DDR2200 Series
Residential Gateway
Installation and Operation Guide

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

HPNA is a trademark of the Home Phoneline Networking Alliance.

The Wi-Fi Protected Setup mark is a mark of the Wi-Fi Alliance. Wi-Fi Protected Setup is a trademark of the Wi-Fi Alliance.

Other third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Disclaimer

The maximum performance for wireless is derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

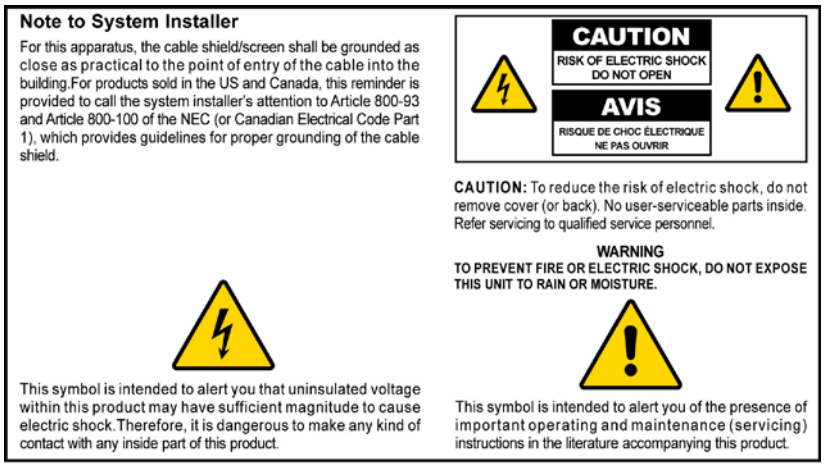
Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing **or** later issued patent.

Copyright

Notice to Installers

The servicing instructions in this notice are for use by qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions, unless you are qualified to do so.



Notice à l'attention des installateurs de réseaux câblés

Les instructions relatives aux interventions d'entretien, fournies dans la présente notice, s'adressent exclusivement au personnel technique qualifié. Pour réduire les risques de chocs électriques, n'effectuer aucune intervention autre que celles décrites dans le mode d'emploi et les instructions relatives au fonctionnement, à moins que vous ne soyez qualifié pour ce faire.

Mitteilung für CATV-Techniker

Die in dieser Mitteilung aufgeführten Wartungsanweisungen sind ausschließlich für qualifiziertes Fachpersonal bestimmt. Um die Gefahr eines elektrischen Schlags zu reduzieren, sollten Sie keine Wartungsarbeiten durchführen, die nicht ausdrücklich in der Bedienungsanleitung aufgeführt sind, außer Sie sind zur Durchführung solcher Arbeiten qualifiziert.

Mitteilung an den Systemtechniker

Für dieses Gerät muss der Kabelschutz/Schirm so nahe wie möglich am Eintrittspunkt des Kabels in das Gebäude geerdet werden. Dieser Erinnerungshinweis liegt den in den USA oder Kanada verkauften Produkten bei.Er soll den Systemtechniker auf Paragraph 800-93 und Paragraph 800-100 der US-Elektrovorschrift NEC (oder der kanadischen Elektrovorschrift Canadian Electrical Code Teil 1) aufmerksam machen, in denen die Richtlinien für die ordnungsgemäße Erdung des Kabelschirms festgehalten sind.

Dieses Symbol weist den Benutzer auf das Vorhandensein von nicht isolierten gefährlichen Spannungen im Gerät hin, die Stromschläge verursachen können. Ein Kontakt mit den internen Teilen dieses Produktes ist mit Gefahren verbunden.

ACHTUNG: Zur Vermeidung eines Stromschlags darf die Abdeckung (bzw. die Geräterückwand) nicht entfernt werden. Das Gerät enthält keine vom Benutzer wartbaren Teile. Wartungsarbeiten dürfen nur von qualifiziertem Fachpersonal durchgeführt werden.

WARNUNG

DAS GERÄT NICHT REGEN ODER FEUCHTIGKEIT AUSSETZEN, UM STROMSCHLAG ODER DURCH EINEN KURZSCHLUSS VERURSACHTEN BRAND ZU VERMEIDEN.

Dieses Symbol weist den Benutzer darauf hin, dass die mit diesem Produkt gelieferte Dokumentation wichtige Betriebs- und Wartungsanweisungen für das Gerät enthält.

Aviso a los instaladores de sistemas CATV

Las instrucciones de reparación contenidas en el presente aviso son para uso exclusivo por parte de personal de mantenimiento cualificado. Con el fin de reducir el riesgo de descarga eléctrica, no realice ninguna otra operación de reparación distinta a las contenidas en las instrucciones de funcionamiento, a menos que posea la cualificación necesaria para hacerlo.

Nota para el instalador del sistema

En lo que se refiere a este aparato, el blindaje del cable debe conectarse a tierra lo más cerca posible al punto por el cual el cable entra en el edificio. En el caso de los productos vendidos en los EE. UU. y Canadá, el presente aviso se suministra para llamar la atención del instalador del sistema sobre los Artículos 800-93 y 800-100 del NEC (o Código Eléctrico de Canadá, Parte 1), que proporcionan directrices para una correcta conexión a tierra del blindaje del cable.

Este símbolo tiene como fin advertirle de que una tensión sin aislamiento en el interior de este producto podría ser de una magnitud suficiente como para provocar una descarga eléctrica. Por consiguiente, resulta peligroso realizar cualquier tipo de contacto con alguno de los componentes internos de este producto.

ATENCIÓN: con el fin de reducir el riesgo de descarga eléctrica, no retire la tapa (ni la parte posterior). No existen en el interior componentes que puedan ser reparados por el usuario. Encargue su revisión a personal de mantenimiento cualificado.

ADVERTENCIA

PARA EVITAR EL RIESGO DE INCENDIO O DESCARGA ELÉCTRICA, NO EXPONGA LA UNIDAD A LA LLUVIA O A LA HUMEDAD.

Este símbolo tiene como fin alertarle de la presencia de importantes instrucciones de operación y mantenimiento (revisión) contenidas en la literatura que acompaña al producto.

Contents

IMPORTANT SAFETY INSTRUCTIONS

1) Read these instructions.
2) Keep these instructions.
3) Heed all warnings.
4) Follow all instructions.
5) Do not use this apparatus near water.
6) Clean only with dry cloth.
7) Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8) Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9) Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding-type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10) Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11) Only use attachments/accessories specified by the manufacturer.
12)  Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.
13) Unplug this apparatus during lightning storms or when unused for long periods of time.
14) Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as a power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.

Power Source Warning

A label on this product indicates the correct power source for this product. Operate this product only from an electrical outlet with the voltage and frequency indicated on the product label. If you are uncertain of the type of power supply to your home or business, consult your service provider or your local power company.

The AC inlet on the unit must remain accessible and operable at all times.

Ground the Product

WARNING: Avoid electric shock and fire hazard! If this product connects to coaxial cable wiring, be sure the cable system is grounded (earthed). Grounding provides some protection against voltage surges and built-up static charges.

Protect the Product from Lightning

In addition to disconnecting the AC power from the wall outlet, disconnect the signal inputs.

Verify the Power Source from the On/Off Power Light

When the on/off power light is not illuminated, the apparatus may still be connected to the power source. The light may go out when the apparatus is turned off, regardless of whether it is still plugged into an AC power source.

Eliminate AC Mains Overloads

WARNING: Avoid electric shock and fire hazard! Do not overload AC mains, outlets, extension cords, or integral convenience receptacles. For products that require battery power or other power sources to operate them, refer to the operating instructions for those products.

Provide Ventilation and Select a Location

- Remove all packaging material before applying power to the product.
- Do not place this apparatus on a bed, sofa, rug, or similar surface.
- Do not place this apparatus on an unstable surface.
- Do not install this apparatus in an enclosure, such as a bookcase or rack, unless the installation provides proper ventilation.
- Do not place entertainment devices (such as VCRs or DVDs), lamps, books, vases with liquids, or other objects on top of this product.
- Do not block ventilation openings.

Protect from Exposure to Moisture and Foreign Objects

WARNING: Avoid electric shock and fire hazard! Do not expose this product to dripping or splashing liquids, rain, or moisture. Objects filled with liquids, such as vases, should not be placed on this apparatus.

WARNING: Avoid electric shock and fire hazard! Unplug this product before cleaning. Do not use a liquid cleaner or an aerosol cleaner. Do not use a magnetic/static cleaning device (dust remover) to clean this product.

WARNING: Avoid electric shock and fire hazard! Never push objects through the openings in this product. Foreign objects can cause electrical shorts that can result in electric shock or fire.

Service Warnings

WARNING: Avoid electric shock! Do not open the cover of this product. Opening or removing the cover may expose you to dangerous voltages. If you open the cover, your warranty will be void. This product contains no user-serviceable parts.

Check Product Safety

Upon completion of any service or repairs to this product, the service technician must perform safety checks to determine that this product is in proper operating condition.

Protect the Product When Moving It

Always disconnect the power source when moving the apparatus or connecting or disconnecting cables.

Telephone Equipment Notice

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric stock and injury to persons, including the following:

1. Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.

2. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

3. Do not use the telephone to report a gas leak in the vicinity of the leak.

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

SAVE THESE INSTRUCTIONS

20090915_Modem No Battery_Safety

United States FCC Compliance

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against such interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment OFF and ON, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the service provider or an experienced radio/television technician for help.

Any changes or modifications not expressly approved by Cisco Systems, Inc., could void the user's authority to operate the equipment.

The information shown in the FCC Declaration of Conformity paragraph below is a requirement of the FCC and is intended to supply you with information regarding the FCC approval of this device. *The phone numbers listed are for FCC-related questions only and not intended for questions regarding the connection or operation for this device. Please contact your service provider for any questions you may have regarding the operation or installation of this device.*

FC Declaration of Conformity

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: 1) the device may not cause harmful interference, and 2) the device must accept any interference received, including interference that may cause undesired operation.

DDR2200 Residential Gateway
Model(s): DDR2200
Manufactured by:
Cisco Systems, Inc.
5030 Sugarloaf Parkway
Lawrenceville, Georgia 30044 USA
Telephone: 678-277-1120

Canada EMI Regulation

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la class B est conforme à la norme NMB-003 du Canada.

FCC Part 68

The Federal Communications Commission (FCC) of the United States restricts specific uses of modems, and places registration responsibilities on both the manufacturer and the individual user.

1. The modem may not be connected to a party line or to a coin-operated telephone.
2. Notification to the telephone company is no longer required prior to connecting registered equipment, but upon request from the telephone company, the user shall tell the telephone company which line the equipment is connected to as well as the registration number and ringer equivalence number of the registered protective circuitry. FCC information is printed on a label on the bottom of the modem.

This equipment complies with Part 68 of FCC Rules and the requirements adopted by the ACTA. On the base unit of this equipment is a label that contains, among other information, a product identifier in the format US: US:GEMDL01BDDR2200. If requested, this number must be provided to the telephone company.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. If advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, please contact the service provider for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

IC (Industry Canada) Notice

Notice: The Industry Canada (formerly Canadian Department of Communications) label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements. The department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single-line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user may give the telecommunications company cause to request the user to disconnect the equipment. Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION:

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

RF Exposure Statements

Note: This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 7.9 inches (20 cm) between the radiator and your body.

US

This system has been evaluated for RF exposure for humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based in accordance with FCC OET Bulletin 65C rev 01.01 in compliance with Part 2.1091 and Part 15.27. The minimum separation distance from the antenna to general bystander is 7.9 inches (20 cm) to maintain compliance.

Canada

This system has been evaluated for RF exposure for humans in reference to Canada Health Code 6 (2009) limits. The evaluation was based on evaluation per RSS-102 Rev 4. The minimum separation distance from the antenna to general bystander is 7.9 inches (20 cm) to maintain compliance.

EU

This system has been evaluated for RF exposure for humans in reference to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The evaluation was based on the EN 50385 Product Standard to Demonstrate Compliance of Radio Base Stations and Fixed Terminals for Wireless Telecommunications Systems with basic restrictions or reference levels related to Human Exposure to Radio Frequency Electromagnetic Fields from 300 MHz to 40 GHz. The minimum separation distance from the antenna to general bystander is 20 cm (7.9 inches).

Australia

This system has been evaluated for RF exposure for humans as referenced in the Australian Radiation Protection standard and has been evaluated to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The minimum separation distance from the antenna to general bystander is 20 cm (7.9 inches).

20091016 FCC DSL_Dom and Intl

CE Compliance

Declaration of Conformity with Regard to the EU Directive 1999/5/EC (R&TTE Directive)

This declaration is only valid for configurations (combinations of software, firmware and hardware) supported or provided by Cisco Systems for use within the EU. The use of software or firmware not supported or provided by Cisco Systems may result in the equipment no longer being compliant with the regulatory requirements.

Български [Bulgarian]	Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/EC.
Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Română [Romanian]	Acest echipament este in conformitate cu cerintele esentiale si cu alte prevederi relevante ale Directivei 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

Note: The full declaration of conformity for this product can be found in the Declarations of Conformity and Regulatory Information section of the appropriate product hardware installation guide, which is available on Cisco.com.

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 300 328
- EMC: EN 301 489-1 and EN 301 489-17
- Safety: EN 60950 and EN 50385

The CE mark and class-2 identifier are affixed to the product and its packaging. This product conforms to the following European directives:

 -1999/5/EC

National Restrictions

This product is for indoor use only.

France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483,5 MHz. There are no restrictions when used in other parts of the 2,4 GHz band. Check http://www.arcep.fr/ for more details.

Pour la bande 2,4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483,5 MHz. Il n'y a pas de restrictions pour des utilisations dans d'autres parties de la bande 2,4 GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a “general authorization.” Please check http://www.comunicazioni.it/it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una “Autorizzazione Generale”. Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2,4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: http://www.esd.lv.

Note: The regulatory limits for maximum output power are specified in EIRP. The EIRP level of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

Antennas

Use only the antenna supplied with the product.

20090312 CE_Gateway

About This Guide

Introduction

This installation and operation guide applies to the DDR2200 series residential gateway. The DDR2200 series residential gateway connects to the DSL network in your home to deliver data, video, voice, and wired (Ethernet) or wireless gateway capabilities all from one device. Use this guide to install the residential gateway in your home.

Purpose

This document provides the information you need to install and operate the DDR2200 series residential gateway.

Audience

This guide is written for two audiences. Subscribers who have purchased a residential gateway and want to experience high-speed Internet and high-quality digital telephone service can use this guide for background information and basic operation. This guide is also written for the service provider's installers who initially set up and configure residential gateway in the subscriber's home. Most subscribers will not want to use the more advanced functionality, and future releases of this software will prevent subscriber access to these screens.

Document Version

This is the first formal release of this document.

1

Introducing the DDR2200 Series Residential Gateway

Introduction

Imagine walking through your home and accessing the Internet from nearly any room. The DDR2200 series residential gateway connects to the DSL line in your home and to your home network to deliver data, video, voice, and wired (Ethernet) or wireless gateway capabilities all from one device. You can use your residential gateway to connect to a variety of devices in the home or small office. The residential gateway supports high-speed data access, VoIP services, and features that support Internet Protocol TV (IPTV) deployment. Use this chapter to learn about your residential gateway.

In This Chapter

Benefits and Features

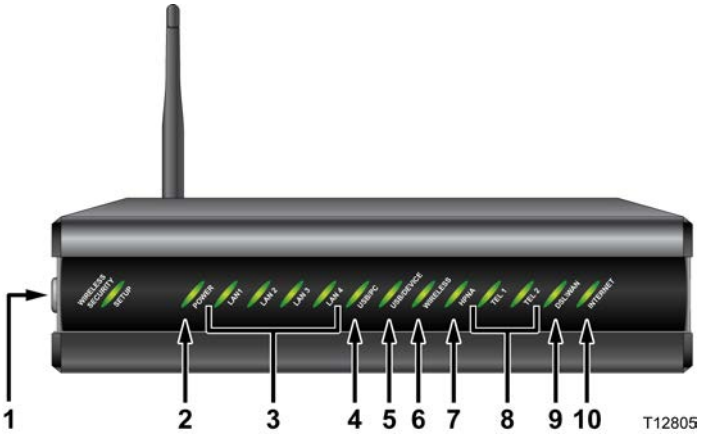
Your residential gateway offers the following benefits and features:

- **Full routing functionality**. The gateway router provides broadband transfer speeds available between your home network and the service provider's network for multi-user sharing. The high-performance router distributes data seamlessly to all devices in the network without a noticeable effect to performance or speed.
- **True firewall capability**. The gateway firewall includes both standard NAT/PAT security and Stateful Packet inspection to defend against external attacks.
- **High-quality data, voice, and IPTV services**. The gateway combines an ADSL2+ bonded modem, 4-port Ethernet switch, Home Phoneline Networking Alliance (HPNA™) 3.0 bridge and router functionality with optional VoIP and Wi-Fi into one integrated platform.
- **Compact design**. The gateway is compact enough to sit on a desktop and versatile enough to be wall mounted in an out of the way location. The residential gateway can also stand vertically.
- **Flexible networking**. The gateway combines a variety of home networking technologies in one box: Ethernet, USB, 802.11g wireless, and HPNA.
  - **Ethernet.** Ethernet is a network standard for data transmission using either coaxial or twisted pair cable over a LAN (local area network). The information can be transmitted at speeds of 10 to 100 Mbps. If the home or office is wired for Ethernet, use one of the four LAN interfaces on the gateway to create a broadband network.
  - **USB**. The USB port allows you to directly connect a computer or other network capable device.
  - **802.11g Wireless**. The gateway includes an integrated wireless access point that allows you to roam wirelessly throughout your home or office. With the high-power wireless technology of the DDR2200, wireless "coldspots" are virtually eliminated in the home.
  - **HPNA.** The HPNA interface allows you to easily share digital services throughout the home using the existing coaxial cable to distribute content such as video, music, and games. HPNA offers the following benefits:
    - Multi-room DVR. Subscribers can record and share digital services simultaneously in every room.
    - Multi-room gaming. Subscribers can access games from various locations in the home and play simultaneously.
    - PC to TV. Subscribers can access data and video services over the HPNA coaxial network throughout the home.

- **ADSL2+**. Asymmetric Digital Subscriber Line (ADSL) provides high-access transmission speeds for delivery of video, voice, and data services to homes over ordinary copper telephone wire.

What's On the Front Panel?

The front panel of your residential gateway provides LED status indicators that indicate the operational state of your gateway. Refer to the following diagram for a description of the front panel.



1 **wifi-sec**—Allows you to automatically configure the wireless device in the home. The WIRELESS SECURITY SETUP LED shows whether automatic wireless security is on or off

2 **POWER**—Illuminates solid green to indicate that AC power is being applied to the residential gateway

3 **LAN1 - LAN4**—Illuminates solid green to indicate that an Ethernet carrier is present and blinks to indicate that Ethernet data is being transferred between the PC and the residential gateway

4 **USB/PC**—Illuminates solid green to indicate that a USB carrier is present and blinks to indicate that USB data is being transferred between the PC and the residential gateway

5 **USB/DEVICE**—Illuminates solid green to indicate that a USB carrier is present and blinks to indicate that USB data is being transferred between the connected USB device and the residential gateway

6 **WIRELESS**—Illuminates solid green when the wireless access point is enabled and operational and blinks to indicate that wireless data is being transferred between the PC and the residential gateway. The LED is off when the wireless access point is disabled by the user

7 **HPNA**—Illuminates solid when linked to another HPNA device and blinks when HPNA activity occurs

8 **TEL 1 and TEL 2**—TEL 1 illuminates solid green when telephony service is in use. TEL2 illuminates solid green when telephony service is in use.

9 **DSL/WAN**—Indicates whether a DSL signal is acquired (or trained). The LED indicators mean the following status:

- Off. Not trained.
- Blinking. In training.
- Solid. Trained.

In addition, once the DSL/WAN LED is solid, if any pair drops, the DSL/WAN LED will blink differently to provide additional status as follows:

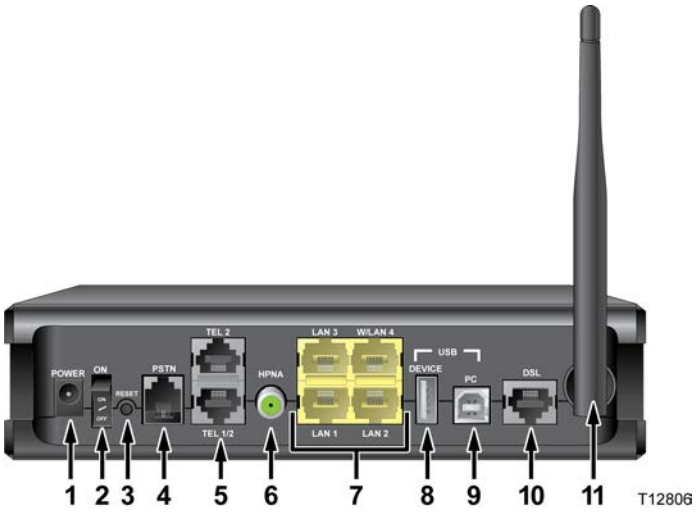
- If the outer pair drops, the LED blinks slowly (about 1 blink every second).
- When the inner pair drops, the LED blinks faster (about 4 blinks every second).

10 **INTERNET**—Indicates wide area network (WAN) traffic. The LED indicators mean the following status:

- Solid. IP is connected.
- Blinking. WAN interface has activity.
- Off. No Internet connection.

What's On the Back Panel?

Refer to the following diagram for a description of the back panel components.



Important! Do not connect your PC to both the Ethernet and USB ports at the same time. Your gateway will not function properly if both the Ethernet and USB ports are connected to your PC at the same time.

1 **POWER**—Connects the residential gateway to the AC power plug that is provided with your residential gateway

2 **On and Off Switch**—Powers the residential gateway on and off

3 **RESET**—Activating this switch resets the residential gateway. Pressing this switch for more than 10 seconds resets the device to factory default values and resets the residential gateway

4 **PSTN**—Connects to the home telephone wiring and is used as a backup to voice over IP (VoIP) service in the event of a power outage to the residential gateway

5 **TEL 1 and TEL 2**—RJ-11 telephone ports connect to home telephone wiring to conventional telephones or fax machines

6 **HPNA**—Connects to the coaxial cable wiring in the house for data and video distribution

7 **LAN 1-LAN 3 W/LAN 4**—Four RJ-45 Ethernet ports connect as follows:

- LAN 1 through 3 connect to the Ethernet port on your PC or your home network
- W/LAN 4 connects to the Ethernet port on your PC if used as a LAN port or optionally as an Ethernet wide area network (WAN) port that connects to the service provider network

8 **USB DEVICE**—12 Mbps USB port connects to the USB port on your device such as a flash drive or digital camera

9 **USB PC**—12 Mbps USB port connects to the USB port on your PC

10 **DSL**—RJ-11 port connects to the DSL line from the service provider

11 **ANTENNA**—Receives and transmits data packets to wireless devices

2

Installing the Residential Gateway

You can install the residential gateway in your home office and access the Internet from your kitchen computer to get your favorite recipe. Use this chapter to properly install your residential gateway and to connect the residential gateway to your computer and other devices in your home.

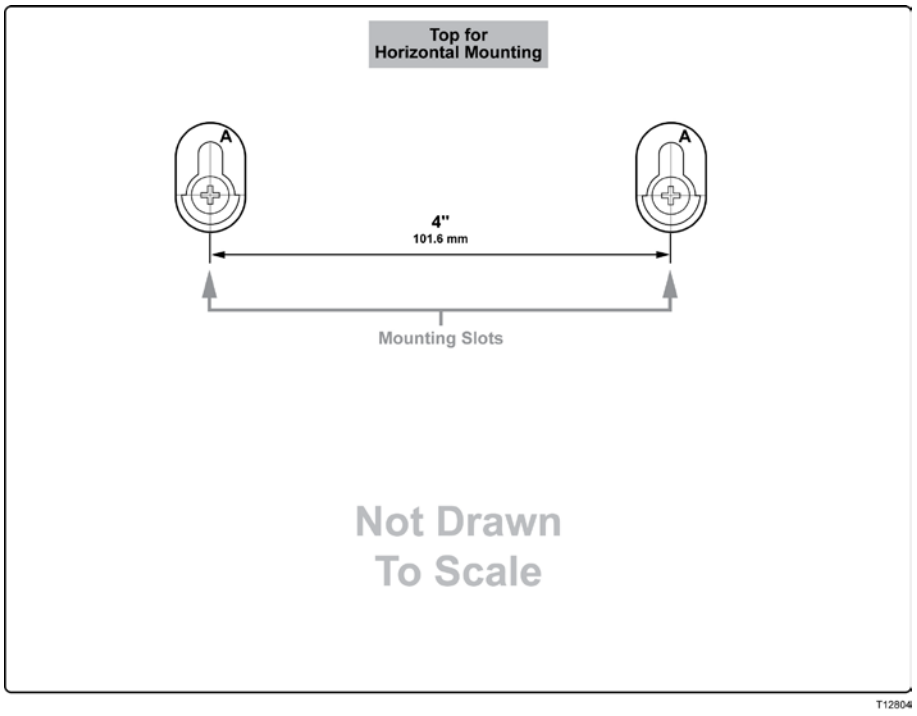
In This Chapter

Mounting the Residential Gateway Vertically

Some installations may require that you place the residential gateway in a vertical position. Use proper care when installing the residential gateway in a vertical position. Be sure that the housing of the residential gateway is vertical and that the stand is extended as shown in the following illustration:

Mounting the Residential Gateway to the Wall

The following illustration shows the location and dimensions of the wall-mounting slots on the bottom of the residential gateway. Use the information on this page as a guide for mounting your residential gateway to the wall.



Connecting Your Computer to the Residential Gateway

You can connect a computer to the residential gateway using one of the following methods:

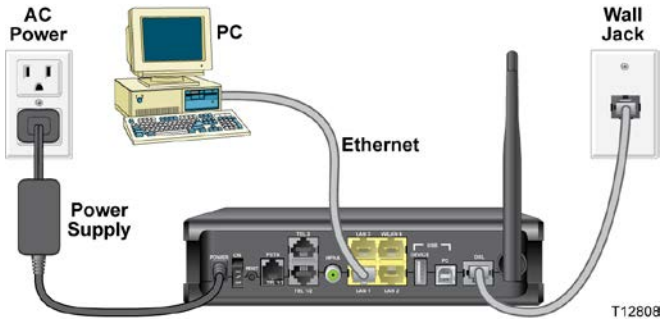
- Ethernet Connection
- Wireless Connection

Note: These instructions describe a PC connection. You could also connect another type of device with a wireless interface. See the owner's manual that came with the device for instructions.

Connecting the Computer with an Ethernet Connection

Complete these steps to connect the computer with an Ethernet connection.

1. Connect the power adapter that came with the residential gateway to the POWER port on the residential gateway and to an electrical outlet.
2. Power on the residential gateway. After the residential gateway has completed its startup process, the POWER LED on the front panel of the residential gateway should be green.
3. Connect the Ethernet cable provided with the residential gateway from any available Ethernet port (LAN 1 through LAN 4) on the gateway to the Ethernet port on the computer.
4. Connect the gray cable provided with the residential gateway from the DSL port on the gateway to a telephone wall jack. See ***Connecting the DSL Interface*** (on page 14) for more information.



Connecting the Computer with a Wireless Connection

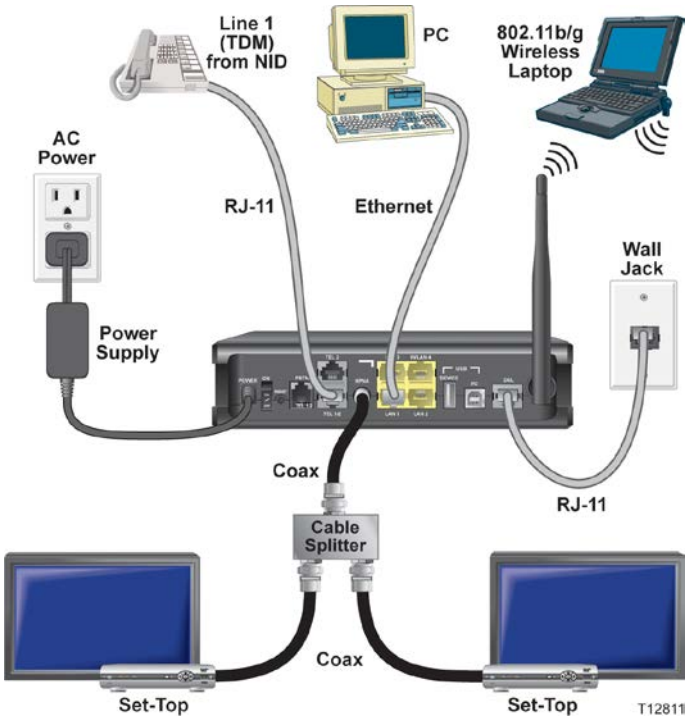
A wireless connection requires a wireless-enabled notebook or a computer with an 802.11b/g wireless network adapter installed.

Complete these steps to connect the computer with a wireless connection.

1. Connect the power adapter that came with the residential gateway to the POWER port on the residential gateway and to an electrical outlet.
2. Power on the residential gateway. After the residential gateway has completed its startup process, the POWER light on the front panel of the residential gateway should be green.
3. Connect the gray cable provided with the residential gateway from the DSL port on the residential gateway to a telephone wall jack. See ***Connecting the DSL Interface*** (on page 14) for more information.
4. Follow the instructions in your owner's manual for your PC or laptop to activate the wireless connection.

Connecting the DSL Interface

Now that you have connected the gateway to power and you have made the LAN connections, you can connect the DSL interface (connection to the wall jack) as shown in the following illustration. This illustration shows all of the attached devices connected to the residential gateway.



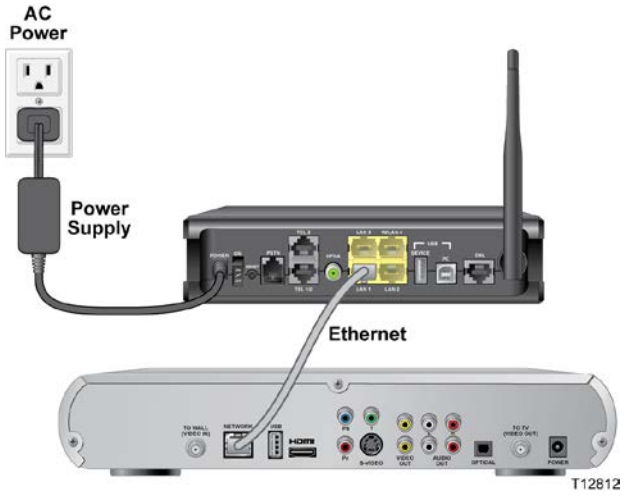
Connecting an IP Set-Top to the Gateway

For IPTV service, you must connect the residential gateway to an IP set-top. You can connect to an IP set-top using an Ethernet or coaxial connection.

Ethernet Connection

Complete the following steps to connect the residential gateway to an IP set-top through Ethernet for IPTV service.

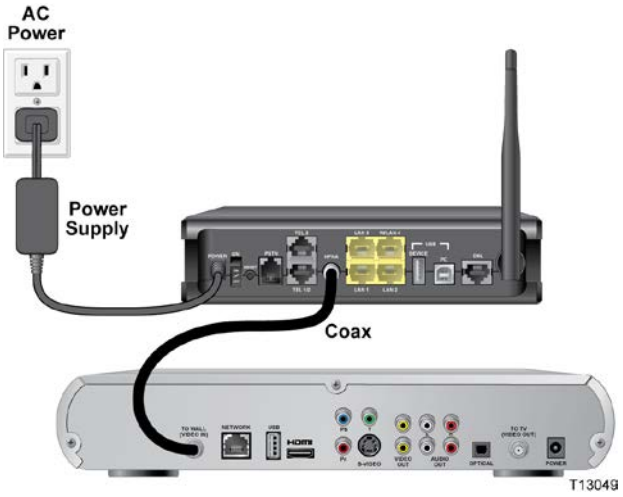
1. Ensure that the residential gateway is powered on.
2. Connect an Ethernet cable from the Ethernet port (LAN 1 through LAN 4) on the gateway to the Network port on the set-top.
3. Power on the IP set-top.



Coaxial Connection

Complete the following steps to connect the residential gateway to an IP set-top with coaxial cable for IPTV service.

1. Ensure that the residential gateway is powered on.
2. Connect a coaxial cable from the HPNA port on the gateway to the TO WALL (Video In) port on the set-top.
3. Power on the IP set-top.



3

Configuration and Operation

The DDR2200 residential gateway contains web pages that show the current status of the residential gateway and that allow you to configure the device. Advanced users can configure parameters such as DHCP (Dynamic Host Configuration Protocol), wireless network settings, port forwarding, parental control, and so forth. This section provides information that you can use to configure and interact with the residential gateway through the user interface. The screens shown in this guide represent the default values for the device.

Use this chapter to help you check the status of the residential gateway and to configure the device.

In This Chapter

Logging In to the Residential Gateway

The default configuration of the residential gateway uses IP address 192.168.1.254. If you have connected the residential gateway correctly and you have properly configured your computer, use the following steps to log in to the residential gateway as an administrator.

Note: A non-administrative user may need a different user name and password for logging in to the residential gateway. These users can access non-privileged information.

1. On your PC, open the web browser that you prefer to use.
2. In the address field, enter the following IP address: 192.168.1.254. The system prompts you to enter your user name and password.

3 Enter **admin** for the user name and **admin** for the password. The residential gateway opens with the System Summary page in the forefront.

You can use this web interface to check the status of the residential gateway and to configure parameters.

Note: The screens shown in this guide represent the default values for the device.

System Summary

The System Summary screen provides a summary of the software used by the residential gateway and indicates the current status of the DSL connection. You can use this screen to find hardware and software information as well as physical and IP layer information.

This screen also provides a link to the Setup Wizard. The Setup Wizard is a step-by-step sequence to set up your residential gateway for the first time to ensure proper operation.

The Log Out button on this screen allows you to quickly log out and log back in without opening a browser.

Path: System > Summary

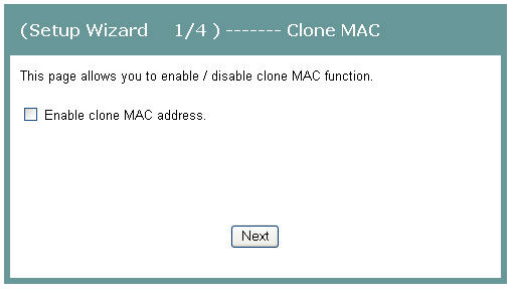
Setting Up Your System with the Setup Wizard

The Setup Wizard is a step-by-step sequence to set up your residential gateway for the first time to ensure proper operation. The wizard combines the various tasks into one convenient tool to reduce configuration time. The wizard requires that you make a few selections within this process. Your selections will depend on your service provider.

To set up your system with the Setup Wizard, complete the following steps.

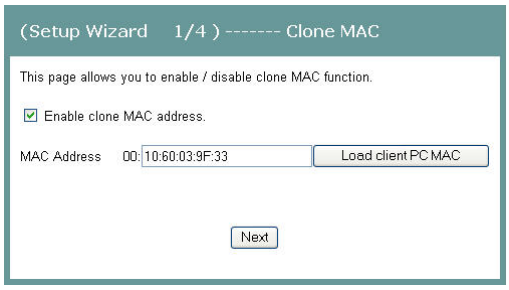
1 Click **System** on the main screen. The System Summary window opens.

2 Click **Setup Wizard** at the top of the screen. The (Setup Wizard 1/4) ------ Clone MAC screen opens.



3 Do you want to enable the clone MAC function? MAC cloning enables you to change the MAC address of the residential gateway to match the MAC address of your PC or any service provider supplied MAC address. If you do not enable MAC cloning, the default MAC address of the residential gateway is used.

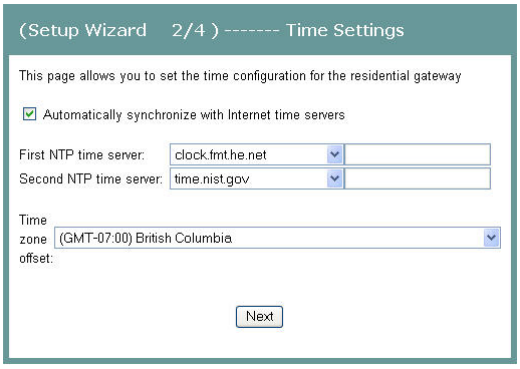
- If **yes**, select the Enable clone MAC address check box. A field appears for you to enter the MAC address you want to clone. Go to step 4.



- If **no**, clear the Enable clone MAC address check box. Go to step 5.

4 In the MAC address field, type in a MAC address or click **Load client PCMAC** to load your PC's MAC address.

5 Click **Next**. The (Setup Wizard 2/4 ------- Time Settings) screen opens. This screen lets you synchronize the time on the residential gateway with an Internet time server. If you do not synchronize the time with an Internet time server, the residential gateway will use its default time.



6 Do you want to automatically synchronize the time on the residential gateway with an Internet Time server?

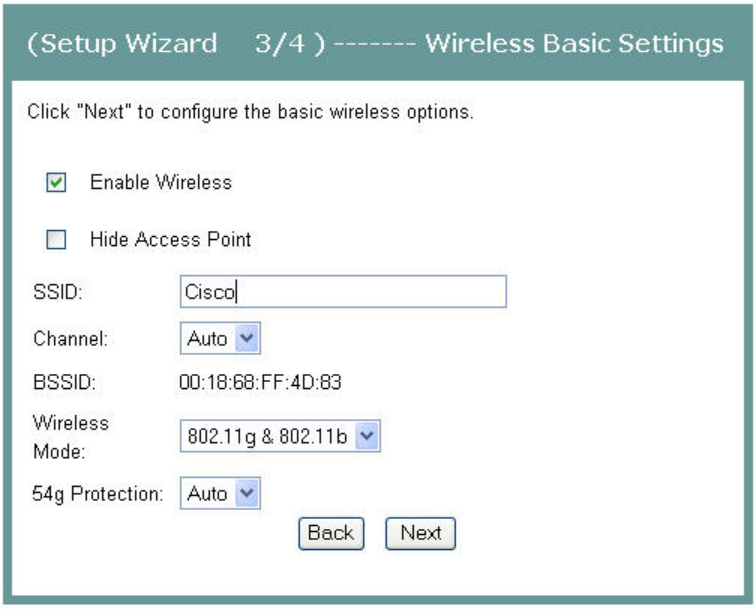
- If **yes**, check the Automatically synchronize with Internet time servers check box. Go to step 7.
- If **no**, clear the Automatically synchronize with Internet time servers check box. The residential gateway will get its time from its own internal clock. Go to step 9.

7 In the First NTP time server field, select the Network Time Protocol (NTP) time server from the drop-down list that you want the residential gateway to check first to get its time.

8 In the Second NTP time server field, select the time server from the drop-down list that you want to use as a backup server for the residential gateway to get its time.

9 In the Time zone offset field, select your time zone from the drop-down list.

10 Click **Next**. The (Setup Wizard 3/4) ------- Wireless Basic Settings screen opens. The residential gateway offers wireless capability by default. This screen allows you to configure the wireless settings to work with the devices in your environment.



11 Do you want to enable wireless?

- If **yes**, check the Enable Wireless check box.
- If **no**, clear the Enable Wireless check box. The wireless capability of the residential gateway is disabled, and all devices communicating with the residential gateway will have to be hard wired.

12 Do you want to prevent other wireless devices from communicating over the wireless network with the residential gateway?

- If **yes**, select the Hide Access Point check box.
- If **no**, clear the Hide Access Point check box. No devices will be locked out from communicating with the residential gateway over the wireless network.

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

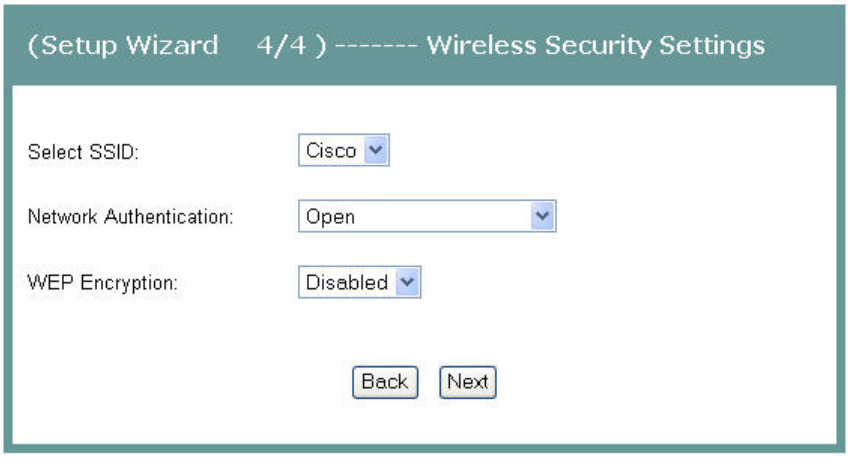
14 In the Channel field, select the channel from the drop-down list to select the frequency that you will use for wireless communication. Values are auto and channels 1 through 11.

15 In the Wireless Mode field, select one of the following modes:

- 802.11g & 802.11b
- 802.11g only
- 802.11b only

16 In the 54g Protection field, select Auto to enable 54g protection or Off to disable the function. The Auto option will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turning the protection off maximizes 802.11g throughput under most conditions.

17 Click **Next.** The (Setup Wizard 4/4) ----- Wireless Security Settings screen opens.



18 In the Select SSID field, select the SSID from the drop-down list that you want to use.

19 In the Network Authentication field, select one of the following authentication methods from the drop-down list:

- 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.
- WPA-PSK (Wi-Fi Protected Access Pre-Shared Key). Your network is secured by encryption of all traffic using a pre-shared dynamic key.

20 Do you want to enable WEP Encryption?

- If **yes**, in the WEP Encryption field, select **Enabled** from the drop-down list.
- If **no**, in the WEP Encryption field, select **Disabled** from the drop-down list.

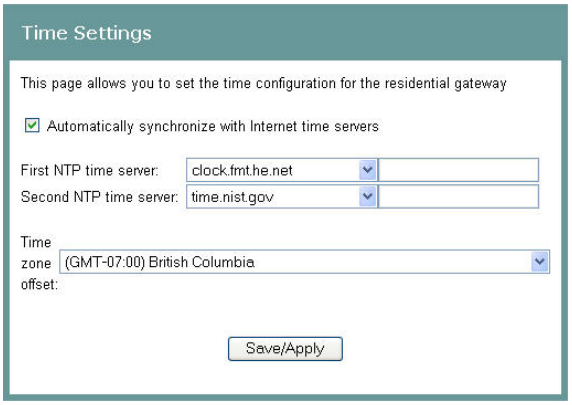
21 Click **Save/Reboot** to save the changes you made. You must reboot the gateway for the changes to take effect.

Setting System Date and Time

When you first set up your system with the wizard, you set your system's date and time. At a later time, you may need to reset the date and time, and you can use the following procedure.

To set the system date and time, complete the following steps.

1. Click **System** on the main screen. The System Summary window opens.
2. Under the Admin section on the screen, click **NTP Server Setting**. The Time Settings screen opens.



3. Make sure the Automatically synchronize with Internet time servers check box is checked.
4. In the First NTP time server field, select **clock.fmt.he.net** from the drop-down list.
5. In the Second NTP time server field, select **time.nist.gov** from the drop-down list.
6. In the Time zone offset field, select the time zone that you want to use from the drop-down list.
7. Click **Save/Apply** to save your settings.

Setting Password

To set the password for the residential gateway, complete the following steps.

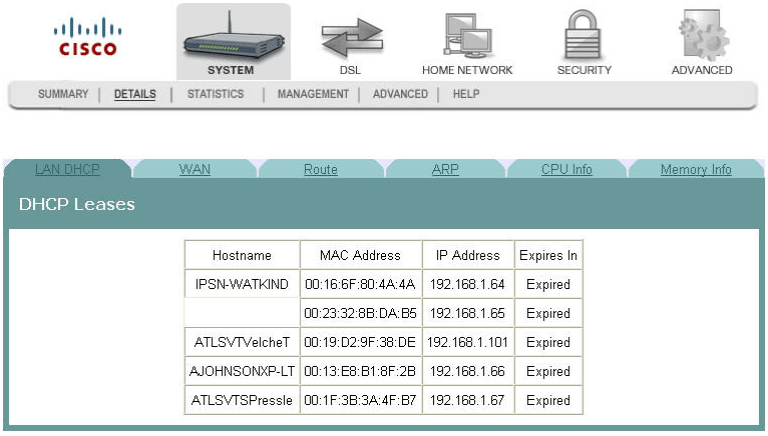
1. Click **System** on the main screen. The System Summary window opens.
2. Under the Admin section on the screen, click **Password Setting**. The Access Control -- Password screen opens.

3. In the Username field, select one of the following options for the user name:
   - admin. Allows unrestricted access to change and view the configuration of the residential gateway. This login allows access to privileged information. The default password for this user name is **admin**.
   - support. Allows an ISP technician to access your residential gateway for maintenance and to run diagnostics. The default password for this user name is **support**.
   - user. Allows access to view configuration settings and statistics, as well as, to update the residential gateway's software. The default password is **user**.
4. In the **Old Password** field, enter the old password you have been using.
5. In the **New Password** field, enter the new password.
6. In the **Confirm Password** field, enter the new password again to confirm it.
7. Click **Save/Apply** to save your user name and password.

DHCP Leases

The DHCP Leases screen displays the Dynamic Host Configuration Protocol (DHCP) table. This screen shows a mapping of hosts (shown by their MAC addresses) and their assigned IP addresses. The DHCP server for the residential gateway assigns these IP addresses to the devices. The screen also shows when the lease for the IP address expires.

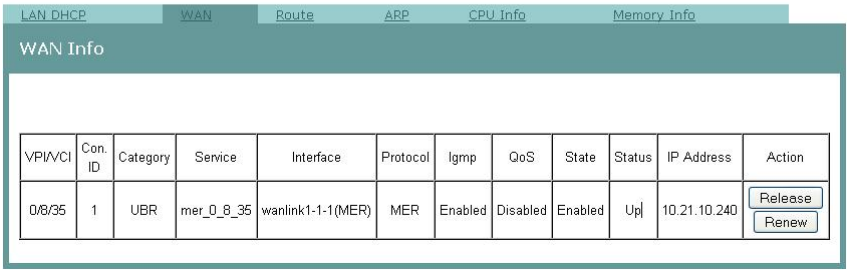
Path: System > Details > LAN DHCP



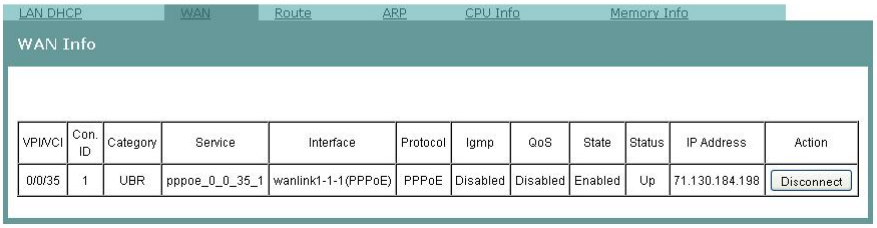
WAN Information

The WAN Info screen provides information about the ADSL2+ wide area network (WAN) parameters and status. You can use this screen to check the ADSL2+ connection.

Path: System > Details > WAN



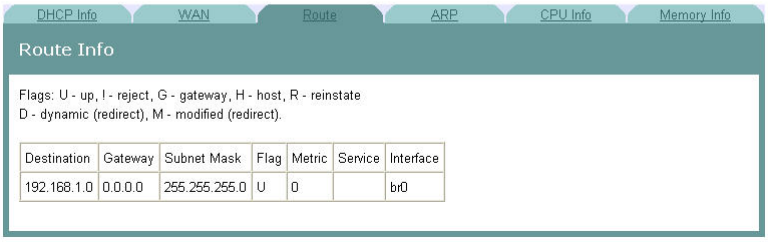
In MER protocol (as shown here), press **Release** or **Renew** to release your current WAN IP address and obtain a new DHCP lease. In PPPoE or PPPoA protocol, press **Connect** to activate a new WAN connection, or press **Disconnect** to disable the connection as shown in the following illustration.



Route Information

The Route Info screen shows the routing table for the residential gateway. This screen provides the gateway address for specific destination IP addresses.

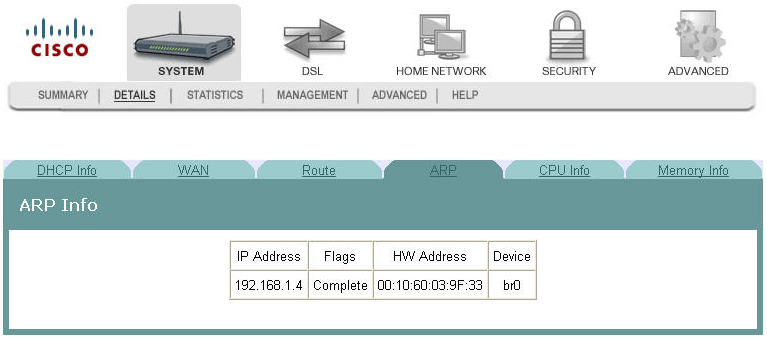
Path: System > Details > Route



ARP Information

The ARP Info screen displays the Address Resolution Protocol (ARP) table. This table shows the IP address to MAC address mapping.

Path: System > Details > ARP



CPU Information

The CPU Info screen shows detailed information about the CPU utilization and the active processes running on the residential gateway.

Path: System > Details > CPU Info

DHCP Info | WAN | Route | ARP | CPU Info | Memory Info

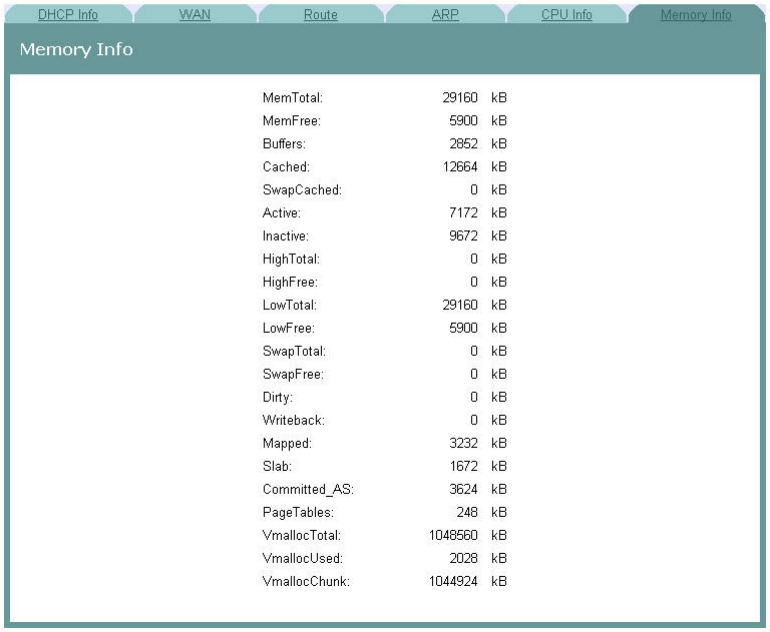
CPU Info

PID	USER	STATUS	RSS	PPID	%CPU	%MEM	COMMAND
1286	admin	running	376	1285	1.9	1.2	exe
2	admin	SWN	0	1	1.9	0.0	ksoftirqd/0
434	admin	sleep	1980	83	0.0	6.7	httpd
83	admin	sleep	1784	44	0.0	6.1	cfm
438	admin	sleep	1776	83	0.0	6.0	cfm
436	admin	sleep	1772	83	0.0	6.0	cfm
370	admin	sleep	1660	83	0.0	5.6	hpnad
371	admin	sleep	1528	83	0.0	5.2	dslled
44	admin	sleep	396	1	0.0	1.3	sh
1	admin	sleep	364	0	0.0	1.2	init
1285	admin	sleep	348	434	0.0	1.1	sh
233	admin	sleep	344	1	0.0	1.1	dhcpd
433	admin	sleep	324	1	0.0	1.1	udhcpd_1
377	admin	sleep	232	1	0.0	0.7	sntp
105	admin	sleep	200	1	0.0	0.6	pvc2684d
28	admin	SW	0	1	0.0	0.0	mtdblockd
4	admin	SW	0	3	0.0	0.0	khelper
202	admin	DW	0	1	0.0	0.0	ra0
5	admin	SW	0	3	0.0	0.0	kblockd/0
6	admin	SW	0	1	0.0	0.0	khubd

Memory Information

The Memory Info screen shows the detailed memory availability of the residential gateway.

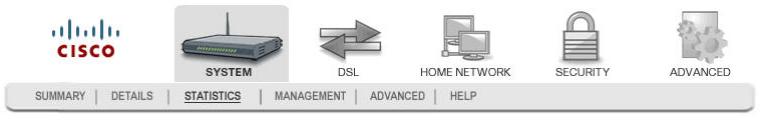
Path: System > Details > Memory Info

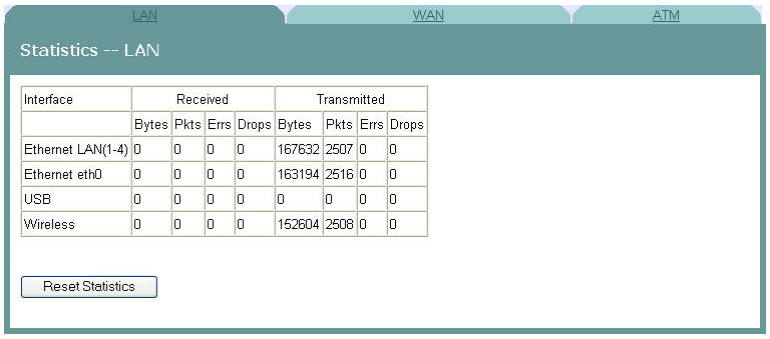


LAN Statistics

The Statistics -- LAN screen displays statistics for the local area network (LAN). This screen shows the number of transmitted and received packets on the LAN interface for Ethernet, USB, and wireless devices.

Path: System > Statistics > LAN





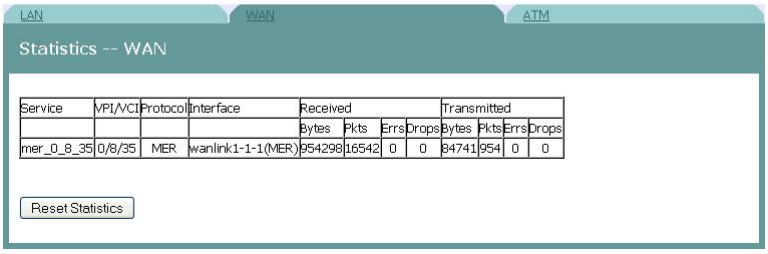
Reset Statistics

To reset the statistics, click **Reset Statistics** on the screen. This action clears the counters and sets them to zero for the packets received and transmitted on the LAN interface.

WAN Statistics

The Statistics -- WAN screen displays statistics for the devices and interfaces on the wide area network (WAN). This screen shows the number of transmitted and received packets for the DSL WAN interface.

Path: System > Statistics > WAN



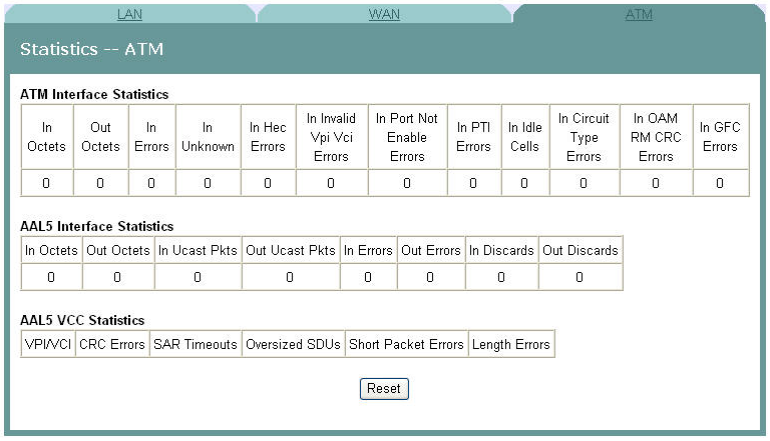
Reset Statistics

To reset the statistics, click **Reset Statistics** on the screen. This action clears the counters and sets them to zero for the packets received and transmitted on the WAN interface.

ATM Statistics

The Statistics -- ATM screen displays statistics on the ATM interface. This screen shows the ATM Layer-2 statistics such as the number of ATM cells transmitted and received over the ATM interface.

Path: System > Statistics > ATM



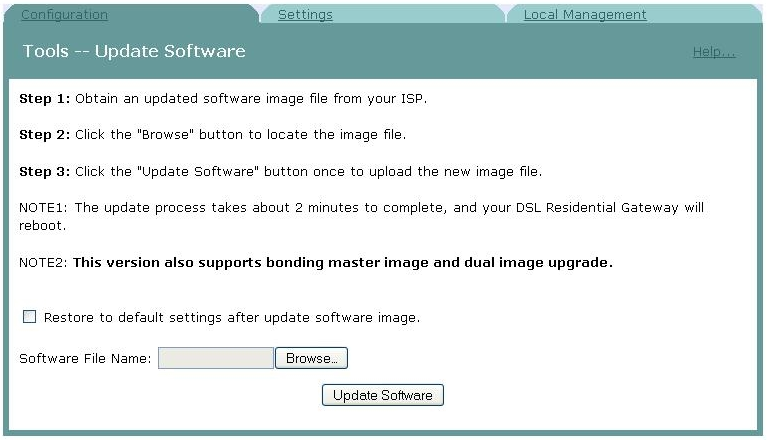
Reset Statistics

To reset the statistics, click **Reset** on the screen. This action clears the counters and sets them to zero for the packets received and transmitted on the ATM interface.

Tools - Update Software

The Tools -- Update Software screen allows you to update the software for the residential gateway with a new version.

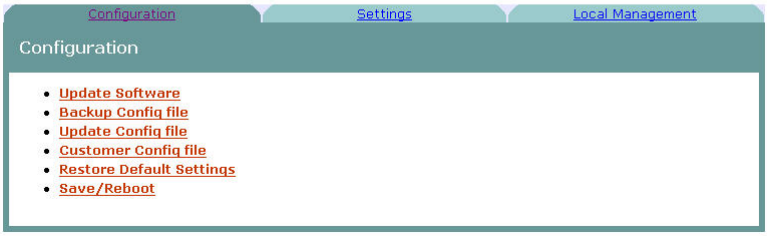
Path: System > Management > Configuration > Update Software



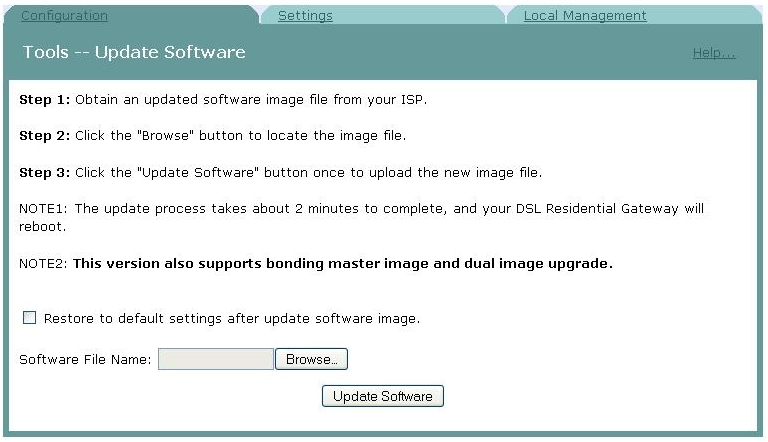
Updating Software

To update the software 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 **Update Software**. The Tools Update Software screen opens.



Note: This screen also gives you the option of uploading the bonding master image or the dual image (master and slave firmware together).

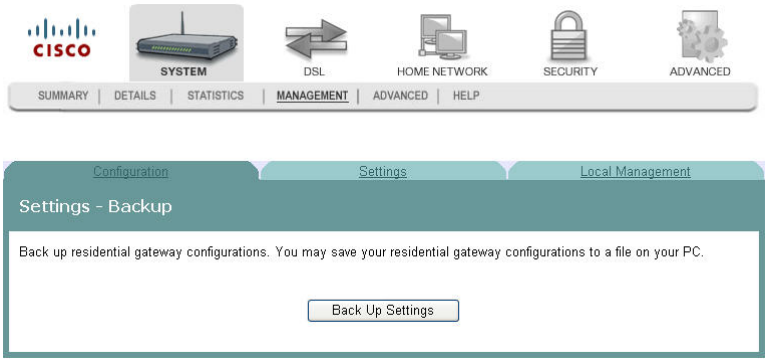
4. In the Software File Name field, click **Browse** to locate the software image file. Then:
   - To restore the residential gateway to factory defaults following the update, check the **Restore to default settings after update software image** option.
   - To retain the current residential configuration following the update, leave this option unchecked.

5 Click **Update Software** to update the software of your residential gateway with the new version. The residential gateway loads the new software and reboots when the software update is complete.

Settings Backup

The Settings - Backup screen allows you to back up the residential gateway configuration and save it to disk.

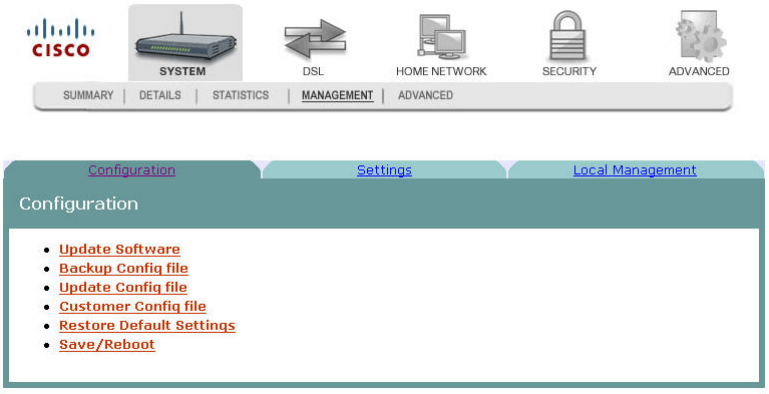
Path: System > Management > Configuration > Back Up Config File



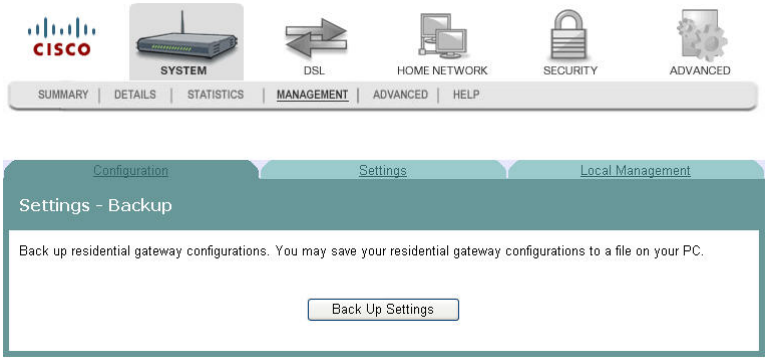
Backing Up Configuration Settings

To back up the configuration settings for the residential gateway, complete the following steps.

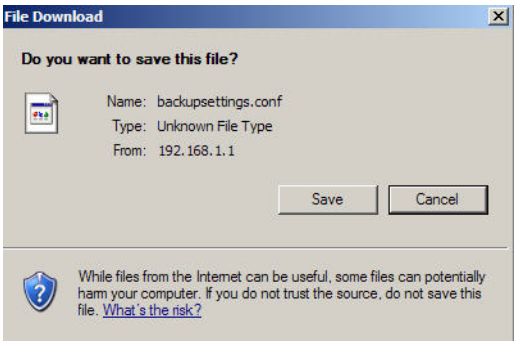
1. Click **System** on the main screen.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



3 Click **Backup Config file**. The Settings - Backup screen opens.



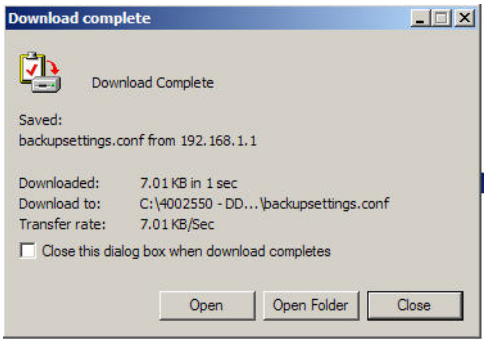
4 Click **Back Up Settings**. The following screen is displayed.



5 Click **Save**. The system prompts you to select a location to store the backup.

6 Select a location and type in a file name.

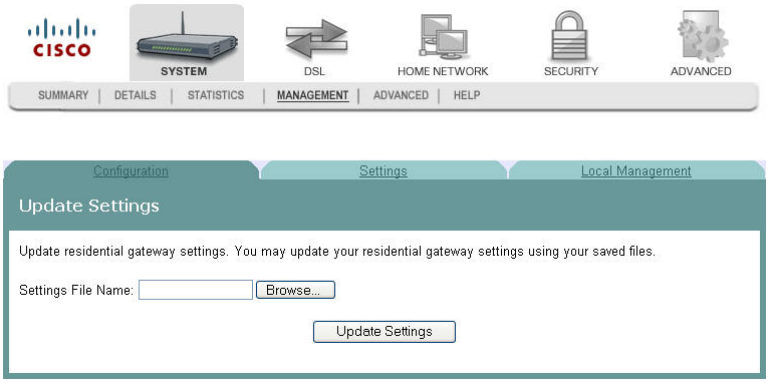
7 Click **Save** to save a backup of the configuration. The system displays a message when the download of the file is complete.



Update Settings

The Update Settings screen allows you to update the settings for the residential gateway from a source file. We recommend that you use this feature if you want to set up multiple residential gateways with a similar configuration.

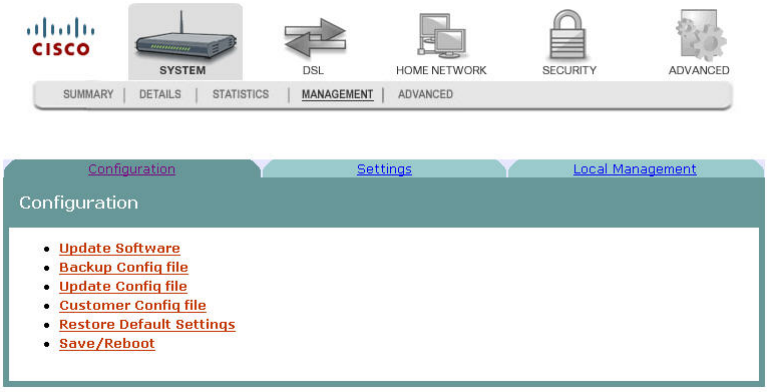
Path: System > Management > Configuration > Update Config File



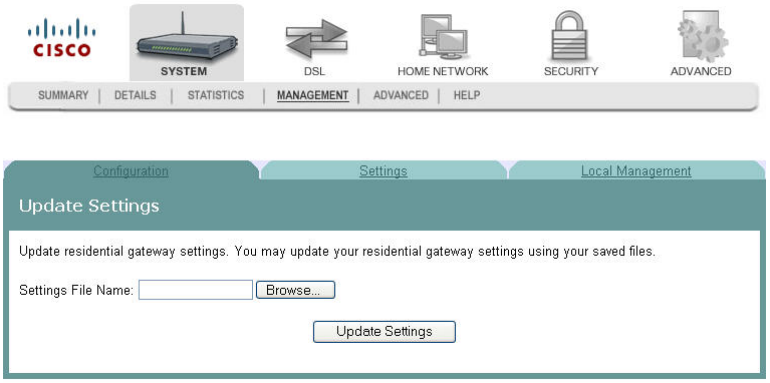
Updating Configuration Settings

To update the configuration settings 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 **Update Config file**. The Update Settings screen opens.



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

5 Click **Update Settings** to update the configuration of the residential gateway.

6 Wait a few minutes while the system reboots the residential gateway. The new configuration takes effect after the residential gateway reboots.

Customer Configuration File

This feature lets you create your own "factory default" configuration so that, when a user presses the Reset button or performs Restore Default Settings from the web UI, the user's device resets to your default settings rather than to the device's original factory default configuration.

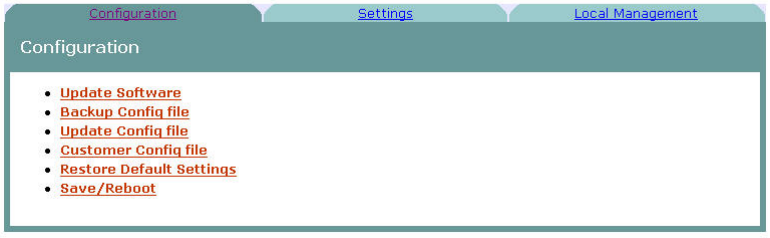
You can use this feature to upload your customized configuration file and make this your own factory default configuration. You also have the option to delete the file.

Note: If you need to revert to the factory default settings, you can press the Restore Default Settings button on the screen or the Reset button on the device. For more information, see ***Restore Default Settings*** (on page 46).

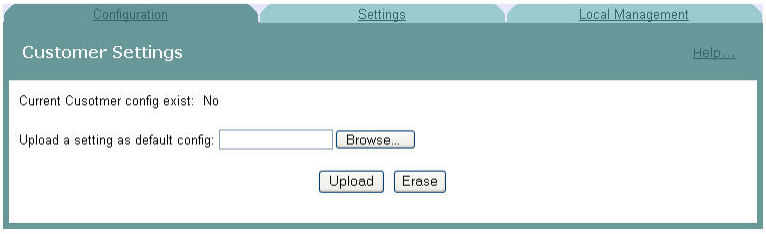
Path: System > Management > Configuration > Update Config File

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

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



3 Click **Customer Config file**. The Customer Settings screen opens.



4 Click **Browse** to select the configuration file that you have previously saved.

5 Click **Upload** to upload your configuration file. You may also delete your uploaded configuration file by pressing the Erase button on the screen.

Notes:

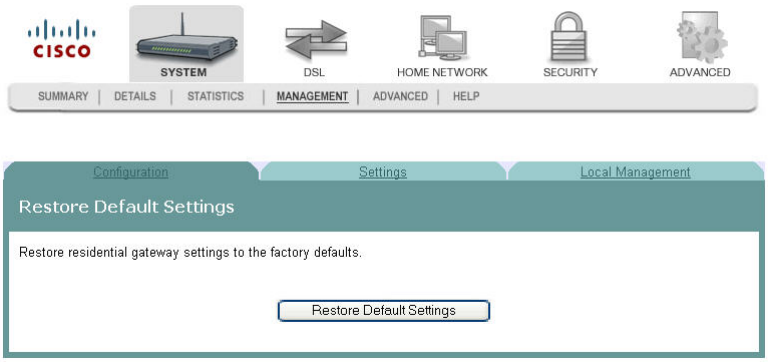
- When you delete your uploaded customer config file by clicking Erase, the system reverts to the device's original factory default settings.
- If the uploaded customer config file exists, the system will reset to the new settings when you click Restore Default Settings in the web UI or press the Reset button on the device.

Restore Default Settings

The Restore Default Settings screen allows you to restore the residential gateway configuration to the default settings.

Note: You can also reset the device by inserting a sharp instrument, such as a paper clip, in the reset area on the back of the residential gateway.

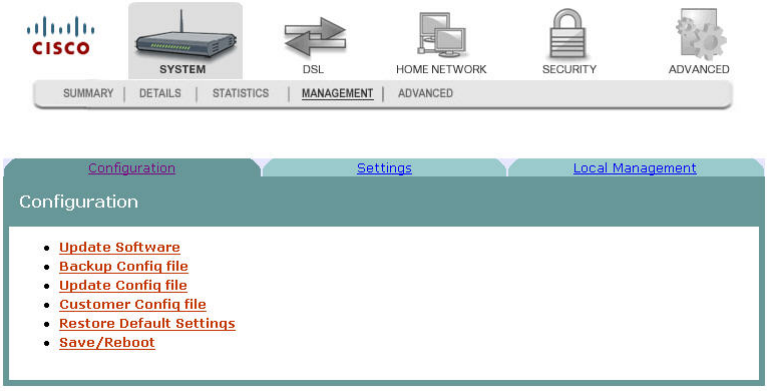
Path: System > Management > Configuration > Restore Default Settings



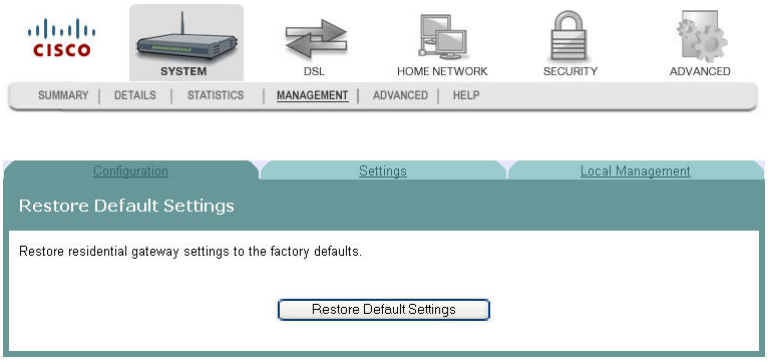
Restoring the Configuration to the Default Settings

To restore the configuration to the default settings, complete the following steps.

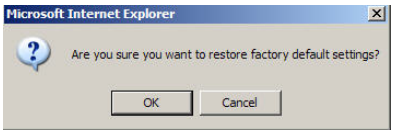
1. Click **System** on the main screen.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



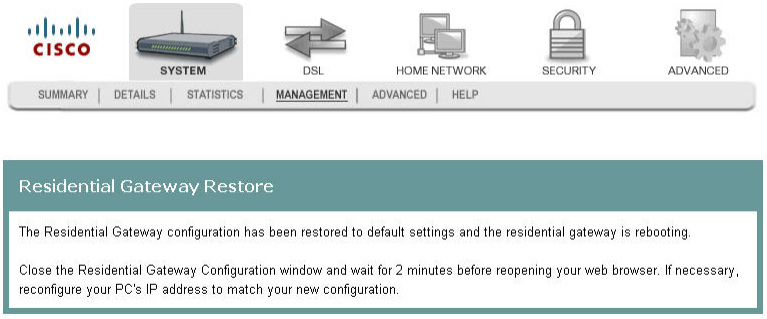
3 Click **Restore Default Settings**. The Tools Restore Default Settings screen opens.



4 Click **Restore Default Settings**. The system displays the following prompt:



5 Click **OK**. The system displays the following message:

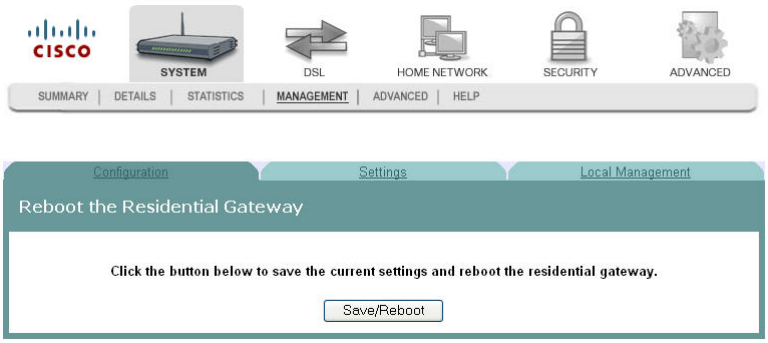


6 Follow the on-screen instructions to restore the default settings.

Saving the Configuration for the Residential Gateway

The Reboot the Residential Gateway screen allows you to save any configuration changes and to reboot the router to make the changes take effect.

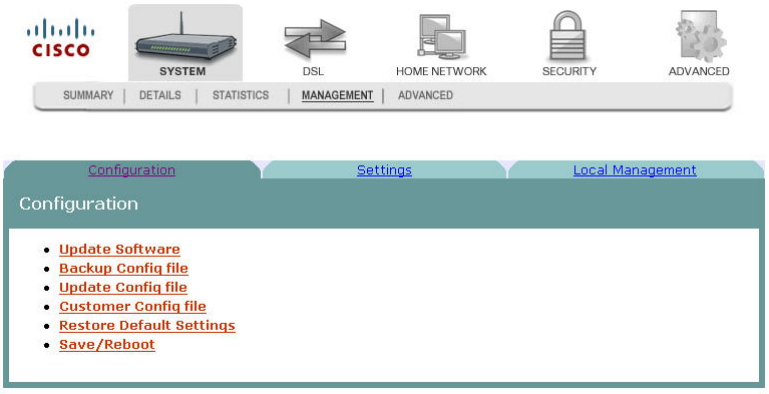
Path: System > Management > Configuration > Restore Default Settings > Save/Reboot



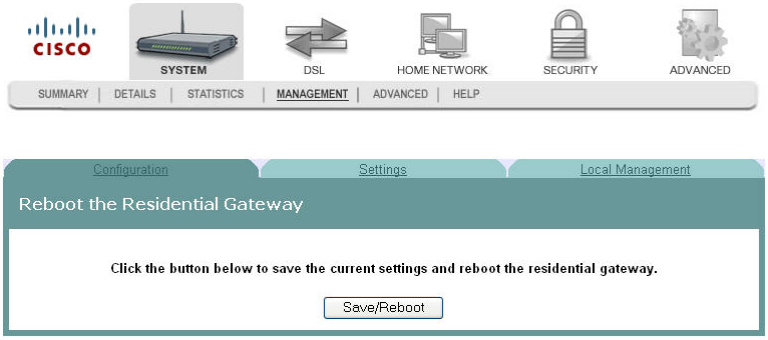
Saving the Configuration and Rebooting the Residential Gateway

To save any configuration changes and to reboot the router to make the changes take effect, complete the following steps.

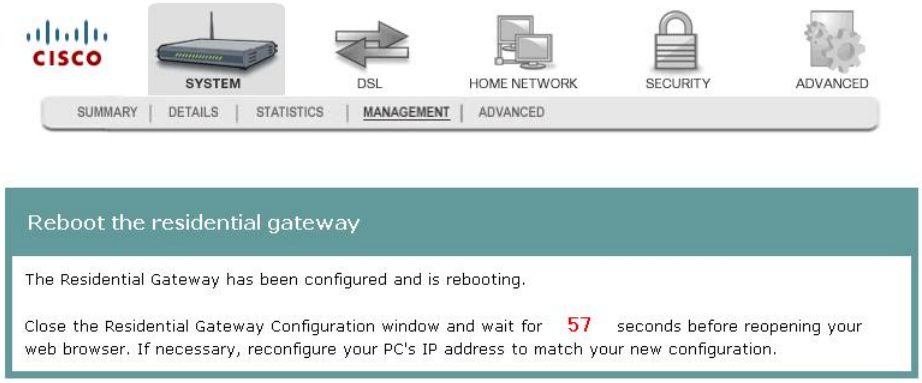
1. Click **System** on the main screen.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



3 Click **Save/Reboot**. The system displays the following message:



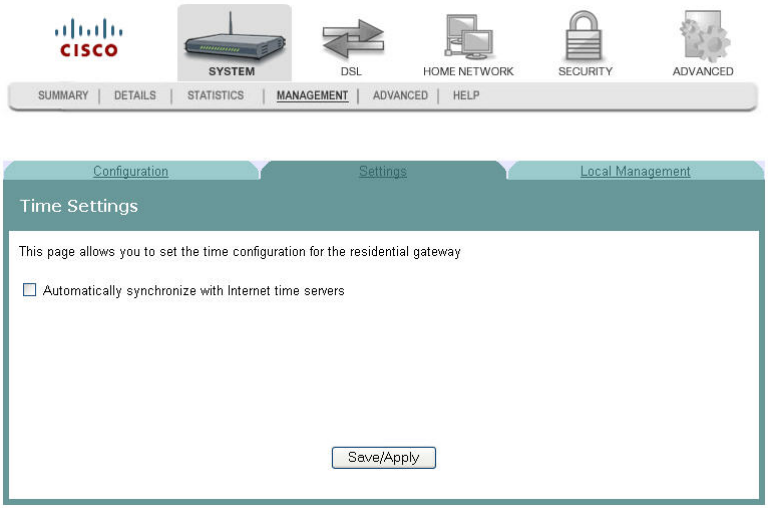
4 Follow the instructions on the screen to save the configuration and to reboot the router. The residential gateway displays the following message shown below. The System Summary screen opens when the residential gateway has finished rebooting. The new settings are displayed.



Time Settings

The Time Settings screen allows you to synchronize the time for the residential gateway with a network-based time server.

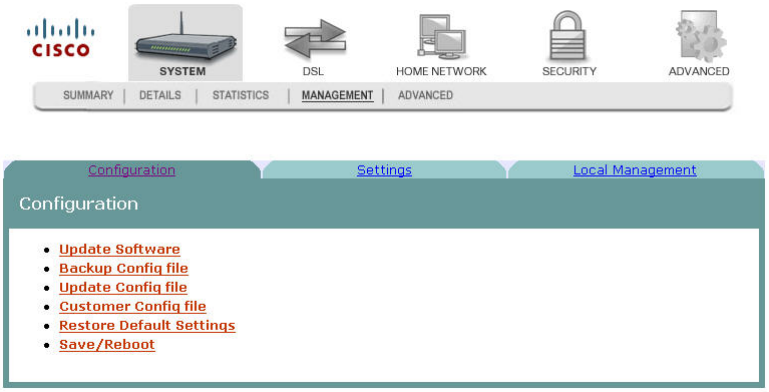
Path: System > Management > Settings > Internet Time



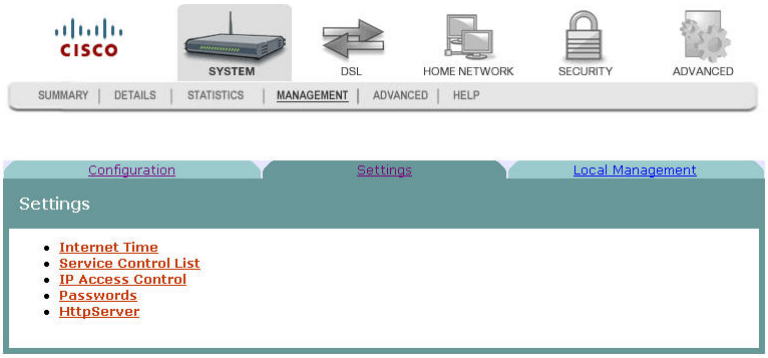
Synchronize with Internet Time

To synchronize the time for the residential gateway with the Internet time, 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.

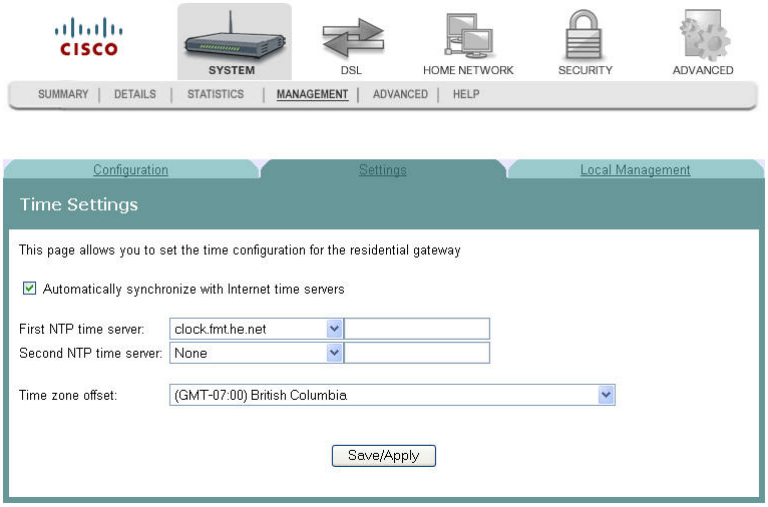


3 Click the **Settings** tab. The Settings screen opens.



4 Click **Internet Time**. The Time Settings screen opens.

5 Check the box **Automatically synchronize with Internet time servers**. The Time Settings screen opens with populated fields.



6 In the First NTP time server field, select a time server from the drop-down list. If you select Other, enter the name of the server in the blank field.

7 In the Second NTP time server field, select a time server from the drop-down list. If you select Other, enter the name of the server in the blank field.

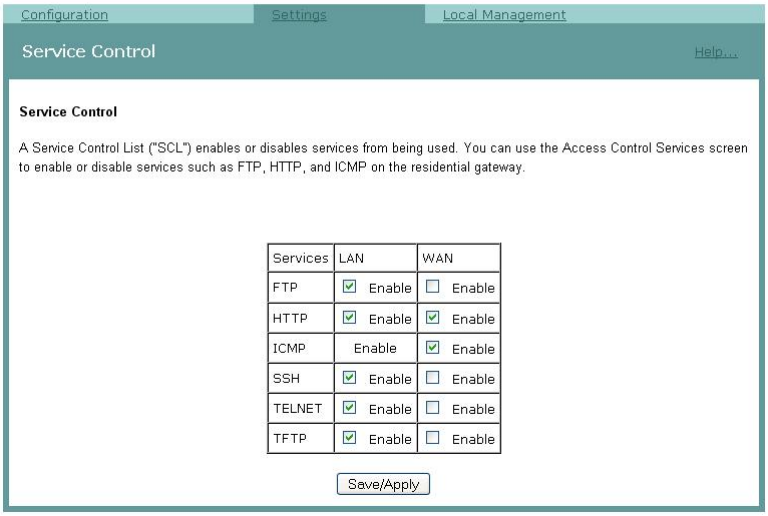
8 In the Time zone offset field, select the time zone specific to your area.

9 Click **Save/Apply**.

Service Control

The Service Control screen allows you to enable or disable services such as FTP, HTTP, and ICMP on the residential gateway.

Path: System > Management > Settings > Service Control List

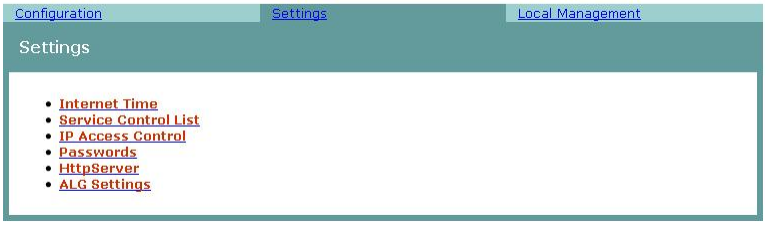


Enabling or Disabling Services

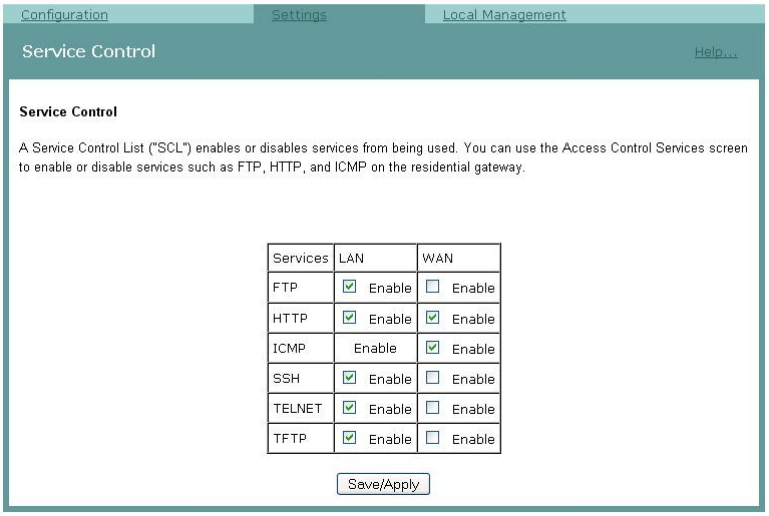
To enable or disable services on the residential gateway, complete the following steps.

1. Click **System** on the main screen.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.

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



4 Click **Service Control List**. The Service Control screen opens.



5 To enable or disable a service, do the following:

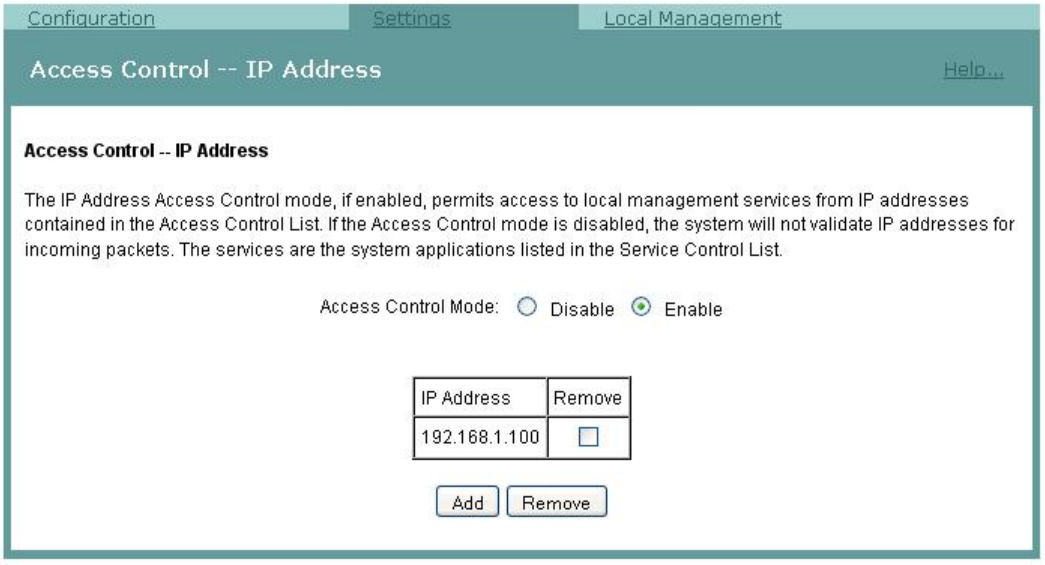
- To enable a service, select the check box next to the service you want to enable. A check box with a check indicates that the service is enabled.
- To disable a service, de-select the check box next to the service you want to disable. A check box without a check indicates that the service is disabled.

6 Click **Save/Apply** to enable or disable the selected services.

IP Access Control

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, you cannot configure the residential gateway from non-local IP addresses. For example, you can use this feature to prevent a remote site from configuring the residential gateway. The services are the system applications listed in the Service Control List.

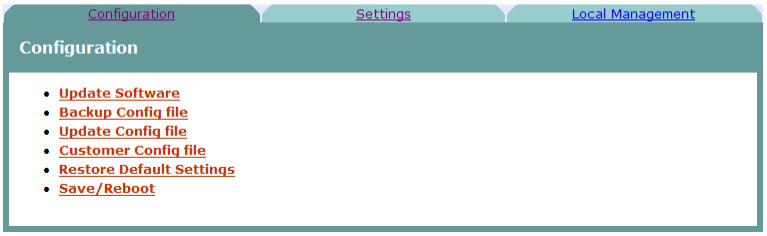
Path: System > Management > Settings > IP Access Control



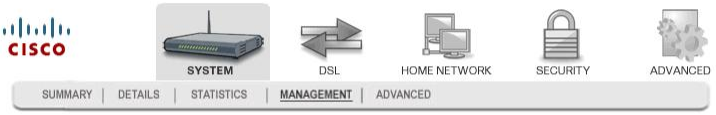
Adding IP Address Access Control

To add IP address access control, complete the following steps.

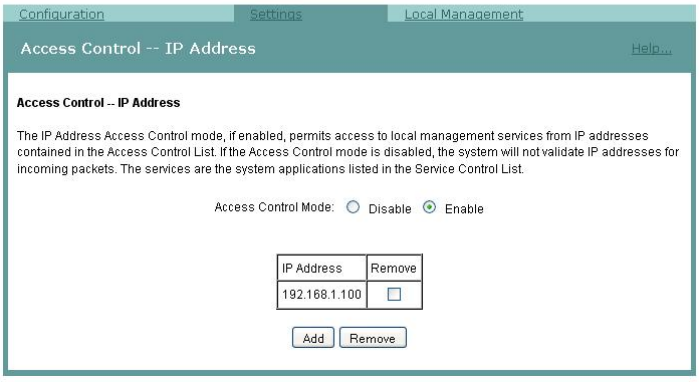
1. Click **System** on the main screen. The System Summary screen opens by default.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



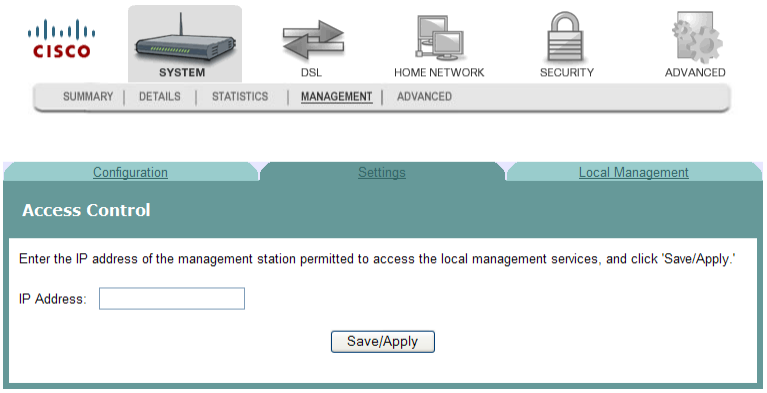
3. Click the **Settings** tab. The Settings screen opens.



4. Click **IP Access Control**. The Access Control -- IP Address screen opens.



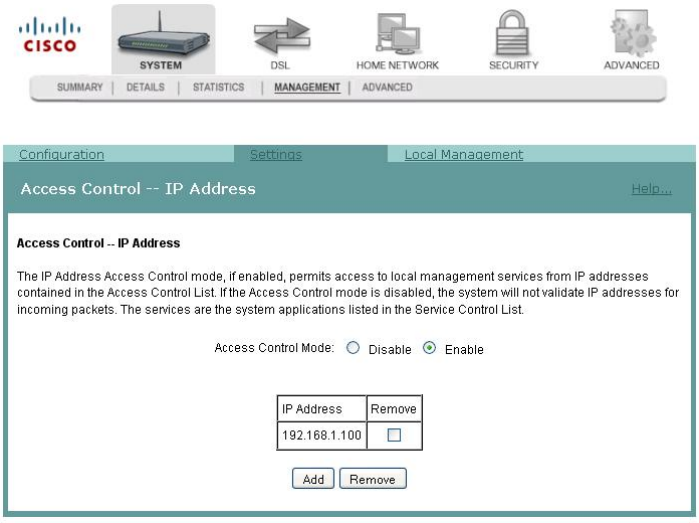
5 Click **Add**. The Access Control screen opens. In the IP Address field, enter the IP address of the management station that you want to allow access to the local management services.



6 In the IP Address field, enter the IP address of the management station that you want to allow access to the local management services.

7 Click **Save/Apply** to allow access for the IP address you entered.

8 Enable the Access Control Mode as shown in the following screen.



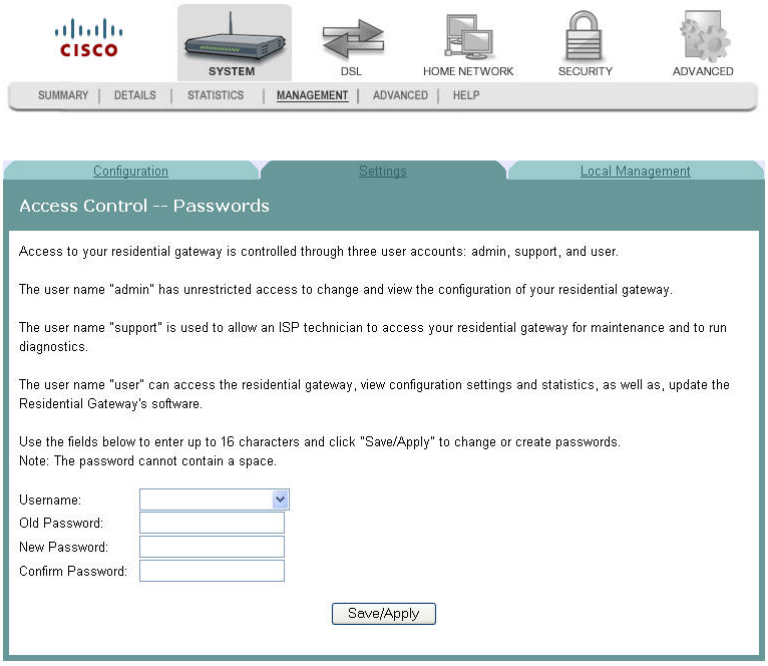
Password Access to the Residential Gateway

Access to the residential gateway is controlled through three user accounts:

- admin. Allows unrestricted access to change and view the configuration of the residential gateway. This login allows access to privileged information.
- support. Allows an ISP technician to access your residential gateway for maintenance and to run diagnostics
- user. Allows access to view configuration settings and statistics, as well as, to update the residential gateway's software.

The admin login provides access to all screens (including privileged information) for the residential gateway. The support login and user login provide access to only a subset of the screens provided to the admin login.

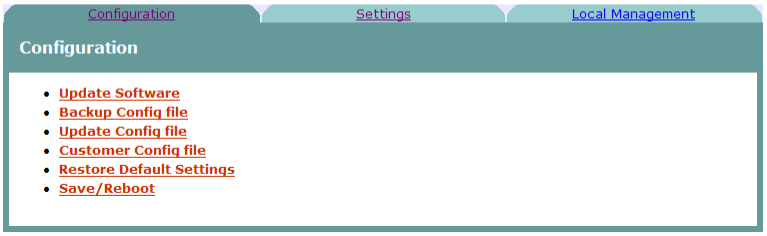
Path: System > Management > Settings > Passwords



Creating Passwords

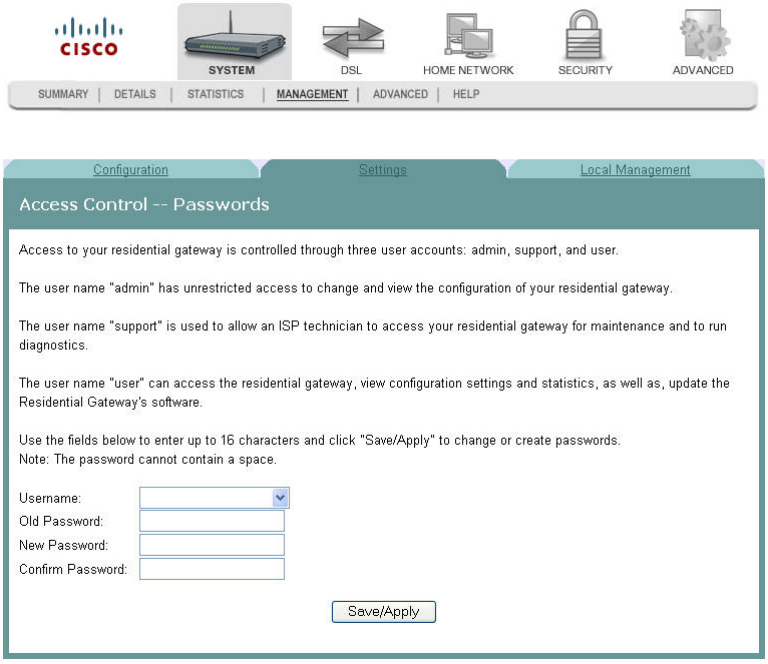
To create passwords for the residential gateway, complete the following steps.

1. Click **System** on the main screen.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



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

4 Click **Passwords**. The Access Control -- Passwords screen opens.



5 In the Username field from the drop-down list, select the type of password you are creating: admin, support, or user. The default user name is **admin**.

6 In the Old Password field, enter the old password. The maximum character length is 16 characters, and passwords cannot contain a space. The default password is **admin**.

7 In the New Password field, enter the new password. The maximum character length is 16 characters, and passwords cannot contain a space.

8 In the Confirm Password field, enter the new password again to confirm your entry.

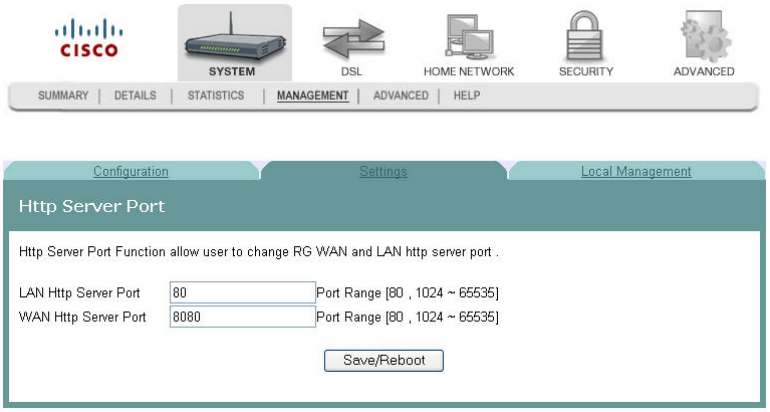
9 Click **Save/Apply** to save the password.

Tip: Another quick way to change passwords is to go to the System (home) page. Scroll down to the last option and click **Password Setting**. A popup screen opens as shown below. Use this screen to enter your new passwords.

HTTP Server Port

The HTTP Server Port screen allows you to specify the TCP port for the HTTP server on both the LAN and WAN interfaces.

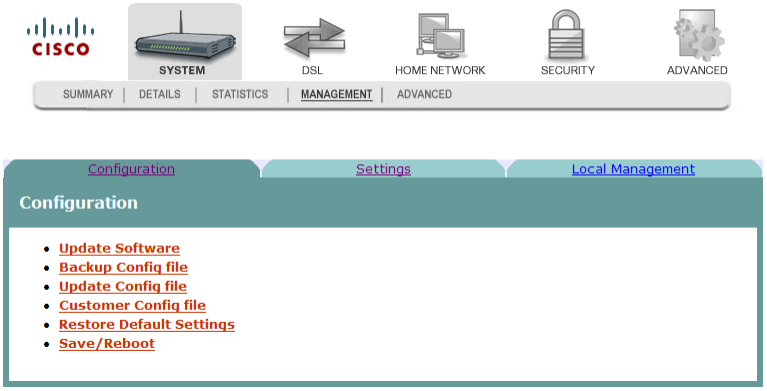
Path: System > Management > Settings > HttpServer



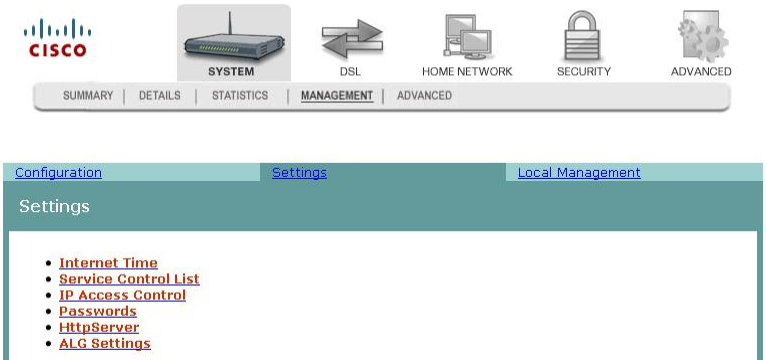
Modifying the Http Server Ports

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

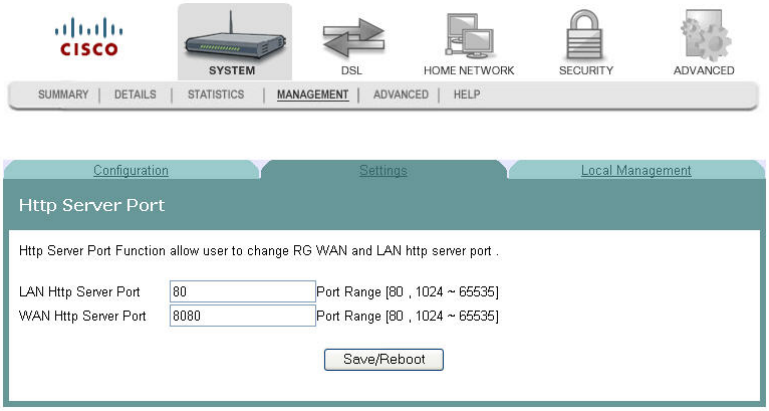
1. Click **System** on the main screen.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



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



4 Click **HttpServer**. The Http Server Port opens.



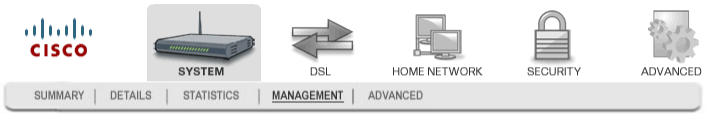
5 In the LAN Http Server Port field, enter the port number for the HTTP server from the LAN side.

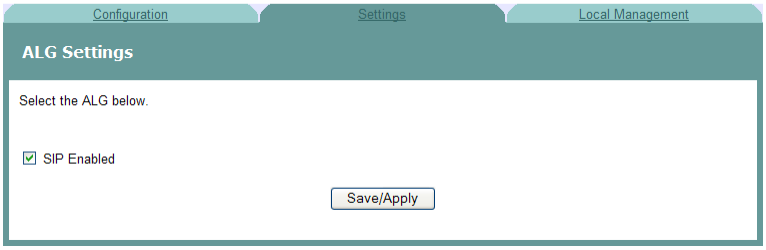
6 In WAN Http Server Port field, enter the port number for the HTTP server from the WAN side.

ALG Settings

The ALG settings allow you to enable or disable the SIP ALG based on the customer's requirement.

Path: System > Management > Settings > ALG Settings

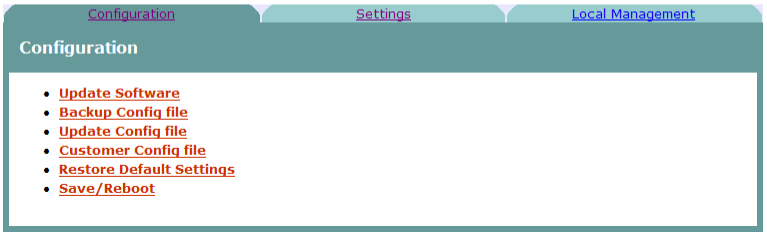




Modifying the ALG Settings

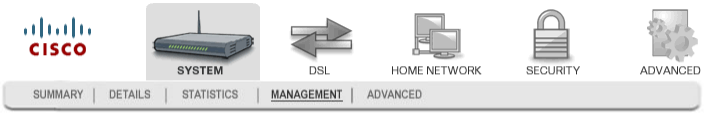
To modify the ALG settings, complete the following steps.

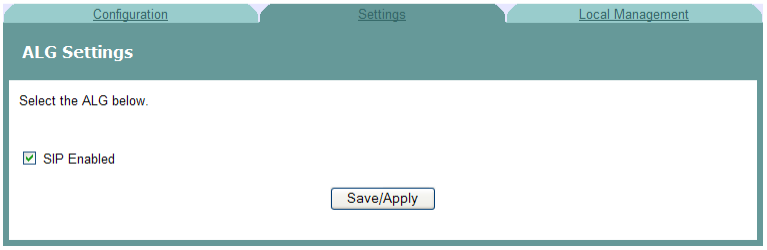
1. Click **System** on the main screen.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



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

4 Click the last option, **ALG Settings**. The ALG Settings page opens.



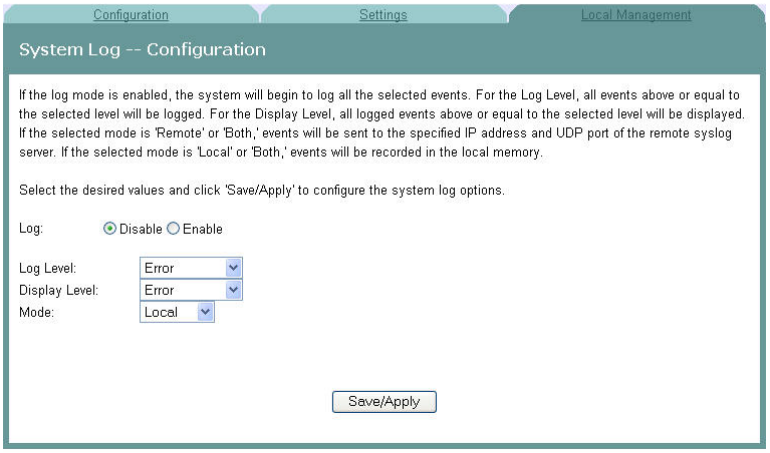


5 Set or clear the **SIP Enabled** check box, depending on your customer's requirement.

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.

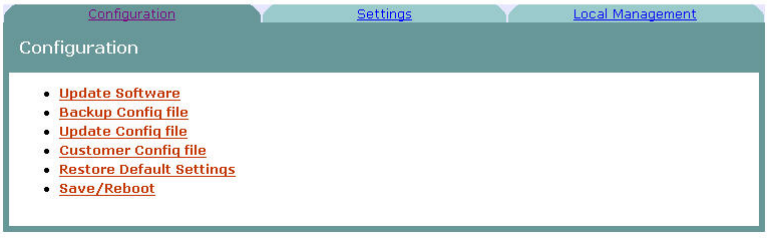
Path: System > Management > Local Management > System Log Configuration



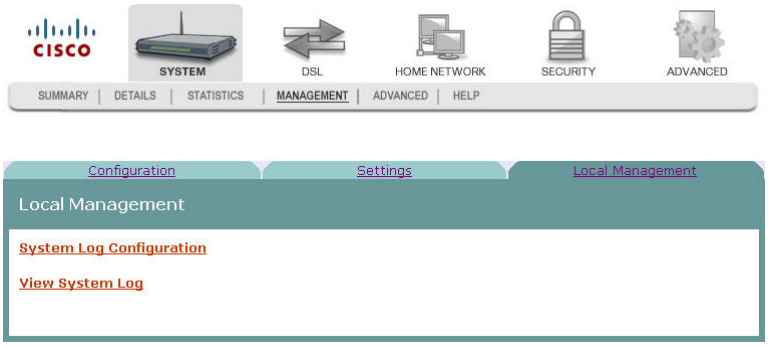
Logging Events

To log selected events, complete the following steps.

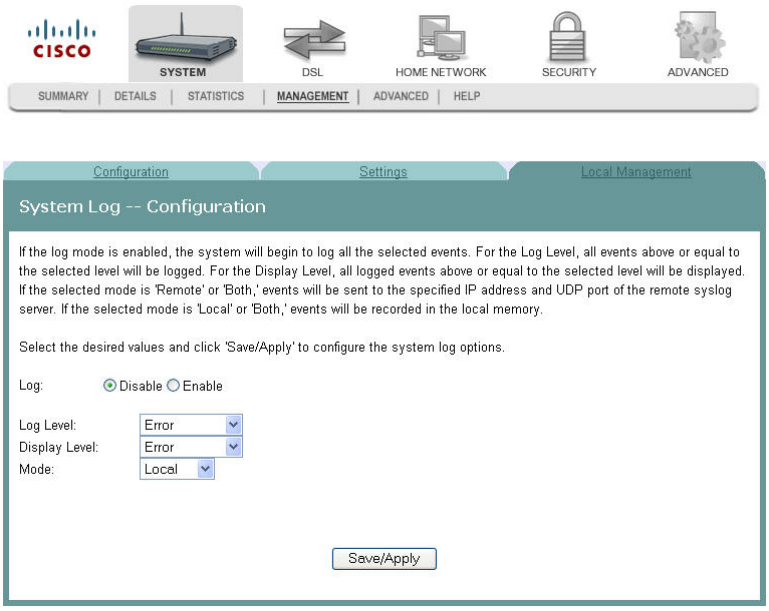
1. Click **System** on the main screen.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



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



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



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.

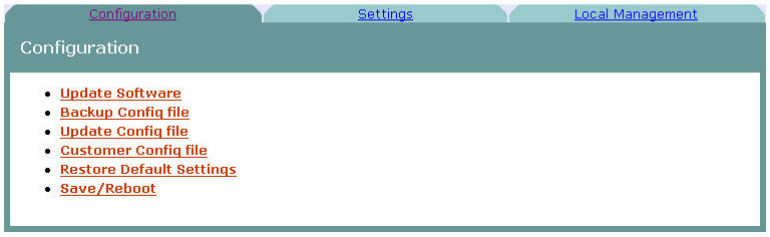
- Local. Events are logged in memory. You must log in to the device to display the events.
- Remote. Events log is sent to a remote server (syslog server).
- Both. Events are logged in memory and are sent to the remote server.

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

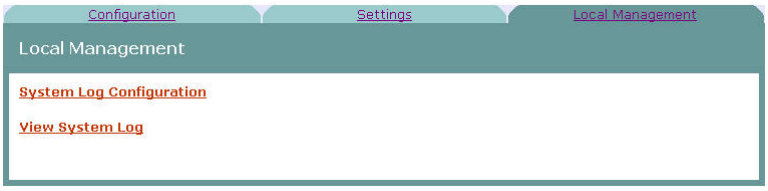
Disabling Logging

To disable the logging function, complete the following steps.

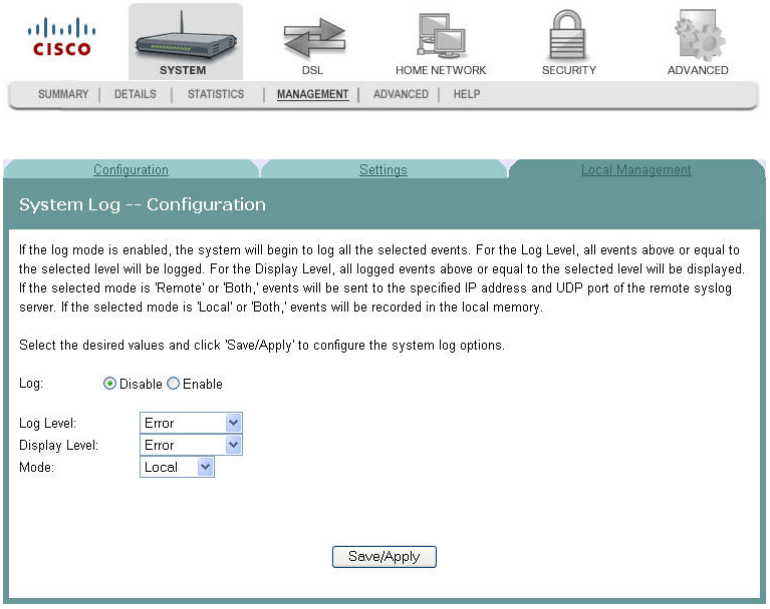
1. Click **System** on the main screen.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



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



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



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

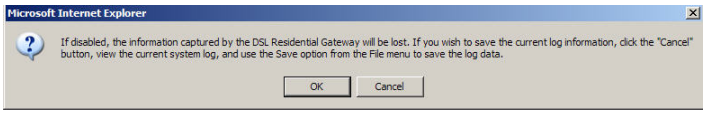
7 In the Display Level field, select from the following options to indicate the level of alarms that you want displayed:

- 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:



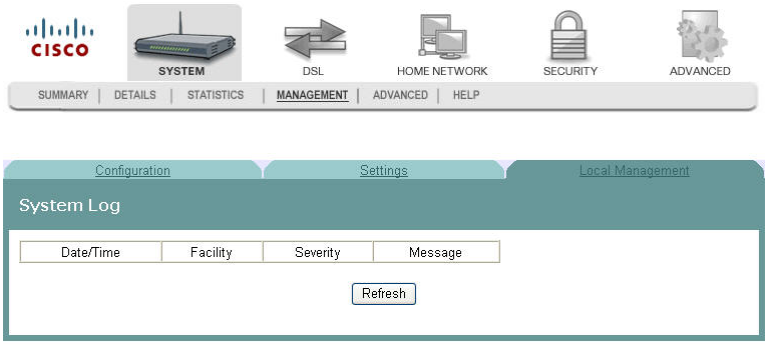
10 Are you sure you want to disable logging and lose the captured data?

- 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.

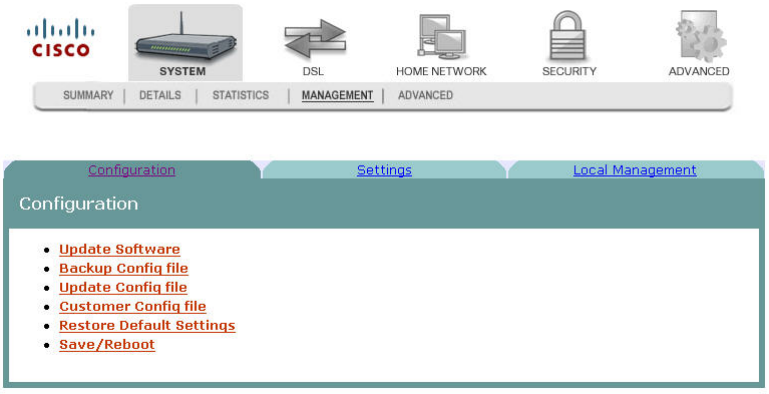
Path: System > Management > Local Management > View System Log



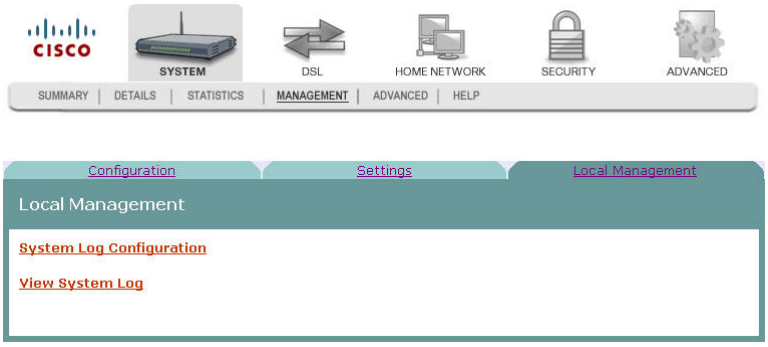
Viewing System Logs

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

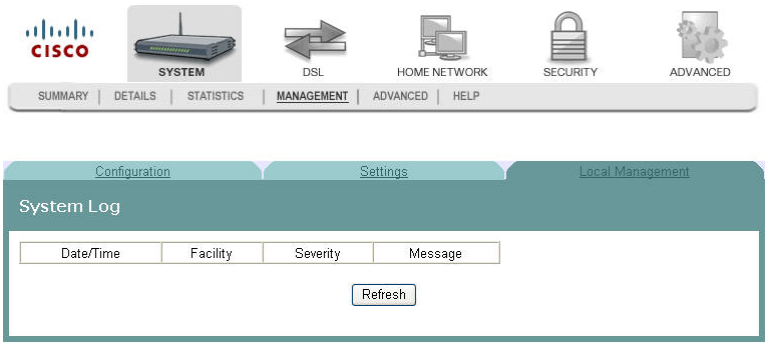
1. Click **System** on the main screen.
2. Click **Management**. The Configuration screen opens with the Configuration tab in the forefront.



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



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



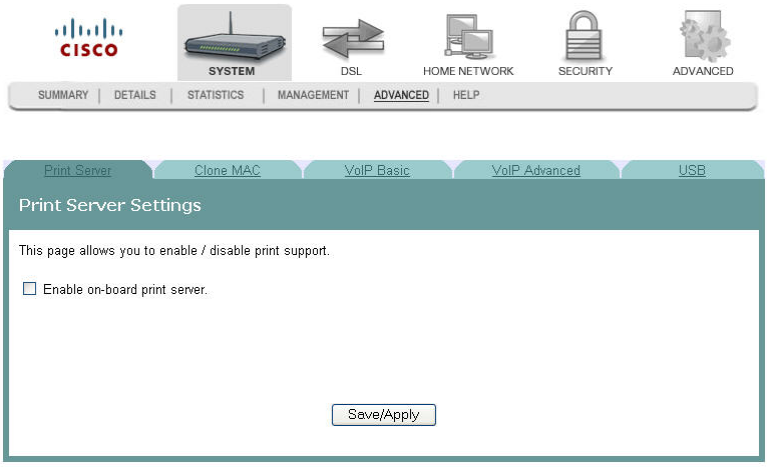
5 Review the log entries on the screen.

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.

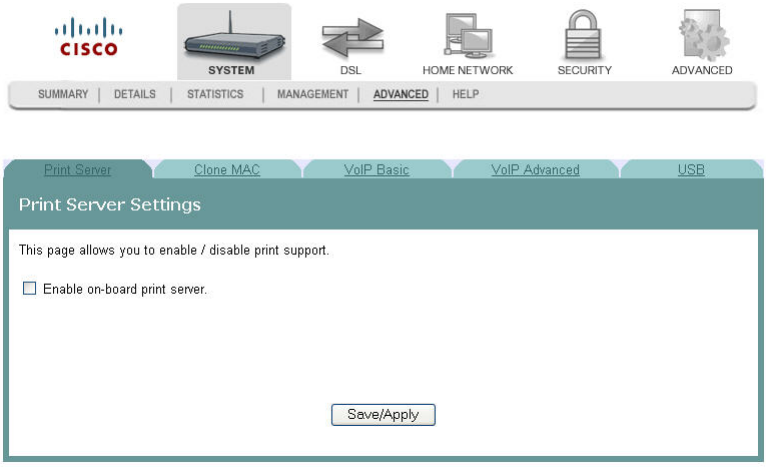
Path: System > Advanced > Print Server



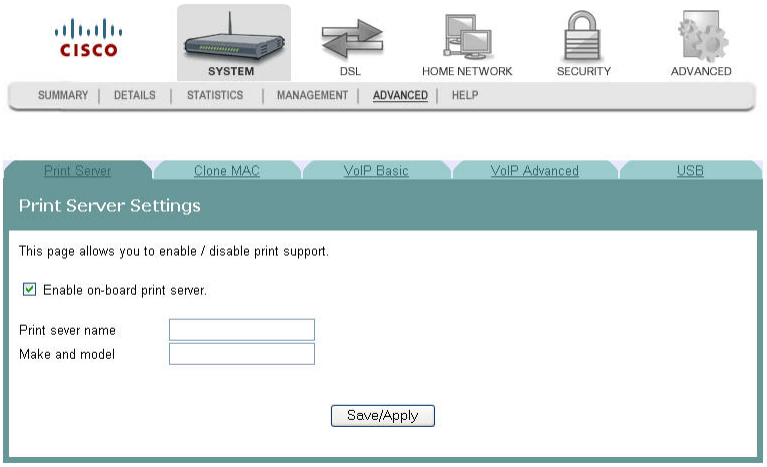
Enabling the Print Server

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



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.

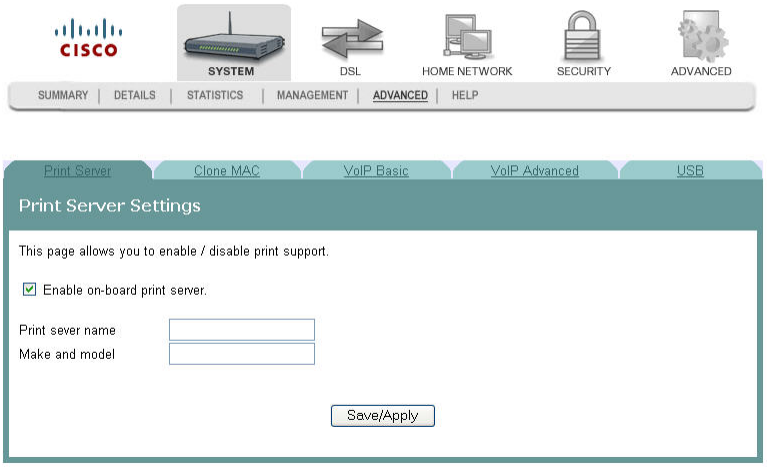
6 Click **Save/Apply** to enable the print server.

Disabling the Print Server

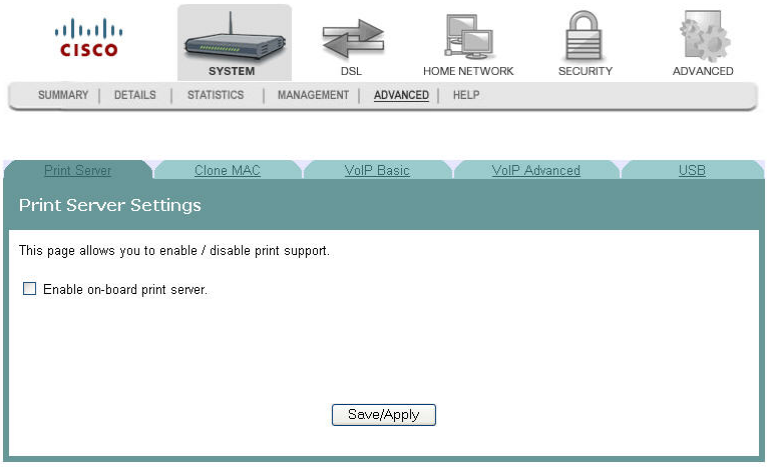
To disable the print server, complete the following steps.

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.



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.

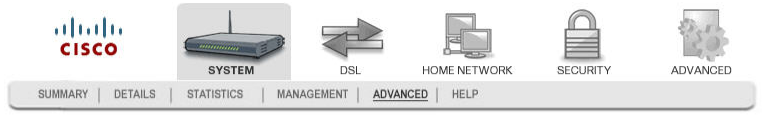


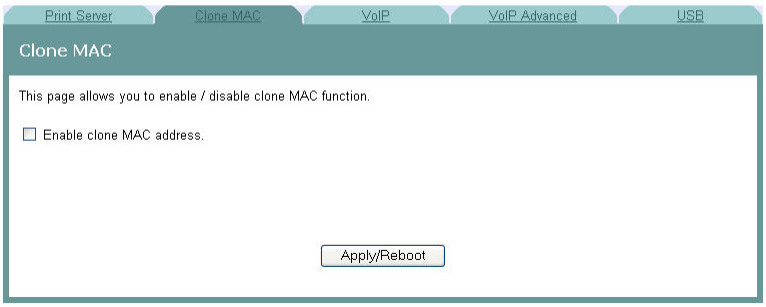
4 Click **Save/Apply** to disable the print server.

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

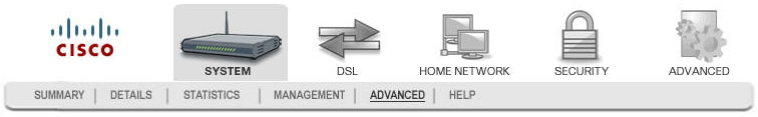


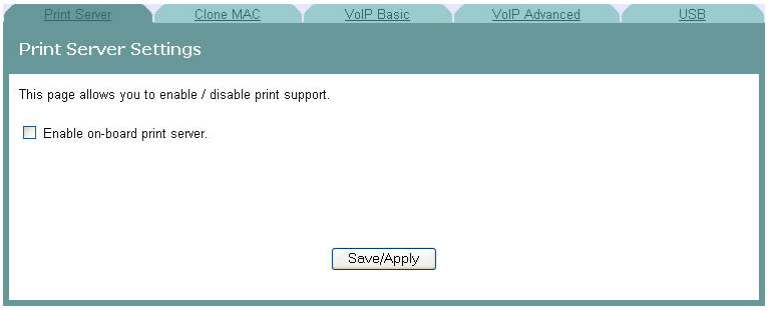


Enabling the Clone MAC Function

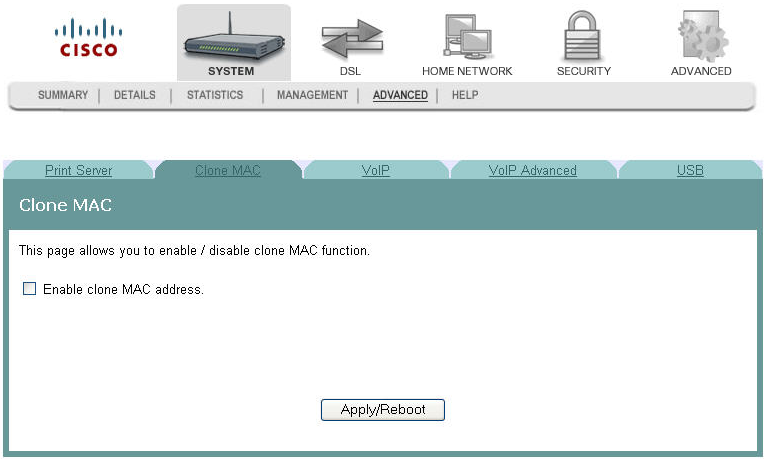
To enable the Clone MAC function, complete the following steps.

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.

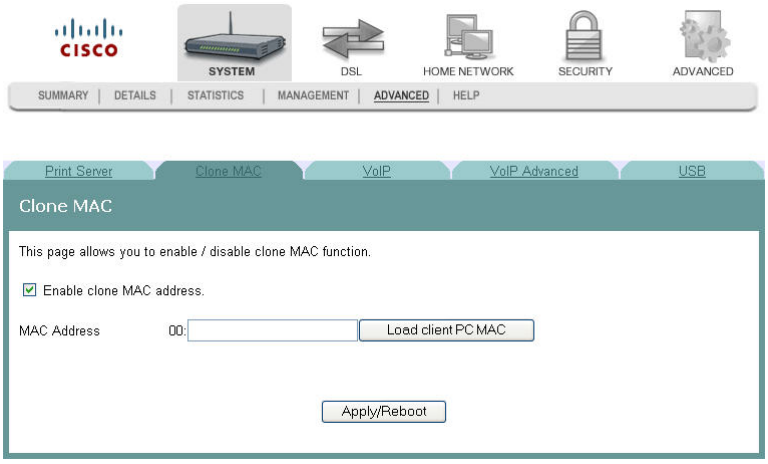




3 Click the **Clone MAC** tab.



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



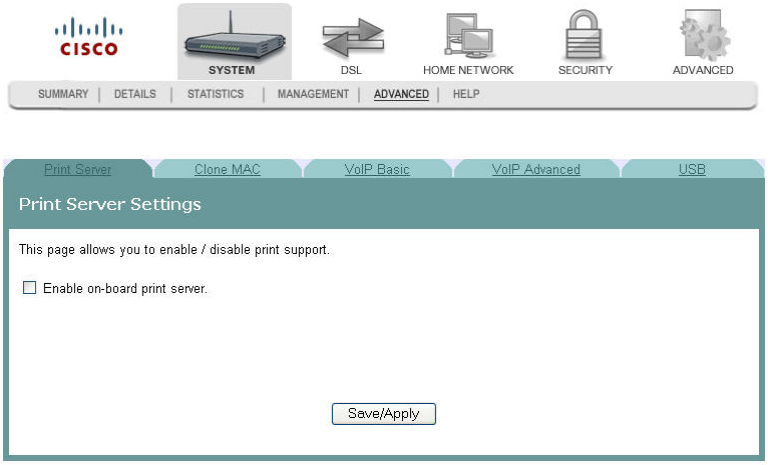
5 In the MAC Address field, enter the MAC address that you want to clone. You can also click Load client PC MAC to locate an address you want to clone.

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

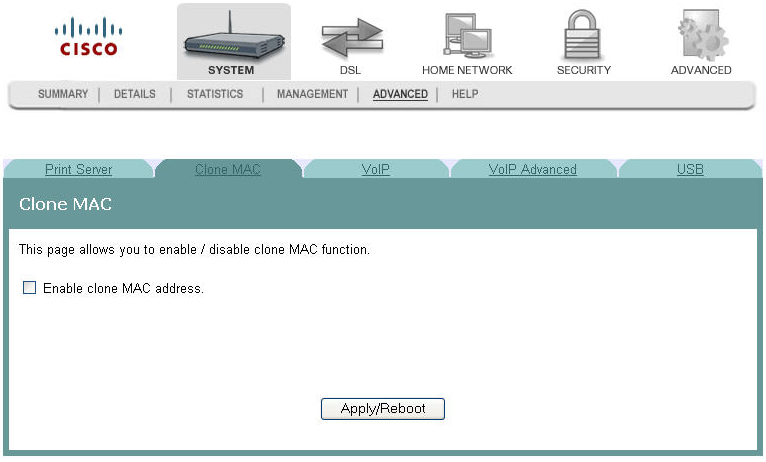
Disabling the Clone MAC Function

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.

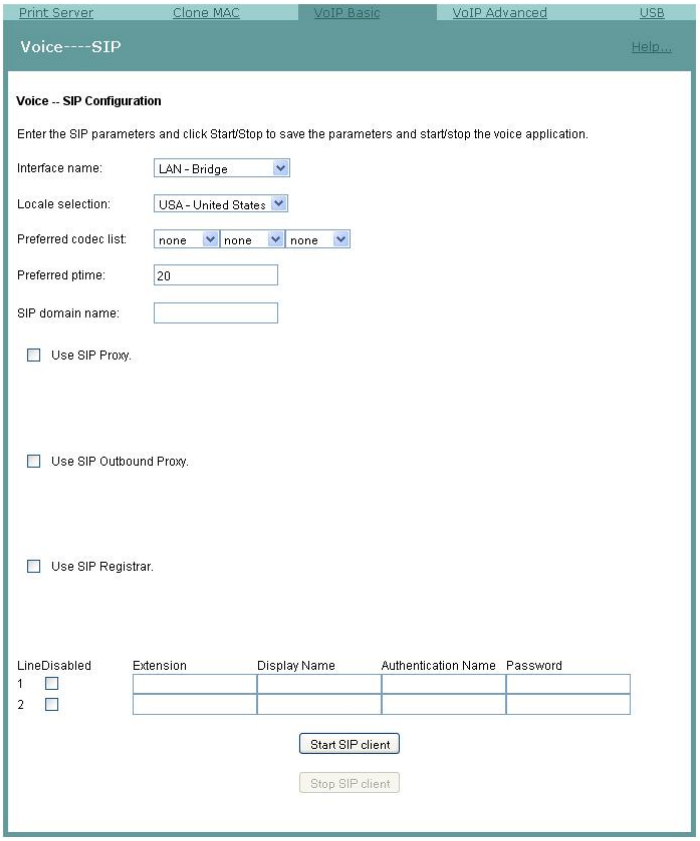


4. Uncheck the **Enable clone MAC address** check box. The screen refreshes and the field for entering the MAC address is removed from the screen.
5. Click **Apply/Reboot** to disable the Clone MAC function.

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.

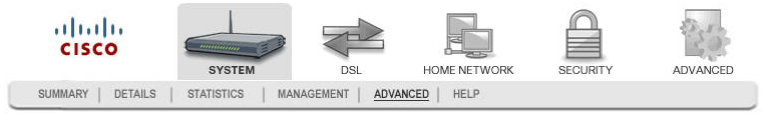
Path: System > Advanced > VoIP Basic

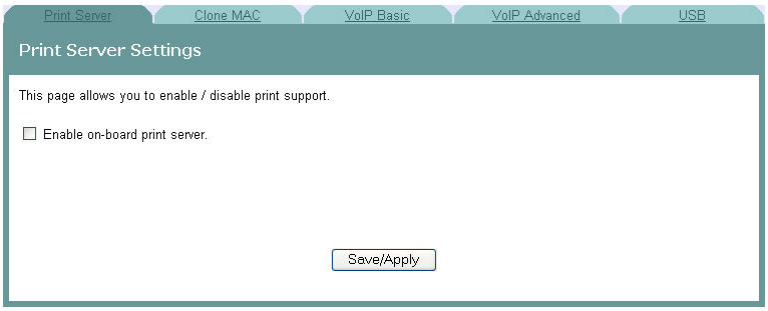


Setting Up VoIP

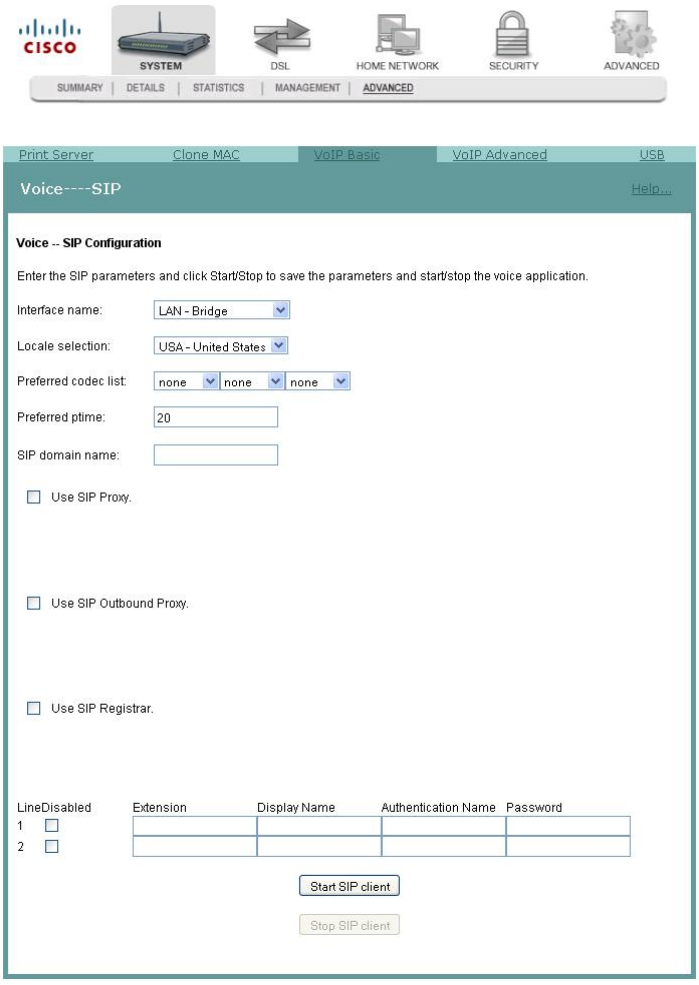
To enter the VoIP parameters, complete the following steps.

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.



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 list 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**, check the Use SIP Proxy check box. The SIP Proxy and the SIP Proxy port fields appear. Enter the SIP proxy server domain name or IP address and the SIP Proxy port.
- If **no**, make sure the Use SIP Proxy check box is unchecked.

10 Do you wish to use an SIP Outbound proxy?

- If **yes**, check the Use SIP Outbound Proxy check box. The SIP Outbound Proxy and the SIP Outbound Proxy port fields appear. Enter the SIP outbound proxy server domain name or IP Address and the SIP outbound proxy port.
- If **no**, make sure the Use SIP Outbound Proxy check box is unchecked

11 Do you wish to use SIP Registrar?

- If **yes**, check the Use SIP Registrar check box. The SIP Registrar and the SIP Registrar port fields appear. Enter the SIP registrar's domain name or IP address and the SIP registrar's port.
- If **no**, make sure the Use SIP Registrar check box is unchecked.

12 Do you want to disable the line?

- If **yes**, check the Line Disabled checkbox to disable the line and prevent the phone connecting to this line from working.
- If **no**, make sure the Line Disabled checkbox is unchecked.

  Note: For normal operation, the Line Disabled Checkbox should be unchecked.

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

14 In the Display Name field, enter the name that you want to be displayed.

15 In the Authentication Name field, enter the name that you want to be authenticated.

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

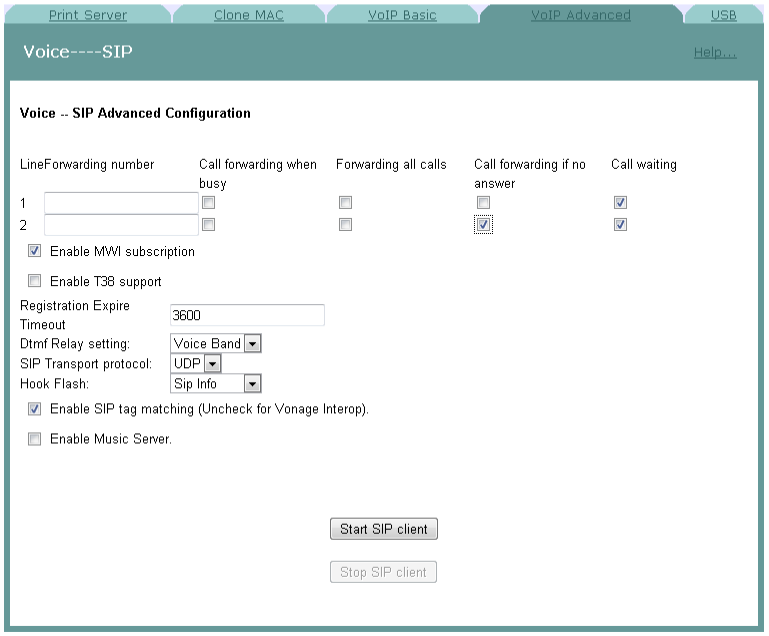
17 Do you want to activate the line?

- 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.

Path: System > Advanced > VoIP Advanced



Setting Up Advanced VoIP Features

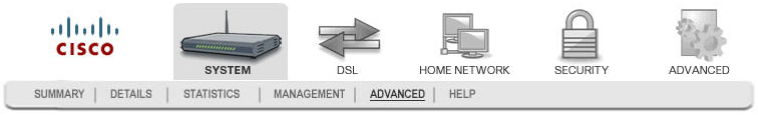
In consultation with your ISP or VOIP service provider, you can use the Voice----SIP screen to set up advanced VOIP features for the residential gateway.

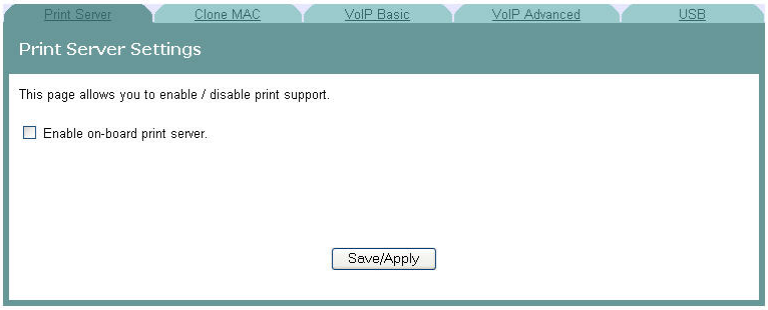
Note: Be sure to consult your ISP or VOIP service provider when making the settings described below.

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

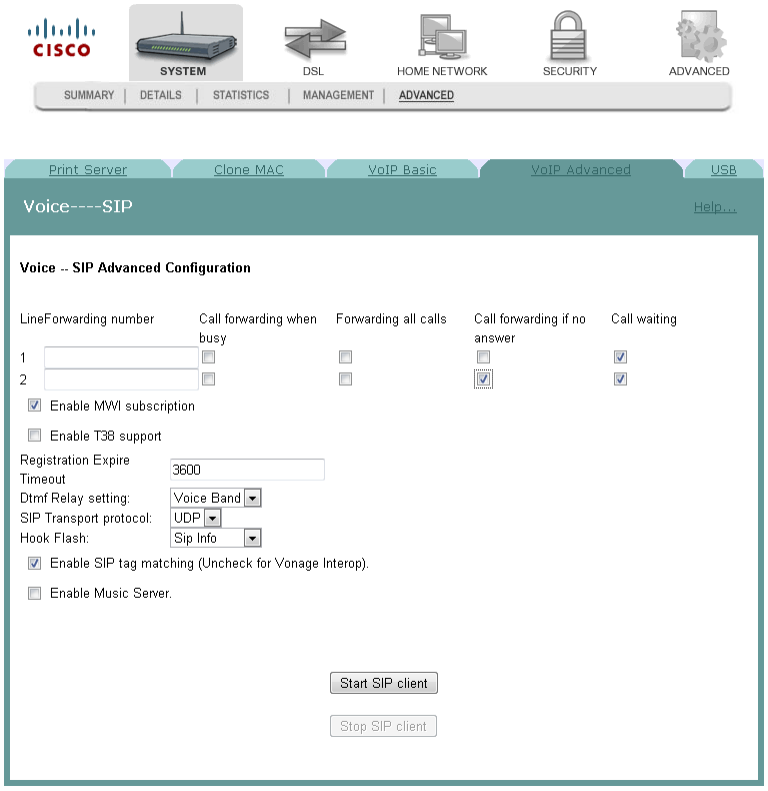
1 Click **System** on the main screen.

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





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



4. In the LineForwarding 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 **Call forwarding when busy** to forward this line to another number when this line is busy.
   b. Check **Forwarding all calls** to forward all calls to this line.
   c. Check **Call forwarding if no answer** to forward this line if the caller receives no answer.
   d. Check **Call waiting** to enable call waiting for this line.
5. Repeat step 4 for a second phone line, if needed.
6. Check **Enable MWI subscription** to enable the message waiting indicator if desired.
7. Check **Enable T38 support** to enable T38 fax support if needed.
8. In the **Registration Expire Timeout** field, enter the registration expiration time of the SIP client.
9. In the **Dtmf Relay setting** field, select one of the following settings:
   - Sip Info
   - RFC2833
   - Voice Band
10. In the **SIP Transport protocol** field, select the protocol you will support from the following options:
    - All
    - TCP
    - UDP
    - TLS
11. In the **Hook Flash** field, select one of the following as instructed by your ISP or VOIP service provider:
    - Sip Info
    - Voice Band
12. Check **Enable SIP tag matching (Uncheck for Vonage Interop)** to enable session initiation protocol.
13. Check **Enable Music Server** to have music playing while callers wait.
14. Click **Start SIP client** or **Stop SIP client** as needed to start or stop the SIP client.

USB File List

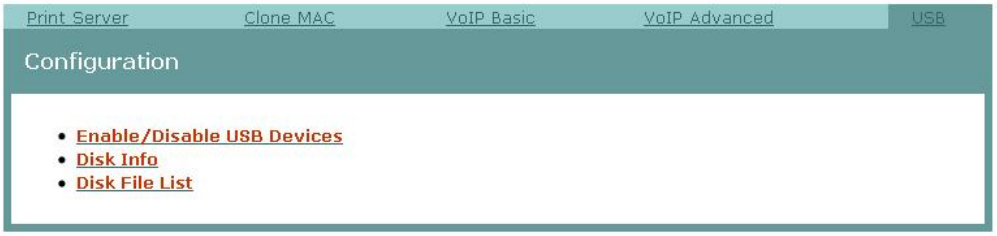
The USB File List screen allows you to view and download the content of a USB flash drive from any computer connected to the gateway. This feature allows your residential gateway to act like a shared network drive.

Path: System > Advanced > USB

Enabling or Disabling USB Devices

To enable or disable a USB device, 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 **USB**. The USB Configuration screen opens.



4 Click **Enable/Disable USB Devices**. The Enable/Disable USB Devices screen opens.

5 Do you wish to enable USB devices?

- If **yes**, check the **Enable on-board usb storage devices** check box to enable the USB devices. After you enable it, you can view the USB disk information or the Disk File List on the page. You can access the files on the USB disk drive from any LAN/WLAN PC since the files are on the network.
- If **no**, make sure the **Enable on-board usb storage devices** check box is unchecked.

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

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

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

Inner Pair Summary

	Inner Pair	
	Downstream	Upstream
SNR Margin (dB):	9.1	6.7
Attenuation (dB):	0.5	0.0
Rate (Kbps):	20799	1208

Mode:	ADSL2+
Status:	Showtime

Outer Pair Summary

	Outer Pair	
	Downstream	Upstream
SNR Margin (dB):	6.3	6.7
Attenuation (dB):	0.5	0.0
Rate (Kbps):	23493	1223

Mode:	ADSL2+
Status:	Showtime

DSL Statistics

The DSL Statistics screen displays statistics for the ADSL connection. This screen shows the number of frames with errors.

Path: DSL > Statistics

Inner Pair 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:		

ADSL BER Test | Reset Statistics

To Test the Quality of the DSL Connection

The ADSL Bit Error Rate (BER) will report the quality of the ADSL connection. The ADSL BER test results will show how many bits are sent and are erred among them.

To test for quality of the DSL connection:

1. Click **DSL** on the main screen.
2. Click the **Statistics** tab.
3. Click **ADSL BER Test**.
4. Enter the duration of the test in seconds for the Tested Time (sec).
5. Click **Start** to start the test.

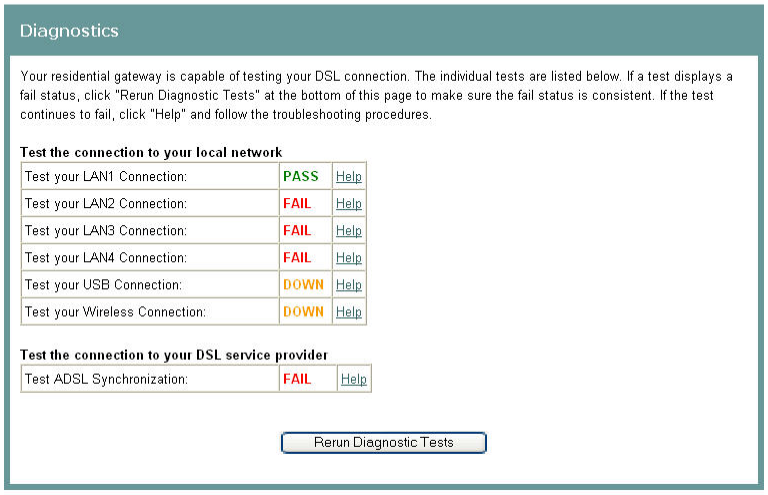
To Reset DSL Statistics

To reset the statistics, click **Reset Statistics** button. This action will clear the numbers and restart the calculation.

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.

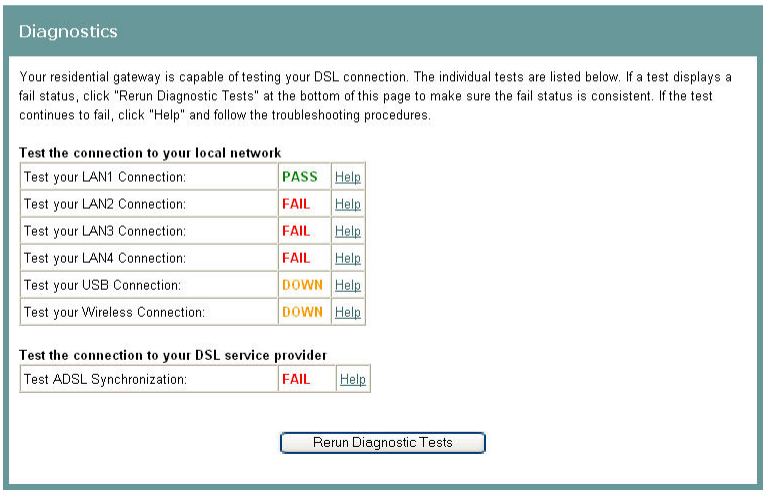
Path: DSL > Diagnostics



Running Diagnostic Tests

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

1. Click **DSL** on the main screen.
2. Click the **Diagnostics** tab. The Diagnostics screen opens.



3. Click **Rerun Diagnostics Tests** to start the diagnostics test. The screen populates with results such as Fail or Pass.

4 When you have a Permanent Virtual Circuit (PVC) up, for example an MER connection as shown in the screen-shot below, then you can see a list of other tests such as OAM F4/F5 or the PING test appear on the DSL Diagnostics page. You can click **Test with OAM F4** to run a OAM F4 test.

mer_0_0_35 Diagnostics Help...

Test the connection to your local network

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

Test the connection to your DSL service provider

Test ADSL Synchronization:	PASS	Help
Test ATM OAM F5 segment ping:	FAIL	Help
Test ATM OAM F5 end-to-end ping:	FAIL	Help

Test the connection to your Internet service provider

Ping default gateway:	PASS	Help
Ping primary Domain Name Server:	PASS	Help

Test | Test With OAM F4

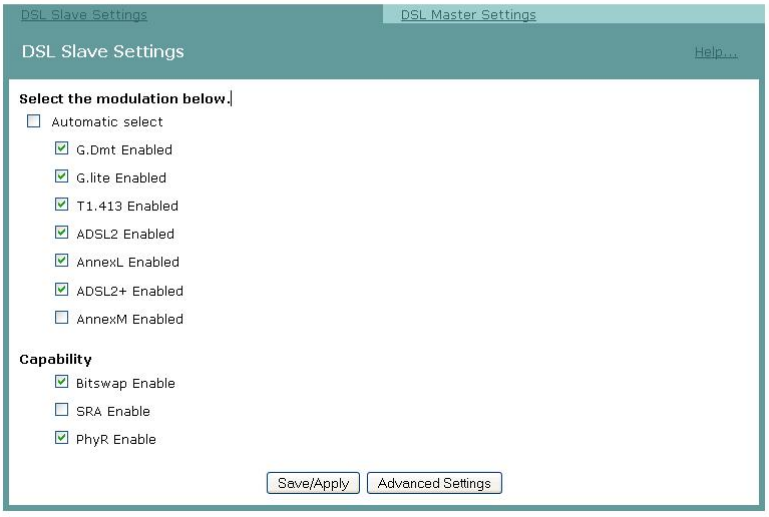
DSL Settings

The DSL Settings screens allow you to configure slave and master settings for the residential gateway.

DSL Slave Settings

The DSL Slave 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), Bitswap Enable, PhyR, and so forth.

Path: DSL > Setting > DSL Slave Settings

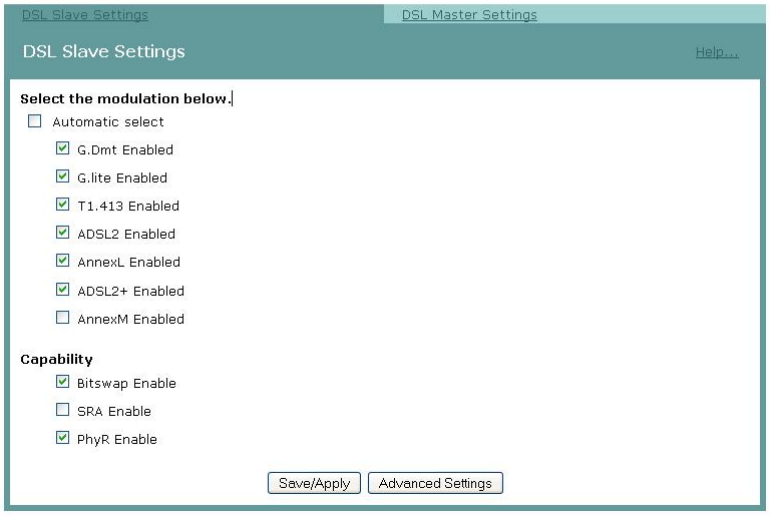


Configuring DSL Slave Settings

To configure DSL slave 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 Slave Settings screen opens by default.



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:

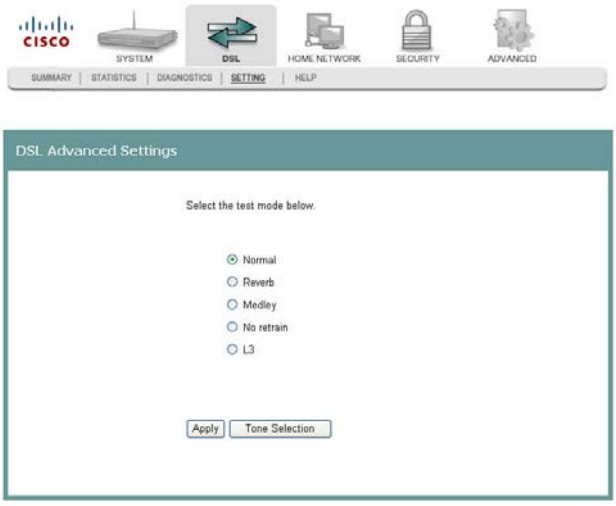
- Bitswap Enable
- SRA Enable
- PhyR Enable

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

DSL Advanced Settings

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

Path: DSL > Setting > DSL Slave Settings > Advanced Settings

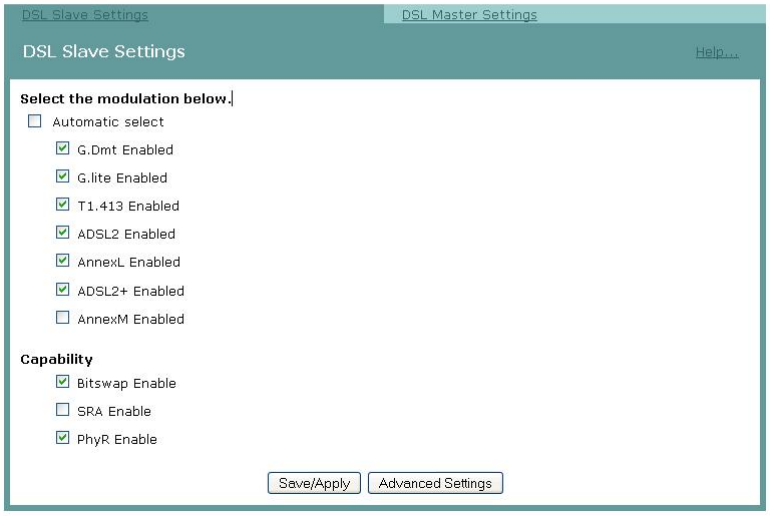


Configuring DSL Advanced Settings

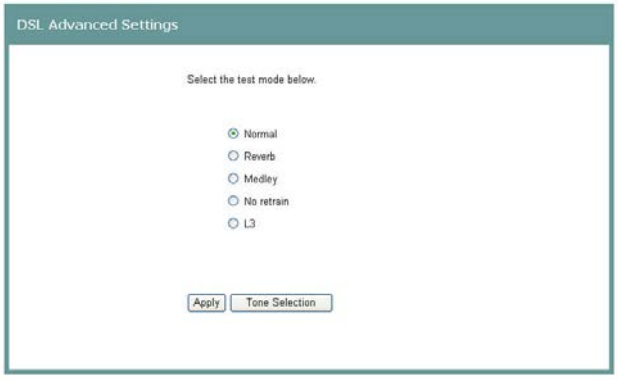
To configure the DSL advanced settings, complete the following steps.

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

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



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



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.

DSL Master Settings

The DSL Master Settings screen allows you to choose the bonding bypass mode for the RG, and to enable or disable PhyR as needed.

Path: DSL > Setting > DSL Master Settings

Configuring DSL Master Settings

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

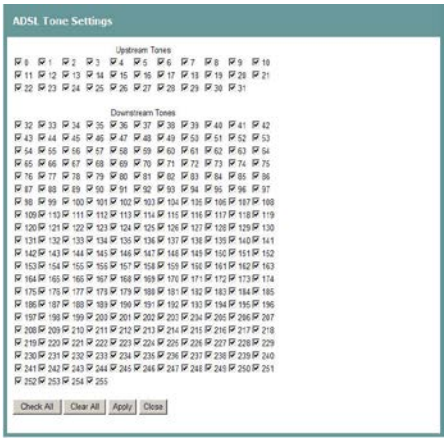
1. Click **DSL** on the main screen. The Summary screen opens by default.
2. Click the **Setting** tab. The DSL Slave Settings screen opens by default.
3. Click the **DSL Master Settings** tab to open the DSL Master Settings screen.

4. Define whether the RG will work on both pairs or a single pair.
   - Choose **Bonding Mode** if you want the RG to work on both pairs.
   - Choose **Non-bonding Mode** if you want the RG to work on a single pair.
5. Set or clear the **PhyR Enable** check box depending on whether you want PhyR enabled.
6. Click **Save/Apply** to save the settings.

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

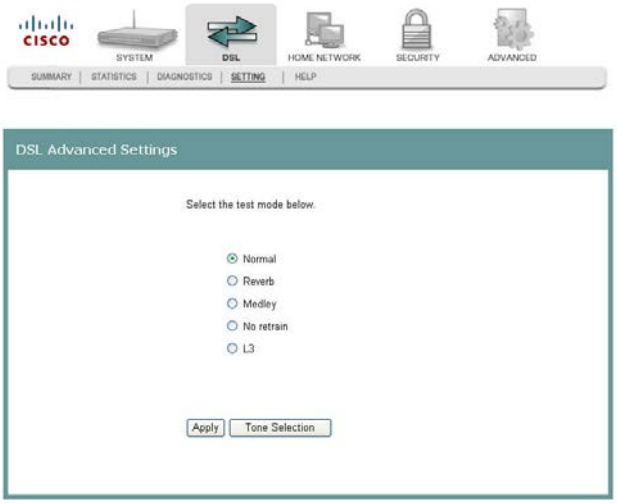


Setting DSL Tones or Frequencies

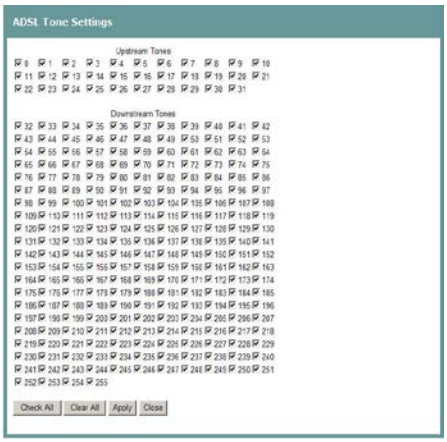
To set DSL tones or frequencies, complete the following steps.

1. Click **DSL** on the main screen. The Summary screen opens by default.
2. Click the **Setting** tab. The DSL Settings screen opens.

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



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



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.

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

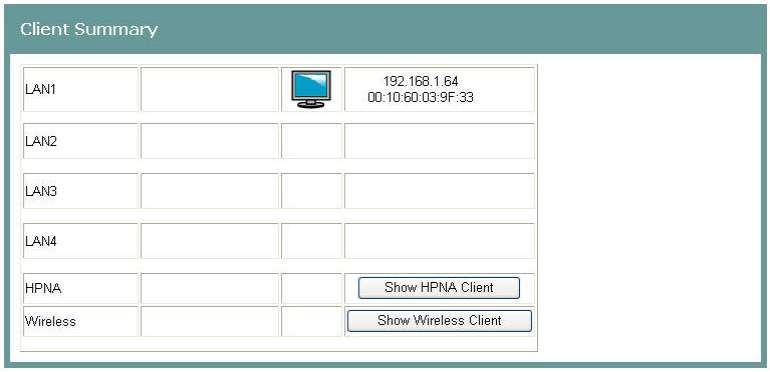
The Client Summary screen shows all the client devices (Wired/Wireless/HPNA) attached to the residential gateway on the LAN side. You can click **Show HPNA Client** to display the HPNA devices attached to the HPNA RF interface of the residential gateway.

Path: Home Network > Summary > Show HPNA Client

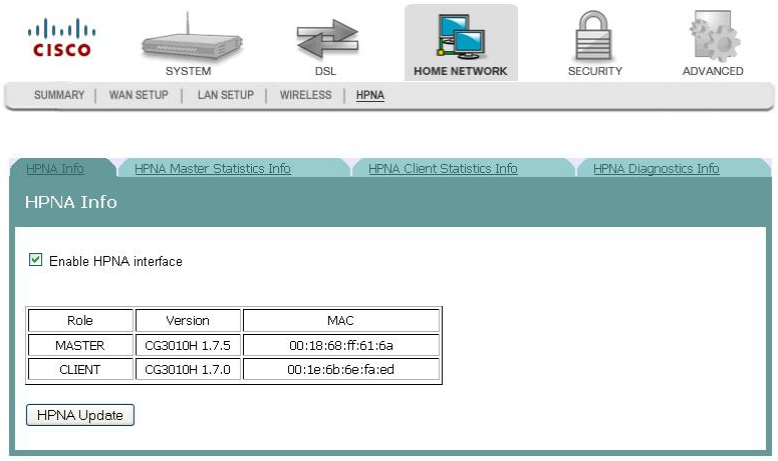
Updating HPNA Clients

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.



3 Click **Show HPNA Client**. After processing, the HPNA Info screen opens. This screen shows the role, MAC Address, and HPNA version of the Master and the Clients, if connected.



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

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** and wait for the software for the attached HPNA devices to be updated.

Wireless Station List

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

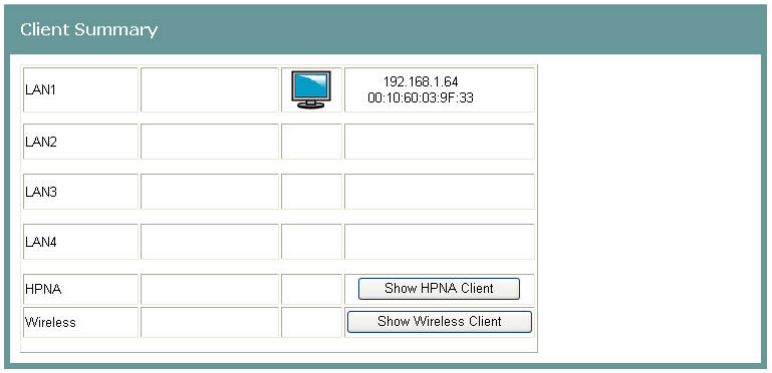
Path: Home Network > Summary > Show Wireless Client

Showing Attached Clients

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

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

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



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

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

WAN Quick Setup

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

Path: Home Network > WAN Setup > WAN Quick Setup

ETH WAN Config | WAN Setup

WAN Quick Setup

Wide Area Network (WAN) Setup

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

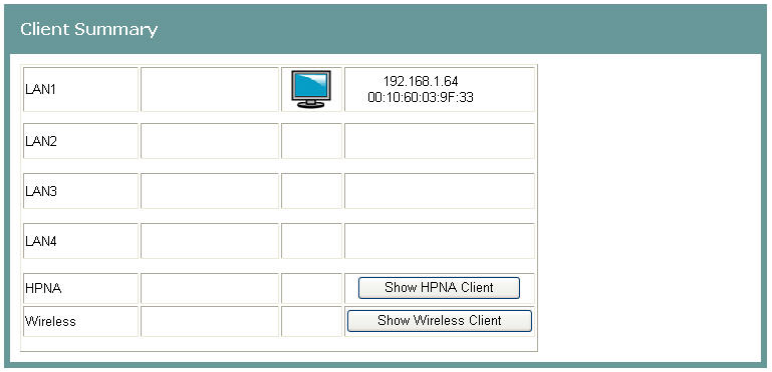
Port/Vpi/Vci	VLAN Mux	Category	Service	Interface	Protocol	IGMP	QoS	State	Remove	Edit
0/8/35	Off	UBR	mer_0_8_35	wanlink1-1-1(MER)	MER	Enabled	Disabled	Enabled	☐	Edit

Add Remove Reboot

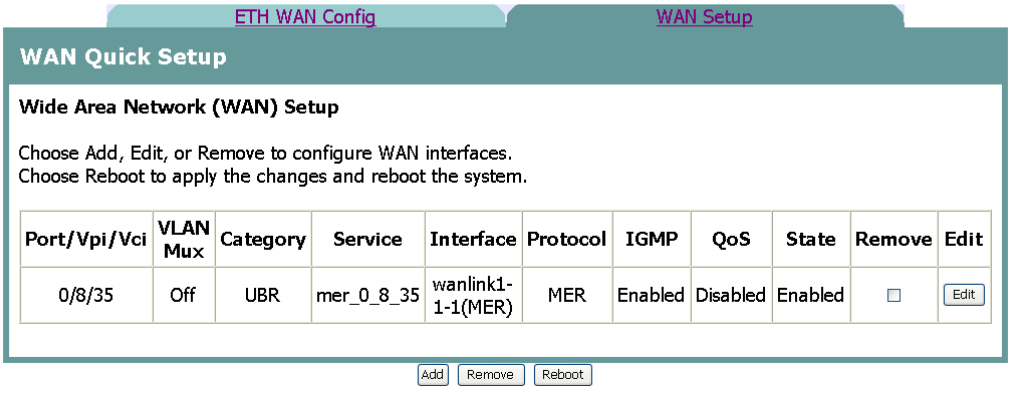
Configuring the WAN Interface (PPPoE Broadband Type)

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

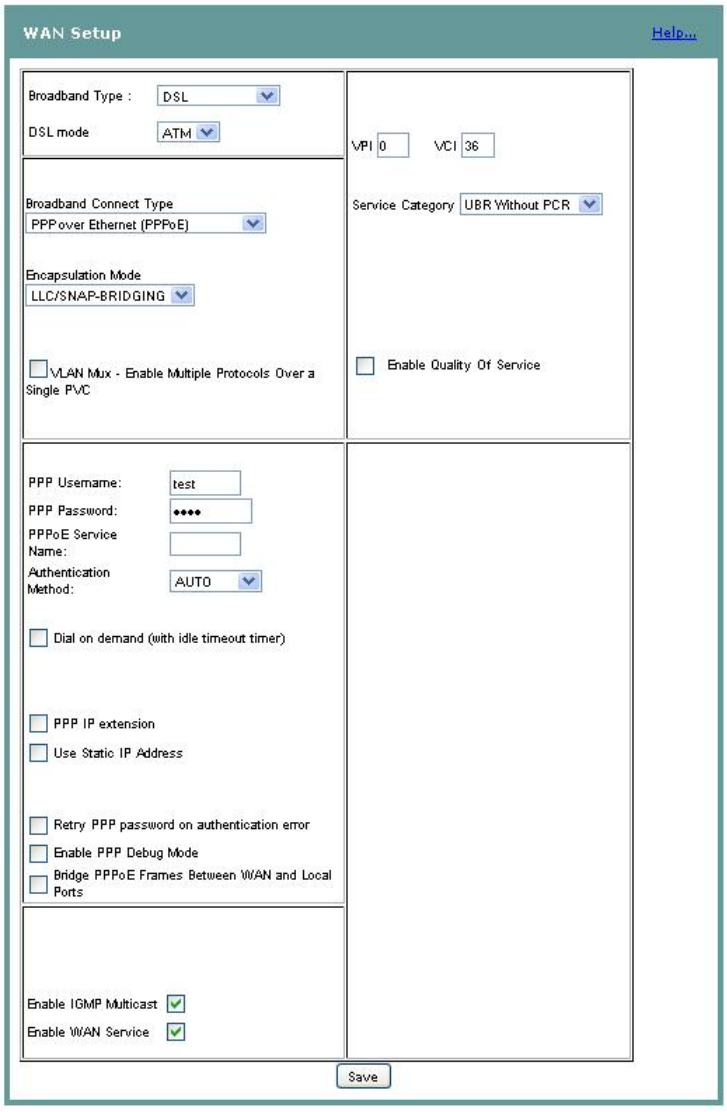
1 Click **Home Network** on the main screen. The Client Summary screen opens.



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



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



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

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

6 Complete the following fields on the screen as follows:

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

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, if applicable.

d In the PPP Username: field, enter the user name for the point-to-point protocol.

e In the PPP Password: field, enter the password for the point-to-point protocol.

f In the PPPoE Service Name: field, enter the name for the point-to-point over Ethernet service.

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

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

i In the Service Category field, select **ABRI Without PCR**.

j Check the **Enable Quality of Service** check box if applicable.

k In the Authentication Method field, select **AUTO**.

l Check **Enable NAT**.

m Check the **Enable IGMP Multicast** check box, if applicable.

n Check the **Enable WAN Service** check box.

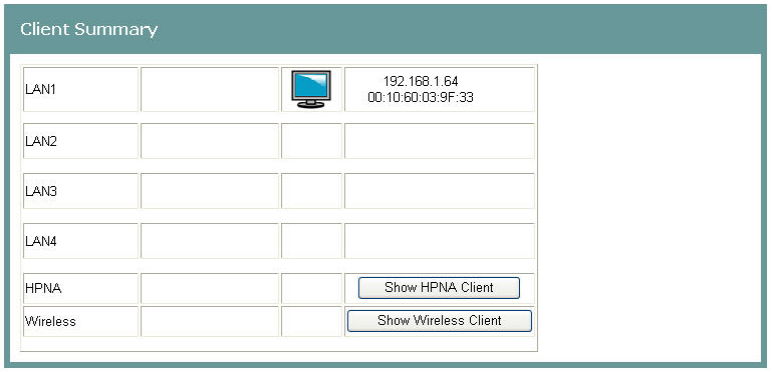
7 Click **Save** to save your settings.

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

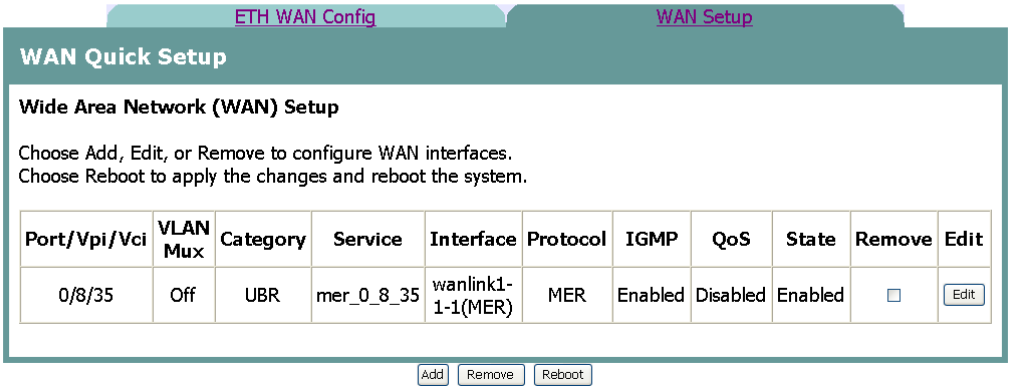
Configuring the WAN Interface (MER Broadband Type)

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

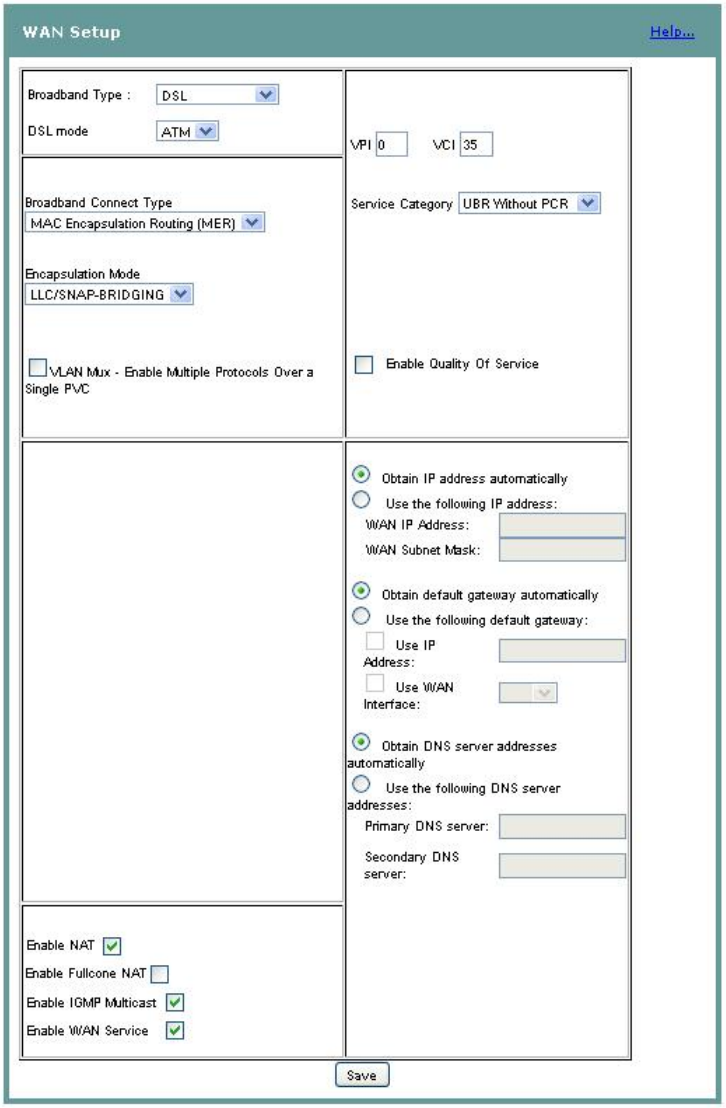
1 Click **Home Network** on the main screen. The Client Summary screen opens.



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



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



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, if applicable.
- **d** In the VLAN ID[0-4095]: field, enter an ID for the VLAN. Values are: 0 to 4095.
- **e** In the VPI field, enter the virtual path identifier (VPI). Values are: 0 to 65535.
- **f** In the VCI field, enter the virtual channel identifier (VCI). Values are: 0 to 65535.
- **g** In the Service Category field, select **UBR Without PCR**.
- **h** Select the **Enable Quality of Service** check box, if applicable.
- **i** Select the **Obtain an IP address automatically** option.
- **j** Select the **Obtain default gateway automatically** option.
- **k** Select the **Obtain DNS server addresses automatically** option.
- **l** Select **Enable NAT**.
- **m** Select the **Enable IGMP Multicast** check box.
- **n** Select the **Enable WAN Service** check box.

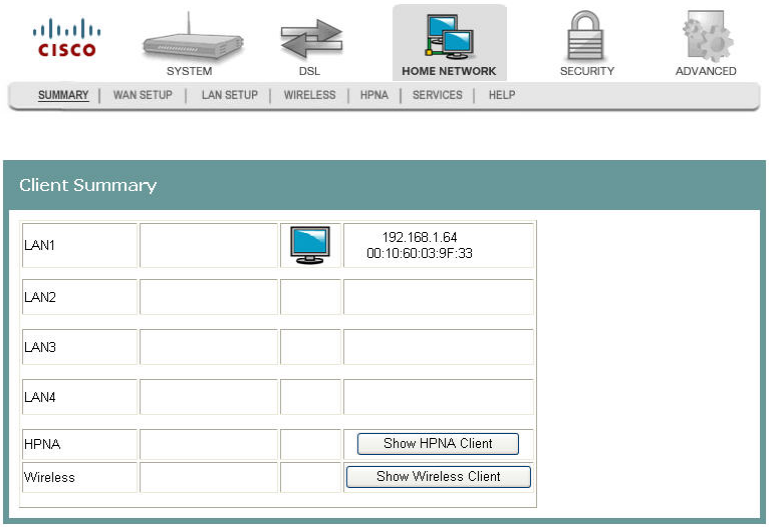
7 Click **Save**. The system returns to the previous screen.

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

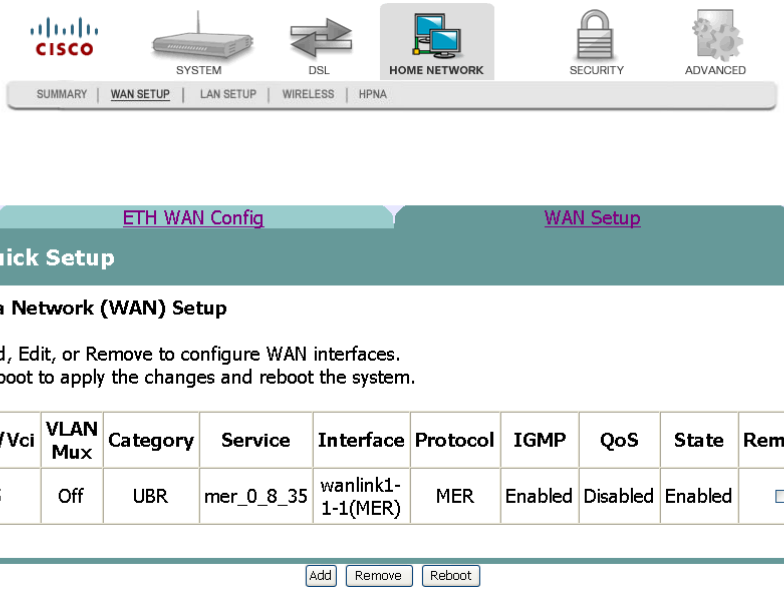
Configuring Ethernet WAN

To configure a WAN interface for Ethernet WAN (ETH-WAN) broadband type, complete the following steps.

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

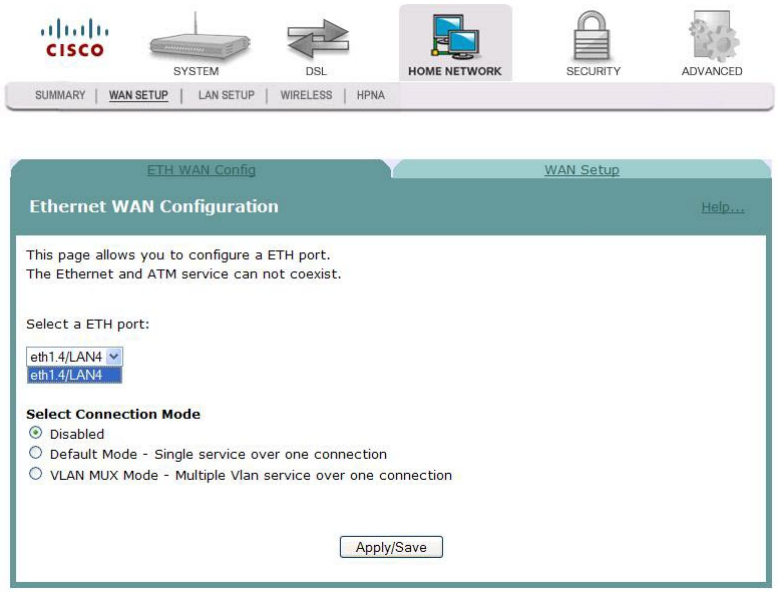


2 Click **WAN Setup.** The WAN Quick Setup screen opens.



3 On the WAN Quick Setup screen, check for any PVCs configured on a DSL connection. If any are listed, check the corresponding **Remove** box and then click the **Remove** button to remove them from the default DSL connection.

4 Click the **ETH WAN Config** tab. The Ethernet WAN Configuration screen opens. By default, LAN port 4 (eth1.4/LAN4) is chosen as the WAN port, and Ethernet WAN mode is disabled.



5 Select the appropriate connection mode as follows:

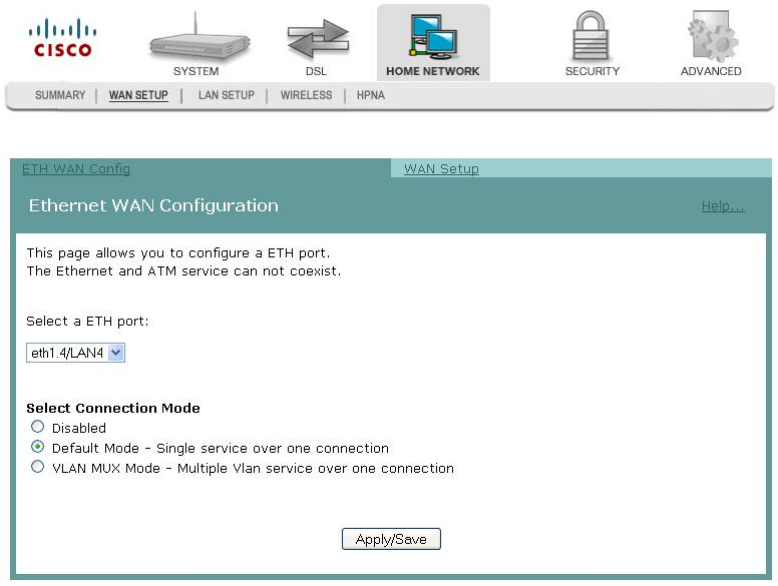
- Choose **Default Mode** if you have only a single service over the WAN interface (i.e., no VLANs)
- Choose **VLAN MUX Mode** if your service has multiple VLAN services over one connection.

6 Click **Save/Apply** to save your selection, and then continue with the appropriate settings below.

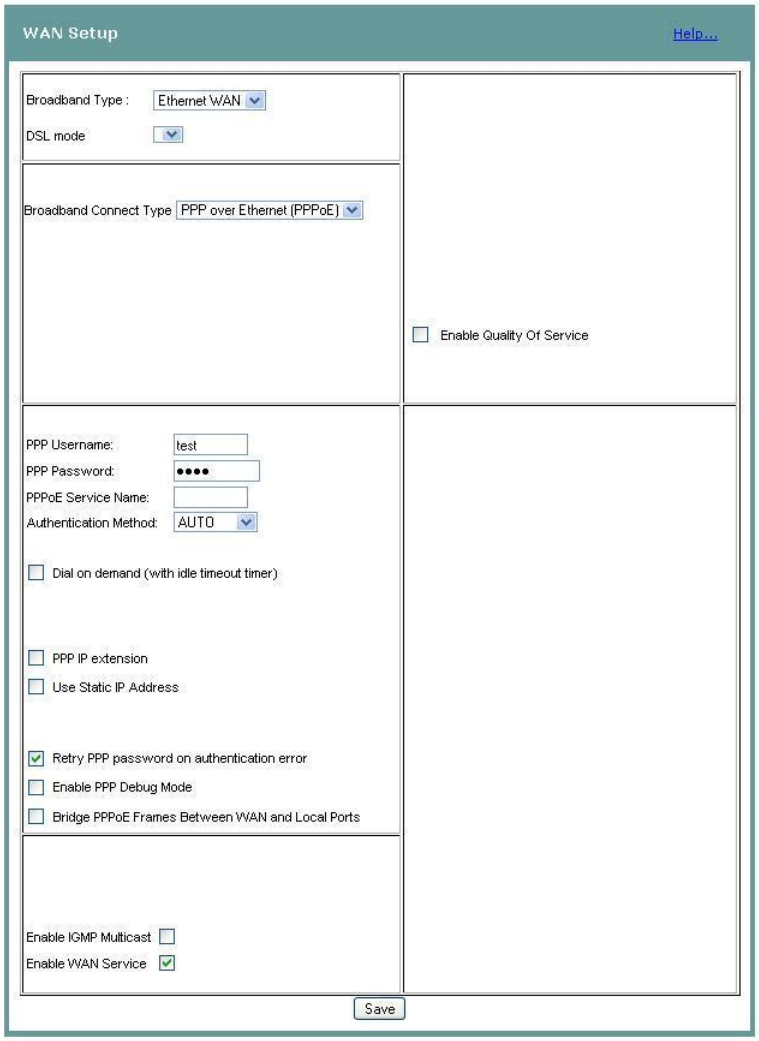
7 Repeat steps 1-6 above for any additional VLAN services that need to be added.

Settings for Default Connection Mode

If you select Default Mode as shown below, this service will have a single service over one connection (i.e., no VLANs).



1 Click the **WAN Setup** tab, and then click **Add** to set up a new WAN interface. The WAN Setup screen appears as shown below.



2 From the Broadband Connect Type drop-down list, choose the appropriate connection type: PPPoE (as in the example above), IPoE, or Bridging.

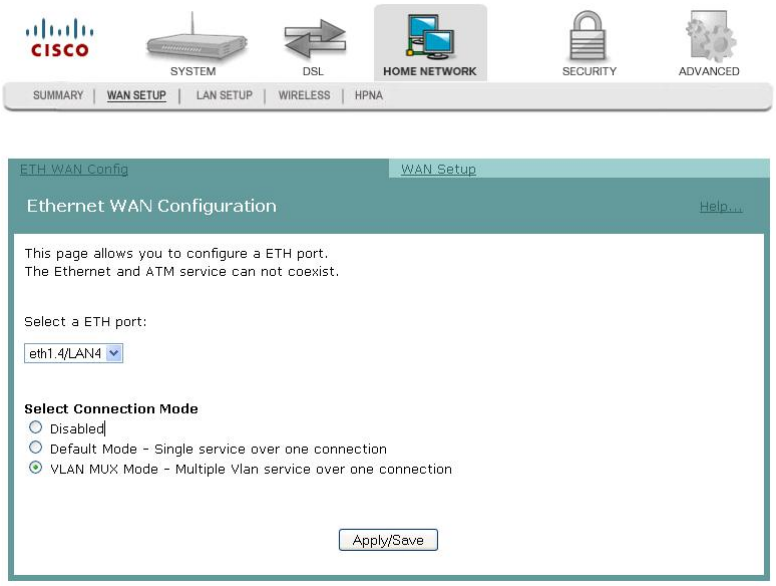
3 Configure the remaining credentials as appropriate for your WAN interface.

4 Check the **Enable WAN Service** check box at the bottom of the screen.

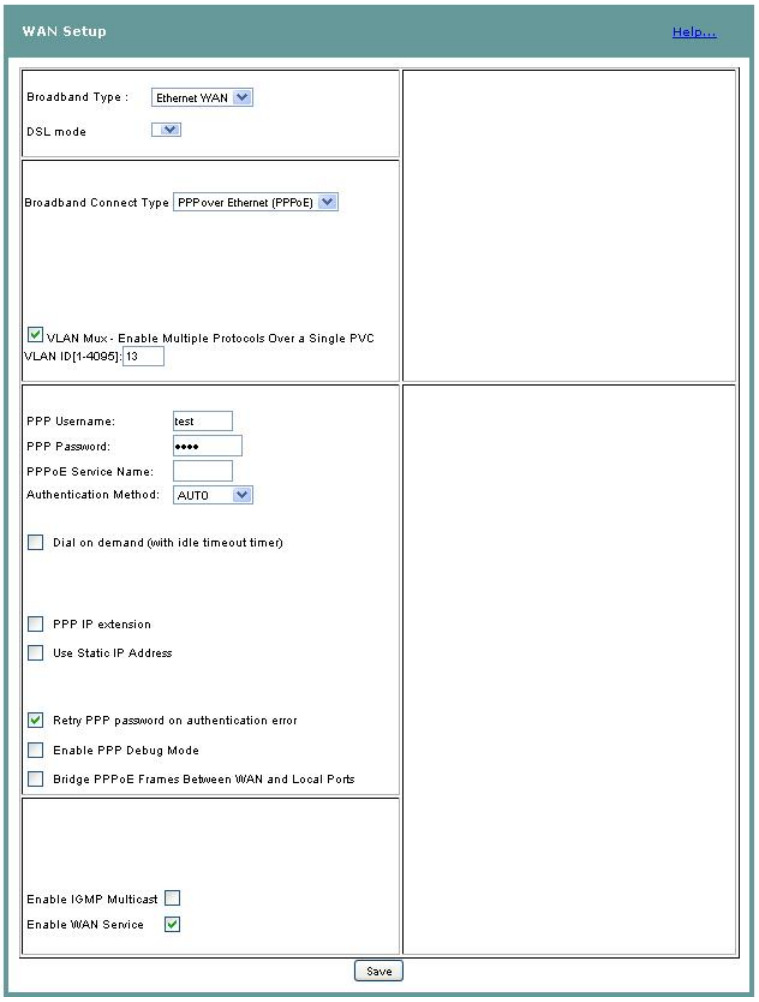
5 Click **Save** to save your settings.

Settings for VLAN MUX Mode

If you select VLAN MUX Mode as shown below, this service will have multiple VLAN services over one connection.



1 Click the **WAN Setup** tab, and then click **Add** to set up a new WAN interface. The WAN Setup screen appears as shown below.



2 From the Broadband Connect Type drop-down list, choose the appropriate connection type: PPPoE (as in the example above), IPoE, or Bridging.

3 Check the **VLAN Mux** checkbox, and then enter the VLAN ID used by your WAN interface.

4 Configure the remaining credentials as appropriate for your WAN interface.

5 Check the **Enable WAN Service** check box at the bottom of the screen.

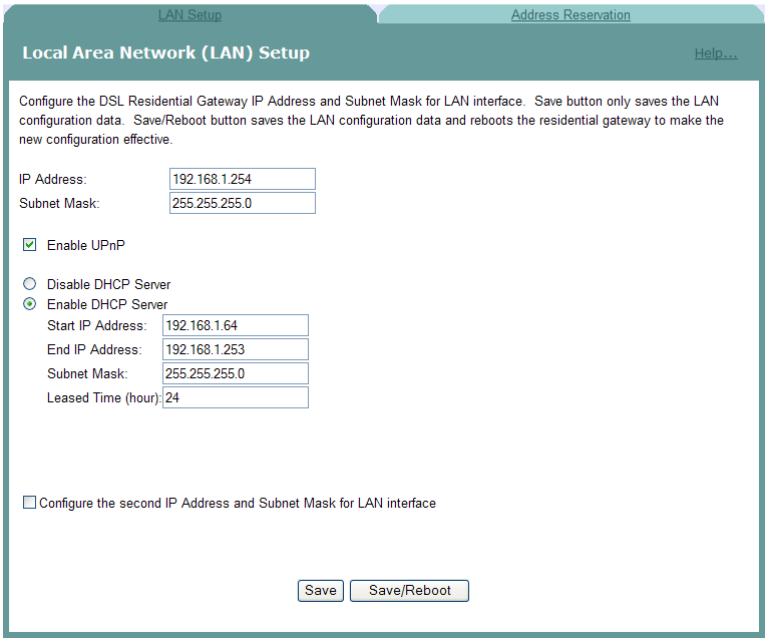
6 Click **Save** to save your settings.

7 Repeat steps 1-6 above for any additional VLAN services that need to be added.

LAN Setup

The Local Area Network (LAN) Setup screen allows users to set up LAN settings such as Dynamic Host Configuration Protocol (DHCP), Internet Gateway Multicast Protocol (IGMP), and Universal Plug and Play (UPnP).

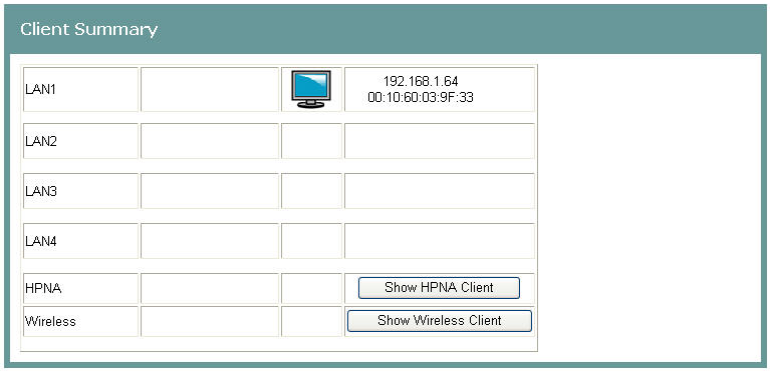
Path: Home Network > LAN Setup



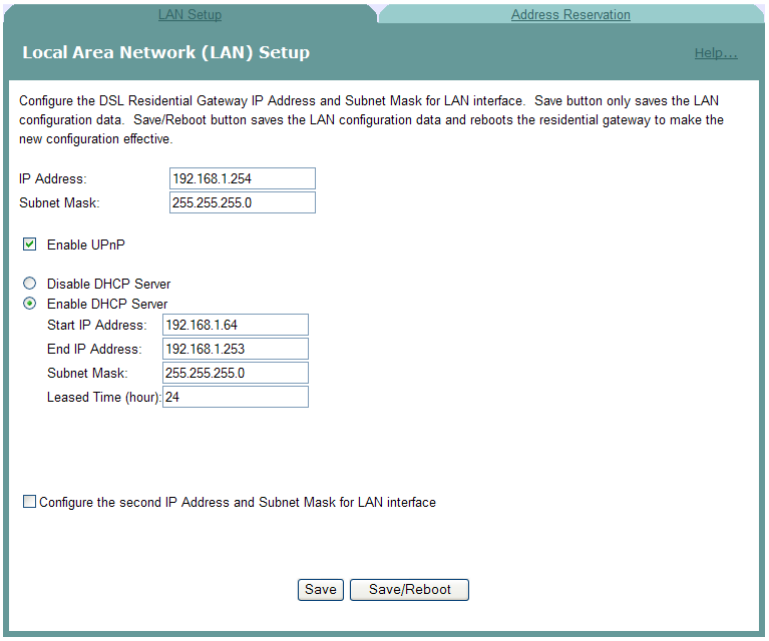
Configuring the LAN Interface

To configure the LAN interface, complete the following steps.

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



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



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

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

5 Do you want to enable UPnP?

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

6 Do you want to Enable the DHCP server?

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

7 Under Enable DHCP server, enter the following information:

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

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

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

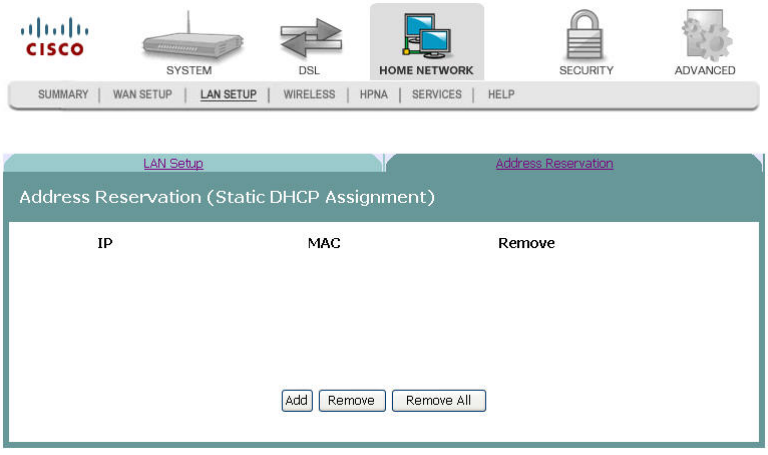
d In the Leased Time (hour) field, enter the duration of the DHCP lease address.

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

Reserving IP Addresses

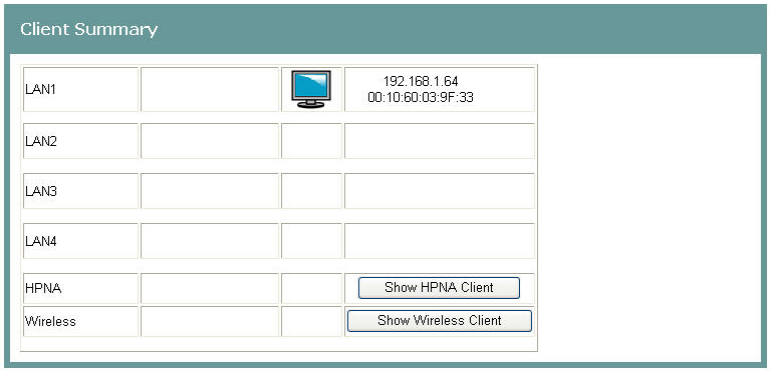
The Address Reservation screen allows you to reserve IP addresses for specific devices. For example, you can reserve IP addresses for your laptop or PC in your home.

Path: Home Network > LAN Setup > Address Reservation

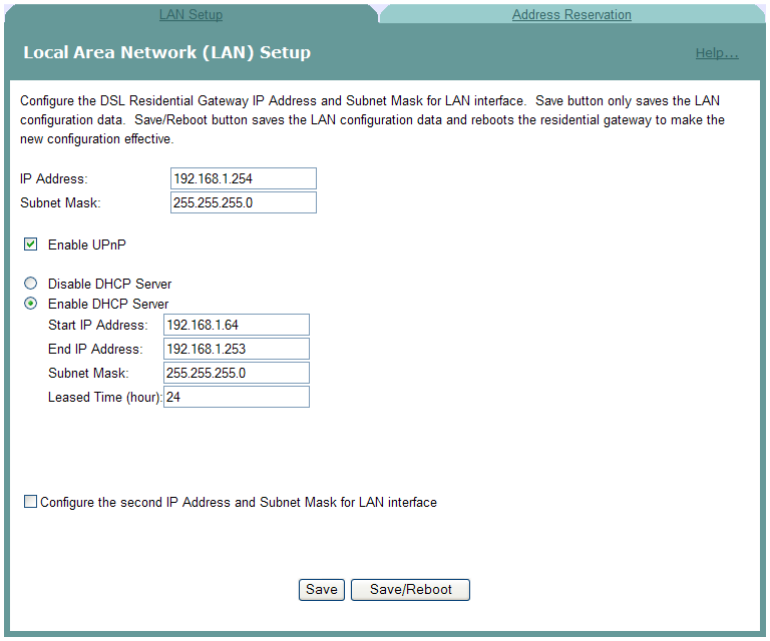


To reserve a specific IP address for a specific MAC address, complete the following steps.

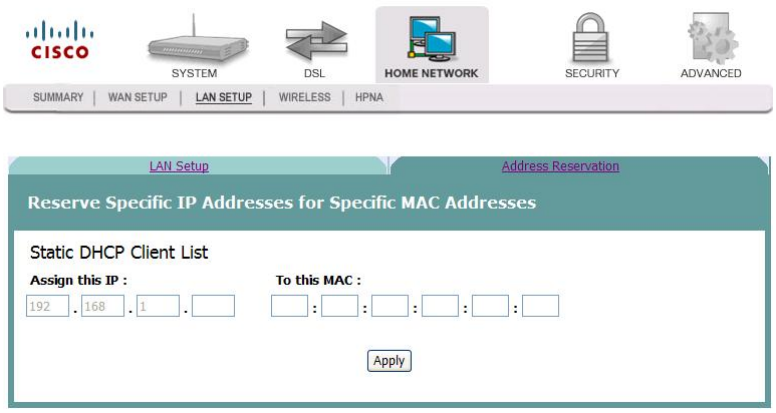
1 Click **Home Network** on the main screen. The Client Summary screen opens.



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



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



4 In the Assign this IP field, enter the IP address you want to assign to the MAC address.

5 In the To this MAC field, enter the MAC address to which you want to assign the IP address.

6 Click **Save** to save your settings.

Configuring a Second LAN IP Address

If needed, complete the following steps to configure a second LAN IP address on the gateway.

1 Click the check-box labeled **Configure the second IP Address and Subnet Mask for LAN Interface**.

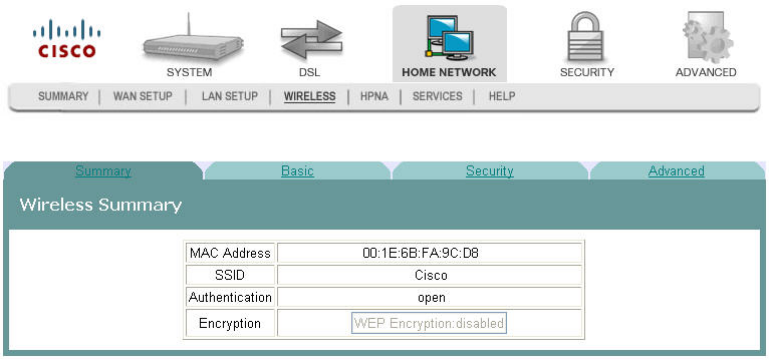
2 In the fields provided, type the IP Address and Subnet Mask for the second IP address.

3 Click **Save/Reboot** for the changes to take effect.

Wireless Summary

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

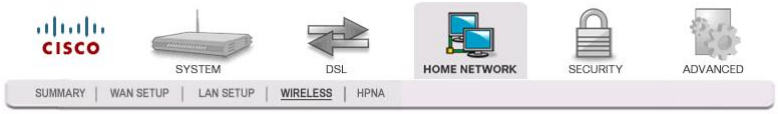
Path: Home Network > Wireless > Summary

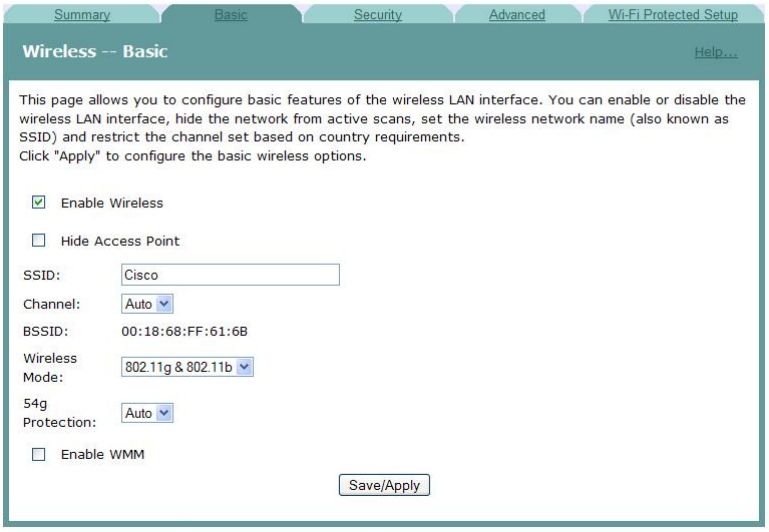


Wireless Basic

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

Path: Home Network > Wireless > Basic

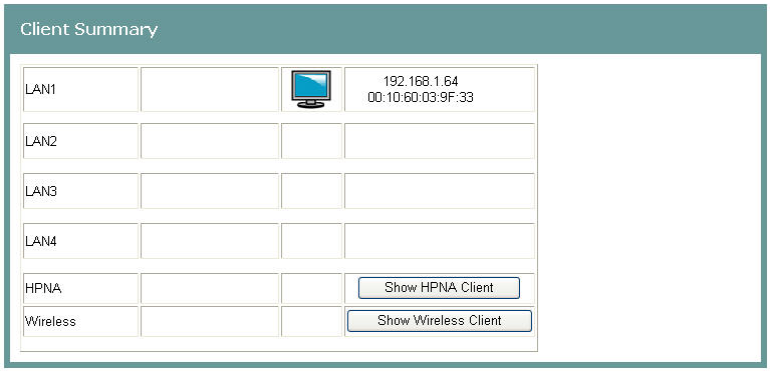




Enabling the Wireless Network

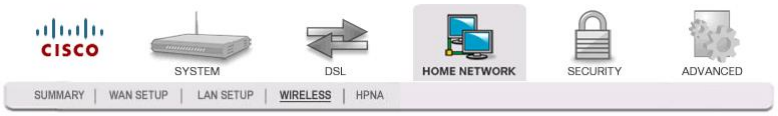
To enable the wireless network, complete the following steps.

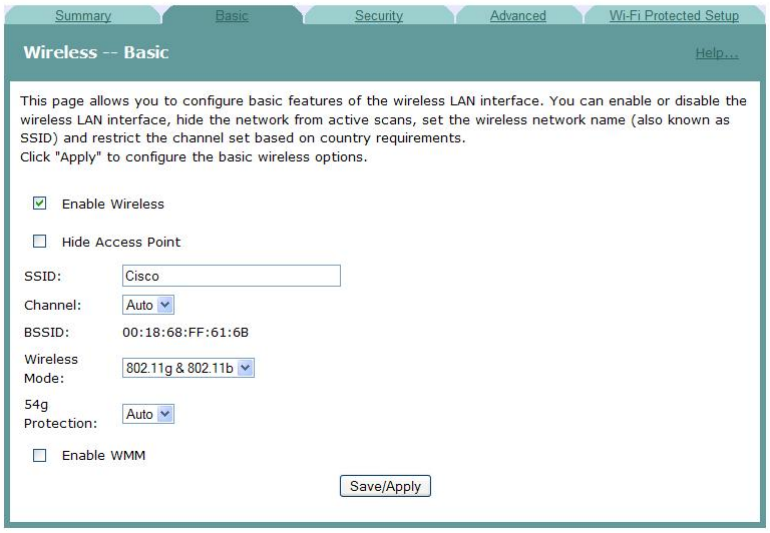
1 Click **Home Network** on the main screen. The Client Summary screen opens.



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

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





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 an 802.11b device may need to use your wireless network.

Notes:

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

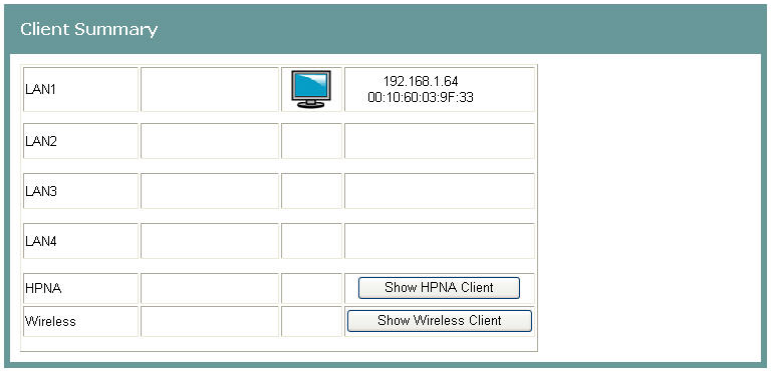
10 Click **Save/Apply** to enable the wireless network.

Securing Your Wireless Network with WEP

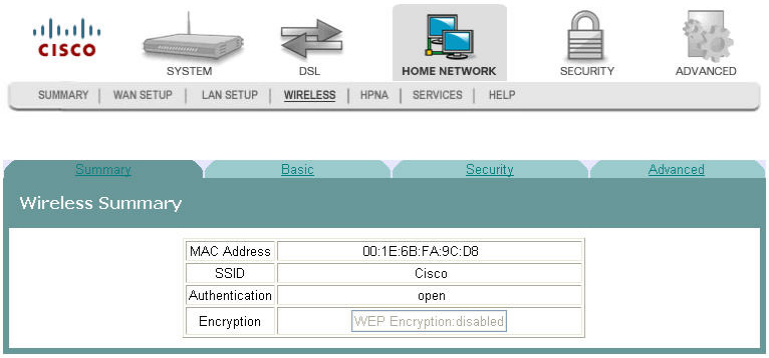
WEP is a security protocol for wireless networks. WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. A shared key (similar to a password) is used to allow communication between the computers and the residential gateway.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

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

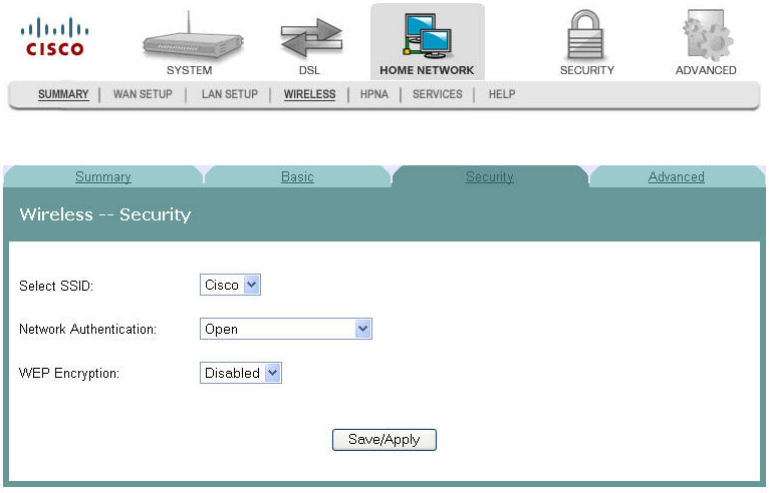
1 Click **Home Network** on the main screen. The Client Summary screen opens.



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



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



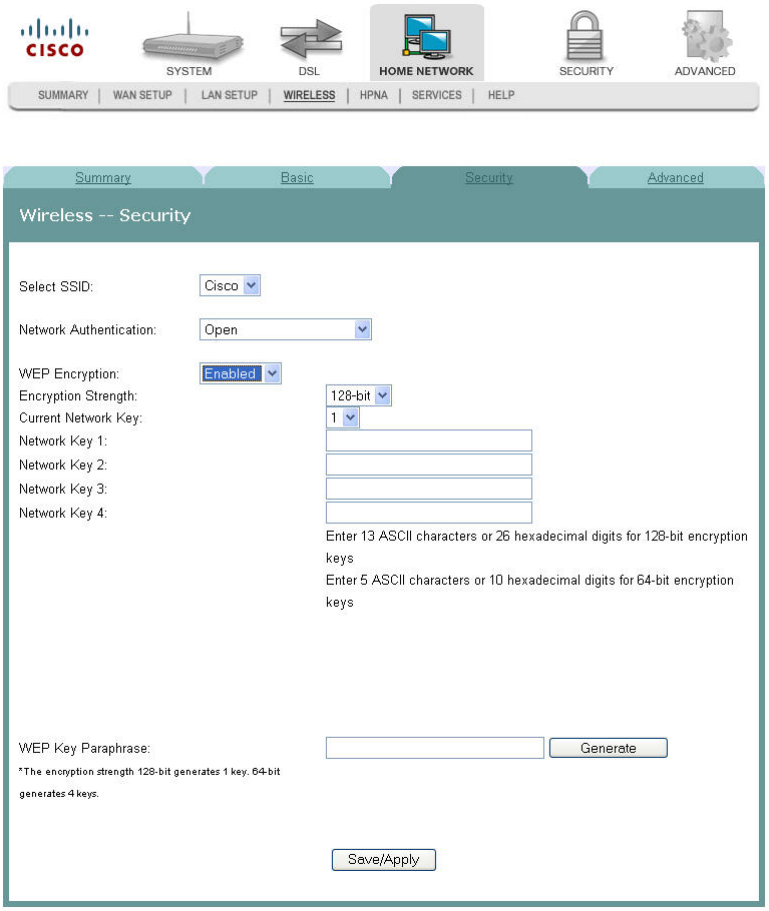
4 In the **Select SSID** field, use the drop-down list to choose an option for the service set identifier (SSID).

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

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

- Open. All devices may access the wireless network when WEP Encryption is disabled. When no authentication is required and if encryption is disabled, then the data that is passing between the access point and the client is also not encrypted. When WEP is enabled, the data is encrypted, but the client is not authenticated.
- 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.



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

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

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

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

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

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

10 In the Network Key 1 field, enter the network key you wish to you use based on the encryption strength as discussed in step 7.

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

- For 64-bit encryption, you can choose to enable Serial Number Encryption. When you enable Serial Number Encryption, the serial number of the gateway is preceded with a 0 (numeric zero) and is then used as the Network Key. Serial Number Encryption is not available for 128-bit encryption. If you don't want to use Serial Number Encryption (64 bit only), disable it by selecting Disabled from the drop-down list. Repeat steps 9 and 10 for keys 1 through 4 if you use 64-bit encryption. Go to step 12.
- For 128-bit encryption, only one network key is used. Go to step 12.

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

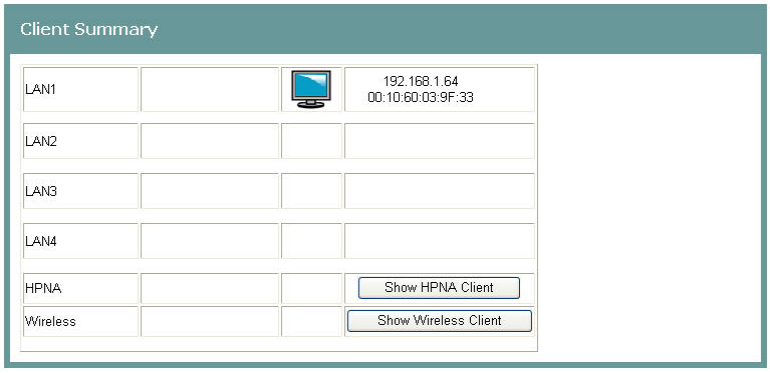
- For 64-bit encryption strength, enter a passphrase (1 to 31 characters) and click **Generate**. Four keys are generated based on the passphrase.
- For 128-bit encryption, enter a passphrase (1 to 31 characters) and click **Generate**. Four keys are generated based on the passphrase.

13 Click **Save/Apply**.

Disabling the Wireless Network

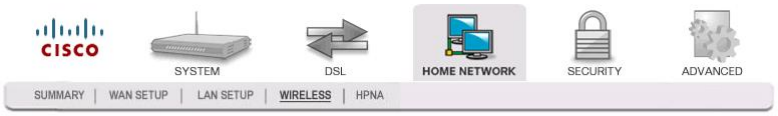
To disable the wireless network, complete the following steps.

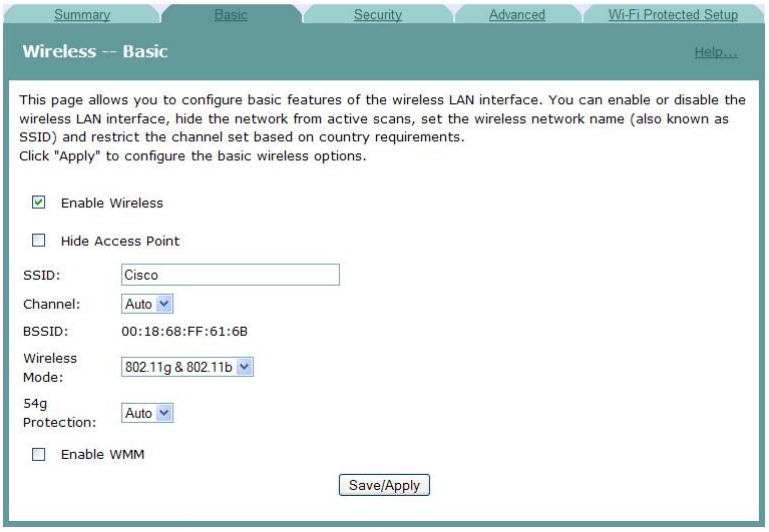
1 Click **Home Network** on the main screen. The Client Summary screen opens.



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

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





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

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

Wireless Security

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

Path: Home Network > Wireless > Security

WEP Encryption Disabled

Securing Your Wireless Network with Encryption Keys

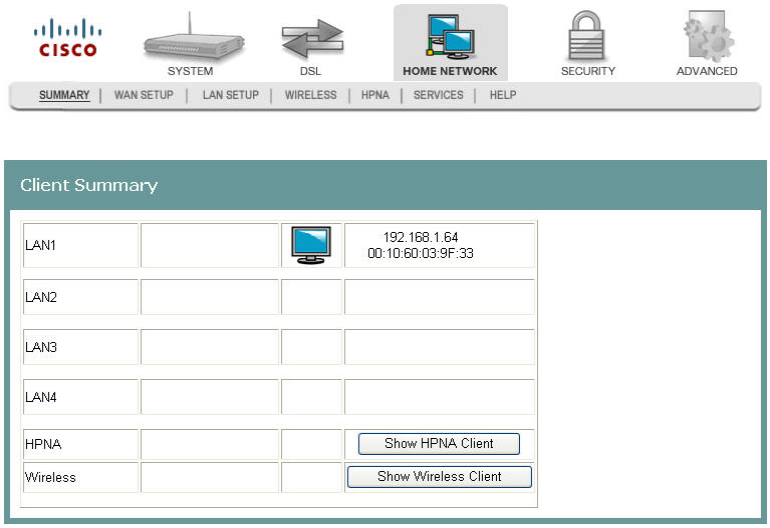
If you choose WPA Personal (also known as Wi-Fi Protected Access-PreShared Key) as the network authentication method, you can secure your network by encrypting all traffic using a pre-shared dynamic key. The following security methods are described:

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

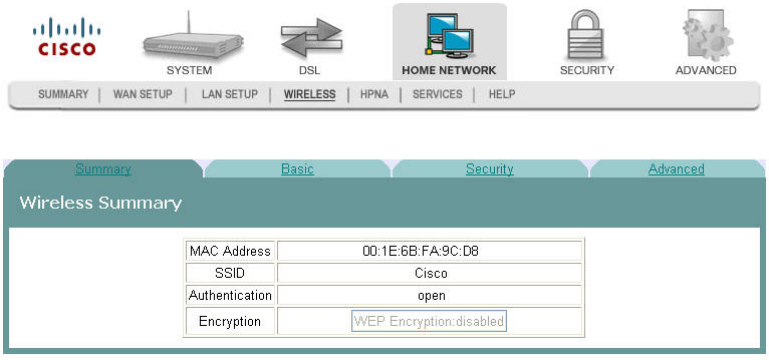
WPA Personal or WPA2 Personal

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

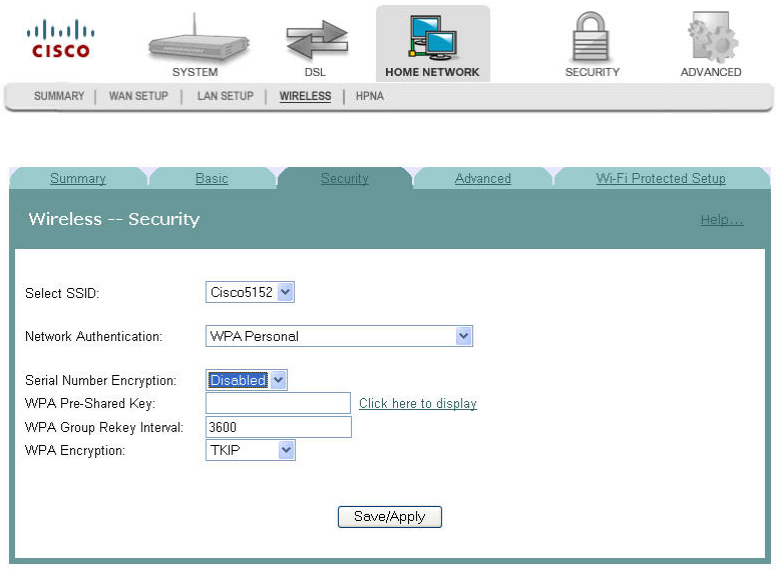
1 Click **Home Network** on the main screen. The Client Summary screen opens.



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



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



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

5 Select **Enabled or Disabled** to enable or disable your Serial Number Encryption function. Your serial number is printed on the back label of your device. If you enable this function, the system will automatically use your serial number as the pre-shared key for WPA Authentication.

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

7 In the WPA Group Rekey Interval field, enter the group key renewal time period (in seconds). This time defines how often the dynamic key is regenerated

8 In the WPA Encryption field, select the encryption from the drop-down list. You have the option of choosing TKIP (Temporal Key Integrity Protocol), AES (Advanced Encryption System), or both. Typically AES is seen to be a more reliable form of encryption.

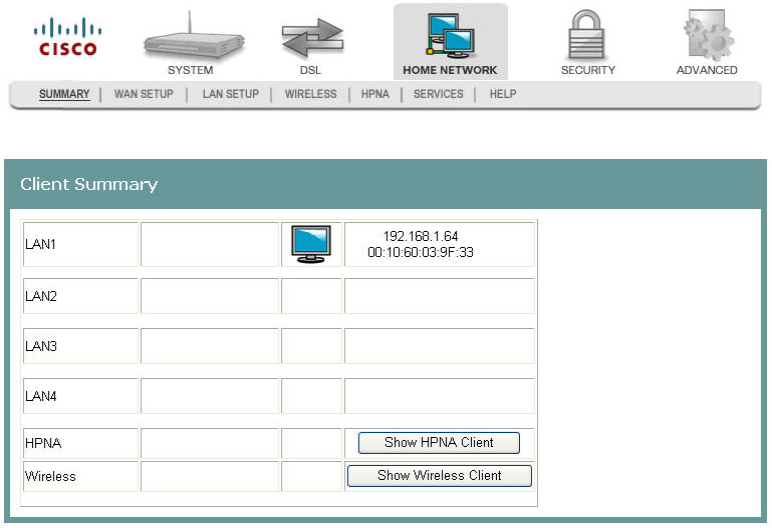
9 Click **Save/Apply** to save your settings.

Mixed WPA2 Personal/WPA Personal

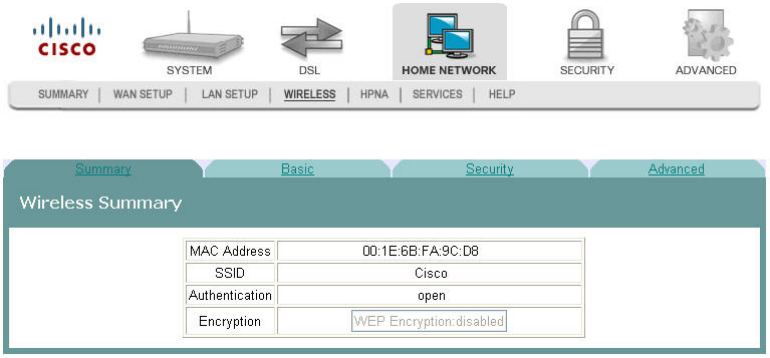
The security mode supports simultaneous WPA Personal and WPA2 Personal connections. You can have devices that use either WPA Personal or WPA2 Personal. The access point automatically chooses the encryption algorithm used by each client device.

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

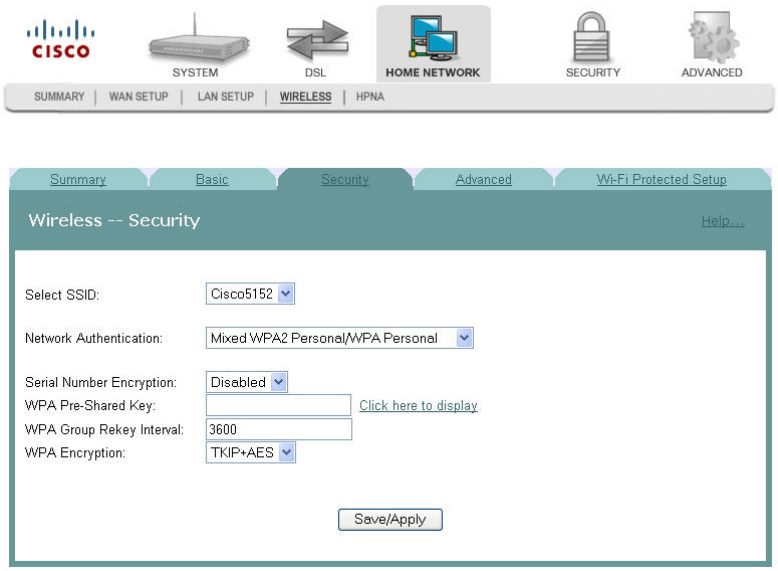
1 Click **Home Network** on the main screen. The Client Summary screen opens.



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



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



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

5 Select **Enabled** or **Disabled** to enable or disable your Serial Number Encryption function. Your serial number will be printed on the back label of your device. If you enable this function, the system will automatically use your serial number as the network key for your WEP encryption.

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

7 In the WPA Group Rekey Interval field, enter the group key renewal time period (in seconds). This time defines how often the dynamic key is regenerated

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

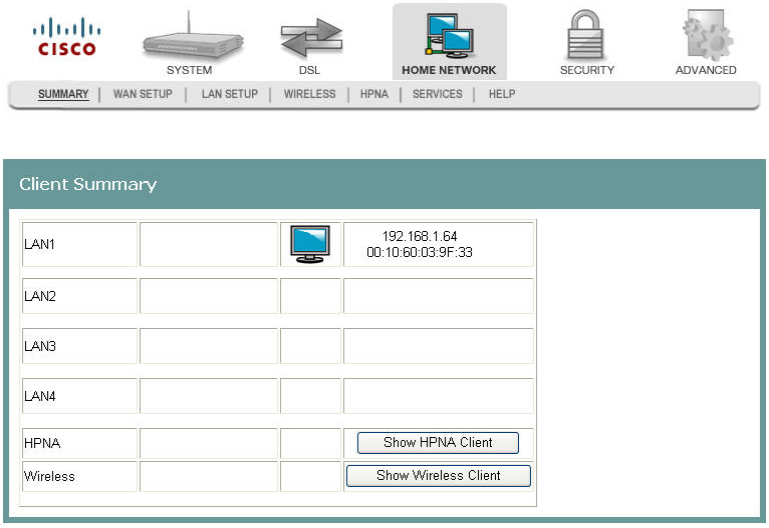
9 Click **Save/Apply** to save your settings.

WPA/WPA2 Enterprise

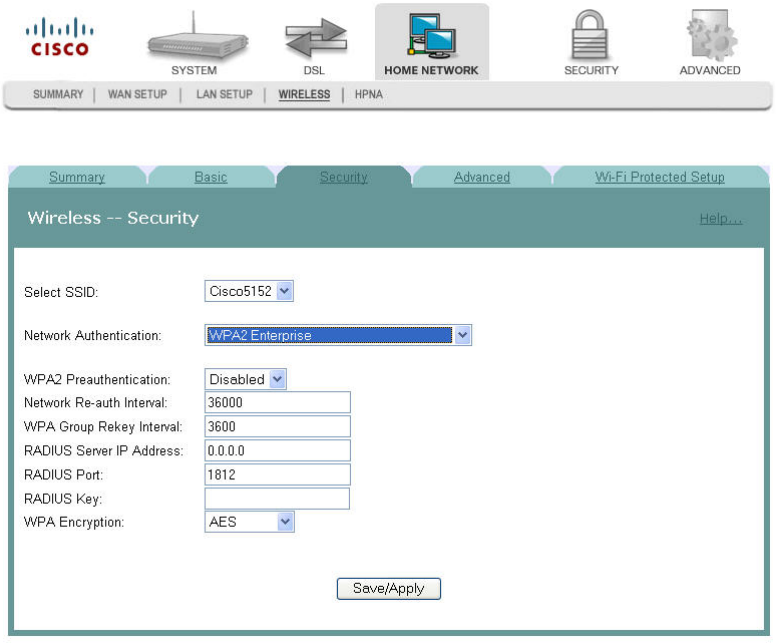
WPA/WPA2 Enterprise is used in coordination with a Remote Authentication Dial-In Use Service (RADIUS) server for client authentication. If you choose this to be your authentication method, make sure that a RADIUS server is available in the network for authentication.

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

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



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



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

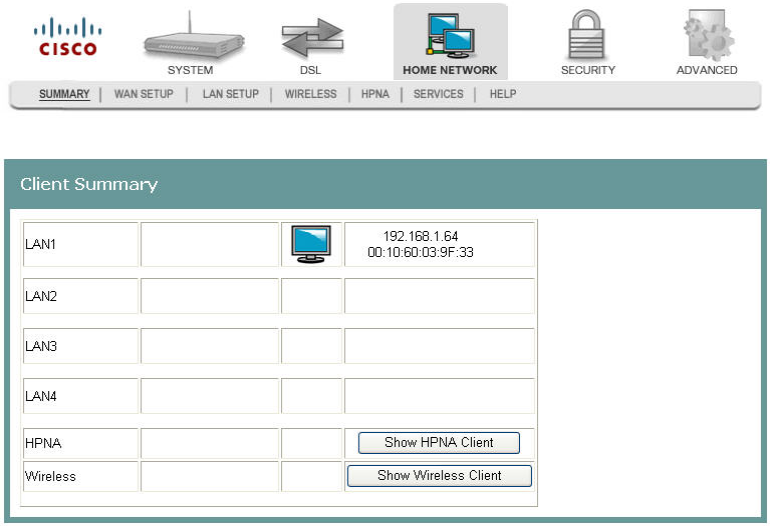
   Note: In pre-authentication, a WPA2 wireless client can perform an 802.1X authentication with other wireless access points in its range when it is still connected to its current wireless access point.
5. In the Network Re-auth Interval, enter the interval at which the re-authentication occurs.
6. In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

Mixed WPA/WPA2 Enterprise

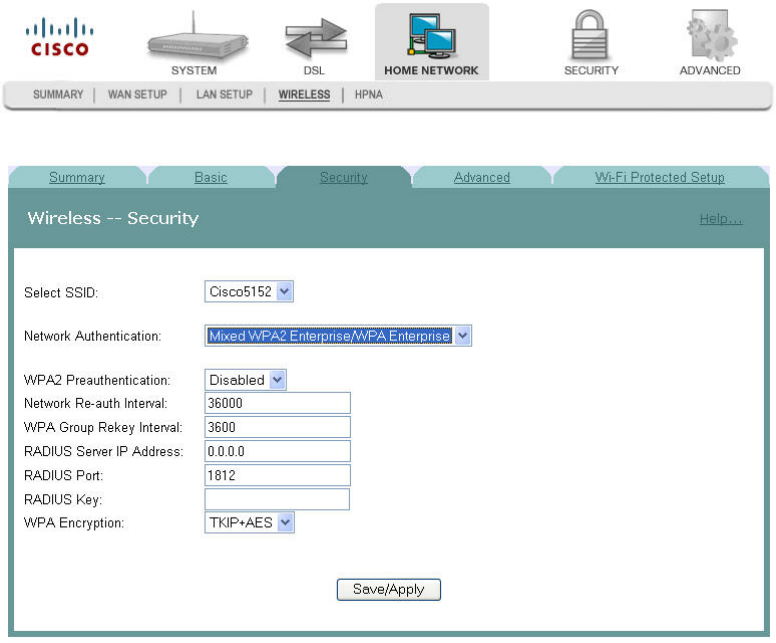
The security mode supports simultaneous WPA Enterprise and WPA2 Enterprise connections. You can have devices that use either WPA Enterprise or WPA2 Enterprise. The access point automatically chooses the encryption algorithm used by each client device.

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

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



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



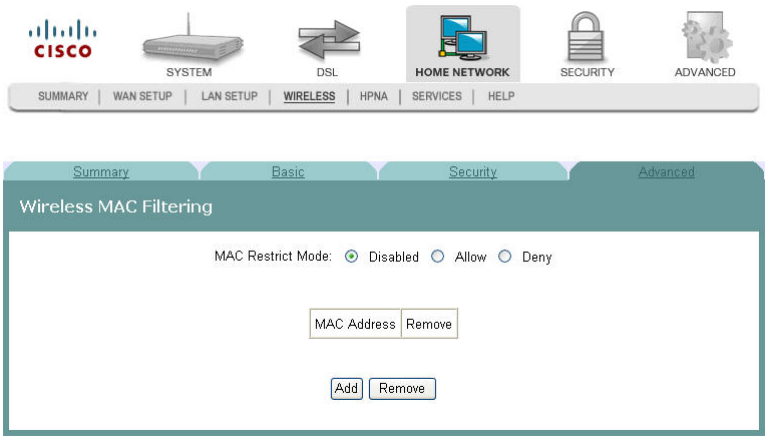
3. In the Network Authentication field, select **Mixed WPA2 Enterprise/WPA Enterprise** from the drop-down list.
4. Select **Enabled** or **Disabled** for your WPA2 Pre-authentication.

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

Wireless MAC Filtering

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

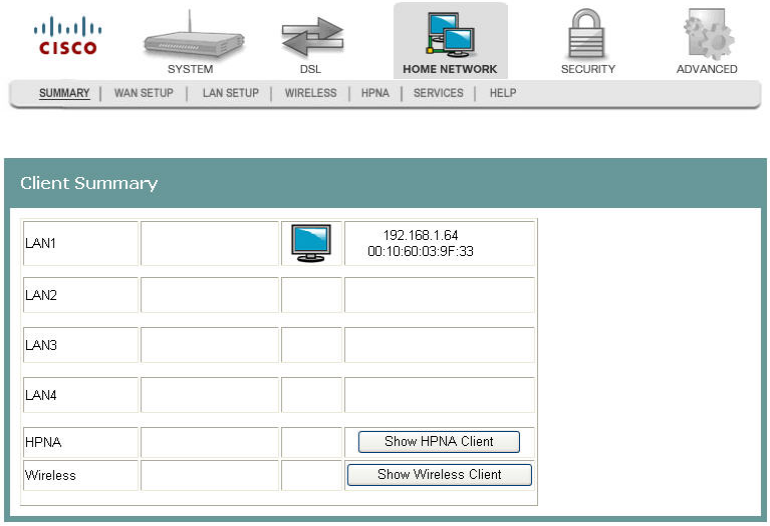
Path: Home Network > Wireless > Advanced > MAC Filter



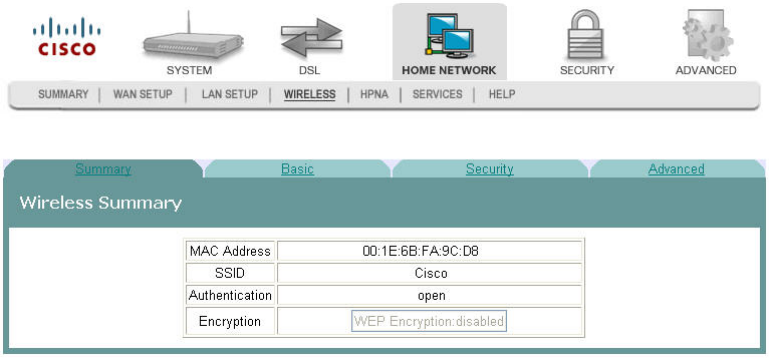
Allowing Wireless Clients to Access the Residential Gateway

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

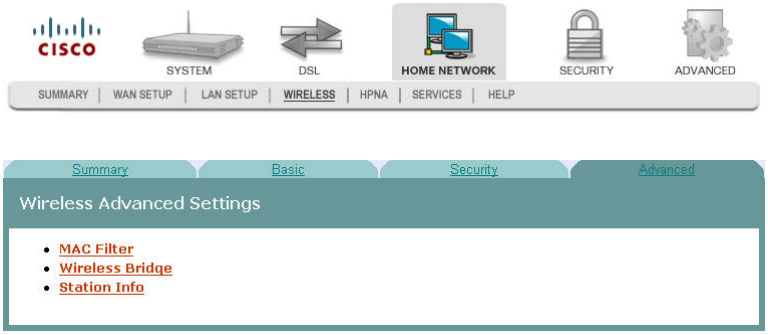
1 Click **Home Network** on the main screen. The Client Summary screen opens.



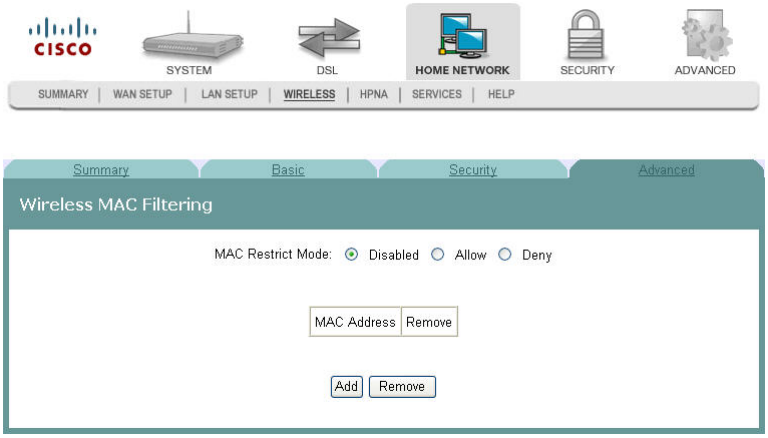
2 Click **Wireless.** The Wireless Summary screen opens.



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



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



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

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

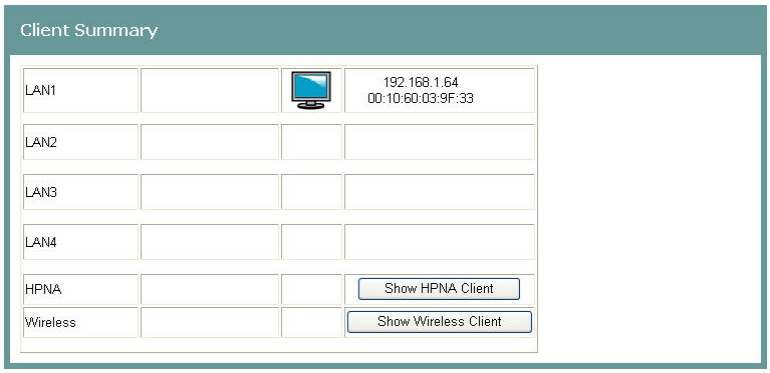
7 In the MAC Address field, enter the MAC address of the client that you want to allow access to the residential gateway.

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

Blocking Wireless Clients

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

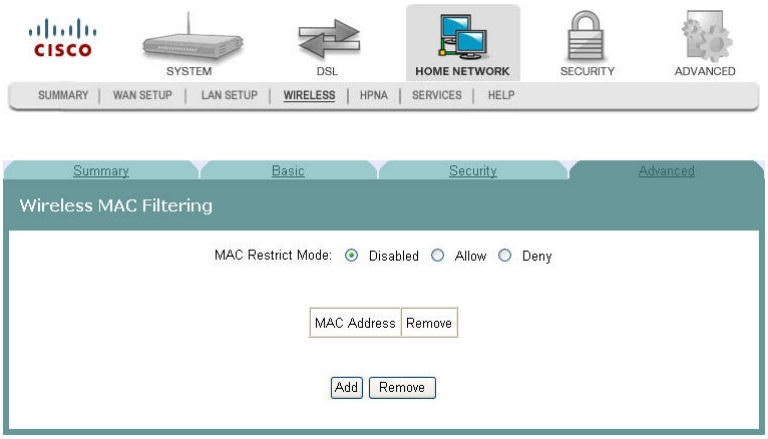
1 Click **Home Network** on the main screen. The Client Summary screen opens.



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

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

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



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

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

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

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

Wireless Bridge

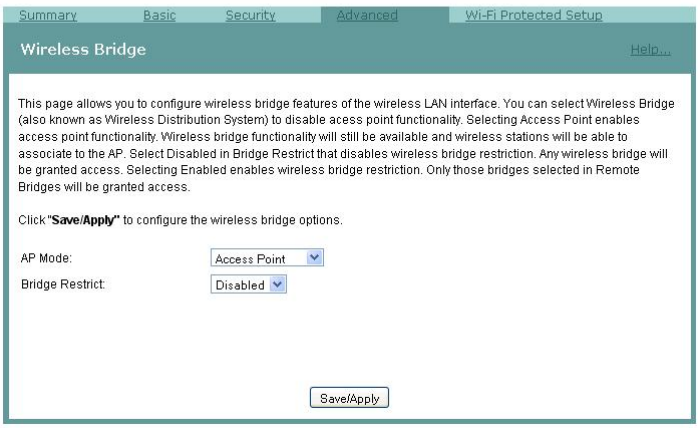
Wireless LAN Bridging (also referred to as a Wireless Distribution System, WDS) refers to two or more 802.11 access points that send traffic between them (from access point to access point) as opposed to between access point and a client computer.

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

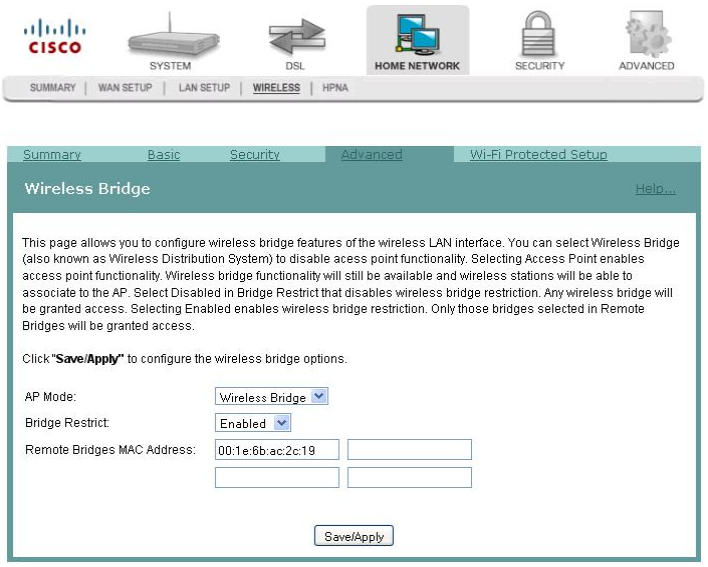
- Select Wireless Bridge in the AP mode to disable access point functionality.
- Select Access Point in the AP mode to enable access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
- Select Disabled in the Bridge Restrict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

Path: Home Network > Wireless > Advanced > Wireless Bridge

Bridge Restrict Disabled



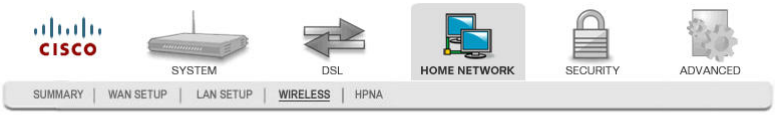
Bridge Restrict Enabled

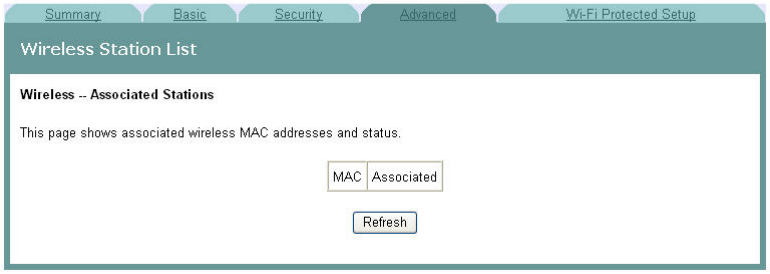


Wireless Station List

This page shows associated wireless MAC addresses and status.

Path: Home Network > Wireless > Advanced > Station Info





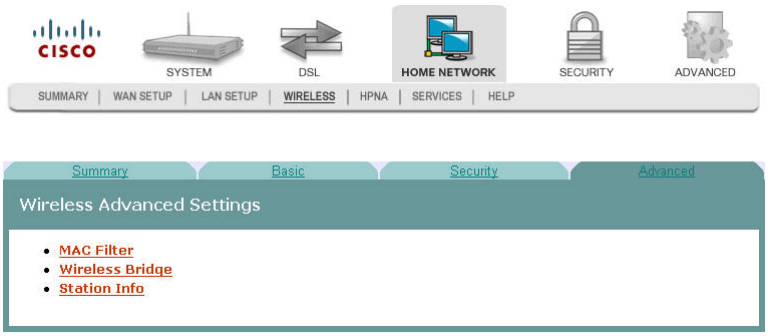
Showing MAC Addresses and Clients

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

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

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

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



4 Click **Station Info**. The Wireless Station List opens.

5 Click **Refresh** to update the list of MAC addresses and associated status.

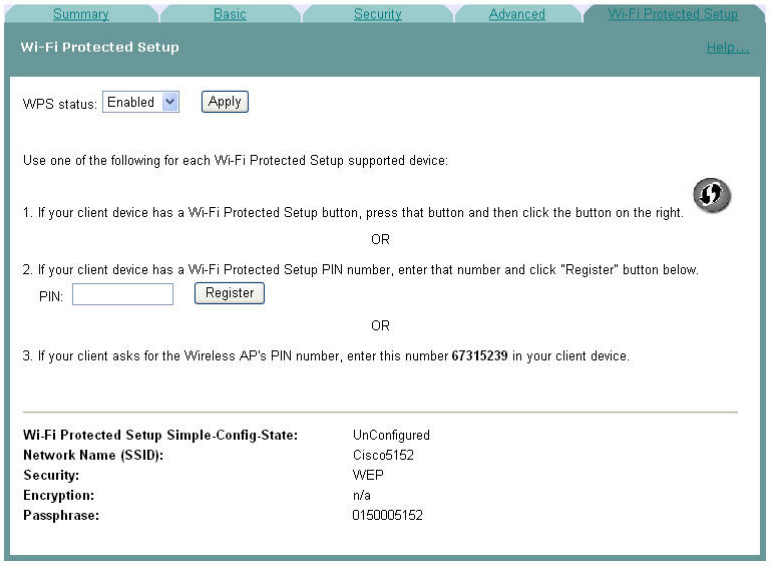
Wi-Fi Protected Setup

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

You can choose to use either the PBC or PIN method for connecting the wireless networks using WPS. But first, you will still need to configure the appropriate authentication on your router. For more information, see ***Security Configuration*** (on page 165).

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

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



PBC Method

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

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

1. Click **Home Network** on the main screen.
2. Click **Wi-Fi Protected Setup**. The Wi-Fi Protected Setup screen opens.
3. For the WPS status drop-down field, select **Enabled** to enable the WPS status.
4. Click the button at the right-hand-side on the page or the Wi-Fi-sec button on the device. Then, within 2 minutes, push another button on your client adapter's WPS setup screen. It should start the process of configuring the wireless security on your client station.

PIN Method

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

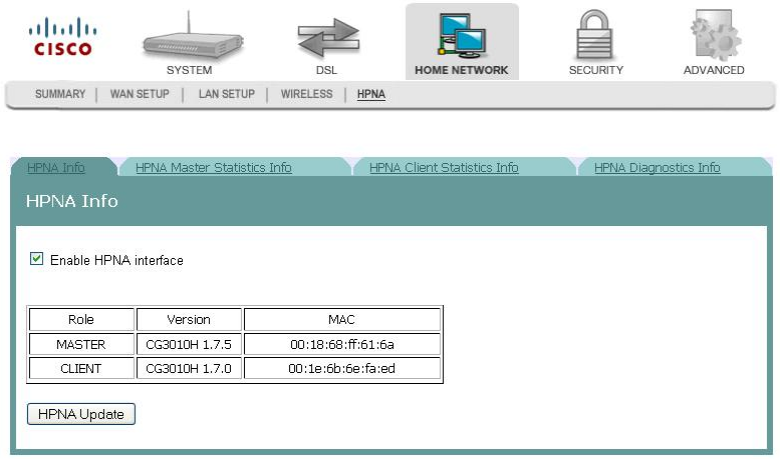
To set up your wireless network using a PIN:

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

HPNA Information

The HPNA Info screen allows you to view the HPNA devices connected to the residential gateway and to examine statistics for these devices.

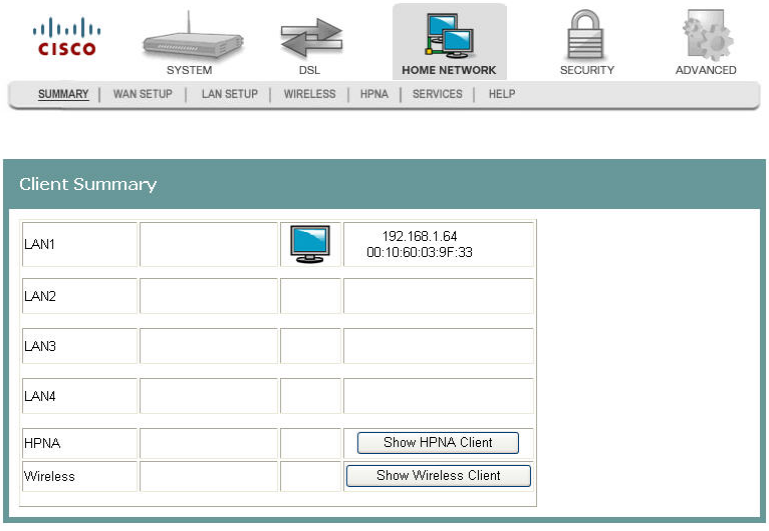
Path: Home Network > HPNA > HPNA Info



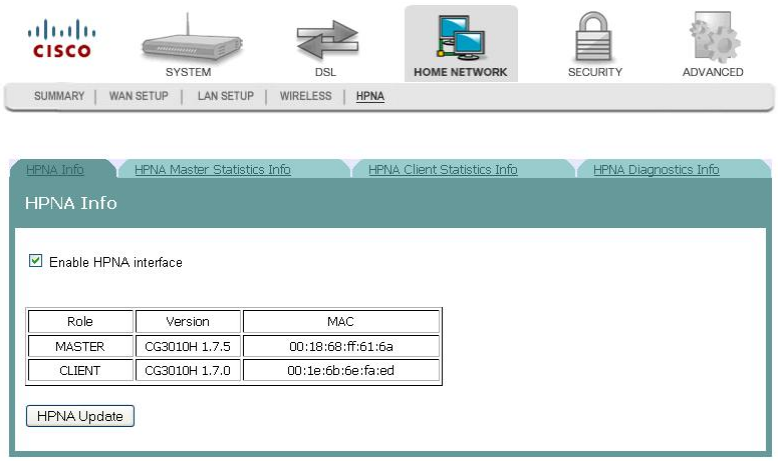
Updating HPNA Information

To update the HPNA information, complete the following steps.

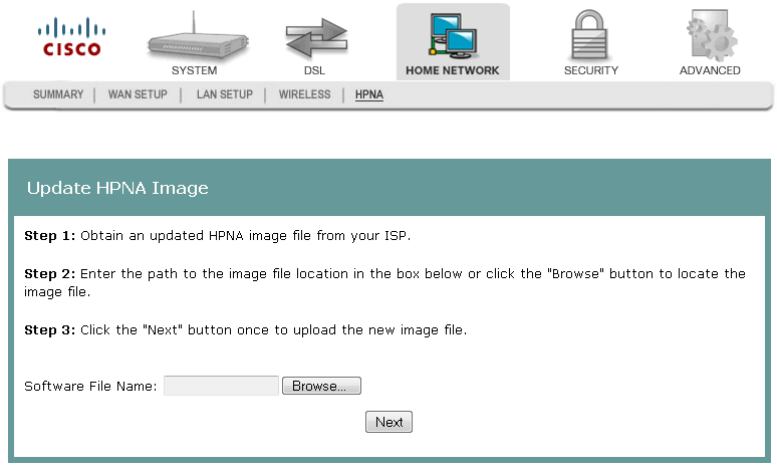
1 Click **Home Network** on the main screen. The Client Summary screen opens.



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



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



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

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

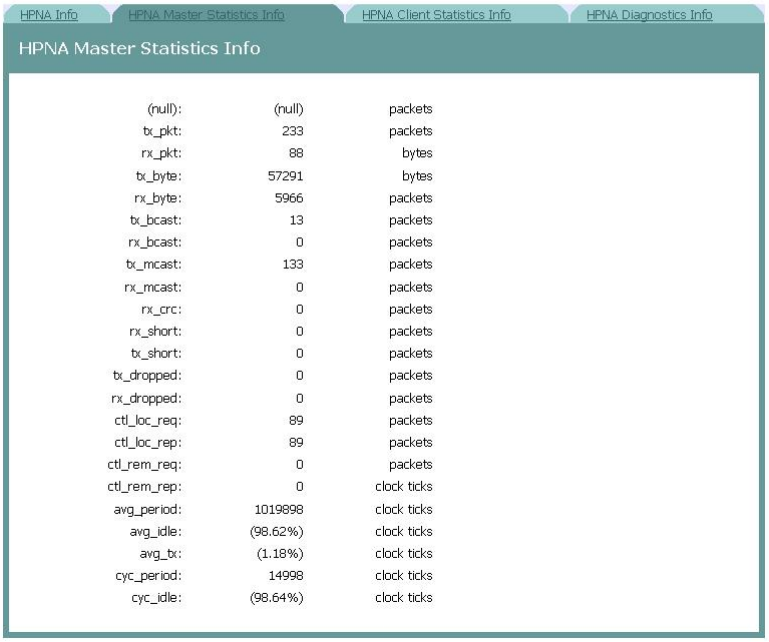
Viewing HPNA Statistics

From the HPNA Info screen, you can choose the HPNA Master Statistics Info, HPNA Client Statistics Info, or HPNA Diagnostics Info tab.

HPNA Master Statistics Info

The HPNA Master Statistics Info screen displays the master statistics for the HPNA connection, such as the number of packets transmitted, received, and dropped.

Path: Home Network > HPNA > HPNA Master Statistics Info

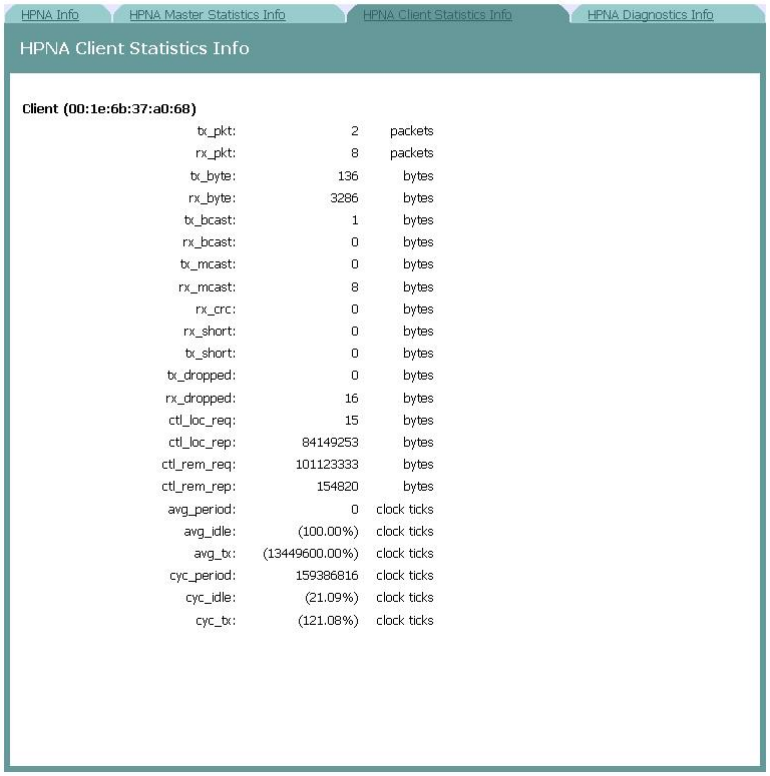


(null):	(null)	packets
tx_pkt:	233	packets
rx_pkt:	88	bytes
tx_byte:	57291	bytes
rx_byte:	5966	packets
tx_bcast:	13	packets
rx_bcast:	0	packets
tx_mcast:	133	packets
rx_mcast:	0	packets
rx_crc:	0	packets
rx_short:	0	packets
tx_short:	0	packets
tx_dropped:	0	packets
rx_dropped:	0	packets
ctl_loc_req:	89	packets
ctl_loc_rep:	89	packets
ctl_rem_req:	0	packets
ctl_rem_rep:	0	clock ticks
avg_period:	1019898	clock ticks
avg_idle:	(98.62%)	clock ticks
avg_tx:	(1.18%)	clock ticks
cyc_period:	14998	clock ticks
cyc_idle:	(98.64%)	clock ticks

HPNA Client Statistics Info

The HPNA Client Statistics Info screen displays the client statistics for the HPNA connection, such as the number of packets transmitted, received, and dropped.

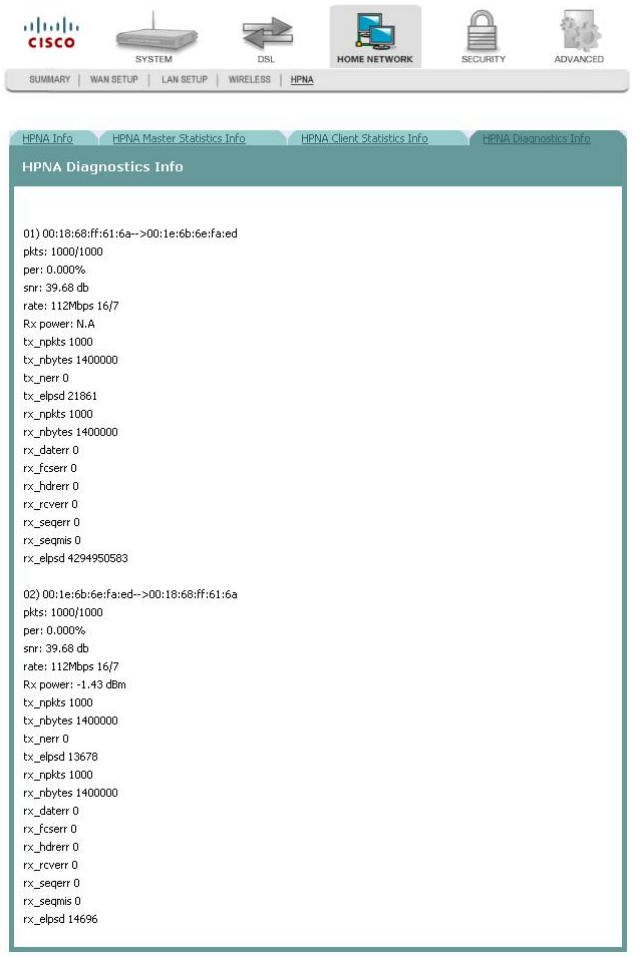
Path: Home Network > HPNA > HPNA Client Statistics Info



HPNA Diagnostics Info

The HPNA Diagnostics Info screen displays the results of the HPNA Diagnostic tests in all possible directions (master to client, client to master, client to client). It also displays diagnostic information such as packets transmitted, PER, SNR, Rx Power, and so on for each direction tested.

Path: Home Network > HPNA > HPNA Diagnostics Info



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

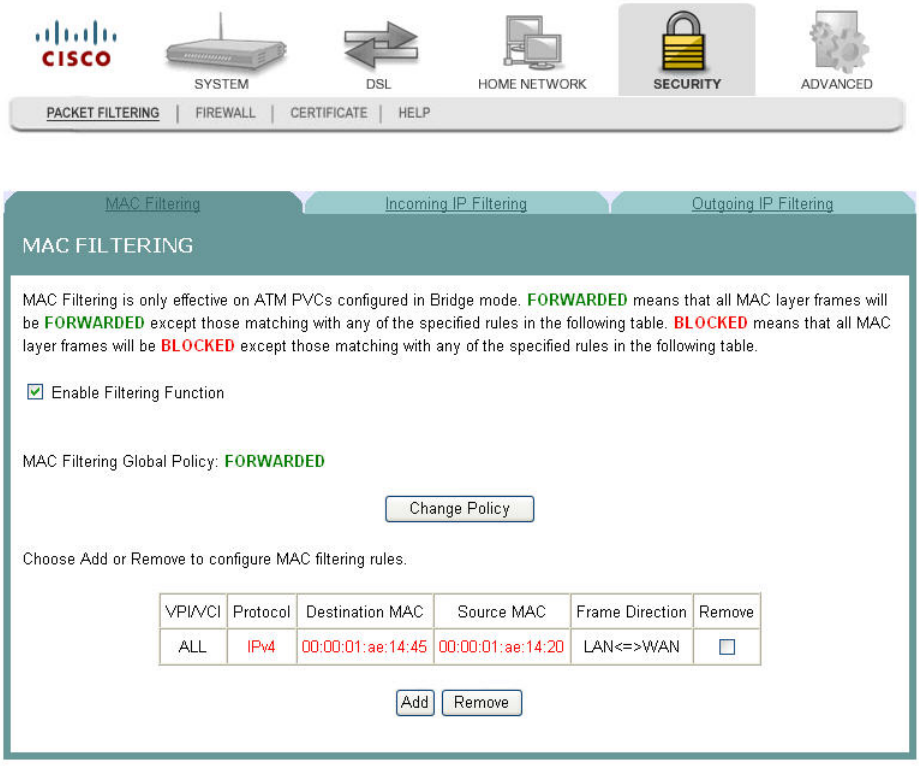
MAC Filtering Setup

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

Path: Security > Packet Filtering > MAC Filtering

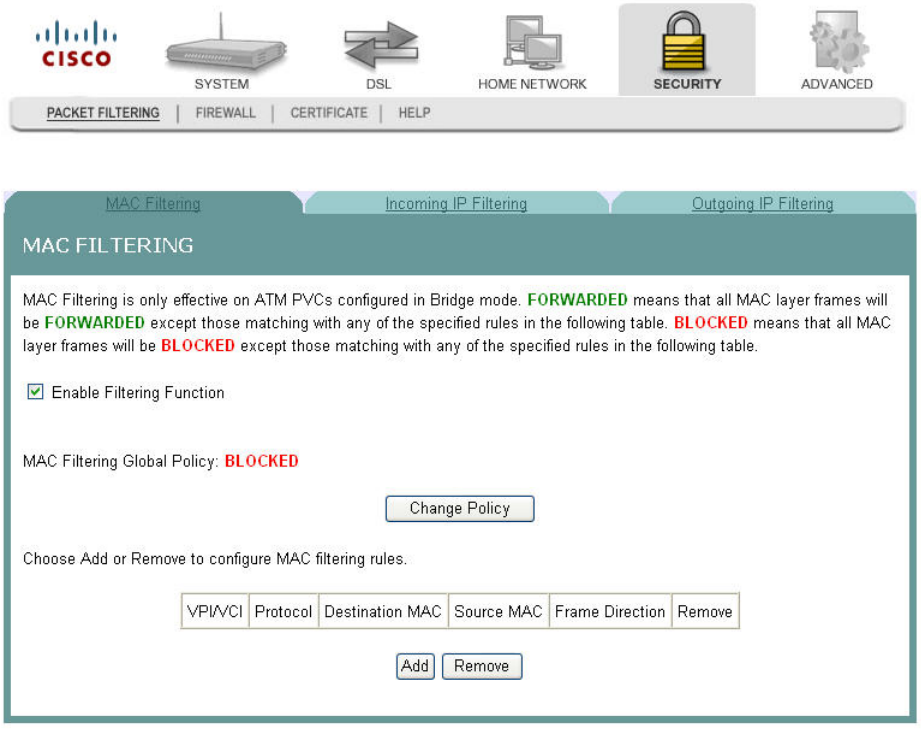
Forwarded MAC Filtering

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



Blocked MAC Filtering

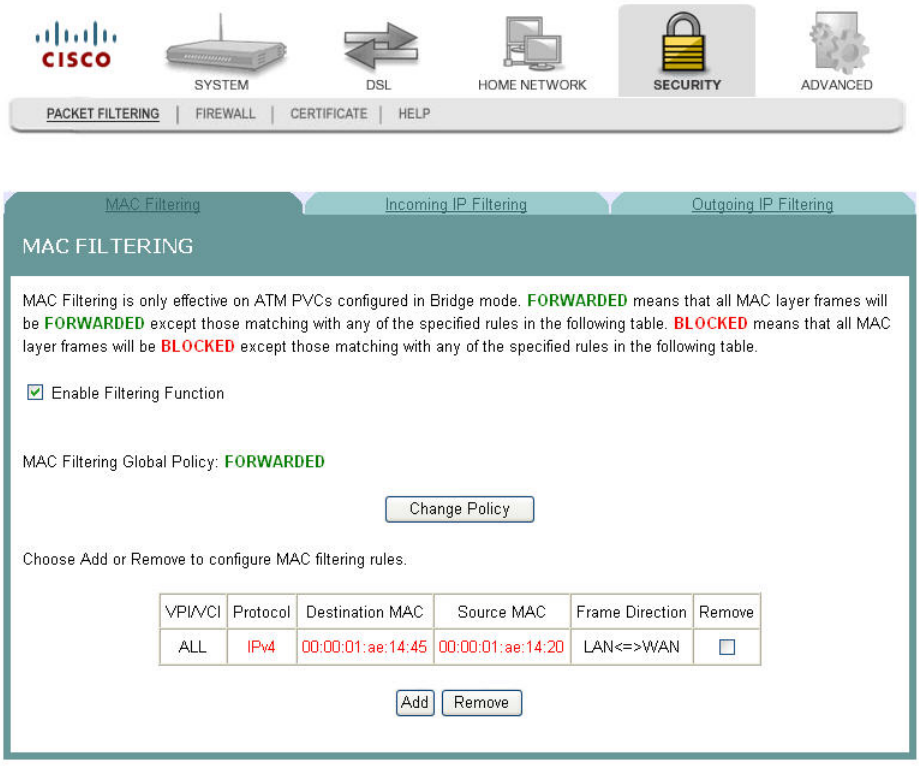
Blocked MAC Filtering means that all MAC layer frames will be BLOCKED except those that match any of the specified rules in the following screen.



Adding MAC Filtering

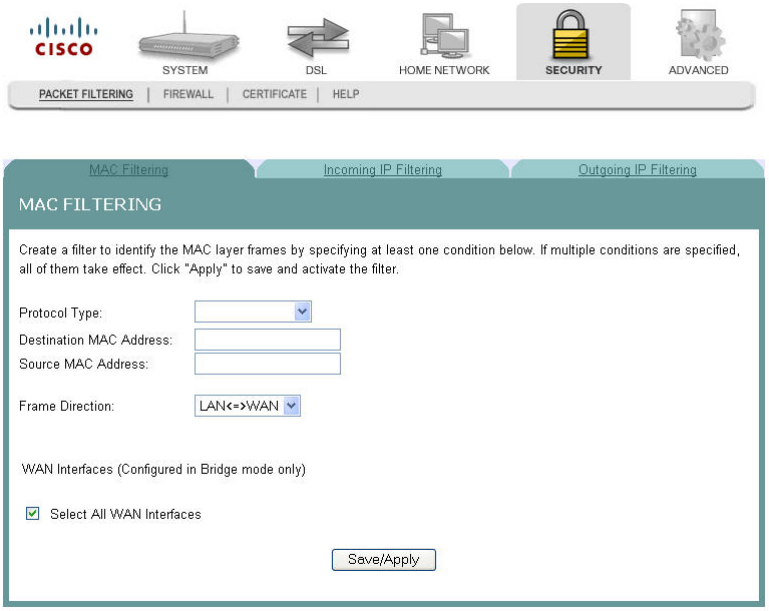
To add MAC Filtering, complete the following steps.

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



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

4 Click **Add** to open a blank MAC Filtering screen.



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

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

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

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

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

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

9 Do you want to select all WAN interfaces?

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

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

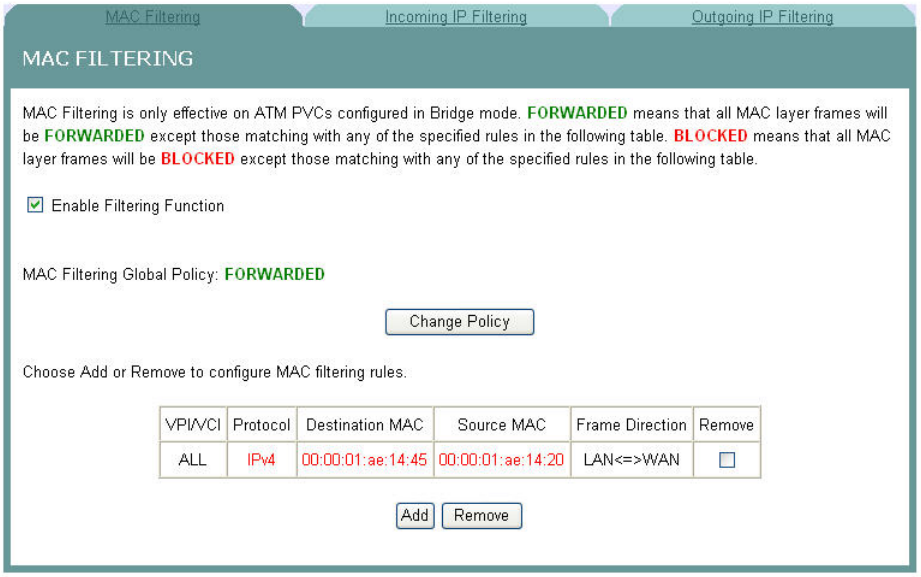
Forwarding or Blocking MAC Layer Frames

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

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

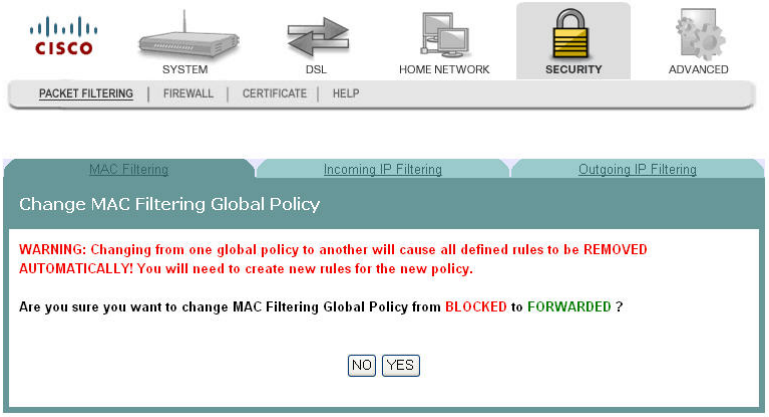
1 Click **Security** on the main screen. The Packet Filtering tab opens by default.

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



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."



5 Do you want to change the Global Policy?

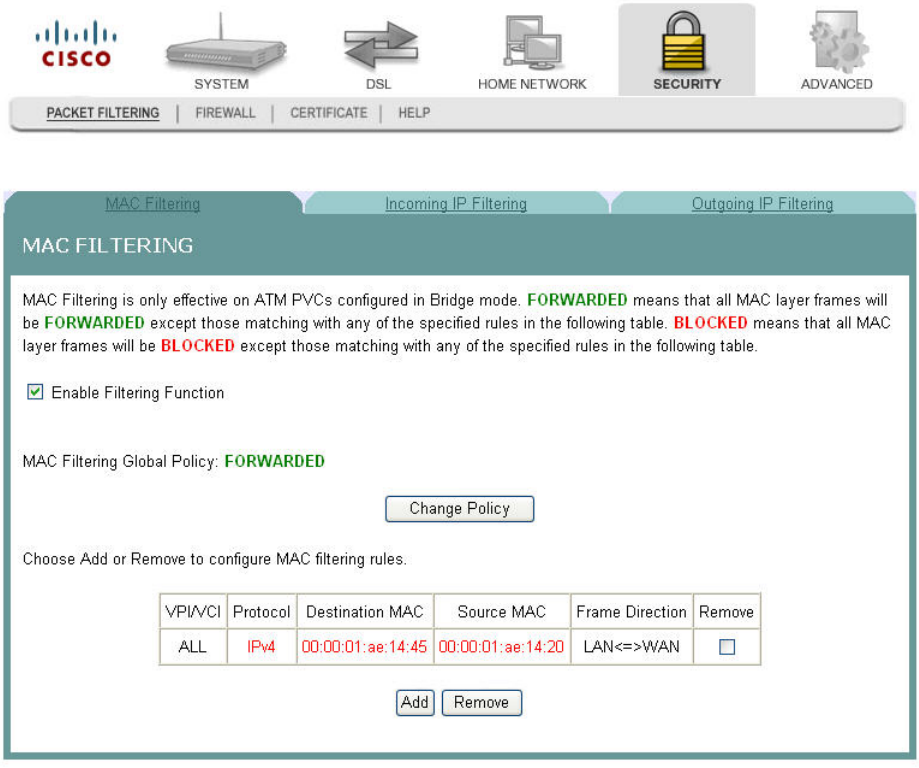
- If **yes**, click **Yes**. If the policy is forwarded, clicking Yes changes the policy to blocked, and vice versa.
- If **no**, click **No** and the policy remains unchanged.

Removing MAC Filtering

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

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

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



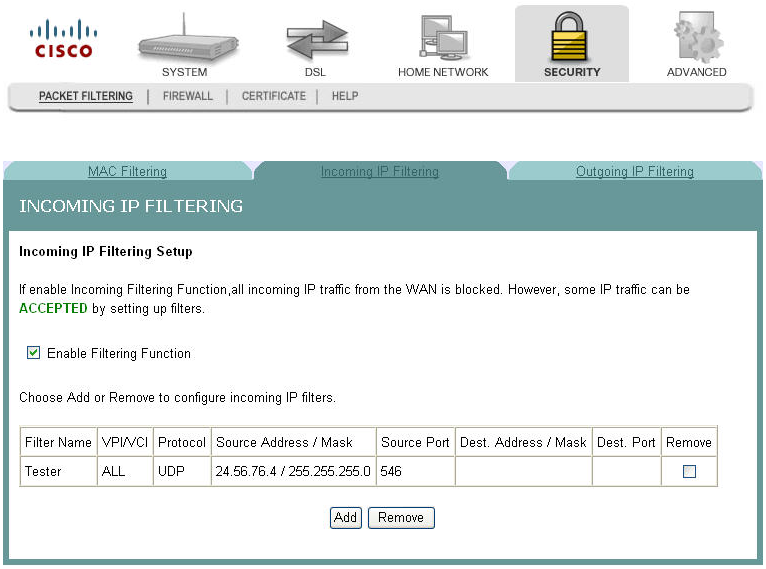
3 From the MAC Filtering screen, select **Remove** in the Remove column next to the MAC filtering rule you wish to remove.

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

Incoming IP Filtering

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

Path: Security > Packet Filtering > Incoming IP Filtering

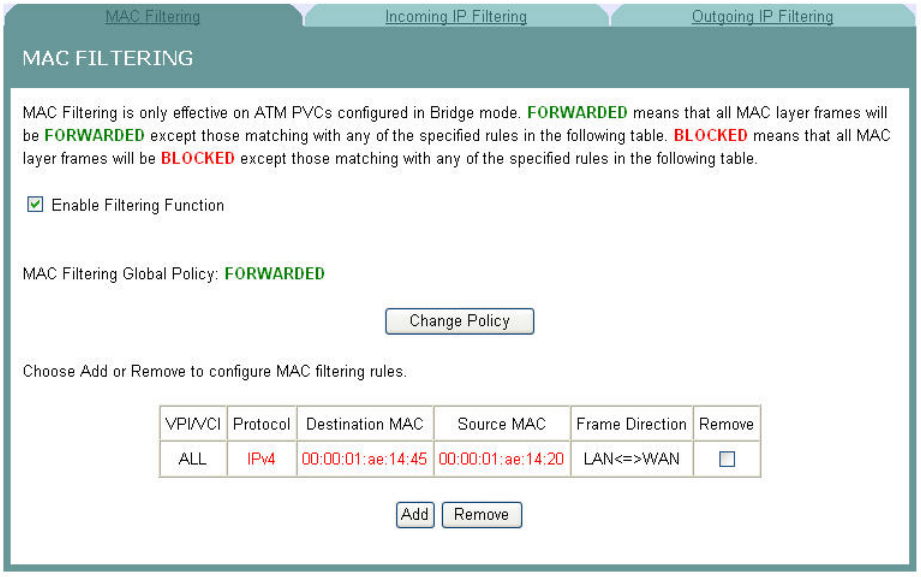


Adding an Incoming IP Filter

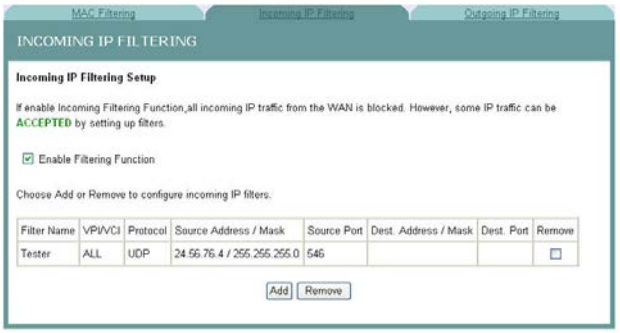
You can create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition for the filter. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.

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

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



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



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

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

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

- TCP/UDP
- TCP
- UDP
- ICMP

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

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

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

Example: 0:5 indicates ports 0 through 5.

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

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

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

Example: 0:5 indicates ports 0 through 5.

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

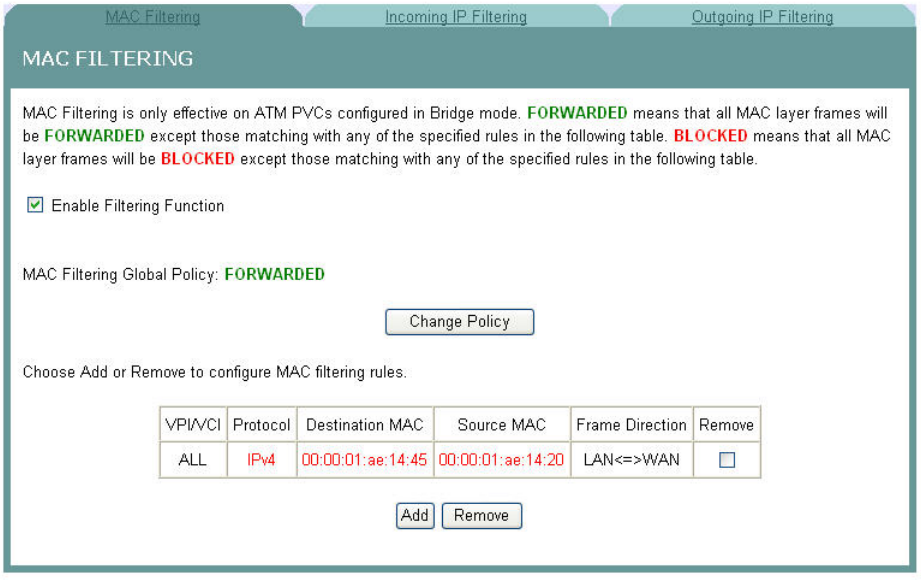
- If **yes**, check the **Select All** field under WAN Interfaces (Configured in Routing mode and with firewall enabled only).
- If **no**, clear the **Select All** field under WAN Interfaces (Configured in Routing mode and with firewall enabled only).

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

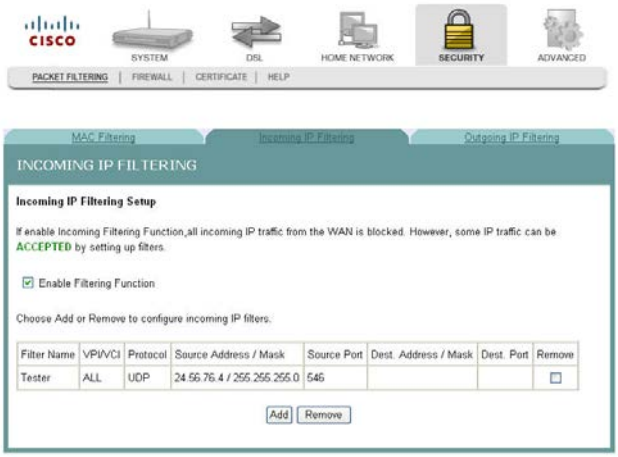
Enabling the Filtering Function

To enable the filtering function, complete the following steps.

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



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

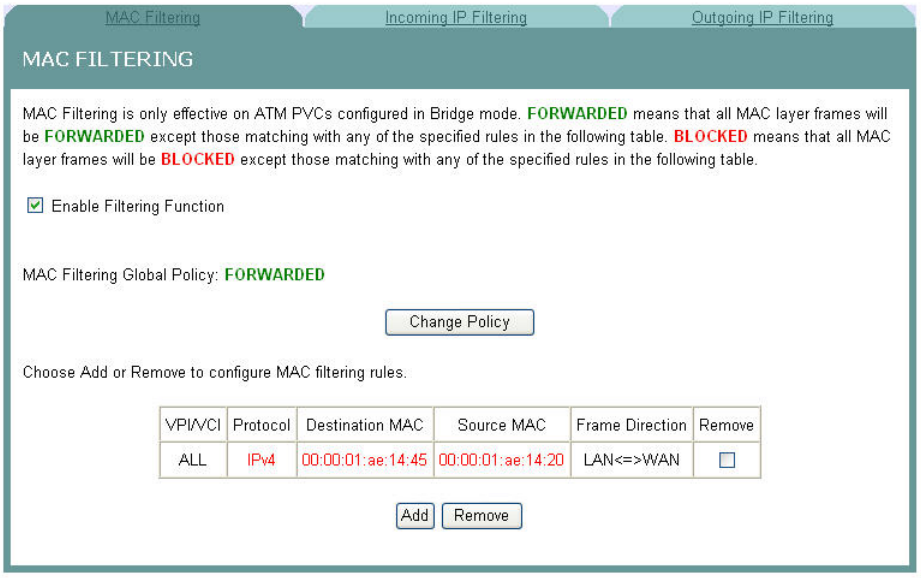


3 Check the **Enable Filtering Function** check box to enable the filtering function.

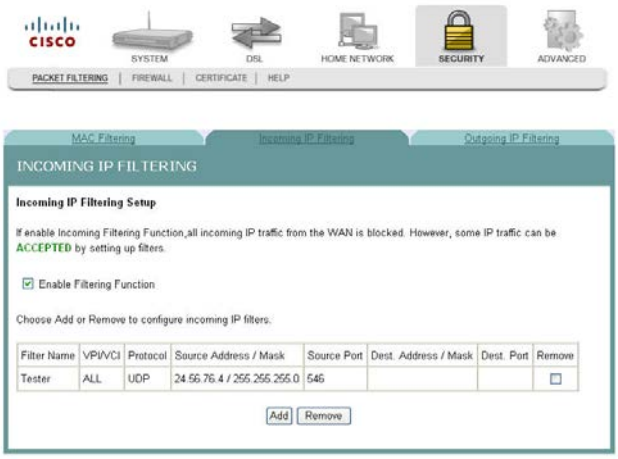
Removing an Incoming IP Filter

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

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



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



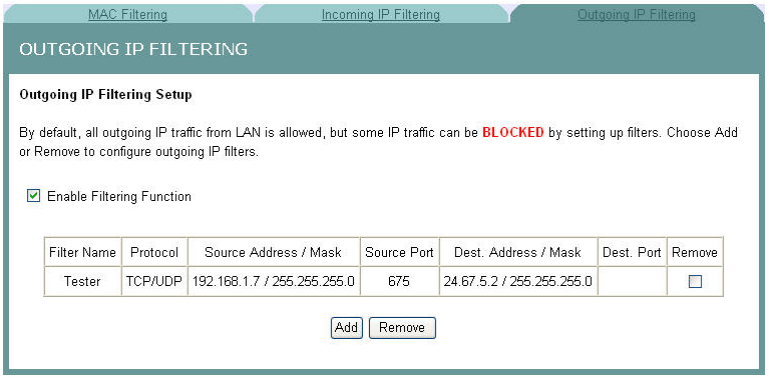
3 From the Incoming IP Filtering screen, select **Remove** in the Remove column next to the filter you wish to remove.

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

Outgoing IP Filtering

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

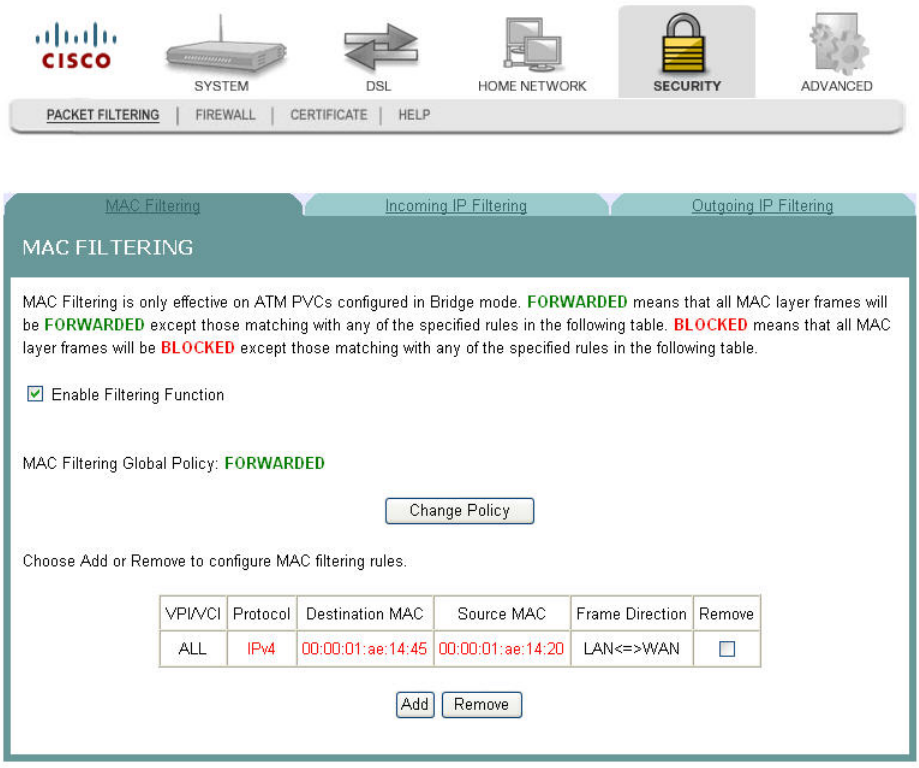
Path: Security > Packet Filtering > Outgoing IP Filtering



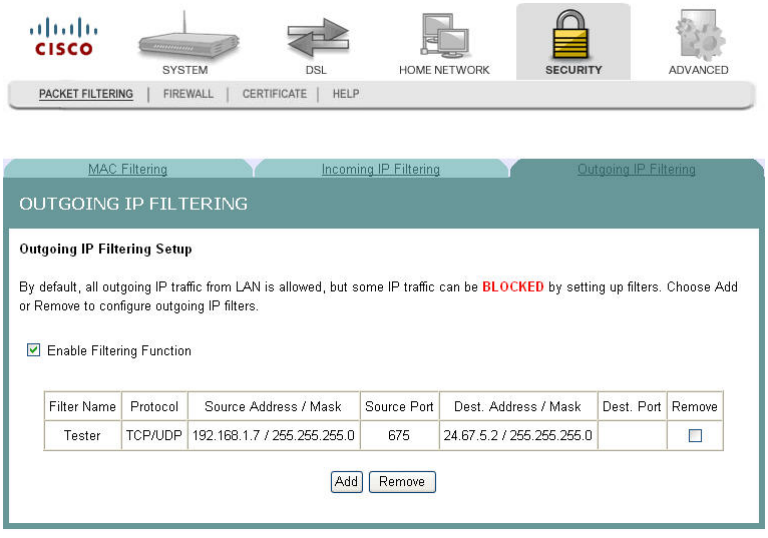
Enabling the Filtering Function

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

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



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

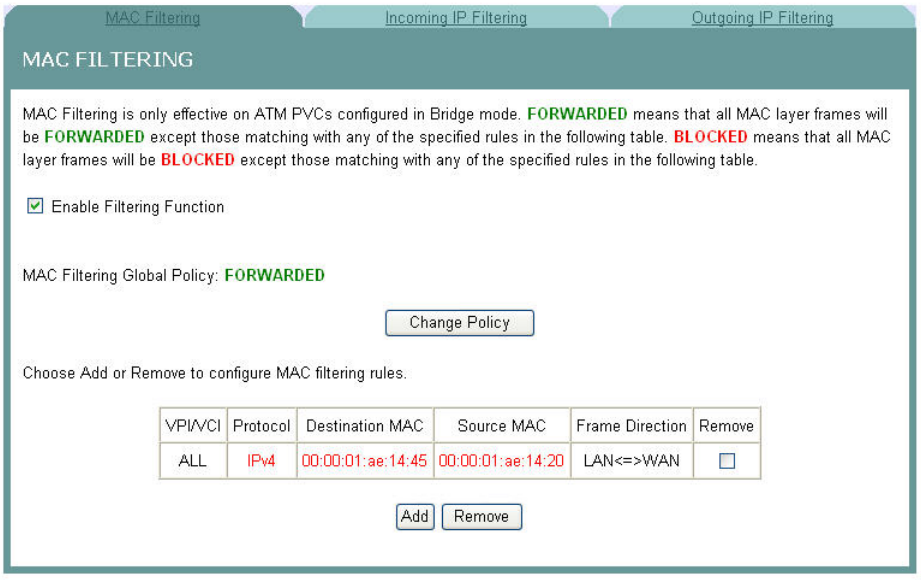


3 Check the **Enable Filtering Function** check box to enable the filtering function.

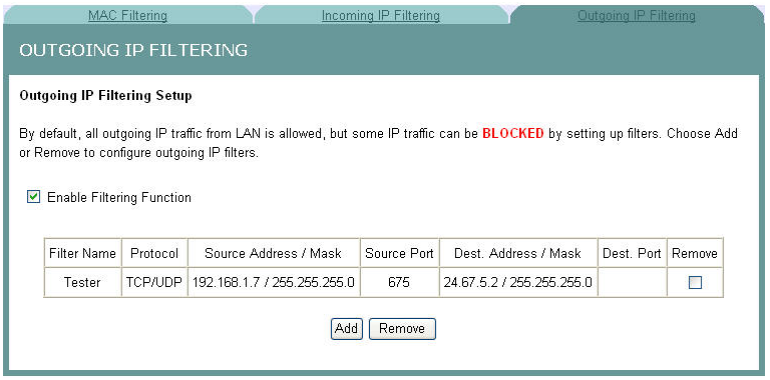
Adding an Outgoing IP Filter

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

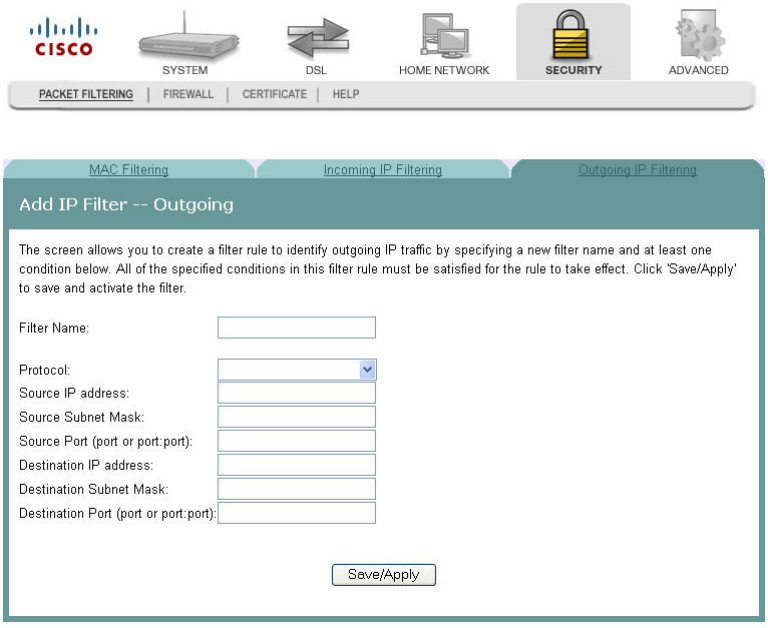
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



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



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



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

Note: You cannot use blank spaces in the filter name.

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

- TCP/UDP
- TCP
- UDP
- ICMP

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

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

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

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

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

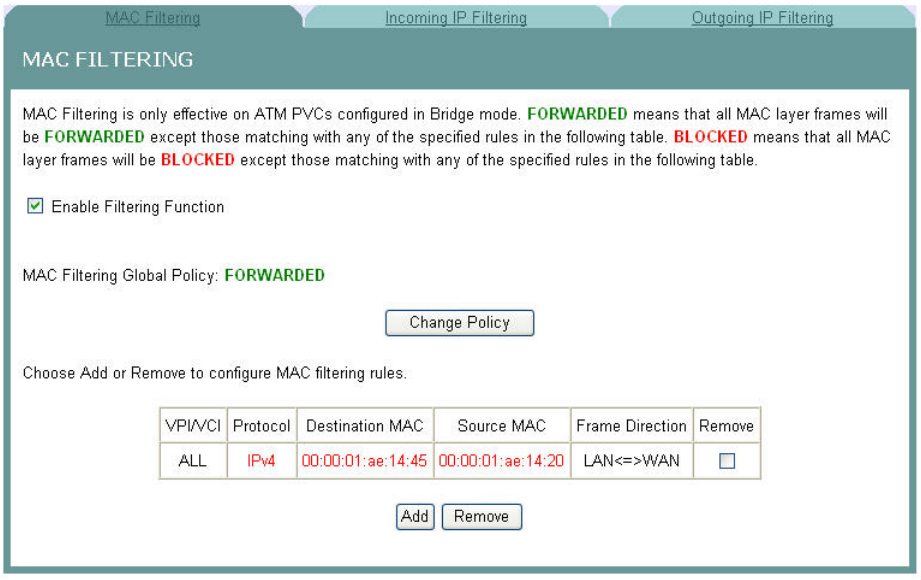
11 In the Destination Port field, enter the port number for the server receiving the packets. Use the following format: port or port:port.

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

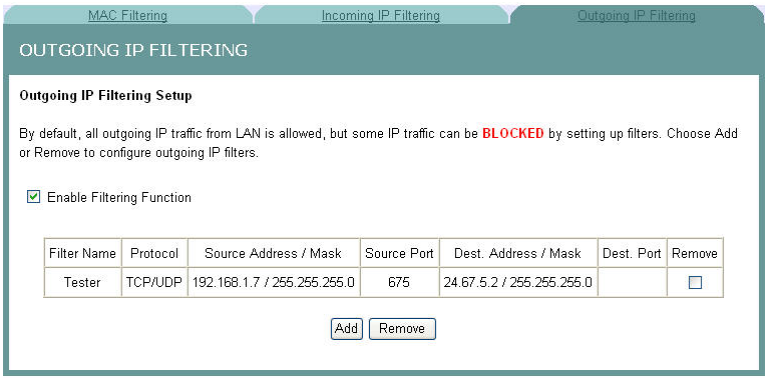
Removing an Outgoing IP Filter

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

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



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



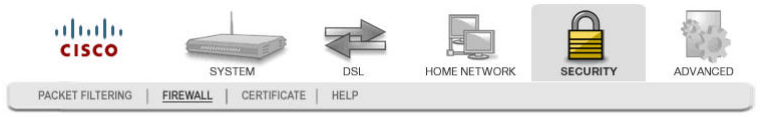
3 From the Outgoing IP Filtering screen, select **Remove** in the Remove column next to the filter you wish to remove.

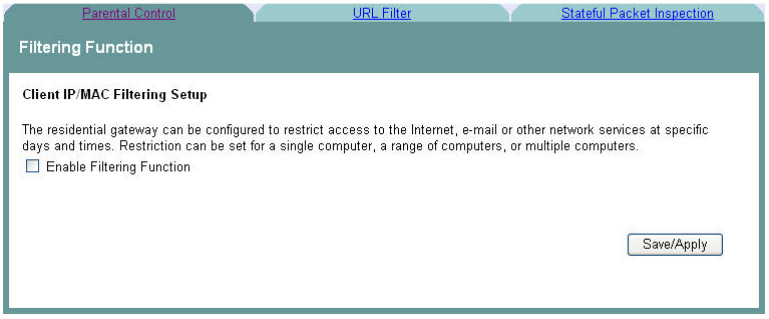
4 Click **Remove** to remove the filter.

Parental Control Setup - Filtering Function

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

Path: Security >Firewall > Parental Control





Adding Time of Day Restrictions

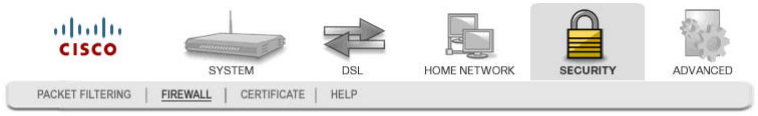
The Filtering Function screen allows you to set restrictions that block access to the Internet during certain times of the day. This screen adds time of day restrictions to a special LAN device connected to the residential gateway. The browser's MAC Address automatically displays the MAC address of the 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**.

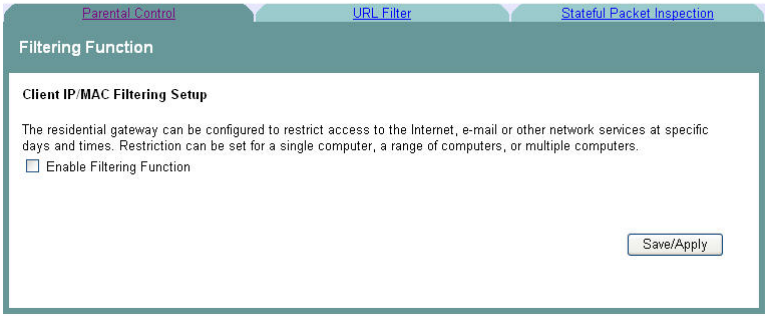
Path: Security > Firewall > Parental Control

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

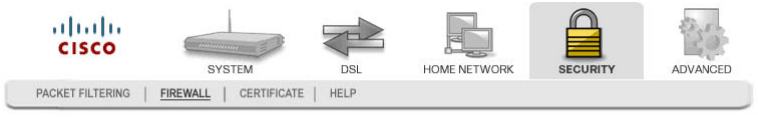
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.

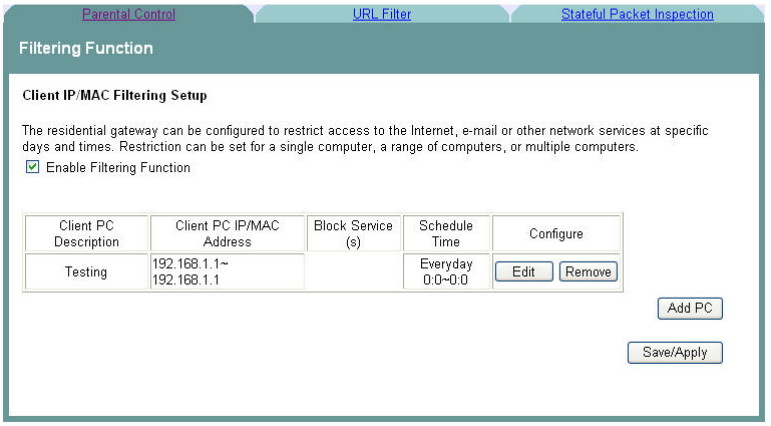
2 Click the **Firewall** tab. The Filtering Function screen opens.



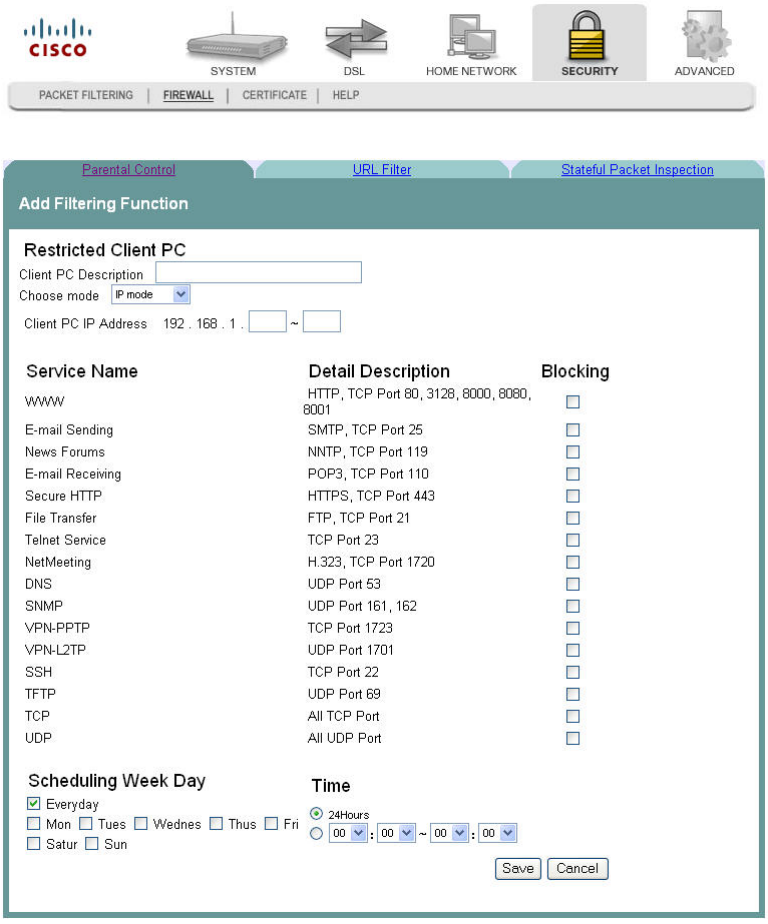


3 Check the **Enable Filtering Function** check box to enable the filtering function. The Client IP MAC Filtering screen populates with any time restrictions that are set.





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



5 In the Client PC Description field, enter a description of the PC for which you want to block services.

6 In the Choose mode field, select IP mode or MAC mode from the drop-down menu.

7 Enter the IP address in the Client PC IP Address field, or enter the MAC address in the MAC address field depending upon the mode you selected in step 6.

8 Under Service Name area, check the **Blocking** check box for every service that you wish to filter.

9 In the Scheduling Week Day area, check the check boxes next to each day where you want to set up time of day restrictions. If you want to apply the time of day restrictions to everyday, check the Everyday check box. For example, check the F, Sa, and Su check boxes to apply time of day restrictions to Friday, Saturday, and Sunday.

10 In the Time area set the time as follows:

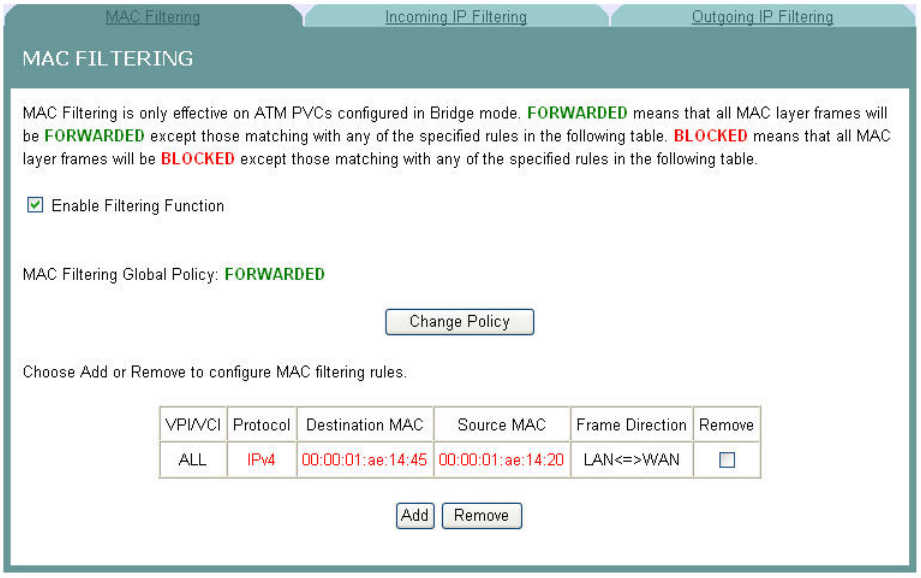
- Click the 24Hours option to apply the restrictions 24 hours a day
- Click the option where you select the time from the drop-down menus. Use the drop down menus to enter the time when you want the restriction to start and end.

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

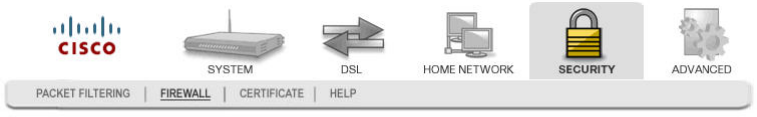
Removing Time of Day Restrictions

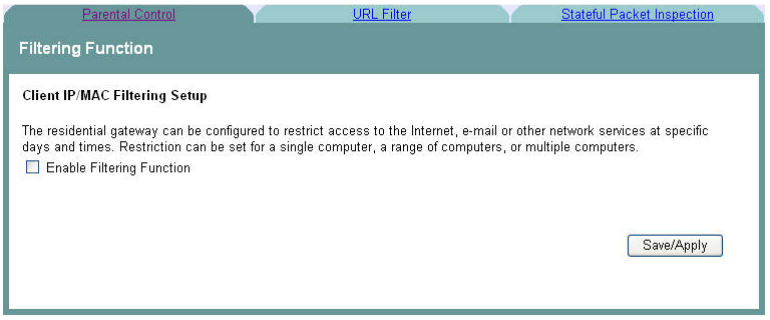
To remove time of day restrictions, complete the following steps.

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

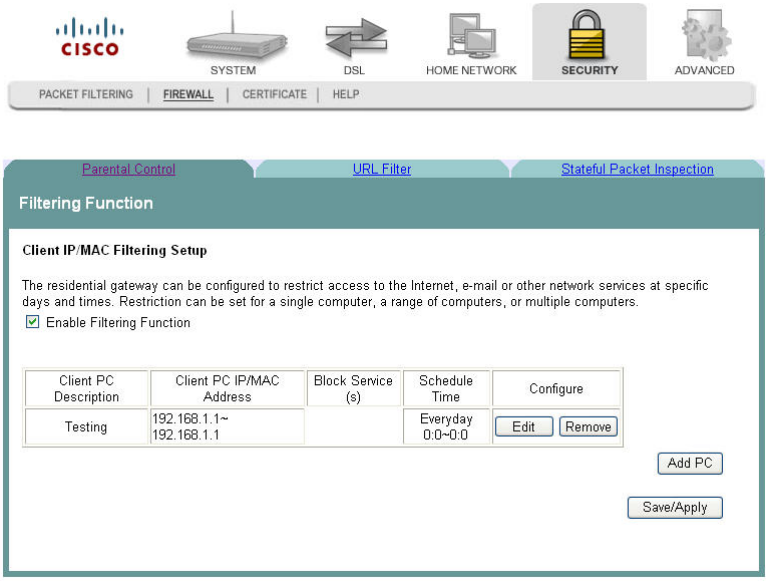


2 Click the **Firewall** tab. The Filtering Function screen opens.





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



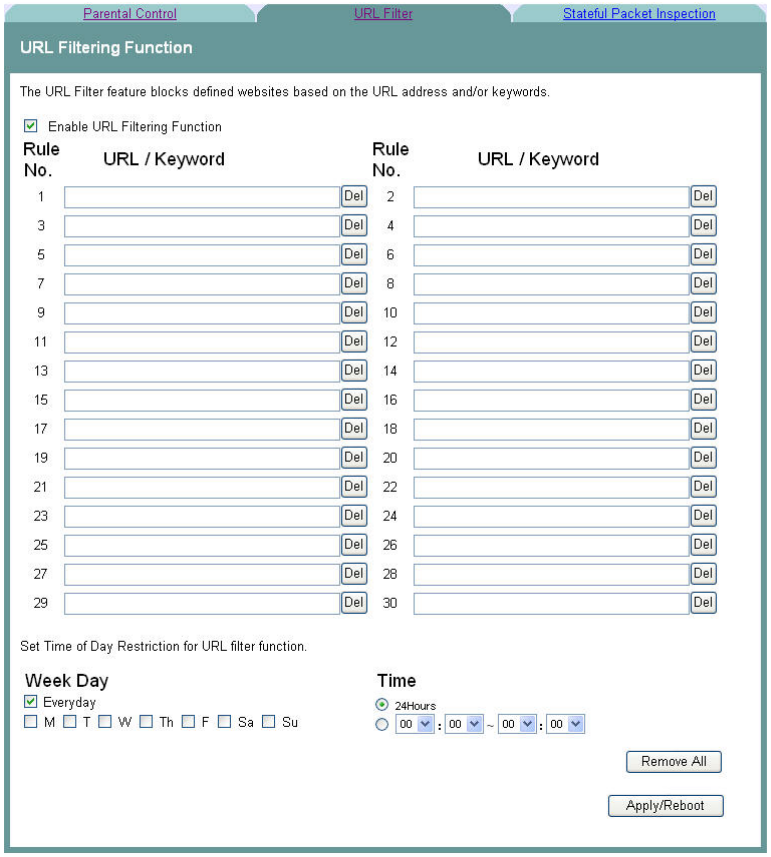
4 From the Configure field select **Remove** in the Remove column next to the time of day restriction that you wish to remove.

5 Click **Remove** to remove the restriction.

URL Filtering Function

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

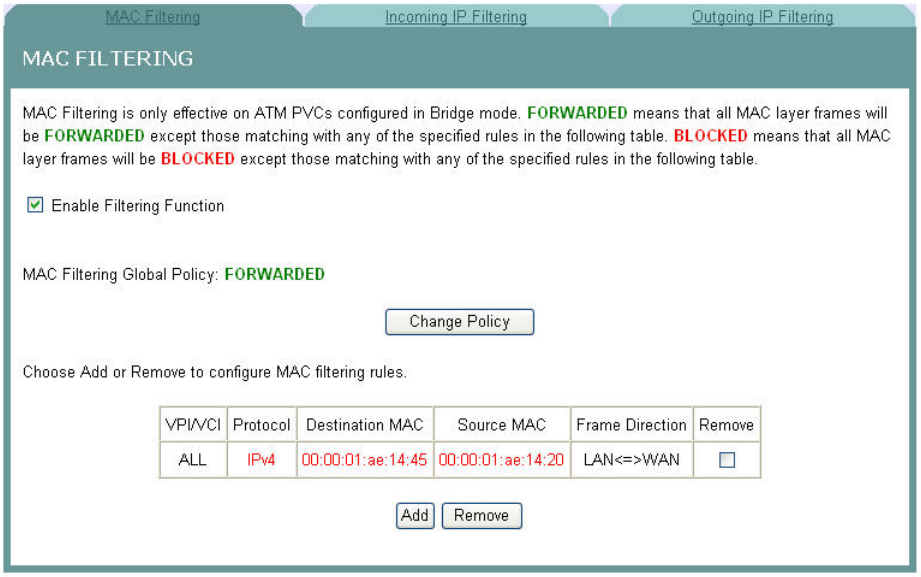
Path: Security > Firewall > URL Filter



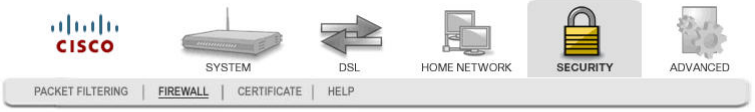
Enabling URL Filtering

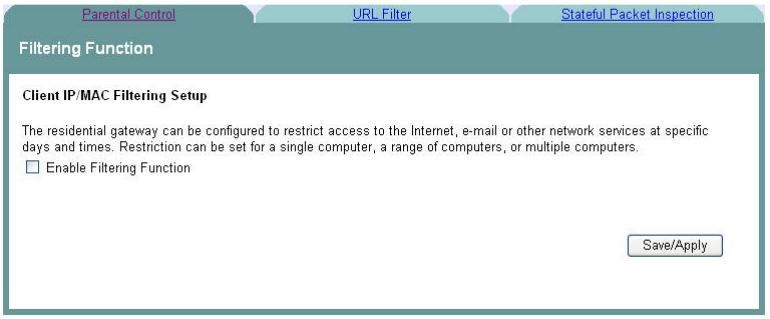
To enable URL filtering for the firewall, complete the following steps.

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



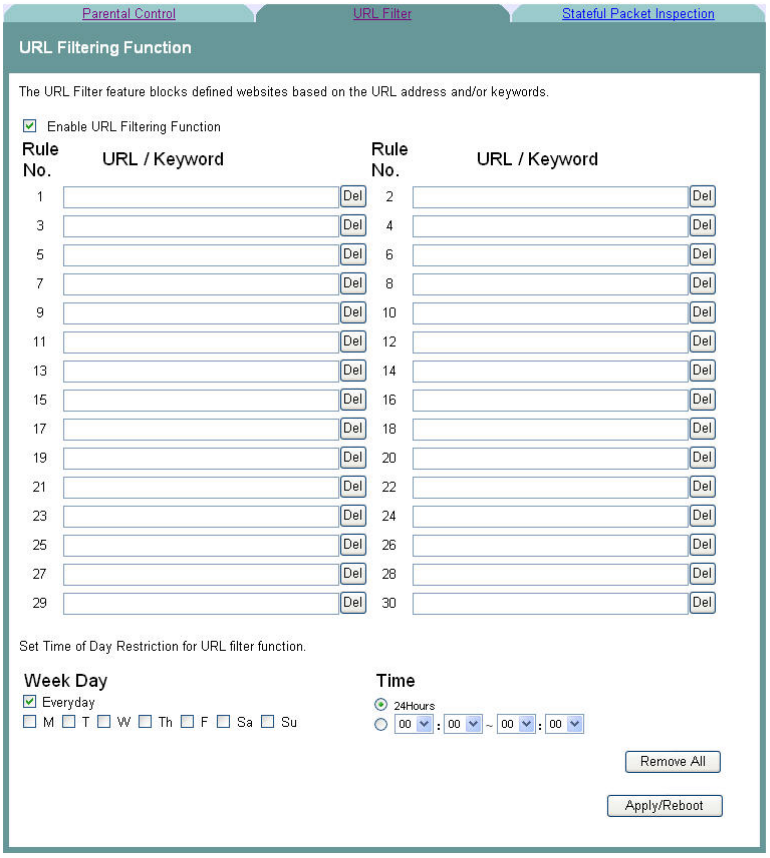
2 Click the **Firewall** tab. The Filtering Function screen opens by default.





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

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



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

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

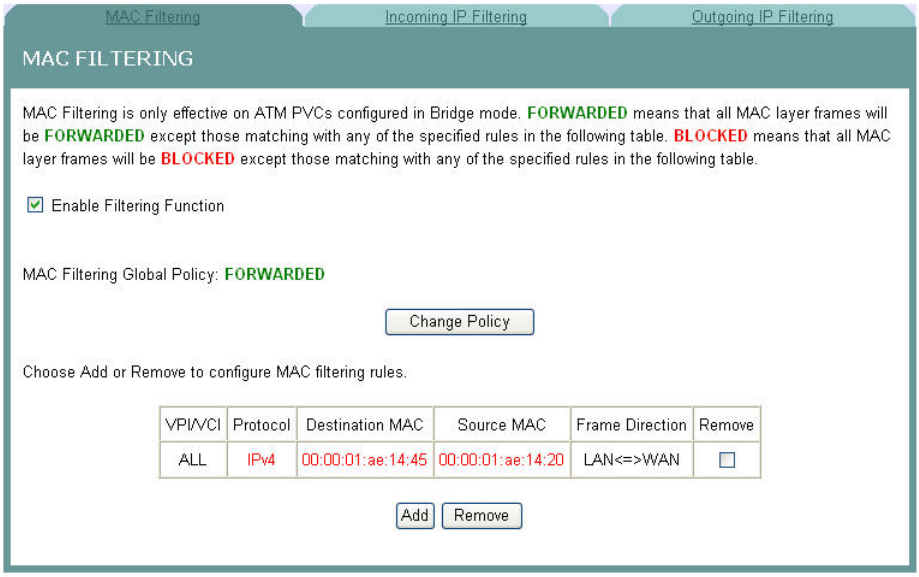
7 In the **Time** area, select 24Hours or select the individual times that you want the filter to take effect.

8 Click **Save**.

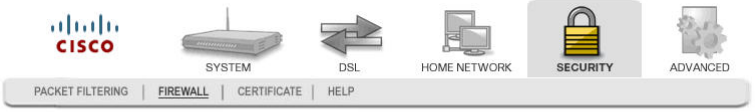
Removing a URL Filter

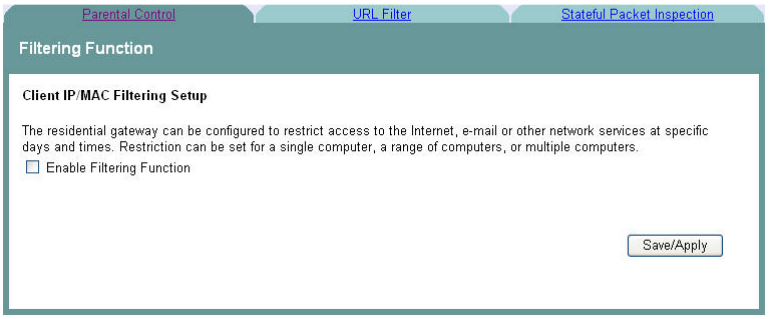
To remove a URL filter from the firewall, complete the following steps.

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



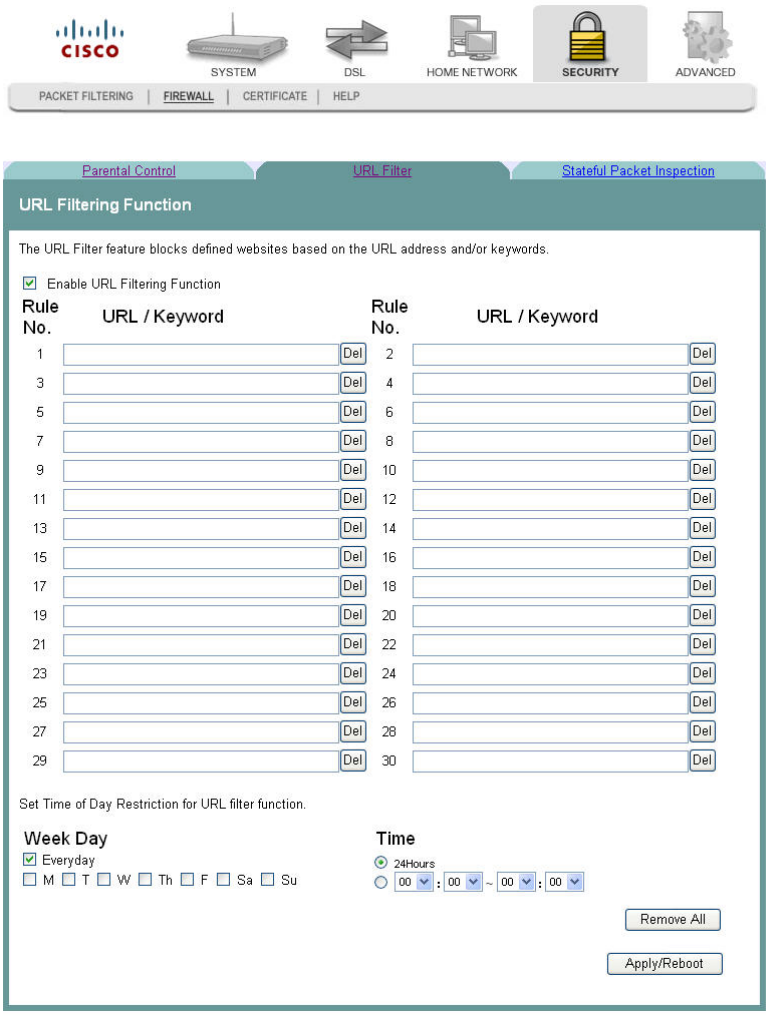
2 Click the **Firewall** tab. The Filtering Function screen opens by default.





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

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



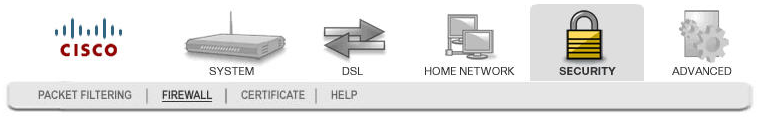
5 Click **Del** next to each rule that you want to delete. If you want to remove all the rules, click **Remove All**.

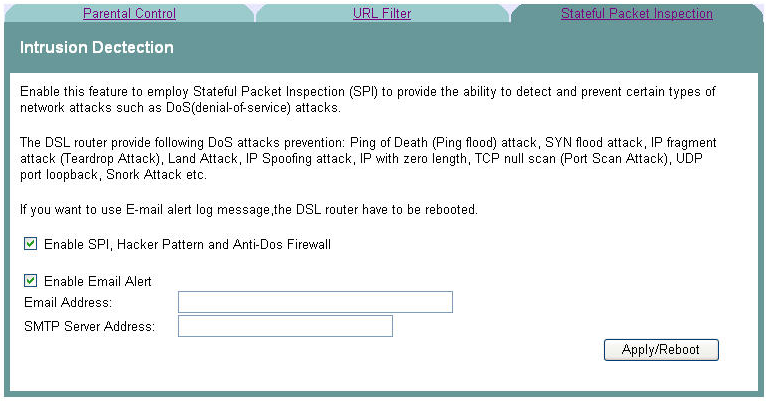
6 Click **Save**.

Stateful Packet Inspection

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

Path: Security > Firewall > Stateful Packet Inspection

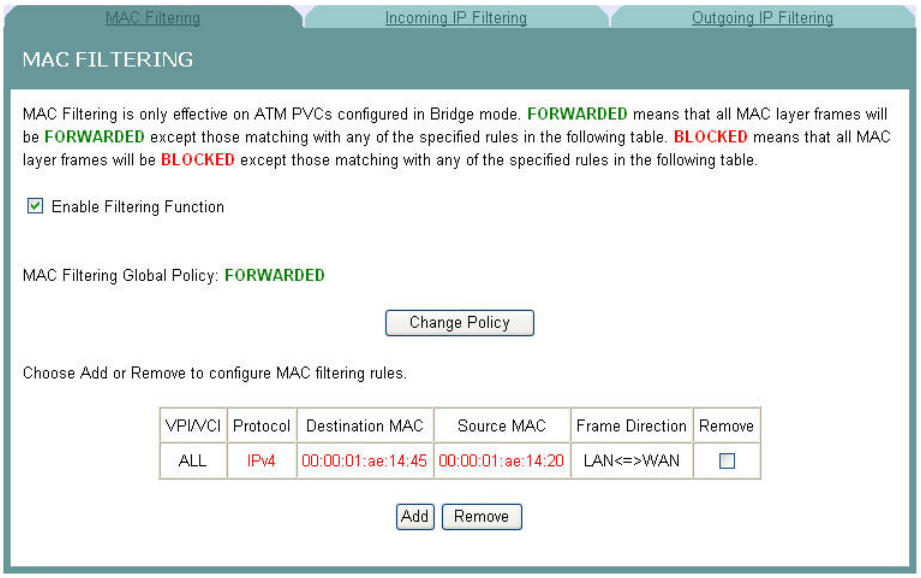




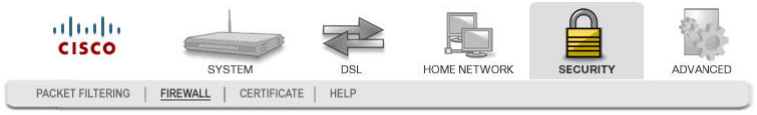
Enabling Stateful Packet Inspection

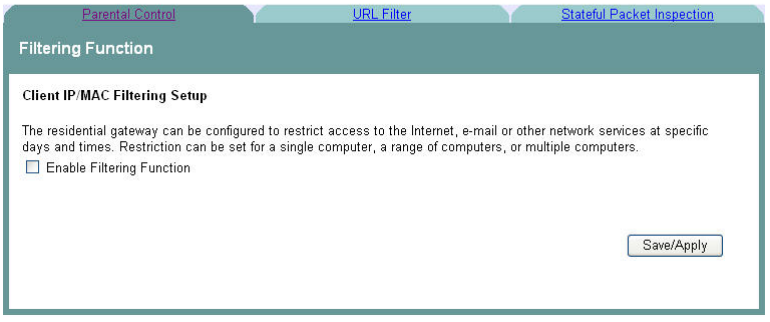
To enable stateful packet inspection (SPI), complete the following steps.

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

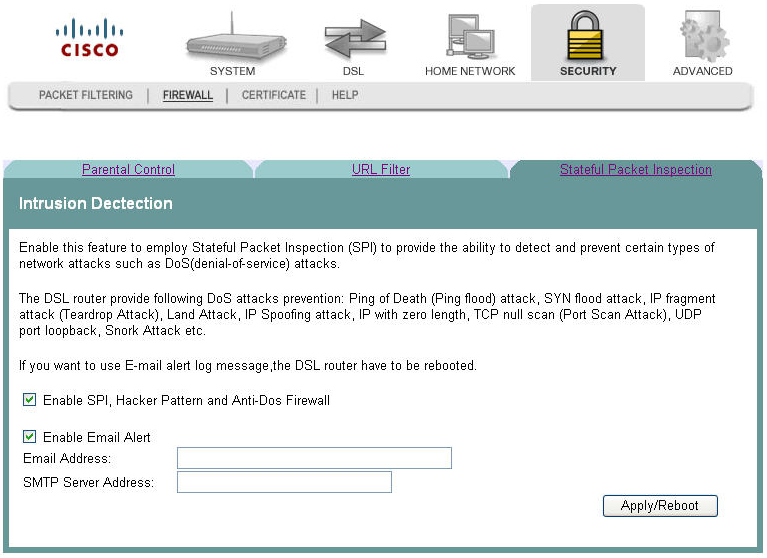


2 Click the **Firewall** tab. The Filtering Function screen opens by default.





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



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

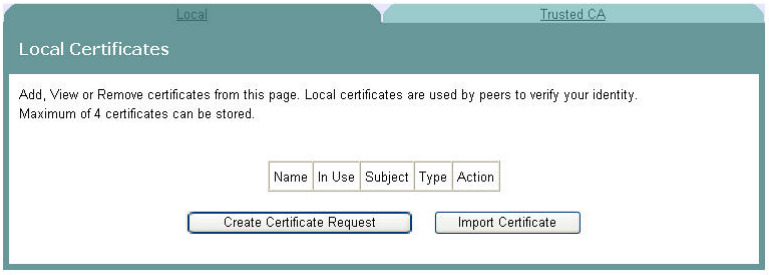
5 Select the **Enable Email Alert** field and fill in the email address and SMTP server address that you want to notify when the DSL must be rebooted.

6 Click **Save/Apply** to enable stateful packet inspection.

Local Certificates

The Local Certificates screen allows you to load certificates onto the residential gateway. Local certificates are used by peers to verify your identity. A maximum of four certificates can be stored on the residential gateway.

Path: Security > Certificate > Local > Local Certificates

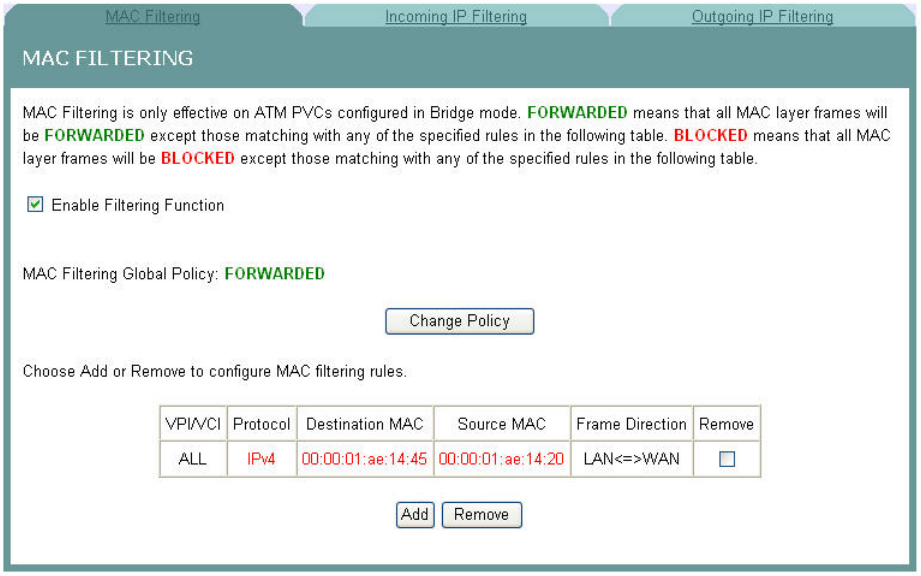


Creating Certificates

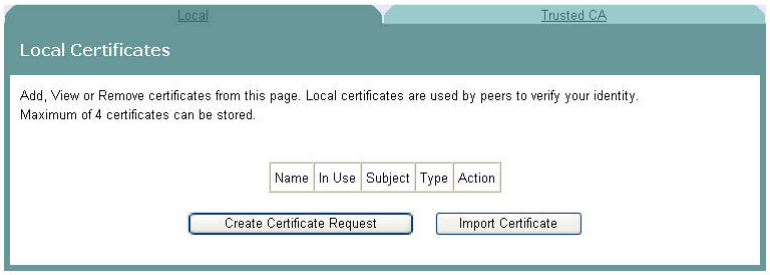
The Create Certificate screen allows you to generate a certificate by specifying certificate parameters shown in this screen.

To create a certificate, complete the following steps.

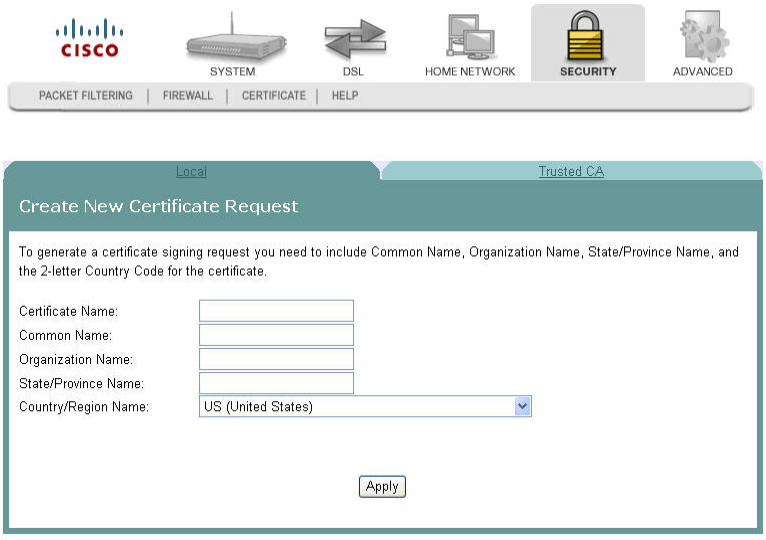
1 Click **Security** on the main screen. The MAC Filtering screen opens.



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



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



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

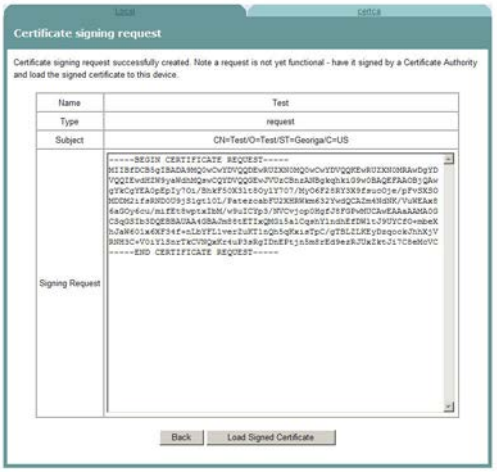
5 In the Common Name field, enter the common name of the certificate.

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

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

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

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



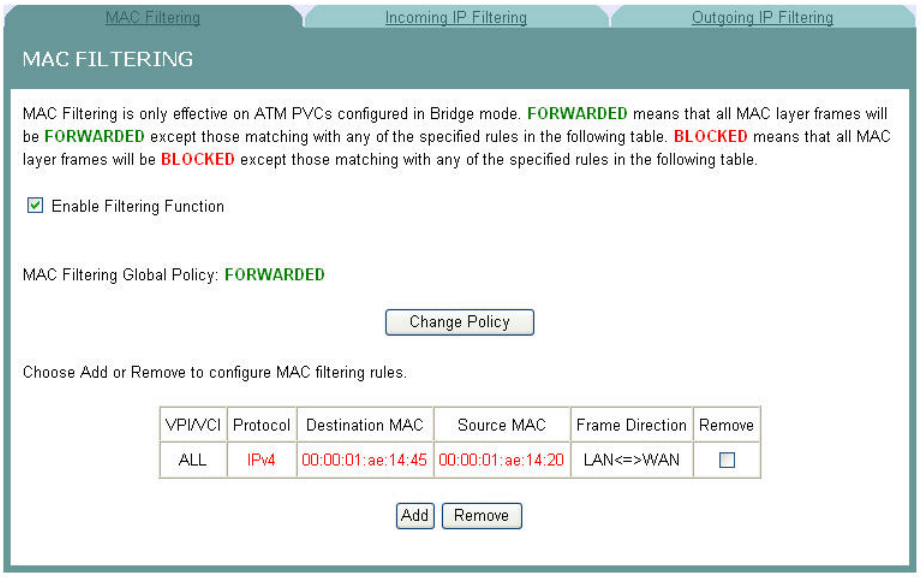
10 Click **Load Signed Certificate** to save the certificate on the residential gateway.

Importing Local Certificates

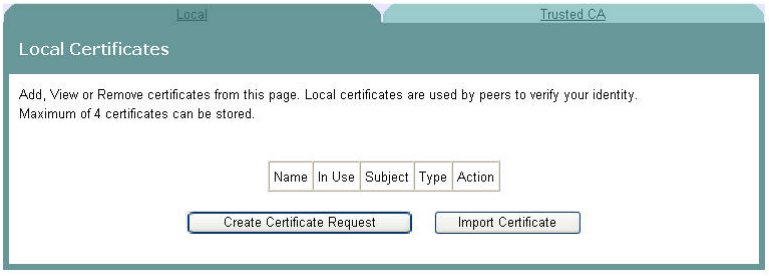
The Import Certificate screen allows you to import a pre-existing certificate to the residential gateway.

To import a certificate, complete the following steps.

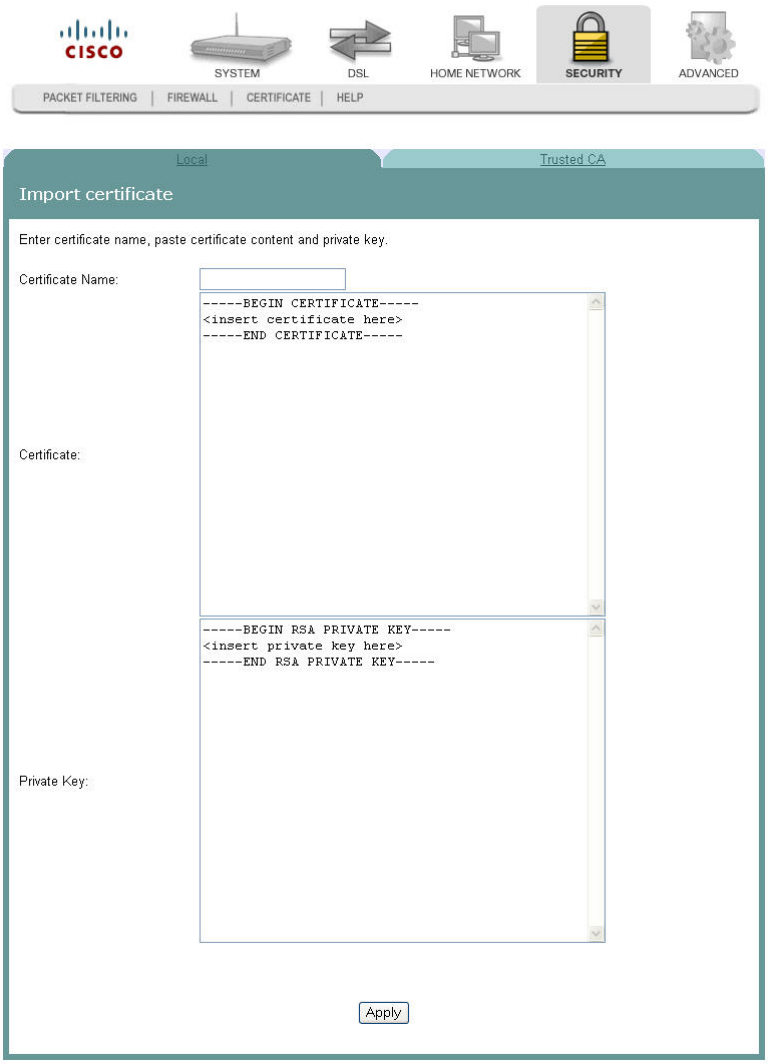
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



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



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



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

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

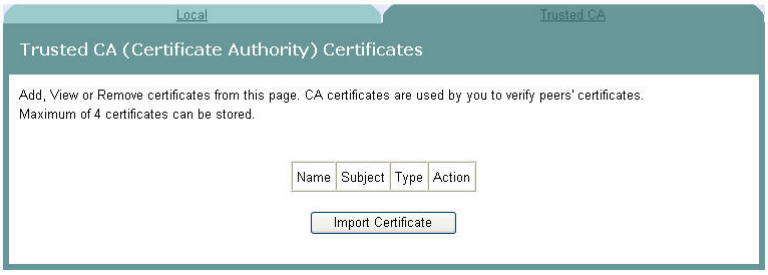
6 In the Private Key area, copy and paste the private key from the certificate file provided by the service provider.

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

Trusted CA Certificates

The Trusted CA (Certificate Authority) Certificates screen allows you to load certificates onto the residential gateway. You can use CA certificates to verify peers' certificates. A maximum of four certificates can be stored.

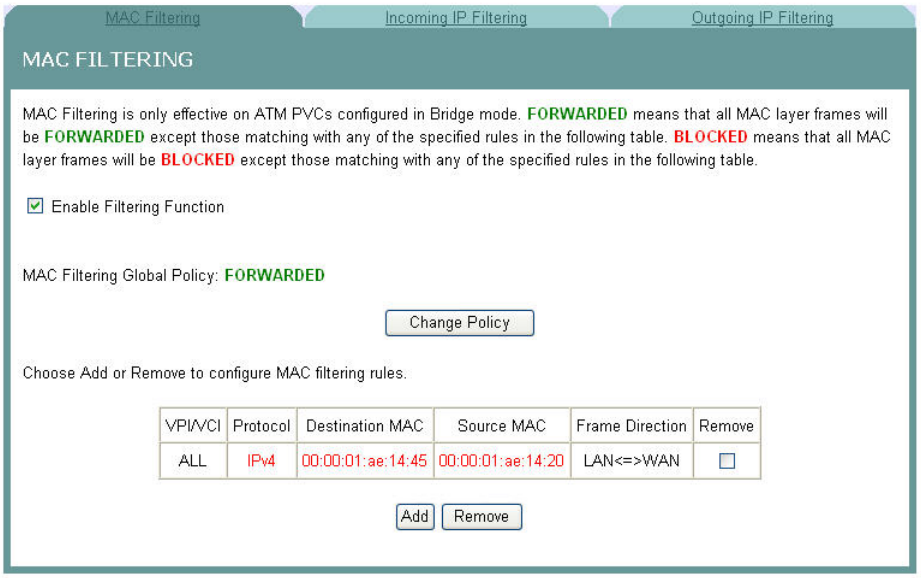
Path: Security > Certificate > Trusted CA > Trusted CA (Certificate Authority) Certificates



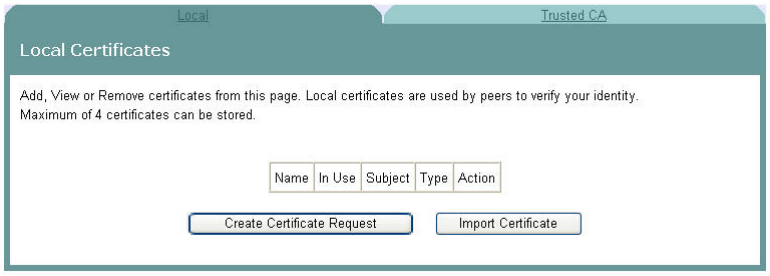
Importing Trusted CA Certificates

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

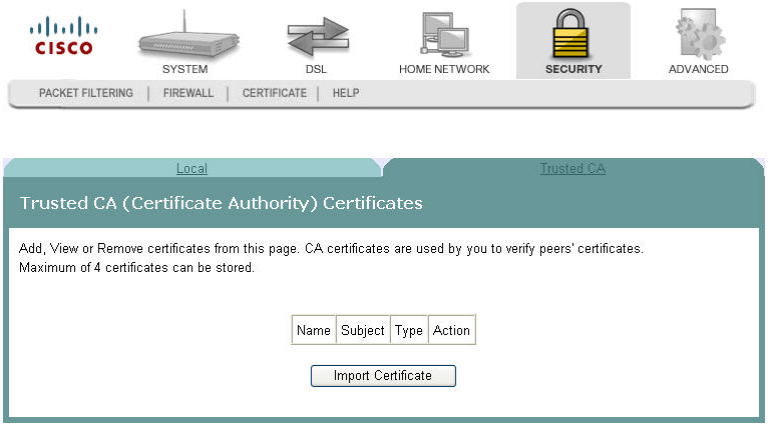
1 Click **Security** on the main screen. The MAC Filtering screen opens by default.



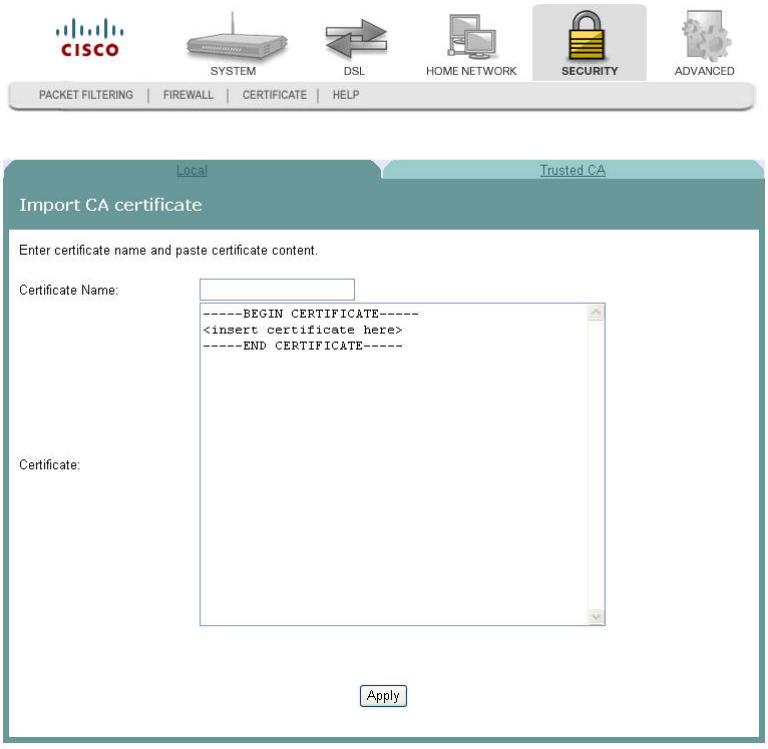
2 Click **Certificate.** The Local Certificates screen opens.



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



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



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

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

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

7

Advanced Configuration

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

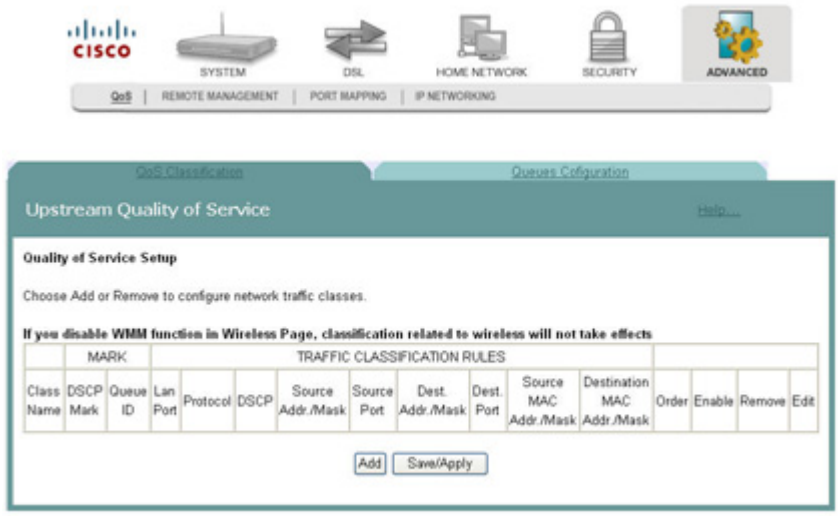
Use this chapter to check the status of the more advanced features of your residential gateway, such as port mapping and DNS server configuration, and to change the configuration.

In This Chapter

Upstream Quality of Service

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

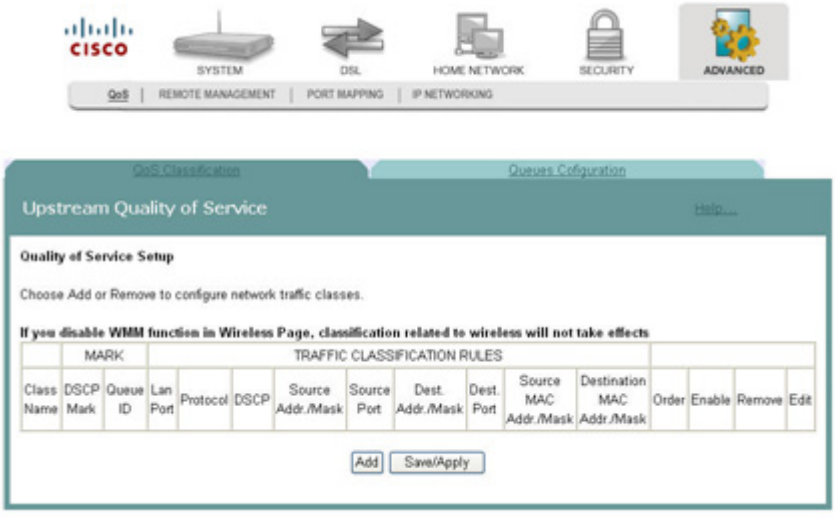
Path: Advanced > QoS > Upstream Quality of Service



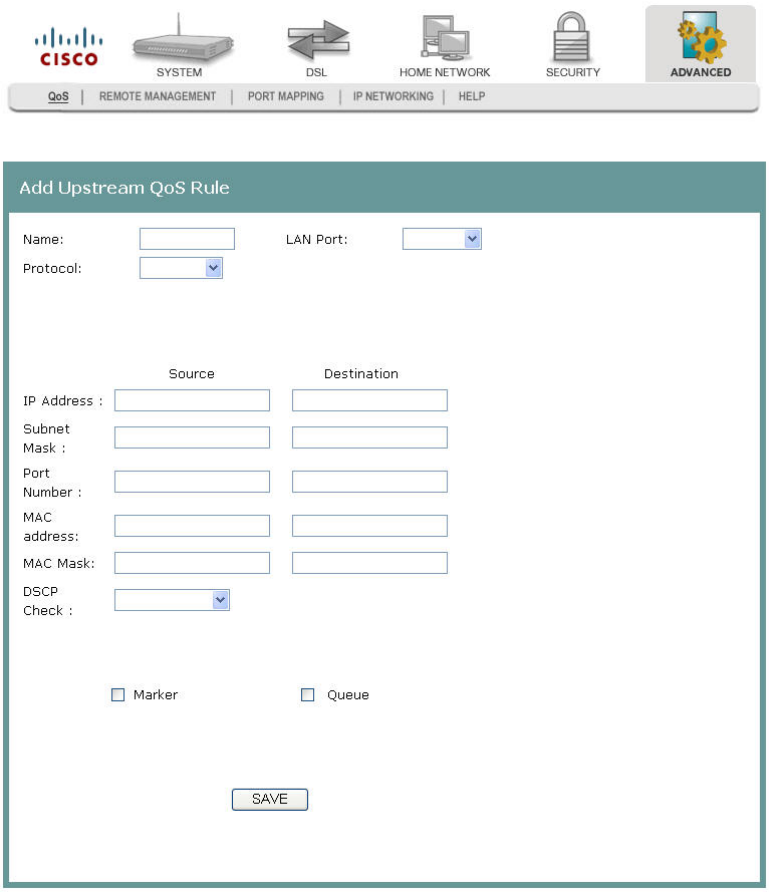
Adding Upstream Quality of Service Settings

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

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



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



3 In the Name field, enter the name of the QoS rule.

4 In the LAN Port field, select the LAN port for which you want to apply the rule.

5 In the Protocol field, select the protocol that you want to use from the following options:

- TCP/UDP
- TCP
- UDP
- ICMP

6 In the IP Address field, enter the source and destination addresses.

7 In the Subnet Mask field, enter the source and destination subnet masks.

8 In the Port Number field, enter the source and destination ports.

9 In the MAC address field, enter the MAC address for the source from which the packets are being sent and the MAC address for the destination. The MAC address should be in the form of 6 pairs of hex digits. For example, aa:ee:ff:11:03:24.

10 In the MAC Mask field, enter the mask for the source MAC address from which the packets are being sent and the MAC Mask for the destination MAC address. A MAC mask of ff:ff:ff:00:00:00 matches all devices made by the same manufacturer (identified by the first three pairs of the MAC address). A MAC mask of ff:ff:ff:ff:ff:ff matches a single device.

11 In the DSCP Check field, select the matching DSCP value from the list of Diffserv code point.

12 Select the **Marker** field and choose from the list of Diffserv code point (DSCP) values to mark the specified data flow.

13 Select the **Queue** field and choose from the list of queues.

14 Click **Save**.

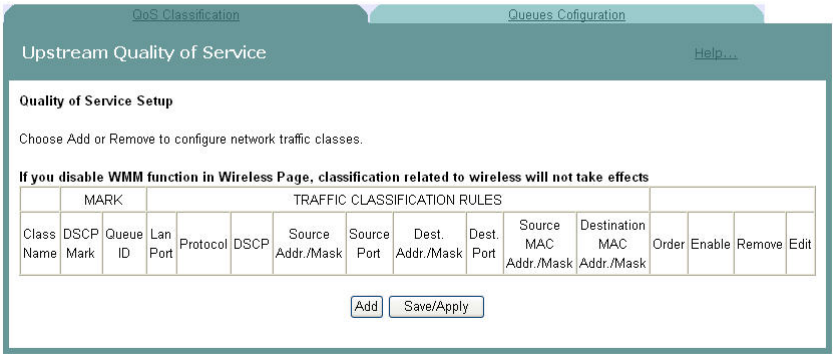
Queues Configuration

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

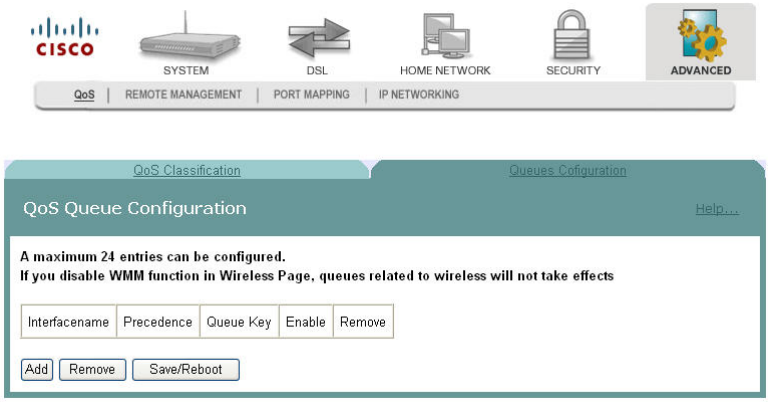
Path: Advanced > QoS > Queues Configuration

To set up your queues, complete the following steps.

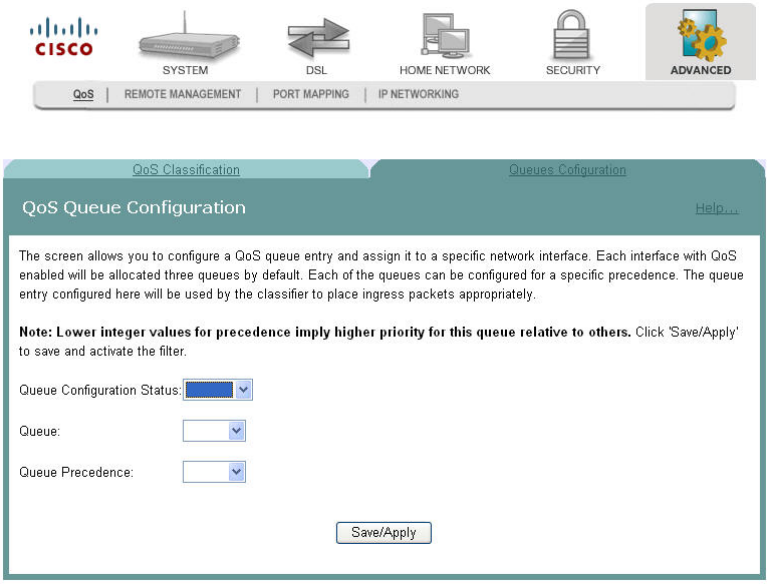
1 Click **Advanced** on the main screen. The Upstream Quality of Service screen opens.



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



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



4 For the Queue Configuration Status, select **Enable** or **Disable** to enable or disable your queue configuration.

5 Select from the Queue drop-down list for the associated WAN interface or connection type for Queue.

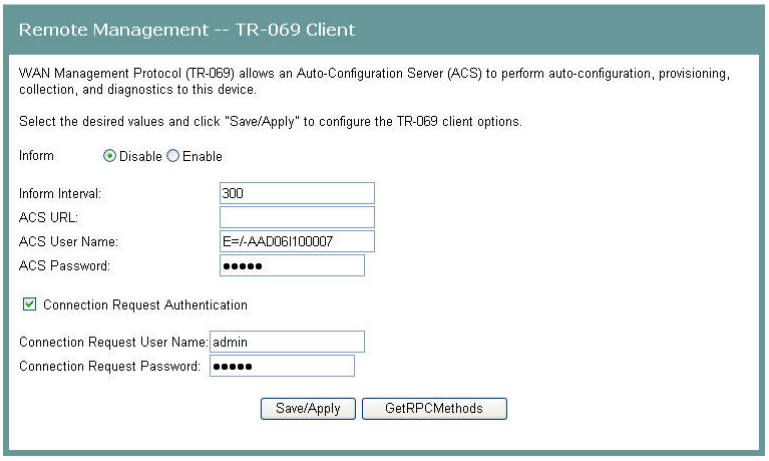
6 For the Queue Precedence field, select the Precedence as the relative priority for the queue. A smaller number indicates a higher priority.

7 Click **Save/Apply** to save the changes.

Remote Management

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

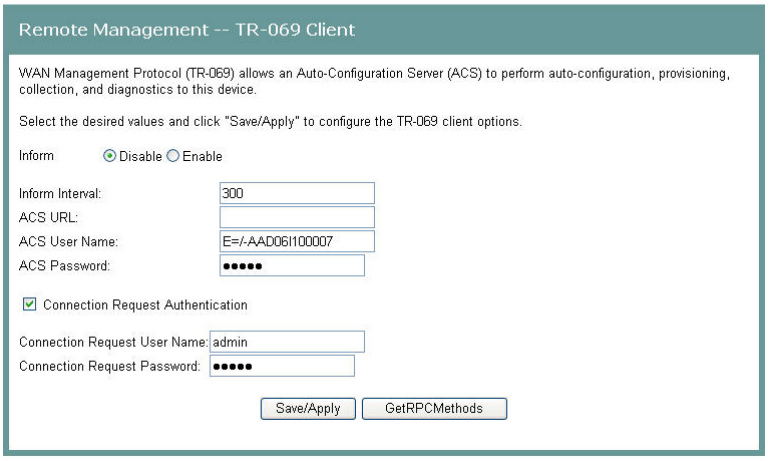
Path: Advanced > Remote Management



Configuring the TR-069 Client Options

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

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



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

- Click **Enable** to enable the periodic "inform" messages from the residential gateway.
- Click **Disable** to disable the inform messages to the residential gateway.

3 In the Inform Interval field, enter the frequency that the inform messages are sent from the residential gateway to the auto-configuration server.

4 In the ACS URL field, enter the URL for the auto-configuration server.

5 In the ACS User Name field, enter the user name for the auto-configuration server.

6 In the ACS Password field, enter the password for the auto-configuration server.

7 Check the **Connection Request Authentication** field.

8 In the Connection Request User Name field, enter the name of the connection request.

9 In the Connection Request Password field, enter the password for the connection request.

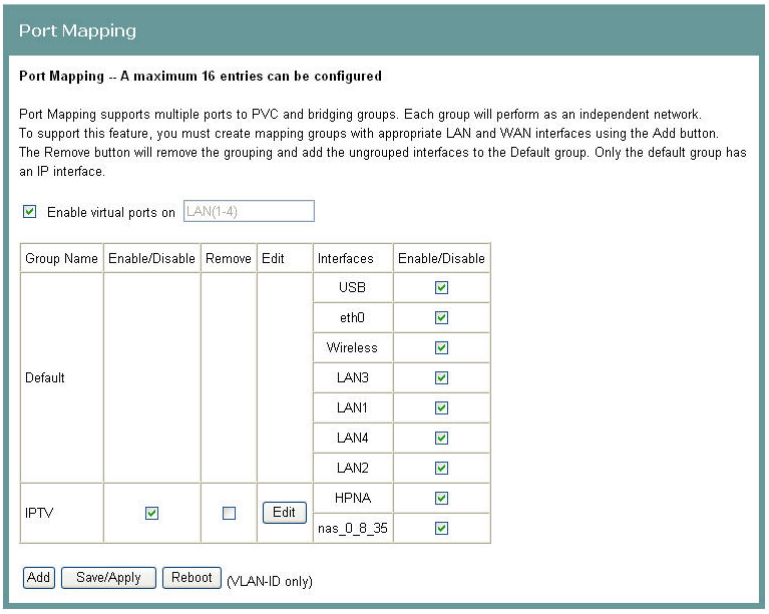
10 Click **GetRPCMethods** to obtain the list of remote procedural calls (RPC) supported by the auto-configuration server.

11 Click **Save/Apply** to save the configuration changes.

Port Mapping

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

Path: Advanced > Port Mapping



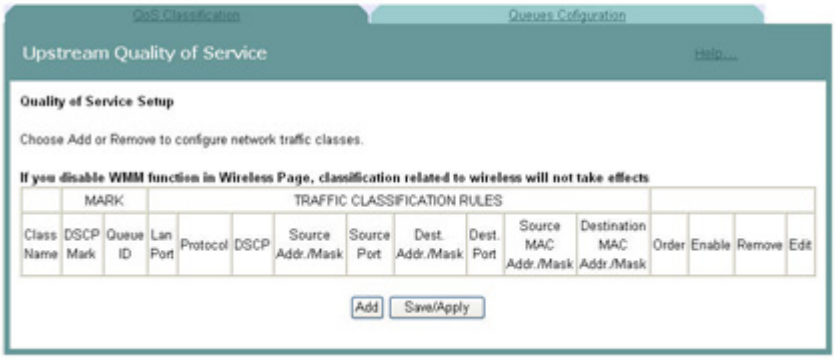
Adding Port Mapping

To add port mapping, complete the following steps.

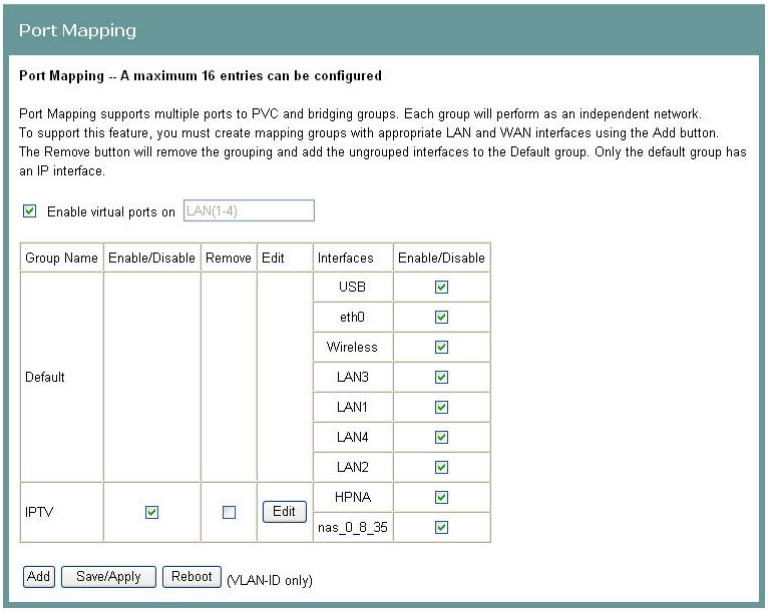
CAUTION:

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

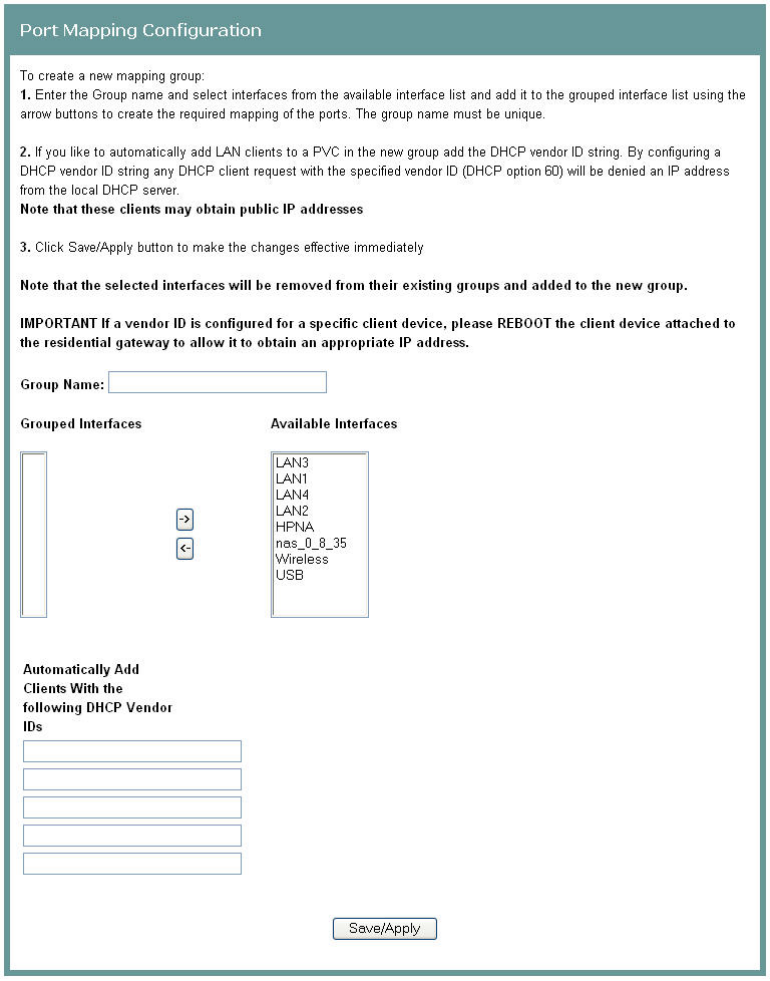
1 Click **Advanced** on the main screen. The Upstream Quality of Service screen opens.



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



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



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

5 For the Grouped Interfaces field, select interfaces from the Available Interfaces list and add them to the grouped interface list using the arrow buttons to create the required mapping of the ports.

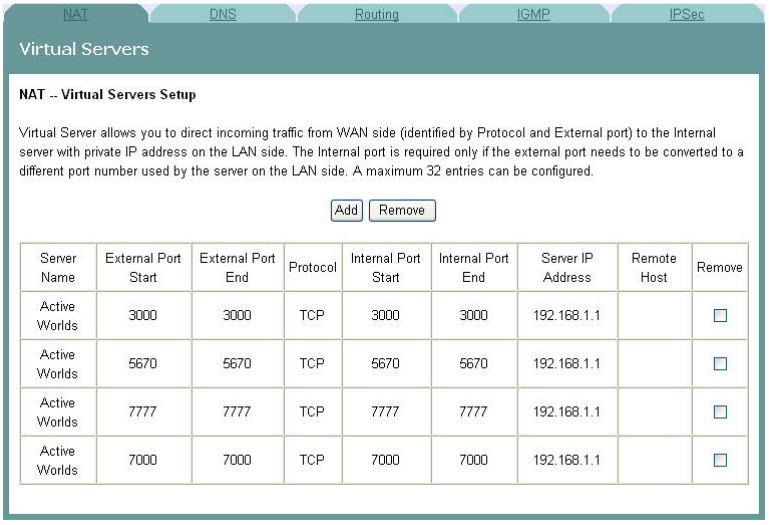
6 In the Automatically Add Clients With the following DHCP Vendor IDs fields, add the DHCP option 60 [vendor ID option] string for the devices (typically IP set-tops) attached to the residential gateway.

7 Click **Save/Apply**.

Virtual Servers Setup

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

Path: Advanced > IP Networking > NAT > Virtual Servers

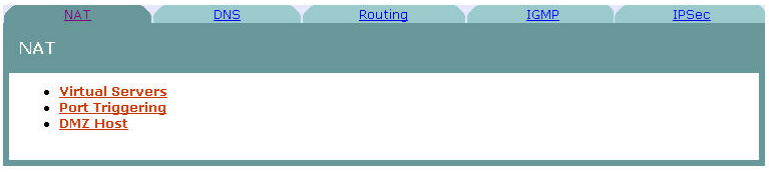


Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remote Host	Remove
Active Worlds	3000	3000	TCP	3000	3000	192.168.1.1		☐
Active Worlds	5670	5670	TCP	5670	5670	192.168.1.1		☐
Active Worlds	7777	7777	TCP	7777	7777	192.168.1.1		☐
Active Worlds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

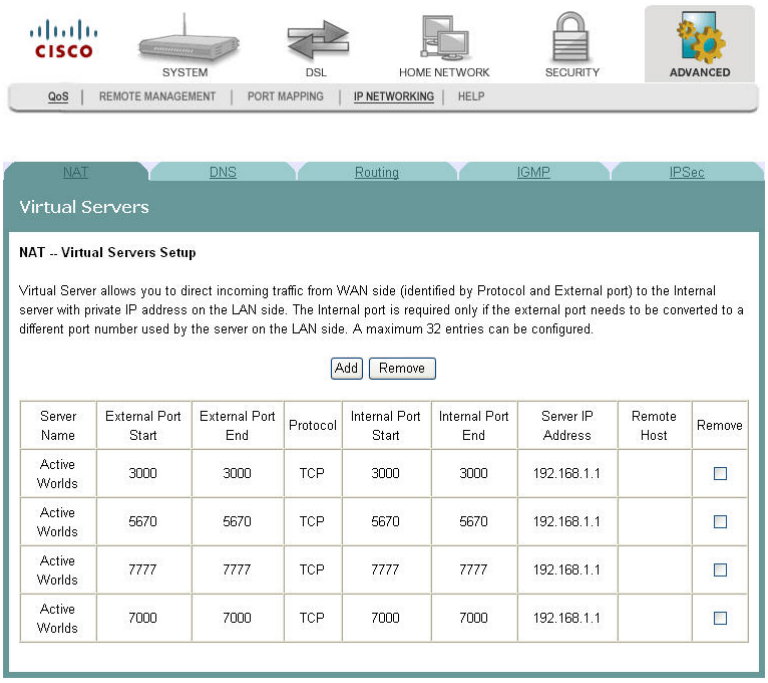
Adding a Virtual Server

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

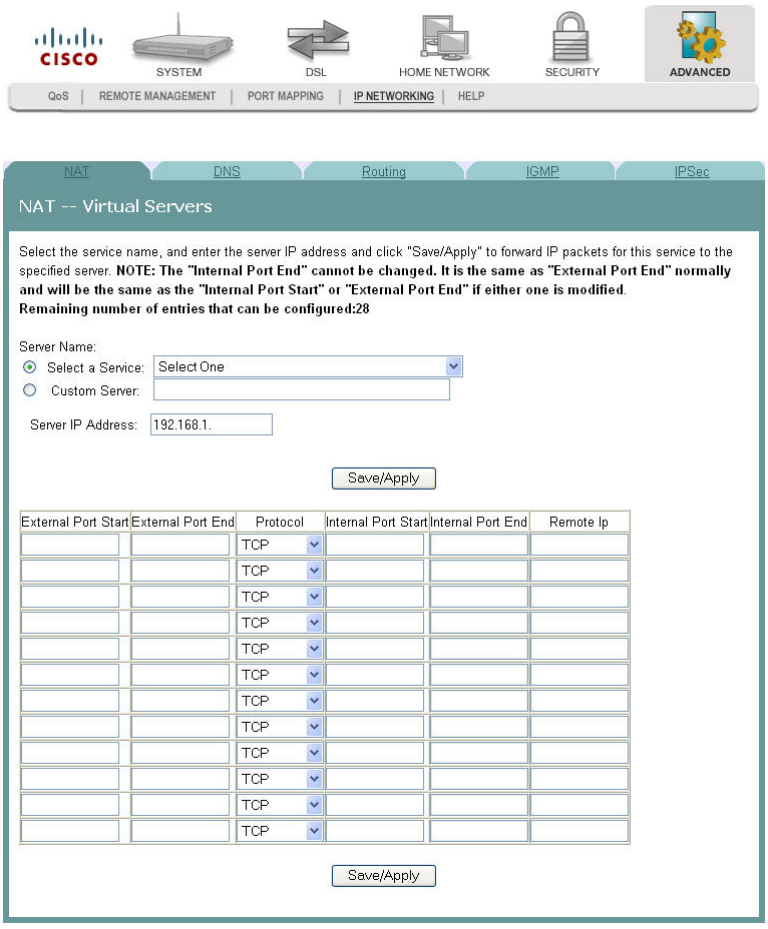
1. Click **Advanced** on the main screen.
2. Click **IP Networking**. The NAT screen opens.



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



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



5 Under Server Name, choose one of the following:

- Click **Select a Service**, and choose a service from the drop-down list.

  OR

- Click **Custom Server**, and enter a server name and the Server IP Address.

6 In the Server IP Address field, enter the IP address for the server.

7 In the External Port Start/End fields, assign the external (Internet) port range of numbers that are associated with the service. These are the ports which will be used for receiving the service request from the WAN. If you have chosen to Select a Service from the above selection, the ports will be entered automatically for you.

8 Under Protocol, select TCP, UDP, or TCP/UDP.

9 In the Internet Port Start/End fields, assign the internal (LAN) port range of numbers that are associated with the service. These are the ports which the actual LAN server defines. If you have chosen to Select a Service from the above selection, the ports will be entered automatically for you.

10 In the Remote IP field, enter the service request (client) sender's IP address. Leave it blank to accept all incoming service requests regardless of the senders' IP address.

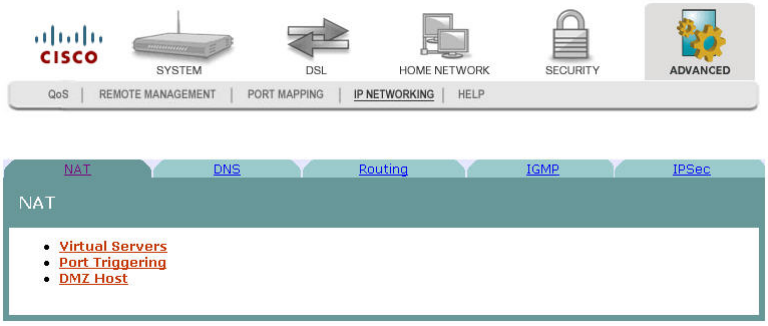
11 Click **Save/Apply** to add the virtual server.

Removing a Virtual Server

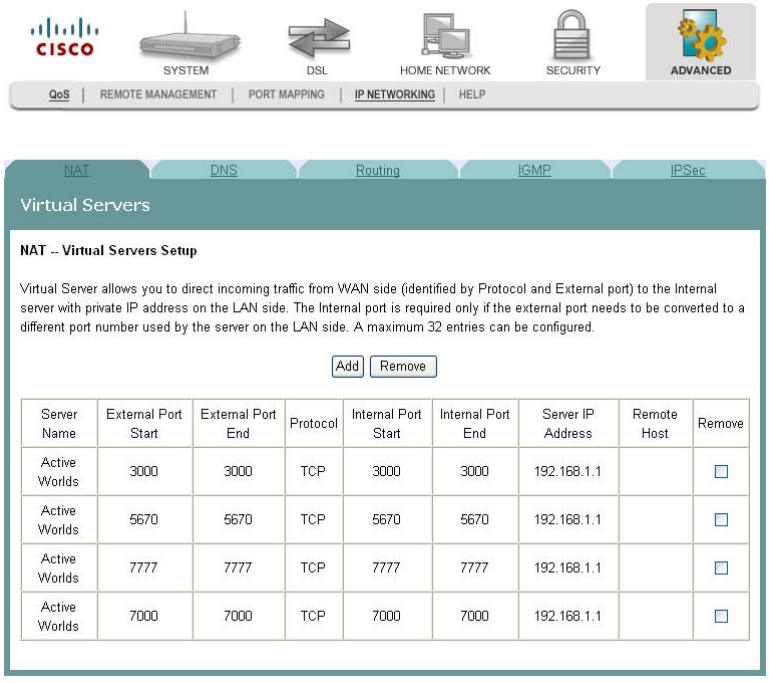
To remove a virtual server, complete the following steps.

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

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



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



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

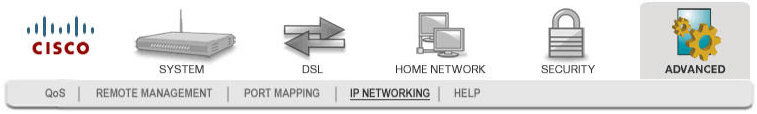
5 Click **Remove** to remove the NAT Virtual Server.

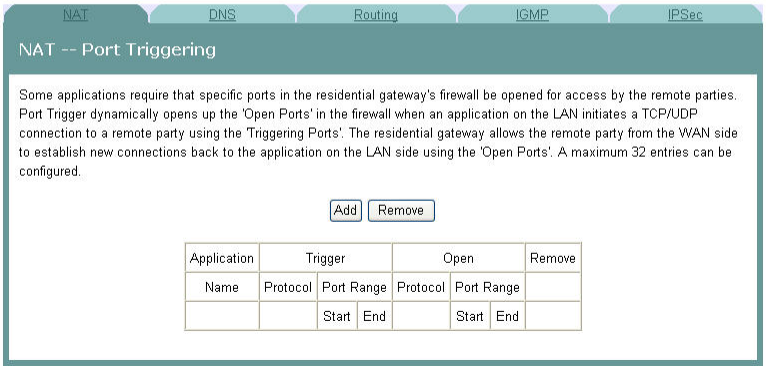
Port Triggering Setup

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

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

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

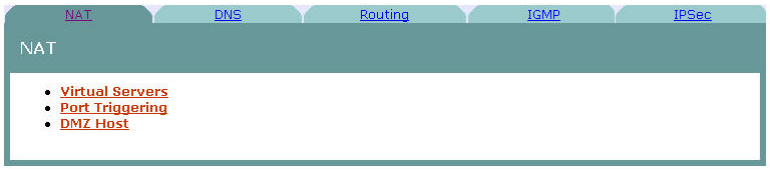




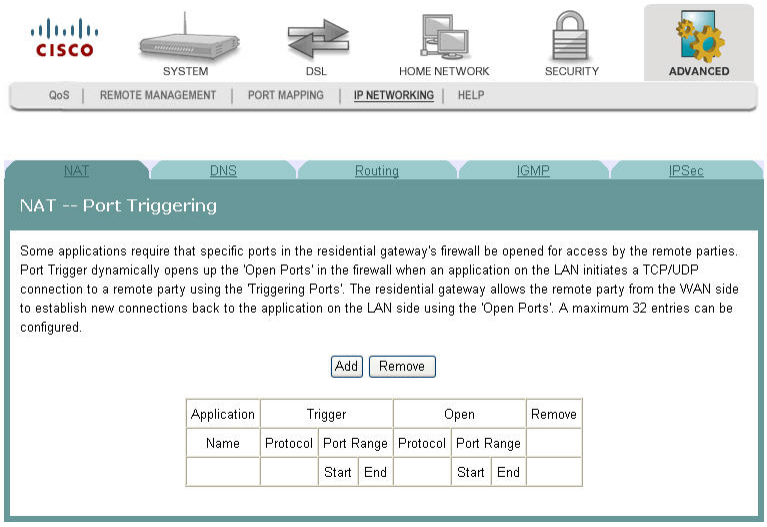
Opening a Port on the Firewall

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

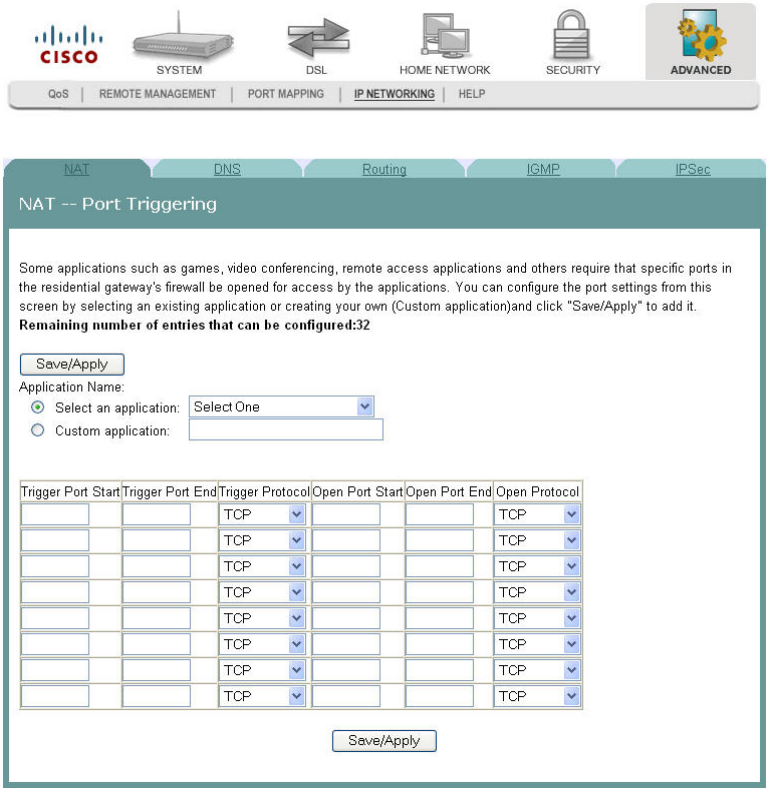
1. Click **Advanced** on the main screen.
2. Click **IP Networking**. The NAT screen opens.



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



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



5 Under Application Name, choose one of the following:

- Click **Select an Application** and choose an application from the drop-down list.

  OR

- Click **Custom Application**, and enter a name for the application.

6 Complete the fields on the screen as follows:

- Under Trigger Port Start, enter the triggering port (start) that will cause the residential gateway to open up the incoming port for the particular LAN computer.
- Under Trigger Port End, enter the triggering port (end) that will cause the residential gateway to open up the incoming port for the particular LAN computer.
- Under Trigger Protocol, select TCP/UDP, TCP, or UDP.
- Under Open Port Start, enter the starting port number of the service you want to open on the firewall.
- Under Open Port End, enter the ending port number of the service you want to open on the firewall.
- Under Open Protocol, select TCP/UDP, TCP, or UDP.

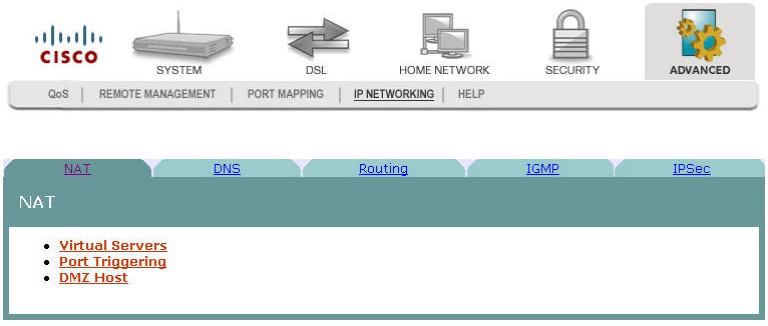
7 Click **Save/Apply** to open the ports on the firewall.

Closing a Port on the Firewall

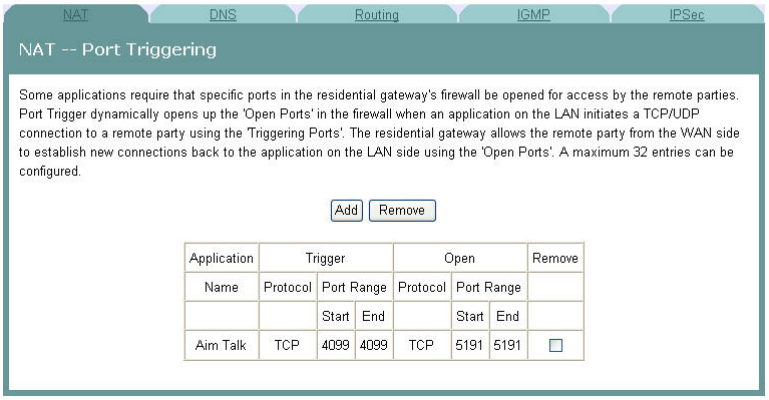
To close a port on the firewall, complete the following steps.

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

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



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



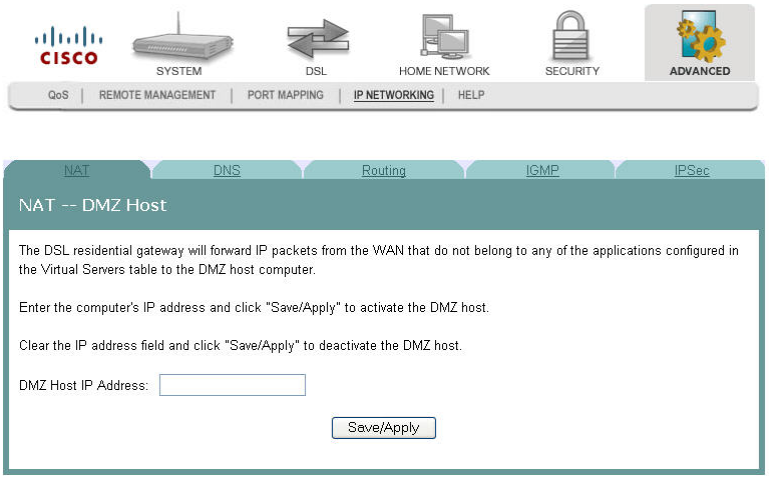
4 From the NAT -- Port Triggering screen, click **Remove** in the Remove column next to the port you wish to close.

5 Click **Remove**. The port you selected is closed.

DMZ Host Setup

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

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



Activate the DMZ Host

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

Deactivate the DMZ Host

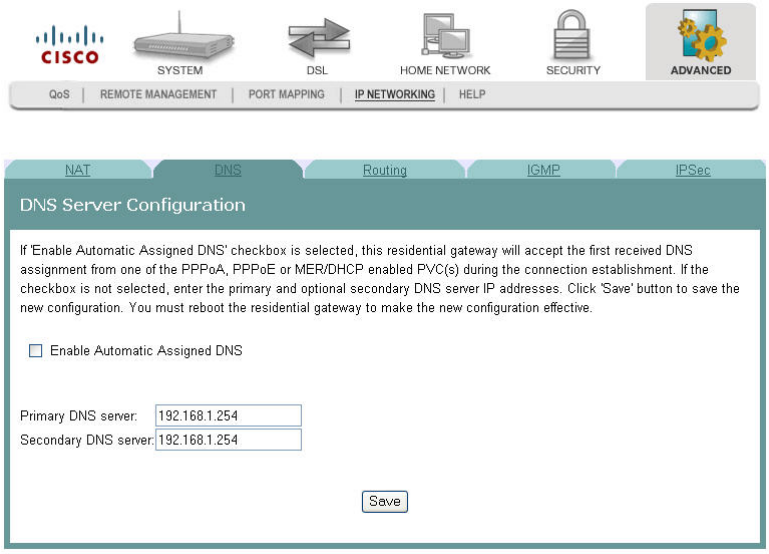
Clear the DMZ Host IP Address field and click **Save/Apply** to deactivate the DMZ host.

DNS Server Configuration

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

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

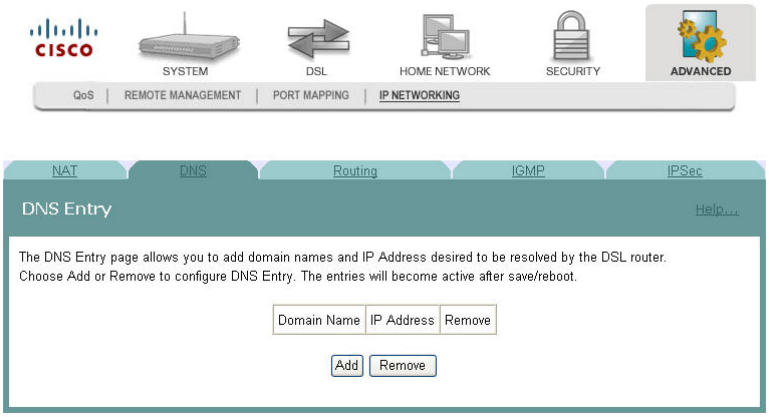
Path: Advanced > IP Networking > DNS > DNS Server



DNS Entries

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

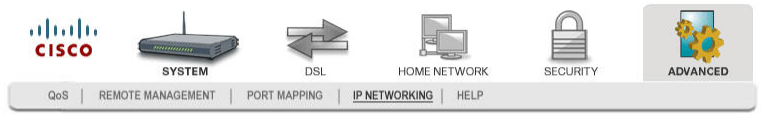
Path: Advanced > IP Networking > DNS > DNS Entries

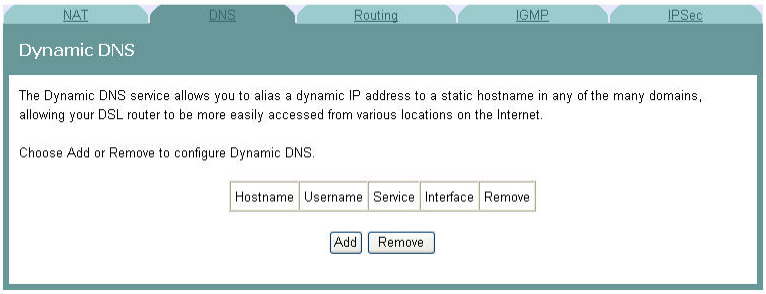


Dynamic DNS

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

Path: Advanced > IP Networking > DNS > Dynamic DNS



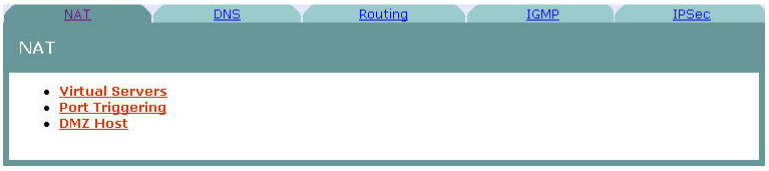


Adding an Alias for a Dynamic IP Address to a Static Host Name

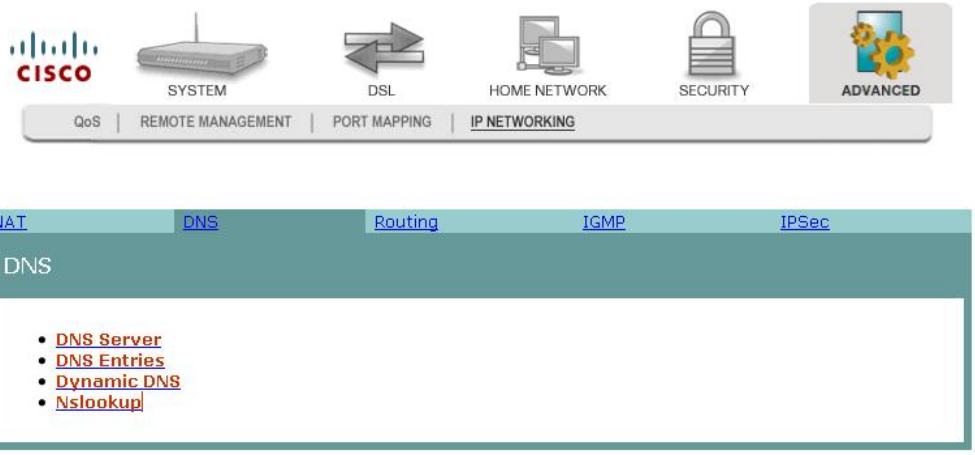
To alias a dynamic IP address to a static host name, complete the following steps.

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

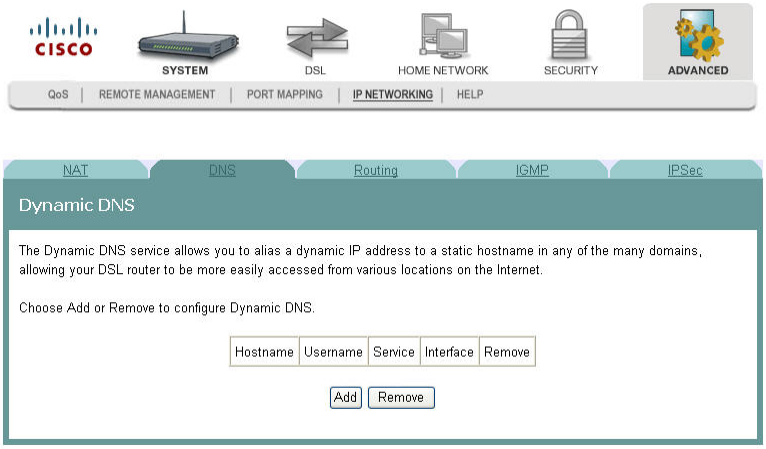
2 Click **IP Networking.** The NAT screen opens.



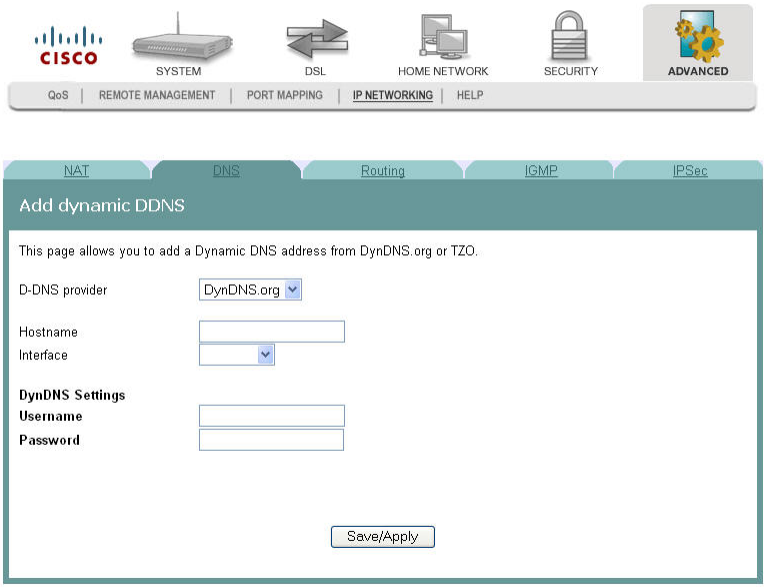
3 Click **DNS**. The DNS screen opens.



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



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



6 In the D-DNS provider field, select the provider from the drop-down list.

7 In the Hostname field, enter the name of the host.

8 In the Interface field, select the interface from the drop-down list.

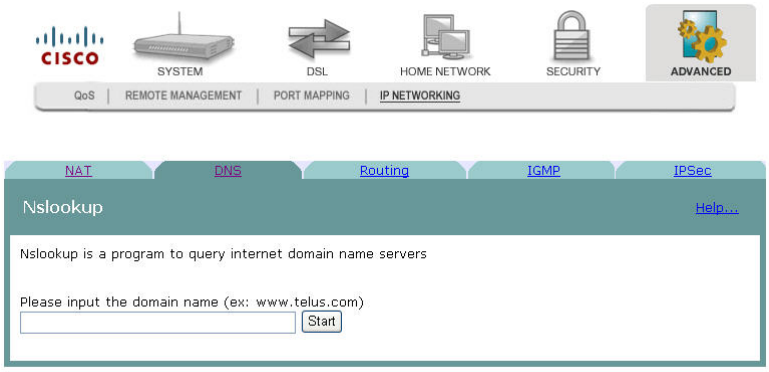
9 Under DynNDS Settings, enter your user name and password.

10 Click **Save/Apply**.

Nslookup

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

Path: Advanced > IP Networking > DNS > Nslookup

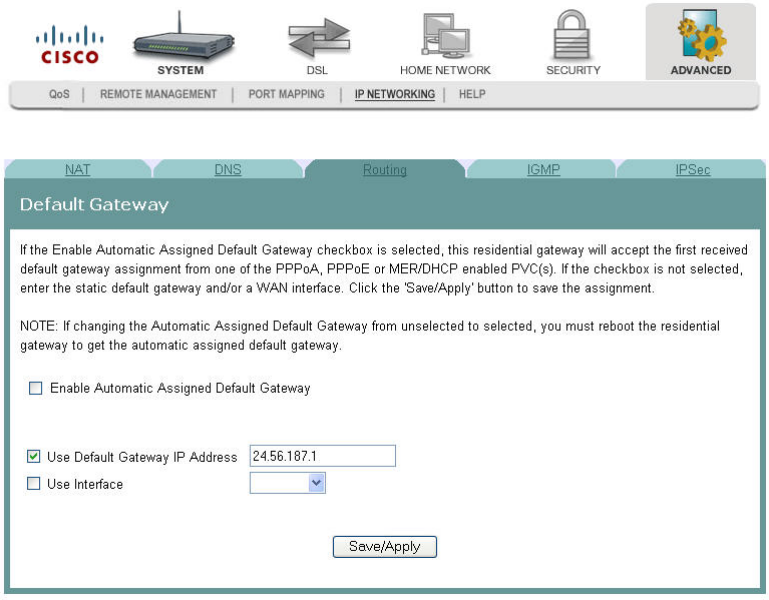


Default Gateway Routing

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

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

Path: Advanced > IP Networking > Routing > Default Gateway

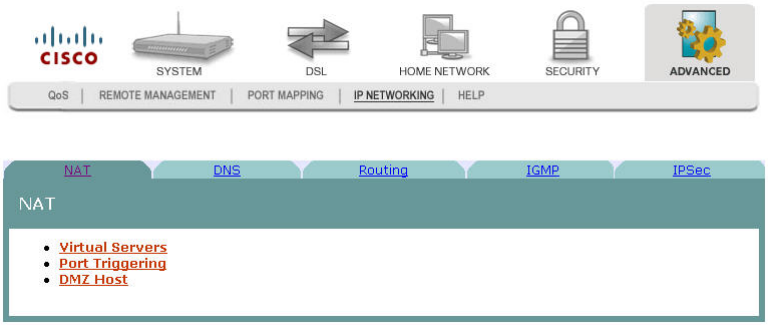


Assigning Default Gateways

To assign a default gateway, complete the following steps.

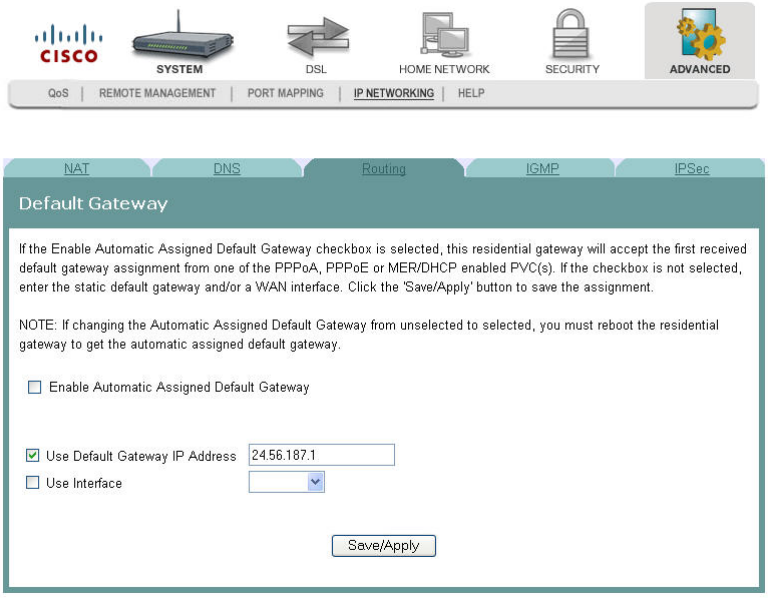
1 Click **Advanced** on the main screen.

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



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

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



5 Do you want to enable the automatic assigned default gateway?

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

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

Static Route

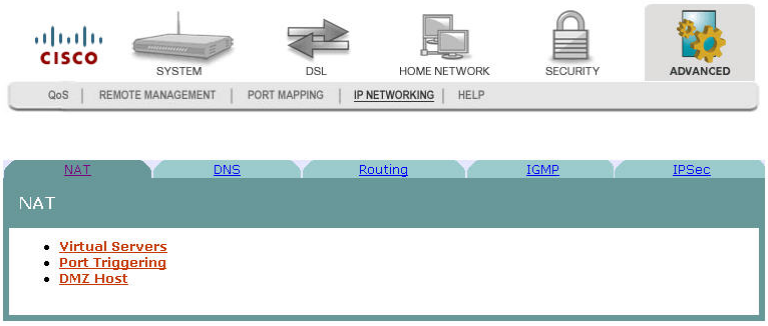
The Residential Gateway lets you set up static routes when routing packets from a specific network to another.

Path: Advanced > IP Networking > Routing > Static Route

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

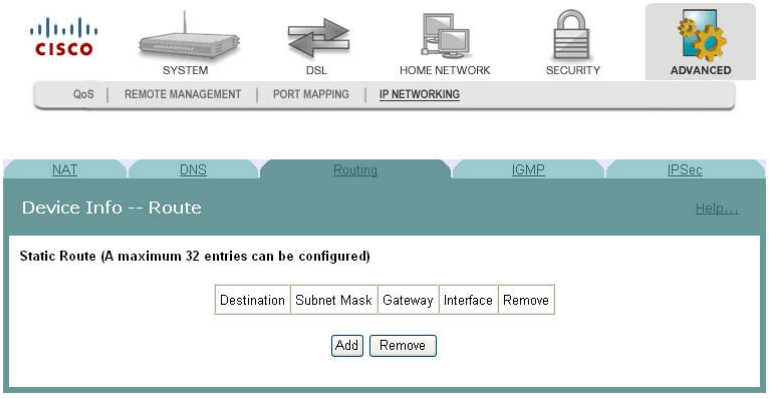
1 Click **Advanced** on the main screen.

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



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

4 Click Static Route. The Device Info -- Route screen opens.



5 Click **Add** to add a new entry.

6 Enter the Destination Network Address which should be a network ID for the destined network.

7 Enter the Subnet Mask for the destined network.

8 Select Use Gateway IP Address and identify the Gateway's IP Address to which the packet is forwarded.

9 Select Use Interface for the interface that is used to forward the packet from the drop-down menu.

10 Click **Save/Apply** at the bottom of the screen.

Ping

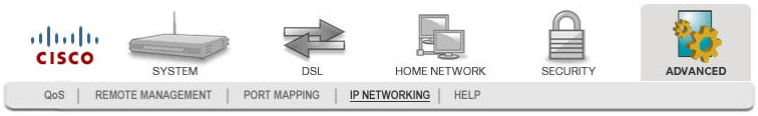
The ping utility can be used to test connectivity with other network devices.

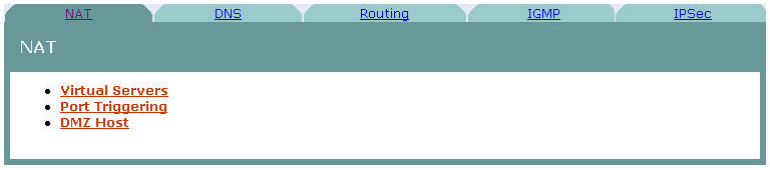
Path: Advanced > IP Networking > Routing > Ping

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

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

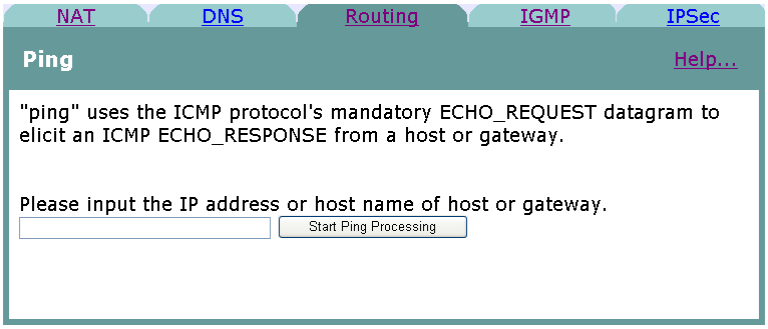
2 Click **IP Networking.** The NAT screen opens.



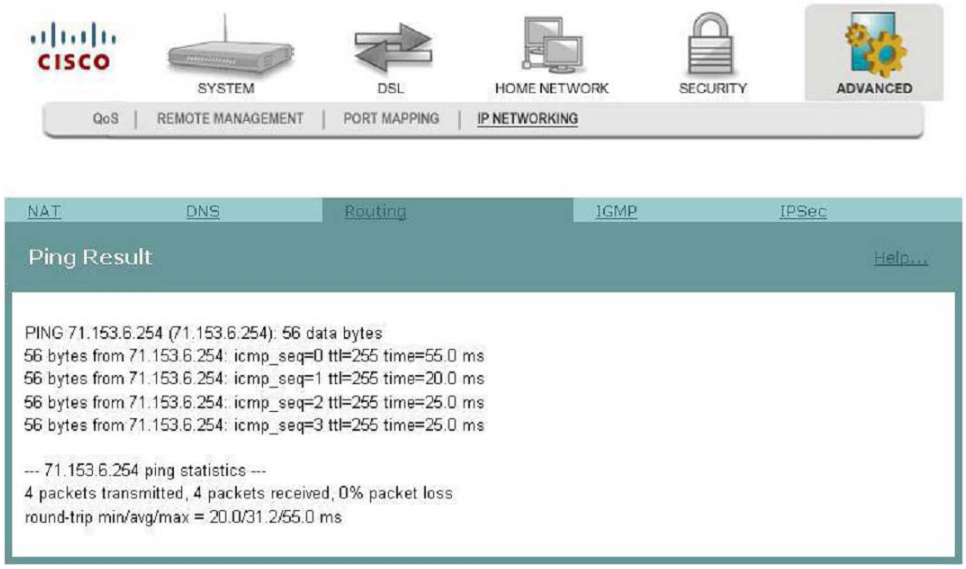


3 Click **Routing.** The Routing screen opens.

4 Click **Ping**. The Ping window opens.



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



DHCP Server Probing

You can set up the residential gateway to perform DHCP server probing, an operation that requests a new DHCP lease if the default gateway happens to be out of service due to a power outage or other problems.

With DHCP server probling, the residential gateway probes the default gateway based on the probing interval value. If the residential gateway encounters consecutive reply failures from the default gateway based on the probing reset trigger value, it will conclude that the default gateway is out of service and will initiate a DHCP request.

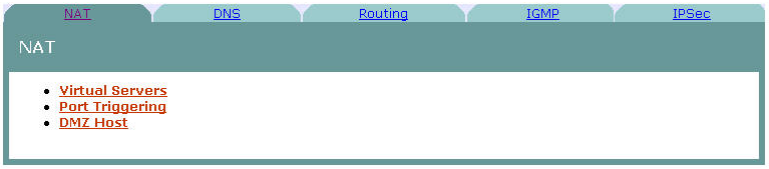
Use the DHCP Server Probing screen to enable (or disable) DHCP server probing and set the probing interval and reset trigger.

Path: Advanced > IP Networking > Routing > DHCP Server Probing

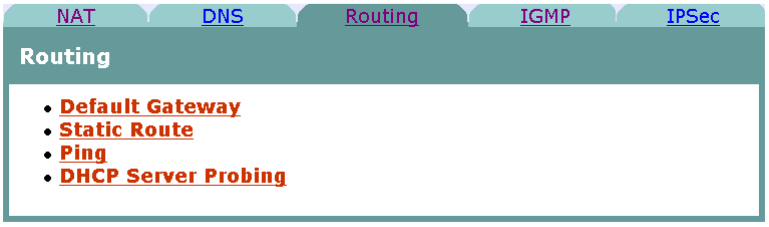
Complete the following steps to access the DHCP Server Probing screen and enable and set up DHCP Server Probing.

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

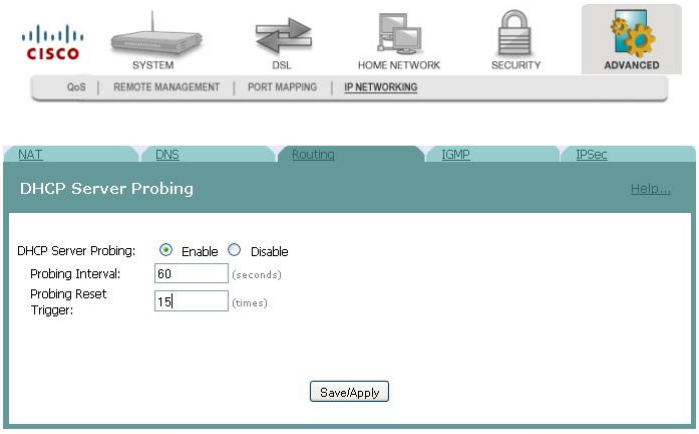
2 Click **IP Networking.** The NAT screen opens.



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



4 Click **DHCP Server Probing**. The DHCP Server Probing screen opens.



5 Select **Enable** to enable DHCP server probing.

6 Enter the **Probing Interval** in seconds, or accept the default value if appropriate.

Note: This parameter defines how often the residential gateway communicates with the default gateway to see if it is still active. The default value is 60 seconds (1 minute).

7 Enter the **Probing Reset Trigger**, or accept the default value if appropriate.

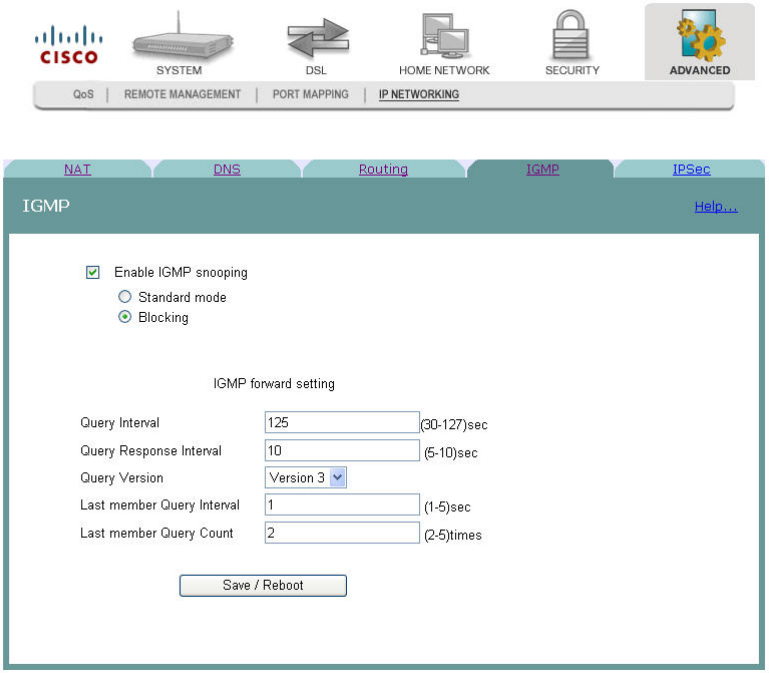
Note: This parameter defines the consecutive number of times the default gateway must fail to respond to probing before a new DHCP lease is requested. the default value is 15.

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

Internet Group Management Protocol

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

Path: Advanced > IP Networking > IGMP



Enabling IGMP Snooping

To enable IGMP snooping, complete the following steps.

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

6 In the Last member Query Interval field, enter the interval in seconds. It is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message.

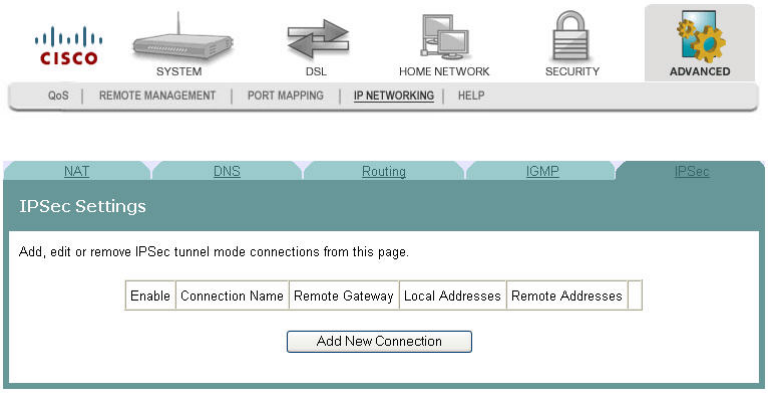
7 In the Last member Query Count field, enter the value in numbers. It is the number of Group-Specific Query messages sent upon receipt of a message indicating a leave. (The default is 2.)

8 Click **Save/Reboot** to save your changes and reboot the system.

IPSec Settings

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

Path: Advanced > IP Networking > IPSec

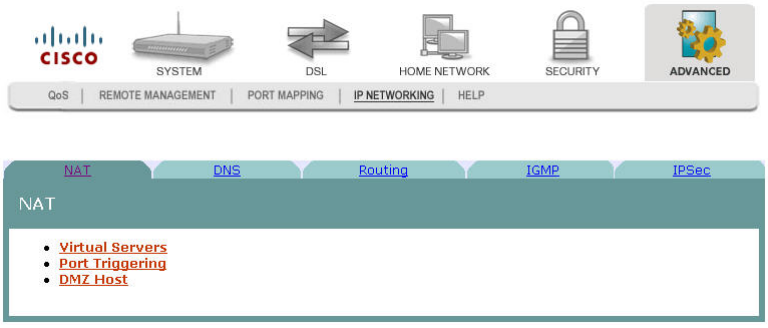


Adding an IPSec Connection

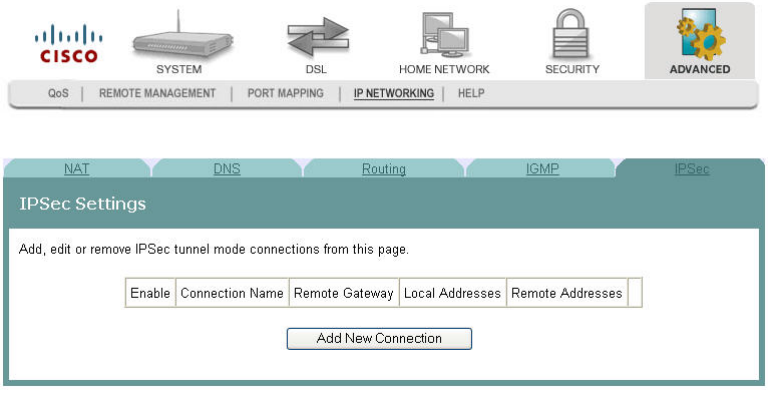
To add an IPSec connection, complete the following steps.

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

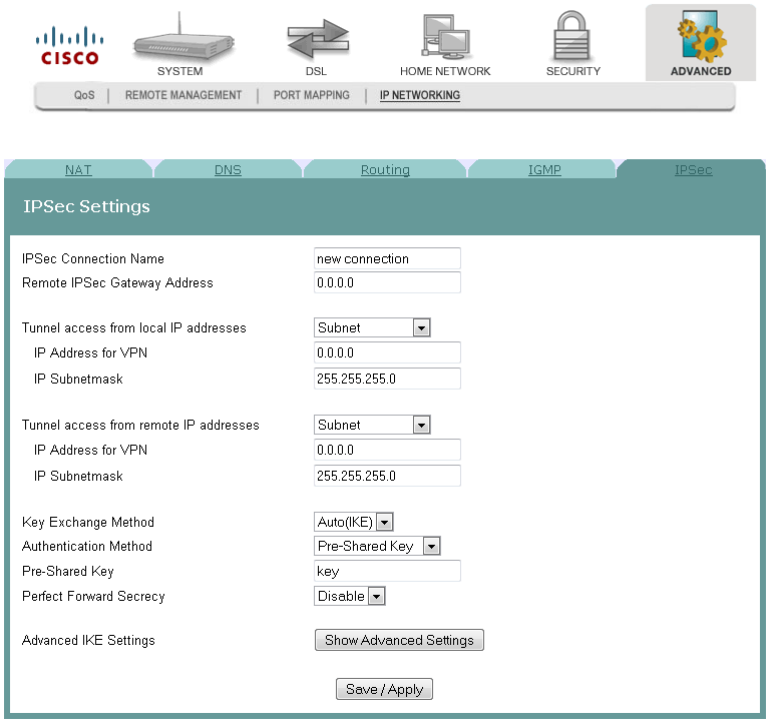
2 Click **IP Networking.** The NAT screen opens.



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



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



5 In the IPSec Connection Name field, enter the name of the connection.

6 In the Remote IPSec Gateway Address field, enter the gateway address for the remote IPSec gateway.

7 In the Tunnel access from local IP addresses field, select Subnet or Single Address.

8 In the IP Address for VPN, enter the IP address for the VPN connection.

9 In the IP Subnetmask field, enter the subnet mask for the VPN IP address.

10 In the Tunnel access from remote IP addresses field, select Subnet or Single Address.

11 In the IP Address for VPN, enter the IP address for the VPN connection.

12 In the IP Subnetmask field, enter the subnet mask for the VPN IP address.

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

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

15 Depending upon the authentication method that you selected, do one of the following:

- If you selected Pre-Shared Key, enter the name of the key in the Pre-Shared Key field.

  OR

- If you selected Certificate (X.509), select a certificate from the drop-down list of certificates in the Certificate field.

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

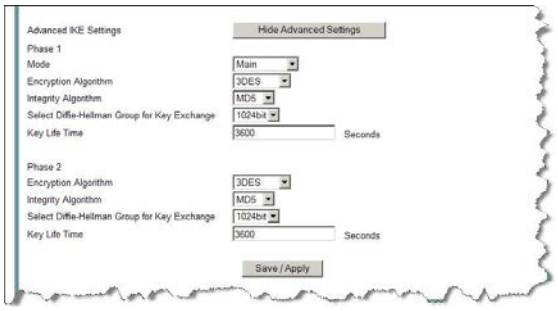
- If you select Enable, Perfect Forward Secrecy is enabled.

  OR

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

17 Do you want to configure the advanced settings?

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



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

18 Complete the advanced settings as follows:

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

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

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

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

d In the Select Diffie-Hellman Group for Key Exchange field, select one of the following options:

- 768 bit
- 1024 bit
- 1536 bit
- 2048 bit
- 3072 bit
- 4096 bit
- 6144 bit
- 8192 bit

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

19 Repeat step 17 for each phase.

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

8

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

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

Index

W

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

678 277-1120
800 722-2009
www.cisco.com

July 2012 Printed in USA

Part Number 4036168 Rev B