ibal Policy: emove to co	FORWAR nfigure M/ Protocol	DED Chi AC filtering rules. Destination MAC	ange Policy Source MAC	Frame Direction	Remove	
MAC Filtering Glo	emove to co	FORWAR nfigure MA Protocol	DED Chitering rules. Destination MAC 00:00:01:ae:14:45	Source MAC	Frame Direction	Remove	
MAC Filtering Glo	emove to co	FORWAR nfigure MA Protocol IPv4	Chi Chi AC filtering rules. Destination MAC 00:00:01:ae:14:45 [Add	Source MAC 00:00:01:ae:14:20	Frame Direction LAN<=>WAN	Remove	

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



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.

cisco	C						23
PACKET FILTERING	SYS	WALL   C	ERTIFICATE   HELP	HOMENETWO	RK SECU	RITY	ADVANCED
MAC F	iltering		Incomi	na IP Filterina		Outaning	IP Filtering
				ing in the ling			- incenting
MAC FILTER.	ING						
MAC Filtering Glob	g Function al Policy:	FORWAR	DED				
			Ch	ange Policy			
Choose Add or Rer	nove to co	nfigure MA	C 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			

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



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

cisco	SYSTEM	DSL	HOME NETWORK	SECURITY	ADVANCED
PACKET FILTERING	FIREWALL   CE	RTIFICATE   HELP			
MAC Fi	Itering	Incoming	IP Filtering	Outgoing I	P Filtering
The screen a least one cor effect. Click ' Filter Name:	llows you to create a ndition below. All of th Save/Apply' to save a	filter rule to identify in the specified condition and activate the filter.	ncoming IP traffic by sp s in this filter rule must	ecifying a new filter na be satisfied for the rul	ime and at e to take
Protocol: Source IP ad Source Port Destination II Destination F WAN Interfa Select at lea IV Select A	dress: et Mask; (port or port): 2 address: 3ubnet Mask; 2 ort (port or port;port) and (port or port;port) cces (Configured in st one or multiple W/4	Routing mode and	with firewall enabled	only) le.	
		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.

### 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.

cisco	C	TEM					200
PACKET FILTERING	E   FIRE	WALL   C	ERTIFICATE   HELP	HOWENETWO	NK SECO	MIT	ADVANGED
MAC F	iltering		Incomi	ng IP Filtering		Outgoing I	P Filtering
MAC FILTER:							
Iayer frames will be	BLOCKE Function	D except t	hose matching with	any of the specified	I rules in the follow	ving table.	
Choose Add or Rer	nove to co	nfigure M4	Ch	ange Policy			
	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		·	

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



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

cisco 🥌					25
S1	STEM	DSL	HOME NETWORK	SECURITY	ADVANCED
PACKET FILTERING   FI	REWALL   CERTIFIC	CATE   HELP			
MAC Filtoving		Incoming	D Ciltoring	Quitagina II	3 Eiltoving
MACTINEIIng		nconing	<u>r i menng</u>	Odigoing in	- r menng
Add IP Filter In	coming				
The screen allows y	ou to create a filter	rule to identify in	coming IP traffic by s	pecifying a new filter na	me and at
effect Click Save/A	pelow. All of the spi upply' to save and a	ecified conditions	In this fliter rule must	. De satisfied for the rule	e to take
circut onen ouron	ppij to ouve and a	envare the inter.			
Filter Name:					
Protocol:			~		
Source IP address:					
Source Subnet Mas	k:				
Source Port (port or	port:port):				
Destination IP addre	ISS:				
Destination Subnet	Mask:				
Destination Port (po	rt or port:port):				
WAN Interfaces (C	onfigured in Rout	ing mode and v	vith firewall enable	l only)	
Select at least one	or multiple www.ini	tenaces displaye	d below to apply this r	ule.	
🗹 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.

CISCO	even	TEM					
PACKET FILTERING	E   FIRE	WALL   0	CERTIFICATE   HELP	HOWENETWO	11K 3200	RUTT	ADVANCED
MAC F	iltering		Incomi	ng IP Filtering	Y	Outgoing I	P Filtering
MAC FILTER							
<ul> <li>Enable Filtering</li> <li>MAC Filtering Glob</li> </ul>	) Function al Policy:	FORWAR	DED				
			Ch	ange Policy			
Choose Add or Ren	nove to co	nfigure MA	AC filtering rules.				
	-	Protocol	Destination MAC	Source MAC	Frame Direction	Remove	
	VPI/VCI	1 1010001					
	VPI/VCI 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.



- **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

	lulu Isco	SYS	TEM	DSL	HOME	NETWORK	SECURIT	Y	ADVANCED	
E	ACKET FILTERI	NG   FIRE	WALL   CERTIF	ICATE   HELP						
	MAC	Filtering	Y	Incom	ing IP Filtering	L	Ou	tgoing IP Fill	ering	
OL	TGOING	IP FILT	ERING							
Out By c or R	Outgoing IP Filtering Setup By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be <b>BLOCKED</b> by setting up filters. Choose Add or Remove to configure outgoing IP filters.									
	Filter Name	Protocol	Source Addr	ess / Mask	Source Port	Dest. Addres	ss / Mask	Dest. Port	Remove	
	Tester	TCP/UDP	192.168.1.7 / 2	55.255.255.0	675	24.67.5.2 / 25	5.255.255.0			
	Tester         TCP/UDP         192.168.1.7 / 255.255.255.0         675         24.67.5.2 / 255.255.255.0         Image: Comparison of the second									

# **Enabling the Filtering Function**

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

cisco		TRA I D					520
PACKET FILTERING	SYS	NALL   C	DSL CERTIFICATE   HELP	HOME NETWO	RK SECU	RITY	ADVANCED
MAC F	iltering		Incomi	ng IP Filtering	Y	Outgoing I	P Filtering
MAC FILTER							
Enable Filtering     MAC Filtering Glob     Choose Add or Ren	g Function al Policy: nove to co	FORWAR	DED Ch:	ange Policy			
	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			

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



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

### Adding an Outgoing IP Filter

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

cisco	SVS	TEM		HOME NETWO		PITY	ADVANCED
PACKET FILTERING	B   FIRE	WALL   C	ERTIFICATE   HELI				ABTATIOLD
MAC F	iltering ING		Incom	ing IP Filtering	Y	Outgoing	IP Filtering
MAC Filtering is on be FORWARDED e layer frames will be Enable Filtering	ly effective except tho BLOCKE	on ATM F se matchir D except t	PVCs configured in ng with any of the s hose matching with	Bridge mode. FORV pecified rules in the in any of the specified	VARDED means t following table. <mark>BL</mark> I rules in the follow	hat all MA . <mark>OCKED</mark> n ring table.	C layer frames will neans that all MAC
MAC Filtering Glob	al Policy: nove to co	nfigure M4	CH	ange Policy			
	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			

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



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

	SYSTEM		HOME NETWORK	SECURITY	ADVANCED
MAC Filte	ring	Incomin	g IP Filtering	Outgoing	IP Filtering
Add IP Filter	Outgoing				
condition below. All of	the specified cond	itions in this filter ru	le must he satisfied for th	he rule to take effect	Click 'Save/Annly'
condition below. All of to save and activate th Filter Name:	the specified cond le filter.	itions in this filter ru	le must be satisfied for th	ne rule to take effect.	Click 'Save/Apply'
condition below. All of to save and activate th Filter Name: Protocol:	the specified cond e filter.	itions in this filter ru	le must be satisfied for th	ne rule to take effect.	Click 'Save/Apply'
condition below. All of to save and activate th Filter Name: Protocol: Source IP address: Source Subsot Mack:	the specified cond le filter.	itions in this filter ru	le must be satisfied for th	ne rule to take effect. ∖	Click 'Save/Apply'
condition below. All of Filter Name: Protocol: Source IP address: Source Subnet Mask: Source Subnet Mask:	the specified cond e filter.	itions in this filter ru	le must be satisfied for th	e rule to take effect.	Click 'Save/Apply'
condition below. All of Filter Name: Protocol: Source IP address: Source Subnet Mask: Source Port (port or pr Destination IP address)	the specified cond e filter.	itions in this filter ru	le must be satisfied for th	e rule to take effect.	Click 'Save/Apply'
condition below. All of Filter Name: Protocol: Source IP address: Source Subnet Mask: Source Port (port or pr Destination IP address) Destination Subnet Mi	the specified cond ie filter.	itions in this filter ru	le must be satisfied for th	e rule to take effect.	Click 'Save/Apply'
condition below. All of Filter Name: Protocol: Source IP address: Source Subnet Mask: Source Port (port or pr Destination IP address Destination Subnet Mi Destination Subnet Mi	the specified cond ine filter.	itions in this filter ru	le must be satisfied for th	e rule to take effect.	Click 'Save/Apply'
condition below. All of Filter Name: Protocol: Source IP address: Source Subnet Mask: Source Port (port or pr Destination IP address Destination Subnet M. Destination Port (port	the specified cond ine filter.	itions in this filter ru	le must be satisfied for th	e rule to take effect.	Click '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.

cisco	SYST	EM	DSL			RITY	ADVANCED
	E   FIRE	VALL   C	CERTIFICATE   HELI	2			
MAC F	iltering		Incom	ing IP Filtering		Outgoing I	P Filtering
MAC ETL TER	ING						
MAG FIETER.							
MAC Filtering is on be FORWARDED e layer frames will be Enable Filtering MAC Filtering Glob	ly effective except tho: BLOCKE g Function al Policy:	on AIM H se matchir D except t FORWAR	-VCs configured in ng with any of the s hose matching with DED	Bridge mode. FORV pecified rules in the to a any of the specified	VARDED means t following table. <mark>BL</mark> I rules in the follow	hat all MA/ .OCKED m ving table.	C layer frames will eans that all MAC
			CH	ange Policy			
Choose Add or Rer	nove to co	nfigure M4	AC 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		
	A		Add	Remove			

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



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

# **Parental Control Setup - Filtering Function**

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

**Path**: Security >Firewall > Parental Control



## Adding Time of Day Restrictions

The 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.