



Cisco Model
DPC2420R2/EPC2420R2
DOCSIS/EuroDOCSIS 2.0
Wireless Residential Gateway with
Embedded Digital Voice Adapter
User 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. DOCSIS is a registered trademark of Cable Television Laboratories, Inc. EuroDOCSIS, EuroPacketCable, and PacketCable are trademarks of Cable Television Laboratories, Inc.

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)

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.

Software and Firmware Use

The software described in this document is protected by copyright law and furnished to you under a license agreement. You may only use or copy this software in accordance with the terms of your license agreement.

The firmware in this equipment is protected by copyright law. You may only use the firmware in the equipment in which it is provided. Any reproduction or distribution of this firmware, or any portion of it, without our express written consent is prohibited.





Copyright

© 2011 Cisco Systems, Inc. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

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.

<p>Note to System Installer</p> <p>For this apparatus, the coaxial cable shield/ screen shall be grounded as close as practical to the point of entry of the cable into the building. For products sold in the US and Canada, this reminder is provided to call the system installer's attention to Article 820-93 and Article 820-100 of the NEC (or Canadian Electrical Code Part 1), which provides guidelines for proper grounding of the coaxial cable shield.</p>	<div><div>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</div><div>AVIS RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR</div></div> <p>CAUTION: To reduce the risk of electric shock, do not remove cover (or back). No user-serviceable parts inside. Refer servicing to qualified service personnel.</p> <p>WARNING TO PREVENT FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS UNIT TO RAIN OR MOISTURE.</p>
<div><p>This symbol is intended to alert you that uninsulated voltage within this product may have sufficient magnitude to cause electric shock. Therefore, it is dangerous to make any kind of contact with any inside part of this product.</p></div>	<div><p>This symbol is intended to alert you of the presence of important operating and maintenance (servicing) instructions in the literature accompanying this product.</p></div>





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.

<p>Remarque à l'attention de l'installateur du système</p> <p>Avec cet appareil, le blindage/écran du câble coaxial doit être mis à la terre aussi près que possible du point d'entrée du câble dans le bâtiment. En ce qui concerne les produits vendus aux États-Unis et au Canada, ce rappel est fourni pour attirer l'attention de l'installateur sur les articles 820-93 et 820-100 du Code national de l'électricité (ou Code de l'électricité canadien, Partie 1) qui fournissent des lignes directrices concernant la mise à la terre correcte du blindage (écran) du câble coaxial.</p>	<div><div>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</div><div>ATTENTION DANGER ÉLECTRIQUE NE PAS OUVRIR</div></div> <p>ATTENTION : Pour réduire les risques de chocs électriques, ne pas enlever le couvercle (ou le panneau arrière). Ne contient aucune pièce réparable par l'utilisateur. Confier les interventions aux techniciens d'entretien qualifiés.</p> <p>AVERTISSEMENT POUR ÉVITER LES INCENDIES OU LES CHOCs ÉLECTRIQUES, NE PAS EXPOSER L'APPAREIL À LA PLUIE OU À L'HUMIDITÉ.</p>
<div><p>Ce symbole a pour but de vous prévenir que des tensions électriques non isolées existent à l'intérieur de ce produit, pouvant être d'une intensité suffisante pour causer des chocs électriques. Il est donc dangereux d'établir un contact quelconque avec l'une des pièces comprises à l'intérieur de ce produit.</p></div>	<div><p>Ce symbole a pour but de vous prévenir de la présence d'instructions importantes relatives au fonctionnement ou à l'entretien (et aux réparations) dans la documentation accompagnant ce produit.</p></div>

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.

<p>Mitteilung an den Systemtechniker</p> <p>Für dieses Gerät muss der Koaxialkabelschutz/ 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 820-93 und Paragraph 820-100 der US-Elektrovorschrift NEC (oder der kanadischen Elektrovorschrift Canadian Electrical Code Teil 1) aufmerksam machen, in denen die Richtlinien für die ordnungsgemäße Erdung des Koaxialkabelschirms festgehalten sind.</p>	<div><div>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</div><div>ACHTUNG STROMSCHLAGGEFAHR, NICHT ÖFFNEN</div></div> <p>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.</p> <p>WARNUNG DAS GERÄT NICHT REGEN ODER FEUCHTIGKEIT AUSSETZEN, UM STROMSCHLAG ODER DURCH EINEN KURZSCHLUSS VERURSACHTEN BRAND ZU VERMEIDEN.</p> <div></div>
<div></div> <p>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.</p>	<p>Dieses Symbol weist den Benutzer darauf hin, dass die mit diesem Produkt gelieferte Dokumentation wichtige Betriebs- und Wartungsanweisungen für das Gerät enthält.</p>

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.

<p>Nota para el instalador del sistema</p> <p>En lo que se refiere a este aparato, el blindaje del cable coaxial 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 820-93 y 820-100 del NEC (o Código Eléctrico de Canadá, Parte 1), que proporcionan directrices para una correcta conexión a tierra del blindaje del cable coaxial.</p>	<div><div>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</div><div>ATENCIÓN RIESGO DE DESCARGA ELÉCTRICA NO ABRIR</div></div> <p>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.</p> <p>ADVERTENCIA PARA EVITAR EL RIESGO DE INCENDIO O DESCARGA ELÉCTRICA, NO EXPONGA LA UNIDAD A LA LLUVIA O A LA HUMEDAD.</p> <div></div>
<div></div> <p>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.</p>	<p>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.</p>


Contents

IMPORTANT SAFETY INSTRUCTIONS	v
About This Guide	xv
Chapter 1 Introducing the DOCSIS Residential Gateway	1
Introduction	2
What's In the Carton?	4
Front Panel Description	6
Back Panel Description.....	7
Chapter 2 Installing the DOCSIS Residential Gateway	9
Installation Preparations	10
Install the Residential Gateway	18
Chapter 3 Configuring the DOCSIS Residential Gateway	23
Log in to the DOCSIS Residential Gateway for the First Time	24
Configure Basic Settings	27
Configure Advanced Settings	47
Configure Firewall Settings.....	68
Configure Parental Control Settings	75
Configure Wireless Settings	84
Chapter 4 Operation of Front Panel Indicators	101
Initial Power Up, Calibration, and Registration (AC Power applied).....	102
Normal Operations (AC Power Applied)	104
Special Conditions	105
Chapter 5 Troubleshooting the DOCSIS Residential Gateway	107
Frequently Asked Questions.....	108
Common Troubleshooting Issues.....	114
Tips for Improved Performance	116

Contents

Chapter 6 Customer Information	117
Index	119

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 is 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.

IMPORTANT SAFETY INSTRUCTIONS

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 Power/Mains Overloads



WARNING: Avoid electric shock and fire hazard! Do not overload AC power/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.

Operating Environment

This product is designed for operation indoors with a temperature range from 32° to 104° F (0° to 40°C). Each product should have adequate spacing on all sides so that the cooling air vents on the chassis are not blocked.

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 shock 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

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.*

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.

<p>DOCSIS Residential Gateway Model(s): DPC2420R2 EPC2420R2 Manufactured by: Cisco Systems, Inc. 5030 Sugarloaf Parkway Lawrenceville, Georgia 30044 USA Telephone: 770 236-1077</p>
--

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.

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.

United States FCC Compliance

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).

20100527 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.
Cesky [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/EU 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 así como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιαστικές 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 è 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 essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Maltese [Maltese]:	Dan l-apparat huwa konformi mal-ftigiet 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 în conformitate cu cerințele esențiale și 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.

CE Compliance

Note: The full declaration of conformity for this product can be found at http://www.cisco.com/web/consumer/support/compliance_info.html.

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:



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.

20110311_CE_Modem/EMTA

About This Guide

Introduction

Welcome. This guide provides instructions and recommendations for placing, installing, configuring, operating, maintaining, and troubleshooting the DPC2420R2 and EPC2420R2 DOCSIS Residential Gateways.

Purpose

This guide covers the following product models:

- DPC2420R2 DOCSIS Residential Gateway
- EPC2420R2 EuroDOCSIS Residential Gateway

All features described in this guide are standard to these models of residential gateways unless otherwise noted. For the purpose of this guide, whenever a feature or option applies to only a specific model, the model number is specified. If a model number is not specified, then the feature or option applies to both of the models.

Audience

This guide is written for the home subscriber.

Document Version

This is the first formal release of this document.

1

Introducing the DOCSIS Residential Gateway

Introduction

This chapter provides an overview of residential gateway features, indicators, and connectors to help you become familiar with the residential gateway and the benefits it offers. This chapter also lists the accessories and equipment that are provided with the residential gateway so you can verify that you received all of these items.

In This Chapter

■ Introduction.....	2
■ What's In the Carton?	4
■ Front Panel Description	6
■ Back Panel Description	7

Introduction

Welcome to the exciting world of high-speed Internet and high-quality digital telephone service. Your new Cisco® Model DPC2420R2 DOCSIS® 2.0 or EPC2420R2 EuroDOCSIS™ 2.0 Wireless Residential Gateway with Embedded Digital Voice Adapter is a cable modem that meets industry standards for high-speed data connectivity and delivers reliable digital telephone service. It can simultaneously provide both wired (Ethernet) and wireless gateway capabilities to support high-speed data access and provide cost-effective voice services – all in one device. With a DPC2420R2 or EPC2420R2 residential gateway, your Internet enjoyment, home and business communications, and personal productivity will surely soar.

This guide provides procedures and recommendations for placing, installing, configuring, operating, and troubleshooting your DPC2420R2 and EPC2420R2 residential gateway for high-speed Internet and digital telephone service for your home or office. Refer to the appropriate section in this guide for the specific information you need for your situation. Contact your service provider for more information about subscribing to these services.

Your new residential gateway offers the following outstanding benefits and features:

- Compliant with DOCSIS 2.0, and 1.x standards along with PacketCable™ and EuroPacketCable™ specifications to deliver high-end performance and reliability
- High performance broadband Internet connectivity to energize your online experience
- One or two-line embedded digital voice adapter for wired telephony service
- One 10/100 BASE-T Ethernet port to provide wired connectivity
- 802.11n Wireless Access Point
- Wi-Fi Protected Setup (WPS), including a push button switch to activate WPS for simplified and secure wireless setup
- A Wireless ON/OFF button (optional) to easily enable and disable the wireless feature
- User configurable Parental Control blocks access to undesirable Internet sites
- Advanced firewall technology deters hackers and protects the home network from unauthorized access
- Attractive compact design that allows for vertical, horizontal, or wall-mounted operation
- Color-coded interface ports and corresponding cables simplify installation and setup

- DOCSIS-5 compliant LED labeling and behavior provides a user and technician friendly method to check operational status and act as a troubleshooting tool
- Allows automatic software upgrades by your service provider

What's In the Carton?

When you receive your residential gateway, you should check the equipment and accessories to verify that each item is in the carton and that each item is undamaged. The carton contains the following items:



One DPC2420R2 or EPC2420R2
DOCSIS Residential Gateway



One wall-mount style power adapter
(Image may vary from actual product.
Used only with models requiring
external power supply.)



One desktop-style power adapter
(Image may vary from actual product.
Used only with models requiring
external power supply.)



One Ethernet cable (May not be
provided with all products.)



One CD-ROM

What's In the Carton?

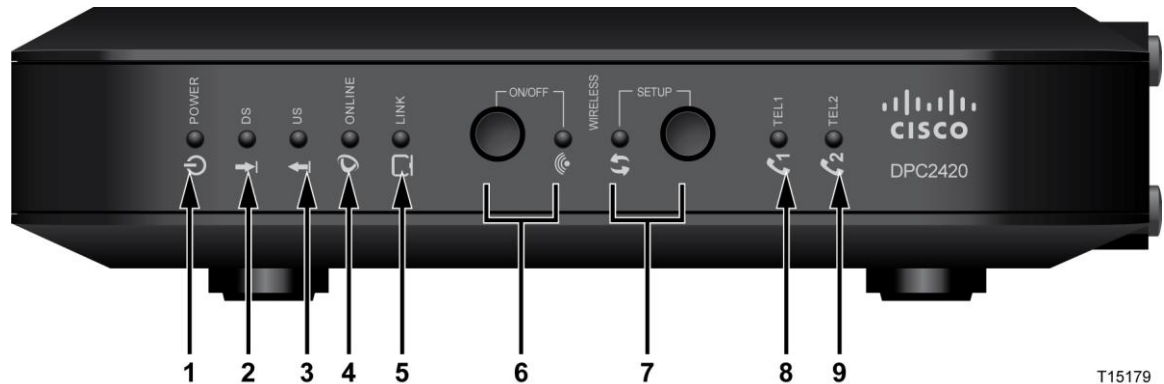
If any of these items are missing or damaged, please contact your service provider for assistance.

Notes:

- You need an optional cable signal splitter and additional standard RF coaxial cables if you want to connect a VCR, a Digital Home Communications Terminal (DHCT) or a set-top converter, or a TV to the same cable connection as your residential gateway.
- If your product supports telephone service, cables and other equipment needed for telephone service must be purchased separately. Contact your service provider to inquire about the equipment and cables you need for telephone service.

Front Panel Description

The front panel of your residential gateway provides LED status indicators that indicate how well and at what state your residential gateway is operating. See *Operation of Front Panel Indicators* (on page 101), for more information on front panel LED status indicator functions.



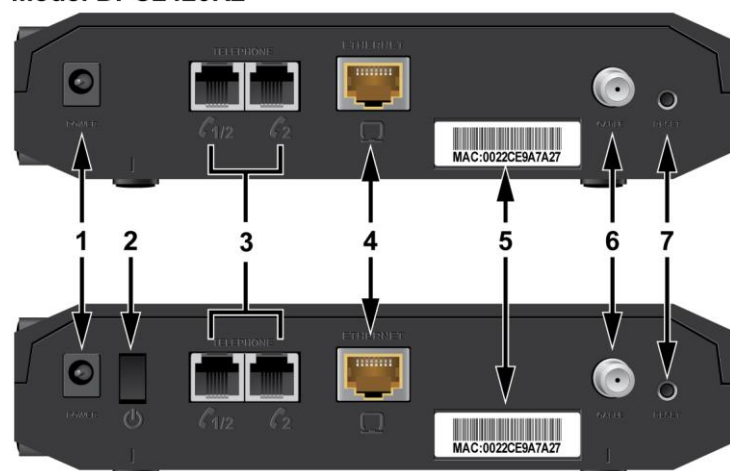
T15179

- 1 **POWER**—ON, power is applied to the residential gateway
- 2 **DS**—ON, the residential gateway is receiving data from the cable network
- 3 **US**—ON, the residential gateway is sending data to the cable network
- 4 **ONLINE**—ON, the residential gateway is registered on the network and fully operational
- 5 **LINK**—ON, the wireless access point is operational. BLINKING indicates that data is being transferred over the wireless connection. OFF indicates that the wireless access point has been disabled by the user
- 6 **WIRELESS ON/OFF** (Optional)—Press this button to activate and turn on the Wireless feature. This feature allows users to transfer data over the wireless connection. When the WIRELESS indicator is ON, it indicates that the Wireless Access Point is operational. BLINKING indicates that data is being transferred over the wireless connection. OFF indicates that the Wireless feature has been disabled.
- 7 **WIRELESS SETUP**—Press this button to activate the Wireless Setup feature. This feature allows users to add new Wireless Protected Setup (WPS) compliant wireless clients to the home network. When the SETUP indicator is OFF (normal condition), it indicates that the wireless setup is not active. BLINKING indicates the user has activated wireless setup to add new wireless clients on the wireless network.
- 8 **TEL1**—ON indicates telephony service is enabled. Blinks when line 1 is in use. OFF indicates that phone service for TEL 1 is not enabled
- 9 **TEL2** (Optional)—ON indicates telephony service is enabled. Blinks when line 2 is in use. OFF indicates that phone service for TEL 2 is not enabled

Back Panel Description

The following illustration identifies the back panel components on the DPC2420R2 and EPC2420R2 residential gateways. Descriptions for each component follow the illustration.

Model DPC2420R2



Model EPC2420R2

T15180

Important: Do not connect your PC to both the Ethernet and USB ports at the same time. Your residential 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 adapter that is provided with your residential gateway
Important: Use only the power supply provided with your residential gateway.
- 2 **ON/OFF SWITCH (Provided only on products that carry the CE mark)** – Allows you to turn off of the residential gateway without removing the power cord. Turning the residential gateway off using this switch ensures that the unit is consuming no energy.
- 3 **TELEPHONE 1/2** – RJ-11 telephone ports connect to home telephone wiring to conventional telephones or fax machines. This port provides connections to Line 1 and Line 2 telephone service. In most installations this connector should be used to connect telephone service
TELEPHONE 2 (Optional) – RJ-11 telephone ports connect to home telephone wiring to conventional telephones or fax machines. This port is used to connect a single -line phone to Line 2 telephone service
- 4 **ETHERNET** – One RJ-45 Ethernet port connects to the Ethernet port on your PC or your home network
- 5 **MAC ADDRESS LABEL** – Displays the MAC address of the residential gateway

Chapter 1 Introducing the DOCSIS Residential Gateway

- 6 **CABLE**—F-connector connects to an active cable signal from your service provider
- 7 **RESET**—A momentary pressing (1-2 seconds) of this switch restarts (power cycles) the device. Pressing and holding the switch for more than ten seconds first causes a reset-to-factory-default of all settings and then restarts (power cycles) the device



CAUTION:

The RESET button is for maintenance purposes only. Do not use unless instructed to do so by your service provider. Doing so may cause you to lose any settings you have selected.

2

Installing the DOCSIS Residential Gateway

Introduction

This chapter describes how to properly install the residential gateway and to connect the residential gateway to a computer and other devices.

In This Chapter

- Installation Preparations..... 10
- Install the Residential Gateway 18

Installation Preparations

Before installing the residential gateway, make sure that your system meets or exceeds the requirements listed in this section. Also, make sure that you have prepared your home and home devices as described in this section.

What Are the System Requirements for Internet Service?

To ensure that your residential gateway operates efficiently for high-speed Internet service, you must have an Internet-capable PC, Mac, or Internet appliance equipped with an Ethernet port. To access the user guide for this product, you must have a CD-ROM drive.

Note: You will also need an active cable input line and an Internet connection.

What Are the Requirements for Telephone Service?

If you intend to use the residential gateway for digital telephone service, verify that your home meets or exceeds all of the following requirements.

Maximum Number of Telephones

The RJ-11 telephone-style connectors on the residential gateway can each provide telephone service to multiple telephones, fax machines, and analog modems.

The maximum number of telephone devices connected to each RJ-11 port is limited by the total Ringing Load of the telephone devices that are connected. Many telephone devices are marked with a Ringer Equivalent Number (REN). Each telephone port on the residential gateway can support up to a 5 REN load.

The sum of the REN load on all of the telephone devices attached to each port must not exceed 5 REN.

Telephone Device Types

You can use telephone devices that are not labeled with a REN number, but the maximum number of attached telephone devices cannot be accurately calculated. With telephone devices that are not labeled, each device should be connected and the ring signal should be tested before adding more devices. If too many telephone devices are attached and the ring signal can no longer be heard, telephone devices should be removed until the ring signal works properly.

Telephones, fax machines, and other telephone devices use the center 2 pins of the RJ-11 connectors to connect to your primary service. The outer 2 pins of the connector may be provisioned to provide a second telephone line. Contact your service provider for more information.

Dialing Requirements

All your telephones should be set to use Dual-Tone Multi-Frequency (DTMF) dialing. Pulse dialing may not be supported by your local service provider.

Telephone Wiring Requirements

The residential gateway supports connecting to the interior telephone wiring as well as connecting directly to a telephone or fax machine. The maximum distance from the unit to the most distant telephone device must not exceed 1000 feet (300 meters). Use 26-gauge twisted-pair, or larger, telephone wiring.

Important: Connection to an existing or a new permanently installed home telephone wiring network should be completed by a qualified installer or at the direction of your telephone service provider.

What Types of Service Accounts Do I Need?

Depending upon the features your service provider offers, you may need to establish one or both of the following accounts:

- A high-speed Internet access account, if your residential gateway supports an Internet connection
- An account for telephone service, if your residential gateway supports digital telephone service

Refer to one of the following topics to learn more about the types of service accounts that you may need to establish.

High-Speed Internet Access Account

If you do *not* have a high-speed Internet access account, your service provider will set up your account and become your Internet Service Provider (ISP). Internet access enables you to send and receive e-mail, access the World Wide Web, and receive other Internet services.

You will need to give your service provider information about the residential gateway in order to use the high-speed internet feature that this product offers. Refer to *Information Your Service Provider Needs* (on page 12) to learn how to locate the information your service provider needs to establish a high-speed Internet access account for the residential gateway

If you have an existing high-speed Internet access account, you will need to give your service provider the serial number and MAC address of the residential gateway in order to use the high-speed internet feature that this product offers. Refer to *Information Your Service Provider Needs* (on page 12) to learn how to locate this information.

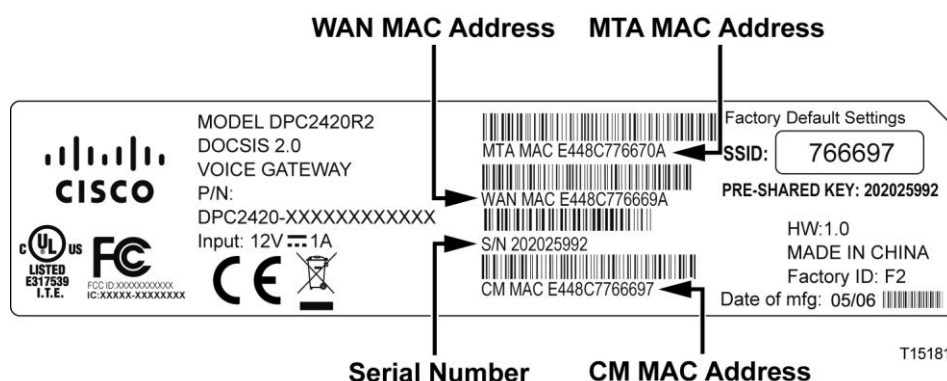
Chapter 2 Installing the DOCSIS Residential Gateway

Information Your Service Provider Needs

You will need to give your service provider the following information, which is printed on the bar code label attached to the device:

- The Serial Number (S/N) serial number of the residential gateway.
- The CM Media Access Control (CM MAC) address of the residential gateway.
- Other MAC address numbers as needed

The following illustration shows a typical bar coded label; the image may vary from the label on the actual product.



Write down these numbers in the spaces provided:

Serial Number _____

CM MAC Address _____

Other MAC Address _____

I Already Have a High-Speed Internet Access Account

Telephone Service

You will need to establish a telephone account with your local service provider to use your residential gateway for telephone service.

When you contact your service provider, you may be able to transfer your existing telephone numbers. If not, then your cable telephony service provider will assign a new telephone number to enable your voice service(s). Discuss these options with your telephony service provider.

Where Is the Best Location for My Residential Gateway?

The ideal location for your residential gateway is where it has access to outlets and other devices. Think about the layout of your home or office, and consult with your service provider to select the best location for your residential gateway. Read this user guide thoroughly before you decide where to place your residential gateway.

Consider these recommendations:

- Choose a location close to your computer if you will also use the residential gateway for high-speed Internet service.
- Choose a location that is near an existing RF coaxial connection to eliminate the need for an additional RF coaxial outlet.
- Choose a location that is relatively protected from accidental disturbance or harm, such as a closet, basement, or other protected area.
- Choose a location so that there is plenty of room to guide the cables away from the residential gateway without straining or crimping them.
- Choose a location that allows adequate ventilation around the residential gateway.
- Choose a location for the residential gateway that is adjacent to your telephone equipment if you plan on connecting your phone directly to the residential gateway.

Note: If you are using the residential gateway to provide service to several telephones, a professional installer can connect the residential gateway to your existing home telephone wiring.

How Do I Mount the Residential Gateway on a Wall? (Optional)

If you wish, you can mount the residential gateway to a wall. This section describes how to mount the residential gateway to a wall, and includes a list of equipment you will need along with suggestions for choosing an appropriate place to mount the residential gateway.

Select an Appropriate Place to Mount the Residential Gateway

You may mount the residential gateway to a wall that is made of cement, wood, or drywall. When choosing an appropriate mounting place, refer to the following recommendations:

- Ensure that the mounting location is free of obstructions on all sides, and the cables should be able to easily reach the residential gateway without strain.
- Leave sufficient clearance between the bottom of the residential gateway and any flooring or shelving underneath to allow access to cabling.
- Allow enough slack in all cables so that the residential gateway can be removed for any required maintenance without disconnecting the cables.
- Choose a location that allows adequate ventilation around the residential gateway.

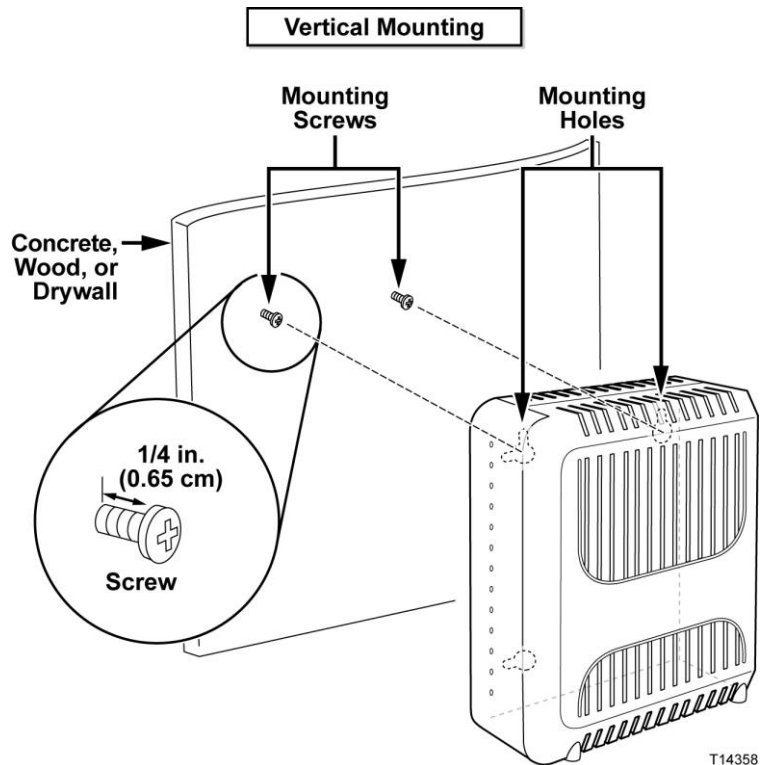
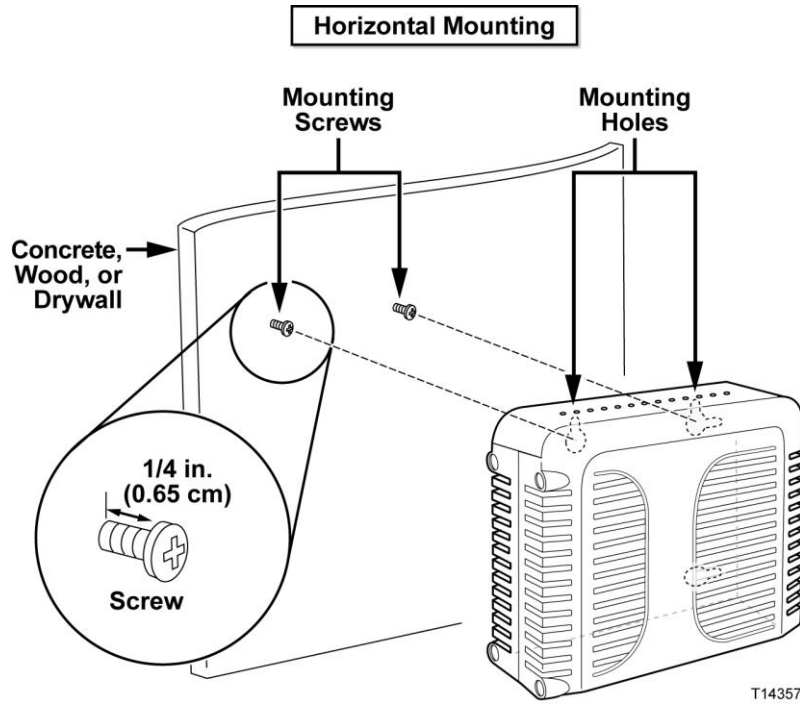
Equipment Needed

Verify that you have the following items that you will need to mount the residential gateway:

- Two wall anchors for #8 x 1-inch screws
- Two #8 x 1-inch pan head sheet metal screws
- Drill with a 3/16-in. wood or masonry bit, as appropriate for the wall composition
- A copy of the wall-mounting illustrations shown on the following pages

Position the Residential Gateway

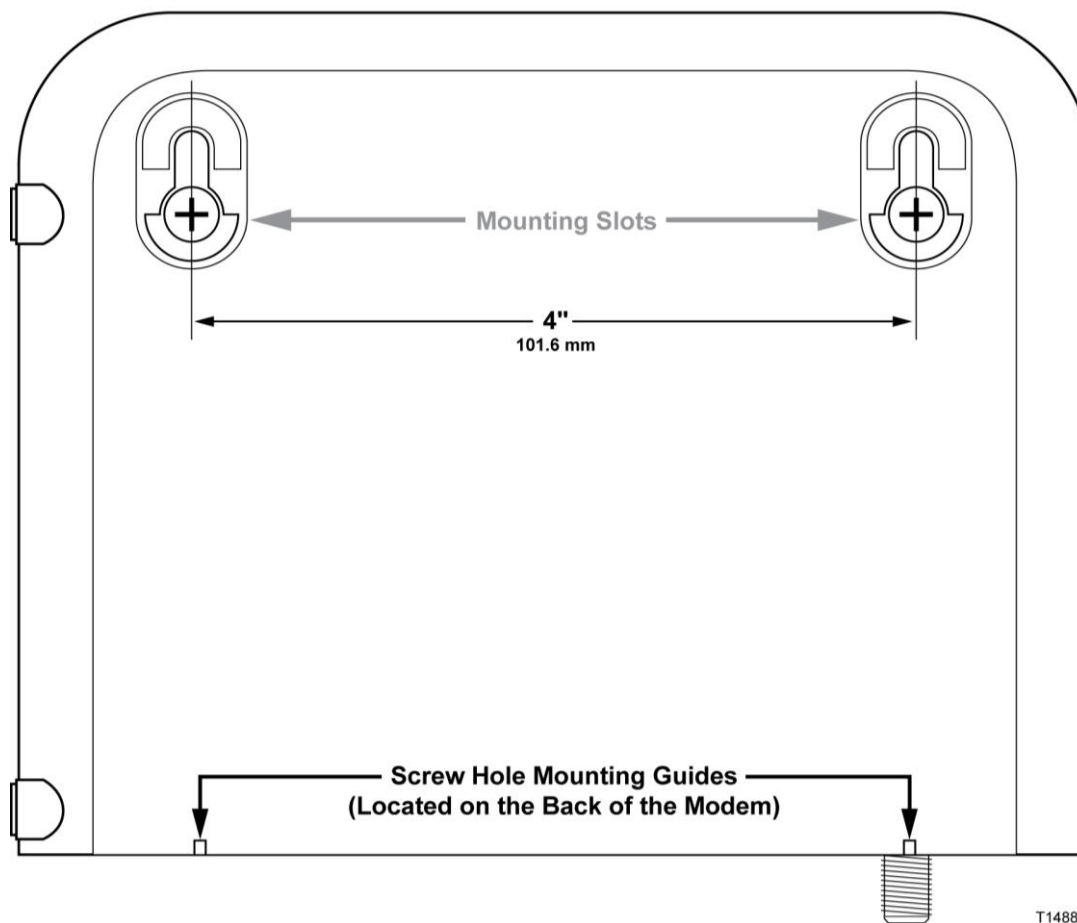
Use the following illustrations to guide you in positioning the residential gateway on the wall.



Location and Dimensions of the Wall-Mounting Slots

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

Note: Image not to scale.



Mounting the Residential Gateway on a Wall

- 1 Using a drill with a 3/16-inch bit, drill two holes at the same height and 4 inches apart.

Note: The preceding graphic illustrates the location of the mounting holes on the back of the residential gateway.

- 2 Are you mounting the residential gateway into a drywall or concrete surface where a wooden stud is available?

- If **yes**, go to step 3.
- If **no**, drive the anchor bolts into the wall, and install the mounting screws into the anchor bolts; leave a gap of about 1/4-inch between the screw head and the wall. Then, go to step 4.

- 3 Install the mounting screws into the wall; leave a gap of about 1/4-inch between the screw head and the wall. Then, go to step 4.

Installation Preparations

- 4 Verify that no cables or wires are connected to the residential gateway.
- 5 Lift the residential gateway into position. Slip the large end of both mounting slots (located in the back of the residential gateway) over the mounting screws, and then slide the residential gateway down until the narrow end of the keyhole slot contacts the screw shaft.

Important: Verify that the mounting screws securely support the residential gateway before you release the unit.

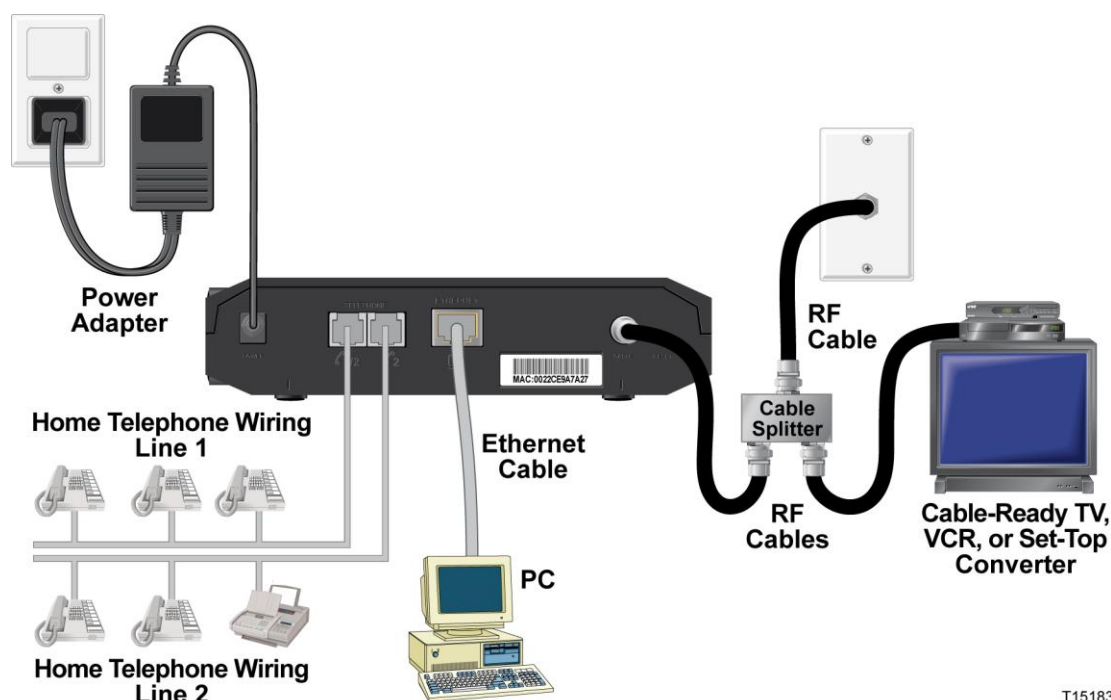
Install the Residential Gateway

This section describes how to connect your residential gateway to support the services that the residential gateway offers.

Connect Devices to the Residential Gateway

The following illustration shows all of the possible connections that can be made to your residential gateway for various services. Although your model may not support all of the services pictured, you can determine which services your model supports by referring to the Benefits and Features list in *Introduction* (on page 2).

Note: Professional installation may be available. Contact your local service provider for further assistance.



T15183

Connect the Residential Gateway

The following installation procedure ensures proper setup and configuration for the residential gateway.

- 1 Choose an appropriate and safe location to install the residential gateway (close to a power source, an active cable connection, your PC — if using high-speed Internet, and your telephone lines — if using VoIP). For assistance, go to *Where Is the Best Location for My Residential Gateway?* (on page 13).



WARNING:

- To prevent possible damage to equipment, disconnect any other telephone service before connecting your residential gateway to the same wires.
- Hazardous electrical voltages can exist on the telephone, Ethernet, or coax cable wiring. Be sure to disconnect AC power from all devices while installing your service.
- All wiring and connections must be properly insulated to prevent electrical shock.
- Telephone connections to an installed home telephone wiring network should be done by a qualified installer. The cable telephone service provider may offer professional installation and connection to the home telephone wiring network. A fee may be charged for this service.

- 2 Power off your PC and other networking device; then, unplug them from the power source.
- 3 Connect the active RF coaxial cable from your service provider to the coax connector labeled **CABLE** on the back of the residential gateway.

Note: To connect a TV, DHCT, set-top, or VCR from the same cable connection, you will need to install a cable signal splitter (not included). Always check with your service provider before using a splitter as a splitter may degrade the signal.

- 4 Connect your PC to the residential gateway using either of the following methods:
 - **Ethernet Connection.** Connect one end of the yellow Ethernet cable to the Ethernet port on your PC, and connect the other end to the yellow **ETHERNET** port on the back of the residential gateway.

Note: To install more than one Ethernet device on a residential gateway that has only one Ethernet port, use an external multi-port Ethernet switch(s) or cable router (not provided).
 - **Wireless Connection.** Make sure that your wireless device is powered up. You will need to associate your wireless device with the wireless gateway once the residential gateway is operational. Follow the directions provided with your wireless device for associating with a wireless access point. If the residential gateway has a WIRELESS ON/OFF button, make sure that WIRELESS is enabled by confirming that the ON/OFF indicator is ON. If the indicator is OFF, press the ON/OFF button to enable the WIRELESS feature.

More information about the factory default configuration of your wireless residential gateway can be found later in *Configure Wireless Settings* (on page 84).
- 5 If your residential gateway supports digital telephone service (VoIP), connect one end of a telephone jumper cable (not included) to a telephone outlet in your home or to a telephone or fax machine. Then connect the other end of the jumper cable to the appropriate RJ-11 **TELEPHONE** port on the back of the residential gateway. The telephone ports are light gray and are labeled 1/2 and 2 or 1 and 2 depending on the region of the world the residential gateway is used.

Notes:

- **Telephone 2** port is an optional feature and may not be supported on your model.
- Make sure to connect your telephone service to the correct RJ-11 port. For single line telephone service, connect to port 1/2 or 1.
- In North America, residential gateways have multi-line capability on the RJ-11 telephone port labeled 1/2. Line 1 is on pins 3 and 4 of port 1/2, and Line 2 is supported on pins 2 and 5. In Europe, residential gateways support only one line per port. Line 1 is on port 1 and line 2 is on port 2.
- Telephones that require electrical connectors other than RJ-11 may require an external adapter (sold separately).

- 6 Locate the AC power adapter provided with your residential gateway. Connect the barrel connector end of the power adapter into the power input on the back of the residential gateway. Then, plug the AC power adapter into an AC outlet to power-up the residential gateway.

Note: If your Residential Gateway is equipped with a power switch (located on the back panel), make sure that the switch is in the ON position to power-up the Residential Gateway.

The residential gateway will perform an automatic search to locate and sign on to the broadband data network. This process may take up to 2-5 minutes. The residential gateway will be ready for use when the **POWER**, **DS**, **US** and **ONLINE** LEDs on the front panel of the residential gateway stop blinking and remain on continuously.

- 7 Plug in and power on your PC and other home network devices. The **LINK** LED on the residential gateway should be on or blinking.
- 8 At this point, the installation is complete, and you can begin surfing the Internet.

Note: If your PC does not have Internet access, refer to *How Do I Configure TCP/IP Protocol?* (on page 108) for information on how to configure your PC for TCP/IP. For Internet devices other than PCs, refer to the DHCP or IP Address configuration section of the User Guide or Operations Manual for those devices.

3

Configuring the DOCSIS Residential Gateway

Introduction

This chapter provides instructions for using the WebWizard to configure the residential gateway to operate correctly.

The WebWizard gives you access to residential gateway settings that were configured at the factory for the most common installation configurations. After you access the WebWizard, you can customize these settings to meet your needs. The WebWizard pages in this chapter are organized in the order shown on the **Setup** page.

When using the instructions in this chapter, keep in mind that examples of the WebWizard pages shown here are for illustration purposes only and may differ from the WebWizard pages shown on your residential gateway. The pages shown in this guide also represent the default values for the residential gateway.

Important: If you are not familiar with the network configuration procedures detailed in this chapter, contact your service provider before attempting to change any of the residential gateway settings.

In This Chapter

- Log in to the DOCSIS Residential Gateway for the First Time 24
- Configure Basic Settings 27
- Configure Advanced Settings 47
- Configure Firewall Settings 68
- Configure Parental Control Settings 75
- Configure Wireless Settings 84

Log in to the DOCSIS Residential Gateway for the First Time

This section provides detailed instructions for logging in to the residential gateway so that you can use the WebWizard to customize the residential gateway to suit your needs, rather than using the default (factory) settings.

The residential gateway uses a default IP address of 192.168.0.1. If you have connected the residential gateway correctly and you have configured your computer properly, use the following procedure to log in to the residential gateway as an administrator.

Accessing the Residential Gateway

You must access the WebWizard in order to configure the residential gateway. To gain access to the WebWizard, use the web browser on the PC attached to the gateway and complete the following steps.

- 1 Open the web browser on your PC.
- 2 Type the following IP address and then select **Go**:
http://192.168.0.1.
- 3 The web browser accesses the WebWizard and displays the default **About Your Modem** page. This page displays information about your cable modem along with a series of tabs for accessing other WebWizard configuration and operation features.

About Your Modem Page Example

The following illustration is an example of the About Your Modem page.

Log in to the DOCSIS Residential Gateway for the First Time

The screenshot shows the 'About Your Modem' page of a Cisco DOCSIS Residential Gateway. The page has a navigation bar with tabs: System, Signal, Status, Log, Provisioning, Setup, and Advanced. The 'System' tab is selected. Below the navigation bar, there is a section titled 'About Your Modem' with a sub-header 'System'. The 'System' section contains a table with the following data:

Field Name	Description
Name	Cisco DPC2425
Modem Serial Number	221852983
Cable Modem MAC Address	00:22:3a:7a:c3:53
Hardware Version	1.0
Receive Power Level	-26.7 dBmV
Transmit Power Level	8.3 dBmV
Cable Modem Status	Not Synchronized
Vendor	Cisco
Boot Revision	2.1.7IR3

Below the system information table, there is a section titled 'Software File Name and Revisions' with a sub-header 'Software File Name and Revisions'. This section contains a table with the following data:

Field Name	Description
Firmware Name	dpc2425-P10-5-v202r12811-090223as.bin
Software Revision	dpc2425-P10-5-v202r12811-090223as

About Your Modem Page Description

The following table provides a description of each field within the About Your Modem page.

Field Name	Description
Name	The name of the residential gateway
Modem Serial Number	A unique sequential series of alphanumeric characters provided to every modem during manufacturing
Cable Modem MAC Address	A unique alphanumeric address for the cable modem coaxial interface, which is used to connect to the cable modem termination system (CMTS) at the headend. A media access control (MAC) address is a hardware address that uniquely identifies each node of a network
Hardware Version	The revision of the circuit board design
Receive Power Level	The input level of the downstream CMTS carrier
Transmit Power Level	The upstream power level

Field Name	Description
Cable Modem Status	<p>Lists one of the following possible current states of the modem:</p> <ul style="list-style-type: none"> ■ other ■ notReady ■ notSynchronized ■ phySynchronized ■ usParametersAcquired ■ rangingComplete ■ ipComplete ■ todEstablished ■ securityEstablished ■ psrsmTransferComplete ■ registrationComplete ■ operational ■ accessDenied
Vendor	The name of the manufacturer
Boot Revision	The boot revision code version

Software File Name and Revisions Section

Field Name	Description
Firmware Name	The name of the firmware
Software Revision	The revision version of the firmware

Configure Basic Settings

This section describes how to configure Basic settings for the residential gateway.

Setting Configuration Options

Use the Setup page to access the various configuration options for the residential gateway. Detailed descriptions of each configuration option follow later in this guide.

Important: After you access the WebWizard by typing the 192.168.0.1 IP address into your web browser while the gateway is online, an authentication window similar to the following window opens:



Enter your password; then, click **OK** to continue to the Setup page.

First Time Users

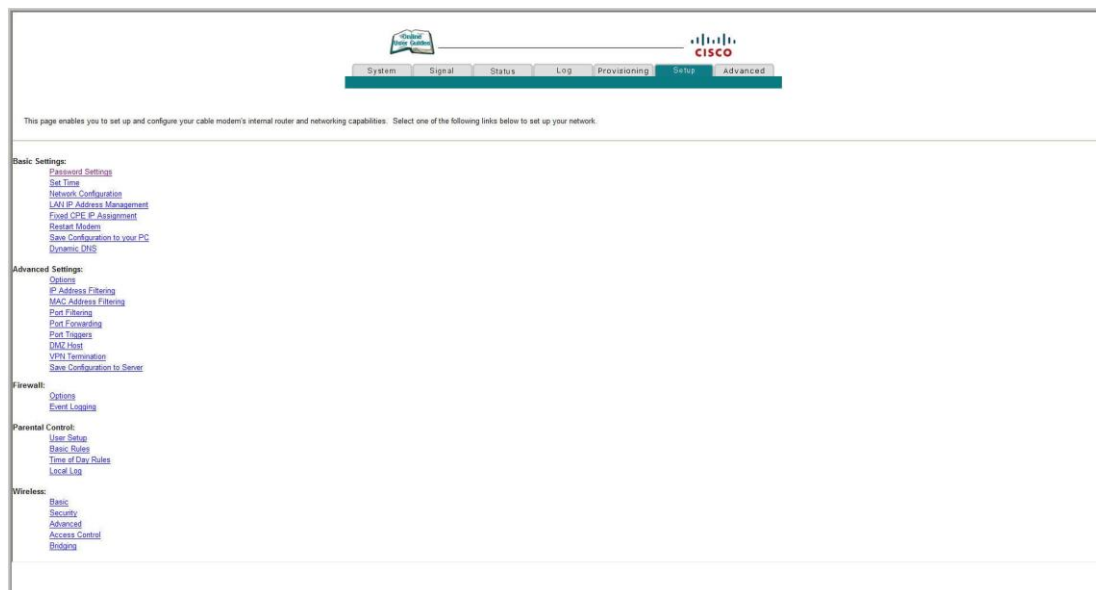
The gateway ships from the factory without a factory-assigned or default password.

Leave the user name and the password fields blank. Then click **OK** to be directed to the Password Settings page.

Note: You will be prompted to set up a password. We highly recommend that you set up a password to prevent unauthorized access to the settings of the gateway. If you choose not to enter a password, this page will appear each time you access the setup pages. See *Configuring Your Password Settings* (on page 32) for assistance in setting up your password. If you choose not to use password security, click the **Setup** tab at the top of the Password Settings page to continue.

Setup Page

The following illustration is an example of the Setup page.



Setup Page Section Headings

The Setup page is divided into the following section headings:

- Basic Settings
- Advanced Settings
- Firewall
- Parental Control
- Wireless

In the Setup page, click the selections listed within these sections to access the WebWizard page for that selection. A description of the selections available in each section follows next.

Basic Settings

The following table provides a description of the pages available from within the Basic Settings section of the Setup page.

Field Name	Description
Password Settings	Use this link to set or modify your password settings.
Set Time	Use this link to enable or disable time synchronization by Network Time protocol.
Network Configuration	Use this link to enter or modify the basic settings for your network.
LAN IP Address Management	Use this link to configure how Internet protocol (IP) addresses are assigned and managed in your network.
Fixed CPE IP Assignment	Use this link to reserve IP addresses in the DHCP pool that will be used as static IP addresses in your local network.
Restart Modem	Use this link to restart your residential gateway.
Save Configuration to your PC	Use this link to save your cable modem RG configuration to your local PC and to restore the RG configuration to your residential gateway, if necessary.

Advanced Settings

The following table provides a description of the pages available from within the Advanced Settings section of the Setup page.

Field Name	Description
Options	Use this link to enable or disable advanced features on your network.
IP Address Filtering	Use this link to configure IP address filters. These filters prevent designated IP addresses from accessing the Internet.
MAC Address Filtering	Use this link to configure MAC address filters. These filters prevent designated MAC addresses from accessing the Internet.
Port Filtering	Use this link to configure transmission control protocol (TCP) and user datagram protocol (UDP) port filters. These filters prevent a range of TCP/UDP ports from accessing the Internet.

Field Name	Description
Port Forwarding	Use this link to configure port forwarding for local IP addresses. Port forwarding allows you to run a server on the local area network (LAN) by specifying the mapping of TCP/UDP ports to local PCs or to the IP address of other devices. This is a static setting that holds the ports open at all times.
Port Triggers	Use this link to configure TCP/UDP port triggers. Port triggering is similar to port forwarding, but is a dynamic function. In other words, the ports are not held open, and the ports close if no outgoing data is detected on the selected ports for a period of 10 minutes.
DMZ Host (Demilitarized Zone)	<p>Use this link to configure an IP address that is visible to the wide area network (WAN). DMZ hosting is commonly referred to as “exposed host,” and allows you to specify the “default” recipient of WAN traffic that Network Address Translation (NAT) is unable to translate to a known local PC.</p> <p>A DMZ is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network. DMZ allows one IP address to be unprotected while others remain protected. The DMZ is located between the Internet and an internal network's line of defense that is a combination of firewalls and bastion hosts.</p> <p>Typically, the DMZ contains devices accessible to Internet traffic, such as web (HTTP) servers, FTP servers, SMTP (e-mail) servers, and domain name system (DNS) servers.</p>
VPN Termination	Use this link to create, configure, and control Virtual Private Network (VPN) protocols and manage Internet Protocol Security (IPsec) VPN tunnels.

Firewall

The following table provides a description of the pages available from within the Firewall section of the Setup page.

Field Name	Description
Options	Use this link to configure web page filtering and firewall protection.
Event Logging	Use this link to access the firewall event log and to enter your e-mail address in order to receive e-mail alerts related to firewall attacks by hackers.

Parental Control

The following table provides a description of the pages available from within the Parental Control section of the Setup page.

Field Name	Description
User Setup	Use this link to add or delete user profiles and to apply access rules to those users.
Basic Rules	Use this link to setup access rules that block certain Internet content and certain websites.
Time of Day Rules	Use this link to configure web access filters to block all Internet traffic to and from specific network devices based on time of day settings that you select.
Local Log	Use this link to view events captured by Parental Control event log feature.

Wireless

The following table provides a description of the pages available from within the Wireless section of the Setup page.

Field Name	Description
Basic	Use this link to configure your wireless access point (WAP) parameters, including service set identifier (SSID) and channel number.
Security	Use this link to configure your WAP authentication and data encryption. Using encryption and authentication prevents unauthorized access to your wireless devices.
Advanced	Use this link to configure your WAP data rates and wireless fidelity (Wi-Fi) thresholds.
Access Control	Use this link to configure the WAP to restrict access to only selected wireless client devices. Authorized clients are selected by MAC address. Use this link to select Open System or Share Key authentication and to enable and disable broadcast of the WAP SSID.
Bridging	Use this link to configure a Wireless Distribution System (WDS) in our network.

Configuring Your Password Settings

Use the Basic Settings - Password Settings page to set up or modify a password to restrict unauthorized persons from accessing to your residential gateway settings. Click **Password Settings** in the Basic Settings section of the Setup page to access the Password Settings page.

Notes:

- Your gateway modem comes from the factory with no password enabled. We highly recommend that you set up a user password to prevent unauthorized users from modifying the settings of your network.
- If you do choose to set up a password, use a password that you can easily remember. Do *not* forget your password.

Setup Basic Settings - Password Settings

The following illustration is an example of the Basic Settings - Password Settings page.

System Signal Status Log Provisioning **Setup** Advanced

Setup
Basic Settings - Password Settings
 This page allows you to modify the password settings for this device.

Important: As a matter of good operating practice, it is highly recommended to use this page to establish a personalized user Password. Setting a user password can help prevent unauthorized access to the Setup pages for this residential gateway. Unauthorized access may result in disrupted home network operation or a breach in your home network security, exposing the equipment in you home network to denial of service attacks and hacking from a variety of potentially malicious sources.

Password

Re-Enter Password

Apply

To set up your password

- 1 To set up your password, type your password in the Password field, and then re-type your password in the Re-Enter Password field.
- 2 Click **Apply** to save your password. A web page appears to indicate that you have successfully set your password.
- 3 Click on the **Setup** tab to proceed with setting up your gateway. The User Name and Password dialogue box appears as shown below.
- 4 Enter your password; then, click **LOGIN** to continue to the main Setup page.

Note: If you set a password, on subsequent access to the Setup pages, a screen similar to the following appears. Do *not* forget your password. Write your password and store it in a secure location known only to you.



Configuring Network Time Synchronization

Use the Basic Settings Enable/Disable time synchronization by Network Time protocol page to enable or disable time synchronization by Network Time protocol.

Note: If you are not familiar with the time configuration procedures detailed in this section, contact your service provider before you attempt to change any of the residential gateway default time synchronization configuration settings.

Click **Set Time** in the Basic Settings section of the Setup page to access the Basic Settings Enable/Disable time synchronization by Network Time protocol page.

Setup Basic Settings - Enable/Disable Time Synchronization by Network Time Protocol

The following illustration is the initial view of the Basic Settings Enable/Disable time synchronization by Network Time protocol page.

Setup Basic Settings - Enable/Disable Time Synchronization by Network Time Protocol Page Description

The following table provides a description of the fields within the Basic Settings Enable/Disable time synchronization by Network Time protocol page.

Field Name	Description
Current System Time	Displays the current system time and date.
Network Time Protocol	Allows you to enable or disable network time protocol. Note: The residential gateway will automatically use the time server in your broadband network. Should there be no current time displayed or if the network time is incorrect, enable Network Time Protocol to use a public Internet time server to set the clock in the gateway.

Field Name	Description
Latest Update Success	Displays the time and date of the last successful time update.
Time Zone	Displays the current time zone. The drop-down list allows you to select your local time zone.
Daylight Saving Time	Allows you to adjust the time during periods when Daylight Saving Time is in effect. Check the Enable box to enable or disable this setting. Note: If the offset for Daylight Savings Time is other than 60 minutes, enter the offset in the minutes field.
Time Server	Add and delete time server URLs or IP addresses to and from the list, as required. When using Network Time Protocol, multiple time servers can be specified for the gateway to query for time of day. The gateway will sequentially step through the listed time servers until it acquires the current time. There are three well known public time servers entered as default servers.

Function Keys

Key	Description
Apply	Saves all additions, edits, and changes.
Add Server	Allows you to add a network time server.
Remove Server	Allows you to remove a network time server.

Under normal conditions, you should use the default network settings. In the event that the network time does not match your local time, or, if your system requires different settings to operate correctly, you can change the default network settings using the Setup Basic Settings - Network Configuration page.

Configuring the Network Settings

Note: If you are not familiar with the network configuration procedures detailed in the following sections, contact your service provider before you attempt to change any of the residential gateway default network configuration settings.

Click **Network Configuration** in the Basic Settings section of the Setup page to access the Setup Basic Settings - Network Configuration page.

Setup Basic Settings - Network Configuration

The following illustration is an example of the Setup Basic Settings - Network Configuration page.

Setup
Basic Settings - Network Configuration
 This page allows you to enter or modify the basic settings for your network.

LAN

IP Address: 192.168.32.1 / 24
 IP Network: 192.168.32.0
 Decimal NetMask: 255.255.255.0
 Broadcast: 192.168.32.255
 MAC Address: 00:22:3a:46:6f:c5

WAN

IP Address: ---:---:---:---:---:---
 Subnet Mask: ---:---:---:---:---:---
 Gateway IP: ---:---:---:---:---:---
 Duration: D: -- H: -- M: -- S: --
 Expires: ---:---:---:---:---:---
 Renew WAN IP Address Lease Apply

Host Name: (Required by some ISPs)
 Domain Name: (Required by some ISPs)
 Static IP Address: 0 0 0 0
 Static IP Mask: 0 0 0 0
 Default Gateway: 0 0 0 0
 Primary DNS (static IP only): 0 0 0 0
 Secondary DNS (static IP only): 0 0 0 0
 MTU Size: 0 (256-1500 octets, 0 = use default)
 Apply

Setup Basic Settings - Network Configuration Page Description

The following table provides a description of the fields within the Setup Basic Settings - Network Configuration page.

Field Name	Description
LAN IP Address	Displays the base IP address of the private home LAN and the WebWizard IP address. Your residential gateway assigns private IP addresses to your attached computers by its internal dynamic host configuration protocol (DHCP) server.
IP Network	Displays the address of the private LAN IP network.
Decimal Netmask	Displays the netmask of the private LAN IP network.
Broadcast	Displays the broadcast IP address.

Field Name	Description
MAC Address	Displays the MAC address for the WAN. The factory assigned MAC address for the WAN is also referred to as the WAN MGT MAC.
WAN IP Address	Displays the public IP address assigned to your gateway by your ISP. The WAN port will be assigned a public IP address automatically by your ISP except when a static IP address is set up as described below. The WAN IP address will be shared by all the PCs in your private local area network to access the Internet.
Subnet Mask	Displays the subnet mask for your WAN port. This address is automatically assigned to your WAN port by your ISP except when a static IP address is set up as described later in this table.
Gateway IP	Displays a Gateway IP address for your WAN port. This address is automatically assigned to your WAN port by your ISP except when a static IP address is set up as described later in this table.
Duration	Displays the length of time your WAN IP address is valid.
Expires	Displays the date and time your WAN IP address expires.
Host Name	Displays the host name that is usually downloaded to your gateway by your ISP. However, some ISPs require this information to be entered manually. If manual entry is required, your ISP will provide the information for you to enter into this field.
Domain Name	Displays the domain name that is usually downloaded to your gateway by your ISP. However, some ISPs require this information to be entered manually. If manual entry is required, your ISP will provide the information for you to enter into this field.
Static IP Address	Manual entry is required. Your ISP will provide the information for you to enter into this field. Note: When setting a static IP address, you must enter the IP address, subnet mask, and default gateway before the static IP address will become operational.
Static IP Mask	Manual entry is required. Your ISP will provide the information for you to enter into this field.
Default Gateway	Manual entry is required. Your ISP will provide the information for you to enter into this field.
Primary DNS (static IP only)	Manual entry is required. Your ISP will provide the information for you to enter into this field.

Field Name	Description
Secondary DNS (static IP only)	Manual entry is required. Your ISP will provide the information for you to enter into this field.
MTU Size	Sets the size of the maximum transmission unit (MTU) for the network interface. The default value is 0 (zero). Important: Do not change this value unless you are an experienced user.

Function Keys

The following function keys appear on the Setup Basic Settings - Network Configuration page.

Key	Description
Renew WAN IP Address Lease	Forces a release and renewal of your WAN IP address.
Apply	Saves the values you enter into the fields without closing the screen.

Configuring and Managing IP Addresses

Use the Setup Basic Settings - IP Management page to configure how your system manages and assigns IP addresses in your network.

Note: If you are not familiar with the IP management procedures detailed in this section, contact your service provider before you attempt to change any of the residential gateway default IP management settings.

Click **LAN IP Address Management** in the Basic Settings section of the Setup page to access the Setup Basic Settings - IP Management page.

Setup Basic Settings - IP Management Page Example

The following illustration is an example of the Setup Basic Settings - IP Management page.

System Signal Status Log Provisioning **Setup** Advanced

Setup
Basic Settings - IP Management
This page allows you to configure how IP addresses are assigned and managed in your network.

DHCP Server ☒ Yes ☐ No
Starting Local Address
Number of CPEs
Lease Time

DHCP Client Lease Info				
MAC Address	IP Address	Subnet Mask	Duration	Expires
00155880a196	192.168.032.010	255.255.255.000	D:00 H:01 M:00 S:00	-----

Current System Time: -----

WINS Addresses

Primary: 0.0.0.0
Secondary: 0.0.0.0
Tertiary: 0.0.0.0

Setup Basic Settings - IP Management Page Description

The following tables provide a description of the fields within the Setup Basic Settings - IP Management page.

Field Name	Description
DHCP Server	Allows you to enable or disable the DHCP server in the residential gateway.
Starting Local Address	<p>Displays the starting address used by the built-in DHCP server to distribute Private LAN IP addresses. In the example shown, addresses between 2 and 9 can be used for devices on your Private LAN that require fixed IP addresses such as printers or a device assigned as a DMZ host.</p> <p>Note: The LAN IP address ending in 1 is reserved for the internal gateway server. The LAN IP address ending in 255 is also reserved and should not be used for CPE devices.</p>
Number of CPEs	<p>Enter the maximum number of devices allowed to connect to the Private LAN.</p> <p>Notes:</p> <ul style="list-style-type: none"> ■ The Factory Default is 245. The maximum number of devices is 253. This is the combined total of addresses reserved for static IP addresses, for example, the sum of the IP addresses between 2 and the value entered in the Starting Local Address field and the value entered in the Number of CPEs field. ■ The sum of the value entered in the Starting Local Address field and the value entered in the Number of CPEs field must always be 255 or less.
DHCP Client Lease Info	Displays the MAC address, IP Address, Subnet Mask, Duration and Expiration date of all devices issued an IP address by the built-in DHCP server. This field also displays the current system time and date.
WINS Addresses	Allows you to manually enter Windows Internet Name Server (WINS) server addresses.

Function Keys

The following function keys appear on the Basic Settings - IP Management page.

Key	Description
Apply	Saves the values you enter into the fields without closing the screen.
Force Available	Forces the release of an IP address for you to re-use.
Add Primary	Saves the WINS address for one server.

Key	Description
Add Secondary	Saves the WINS address for a second server.
Add Tertiary	Saves the WINS address for a third server.
Remove WINS Address	Removes the WINS address selected.
Clear All	Removes all defined WINS addresses.

Reserving IP Addresses

Use the Setup Basic Settings - Fixed CPE IP Assignment page to reserve IP addresses. This feature allows you to assign a fixed IP address to any device in your network by setting static IP addresses in your PC or other network device.

These addresses will be removed from the pool of the IP addresses to be used by your gateway's DHCP server when issuing IP addresses to devices that are connected to your local network.

Reserving IP addresses is useful in making sure that there are no IP address conflicts on the network, for example, two devices using the same IP address. Another example: when using DMZ Host, the IP address for the DMZ Host should always have the same IP address.

Note: If you are not familiar with the Fixed CPE IP Assignment procedures detailed in this section, contact your service provider before you attempt to change any of the residential gateway default Fixed CPE IP Assignment settings.

Click **Fixed CPE IP Assignment** in the Basic Settings section of the Setup page to access the Setup Basic Settings - Fixed CPE IP Assignment page.

Setup Basic Settings - Fixed CPE IP Assignment Page

The following illustration is an example of the Setup Basic Settings - Fixed CPE IP Assignment page.

Setup Basic Settings - Fixed CPE IP Assignment Page Description

The following tables provide a description of the fields within the Setup Basic Settings - Fixed CPE IP Assignment page.

Field Name	Description
MAC Address	The MAC address of the PC or device (for example, a printer) for which you want to reserve a specific IP address on the network.
Assign to IP	The IP address you assign to the PC or device for which you want to reserve a specific IP address on the network. Only MAC addresses within the range of the gateway's DHCP address pool can be reserved with this feature. Note: The factory configuration of your gateway sets aside IP addresses 192.168.0.2 through 192.168.0.9 for static IP addresses.

Function Keys

Key	Description
Add Static IP	Adds the Static IP address to the list of assigned IP addresses.
Remove Static IP	Removes the Static IP address from the list of assigned IP addresses.

Restarting the Gateway Modem

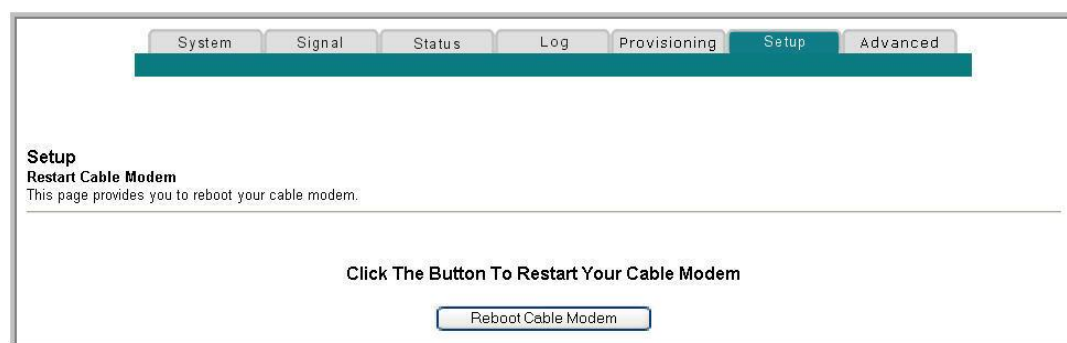
Use the Setup Basic Settings - Restart Cable Modem page to restart your cable modem.

- 1 Click **Restart Modem** in the Basic Settings section of the Setup page to access the Basic Settings - Restart Cable Modem page.
- 2 Click **Reboot Cable Modem** to restart the gateway modem.

Note: Restarting your gateway modem does not reset any of the settings.

Setup Basic Settings - Restart Cable Modem Page

The following illustration is an example of the Restart Cable Modem page.



Saving Your Configuration to a PC

Use the Setup Basic Settings - Save RG Configuration to Local PC page to save your current cable modem RG configuration to the hard drive on your PC or to a floppy disk. You will then be able to restore the RG configuration, if necessary.

Note: If you are not familiar with the procedures detailed in this section, contact your service provider before you attempt to change any of the residential gateway default settings.

Click **Save Configuration to your PC** in the Basic Settings section of the Setup page to access the Setup Basic Settings - Save RG Configuration to Local PC page.

Setup Basic Settings - Save RG Configuration to Local PC Page

The following illustration is an example of the Setup Basic Settings - Save RG Configuration to Local PC page.

System Signal Status Log Provisioning Setup Advanced

Save RG Configuration to Local PC

This page provides you with the ability of saving current RG configuration in this device to your Local PC and restoring RG configuration to your device

Download user setting file to your gateway

File Name Browse...

Download

Save current user setting to your computer

FDD

To **Save** your current setting to your computer, click the floppy disk icon in the lower portion of the screen. You will be prompted to provide a file name and location for the backup configuration file.

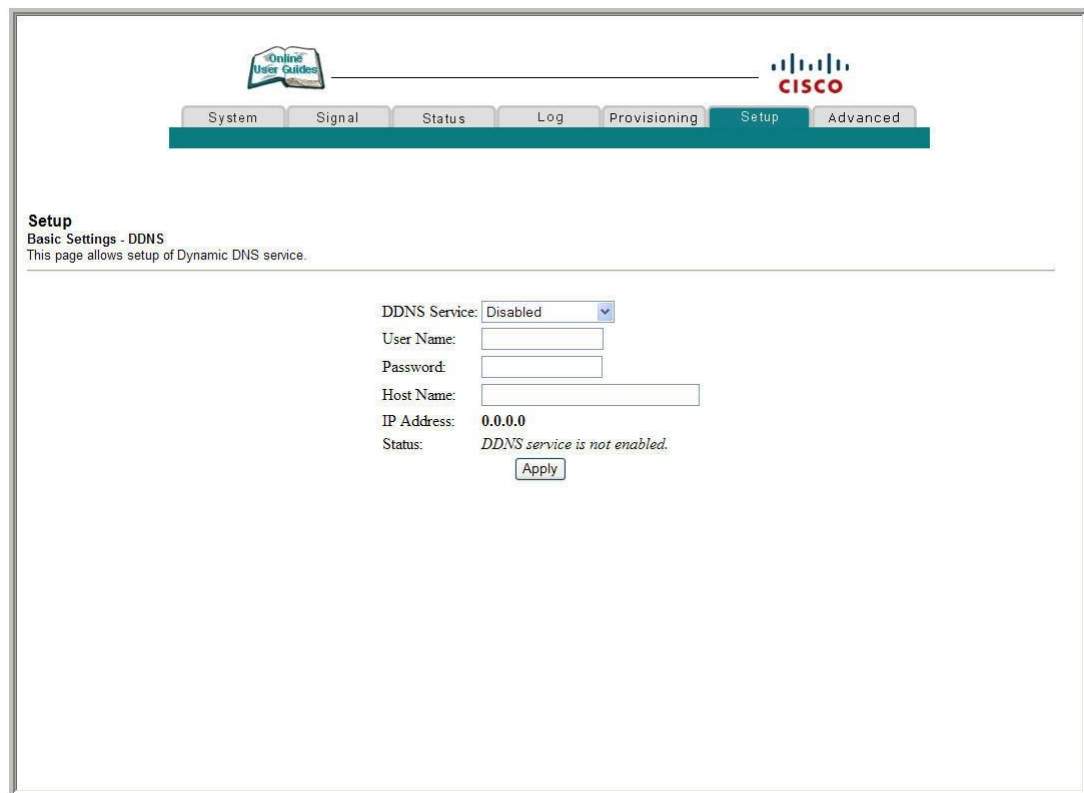
To **Restore** your setting, click **Browse** and select the backup configuration file name that you saved on your PC. The path and filename of the backup configuration appears in the File Name field. Then, click **Download** to restore your configuration file. A **Download Success** message appears when the restore is complete.

Configure Dynamic DNS

Use the Setup Advanced Settings - Dynamic DNS page to configure the Dynamic Domain Name Service (DDNS). This service provides the residential gateway that has a variable and frequently changing IP address with a well known host name resolvable by network applications through standard DNS queries. If you have a fixed IP address, you don't need to use DDNS. It is useful when you are hosting your own website, FTP server, or other server behind the device. Before using this feature, you need to sign up for DDNS service at a supported DDNS service provider.

Setup Basic Settings - Dynamic DNS Page

The following illustration is an example of the Setup Basic Settings - Dynamic DNS page.



The screenshot shows the Cisco DDNS configuration page. At the top, there is a navigation bar with tabs: System, Signal, Status, Log, Provisioning, Setup (selected), and Advanced. Below the navigation bar, the page title is "Setup Basic Settings - DDNS" with a subtitle "This page allows setup of Dynamic DNS service." The main configuration area contains the following fields:

- DDNS Service: Disabled (dropdown menu)
- User Name:
- Password:
- Host Name:
- IP Address: 0.0.0.0
- Status: DDNS service is not enabled.

An "Apply" button is located at the bottom of the configuration area.

Setup Basic Settings - Dynamic DNS Page Description

The following tables provide a description of the fields within the Setup Basic Settings - Dynamic DNS page.

Field Name	Description
DDNS Service	Provides option to disable or activate the DDNS feature. <ul style="list-style-type: none">■ Disable - Select this option to disable this feature.■ www.DynDNS.org - Select this option to set up service with a DDNS service provider. You will need to record the user name, password, and host name you create when you set up the DDNS service.
User Name	Manually enter the user name you created when you signed up for DDNS service.
Password	Manually enter the password you created when you signed up for DDNS service.
Host Name	Manually enter the host name you created when you signed up for DDNS service.
IP Address	The fixed IP address of your Residential Gateway. The device will advise the DDNS service of your current WAN (Internet) IP address whenever the address changes.
Status	Displays the status of the DDNS service connection.

Function Key

Key	Description
Apply	Saves the values you enter into the fields without closing the screen.

Configure Advanced Settings

This section describes how to configure Advanced settings for the residential gateway.

Enabling and Disabling Advanced Features

Use the Setup Advanced Settings - Options page to enable or disable advanced features on your network. When the wireless interface is disabled, the transmitter is turned off.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default advanced options settings.

Click **Options** in the Advanced Settings section of the Setup page to access the Setup Advanced Settings - Options page.

Setup Advanced Settings - Options Page

The following illustration is an example of the Setup Advanced Settings - Options page.

Feature	Enabled
WAN Blocking	<input checked="" type="checkbox"/> Enable
Isec PassThrough	<input checked="" type="checkbox"/> Enable
PPTP PassThrough	<input checked="" type="checkbox"/> Enable
Remote Config Management	<input type="checkbox"/> Enable
Multicast Enable	<input checked="" type="checkbox"/> Enable
UPnP Enable	<input type="checkbox"/> Enable

Apply

Setup Advanced Settings - Options Page Description

The following table provides a description of the fields within the Setup Advanced Settings - Options page.

Note: If you make changes in the Setup Advanced Settings - Options page, click **Apply** to apply and save your new IP address filter settings.

Field Name	Description
WAN Blocking	Checking this box prevents the residential gateway from being visible to the WAN. For example, pings to the WAN IP address are not returned.
IPsec PassThrough	Checking this box allows applications that use IPsec (IP Security) to pass through the firewall.
PPTP PassThrough	Checking this box allows applications that use Point to Point Tunneling Protocol (PPTP) to pass through the firewall.
Remote Config Management	<p>Checking this box enables Remote Configuration Management that allows the user or network operator to view and/or modify the gateway set-up parameters from a location on the WAN, as opposed to the LAN side of the gateway. Access to the set-up parameters is obtained by using the password to access the WebWizard.</p> <p>Enable this feature by checking the Remote Config Management box on the Setup Advanced Settings - Options page. To access your gateway from a remote location, you must also know the WAN IP address of the gateway. To find the WAN IP address, go to the Network Configuration page under Basic Settings. You will find the gateway's WAN IP address list on this page.</p> <p>Enter the WAN IP address of your gateway into the address field of any web browser using the following format: http://xxx.xxx.xxx.xxx:8080 where xxx.xxx.xxx.xxx represents the WAN IP address of your gateway.</p> <p>Be sure to follow the syntax exactly, and then click Go or press Enter. Your gateway web pages will appear on the remote computer. You will still need to enter your password to access the Setup pages of your gateway.</p> <p>Note: If you choose to enable (check) this feature, be sure to set up a user password to prevent unauthorized access to your gateway settings.</p>
Multicast Enable	Checking this box allows multicasts to pass from the WAN side through to the private network.
UPnP Enable	Checking this box enables Universal Plug and Play features.

Configuring IP Address Filters

Use the Setup Advanced Settings - IP Filtering page to configure IP address filters. These filters block a range of IP addresses from accessing the Internet.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default advanced IP filtering settings.

Click **IP Address Filtering** in the Advanced Settings section of the Setup page to access the Setup Advanced Settings - IP Filtering page.

Setup Advanced Settings - IP Filtering Page

The following illustration is an example of the Setup Advanced Settings - IP Filtering page.

IP Filtering		
Start Address	End Address	Enable
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>

Apply

Setup Advanced Settings - IP Filtering Page Description

Use this link to specify and enable a range of IP addresses that cannot have access to the Internet. Click **Apply** to apply and save your new IP address filter settings.

Configuring MAC Address Filters

Use the Setup Advanced Settings - MAC Filtering page to configure MAC address filters. These filters allow you to deny or block access to the Internet by the individual MAC addresses listed in the table. You can also prevent individual PCs from sending outgoing TCP/UDP traffic to the WAN using their MAC address.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default advanced MAC filtering settings.

Click **MAC Address Filtering** in the Advanced Settings section of the Setup page to access the Setup Advanced Settings - MAC Filtering page.

Setup Advanced Settings - MAC Filtering Page

The following illustration is an example of the Setup Advanced Settings - MAC Filtering page.

System Signal Status Log Provisioning **Setup** Advanced

Setup
Advanced Settings - MAC Filtering
This page allows you to configure MAC address filters.

Block Listed

MAC Addresses (example: 01:23:45:67:89:AB)

Addresses entered: 0/20

Setup Advanced Settings - MAC Filtering Page Description

Use this link to enter the MAC address or MAC addresses of devices whose Internet access you want to control. Click **Apply** to apply and save your new MAC address filter settings.

Setting Up MAC Address Filters

The Block/Pass drop down menu allows you to block or pass Internet access to the MAC addresses of the devices you list in the MAC Address Filters table. The following table describes the function of the Block/Pass drop down menu.

Field Name	Description
Block Listed (Default)	Select Block to deny Internet access to the MAC addresses of the devices you list in the table. All other MAC addresses will be allowed Internet access.
Pass	Select Pass to allow Internet access only to the MAC addresses of the devices you list in the table. Any MAC addresses <i>not</i> listed in the table will be denied Internet access.

Function Keys

The following function keys appear on the Advanced Settings - MAC Filtering page.

Key	Description
Apply	Saves the values you enter into the fields without closing the screen.
Add MAC Address	Saves the MAC Address entered in the associated text field.
Remove MAC Address	Removes the selected MAC address.
Clear All	Removes all defined MAC addresses.

Configuring and Enabling TCP and UDP Port Filters

Use the Setup Advanced Settings - Port Filtering page to configure and enable TCP and UDP port filters. These filters prevent a range of TCP/UDP ports from accessing the Internet. You can also prevent PCs from sending outgoing TCP/UDP traffic to the WAN on specific IP port numbers. This filter is not IP address- or MAC address-specific. The system blocks the specified port ranges for all PCs.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default advanced port filtering settings.

Click **Port Filtering** in the Advanced Settings section of the Setup page to access the Setup Advanced Settings - Port Filtering page.

Setup Advanced Settings - Port Filtering Page

The following illustration is an example of the Setup Advanced Settings - Port Filtering page.

Start Port	End Port	Protocol	Enable
0	0	Both	<input type="checkbox"/>
0	0	Both	<input type="checkbox"/>
0	0	Both	<input type="checkbox"/>
0	0	Both	<input type="checkbox"/>
0	0	Both	<input type="checkbox"/>
0	0	Both	<input type="checkbox"/>
0	0	Both	<input type="checkbox"/>
0	0	Both	<input type="checkbox"/>
0	0	Both	<input type="checkbox"/>
0	0	Both	<input type="checkbox"/>

Apply

Setup Advanced Settings - Port Filtering Page Description

Use this link to enter and enable the desired port filtering ranges and protocols in the appropriate fields and then click **Apply** to apply and save your new port filtering settings.

Configuring Port Forwarding for Local IP Addresses

Use the Setup Advanced Settings - Port Forwarding page to configure port forwarding for local IP addresses. Port forwarding allows you to run a server on the LAN by specifying the mapping of TCP/UDP ports to a local PC. You must also set up a fixed private LAN IP address for the destination device.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default advanced port forwarding settings.

Click **Port Forwarding** in the Advanced Settings section of the Setup page to access the Setup Advanced Settings - Port Forwarding page.

Setup Advanced Settings - Port Forwarding Page

The following illustration is an example of the Setup Advanced Settings - Port Forwarding page.

Local IP Addr	Start Port	End Port	Protocol	Enable
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>
0.0.0.0	0	0	TCP	<input type="checkbox"/>

Apply

Setup Advanced Settings - Port Forwarding Page Description

The following example illustrates how to use the port forwarding feature to configure the Microsoft X-Box Online Live for Internet gaming.

Note: For most widely used applications (including Microsoft X-Box Online Live), the built-in firewall automatically maps and opens ports required for that application while the application is in use.

- 1 Set the device to be used for port forward to a fixed IP address, for example, **192.168.0.5**.
- 2 In the first entry of the Port Forwarding area of the page, enter the same IP address (192.168.0.5) in the Local IP Address field.
- 3 In the same row, enter the appropriate port numbers in the Start Port and End Port fields.
- 4 In the same row, select the appropriate protocol from the drop-down list in the Protocol field, and then select the box in the **Enable** field.
- 5 To add additional ports, repeat steps 1 through 4, and then go to step 6.
- 6 Click **Apply** to apply and save your new port forwarding settings.

Configuring TCP/UDP Port Triggers

Use the Setup Advanced Settings - Port Triggers page to configure TCP/UDP port triggers. Port triggering is similar to port forwarding but is dynamic. In other words, the system does not hold the ports open indefinitely. For example, when the residential gateway detects outgoing data on a specific IP port number set in the “Trigger Range,” the resulting ports set in the “Target Range” will open for incoming data. If the system detects no outgoing traffic on the “Trigger Range” ports for a period of 10 minutes, the “Target Range” ports close. This is a safer method for opening specific ports for special applications, such as, video conferencing programs, interactive gaming, and file transfer in chat programs. This is safe because the ports are dynamically triggered and not held open continuously or left open erroneously by the router administrator. Therefore, these ports are not exposed and vulnerable for potential hackers to discover.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default advanced port triggers settings.

Click **Port Triggers** in the Advanced Settings section of the Setup page to access the Setup Advanced Settings - Port Triggers page.

Setup Advanced Settings - Port Triggers Page

The following illustration is an example of the Setup Advanced Settings - Port Triggers page.

Setup
Advanced Settings - Port Triggers
 This page allows you to configure TCP/UDP port triggers.

Port Triggering					
Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>

Apply

Setup Advanced Settings - Port Triggers Page Description

Use this link to enter and enable the port forwarding trigger and target range start and end ports along with protocol information in the appropriate fields. The following example illustrates how to use the port triggering feature to configure the Microsoft X-Box Online Live for Internet gaming.

Note: For most widely used applications (including Microsoft X-Box Online Live), the built-in firewall automatically maps and opens ports required for that application while the application is in use.

- 1 In the first row, enter **88** in both Start Port and End Port fields.
- 2 In the same row, select **UDP** from the drop-down list in the Protocol field, and then select the box in the **Enable** field.
- 3 In the second row, enter **3074** in both Start Port and End Port fields.
- 4 In the same row as the second entry, select **Both**, and then select the box in the Enable field.
- 5 Click **Apply** to apply and save your new port forwarding settings.

Configuring the DMZ Host

Use the Setup Advanced Settings - DMZ Host page to configure an IP address that is visible to the WAN. DMZ hosting is commonly referred to as “exposed host,” and allows you to specify the “default” recipient of WAN traffic that Network Address Translation (NAT) is unable to translate to a known local PC. DMZ allows one IP address to be unprotected while others remain protected.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default advanced DMZ host settings.

Click **DMZ Host** in the Advanced Settings section of the Setup page to access the Setup Advanced Settings - DMZ Host page.

Setup Advanced Settings - DMZ Host Page

The following illustration is an example of the Setup Advanced Settings - DMZ Host page.

System Signal Status Log Provisioning Setup Advanced

Setup
Advanced Settings - DMZ Host
The LAN IP address listed as the DMZ Host will have traffic forwarded to it from the public Internet. The DMZ Host is exposed to the public Internet and not protected by filtering.

DMZ Address 0.0.0.0

Apply

Setup Advanced Settings - DMZ Host Page Description

Use this link to place a Private LAN IP device, for example, an FTP, Mail, or web server directly on the Internet (bypassing the firewall). You set the server with a fixed IP address as a DMZ Host by entering its IP address in the DMZ Address field. Make sure the IP address used is not in the range of addresses delivered by the built-in DHCP server. After setting up a DMZ Host, all ports on this device are open to the Internet. You may configure only one PC to be the DMZ host. DMZ is generally used for PCs running “problem” applications that use random port numbers and do not function correctly with the specific port triggers or port forwarding setups described earlier in this guide. After entering a DMZ Address, click **Apply** to apply and save your new DMZ Host setting.

Configuring VPN Termination

Use the Setup Advanced Settings - VPN Termination page to configure VPN protocols and manage VPN tunnels. A VPN is a connection between two endpoints in different networks that allows private data to be sent securely and transparently over public networks or other private networks. With a VPN, you can send data securely between these two locations or networks. This is accomplished by creating a "VPN tunnel." A VPN tunnel connects the two PCs or networks and allows data to be transmitted over the Internet as if it were still within those networks. The VPN tunnel uses IPsec (Internet Protocol security) to encrypt the data sent between the two networks and encapsulate the data within a normal Ethernet/IP frame so as to transport the private network securely and seamlessly through other public or private networks.

A VPN provides a cost-effective and more secure alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques, an Internet Protocol Security (IPsec) VPN creates a secure connection that operates as if you were directly connected to your local network.

For example, a VPN allows users to sit at home and connect to his/her employer's corporate network and receive an IP address in their private network just as though they were sitting in their office connected to their corporate LAN.

Another advantage of a VPN network is that all proprietary Microsoft Windows-based networking protocols can pass through the router using the VPN tunnel to access corporate shared network drives.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the wireless home gateway defaults advanced VPN Termination settings.

Click **VPN Termination** in the Advanced Settings section of the Setup page to access the Setup Advanced Settings - VPN Termination - Status page. The VPN Termination - Status page allows you to create, configure, and control IPsec VPN tunnels.

Setup Advanced Settings - VPN Termination - Blank Status Page

The following illustration is an example of a blank Setup Advanced Settings - VPN Termination - Status page. No VPN tunnels are configured.

VPN Termination - Status
This page allows you to enable VPN protocols and manage VPN tunnels.

IPsec
IPsec Endpoint: Disabled

#	Name	Status	Control	Configure
1		NOT Connected	Endpoint disabled	Edit Delete

[Add New Tunnel...](#)

[Event Log](#)

Setup Advanced Settings - VPN Termination - Status Page with VPN Tunnel Configured

The following illustration is an example of the Setup Advanced Settings - VPN Termination - Status page with a VPN tunnel configured.

VPN Termination - Status
This page allows you to enable VPN protocols and manage VPN tunnels.

IPsec
IPsec Endpoint: Disabled

#	Name	Status	Control	Configure
1		NOT Connected	Endpoint disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Setup Advanced Settings - VPN Termination - Status Page Description

This section describes the section headings and field descriptions of the Setup Advanced Settings - VPN Termination - Status page. This page allows you to create, configure, and control IPsec VPN tunnels.

Note: You can set up and manage up to 50 different VPN tunnels.

Field Name	Description
IPsec Endpoint	Enables/disables the IPsec endpoint mode.
Name	Displays the user-defined tunnel name entered from the VPN Setup page.
Status	Displays the current connection state (Connected/NOT Connected).
Control	Displays one of the following three keys based on the current tunnel enable and connection state: <ul style="list-style-type: none"> ■ Enable ■ Connect ■ Endpoint disabled
Configure	Displays Edit or Delete keys used for settings management.
Add New Tunnel	Allows you to create a new tunnel configuration. When you click Add New Tunnel , the VPN Setup page opens.
Event Log	Allows you to access the Event Log page. The Event Log page shows a history of VPN connections and activity in chronological order and also displays the IP address of both endpoints on the tunnel (local and remote).

Note: On the Event Log page, pressing the **Refresh** key updates the Event Log table to show any changes since the page was loaded. Pressing the **Clear** key clears the log table of its current contents and only the most recent data appears.

Creating and Configuring IPsec VPN Tunnels

To create and configure IPsec VPN tunnels, click **Add New Tunnel** on the VPN Termination - Status page. The VPN Setup page opens. The following illustration is an example of the VPN Setup page.

The screenshot displays the 'VPN Setup' page with a navigation bar at the top containing tabs for System, Signal, Status, Log, EMTA, and Setup. The 'Setup' tab is active. Below the navigation bar, the page title 'VPN Setup' is followed by a description: 'This page allows you to configure and manage VPN tunnels.'

The configuration area is divided into several sections:

- Tunnel Selection:** A dropdown menu shows 'Tunnel 1'. To its right are buttons for 'Delete Tunnel', 'Add New Tunnel', and 'Apply'.
- Name:** A text input field is present.
- Status:** A dropdown menu is set to 'Disabled'.
- Local endpoint settings:**
 - Address group type:** A dropdown menu set to 'IP subnet'.
 - Subnet:** A text input field containing '192.168.0.0'.
 - Mask:** A text input field containing '255.255.255.0'.
 - Identity type:** A dropdown menu set to 'IP address'.
 - Identity:** A text input field.
- Remote endpoint settings:**
 - Address group type:** A dropdown menu set to 'IP subnet'.
 - Subnet:** A text input field containing '0.0.0.0'.
 - Mask:** A text input field containing '0.0.0.0'.
 - Identity type:** A dropdown menu set to 'IP address'.
 - Identity:** A text input field.
 - Network address type:** A dropdown menu set to 'IP address'.
 - Remote Address:** A text input field containing '0.0.0.0'.
- IPsec settings:**
 - Pre-shared key:** A text input field containing 'EnterAKey'.
 - Phase 1 DH group:** A dropdown menu set to 'Group 1 (768 bits)'.
 - Phase 1 encryption:** A dropdown menu set to 'DES'.
 - Phase 1 authentication:** A dropdown menu set to 'MD5'.
 - Phase 1 SA lifetime:** A text input field containing '28800' followed by the unit 'seconds'.
 - Phase 2 encryption:** A dropdown menu set to 'DES'.
 - Phase 2 authentication:** A dropdown menu set to 'MD5'.
 - Phase 2 SA lifetime:** A text input field containing '3600' followed by the unit 'seconds'.

At the bottom of the page, there is a 'Show Advanced Settings' button and two buttons: 'Apply' and 'VPN Status'.

Setup Advanced Settings - VPN Setup Page Description

This section describes the section headings and field descriptions of the Setup Advanced Settings - VPN Setup page. This page allows you to create, configure, and control IPsec VPN tunnels.

Tunnel Section

Field Name	Description
Tunnel	Displays existing tunnels and allows each tunnel to be individually configured.
Name	Displays the name of a group of settings for a single tunnel. If no name is entered, the tunnels are named sequentially 1, 2, 3, and so on.
Enable/Disable	Enables/disables a VPN tunnel after the tunnel is named and configured. Click Apply to activate the selected setting (Enabled or Disabled).

Function Keys

The following table describes the function keys associated with the Tunnel section of the VPN Setup page.

Key	Description
Delete Tunnel	Allows you to delete a tunnel.
Add New Tunnel	Allows you to create a heading for the tunnel settings that you can select using the Tunnel drop-down menu.
Apply	Activates the selected setting (Enabled or Disabled).

Local Endpoint Settings

The following table describes the fields in the Local endpoint settings section of the VPN Setup page.

Field Name	Description
Address group type	<p>Allows you to select the address group type for the local VPN access group. The following types are available:</p> <ul style="list-style-type: none"> ■ IP subnet ■ Single IP address ■ IP address range

Field Name	Description
Subnet	<p>Allows you to enter Subnet information based on the selected Address group type as follows:</p> <ul style="list-style-type: none"> ■ For IP subnet, enter the subnet. ■ For single IP address, enter only the specific IP address. ■ For IP address range, enter the starting and ending IP addresses.
Mask	<p>Allows you to enter Mask information based on the selected Address group type as follows:</p> <ul style="list-style-type: none"> ■ For IP subnet, enter the subnet mask. ■ For single IP address, enter only the specific IP address in the Subnet field. Leave this field blank. ■ For IP address range, enter the starting IP and ending IP addresses.
Identity type	<p>Allows you to select the local Identity type from one of the following options:</p> <ul style="list-style-type: none"> ■ WAN IP address of the router (default) ■ User-specified IP address ■ Fully qualified domain name (FQDN) ■ Email address <p>This is the identity that the far endpoint will use for identification of the VPN termination point. The remote VPN endpoint on the other end of the tunnel should match these settings for its remote endpoint settings.</p>
Identity	<p>Allows you to enter the identity string after you have selected the identity type using one of the following formats:</p> <ul style="list-style-type: none"> ■ For IP address mode, use the format xxx.xxx.xxx.xxx. ■ For FQDN, use the format "yourdomain.com." ■ For email address, use the format "yourname@yourdomain.com." <p>The remote VPN endpoint on the other end of the tunnel should match these settings for its remote endpoint settings.</p>

Remote Endpoint Settings

These settings control how the local endpoint (router) connects to the far VPN termination point (the other end of the VPN tunnel).

Field Name	Description
Address group type	<p>Allows you to select the address group type for the remote VPN access group. The following types are available:</p> <ul style="list-style-type: none"> ■ IP subnet ■ Single IP address ■ IP address range <p>The remote VPN endpoint on the other end of the tunnel should match these settings for its remote endpoint settings.</p>
Subnet	<p>Allows you to enter Subnet information based on the selected Address group type as follows:</p> <ul style="list-style-type: none"> ■ For IP subnet, enter the subnet. ■ For single IP address, enter only the specific IP address. ■ For IP address range, enter the starting and ending IP addresses.
Mask	<p>Allows you to enter Mask information based on the selected Address group type as follows:</p> <ul style="list-style-type: none"> ■ For IP subnet, enter the subnet mask. ■ For single IP address, enter only the specific IP address in the Subnet field. Leave this field blank. ■ For IP address range, enter the starting IP and ending IP addresses.
Identity type	<p>Allows you to select the remote Identity type from one of the following options:</p> <ul style="list-style-type: none"> ■ WAN IP address of the router (default) ■ User-specified IP address ■ Fully qualified domain name (FQDN) ■ Email address <p>This is the identity that the far endpoint will use for identification of the VPN termination point. The remote VPN endpoint on the other end of the tunnel should match these settings for its remote endpoint settings.</p>

Field Name	Description
Identity	<p>Allows you to enter the identity string after you have selected the identity type using one of the following formats:</p> <ul style="list-style-type: none"> ■ For IP address mode, use the format xxx.xxx.xxx.xxx. ■ For FQDN, use the format "yourdomain.com." ■ For email address, use the format "yourname@yourdomain.com." <p>The remote VPN endpoint on the other end of the tunnel should match these settings for its remote endpoint settings.</p>
Network address type	<p>Allows you to enter the address type for the endpoint WAN. Choose one of the following options:</p> <ul style="list-style-type: none"> ■ IP address ■ FQDN
Remote address	<p>Allows you to enter either the IP address or the FQDN of the remote endpoint depending on what Network Address type you selected.</p>

IPsec Settings

With VPN tunnels, there are two phases of Security Association (SA).

- Phase 1 - Phase 1 creates an Internet Key Exchange (IKE) SA.
- Phase 2 - When Phase 1 is complete, Phase 2 creates one or more IPsec SAs that are then used to key IPsec sessions.

Field	Description
Pre-shared key	<p>Allows you to enter the Pre-shared key of the firewall identifier if one side of the VPN tunnel is using a unique firewall.</p>
Phase 1 DH group	<p>Allows you to select one of following three Diffie-Hellman (DH) encryption/decryption groups:</p> <ul style="list-style-type: none"> ■ 768 bits ■ 1024 bits ■ 1536 bits <p>Diffie-Hellman is a cryptographic technique that uses public and private keys for encryption and decryption. The higher number of bits selected, the more secure the connection.</p>

Field	Description
Phase 1 encryption	<p>Allows you to select the form of encryption to secure the VPN connection between endpoints. Select from the following five encryption types:</p> <ul style="list-style-type: none"> ■ DES ■ 3DES ■ AES-128 ■ AES-192 ■ AES-256 <p>You may choose any encryption type as long as the other end of the VPN tunnel uses the same method.</p>
Phase 1 authentication	<p>Allows you to select an authentication type for another level of security. Select one of the following authentication types:</p> <ul style="list-style-type: none"> ■ MD5 ■ SHA <p>You may choose either authentication type as long as the other end of the VPN tunnel uses the same method.</p> <p>Note: SHA is recommended because it is more secure.</p>
Phase 1 SA lifetime	<p>Allows you to enter the number of seconds for an individual rotating key to last until a re-key negotiation between each endpoint occurs. Smaller lifetimes are generally more secure since it would give a hacker a smaller amount of time to try to crack the key. However, key negotiation does take up bandwidth, so network throughput is sacrificed with small lifetimes. The default setting is 28,800 seconds.</p>
Phase 2 encryption	<p>Allows you to select the form of encryption to secure the VPN connection between endpoints. Select from the following five encryption types:</p> <ul style="list-style-type: none"> ■ DES ■ 3DES ■ AES-128 ■ AES-192 ■ AES-256 <p>You may select any form of encryption as long as the other end of the VPN tunnel uses the same method.</p> <p>Note: 3DES encryption is commonly used, but AES is recommended because it is very difficult to crack.</p>

Field	Description
Phase 2 authentication	<p>Allows you to select an authentication type for another level of security. Select one of the following three authentication types:</p> <ul style="list-style-type: none"> ■ MD5 ■ SHA ■ Null (none) <p>You may choose any authentication type as long as the other end of the VPN tunnel uses the same method.</p> <p>Note: SHA is recommended because it is more secure.</p>
Phase 2 SA lifetime	<p>Allows you to enter the number of seconds for an individual rotating key to last until a re-key negotiation between each endpoint occurs. Smaller lifetimes are generally more secure since it would give a hacker a smaller amount of time to try to crack the key. However, key negotiation does take up bandwidth, so network throughput is sacrificed with small lifetimes. The default setting for Phase 2 is 3,600 seconds.</p>

Save Configuration to Server

Use the Setup Advanced Settings - Save Configuration to Server page to save the gateway settings to a remote server in the network. When the gateway is rebooted or reset, the gateway will automatically retrieve its configuration file and restore the saved settings.

Setup Advanced Settings - Save Configuration to Server Page

The following illustration is an example of the Setup Advanced Settings - Save Configuration to Server page.

Setup Advanced Settings - Save Configuration to Server Page Description

The following table describes the fields available on the Setup Advanced Settings - Save Configuration to Server page.

Field Name	Description
Configuration file name	The name of the file that is used to store the gateway's settings
Configuration file server	The IP address of a host (TFTP server) with the configuration file

Function Keys

The following table describes the function keys available on the Setup Advanced Settings - Save Configuration to Server page.

Key	Description
Get configuration file now	Click to retrieve file used to store the gateway's settings.
Save configuration file now	Click to save the gateway's settings.
Apply	Click to save changes without closing the page.

Configure Firewall Settings

This section describes how to configure Firewall settings for the residential gateway.

Configuring Firewall Protection

Use the Setup Firewall - Options page to configure web page filtering and firewall protection. This page allows you to enable various firewall protection filters.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default firewall options settings.

Click **Options** in the Firewall section of the Setup page to access the Setup Firewall - Options page.

Setup Firewall - Options Pages

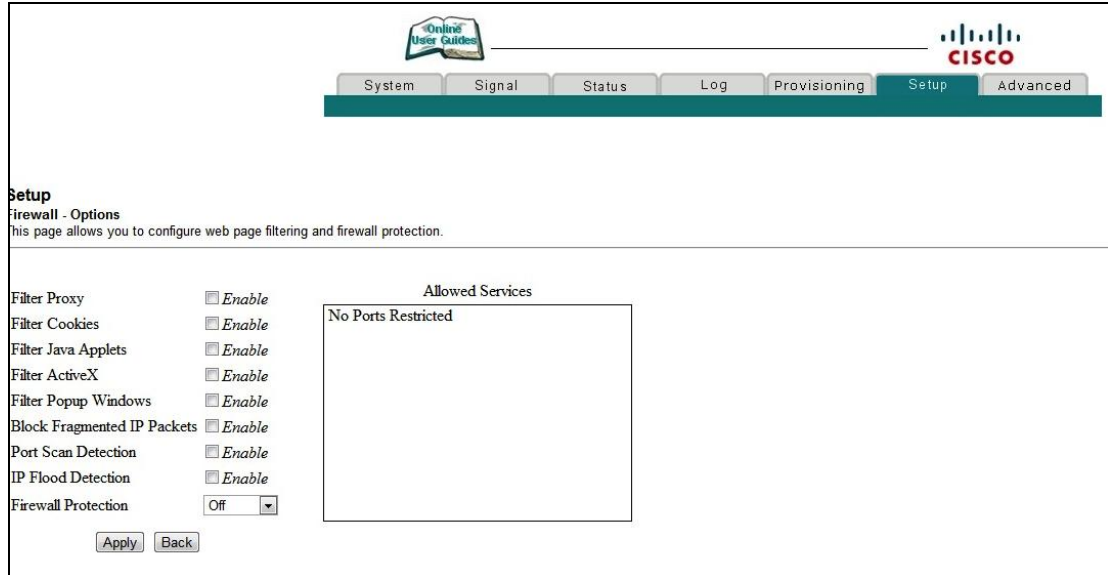
The following sections provide examples of the Setup Firewall - Options pages when the firewall option is set to provide the following levels of protection:

- Off
- Low
- Medium
- High

Note: A Low level corresponds to the previous **Firewall ON** setting.

Setup Firewall - Options Page (Off)

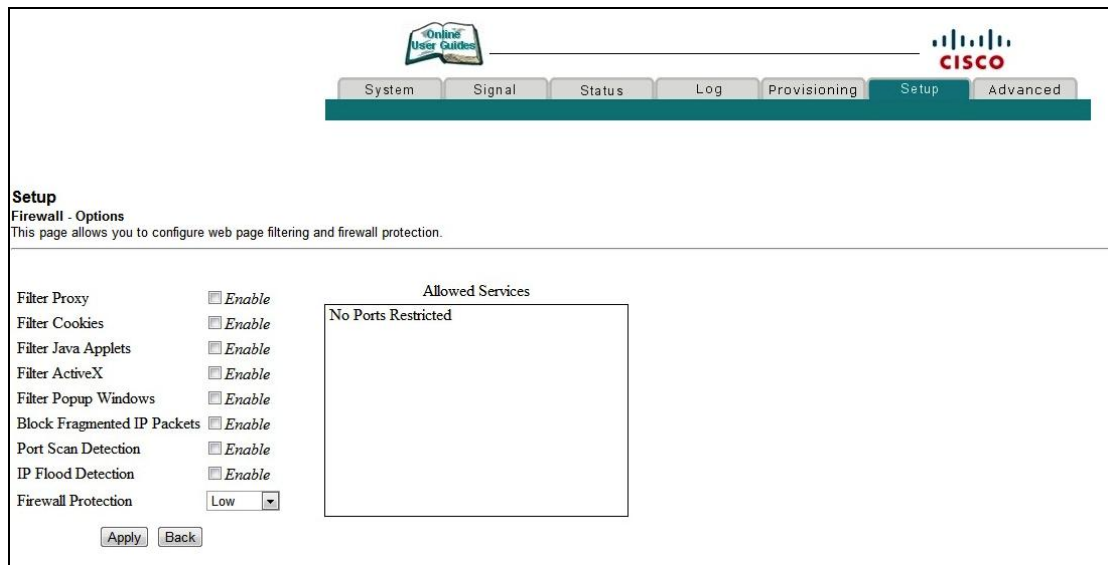
When the SPI firewall is completely disabled, a page similar to the following appears.



The screenshot shows the 'Setup Firewall - Options' page in a Cisco web interface. The 'Setup' tab is selected in the top navigation bar. The page title is 'Setup Firewall - Options' with a subtitle 'This page allows you to configure web page filtering and firewall protection.' On the left, there is a list of settings: 'Filter Proxy', 'Filter Cookies', 'Filter Java Applets', 'Filter ActiveX', 'Filter Popup Windows', 'Block Fragmented IP Packets', 'Port Scan Detection', 'IP Flood Detection', and 'Firewall Protection'. Each of the first eight settings has a checkbox labeled 'Enable'. The 'Firewall Protection' setting is set to 'Off' in a dropdown menu. To the right, under the heading 'Allowed Services', there is a box containing the text 'No Ports Restricted'. At the bottom left, there are 'Apply' and 'Back' buttons.

Setup Firewall - Options Page (Low)

When the SPI firewall is enabled with no ports restricted, a page similar to the following appears.



The screenshot shows the 'Setup Firewall - Options' page in a Cisco web interface, similar to the previous one but with 'Firewall Protection' set to 'Low'. The 'Setup' tab is selected in the top navigation bar. The page title is 'Setup Firewall - Options' with a subtitle 'This page allows you to configure web page filtering and firewall protection.' On the left, the same list of settings is present, with 'Filter Proxy' through 'IP Flood Detection' all set to 'Enable' and 'Firewall Protection' set to 'Low' in a dropdown menu. To the right, under the heading 'Allowed Services', there is a box containing the text 'No Ports Restricted'. At the bottom left, there are 'Apply' and 'Back' buttons.

Chapter 3 Configuring the DOCSIS Residential Gateway

Setup Firewall - Options Page (Medium)

When the SPI firewall is enabled with a list of Allowed Services that are allowed through the firewall, a page similar to the following appears.

The screenshot shows the 'Setup Firewall - Options' page. The 'Firewall Protection' is set to 'Medium'. The 'Allowed Services' table lists the following services:

Service	Port	Protocol
DHCPv6	546	UDP
DNS TCP	53	TCP
DNS UDP	53	UDP
FTP-S	989	TCP
HTTP	80	TCP
HTTP ALT	8080	TCP
HTTP-S	443	TCP
IMAP	143	TCP
IMAP-S	993	TCP
IPSec NAT-T	4500	UDP
NTP	123	UDP

Setup Firewall - Options Page (High)

When the SPI firewall is enabled with a shortened list of Allowed Services that are allowed through the firewall, a page similar to the following appears.

The screenshot shows the 'Setup Firewall - Options' page. The 'Firewall Protection' is set to 'High'. The 'Allowed Services' table lists the following services:

Service	Port	Protocol
DNS TCP	53	TCP
DNS UDP	53	UDP
HTTP	80	TCP
HTTP-S	443	TCP
IMAP-S	993	TCP
IPSec NAT-T	4500	UDP
NTP	123	UDP
POP3-S	995	TCP
SSH	22	TCP
SMTP	25	TCP

Setup Firewall - Options Pages Description

This section describes the section headings and fields descriptions of the Setup Firewall - Options pages.

Note: If you make changes in any of the fields in a Setup Firewall - Options page, click **Apply** to apply and save your Firewall settings.

The following table provides a description of each field name within the Setup Firewall - Options page.

Field Name	Description
Filter Proxy	Enables/disables proxy
Filter Cookies	Enables/disables cookie blocking. This feature filters the unsolicited delivery of cookies to devices from the Internet to devices in your private local network. Cookies are computer files that contain personal information or web surfing behavior data.
Filter Java Applets	Enables/disables java applets. This feature helps to protect the devices in your private network from irritating or malicious Java applets that are sent, unsolicited, to devices in your private network from the Internet. These applets run automatically when they are received by a PC.
Filter ActiveX	Enables/disables ActiveX controls. This feature helps to protect the devices in your private network from irritating or malicious ActiveX controls that are sent, unsolicited, to devices in your private network from the Internet. These ActiveX controls run automatically when they are received by a PC.
Filter Popup Windows	Enables/disables popup windows. Some commonly used applications employ popup windows as part of the application. If you disable popup windows, it may interfere with some of these applications.
Block Fragmented IP Packets	Enables/disables filtering of fragmented IP packets. This feature helps protect your private local network from Internet based denial of service attacks.
Port Scan Detection	Enables/disables the gateway from responding to Internet based port scans. This feature is designed to protect your private local network from Internet based hackers who attempt to gain unsolicited access your network by detecting open IP ports on your gateway.
IP Flood Detection	Blocks malicious devices that are attempting to flood devices or networks with illegal broadcast packets. Also referred to as "broadcast storm." The default setting is OFF.
Firewall Protection	Enables/disables the firewall. When the firewall is enabled, the firewall will allow most commonly used applications to automatically open IP ports and pass data without any special setup or manual port configuration.

Setup Firewall - Options Page Description

This section describes the section headings and fields descriptions of the Setup Firewall - Options page.

Note: If you make changes in any of the fields in the Setup Firewall - Options page, click **Apply** to apply and save your Firewall settings.

The following table provides a description of each field name within the Setup Firewall - Options page.

Field Name	Description
Filter Proxy	Enables/disables proxy.
Filter Cookies	Enables/disables cookie blocking. This feature filters the unsolicited delivery of cookies to devices from the Internet to devices in your private local network. Cookies are computer files that contain personal information or web surfing behavior data.
Filter Java Applets	Enables/disables java applets. This feature helps to protect the devices in your private network from irritating or malicious Java applets that are sent, unsolicited, to devices in your private network from the Internet. These applets run automatically when they are received by a PC.
Filter ActiveX	Enables/disables ActiveX controls. This feature helps to protect the devices in your private network from irritating or malicious ActiveX controls that are sent, unsolicited, to devices in your private network from the Internet. These ActiveX controls run automatically when they are received by a PC.
Filter Popup Windows	Enables/disables popup windows. Some commonly used applications employ popup windows as part of the application. If you disable popup windows, it may interfere with some of these applications.
Block Fragmented IP Packets	Enables/disables filtering of fragmented IP packets. This feature helps protect your private local network from Internet based denial of service attacks.
Port Scan Detection	Enables/disables the gateway from responding to Internet based port scans. This feature is designed to protect your private local network from Internet based hackers who attempt to gain unsolicited access your network by detecting open IP ports on your gateway.
IP Flood Detection	Blocks malicious devices that are attempting to flood devices or networks with illegal broadcast packets. Also referred to as "broadcast storm."
Firewall Protection	Enables/disables the firewall. When the firewall is enabled, the firewall will allow most commonly used applications to automatically open IP ports and pass data without any special setup or manual port configuration.

Configuring Firewall Event Logging and E-mail Alerts

Use the Setup Firewall - Event Logging page to access the firewall event log and allows you to enter your e-mail address in order for you to receive e-mail alerts related to firewall attacks by hackers.

Note: If you are not familiar with the settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default firewall event logging settings.

Click **Event Logging** in the Firewall section of the Setup page to access the Setup Firewall - Event Logging page.

Setup Firewall - Event Logging Page

The following illustration is an example of the Setup Firewall - Event Logging page.

Setup
Firewall - Event Logging
 This page provides access to the firewall event log and allows you to enter your email address for email alerts related to firewall attacks.

Contact Email Address

SMTP Server Name

E-mail Alerts ☐ *Enable*

Description	Count	Last Occurrence	Target	Source
-------------	-------	-----------------	--------	--------

Setup Firewall - Event Logging Page Description

The Setup Firewall - Event Logging page shows events captured by the firewall. The log displays the following items:

- Description of the event
- Number of events that have occurred
- Last occurrence of an event
- Target and source addresses

You can configure the system to send e-mails regarding log events to the administrator in order for the administrator to monitor the firewall.

This section describes the section headings and fields descriptions of the Setup Firewall - Event Logging page.

Field Name	Description
Enable E-mail Address	Allows you to enter the e-mail address of the person who monitors the firewall. When an event occurs, it will be logged and an e-mail will be sent to this address automatically reporting the event.
SMTP Server Name	Allows you to enter the mail server name of your outgoing mail server, or the mail server of your Internet service provider (ISP).
E-mail Alerts	Allows you to enable or disable sending e-mail alerts.
Description	Describes what event was detected by the gateway's firewall.
Count	Displays the number of times the event has been detected.
Last Occurrence	Displays the time the last occurrence of this event was detected.
Target	Displays the IP address of the device in your private local network to which the event was directed along with the IP port number targeted by the event.
Source	Displays the IP address of the Internet based source of the event along with the IP port number used by that device.

Function Keys

The following function keys appear on the Setup Firewall - Event Logging page.

Key	Description
Apply	Saves the values you enter into the fields without closing the screen.
E-mail Log	Allows you to force the system to send an e-mail alert even if the E-mail Alerts box is left unchecked.
Clear Log	Allows you to clear all entries in the log.

Configure Parental Control Settings

This section describes how to configure Parental Control settings for the residential gateway.

Configuring Parental Control

Use the Setup Parental Control - User Setup page to configure parental controls on the residential gateway, and to add or delete the individuals who are authorized to set parental controls.

Note: If you are not familiar with the settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default parental control settings.

Click **User Setup** in the Parental Control section of the Setup page to access the Setup Parental Control - User Setup page.

Setup Parental Control - User Setup Page

The following illustration is an example of the Setup Parental Control - User Setup page.

SystemSignalStatusLogProvisioningSetupAdvanced

Setup

Parental Control - User Setup

This page allows configuration of users.

User Configuration

Add User

User Settings

1. Default

☐ Enable

Remove User

Password

Re-Enter Password

Trusted User

☐ Enable

Content Rule

1. Default

Time Access Rule

No rule set

Session Duration

0 min

Inactivity time

0 min

Apply

Setup Parental Control - User Setup Page Description

This section describes the section headings and fields descriptions of the Setup Parental Control - User Setup page. This page allows you to set up user profiles. Each profile can be assigned customized levels of Internet access as defined by the access rules assigned to that user's profile.

Note: Once you define and enable user profiles, each user must sign-on each time they wish to access the Internet. The user can sign-on when the pop-up sign-on screen appears in their web browser. The user must enter their correct user name and password in order to gain Internet access.

Important:

- Make sure to disable pop-up blockers on your web browser when using user profiles.
- User names and passwords are case-sensitive.

Field Name	Description
Add User	Allows you to add a new user profile. Enter the name of the user and click the Add User button to add the user to the list.
User Settings	<p>Allows you to edit a user profile by using the drop-down menu to edit a user profile. The drop-down menu allows you to recall the profile to be edited. User names and passwords are case-sensitive.</p> <p>Make sure to check the Enable box to activate the user profile. If a profile is not active, that user will not have any access to the Internet.</p> <p>To remove a user profile, use the drop-down menu to select the user to be removed and click the Remove User button.</p>
Password	<p>Enter the selected user's password in this field. Each user must enter their user name and password each time they use the Internet. User names and passwords are case-sensitive.</p> <p>Note: The gateway will allow each user access to the Internet, subject to the rules selected on this page for that user.</p>
Re-Enter Password	Re-enter the same password for confirmation of the password in the previous field.
Trusted User	Check this box if the currently selected user is to be designated a trusted user. Trusted users are not subject to Internet access rules.
Content Rule	Select the Content Rule for the current user profile. Content Rules must first be defined by going to the Rules Configuration page. You can access the Rule Configuration page by clicking the Basic Rules link under the Parental Control section of the Setup page.

Field Name	Description
Time Access Rule	Select the Time Access Rule for the current user profile. Time Access Rules must first be defined by going to the Time of Day Filter page. You can access the Time of Day Filter page by clicking the Time of Day Rules link under the Parental Control section of the Setup page.
Session Duration	<p>1440 minutes (factory default).</p> <p>Enter the amount of time in minutes that the user will be granted Internet access beginning at the time they sign on using their user name and password.</p> <p>Note: Set the Session Duration to 0 (zero) to prevent session timeout.</p>
Inactivity time	<p>60 minutes (factory default).</p> <p>Enter the amount of time during a user session where there is no Internet access activity, indicating that the user is no longer online. If the inactivity timer is triggered, the user session will be closed automatically. In order to regain Internet access, the user must log in again with their user name and password.</p> <p>Note: Set the Inactivity time value to 0 (zero) to prevent timeout due to inactivity.</p>
Available Rules	<p>Lists available rules. Apply a rule by selecting it from the list and adding it to the current user profile.</p> <p>Note: This field appears only if rules have been created. Create rules using the Parental Control Setup pages that follow next.</p>
Current Used Rules	<p>Lists rules in use for the current user profile. You can apply a maximum of four rules to each user profile.</p> <p>Note: This field appears only when a rule is associated with a user profile.</p>

Function Keys

The following function keys appear on the Setup Parental Control - User Setup page.

Key	Description
Add User	Adds and saves a new user to the list of user profiles.
Remove User	Removes the selected user from the list of user profiles.
Apply	Saves all additions, edits, and changes.

Configuring Parental Control Basic Rules

Use the Setup Parental Control - Basic Setup page to select the rules that block certain Internet content and certain websites.

Note: If you are not familiar with the settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default parental control settings.

Click **Basic Rules** in the Parental Control section of the Setup page to access the Setup Parental Control - Basic Setup page.

Setup Parental Control - Basic Setup Page

The following illustration is an example of the Setup Parental Control - Basic Setup page.

Setup

Parental Control - Basic Setup

This page allows basic selection of rules which block certain Internet content and certain Web sites. When you change your Parental Control settings, you must click on the appropriate "Apply", "Add" or "Remove" button for your new settings to take effect. If you refresh your browser's display, you will see the currently active settings.

Parental Control Activation

This box must be checked to turn on Parental Control

☐ Enable Parental Control

Rule Configuration

Rule Settings

1. Default

Keyword List

anonymizer

Blocked Domain List

anonymizer.com

Allowed Domain List

Override Password

If you encounter a blocked website, you can override the block by entering the following password

Password

Re-Enter Password

Access Duration 30

Setup Parental Control - Basic Setup Page Description

This section describes the section headings and fields descriptions of the Setup Parental Control - Basic Setup page. This page allows you to create Internet access rules based on the content found in the URLs of Internet sites.

Field Name	Description
Parental Control Activation	Allows you to enable or disable parental controls. To enable parental controls, select the Enable Parental Control check box and click Apply . To disable parental controls, clear the Enable Parental Control check box and click Apply .
Rule Configuration	<p>Allows you to add a new content rule. Enter the name of the rule and click the Add Rule button to add the content rule to the list. Content rules are used to restrict Internet access based on IP addresses, domains, and keywords found in the URLs of Internet sites.</p> <p>Note: It may be useful to set up your first rule as “No Rule,” without any restrictions or settings. This setting will allow you to assign “No Rule” status to users who are not subject to “content-related” access restrictions.</p>
Rule Settings	<p>Allows you to edit a content rule by using the drop-down menu to recall the rule to be edited.</p> <p>To remove a user profile, use the drop-down menu to select the rule to be removed and click on the Remove Rule button.</p>
Keyword List	Allows you to create a list of keywords. Any attempt to access a URL that contains any of the keywords in this list will be blocked by the gateway.
Blocked Domain List	Allows you to create a list of domains that the gateway should block access to. Any attempt to access any of the domains in this list will be blocked by the gateway.
Allowed Domain List	Allows you to create a list of domains to which the gateway allows access.
Override Password	Allows you to create a password to temporarily override user access restrictions to a blocked Internet site.
Re-enter Password	Re-enter the same password for confirmation of the override password in the previous field.
Duration	Allows you to designate an amount of time in minutes that the Override password will allow temporary access to a restricted Internet site.

Function Keys

The following function keys appear on the Setup Parental Control - Basic Setup page.

Key	Description
Add Rule	Adds and saves a new Rule to the list of content Rules.
Remove Rule	Removes the selected rule from the content rule list.
Add/Remove Keyword	Allows you to add new keywords to the list or to delete selected keywords from the list.
Add/Remove Domain	Allows you to add new domains to the list or to delete selected domains from the list.
Add/Remove Allowed Domain	Allows you to add new domains to the list or to delete selected domains from the list.
Apply	Saves all additions, edits, and changes.

To use Keyword and Domain Blocking

Keyword and Domain blocking allows you to restrict access to Internet sites by blocking access to those sites based on a word or a text string contained in the URLs used to access those Internet sites.

Domain blocking allows you to restrict access to websites based on the site's domain name. The domain name is the portion of the URL that precedes the familiar .COM, .ORG, or .GOV extension.

Keyword blocking allows you to block access to Internet sites based on a Keyword or text string being present anywhere in the URL, not just in the domain name.

Note: The Domain blocking feature blocks access to any domain in the Domain List. It will also block domains, any portion of which contains an exact match to entries in the list.

For example, if you enter **example.com** as a domain, any site that contains "example.com" will be blocked. Generally, you do not want to include "www." in a domain name since doing so limits the blocking to only the site that matches that domain name exactly. For instance, if you enter www.example.com into the list, only the one site that matches that name exactly will be blocked. Consequently, if you do not include the "www.," then all sites within and associated with "example.com" will be blocked.

Configuring Parental Control Time of Day Access Filters

Use the Setup Parental Control - Time of Day Access Filter page to configure web access filters to block all Internet traffic to and from specific network devices based on day of week and time of day settings that you select.

Note: If you are not familiar with the settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default parental control settings.

Click **Time of Day Rules** in the Parental Control section of the Setup page to access the Parental Control - Time of Day Access Filter page.

Setup Parental Control - Time of Day Access Filter Page

The following illustration is an example of the Setup Parental Control - Time of Day Access Filter page.

Note: The residential gateway uses the network time of day clock that is managed by your data service provider. The time of day clock must be accurate and represent the time of day in your time zone for this feature to operate properly. Verify that the Status and Set Time pages reflect the correct time of day. If they do not reflect the correct time of day, contact your data service provider. You can also adjust your settings to account for the difference.

System Signal Status Log Provisioning **Setup** Advanced

Setup
Parental Control - Time of Day Access Filter
 This page allows configuration of web access filters to block all internet traffic to and from specific network devices based on time of day settings.

No filters entered. ☐ Enabled

Days to Block

☐ Everyday ☐ Sunday ☐ Monday ☐ Tuesday
☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Time to Block

☐ All day

Start: 12 (hour) 00 (min) AM
 End: 12 (hour) 00 (min) AM

Function Keys

The following function keys appear on the Setup Parental Control - Time of Day Access Filter page.

Key	Description
Add	Allows you to add a new Time of Day access filter or rule. Enter the name of the filter and click the Add key to add the filter to the list. Time of Day rules are used to restrict Internet access based on the day and time.
Remove	Removes the selected filter from the Time of Day filter list.
Apply	Saves all additions, edits, and changes.

Configure Parental Control Event Reporting

Use the Setup Parental Control - Event Log page to view events captured by the parental control event-reporting feature.

Note: If you are not familiar with the settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default parental control settings.

Click **Local Log** in the Parental Control section of the Setup page to access the Setup Parental Control - Event Log page.

Setup Parental Control - Event Log Page

The following illustration is an example of the Setup Parental Control - Event Log page.



Setup Parental Control - Event Log Page Description

This section describes the section headings and fields descriptions of the Setup Parental Control - Event Log page. This page allows you to track, by user, any attempts made by that user to access Internet sites that are restricted.

Field Name	Description
Last Occurrence	Displays the time of the most recent attempt to access a restricted Internet site.
Target	Displays the URL of the restricted site.
User	Displays the user who attempted a restricted site.
Source	Displays the IP address of the PC that was used when attempting to access a restricted website.

Configure Wireless Settings

This section describes how to configure Wireless settings for the residential gateway.

Configuring Your Wireless Access Point Parameters

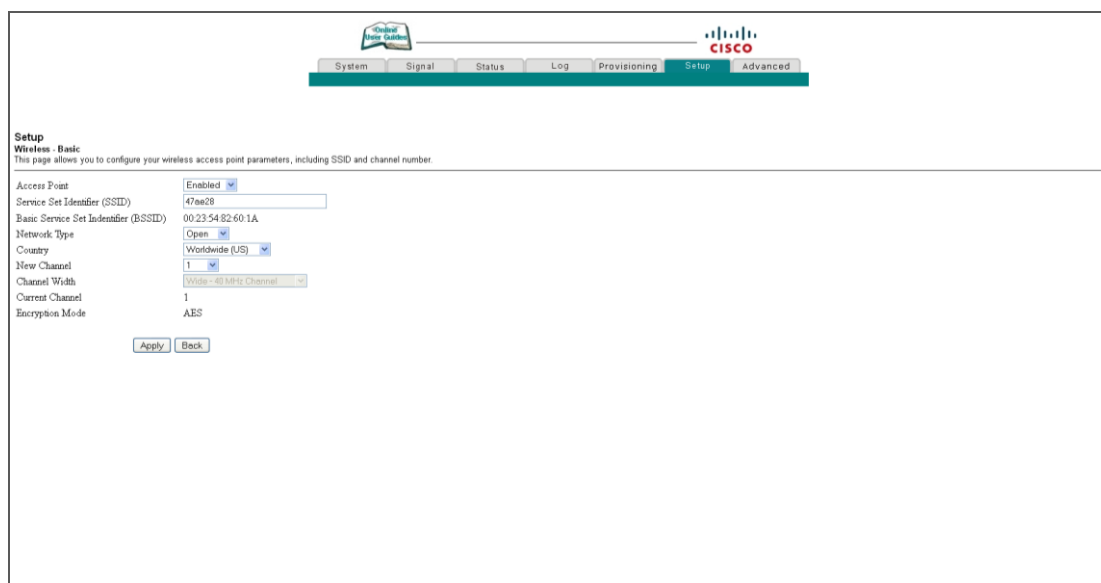
Use the Setup Wireless - Basic page to configure your wireless access point (WAP) parameters, including SSID and channel number.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default wireless basic settings.

Click **Basic** in the Wireless section of the Setup page to access the Setup Wireless - Basic page.

Setup Wireless - Basic Page

The following illustration is an example of the Setup Wireless - Basic page showing the factory default settings.



The screenshot displays the 'Setup Wireless - Basic' configuration page. At the top, there is a navigation bar with tabs: System, Signal, Status, Log, Provisioning, Setup (highlighted), and Advanced. Below the navigation bar, the page title 'Setup Wireless - Basic' is followed by a description: 'This page allows you to configure your wireless access point parameters, including SSID and channel number.' The configuration fields are as follows:

Access Point	Enabled
Service Set Identifier (SSID)	47ae28
Basic Service Set Identifier (BSSID)	00:23:54:82:60:1A
Network Type	Open
Country	Worldwide (US)
New Channel	1
Channel Width	Wide - 40 MHz Channel
Current Channel	1
Encryption Mode	AES

At the bottom of the configuration fields, there are two buttons: 'Apply' and 'Back'.

Setup Wireless - Basic Page Description

This section describes the section headings and fields descriptions of the Setup Wireless - Basic page.

Note: If you make changes in the Setup Wireless - Basic page, click **Apply** to apply and save your wireless basic settings.

Field Name	Description
Access Point	Allows you to turn the access point on the gateway on or off.
Service Set Identifier (SSID)	Identifies the name assigned to this access point. Note: The factory default for the SSID field is the last 6 digits of the cable modem's MAC address as found on the label. The factory default for the SSID field is either the last 6 digits of the cable modem's MAC address as found on the product label attached to your gateway, or the SSID specified on the product label. As a good security practice, we recommend that you change the default SSID to one that is unique to your wireless network.
Basic Service Set Identifier (BSSID)	Identifies the MAC address of the wireless access point.
Network Type	Allows you to select Open or Closed for your network type,
Country	Allows you to select the country in which you are using your access point.
New Channel (1-11)	Allows setting a communications channel for your access point, Note: Wireless networking channels overlap. Channels 1, 6, and 11 do not overlap with each other. For best performance, select one of these channels. If there are other access points in use in the area, select one of these channels that is farthest away from the other access points. Example: If channel 8 is in use by another access point, use channel 1 for your wireless network. Note: If your wireless network is not operating correctly, or if external devices are interfering with your signal, select a different channel. Use your PC wireless utility software to scan for other access points in your area.
Channel Width	Allows setting the channel width for 802.11n radios. Default is 20 MHz channel.
Current Channel	Identifies the present channel the WAP is using.
Encryption Mode	Shows current encryption mode.

Configuring Your Wireless Network Security and Encryption Parameters

Use the Setup Wireless - Security page to configure your WAP wireless equivalent privacy (WEP) encryption keys and authentication.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default wireless security settings.

Click **Security** in the Wireless section of the Setup page to access the Setup Wireless - Security page.

Important: Your residential gateway ships from the factory with WPA security enabled to provide you with a basic level of wireless network security. To gain initial access to your wireless network, select WPA security on your computer's wireless adapter and enter the WPA key to match the key setup in your gateway. The factory default WPA key in the gateway is the serial number of the device. You can continue to use this factory default key. However, to maximize your wireless security, it is highly recommended that you use something other than the factory default key.

Using Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) allows you to easily attach wireless devices that also support WPS. When WPS is enabled and activated, you can attach other wireless clients with the press of a button or by entering the station PIN.

After enabling WPS, you can activate the automatic registration by clicking the **Start WPS** button in the WPS section of the Setup Wireless - Security page.

Setup Wireless - Security Page

The following illustration is an example of the Setup Wireless - Security page.

Setup
Wireless - Security
 This page allows you to configure your wireless privacy settings.

Primary Network: Enabled
 WPA: Disabled
 WPA-PSK: Enabled
 WPA2: Disabled
 WPA2-PSK: Disabled

WPA/WPA2 Encryption: TKIP
 WPA Pre-Shared Key:
 RADIUS Server: 00.0.0
 RADIUS Port: 1812
 RADIUS Key:
 Group Key Rotation Interval: 0
 WPA/WPA2 Re-auth Interval: 3600

WEP Encryption: Disabled
 Shared Key Authentication: Optional
 802.1x Authentication: Disabled
 Network Key 1:
 Network Key 2:
 Network Key 3:
 Network Key 4:
 Current Network Key: 1
 PassPhrase:
 Generate WEP Keys

WiFi Protected Setup (WPS)
 WPS Config: Enable
 Device Name: 466fc2
 Apply

WPS Setup AP
 PIN: 12345670
 Start WPS
 Status:

WPS Add Client
 Add a client: Push-Button PIN
 PIN: 94380507
 Start WPS
 Status:

Apply

Setup Wireless - Security Page Description

This section describes the section headings and fields descriptions of the Setup Wireless - Security page.

Note: If you are not familiar with the settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default wireless security settings. If you make changes in the Setup Wireless - Security page, click **Apply** to save your wireless security settings.

Field Name	Description
Network Authentication	<p>Network Authentication allows only authorized users to gain access to your wireless network. Only users with an authorized user name, password, or pre-shared key are allowed access to the wireless network.</p> <p>Select from the following Network Authentication protocols:</p> <ul style="list-style-type: none"> ■ Primary Network ■ WPA ■ WPA-PSK ■ WPA2 ■ WPA2-PSK <p>Note: Network Authentication restricts access to your wireless network to only authorized computers or users. Authentication does not protect the data you send over the wireless network connection. You must enable encryption to protect data that is transmitted over your wireless network.</p>
WPA/WPA2 Encryption	<p>Allows you to select a WPA/WPA2 security method. The factory default security is WPA-PSK.</p> <ul style="list-style-type: none"> ■ TKIP (Temporal Key Integrity Protocol) ■ AES (Advanced Encryption Standard) - factory default ■ TKIP-AES
WPA Pre-Shared Key	<p>Allows you to set a WPA Pre-Shared key. Enter a text string in this field. The text string or phrase is used to generate a unique set of encryption keys for your network. Use this string to set up wireless devices in your network.</p> <p>The factory default security key is the 9-digit serial number of the gateway. For example: 20167792. See <i>What Types of Service Accounts Do I Need?</i> (on page 11) for the location of the serial number on the label.</p> <ul style="list-style-type: none"> ■ The PSK can be either a text string or a 64 character hexadecimal number. ■ The text string must be an ASCII character string with a minimum of 8 characters but no more than 63. <p>Note: Not all wireless adapter devices support PSK. For these devices, you must enter the encryption keys exactly as they appear in the in wireless gateway fields in the preceding illustration of the Setup Wireless Security page.</p>

Field Name	Description
RADIUS Server	<p>Allows you to enter the IP address of the RADIUS server used for authentication and encryption key derivation.</p> <ul style="list-style-type: none"> ■ This field is used with 802.1x and WPA Network Authentication. ■ The factory default for this field is 0.0.0.0.
RADIUS Port	<p>Determines the port number of the RADIUS server. The port number is usually 1812 (factory default) or 1645, depending on the server used.</p> <p>This field is used with 802.1x and WPA Network Authentication.</p>
RADIUS Key	<p>Allows you to set the Shared Secret key for your RADIUS connection.</p> <ul style="list-style-type: none"> ■ The factory default for this field is empty. ■ This field is used with 802.1x and WPA Network Authentication.
Group Key Rotation Interval	<p>Allows you to set the WPA Group Key Rotation Interval in seconds. This only applies when WPA or WPA2 Network Authentication is enabled.</p> <p>Set this value to 0 (factory default) to disable periodic rekeying. The valid range is 1 to 4,294,967,295 seconds.</p>
WPA/WPA2 Re-auth Interval	<p>Allows you to set the WPA/WPA2 Re-authorization Interval in seconds. This only applies when WPA/WPA2 Network Authentication is enabled.</p> <p>Set this value to 0 (factory default) to disable periodic rekeying. The valid range is 1 to 4,294,967,295 seconds.</p>

Field Name	Description
WEP Encryption	<p>Allows you to enable data encryption to help secure the data that is sent over your wireless network.</p> <p>WEP 128-bit</p> <ul style="list-style-type: none"> 128-bit or 64-bit static key data encryption can be selected when the network is configured to have no authentication. 128-bit static key data encryption is automatically selected when 802.1x network authentication is enabled. <p>Notes:</p> <ul style="list-style-type: none"> Static key authentication uses one of the four encryption keys, as defined below, to encrypt your data. You must manually change keys. The keys do not change or rotate automatically as they do with TKIP. 64-bit and 40-bit encryption are two different names for the same encryption. 128-bit and 104-bit encryption are two different names for the same encryption.
Shared Key Authentication	<p>Allows you to determine if Shared Key Authentication is used in the network. Shared Key Authentication can be used when there is no other network authentication in the network.</p> <ul style="list-style-type: none"> Optional (factory default) - Wireless clients can associate with the wireless access point without authentication. Required - Only wireless clients with a valid network key are allowed to associate with the access point.
802.1x Authentication	<p>Allows you to use 802.1x authentication with WEP encryption (similar to when WPA or WPA2 is enabled).</p>
Network Keys 1 through 4 64 bit keys	<p>Select these keys for use with Encryption Mode set to 64-bit encryption. Enter 5-byte values for a Key. You do not have to set all four Keys. Only one Key is used for a home network. Each value is represented in hexadecimal. Use only these numbers or letters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f to set up your encryption keys.</p> <p>Note: It is generally a good practice to use only lowercase letters when entering WEP encryption keys. Uppercase letters can sometimes be confused with numbers. For example, the uppercase letter "B" is often mistaken for the number "8." Using lowercase characters minimizes the risk of confusing characters when copying keys from one device to another. Uppercase characters will automatically be converted to lowercase when the key or keys are applied and saved to memory.</p> <p>Use two numbers or letters in each box. Record your Key values. You will need these Key values when you set up your client wireless adapter. The Key values in each wireless network device must match.</p>

or

Field Name	Description
Network Keys 1 through 4 128 bit keys	<p>Select these keys for use with Encryption Mode set to 128-bit encryption. Enter 13-byte values for a Key. You do not have to set all four Keys. Usually only one is needed for a home network. Each value is represented in hexadecimal. Use only these numbers or letters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f to set up your encryption keys.</p> <p>It is generally a good practice to use only lowercase letters when entering WEP encryption keys. Uppercase letters can sometimes be confused with numbers. For example, the uppercase letter "B" is often mistaken for the number "8." Using lowercase characters minimizes the risk of confusing characters when copying keys from one device to another. Uppercase characters will automatically be converted to lowercase when the key or keys are applied and saved to memory.</p> <p>Use two numbers or letters in each box. Record your Key values. You will need these Key values when you set up your client wireless adapter. The Key values in each wireless network device <i>must</i> match.</p>
Current Network Key	<p>Allows you to select which of the four 64-bit or 128-bit keys to use to encrypt your data when you are using encryption that requires the manual entry of an encryption key. Only one WEP key is in use at a time. You must manually change keys. They do not change automatically.</p> <p>Notes:</p> <ul style="list-style-type: none"> ■ 64-bit and 40-bit encryption are two different names for the same encryption. ■ 128-bit and 104-bit encryption are two different names for the same encryption.
PassPhrase	<p>Automatically generates WEP encryption keys required to communicate with the network.</p> <p>Although not required for WEP operation, use of a PassPhrase can simplify the configuration and setup of each of your client wireless adapters.</p> <p>Using a PassPhrase eliminates the need to manually enter lengthy encryption keys and reduces the chance of error associated with entering entry of large numbers.</p> <p>Important: Click Generate WEP Keys when complete.</p>

Wi-Fi Protected Setup (WPS) Section

The selections available in this section allow you to configure WPS.

Field Name	Description
WPS Config	Allows you to enable or disable WPS.
Device Name	Allows you to enter your device name.

WPS Setup AP Section

The selections available in this section allow you to use PIN-protected security.

Field Name	Description
PIN	Identifies the personal identification number (PIN) of a device trying to connect.
Status	Displays WPS status.

WPS Add Client Section

The selections available in this section allow you to add a WPS client.

Field Name	Description
Add a Client	Allows you to select your WPS method (push button or PIN).
WPS Status	Displays WPS status.

Function Keys

Keys	Description
Generate WEP Keys	Automatically generates four WEP keys based on the PassPhrase entry. Notes: <ul style="list-style-type: none"> ■ For 64-bit WEP, four unique 64-bit WEP keys will be generated. ■ For 128-bit WEP, only one 128-bit WEP key will be generated. The same key will be entered into all four key locations.
Apply	Saves all additions, edits, and changes for the associated section.
Start WPS	Starts WPS after you select your WPS Method.
Generate PIN Code	Automatically generates a PIN code.

Configuring Wireless Data Rates and Wi-Fi Thresholds

Use the Setup Wireless - Advanced page to configure your WAP data rates and wireless fidelity (Wi-Fi) thresholds.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default wireless advanced settings.

Click **Advanced** in the Wireless section of the Setup page to access the Setup Wireless - Advanced page.

Setup Wireless - Advanced Page Example for 802.11g Radios

The following illustration is an example of the Setup Wireless - Advanced page for 802.11g radios.

Note: We recommend that you do not change the default wireless settings that are shown in the illustration unless you are instructed to do so by your service provider.

Setup
Wireless - Advanced
 This page allows you to configure your wireless access point data rates and WiFi thresholds.

54g™ Network Mode	54g Only
Basic Rate Set	Default
54g™ Protection	Auto
XPress™ Technology	Disabled
Afterburner™ Technology	Disabled
Rate	Auto
Output Power	100%
Beacon Interval	100 ms (1-65535)
DTIM Interval	1 ms (1-255)
Fragmentation Threshold	2346 bytes (256-2346)
RTS Threshold	2347 (0-2347)
Short Retry Limit	7 (1-255)
Long Retry Limit	4 (1-255)

Apply

Setup Wireless - Advanced Page Description for 802.11g Radios

This section describes the section headings and fields descriptions of the Setup Wireless - Advanced page for 802.11g radios.

Note: If you make changes in the Setup Wireless - Advanced page, click **Apply** to apply and save your wireless advanced settings.

Field Name	Description
54G Network Mode	<p>Allows you to optimize the performance of your wireless network using one of the following options:</p> <ul style="list-style-type: none"> ■ Max compatibility (factory default) Allows the access point to interpolate with 802.11b and 802.11g wireless client devices and minimizes interference with nearby 802.11b wireless networks. ■ Only 11G Maximum throughput. In this mode, the wireless access point accepts only 802.11g wireless clients. Setting the device in this mode may degrade the operation of nearby 802.11b and 802.11n wireless networks.

Field Name	Description
Basic Rate Set	Allows you to select the Basic Rate Set.
Xpress Technology	Allows you to enable or disable Xpress Technology.
Afterburner Technology	Allows you to enable or disable Afterburner Technology.
54g Protection	<p>Allows you to prioritize 802.11g communication when there is a mix of 802.11b and 802.11g devices in the wireless network using one of the following options:</p> <ul style="list-style-type: none"> ■ Auto (factory default) Allows 802.11b and 802.11g cells to interoperate seamlessly. ■ Off Maximum performance. Networks with 802.11g-only wireless client devices.
Rate	<p>Allows you to fix the data rate for wireless connections. The following data rates are available:</p> <p>Auto (factory default), 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps</p> <p>Note: In the automatic mode, data rate is a function of signal strength and signal quality.</p>
Output Power	<p>Allows you to adjust the relative output power of your gateway wireless transmitter. The following settings are available:</p> <p>100% (factory default), 75%, 50%, and 25%.</p>
Beacon Interval	Displays the time interval that the WAP uses to announce itself to remote devices. The Beacon Interval should be left at 100ms for compliance with most client cards. The Beacon Interval specifies how often packets are sent by the Access Point (AP) to synchronize a wireless network and its clients.
DTIM Interval	Displays the time interval between Broadcasts/Multicast transmissions. The DTIM (Delivery Traffic Indication Message) Interval is a countdown informing the wireless clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The DTIM Interval should be left at 3 ms for compliance with most client cards.
Fragmentation Threshold	Allows you to set the fragmentation threshold. This threshold should be set equivalent to the maximum Ethernet frame size allowable on the link including overhead (1536 bytes). Lesser settings can damage data throughput as large frames could be fragmented or collisions could occur. The factory default is 2346.

Field Name	Description
RTS Threshold	Determines at what packet size beyond which the ready to send/clear to send (RTS/CTS) mechanism is invoked. The factory default is 2347.
Short Retry Limit	The number of times the gateway transmits an unacknowledged unicast frame that is shorter than the RTS threshold before discarding the frame. The factory default is 7.
Long Retry Limit	The number of times the gateway transmits an unacknowledged unicast frame that is longer than the RTS threshold before discarding the frame. The factory default is 4.

Setup Wireless - Advanced Page Example for 802.11n Radios

The following illustration is an example of the Setup Wireless - Advanced page for 802.11n radios.

Note: We recommend that you do not change the default wireless settings that are shown in the illustration unless you are instructed to do so by your service provider.

The screenshot displays the 'Setup Wireless - Advanced' configuration page. At the top, there is a navigation bar with tabs: System, Signal, Status, Log, Provisioning, Setup, and Advanced. The 'Setup' tab is selected. Below the navigation bar, the page title is 'Setup Wireless - Advanced' with a sub-header 'This page allows you to configure your wireless access point data rates and WIFI thresholds.' The main configuration area contains the following settings:

- Network Mode: B/G Mixed
- Basic Rate Set: Default
- CTS Protection Mode: Auto
- Rate: Auto
- Output Power: 100%
- Beacon Interval: 100 ms (1-65535)
- D/TIM Interval: 1 ms (1-255)
- Fragmentation Threshold: 2346 bytes (256-2346)
- RTS Threshold: 2347 (0-2347)
- Short Retry Limit: 7 (1-255)
- Long Retry Limit: 4 (1-255)

At the bottom of the configuration area, there are 'Apply' and 'Back' buttons.

Setup Wireless - Advanced Page Description for 802.11n Radios

This section describes the section headings and fields descriptions of the Setup Wireless - Advanced page for 802.11n radios.

Note: If you make changes in the Setup Wireless - Advanced page, click **Apply** to apply and save your wireless advanced settings.

Field Name	Description
Network Mode	<p>Allows you to optimize the performance of your wireless network using one of the following options:</p> <ul style="list-style-type: none"> ■ Mixed (factory default) Allows the access point to interpolate with 802.11b, 802.11g, and 802.11n wireless client devices and minimizes interference with nearby 802.11b wireless networks. ■ G Only Locks data rates to 802.11g only rates. This will optimize performance for these devices, but will limit the throughput of 802.11n clients and disallow 802.11b clients. ■ B/G Mixed Locks data rates to 802.11b/g rates. This will optimize performance for these devices, but will limit the throughput of 802.11n and 802.11b clients.
Basic Rate Set	Allows you to select the Basic Rate Set. Options are Auto and ALL .
CTS Protection Mode	<p>Allows you to manually control the protection mechanisms used to operate with legacy clients (802.11b).</p> <ul style="list-style-type: none"> ■ Auto (factory default) Allows 802.11b/g/n cells to interoperate seamlessly. ■ Off Will affect the throughput of the cell in the presence of 802.11b clients.
Rate	<p>Allows you to fix the data rate for wireless connections. The following data rates are available:</p> <p>Auto (factory default), 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps, and MCS 0-15 rates which are a function of channel width.</p> <p>The rates available will be based on the Network Mode chosen previously.</p> <p>Note: In the automatic mode, data rate is a function of signal strength and signal quality.</p>

Configuring Wireless Access Point Access Control

Use the Setup Wireless - Access Control page to configure your wireless access point access control.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the residential gateway default wireless advanced settings.

Click **Access Control** in the Wireless section of the Setup page to access the Setup Wireless - Access Control page.

Setup Wireless Access Control Page

The following illustration is an example of the Setup Wireless - Access Control page.

Setup Wireless - Access Control Page Description

This section describes the section headings and field descriptions of the Setup Wireless - Access Control page.

Field Name	Description
Access restriction	<p>When encryption is enabled, this selection allows you to choose one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Disable (factory default)–No access restrictions based on MAC address of wireless access devices. ■ Allow–Allows wireless access to only the MAC addresses listed in the Access List. ■ Deny–Denies wireless access to only the MAC address listed in the Access List.
Closed Network	<p>Allows you to disable or enable the network to prevent access by wireless clients. When ON is selected, the access point does not broadcast the SSID. The client device must be configured manually with the SSID and the MAC address of the access point in order to access with wireless network.</p>
Access List	<p>Displays the MAC address of the clients that are subject to wireless access control.</p>

Field Name	Description
Connected Clients	Displays the Host Name, IP Address, and Client ID of wireless clients that are connected to (associated with) the gateway modem.

Function Keys

The following function keys appear on the Setup Wireless - Access Control page.

Key	Description
Apply	Applies and saves the values you enter into the fields without closing the screen.
Clear All	Clears the Access List.
Remove	Removes entries from the Access List.
Add	Adds a client to the Access List using the MAC address of the client.

Configuring Remote Bridges

Use the Setup Wireless - Bridging page to configure your configure remote bridges.

Note: If you are not familiar with the advanced settings detailed in this section, contact your service provider before you attempt to change any of the wireless home gateway default wireless advanced settings.

Click **Bridging** in the Wireless section of the Setup page to access the Setup Wireless - Bridging page.

Setup Wireless Access Control Page Example

The following illustration is an example of the Setup Wireless - Bridging page.

The screenshot shows the 'Setup Wireless - Bridging' page. At the top, there is a navigation bar with tabs: System, Signal, Status, Log, Provisioning, Setup (highlighted in teal), and Advanced. Below the navigation bar, the page title is 'Setup Wireless - Bridging' and the subtitle is 'This page allows configuration of WDS features.' The main content area contains a 'Wireless Bridging' dropdown menu set to 'Disabled'. Below this, there is a 'Remote Bridges' section with three empty input fields. At the bottom of the form, there is an 'Apply' button.

Chapter 3 Configuring the DOCSIS Residential Gateway

Setup Wireless - Bridging Page Description

The Setup Wireless - Bridging page allows you to Enable or Disable wireless bridging and to add remote bridges. Click **Apply** to apply and save your new settings.

4

Operation of Front Panel Indicators

Introduction

This section describes the behavior of the front panel indicators when the residential gateway is first powered up, during normal operations, and in special conditions.

In This Chapter

- Initial Power Up, Calibration, and Registration (AC Power applied) 102
- Normal Operations (AC Power Applied) 104
- Special Conditions 105

Initial Power Up, Calibration, and Registration (AC Power applied)

The following chart illustrates the sequence of steps and the corresponding appearance of the residential gateway front panel LED status indicators during power up, calibration, and registration on the network when AC power is applied to the residential gateway. Use this chart to troubleshoot the power up, calibration, and registration process of your residential gateway.

Note: After the residential gateway completes Step 7 (Data Network Registration Complete), the residential gateway proceeds immediately to Normal Operations. See *Normal Operations (AC Power applied)* (on page 104).

Front Panel LED Status Indicators During Initial Power Up, Calibration, and Registration							
		Part 1, High Speed Data Registration					
Step:		1	2	3	4	5	6
Front Panel Indicator		Self Test	Downstream Scan	Downstream Signal Lock	Ranging	Requesting IP Address	Request High Speed Data Provisioning File
1	POWER	On	On	On	On	On	On
2	DS	On	Blinking	On	On	On	On
3	US	On	Off	Off	Blinking	On	On
4	ONLINE	On	Off	Off	Off	Off	Blinking
5	LINK	On	On or Blinking	On or Blinking	On or Blinking	On or Blinking	On or Blinking
6	WIRELESS ON/OFF (Optional)	On	On or Blinking	On or Blinking	On or Blinking	On or Blinking	On or Blinking
7	WIRELESS SETUP	Off	On or Blinking	On or Blinking	On or Blinking	On or Blinking	On or Blinking
8	TEL 1	On	Off	Off	Off	Off	Off
9	TEL 2 (Optional)	On	Off	Off	Off	Off	Off

Initial Power Up, Calibration, and Registration (AC Power applied)

Front Panel LED Status Indicators During Initial Power Up, Calibration, and Registration						
		Part 2, Telephone Registration				
Step:		7	8	9	10	11
Front Panel Indicator		Data Network Registration Complete	Requesting Telephone IP Address	Request Telephone Provisioning File	Restarting Voice Service	Telephone Registration Complete
1	POWER	On	On	On	On	On
2	DS	On	On	On	On	On
3	US	On	On	On	On	On
4	ONLINE	On	On	On	On	On
5	LINK	On or Blinking	On or Blinking	On or Blinking	On or Blinking	On or Blinking
6	WIRELESS ON/OFF (Optional)	On or Blinking	On or Blinking	On or Blinking	On or Blinking	On or Blinking
7	WIRELESS SETUP	On or Blinking	Off	On	On or Blinking	On or Blinking
8	TEL 1	Off	Blinking	Off	Blinking	On
9	TEL 2 (Optional)	Off	Off	Blinking	Blinking	On

Normal Operations (AC Power Applied)

The following chart illustrates the appearance of the residential gateway front panel LED status indicators during normal operations when AC power is applied to the gateway.

Front Panel LED Status Indicators During Normal Conditions		
Front Panel Indicator		Normal Operations
1	POWER	On
2	DS	On
3	US	On
4	ONLINE	On
5	LINK	<ul style="list-style-type: none"> ■ On - When a single device is connected to the Ethernet port and no data is being sent to or from the residential gateway ■ Blinks - When an Ethernet device is connected and data is being transferred between the consumer premise equipment (CPE) and the wireless home gateway ■ Off - When no devices are connected to the Ethernet ports
6	WIRELESS ON/OFF	<ul style="list-style-type: none"> ■ On - When the wireless access point is enabled and operational ■ Blinks - When data is being transferred between the CPE and the wireless home gateway ■ Off - When the wireless access point is disabled
7	WIRELESS SETUP	<ul style="list-style-type: none"> ■ Off - When wireless setup is not active ■ Blinks - When wireless setup is active to add new wireless clients on the wireless network
8	TEL 1	<ul style="list-style-type: none"> ■ On - When telephony service is enabled ■ Blinks - When line 1 is in use
9	TEL 2 (Optional)	<ul style="list-style-type: none"> ■ On - When telephony service is enabled ■ Blinks - When line 2 is in use

Note: In addition to the status shown in the previous table, some service providers use color-coded LEDs to indicate detailed channel bonding and data link status. For additional information about color-coded LEDs, check with your service provider.

Special Conditions

The following chart describes the appearance of the residential gateway front panel LED status indicators during special conditions to show when you have been denied network access.

Front Panel LED Status Indicators During Special Conditions		
Front Panel Indicator		Network Access Denied
1	POWER	On
2	DS	Slow Blinking (once per second)
3	US	Slow Blinking (once per second)
4	ONLINE	Off
5	LINK	On
6	WIRELESS On/OFF (Optional)	Off
7	WIRELESS SETUP	Off
8	TEL 1	Off
9	TEL 2 (Optional)	Off

5

Troubleshooting the DOCSIS Residential Gateway

Introduction

This chapter describes the most common issues that may occur after the residential gateway is installed and provides possible solutions and tips for improved performance of the residential gateway.

In This Chapter

- Frequently Asked Questions..... 108
- Common Troubleshooting Issues..... 114
- Tips for Improved Performance 116

Frequently Asked Questions

This section provides answers to common questions about the residential gateway.

How Do I Configure TCP/IP Protocol?

To configure TCP/IP protocol, you need to have an Ethernet Network Interface Card (NIC) with TCP/IP communications protocol installed on your system. TCP/IP is a communications protocol used to access the Internet. This section contains instructions for configuring TCP/IP on your Internet devices to operate with the residential gateway in Microsoft Windows or Macintosh environments.

TCP/IP protocol in a Microsoft Windows environment is different for each operating system. Follow the appropriate instructions in this section for your operating system.

Configuring TCP/IP on Windows 7 Systems

- 1 Open Network Connections by clicking the **Start** button, and then clicking **Control Panel**.
- 2 In the Search box, type **adapter**, and then, under **Network and Sharing Center**, click **View network connections**.
- 3 Right-click the connection that you want to change, and then click **Properties**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation. The Local Area Connection Properties window opens.
- 4 Click the **Networking** tab.
- 5 Under **This connection uses the following items**, click either **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
- 6 To specify IPv4 IP address settings, do one of the following:
 - To get IP settings automatically using DHCP, click **Obtain an IP address automatically**, and then click **OK**.
 - To specify an IP address, click **Use the following IP address**, and then, in the **IP address**, **Subnet mask**, and **Default gateway** boxes, type the IP address settings.
- 7 To specify IPv6 IP address settings, do one of the following:
 - To get IP settings automatically using DHCP, click **Obtain an IPv6 address automatically**, and then click **OK**.
 - To specify an IP address, click **Use the following IPv6 address**, and then, in the **IPv6 address**, **Subnet prefix length**, and the **Default gateway** boxes, type the IP address settings.

- 8 To specify DNS server address settings, do one of the following:
 - To get a DNS server address automatically using DHCP, click **Obtain DNS server address automatically**, and then click **OK**.
 - To specify a DNS server address, click **Use the following DNS server addresses**, and then, in the **Preferred DNS server** and **Alternate DNS server** boxes, type the addresses of the primary and secondary DNS servers.
- 9 To change advanced DNS, WINS, and IP settings, click **Advanced**.
- 10 When you are finished, click **OK**.
- 11 Try to access the Internet. If you cannot access the Internet, contact your service provider for further assistance.

Configuring TCP/IP on Windows XP Systems

- 1 Click **Start**, and depending on your Start menu setup, choose one of the following options:
 - If you are using the Windows XP Default Start Menu, select **Connect to**, choose **Show all connections**, and then go to step 2.
 - If you are using the Windows XP Classic Start Menu, select **Settings**, choose **Network Connections**, click **Local Area Connection**, and then go to step 3.
- 2 Double-click the **Local Area Connection** icon in the LAN or High-Speed Internet section of the Network Connections window.
- 3 Click **Properties** in the Local Area Connection Status window.
- 4 Click **Internet Protocol (TCP/IP)**, and then click **Properties** in the Local Area Connection Properties window.
- 5 Select both **Obtain an IP address automatically** and **Obtain DNS server address automatically** in the Internet Protocol (TCP/IP) Properties window, and then click **OK**.
- 6 Click **Yes** to restart your computer when the Local Network window opens. The computer restarts. The TCP/IP protocol is now configured on your PC, and your Ethernet devices are ready for use.
- 7 Try to access the Internet. If you cannot access the Internet, contact your service provider for further assistance.

Configuring TCP/IP on Macintosh Systems

- 1 Click the **Apple** icon in the upper-left corner of the Finder. Scroll down to **Control Panels**, and then click **TCP/IP**.
- 2 Click **Edit** on the Finder at the top of the screen. Scroll down to the bottom of the menu, and then click **User Mode**.
- 3 Click **Advanced** in the User Mode window, and then click **OK**.
- 4 Click the Up/Down selector arrows located to the right of the Connect Via section of the TCP/IP window, and then click **Using DHCP Server**.
- 5 Click **Options** in the TCP/IP window, and then click **Active** in the TCP/IP Options window.

Note: Make sure that the **Load only when needed option** is *unchecked*.

- 6 Verify that the **Use 802.3** option located in the upper-right corner of the TCP/IP window is unchecked. If there is a check mark in the option, uncheck the option, and then click **Info** in the lower-left corner.
- 7 Is there a Hardware Address listed in this window?
 - If **yes**, click **OK**. To close the TCP/IP Control Panel window, click **File**, and then scroll down to click **Close**. You have completed this procedure.
 - If **no**, you must power off your Macintosh.
- 8 With the power off, simultaneously press and hold down the **Command (Apple)**, **Option**, **P**, and **R** keys on your keyboard. Keeping those keys pressed down, power on your Macintosh but do not release these keys until you hear the Apple chime at least three times, then release the keys and let the computer restart.
- 9 When your computer fully reboots, repeat steps 1 through 7 to verify that all TCP/IP settings are correct. If your computer still does not have a Hardware Address, contact your authorized Apple dealer or Apple technical support center for further assistance.

How Do I Renew the IP Address on My PC?

If your PC cannot access the Internet after the residential gateway is online, it is possible that your PC did not renew its IP address. Follow the appropriate instructions in this section for your operating system to renew the IP address on your PC.

Renewing the IP Address on Windows 7 Systems

- 1 Click the Windows **Start** button.
- 2 Type **cmd** in the Search box. The cmd window opens.
- 3 Type **ipconfig /renew** and press **Enter** to renew the IP address of the computer.

Renewing the IP Address on Windows XP Systems

- 1 Click **Start**, and then click **Run**. The Run window opens.
- 2 Type **cmd** in the Open field and click **OK**. A window with a command prompt opens.
- 3 Type **ipconfig /release** at the C:/ prompt and press **Enter**. The system releases the IP address.
- 4 Type **ipconfig /renew** at the C:/ prompt and press **Enter**. The system displays a new IP address.
- 5 Click the **X** in the upper-right corner of the window to close the Command Prompt window. You have completed this procedure.

Note: If you cannot access the Internet, contact your service provider for further assistance.

Renewing the IP Address on Macintosh Systems

- 1 Close all open programs.
- 2 Open your **Preferences** folder.
- 3 Drag the **tcp/ip preferences** file to the Trash.
- 4 Close all open windows and empty the Trash.
- 5 Restart your computer.
- 6 As your computer starts, simultaneously press and hold down the **Command (Apple)**, **Option**, **P**, and **R** keys on your keyboard. Keeping those keys pressed down, power on your Macintosh but do not release these keys until you hear the Apple chime at least three times; then, release the keys and let the computer restart.
- 7 When your computer fully reboots, click the **Apple** icon in the upper-left corner of the Finder. Scroll down to **Control Panels**, and then click **TCP/IP**.
- 8 Click **Edit** on the Finder at the top of the screen. Scroll down to the bottom of the menu, and then click **User Mode**.
- 9 Click **Advanced** in the User Mode window, and then click **OK**.
- 10 Click the Up/Down selector arrows located to the right of the Connect Via section of the TCP/IP window, and then click **Using DHCP Server**.
- 11 Click **Options** in the TCP/IP window, and then click **Active** in the TCP/IP Options window.

Note: In some cases, the **Load only when needed** option does not appear. If it appears, select the option. A check mark appears in the option.

- 12 Verify that the **Use 802.3** option located in the upper-right corner of the TCP/IP window is not selected. If there is a check mark in the option, select the option to clear the check mark, and then click **Info** in the lower-left corner.

13 Is there a Hardware Address listed in this window?

- If **yes**, click **OK**. To close the TCP/IP Control Panel window, click **File**, and then scroll down to click **Close**.
- If **no**, repeat these instructions from step 6.

14 Reboot your computer.

What if I Don't Subscribe to Cable TV?

If cable TV is available in your area, data service may be made available with or without subscribing to cable TV service. Contact your local service provider for complete information on cable services, including high-speed Internet access.

How Do I Arrange for Installation?

Call your service provider to inquire about professional installation. A professional installation ensures proper cable connection to the residential gateway and to your PC, and it ensures the proper configuration of all hardware and software settings. Contact your service provider for more information about installation.

How Does the Residential Gateway Connect to My Computer?

The residential gateway connects to the 10/100BASE-T Ethernet port on your PC. To use the Ethernet interface, Ethernet cards available from your local PC or office supply retailer, or from your service provider. For best performance over an Ethernet connection, your PC should be equipped with a Gigabit Ethernet card.

After My Residential Gateway Is Connected, How Do I Access the Internet?

Your local service provider becomes your Internet Service Provider (ISP). They offer a wide range of services including e-mail, chat, news, and information services. Your service provider will provide the software you will need.

Can I Watch TV and Surf the Internet at the Same Time?

Absolutely! If you subscribe to cable television service, you can watch TV and use your residential gateway at the same time by connecting your TV and your residential gateway to the cable network using an optional cable signal splitter.

Can I Use my Existing Phone Number with the Residential Gateway?

Telephone numbers are portable in some areas. Contact your telephone service provider for more information about using an existing telephone number.

How Many Telephones Can I Connect?

The RJ-11 telephone-style connectors on the residential gateway can each provide telephone service to multiple telephones, fax machines, and analog modems. The maximum number of telephone devices connected to each RJ-11 port is limited by the total Ringing Load of the telephone devices that are connected. Many telephone devices are marked with a Ringer Equivalent Number (REN). Each telephone port on the residential gateway can support up to a 5 REN load. The sum of the REN load on all of the telephone devices attached to each port must not exceed 5 REN.

Common Troubleshooting Issues

This section describes common problems and offers solutions.

I don't understand the front panel status indicators

See *Operation of Front Panel Indicators* (on page 101), for more detailed information on front panel LED status indicator operation and function.

The Residential Gateway does not register an Ethernet connection

Try one of the following solutions:

- Verify that your computer has an Ethernet card and that the Ethernet driver software is properly installed. If you purchase and install an Ethernet card, follow the installation instructions very carefully.
- Verify the status of the front panel status indicator lights.

The Residential Gateway does not register an Ethernet connection after connecting to a hub

If you are connecting multiple PCs to the residential gateway, you should first connect the residential gateway to the uplink port of the hub using the correct crossover cable. The LINK LED of the hub will illuminate continuously.

The Residential Gateway does not register a cable connection

The residential gateway works with a standard, 75-ohm, RF coaxial cable. If you are using a different cable, your residential gateway will not function properly. Contact your service provider to determine whether you are using the correct cable.

There is no dial tone when I lift the handset

Try the following solutions if you cannot hear a dial tone:

- Your telephone wiring may be connected to the wrong RJ-11 port on the residential gateway. The residential gateway has two telephone ports. Verify that you are connected to the correct telephone port.
- There may be a problem with your telephone set. Use a different telephone set and listen to hear dial tone.
- There may be a problem with your home telephone wiring. Use a telephone and connect directly to the same RJ-11 port on the back of the unit. If the dial tone is working here but does not work at other locations in the home, a professional may need to diagnose and repair a problem with your telephone wiring.
- Verify that the telephone company has removed the previous telephone service from your home telephone wiring.
- Your telephone service may not be enabled from your cable telephony service provider. Contact your cable telephony service provider for more information.

Tips for Improved Performance

If your residential gateway does not perform as expected, the following tips may help. If you need further assistance, contact your service provider.

- Verify that the plug to your residential gateway AC power is properly inserted into an electrical outlet.
- Verify that your residential gateway AC power cord is not plugged into an electrical outlet that is controlled by a wall switch. If a wall switch controls the electrical outlet, make sure the switch is in the **ON** position.
- Verify that the **ONLINE** LED status indicator on the front panel of your residential gateway is illuminated.
- Verify that your cable service is active and that it supports two-way service.
- Verify that all cables are properly connected, and that you are using the correct cables.
- If you are using the Ethernet connection, verify that your TCP/IP is properly installed and configured.
- Verify that you have called your service provider and given them the serial number and MAC address of your residential gateway.
- If you are using a cable signal splitter so that you can connect the residential gateway to other devices, remove the splitter and reconnect the cables so that the residential gateway is connected directly to the cable input. If the residential gateway now functions properly, the cable signal splitter may be defective and may need to be replaced.
- If you are connected to your PC with an Ethernet connection, your PC should be equipped with a Gigabit Ethernet card for best performance.

6

Customer Information

Introduction

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

A

- accessing the Internet • 112
- accessories • 4
- advanced settings • 47

C

- cable service • 112
- connections
 - description of • 7
 - how to connect • 18
 - to computer • 112

D

- default network settings • 35
- DMZ Host settings • 55
- Dynamic DNS settings • 45

E

- Ethernet • 114
- exposure to moisture • vi

F

- features, product • 2
- filters, IP address • 49
- filters, MAC address • 50
- firewall event logging • 73
- Firewall settings • 68
- Fixed CPE IP Assignment settings • 42

I

- indicators
 - behavior • 102, 104, 105
 - described • 6
 - operation of • 101
- installation
 - professional • 112
- installation requirements
 - for telephone service • 10, 12
 - minimum system requirements • 10, 11
 - ventilation • vi

Internet

- how to access • 112
- surfing while watching TV • 112
- unable to access • 110
- IP address filters • 49
- IP address, renewing • 110

L

- LAN IP ad • 36
- LEDs • 6, 102, 104, 105
- location
 - selecting • vi, 13

M

- MAC address filters • 50

N

- Network Configuration settings • 35
- Network Time protocol • 34

O

- overview
 - power switch • 7
 - product • 2
 - WebWizard • 23

P

- Parental Control settings • 75, 78, 81, 82
- password • 32
- performance, tips to improve • 116
- port filtering • 52
- Port Forwarding settings • 53
- product
 - accessories • 4
 - features • 2
 - overview • 2

R

- restarting • 43

S

- safety instructions • v
 - ground product • v
- save configuration to local PC • 43
- save configuration to server • 66
- Setup • 28
- system requirements • 10

T

- TCP port filtering • 51
- TCP/IP
 - configuring for Macintosh systems • 110
 - configuring for Windows XP • 111
- telephone
 - requirements • 10
 - service • 112, 113, 115
- time synchronization • 34
- troubleshooting • 107

U

- UDP port filtering • 51
- unpacking • 4

V

- ventilation requirements • vi
- Voice settings
 - LEDs • 6, 102, 104, 105
- VPN Termination settings • 56
- VPN Tunnel settings • 59

W

- wall mounting
 - instructions • 16
 - slots • 16
- WebWizard
 - logging in • 24
 - overview • 23
 - password • 32
- Wireless Access Control settings • 98
- Wireless Bridging settings • 99
- Wireless Security settings • 86



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

678 277-1120
800 722-2009
www.cisco.com

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

Product and service availability are subject to change without notice.

© 2011 Cisco and/or its affiliates. All rights reserved.

October 2011 Printed in USA

Part Number 4042835 Rev A