



Cisco Model DPC3825 and EPC3825 8x4 DOCSIS 3.0 Wireless Residential Gateway User Guide




In This Document

■ IMPORTANT SAFETY INSTRUCTIONS	2
■ Introduction.....	12
■ What's In the Carton?.....	14
■ Front Panel Description	15
■ Back Panel Description	16
■ What Are the System Requirements for Internet Service?.....	18
■ How Do I Subscribe to High-Speed Internet Service?.....	19
■ Where Is the Best Location for My DOCSIS Residential Gateway?	20
■ How Do I Mount the Modem on a Wall? (Optional).....	21
■ How Do I Connect My Gateway for Internet Service?.....	24
■ How Do I Configure My DOCSIS Residential Gateway?	26
■ Configure Wireless Settings	35
■ Configure Security.....	51
■ Control Access to the Gateway	60
■ Configure Applications and Gaming.....	69
■ Manage the Gateway.....	75
■ Monitor Gateway Status	84
■ Frequently Asked Questions.....	91
■ Tips for Improved Performance	95
■ Front Panel LED Status Indicator Functions.....	96
■ Notices.....	100

IMPORTANT SAFETY INSTRUCTIONS



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>	
	<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> 
<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>	<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>

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>	
	<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 CHOC ÉLECTRIQUES, NE PAS EXPOSER L'APPAREIL À LA PLUIE OU À L'HUMIDITÉ.</p> 
<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>	<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>

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>  <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>	<table border="1"> <tr> <td></td> <td style="text-align: center;"> <p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p> </td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> <p>ACHTUNG STROMSCHLAGEGFAHR, NICHT ÖFFNEN</p> </td> <td></td> </tr> </table> <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>  <p>Dieses Symbol weist den Benutzer darauf hin, dass die mit diesem Produkt gelieferte Dokumentation wichtige Betriebs- und Wartungsanweisungen für das Gerät enthält.</p>		<p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p>			<p>ACHTUNG STROMSCHLAGEGFAHR, NICHT ÖFFNEN</p>	
	<p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p>						
	<p>ACHTUNG STROMSCHLAGEGFAHR, NICHT ÖFFNEN</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>  <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>	<table border="1"> <tr> <td></td> <td style="text-align: center;"> <p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p> </td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> <p>ATENCIÓN RIESGO DE DESCARGA ELÉCTRICA NO ABRIR</p> </td> <td></td> </tr> </table> <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>  <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>		<p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p>			<p>ATENCIÓN RIESGO DE DESCARGA ELÉCTRICA NO ABRIR</p>	
	<p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p>						
	<p>ATENCIÓN RIESGO DE DESCARGA ELÉCTRICA NO ABRIR</p>						

20080814_Installer820_Intl

IMPORTANT SAFETY INSTRUCTIONS

IMPORTANT SAFETY INSTRUCTIONS

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

Power Source Warning

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

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

Ground the Product



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

Protect the Product from Lightning

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

Verify the Power Source from the On/Off Power Light

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

Eliminate AC Mains Overloads



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

Provide Ventilation and Select a Location

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

Protect from Exposure to Moisture and Foreign Objects



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



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



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

Service Warnings



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

IMPORTANT SAFETY INSTRUCTIONS

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.

20090915_Modem No Battery_Safety

United States FCC Compliance

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

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

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

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

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.

DOCSIS Residential Gateway
 Model: DPC3825/EPC3825
 Manufactured by:
 Cisco Systems, Inc.
 5030 Sugarloaf Parkway
 Lawrenceville, Georgia 30044 USA
 Telephone: 770-236-1077

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.

Dynamic Frequency Selection (DFS) Dual Band Frequencies

Some configurations of this product may operate in the 5150-5250MHz and 5470-5725MHz bands. If you select a channel in these frequency ranges, the product is restricted to indoor operation only per FCC guidance. The use of this product on the affected frequencies when outside is in non-compliance of the FCC regulations and guidelines.

Radiation Exposure Statements

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

US

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

Canada

This system has been evaluated for RF exposure for humans in reference to ANSI C 95.1 limits. The evaluation was based on evaluation per RSS-102 Rev 2. The minimum separation distance from the antenna to general bystander is 7.9 inches (20 cm) to maintain compliance.

EU

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

Australia

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

20091016 FCC DSL_Dom and Intl

CE Compliance

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

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

Български [Bulgarian]:	Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/EC.
Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales 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.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-htigiet 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.

IMPORTANT SAFETY INSTRUCTIONS

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

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

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

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



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

Latvia

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

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

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

Antennas

Use only the antenna supplied with the product.

20090312 CE_Gateway

Introduction

Welcome to the exciting world of high-speed Internet service. Your new Cisco® Model DPC3825 DOCSIS® 3.0 or EPC3825 EuroDOCSIS™ Wireless Residential Gateway is a cable modem that meets industry standards for high-speed data connectivity. The DPC3825 and EPC3825 residential gateway delivers data and wired (Ethernet) or wireless gateway capabilities to connect a variety of devices in the home or small office and support high-speed data access, all in one device. With a DPC3825 or EPC3825 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 DPC3825 and EPC3825 residential gateway for high-speed Internet 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.

Benefits and Features

Your new DPC3825 and EPC3825 residential gateway offers the following outstanding benefits and features:

- Compliant with DOCSIS 3.0, 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
- Four 1000/100/10BASE-T Ethernet ports to provide wired connectivity
- 802.11n Wireless Access Point
- Wireless Protected Setup (WPS), including a push button switch to activate WPS for simplified and secure wireless setup
- 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 wireless 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 of the DOCSIS Residential Gateway models (DPC3825 or EPC3825)



One wall-mount style power adapter (models requiring external power supply)

OR



One desktop-style power adapter (models requiring external power supply)



One Ethernet cable (CAT5/RJ-45)



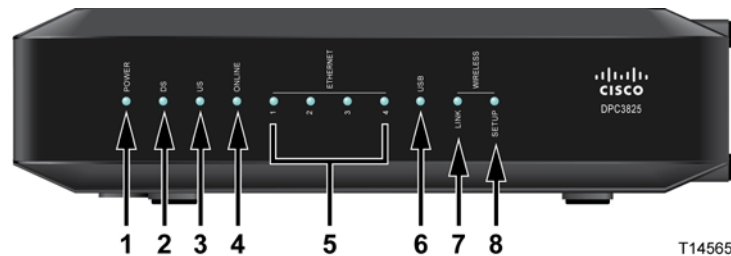
One CD-ROM

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

Note: You will 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 wireless residential gateway.

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 *Front Panel LED Status Indicator Functions* (on page 96), for more information on front panel LED status indicator functions.



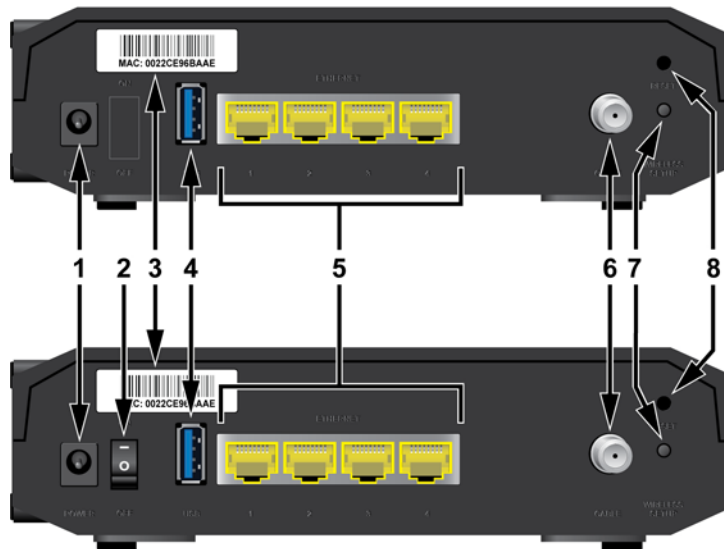
Model DPC3825 shown here

- 1 **POWER**—ON, power is applied to the wireless residential gateway
- 2 **DS**—ON, the wireless residential gateway is receiving data from the cable network
- 3 **US**—On, the wireless residential gateway is sending data to the cable network
- 4 **ONLINE**—ON, the wireless residential gateway is registered on the network and fully operational
- 5 **ETHERNET 1 - 4**—ON, a device is connected to one of the Ethernet ports. BLINKING indicates that data is being transferred over the Ethernet connection
- 6 **USB**—ON, a device is connected to the USB port. BLINKING indicates that data is being transferred over the USB connection
- 7 **WIRELESS 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
- 8 **WIRELESS SETUP**—OFF (normal condition) wireless setup is not active. BLINKING indicates the user has activated wireless setup to add new wireless clients on the wireless network

Back Panel Description

The following illustrations show the description and function of the back panel components on the Cisco DPC3825 residential gateway.

Model DPC3825



Model EPC3825

T14566

- 1 **POWER** – Connects the residential gateway to the AC power adapter that is provided with your residential gateway



CAUTION:

Avoid damage to your equipment. Only use the power supply that is provided with your residential gateway.

- 2 **ON/OFF SWITCH (European models only)** – Allows you to power of the residential gateway without removing the power cord
- 3 **MAC ADDRESS LABEL** – Displays the MAC address of the residential gateway
- 4 **USB** – Connects to selected client devices
- 5 **ETHERNET** – Four RJ-45 Ethernet ports connect to the Ethernet port on your PC or your home network
- 6 **CABLE** – F-connector connects to an active cable signal from your service provider
- 7 **WIRELESS SETUP** – Pressing this switch initiates wireless setup, this feature allows the user to add new Wireless Protected Setup (WPS) compliant wireless clients to the home network

- 8 **RESET** – A momentary pressing (1-2 seconds) of this switch reboots the EMTA. Pressing the switch for more than ten seconds first causes a reset-to-factory-default of all settings and then reboots the gateway



CAUTION:

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

What Are the System Requirements for Internet Service?

To ensure that your residential gateway operates efficiently for high-speed Internet service, verify that all of the Internet devices on your system meet or exceed the following minimum hardware and software requirements.

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

Minimum System Requirements for a PC

- A PC with a Pentium MMX 133 processor or greater
- 32 MB of RAM
- Web browsing software
- CD-ROM drive

Minimum System Requirements for Macintosh

- MAC OS 7.5 or later
- 32 MB of RAM

System Requirements for an Ethernet Connection

- A PC with Microsoft Windows 2000 operating system (or later) with TCP/IP protocol installed, or an Apple Macintosh computer with TCP/IP protocol installed
- An active 10/100/1000BASE-T Ethernet network interface card (NIC) installed

How Do I Subscribe to High-Speed Internet Service?

Before you can use your residential gateway, you need to have a high-speed Internet access account. If you do not have a high-speed Internet access account, you need to set up an account with your local service provider. Choose one of the options in this section.

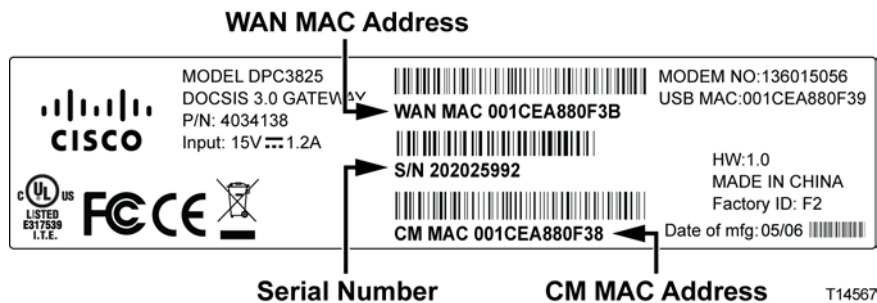
I Do Not Have a High-Speed Internet Access Account

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 the following information:

- The serial number of the modem
- The Media Access Control (MAC) address of the modem (CM MAC)
- Other MAC address numbers as needed

These numbers appear on a bar code label located on the residential gateway. The serial number consists of a series of alphanumeric characters preceded by **S/N**. The MAC address consists of a series of alphanumeric characters preceded by **CM MAC**. The following illustration shows a sample bar code label.



Write down these numbers in the space provided here.

Serial Number _____

MAC Address _____

I Already Have an Existing High-Speed Internet Access Account

If you have an existing high-speed Internet access account, you must give your service provider the serial number and the MAC address of the residential gateway. Refer to the serial number and MAC address information listed previously in this section.

Where Is the Best Location for My DOCSIS 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 modem without straining or crimping them.
- Airflow around the residential gateway should not be restricted.
- Read this user guide thoroughly before installing the residential gateway.

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

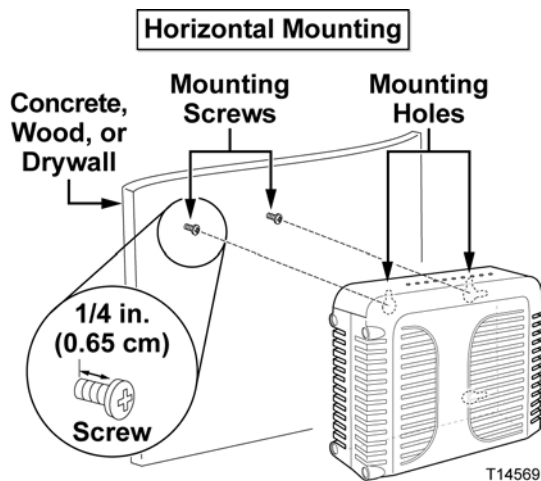
You can mount the residential gateway on a wall using two wall anchors, two screws, and the mounting slots located on the unit. The modem can be mounted vertically or horizontally.

Before You Begin

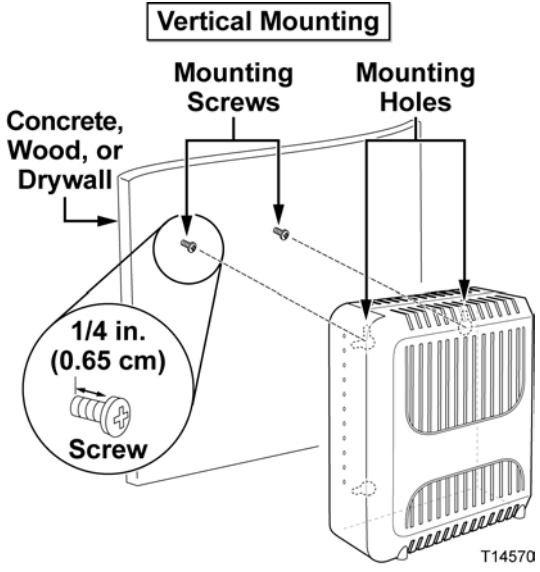
Before you begin, choose an appropriate mounting place. The wall can be made of cement, wood, or drywall. The mounting location should be free of obstructions on all sides, and the cables should be able to easily reach the residential gateway without strain. Leave sufficient clearance between the bottom of the residential gateway and any flooring or shelving underneath to allow access to cabling. In addition, leave enough slack in all cables so that the residential gateway can be removed for any required maintenance without disconnecting the cables. Also, verify that you have the following items:

- 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

Mount the modem as shown in one of the following illustrations.

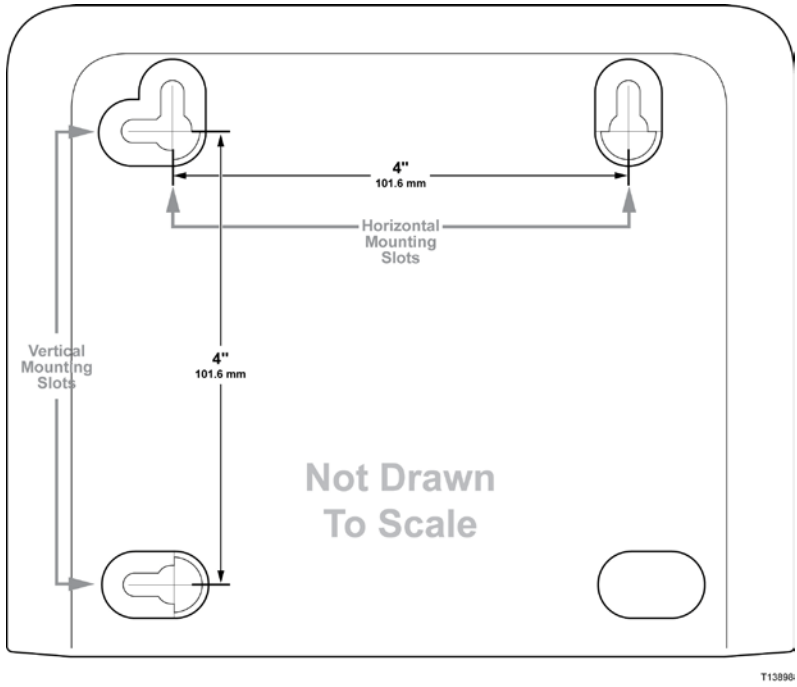


How Do I Mount the Modem on a Wall? (Optional)



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 modem. Use the information on this page as a guide for mounting your modem to the wall.



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.
- 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.

How Do I Connect My Gateway for Internet Service?

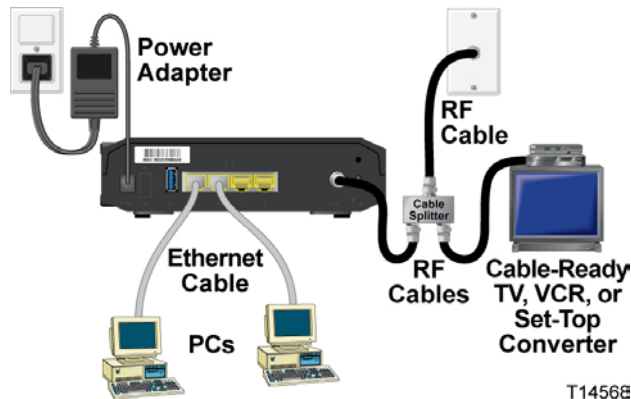
You can use your residential gateway to provide Internet access, and you can share that Internet connection with other Internet devices in your home or office. Sharing one connection among many devices is called networking.

Connecting and Installing Internet Devices

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

To connect devices

The following diagram illustrates one of the various networking options that are available to you.



Connecting the Residential Gateway for High-Speed Data Service

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).



WARNING:

- To avoid personal injury, follow the installation instructions in the exact order shown.
- Wiring and connections must be properly insulated to prevent electrical shock.
- Disconnect power from the residential gateway before attempting to connect to any device.

- 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:** Locate the yellow Ethernet cable, connect one end of the 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 Ethernet devices than ports provided on the residential gateway, use an external multi-port Ethernet switch(s).

- **Wireless:** Make sure that your wireless device is powered up. You will need to associate your wireless device with the wireless gateway once the gateway is operational. Follow the directions provided with your wireless device for associating with a wireless access point.

More information about the factory default configuration of your wireless gateway can be found later in this user guide in *Configure Wireless Settings* (on page 35).

- 5 Locate the AC power cord provided with your residential gateway. Insert one end of the power cord into the AC connector on the back of the residential gateway. Then, plug the AC power cord into an AC outlet 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 modem 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.
- 6 Plug in and power on your PC and other home network devices. The **LINK** LED on the residential gateway corresponding to the connected devices should be on or blinking.
- 7 Once the residential gateway is online, most Internet devices will have immediate Internet access.

Note: If your PC does not have Internet access, refer to *Frequently Asked Questions* (on page 91) 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.

How Do I Configure My DOCSIS Residential Gateway?

To configure your residential gateway, you must first access the WebWizard configuration pages. This section provides detailed instructions and procedures for accessing the WebWizard pages and for configuring your residential gateway to operate correctly. This section also presents examples and descriptions of each WebWizard configuration page. Use the WebWizard pages to customize your residential gateway to your needs rather than using the default settings. The WebWizard pages in this section are organized in the order shown on the **Setup** page.

Important: The WebWizard pages and the examples shown in this section are for illustration purposes only. Your pages may differ from the pages shown in this guide. The pages shown in this guide also represent the default values for the device.

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

Logging in to the Gateway for the First Time

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

- 1 On your PC, open the web browser that you prefer to use.

- In the address field, enter the following IP address: **192.168.0.1**. A Status DOCSIS WAN login page similar to the following page opens.

Log In

User Name:

Password:

Log In

About

Model: Cisco EPC3825
 Vendor: Cisco
 Hardware Revision: 1.0
 Serial Number: 222596078
 MAC Address:: 00:22:3a:ce:d8:75
 Bootloader Revision: 2.3.0_R1
 Current Software Revision: epc3825-ESIP-16-v302r12911-091029c
 Firmware Name: epc3825-ESIP-16-v302r12911-091029c.bin
 Firmware Build Time: Oct 29 2009 15:48:04
 Cable Modem Status: Operational

Downstream Channels

	Power Level	Signal to Noise Ratio
Channel 1:	-17.1 dBmV	33.9 dBmV
Channel 2:	0.0 dBmV	0.0 dBmV
Channel 3:	0.0 dBmV	0.0 dBmV
Channel 4:	0.0 dBmV	0.0 dBmV
Channel 5:	0.0 dBmV	0.0 dBmV
Channel 6:	0.0 dBmV	0.0 dBmV
Channel 7:	0.0 dBmV	0.0 dBmV
Channel 8:	0.0 dBmV	0.0 dBmV

Upstream Channels

	Power Level
Channel 1:	41.0 dBmV
Channel 2:	0.0 dBmV
Channel 3:	0.0 dBmV
Channel 4:	0.0 dBmV

- On the Status DOCSIS WAN page, leave the User Name and Password field blank and click **Log In**. The gateway opens with an Administration Management page in the forefront. You can use the Administration Management page to set your User Name and Password.

Important: We highly recommend that you set up a new password to safeguard against the possibility of Internet attacks that look for devices operating with well-known or factory default user names and/or passwords.

How Do I Configure My DOCSIS Residential Gateway?

The screenshot shows the Administration Management page with the following settings:

- Gateway Setup (WAN):** Connection Mode: DHCP, MTU size: 0.
- Gateway Access:**
 - Local Access:** Current User Name, Change Current User Name to, Change Password to, Re-Enter New Password. A security warning is present: "SECURITY WARNING - The password is currently set to the factory default password. As a security measure, it is highly recommended that you change the password."
 - Remote Access:** Remote Management: Disable, Management Port: 8080.
- UPnP:** UPnP: Disable.
- IGMP:** IGMP Proxy: Enable.

Buttons at the bottom: Save Settings, Cancel Changes.

- 4 On the Administration Management page, create a User Name and Password and then click **Save Settings**. Once you save the settings for your User Name and Password on the Administration Management page, the Setup Quick Setup page opens.

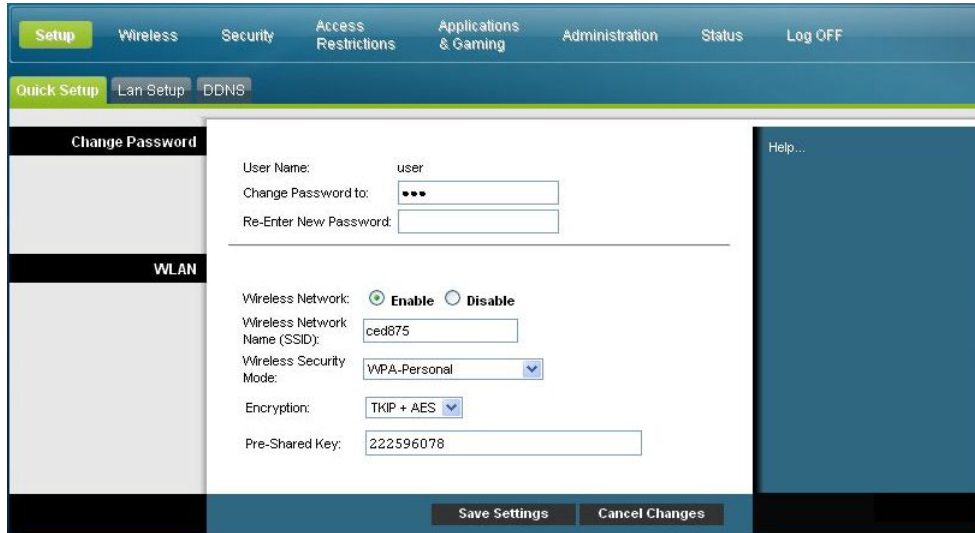
Important: You have the option to leave the password field blank (factory default). However, if you do not change your User Name and Password, you will be directed to the Administrative Management page each time you access the gateway. This serves as a reminder to set up your personalized password. Once you have personalized your Password, subsequent logins will take you directly to the Setup Quick Setup page.

- 5 After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Setup > Quick Setup

The Setup Quick Setup page is the first page to open after you have logged on to your gateway. You can use the settings on this page to change your password and to configure the WLAN.

Important: The settings on this page are unique to your device. If you choose, you do not need to make any changes to the settings on this page. These default settings are all that you need to operate a secure wireless network.



Configuring Quick Settings

Use the descriptions and instructions in the following table to configure the network settings for the device. After you make your selections, click **Save Settings** to apply your changes or click **Cancel Changes** to cancel.

Section	Field Description
Change Password	User Name
	Displays the user name for the operator currently logged in
	Change Password to
	Allows you to change your password
	Re-Enter New Password
	Allows you to re-enter the new password. You must enter the same password as the one entered in the field Change Password to

Section	Field Description
WLAN	<p>Wireless Network</p> <p>Allows you to enable or disable the wireless network. Select the desired option:</p> <ul style="list-style-type: none">■ Enable■ Disable <p>Wireless Network Name (SSID)</p> <p>Allows you to enter a name for your wireless network or to use the default value. The value you enter he will be viewable on PCs and other wireless client devices such as the wireless network name.</p> <p>Note: The factory default Service Set Identifier (SSID) is either the last 6 characters of the CM MAC Address or the SSID as identified on the product label.</p> <p>Some service providers supply a special wireless configuration card that provides the SSID information and wireless security information.</p> <p>Wireless Security Mode</p> <p>Allows you to select a wireless security mode to help protect your network. If you select Disable then your wireless network is not secure and any wireless device within range may connect to it. See <i>Wireless Security</i> (on page 39) for detailed descriptions of wireless security modes.</p> <p>Note: The factory default Wireless Security Mode is WPA or WPA2-Personal.</p> <p>Encryption</p> <p>Allows you to select a level of encryption based on the wireless security mode you choose. See <i>Wireless Security</i> (on page 39) for detailed descriptions of encryption.</p> <p>Pre-Shared Key</p> <p>The pre-shared key for the device. The key can be from 8 to 63 characters. The factory default Pre-Shared Key is equal to the 9-digit serial number of your gateway. The serial number can be found on the rating label attached to your wireless gateway.</p> <p>Note: Your service provider may provide you with a wireless configuration card that contains SSID and wireless security configuration information for your home network that may differ from what is described above.</p>

Setup > Lan Setup

The Setup Lan Setup page allows you to configure the settings for the Local Area Network (LAN) in your home. These settings include the range of IP addresses that define the LAN itself as well as how the addresses are assigned (automatically by DHCP or manually) as new devices are added to the network.

Important: Unless you are knowledgeable about administering IP addresses, we recommend that you do not change these settings. If you change these values incorrectly, you can lose Internet access.

Select the **Lan Setup** tab to open the Setup Lan Setup page.

The screenshot shows the 'Lan Setup' configuration page. At the top, there are navigation tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, Status, and Log OFF. Below these are sub-tabs: Quick Setup, Lan Setup (selected), and DDNS. The main content area is titled 'Network Setup (LAN)' and is divided into three sections: Gateway IP, Network Address Server Settings (DHCP), and Time Settings. In the Gateway IP section, the Local IP Address is set to 192.168.0.1 and the Subnet Mask is 255.255.255.0. A warning message states: 'Warning: Changes to LAN IP network settings may require reconfiguration of all attached devices. Some network devices may be out of service until the change is detected.' In the DHCP Server section, the DHCP Server is set to 'Enable'. There are buttons for 'Connected Devices Summary' and 'Pre-assigned DHCP IP Addresses'. The Starting IP Address is 192.168.0.10, Maximum Number of DHCP Users is 2, and Client Lease Time is 60 minutes. There are three fields for LAN 1 Static DNS, all set to 0.0.0.0. In the Time Settings section, the Time Zone is '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London' and the 'Automatically adjust clock for daylight saving time' checkbox is unchecked. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons.

Configuring Your Network Settings

Use the descriptions and instructions in the following table to configure the network settings for your residential gateway. After you make your selections, click **Save Settings** to apply your changes or click **Cancel Changes** to cancel.

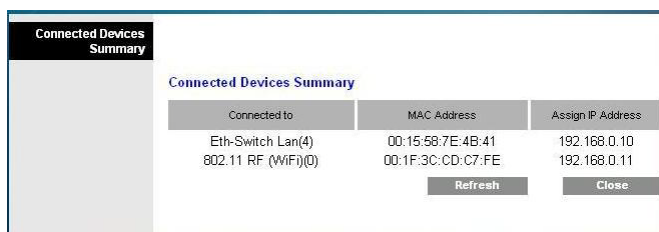
Section	Field Description
Network Setup (LAN)	Local IP Address
Gateway IP	The base IP address of the private home LAN. The factory default LAN IP Address is 192.168.0.1.
	Subnet Mask
	The subnet mask for your LAN

Section	Field Description
Network Address Server Settings (DHCP)	DHCP Server

Allows you to enable or disable the DHCP server in the residential gateway. The DHCP server is used to automatically allocate IP addresses to devices as they are attached to your home network.

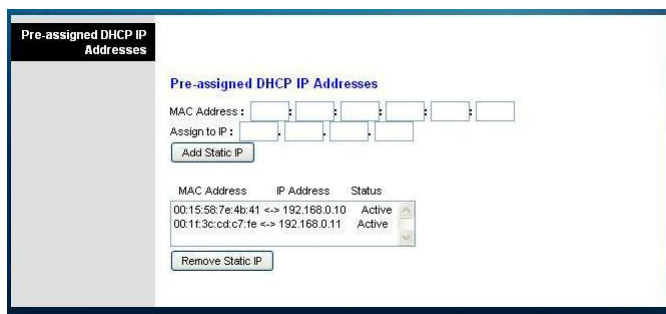
■ **Connected Devices Summary page**

Click **Connected Devices Summary** in the Lan Setup page. The Connected Devices Summary page opens. This page is a pop-up window that displays the MAC Address and IP Address of the devices that are connected to the residential gateway.



■ **Pre-assigned DHCP IP Addresses page**

Click **Pre-assigned DHCP IP Addresses** in the Lan Setup page. The Pre-assigned DHCP IP Addresses page opens. This page allows you to assign a specific IP address to a PC or other device when they request an IP address using DHCP. Only addresses within the range of the gateway's DHCP address pool can be reserved with this feature.



Notes:

- The **Add Static IP** button adds the Static IP address to the list of pre-assigned IP addresses.
- The **Remove Static IP** button removes the Static IP address from the list of pre-assigned IP addresses

Starting IP Address

Displays the starting address used by the built-in DHCP server to distribute Private LAN IP addresses. Because the device default IP address of the gateway is **192.168.0.1**, the starting IP address must be **192.168.0.2** or greater, but smaller than **192.168.0.253**. The default Starting IP Address is **192.168.0.10**.

Section	Field Description
	<p data-bbox="613 268 1036 296">Maximum Number of DHCP Users</p> <p data-bbox="613 317 1383 443">Enter the maximum number of users to which the DHCP server can assign IP addresses for use in the LAN. This number cannot be greater than 254 minus the starting IP address described above.</p> <p data-bbox="613 464 829 491">Client Lease Time</p> <p data-bbox="613 512 1383 737">The Client Lease Time is the amount of time an IP address is valid. IP address leases are renewed automatically by your PC and other devices that use DHCP to obtain IP addresses. If a lease is allowed to expire, the IP address will be returned to the pool of available IP addresses that can be assigned by the DHCP server as new devices are added to your network. The default is 60 minutes when the gateway is online.</p> <p data-bbox="613 758 1138 785">LAN Static DNS (Domain Name Server) 1-3</p> <p data-bbox="613 806 1383 1031">DNS is used by a PC or other client devices to discover the public IP address associated with a URL or the name-based address of a website. You can manually specify which DNS servers are to be used by devices in your network by entered the IP addresses of those servers in these fields. Otherwise, the gateway will forward the DNCS server information from your service provider automatically. The default is to leave these fields blank.</p>
Time Settings	<p data-bbox="613 1052 743 1079">Time Zone</p> <p data-bbox="613 1100 1383 1199">Select the time zone for your location. If your location follows daylight saving time, select Automatically adjust clock for daylight saving time.</p>

Setup > DDNS

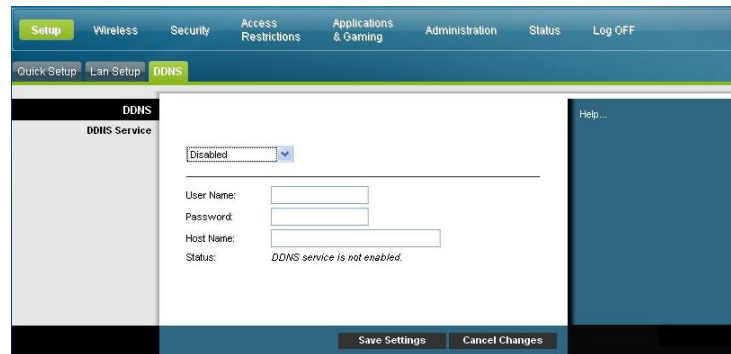
Dynamic Domain Name Service (DDNS) provides the residential gateway (that may have a changing IP address) with a host name or URL resolvable by network applications through standard DNS queries. DDNS is useful when you are hosting your own website, FTP server, or other server behind the device. Before using this feature, you need to sign up for DDNS service.

Select the **DDNS** tab to open the Setup DDNS page.

Section	Field Description
---------	-------------------

DDNS Service	Disabling DDNS (Factory Default Settings)
--------------	--

To disable DDNS, select **Disabled** from the drop-down list and click **Save Settings**.



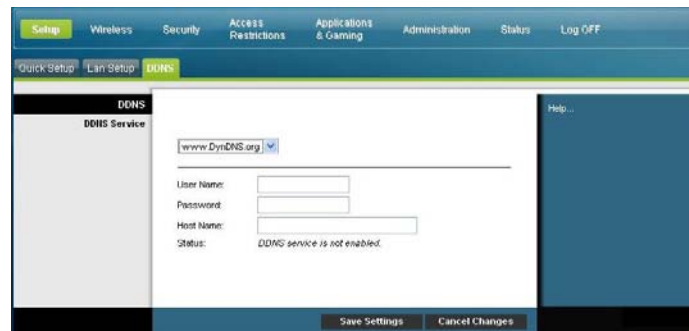
Enabling DDNS

Note: In order to use the DDNS feature, you must first set up an account and establish a URL with www.DynDNS.org. The DDNS feature will not work without a valid account.

To set up a DDNS account, open your browser and enter www.DynDNS.org in the address bar. Follow the instructions on the website to set up an account.

To enable DDNS, follow these steps.

- 1 On the DDNS page, select **www.DynDNS.org** as your DDNS server.



- 2 Configure the following fields:

- User Name
- Password
- Host Name

- 3 Click **Save Settings**. The device will now advise the DDNS service of your current WAN (Internet) IP address whenever this address changes.

Important: The Status area of the window will display the status of the DDNS service connection.

Configure Wireless Settings

This section describes the options available from the Wireless pages that you can use to configure the parameters of the WAP to meet your specific requirements and needs.

Wireless > Basic Settings

Setting up your residential gateway for wireless communication provides you with the freedom to connect to the Internet from any location within range of the WAP without having to use wired connections. Select the **Basic Settings** tab to open the Wireless Basic Settings page.

The Wireless Basic Settings page allows you to choose your wireless network mode and other basic features.

- Wireless Network: Enable or Disable
- Wireless Configuration: Manual or Wi-Fi Protected Setup
- Network Mode
- Radio Band
- Channel Width
- Standard Channel
- Wireless Network Name (SSID)

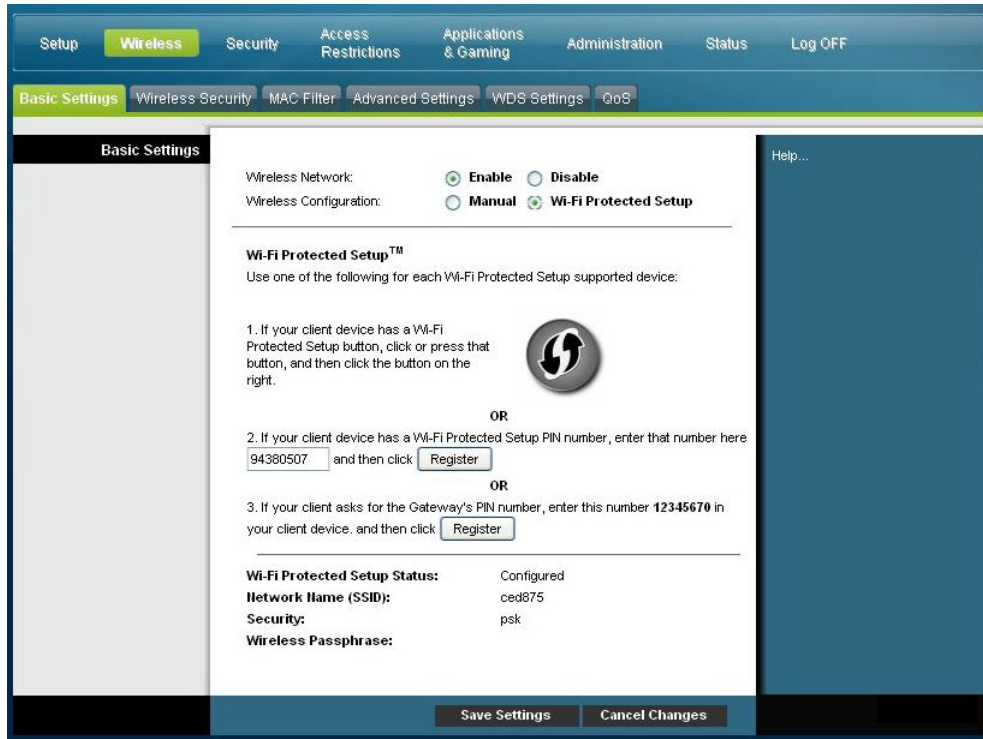
Wi-Fi Protected Setup (WPS)

When you select Wi-Fi Protected Setup as your wireless configuration, many settings will be pre-configured. WPS allows simplified setup that allows you to easily attach new WPA-enabled devices to your network.

Important: When using WPS mode, WEP is not supported. If you must use WEP encryption, WPS must be disabled by setting the Wireless Configuration to **Manual**.

Note: WPS is the default setting.

Wireless Configuration Wi-Fi Protected Setup Example



Wireless Configuration Wi-Fi Protected Setup Page Description

Use the descriptions and instructions in the following table to configure the basic settings for Wi-Fi Protected Setup for the residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
Basic Settings	<p>Enable or Disable the wireless network</p> <p>Wi-Fi Protected Setup Configuration</p> <p>The Wi-Fi Protected Setup feature automatically configures an encryption-secured, wireless network. To use Wi-Fi Protected Setup, you must have at least one other device that supports Wi-Fi Protected Setup in your network. After you have configured your Wi-Fi Protected Setup devices, you can manually configure other devices.</p> <p>WPS Push Button Setup (Option 1)</p> <p>Press the Wi-Fi Protected Setup button on the Basic Wireless Settings page or the button on the back panel of the gateway to register a wireless client with the gateway. Press the Wi-Fi Protected Setup software button on the client side at the same time as the Wi-Fi Protected Setup button is pushed on the gateway. The connection will be automatically set up.</p>

Section	Field Description
---------	-------------------

WPS Setup Using Your Wi-Fi Adapter PIN (Option 2)

This is the most secure option to register a wireless client with the gateway. You need the Wi-Fi Protected Setup PIN number, which is found in the client Wi-Fi Protected Setup utility. After entering the client's Wi-Fi Protected Setup PIN number, you can then connect to the gateway.

WPS Setup Using the Gateway PIN (Option 3)

Note the gateway's Wi-Fi Protected Setup PIN number that is displayed on the Wi-Fi Protect Setup page. Click the Register button in Option 3, then using any Wi-Fi Protected Setup client utility or Microsoft Vista, enter the gateway's Wi-Fi Protected Setup PIN number into the client device to complete registration.

Wireless Configuration Manual Page Example

The screenshot shows the 'Basic Settings' page for wireless configuration. At the top, there are navigation tabs: Setup, **Wireless**, Security, Access Restrictions, Applications & Gaming, Administration, Status, and Log OFF. Below these are sub-tabs: Basic Settings, Wireless Security, MAC Filter, Advanced Settings, WDS Settings, and QoS. The 'Basic Settings' sub-tab is active.

Options for Wireless Network: Enable Disable
 Options for Wireless Configuration: Manual Wi-Fi Protected Setup

Network Mode: B/G/N Mixed
 Radio Band: Enabled 2.4GHz
 Channel Width: Standard - 20 MHz Channel
 Standard Channel: Auto

Wireless Network Name (SSID)	BSSID	Broadcast SSID	Enable
ced875	00:22:CE:7B:D9:EC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons: Save Settings, Cancel Changes

Wireless Basic Settings Page Description

Use the following table to configure the basic settings for wireless communication for the residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Configure Wireless Settings

Section	Field Description
Basic Settings	<p>Wireless Network</p> <p>Enable or Disable the wireless network</p> <p>Wireless Configuration</p> <p>The default is WPS. See <i>Wi-Fi Protected Setup (WPS)</i> (on page 35) for more information about using WPS.</p> <p>Select Manual to manually set up your network using this option.</p> <hr/> <p>Network Mode</p> <p>Choose one of these options for the network mode:</p> <p>G only, B/G Mixed, B/G/N Mixed (factory default)</p> <p>Important: When TKIP authentication only is selected, B/G/N Mixed network mode is not available.</p> <p>Radio Band</p> <p>Select Enabled 2.4GHz (factory default) or Enabled 5GHz</p> <p>Note: The 5GHz radio band may not be supported on some models.</p> <p>Channel Width</p> <p>Choose Standard - 20 MHz Channel or Wide 40 MHz Channel</p> <p>Standard Channel</p> <p>Select one of the channels from the drop-down list to correspond with your network settings. All devices in your wireless network must broadcast on the same channel in order to communicate. You can select Auto (factory default) for automatic channel selection.</p> <hr/>

Section	Field Description
	<p data-bbox="483 268 870 296">Wireless Network Name (SSID)</p> <p data-bbox="483 317 1427 478">The SSID is the name of your wireless network. The SSID is used by wireless technology to identify your network from other wireless networks in the area. The SSID can be up to 32 characters long. The factory default SSID is typically the last 6 characters of the CM MAC address found on the rating label located on the bottom of your gateway.</p> <p data-bbox="483 499 1427 590">This SSID is a unique identity and does not need to be changed unless you choose to do so. Your service provider may provide you with wireless setup information that may call for a different SSID.</p> <p data-bbox="483 611 565 638">BSSID</p> <p data-bbox="483 659 1427 720">Displays the Basic Service Set Identifier (BSSID) of your wireless network. The BSSID is typically the MAC Address of the wireless access point.</p> <p data-bbox="483 741 1427 802">Note: This may not be the same MAC Address as the CM MAC Address used to determine the factory default SSID.</p> <p data-bbox="483 823 672 850">Broadcast SSID</p> <p data-bbox="483 871 1427 961">When this box is checked (factory default), the gateway transmits or advertises its presence to other wireless devices. Client devices can automatically detect the access point when this beacon is enabled.</p> <p data-bbox="483 982 1427 1073">Uncheck this box if you want to hide your network from wireless clients. If you hide your network, you will need to configure each of your wireless client devices manually.</p> <p data-bbox="483 1094 1427 1155">Important: The Enable check box is not currently in use and does not impact operation of the gateway.</p>

Wireless > Wireless Security

Selecting a wireless security mode helps protect your network. If you select **Disable**, then your wireless network is not secure and any wireless device within range may connect to it.

To keep intruders out of your wireless network, use the Wireless Security page to configure your security parameters including the security mode (the level of encryption), encryption keys, and other security settings.

Select the **Wireless Security** tab to open the Wireless Security page. The following table shows examples of the Wireless Security page with various wireless security modes selected.

Configure Wireless Settings

Wireless Security Page Description

Use the following table to configure the wireless security for the residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

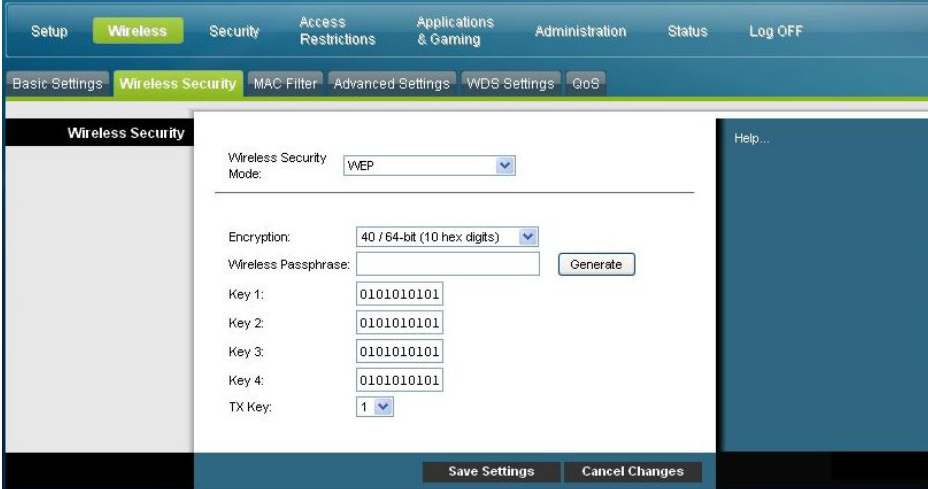
Section	Field Description
---------	-------------------

Wireless Security	Wireless Security Mode
--------------------------	-------------------------------

Choose one of these options for the security mode:

WEP

Wired Equivalent Privacy (WEP) security mode is defined in the original IEEE 802.11 standard. This mode is no longer recommended because of its weak security protection. Users are urged to migrate to either WPA-Personal or WPA2-Personal.



Field Descriptions

- **Encryption.** Select a level of WEP encryption, 40 / 64 bits (10 hex digits) or 104 / 128 bits (26 hex digits).
- **Wireless Passphrase.** To complete your wireless security setup, you should choose a wireless passphrase that is easy for you to remember and hard for anyone else to guess. The first time you connect a new wireless device to this network you may need to enter this passphrase into the appropriate setup section in the connected device. To improve your network security, do not give out this passphrase to unauthorized users. Please enter a phrase of letters and/or numbers from 4 to 24 digits long. Then, click **Generate** to create the Passphrase.
- **Key 1-4.** If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters A through F and the numbers 0 through 9. It should be 10 characters in length for 40/64-bit encryption or 26 characters in length for 104/128-bit encryption.
- **TX Key.** Choose a Transmit (TX) Key from 1 to 4. The TX key is the key that will be used to encrypt your data. Although four keys can be created, only one key is used for encrypting data. Select one of the four keys for WEP encryption. Use the selected TX key to set up your wireless clients.

Section	Field Description
---------	-------------------

WPA

Security for Personal Networks – WPA or WPA2 Personal Modes

Wi-Fi Protected Access (WPA) is a more secure wireless technology than WEP. WPA can be used for both Enterprise (corporate applications) and Personal (home network) wireless networks. We strongly recommend that you select either WPA-Personal or WPA2-Personal as the security mode for your home network, depending on which mode is supported by the wireless adapter in your PC or wireless clients.

WPA-Personal (aka WPA-PSK or WPA-Pre-Shared Key), provides a more secure wireless network than WEP. WPA-Personal introduces TKIP user authentication and stronger encryption keys than WEP.

WPA2-Personal (aka WPA2-PSK or WPA2-Pre-Shared Key) provides the most secure standards-based wireless networking. WPA2-Personal incorporates AES (Advanced Encryption Standard) for data transmission.

Note: Not all wireless adapters support WPA2. WPA is supported across a wider range of devices. Whether you use WPA or WPA2, make sure to use a “strong” passphrase. A strong passphrase is a string of random characters at least 21 characters in length.

Select from one of the following three WPA or WPA2 Personal modes:

- **WPA-Personal**
- **WPA2-Personal**
- **WPA or WPA2-Personal**

The screenshot shows a web interface for configuring wireless settings. The top navigation bar includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', 'Status', and 'Log OFF'. Below this, there are tabs for 'Basic Settings', 'Wireless Security', 'MAC Filter', 'Advanced Settings', 'WDS Settings', and 'QoS'. The 'Wireless Security' tab is active, showing a 'Wireless Security' section with the following fields:

- Wireless Security Mode: WPA-Personal (dropdown menu)
- Encryption: AES (dropdown menu)
- Pre-Shared Key: 222596078 (text input field)
- Key Renewal: 3600 seconds (text input field)

At the bottom of the form, there are two buttons: 'Save Settings' and 'Cancel Changes'.

Field Descriptions

- **Encryption.** The default is TKIP+AES.
- **Pre-Shared Key.** Enter a key of 8 to 63 characters.
- **Key Renewal.** Enter a Key Renewal period, which instructs the device how often it should change encryption keys. The default is 3600 seconds.

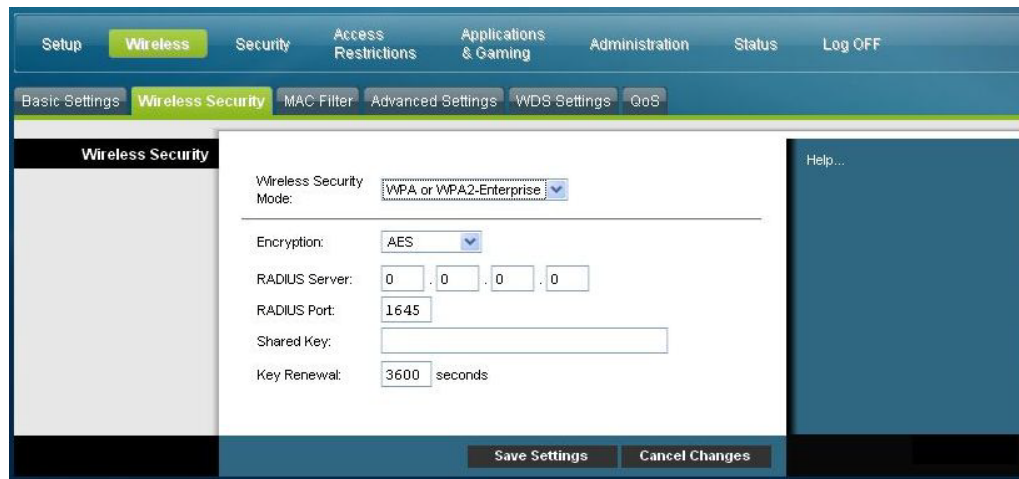
Section Field Description

Security for Enterprise Networks - WPA-Enterprise Modes

This option features WPA used in coordination with a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the device.)

Select from one of the following three WPA or WPA2 Enterprise modes:

- **WPA-Enterprise**
- **WPA2-Enterprise**
- **WPA or WPA2-Enterprise**



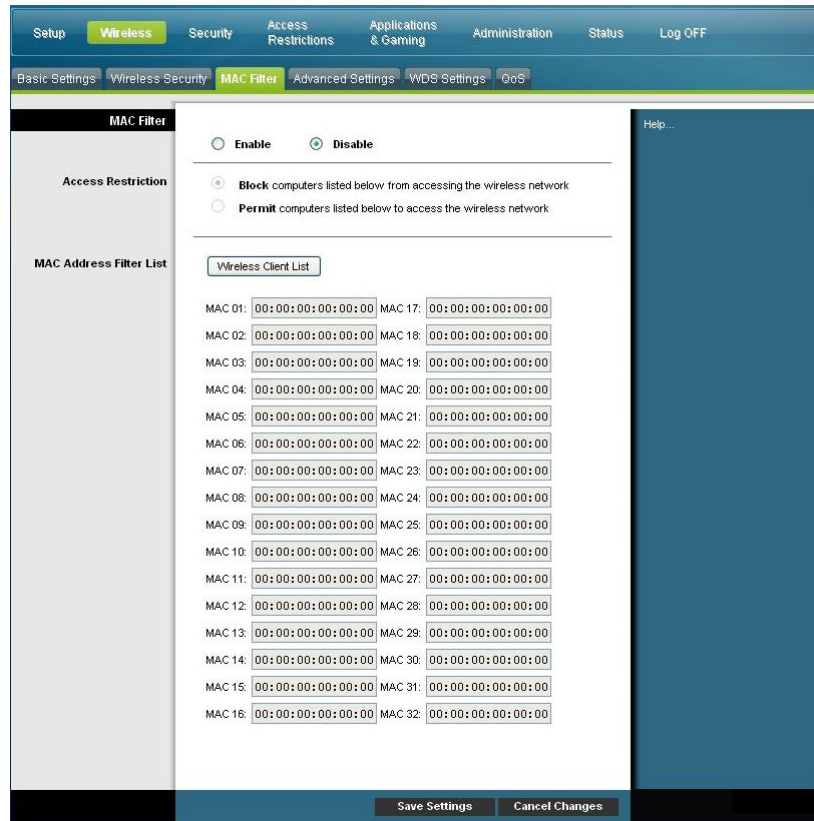
Field Descriptions

- **Encryption.** The default is TKIP+AES.
 - **RADIUS Server.** Enter the RADIUS server's IP address.
 - **RADIUS Port.** Enter the port number used by the RADIUS server. The default is **1812**.
 - **Shared Key.** Enter the key used by the device and RADIUS server.
 - **Key Renewal.** Enter a Key Renewal period, which instructs the device how often it should change encryption keys. The default is **3600** seconds.
-

Wireless > MAC Filter

The MAC Filter feature is used to either allow or block access to your wireless LAN based on the MAC Address of the wireless client devices. The MAC Filter feature, also known as an access list, can be used to help protect your wireless network from access by unauthorized users.

Select the **MAC Filter** tab to open the Wireless MAC Filter page.



Wireless MAC Filter Page Description

Use the descriptions and instructions in the following table to configure the MAC address filtering for the wireless network for your residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
MAC Filter	Allows you to Enable or Disable MAC Filtering for the residential gateway

Section	Field Description
Access Restriction	<p>Access Restriction</p> <p>Allows you to permit or block computers from accessing the wireless network. The choice that you make here affects the addresses listed on this page. Choose one of the following options:</p> <ul style="list-style-type: none"> ■ Block computers listed below from accessing the wireless network. Select this option 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. ■ Permit computers listed below access to the wireless network. Select this option to allow Internet access only to the MAC addresses of the devices you list in the table. Any MAC addresses not listed in the table will be denied Internet access
MAC Address Filter List	<p>MAC Address Filter List</p> <p>The MAC Address Filter List displays users whose wireless access you want to control. Click Wireless Client List to display a list of network users by MAC address. From the To Sort by drop-down menu, you can sort the table by IP Address, MAC Address, Status, Interface, or Client Name. To view the most up-to-date information, click the Refresh button.</p>

Wireless > Advanced Settings

Your advanced wireless settings add another layer of security to the wireless network for your residential gateway. This page is used to set up the advanced wireless functions. Only an expert administrator should adjust these settings. Incorrect settings can reduce wireless performance.

Select the **Advanced Settings** tab to open the Wireless Advanced Settings page.

Use this page to configure the following options:

- N Transmission Rate
- CTS Protection Mode
- Beacon Interval
- DTM Interval
- Fragmentation Threshold
- RTS Threshold



Wireless Advanced Settings Page Description

Use the descriptions and instructions in the following table to configure the advanced wireless settings for your residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

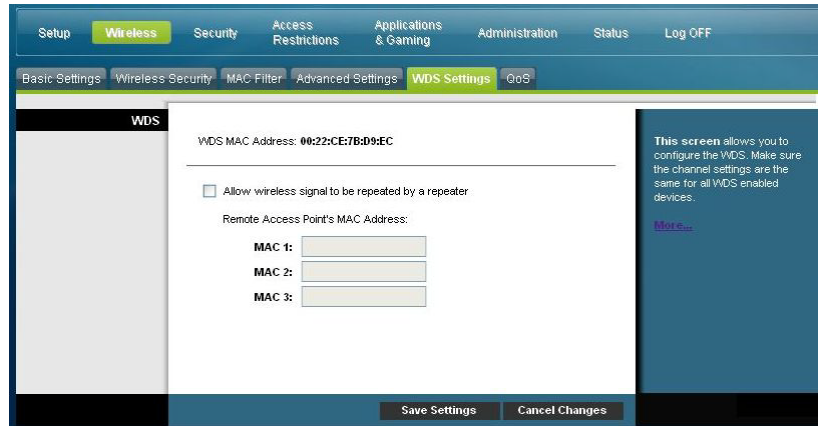
Section	Field Description
Advanced Wireless	<p data-bbox="446 321 706 350">N Transmission Rate</p> <p data-bbox="446 373 1421 533">The rate of data transmission should be set depending on the speed of your Wireless-N networking. Select from a range of transmission speeds, or select Auto to have the device automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback negotiates the best possible connection speed between the device and a wireless client. The factory default setting is Auto.</p> <p data-bbox="446 552 1128 581">Choose one of the following options for transmission rate:</p> <ul data-bbox="446 604 755 1476" style="list-style-type: none"> <li data-bbox="446 604 755 634">■ Auto (factory default) <li data-bbox="446 653 690 682">■ Use Legacy Rate <li data-bbox="446 701 714 730">■ 0: 6.5 or 13.5 Mbps <li data-bbox="446 749 690 779">■ 1: 13 or 27 Mbps <li data-bbox="446 798 730 827">■ 2: 19.5 or 40.5 Mbps <li data-bbox="446 846 690 875">■ 3: 26 or 54 Mbps <li data-bbox="446 894 690 924">■ 4: 39 or 81 Mbps <li data-bbox="446 942 706 972">■ 5: 52 or 108 Mbps <li data-bbox="446 991 738 1020">■ 6: 58.5 or 121.5 Mbps <li data-bbox="446 1039 706 1068">■ 7: 65 or 135 Mbps <li data-bbox="446 1087 690 1117">■ 8: 13 or 27 Mbps <li data-bbox="446 1136 690 1165">■ 9: 26 or 54 Mbps <li data-bbox="446 1184 706 1213">■ 10: 39 or 81 Mbps <li data-bbox="446 1232 714 1262">■ 11: 52 or 108 Mbps <li data-bbox="446 1281 714 1310">■ 12: 78 or 162 Mbps <li data-bbox="446 1329 730 1358">■ 13: 104 or 216 Mbps <li data-bbox="446 1377 722 1407">■ 14: 117 or 243 Mbps <li data-bbox="446 1425 730 1455">■ 15: 130 or 270 Mbps <hr/> <p data-bbox="446 1493 706 1522">CTS Protection Mode</p> <p data-bbox="446 1541 1437 1701">CTS (Clear-To-Send) Protection Mode boosts the device's ability to catch all wireless transmissions, but can severely decrease performance. Select Auto to use this feature when needed, when the Wireless-N/G products are not able to transmit to the device in an environment with heavy 802.11b traffic. Select Disable to permanently disable this feature.</p> <hr/> <p data-bbox="446 1730 641 1759">Beacon Interval</p> <p data-bbox="446 1778 1421 1837">The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the device to synchronize the wireless network.</p> <p data-bbox="446 1856 860 1885">(Default: 100 msec, Range: 20-1000)</p>

Section	Field Description
	<p data-bbox="440 254 1446 296">DTIM Interval</p> <p data-bbox="440 296 1446 506">The Delivery Traffic Indication Message (DTIM) indicates the interval between Broadcasts/Multicast transmissions. DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the device has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.</p> <p data-bbox="440 506 1446 569">(Default: 1, Range: 1-255)</p>
	<p data-bbox="440 569 1446 611">Fragmentation Threshold</p> <p data-bbox="440 611 1446 831">The fragmentation threshold value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346.</p>
	<p data-bbox="440 831 1446 873">RTS Threshold</p> <p data-bbox="440 873 1446 1188">The RTS Threshold determines at what packet size beyond which the ready to send/clear to send (RTS/CTS) mechanism is invoked. Should you encounter inconsistent data flow, only minor reduction of the default value, 2346, is recommended. If a network packet is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will not be enabled. The device sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.</p>

Wireless > WDS Settings

The Wireless Distribution System (WDS) Settings page allows you to expand the coverage of your wireless network by deploying signal repeaters. Make sure the channel settings are the same for all WDS enabled devices.

Select the **WDS Settings** tab to open the Wireless WDS Settings page. Use this page to configure the WDS settings.



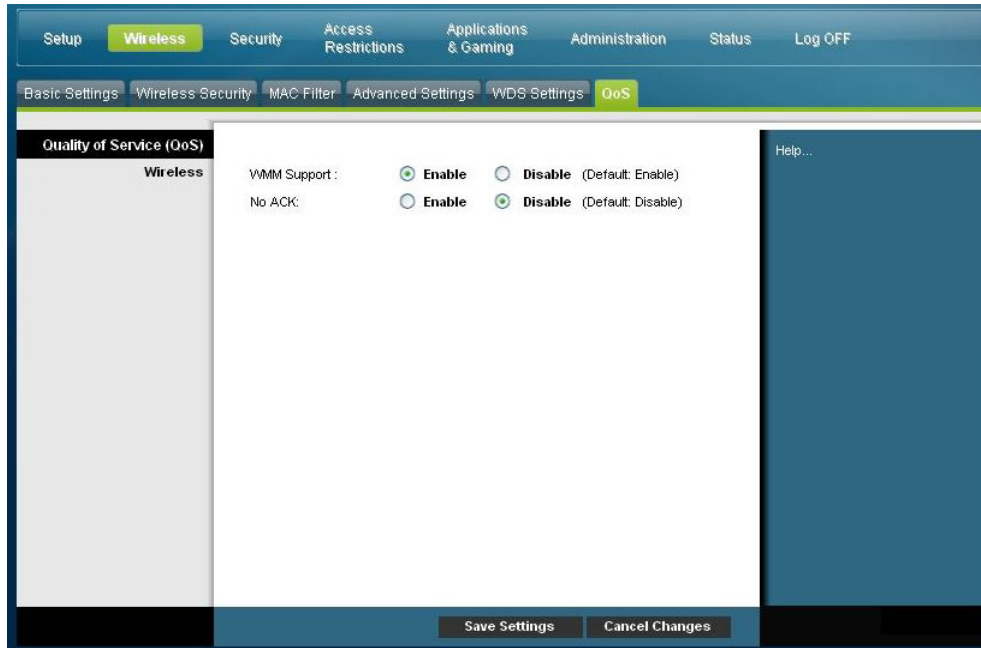
Wireless WDS Settings Page Description

Use the descriptions and instructions in the following table to configure the wireless distribution system settings for your residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
WDS	<p>WDS MAC Address</p> <p>Displays the WDS MAC Address (or BSSID) of your gateway access point</p> <hr/> <p>Allow Wireless Signal To Be Repeated by a Repeater</p> <p>Check this box to allow a wireless client to connect to a repeater and route traffic between the wireless client and a repeater. A maximum of 3 repeaters are allowed.</p> <hr/> <p>Remote Access Point's MAC Address (MAC 1 through 3)</p> <p>Use the three fields (MAC 1, 2, and 3) to enter the MAC address of the repeaters</p>

Wireless > QoS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as video conferencing. QoS settings allow you to specify priorities for different types of traffic. Lower priority traffic will be slowed down to allow greater throughput or less delay for high priority traffic. Select the **QoS** tab to open the Wireless QoS page.



Wireless QoS Page Description

Use the descriptions and instructions in the following table to configure each QoS setting. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
Quality of Service (QoS)	
Wireless	WMM Support If WMM (Wi-Fi Multimedia) is supported by your wireless clients, enabling this feature means that multimedia traffic will be given higher priority than other traffic. Select the desired option: <ul style="list-style-type: none"> ■ Enable (factory default) ■ Disable

Configure Wireless Settings

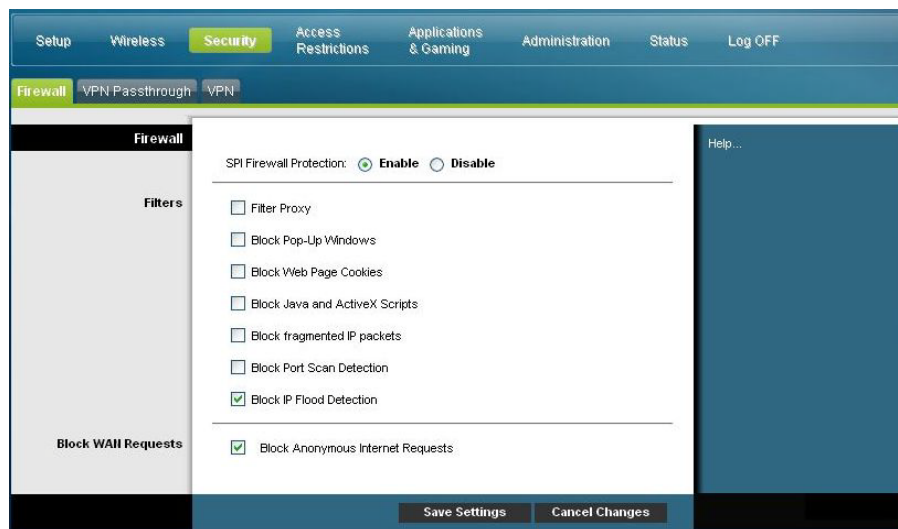
Section	Field Description
	<p data-bbox="623 268 732 296">No ACK</p> <p data-bbox="623 317 1321 541">Allows you to enable or disable NO ACK. This feature is recommended for data services where transmission is important and packet loss is tolerable to a certain degree. If you select Disable, an acknowledge packet is returned for every packet received. This provides a more reliable transmission, but it increases traffic load, which decreases performance.</p> <p data-bbox="623 562 915 590">Select the desired option:</p> <ul data-bbox="623 611 964 688" style="list-style-type: none"><li data-bbox="623 611 753 638">■ Enable<li data-bbox="623 659 964 688">■ Disable (factory default)

Configure Security

Security > Firewall

Advanced firewall technology deters hackers and protects the home network from unauthorized access. Use this page to configure a firewall that can filter out various types of unwanted traffic on the gateway’s local network.

Select the **Firewall** tab to open the Security Firewall page.



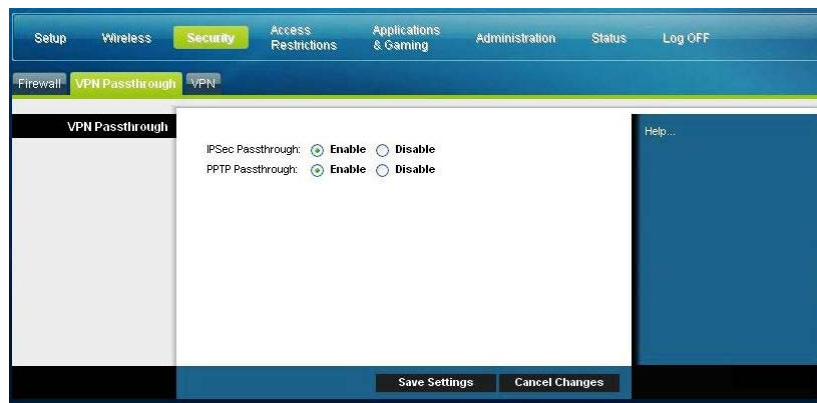
Use the descriptions and instructions in the following table to configure the firewall for your residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
Firewall	<p>SPI Firewall Protection</p> <p>SPI Firewall Protection blocks Denial of Service (DoS) attacks. A DoS attack does not attempt to steal data or damage your computers, but it overloads your Internet connection so you cannot use it.</p> <p>Select the desired option:</p> <ul style="list-style-type: none"> ■ Enable (factory default) ■ Disable

Section	Field Description
Filters	Filter Proxy
	Enables/disables filter proxy. If local users have access to WAN proxy servers, they may be able to circumvent the content filters and access Internet sites blocked by the device. If you select the Filter Proxy feature, it will block access to any WAN proxy servers.
	Block Pop-Up 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 Web Page 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.
	Block Java and ActiveX Scripts
	Enables/disables java applets and ActiveX scripts. 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.
	Java is a programming language for websites. If you select the Filter Java Applets feature, you may not have access to Internet sites created using this programming language.
	This feature also 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.
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.	
Block 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.	
Block IP Flood Detection (checked – factory default)	
Blocks malicious devices that are attempting to flood devices or networks with illegal broadcast packets. Also referred to as “broadcast storm.”	
Block WAN Requests	Block Anonymous Internet Requests (checked – factory default)
	Enable this feature to keep your network from being "pinged" or detected by other Internet users. The Block Anonymous Internet Requests feature also hides your network ports. Both make it more difficult for outside users to enter your network.

Security > VPN Passthrough

Use this page to configure Virtual Private Network (VPN) support. Enabling the settings on this page allows VPN tunnels using IPsec or PPTP protocols to pass through the gateway's firewall. Select the **VPN Passthrough** tab to open the Security VPN Passthrough page.



Use the descriptions and instructions in the following table to configure the VPN passthrough for your residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
VPN Passthrough	<p>IPSec Passthrough</p> <p>Enables/disables Internet Protocol Security (IPsec). IPsec is a suite of protocols used to implement secure exchange of packets at the IP layer. If you enable IPsec Passthrough, applications that use IPsec (IP Security) can pass through the firewall. To disable IPsec Passthrough select Disable.</p> <p>Select the desired option:</p> <ul style="list-style-type: none"> ■ Enable (factory default) ■ Disable
	<p>PPTP Passthrough</p> <p>Enables/disables Point-to-Point Tunneling Protocol (PPTP). PPTP allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. If you enable PPTP passthrough, applications that use Point to Point Tunneling Protocol (PPTP) can pass through the firewall To disable PPTP Passthrough select Disable.</p> <p>Select the desired option:</p> <ul style="list-style-type: none"> ■ Enable (factory default) ■ Disable

Security > VPN

A Virtual Private Network (VPN) is a connection between two endpoints in different networks that allows private data to be sent securely over public networks or other private 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 on a private network. The VPN tunnel uses IPsec to encrypt the data sent between the two endpoints and encapsulate the data within a normal Ethernet/IP frame allowing the data to pass between networks securely and seamlessly.

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 IPsec VPN creates a secure connection that operates as if you were directly connected to your local private 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.

Select the **VPN** tab to open the Security VPN page.

Use this page to configure the VPN for your residential gateway.

The screenshot displays the 'VPN Tunnel' configuration page. At the top, there are navigation tabs: Setup, Wireless, Security (highlighted), Access Restrictions, Applications & Gaming, Administration, Status, and Log OFF. Below these are sub-tabs: Firewall, VPN Passthrough, and VPN (highlighted). The main content area is titled 'VPN Tunnel' and includes a 'Select Tunnel Entry' dropdown (currently showing 'Tunnel list is EMPTY'), 'Create', 'Delete', and 'Summary' buttons. The 'IPSec VPN Tunnel' section has radio buttons for 'Enable' and 'Disable' (selected), and a 'Tunnel Name' field with '(null)'. The 'Local Secure Group' section has a 'Subnet' dropdown and IP/Mask input fields (IP: 0.0.0.0, Mask: 0.0.0.0). The 'Remote Secure Group' section has a 'Subnet' dropdown and IP/Mask input fields (IP: 0.0.0.0, Mask: 0.0.0.0). The 'Remote Secure Gateway' section has an 'IP Addr.' dropdown and an IP input field (IP: 0.0.0.0). The 'Key Management' section includes 'Key Exchange Method' (Auto (IKE)), 'Encryption' (3DES), 'Authentication' (MD5), 'PFS' (Disable), 'Pre-Shared Key' (masked with dots), and 'Key Lifetime' (0 seconds). At the bottom, the status is 'NOT Connected', and there are 'Connect', 'Disconnect', 'View Log', and 'Advanced Settings' buttons.

Security VPN Tunnel Page Description

Use the descriptions and instructions in the following table to configure the VPN tunnel for your gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
VPN Tunnel	<p>Select Tunnel Entry</p> <p>Allows you to display a list of created VPN tunnels</p> <p>Create Button</p> <p>Click this button to create a new tunnel entry</p> <p>Delete Button</p> <p>Click this button to delete all settings for the selected tunnel</p> <p>Summary Button</p> <p>Click this button to display the settings and status of all enabled tunnels</p> <p>IPSec VPN Tunnel</p> <p>Allows you to enable or disable Internet Security Protocol for the VPN tunnel</p> <p>Tunnel Name</p> <p>Enter the name for this tunnel</p>
Local Secure Group	<p>Select the local LAN user(s) that can use this VPN tunnel. This may be a single IP address or sub-network. Note that the Local Secure Group must match the remote gateway's Remote Secure Group.</p> <p>IP</p> <p>Enter the IP address of the local network</p> <p>Mask</p> <p>If the Subnet option is selected, enter the mask to determine the IP address on the local network</p>
Remote Secure Group	<p>Select the remote LAN user(s) behind the remote gateway who can use this VPN tunnel. This may be a single IP address, a sub-network, or any addresses. If "Any" is set, the Gateway acts as responder and accepts requests from any remote user. Note that the Remote Secure Group must match the remote gateway's Local Secure Group.</p> <p>IP</p> <p>Enter the IP address of the remote network</p> <p>Mask</p> <p>If the Subnet option is selected, enter the mask to determine the IP addresses on the remote network</p>

Configure Security

Section	Field Description
Remote Secure Gateway	<p>Select the desired option, IP Addr., Any, or FQDN. If the remote gateway has a dynamic IP address, select Any or FQDN. If Any is selected, then the Gateway will accept requests from any IP address.</p> <p>FQDN</p> <p>If FQDN is selected, enter the domain name of the remote gateway, so the Gateway can locate a current IP address using DDNS</p> <p>IP</p> <p>The IP address in this field must match the public (WAN or Internet) IP address of the remote gateway at the other end of this tunnel</p>
Key Management	<p>Key Exchange Method</p> <p>The gateway supports both automatic and manual key management. When automatic key management is selected, Internet Key Exchange (IKE) protocols are used to negotiate key material for Security Association (SA). If manual key management is selected, no key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purposes. Note that both sides must use the same key management method.</p>

Section	Field Description
Key Management (continued)	<p>Select one of the following options for the key exchange method:</p> <ul style="list-style-type: none"> ■ Auto (IKE) <ul style="list-style-type: none"> – Encryption: The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. Notice that both sides must use the same method. – Authentication: The Authentication method authenticates the Encapsulating Security Payload (ESP) packets. Select MD5 or SHA. Notice that both sides (VPN endpoints) must use the same method. <ul style="list-style-type: none"> ▪ MD5: A one-way hashing algorithm that produces a 128-bit digest ▪ SHA: A one-way hashing algorithm that produces a 160-bit digest – Perfect Forward Secrecy (PFS): If PFS is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication. Note that both sides must have PFS enabled. – Pre-Shared Key: IKE uses the Pre-Shared Key to authenticate the remote IKE peer. Both character and hexadecimal values are acceptable in this field, e.g., "My_@123" or "0x4d795f40313233". Note that both sides must use the same Pre-Shared Key. – Key Lifetime: This field specifies the lifetime of the IKE generated key. If the time expires, a new key will be renegotiated automatically. The Key Lifetime may range from 300 to 100,000,000 seconds. The default lifetime is 3600 seconds. ■ Manual <ul style="list-style-type: none"> – Encryption: The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. Notice that both sides must use the same method. – Encryption Key: This field specifies a key used to encrypt and decrypt IP traffic. Both character and hexadecimal values are acceptable in this field. Note that both sides must use the same Encryption Key. – Authentication: The Authentication method authenticates the Encapsulating Security Payload (ESP) packets. Select MD5 or SHA. Notice that both sides (VPN endpoints) must use the same method. <ul style="list-style-type: none"> ▪ MD5: A one-way hashing algorithm that produces a 128-bit digest ▪ SHA: A one-way hashing algorithm that produces a 160-bit digest – Authentication Key: This field specifies a key used to authenticate IP traffic. Both character and hexadecimal values are acceptable in this field. Note that both sides must use the same Authentication Key. – Inbound SPI/Outbound SPI: The Security Parameter Index (SPI) is carried in the ESP header. This enables the receiver to select the SA, under which a packet should be processed. The SPI is a 32-bit value. Both decimal and hexadecimal values are acceptable. e.g., "987654321" or "0x3ade68b1". Each tunnel must have a unique Inbound SPI and Outbound SPI. No two tunnels share the same SPI. Note that the Inbound SPI must match the remote gateway's Outbound SPI, and vice versa.

Section	Field Description
Status	This field shows the connection status for the selected tunnel. The state is either Connected or Disconnected .
Buttons	<p data-bbox="397 352 495 380">Connect</p> <p data-bbox="397 401 1356 464">Click this button to establish a connection for the current VPN tunnel. If you have made any changes, click Save Settings to first apply your changes.</p> <p data-bbox="397 485 535 512">Disconnect</p> <p data-bbox="397 533 1177 560">Click this button to break a connection for the current VPN tunnel.</p> <p data-bbox="397 581 511 609">View Log</p> <p data-bbox="397 630 1315 693">Click this button to view the VPN log, which shows details of each established tunnel.</p> <p data-bbox="397 714 625 741">Advanced Settings</p> <p data-bbox="397 762 1315 888">If the Key Exchange Method is Auto (IKE), this button provides access to additional settings relating to IKE. Click this button if the gateway is unable to establish a VPN tunnel to the remote gateway, and make sure the Advanced Settings match those on the remote gateway.</p> <ul style="list-style-type: none"> <li data-bbox="397 909 755 936">■ Phase 1 - Operation Mode <ul style="list-style-type: none"> <li data-bbox="446 957 1153 984">Select the method appropriate for the remote VPN endpoint. <li data-bbox="446 1005 998 1033">– Main: Main mode is slower but more secure <li data-bbox="446 1054 1112 1081">– Aggressive: Aggressive mode is faster but less secure <li data-bbox="397 1102 609 1129">■ Local Identity <ul style="list-style-type: none"> <li data-bbox="446 1150 1356 1213">Select the desired option to match the Remote Identity setting at the other end of this tunnel. <li data-bbox="446 1234 1079 1262">– Local IP Address: Your WAN (Internet) IP address <li data-bbox="446 1283 795 1310">– Name: Your domain name <li data-bbox="397 1331 641 1358">■ Remote Identity <ul style="list-style-type: none"> <li data-bbox="446 1379 1364 1442">Select the desired option to match the Local Identity setting at the other end of this tunnel. <li data-bbox="446 1463 1356 1491">– Local IP Address: WAN (Internet) IP address of the remote VPN endpoint <li data-bbox="446 1512 1079 1539">– Name: Domain name of the remote VPN endpoint. <li data-bbox="397 1560 576 1587">■ Encryption <ul style="list-style-type: none"> <li data-bbox="446 1608 1372 1671">This is the Encryption algorithm used for the IKE SA. It must match the setting used at the other end of the tunnel.

View Log

The Security VPN View Log 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 view the following logs from this page:

- Access log
- Firewall log
- VPN log
- Parental Control log

The screenshot shows a web interface for viewing logs. At the top left is a 'Log' tab. To the right, there is a 'Type:' dropdown menu set to 'Firewall Log' and a 'Refresh' button. Below this is a table with the following data:

Description	Count	Last Occurrence	Target	Source
LAN-side SYN Flood	4	Thu Jan 01 00:00:54 1970	192.168.0.1:80	64.100.106.97:1332

At the bottom right of the interface is a 'Clear' button.

Click **Clear** to clear the log data.

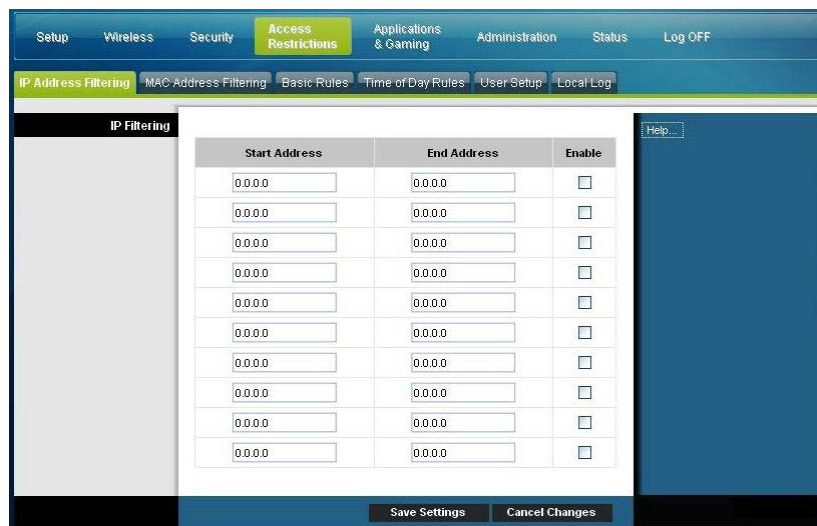
Control Access to the Gateway

Access Restrictions > IP Address Filtering

Use the Access Restrictions 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.

Select the **IP Address Filtering** tab to open the Access Restrictions IP Address Filtering page. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.



The screenshot shows a web interface for configuring IP Address Filtering. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions (selected), Applications & Gaming, Administration, Status, and Log OFF. Below this, there are sub-tabs for IP Address Filtering (selected), MAC Address Filtering, Basic Rules, Time of Day Rules, User Setup, and Local Log. The main content area is titled 'IP Filtering' and contains a table with three columns: Start Address, End Address, and Enable. The table has 10 rows, each with input fields for the start and end addresses and a checkbox for the enable status. All input fields currently contain '0.0.0.0'. At the bottom of the page, there are two buttons: 'Save Settings' and 'Cancel Changes'. A 'Help...' link is visible on the right side of the table area.

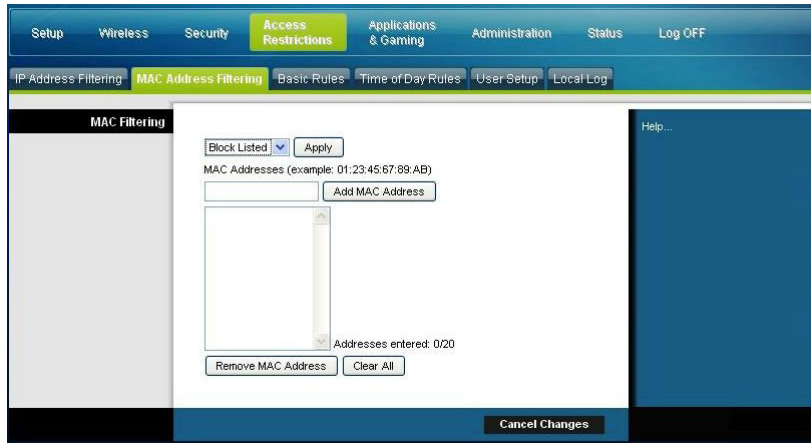
Start Address	End Address	Enable
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input type="checkbox"/>
0.0.0.0	0.0.0.0	<input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

Access Restrictions > MAC Address Filtering

Use the Access Restrictions MAC Address Filtering page to configure MAC address filters. These filters permit you to allow or block a range of MAC addresses from accessing the Internet based on 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 IP filtering settings.

Select the **MAC Address Filtering** tab to open the Access Restrictions MAC Address Filtering page.



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. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Field Name	Description
MAC Filtering	Block Listed (Default) Select Block Listed 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 Listed Select Pass Listed 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 Address Filtering page.

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

Access Restrictions > Basic Rules

Access restrictions allow you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated applications, websites, and inbound traffic during specific days and times. The Access Restrictions Basic Rules page allows you to configure parental controls on the residential gateway, and to monitor the individuals who are authorized to set parental controls.

Select the **Basic Rules** tab to open the Access Restrictions Basic Rules page.

The screenshot shows a web interface for configuring parental controls. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions (highlighted), Applications & Gaming, Administration, Status, and Log OFF. Below this, a sub-navigation bar shows IP Address Filtering, MAC Address Filtering, Basic Rules (highlighted), Time of Day Rules, User Setup, and Local Log.

The main content area is titled "Parental Basic Setup" and is divided into several sections:

- Parental Control Activation:** A checkbox labeled "Enable Parental Control" is currently unchecked. Below it is an "Apply" button.
- Rule Settings:** A dropdown menu shows "1. Default" and a "Remove Rule" button.
- Keyword List:** A list box contains "anonymizer". Below the list are "Add Keyword" and "Remove Keyword" buttons.
- Blocked Domain List:** A list box contains "anonymizer.com". Below the list are "Add Domain" and "Remove Domain" buttons.
- Allowed Domain List:** An empty list box with "Add Allowed Domain" and "Remove Allowed Domain" buttons below it.
- Override the Password:** Fields for "Password" and "Re-Enter Password" (both masked with dots), "Access Duration" (set to 30), and an "Apply" button.

A "Help..." link is visible on the right side of the page.

Use the descriptions and instructions in the following table to configure the access restrictions basic rules for your residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
Parental Control Basic Setup	<p>Parental Control Activation</p> <p>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.</p> <p>Add Rule</p> <p>Adds and saves a new Rule to the list of content rules</p> <p>Remove Rule</p> <p>Removes the selected rule from the content rule list</p>
Keyword List	<p>Keyword List</p> <p>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</p> <p>Add/Remove Keyword</p> <p>Allows you to add new keywords to the list or to delete selected keywords from the list</p>
Blocked Domain List	<p>Blocked Domain List</p> <p>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</p> <p>Add/Remove Domain</p> <p>Allows you to add new domains to the list or to delete selected domains from the list</p>
Allowed Domain List	<p>Allowed Domain List</p> <p>Allows you to create a list of domains to which the gateway allows access</p> <p>Add/Remove Allowed Domain</p> <p>Allows you to add new domains to the list or to delete selected domains from the list</p>

Section	Field Description
Override the Password	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
	Access Duration Allows you to designate an amount of time in minutes that the Override password will allow temporary access to a restricted Internet site
	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.

Block Access to Websites

If you wish to block access to websites, use the **Blocked Domain List** or the **Keyword List**

To use the **Blocked Domain List**, enter the URLs or domain names of the websites you wish to block.

Use the **Keyword List** to enter the keywords you wish to block. If any of these keywords appears in the URL of a website, access to the site will be blocked. Note that only the URL is check, not the content of each webpage.

Access Restrictions > Time of Day Rules

Use the Access Restrictions Time of Day Rules 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.

Select the **Time of Day Rules** tab to open the Access Restrictions Time of Day Rules Page. The following illustration is an example of the Access Restrictions Time of Day Rules 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.

Access Restrictions Time of Day Rules Page Description

Use the descriptions and instructions in the following table to configure the time of day rules for your residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
Tod Filter	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
Schedule	Days to Block Allows you to control access based on days of the week
	Time to Block Allows you to control access based on time of day

Access Restrictions > User Setup

Use the Access Restrictions User Setup page to set up additional accounts and user profiles for household members. Each profile can be assigned customized levels of Internet access as defined by the access rules assigned to that user's profile.

Important: These additional accounts do not grant administrative access to the gateway.

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.

Select the **User Setup** tab to open the Access Restrictions User Setup page.



Access Restrictions User Setup Page Description

Use the descriptions and instructions in the following table to configure the user setup for your residential gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
User Configure	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
	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.
	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.
	To remove a user profile, use the drop-down menu to select the user to be removed and click the Remove User button.
	Password
	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.
	Note: The residential gateway will allow each user access to the Internet, subject to the rules selected on this page for that user.
	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 on the "Basic Rules" tab on this page.	
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 Rules page. You can access the Time of Day Rules page by clicking on the "Time of Day Rules" tab on this page.	
Session Duration	
1440 minutes [Factory default when a user is created. Otherwise, it is 0 (zero)].	
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.	
Note: Set the Session Duration to 0 (zero) to prevent session timeout.	

Section	Field Description
---------	-------------------

Inactivity Time

60 minutes [Factory default when a user is created. Otherwise, it is 0 (zero)].

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.

Note: Set the Inactivity time value to 0 (zero) to prevent session timeout.

Access Restrictions > Local Log

This page allows you to track, by user, any attempts made by that user to access Internet sites that are restricted. From this page you can also view events captured by the parental control event-reporting feature.

Select the **Local Log** tab to open the Access Restrictions Local Log page.

The following illustration is an example of the Access Restrictions Local Log page.



Section	Field Description
Local Log	Last Occurrence
Parental Control - Event Log	Displays the time of the most recent attempt to access a restricted Internet site
	Action
	Displays the action taken by the system
	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 Applications and Gaming

Overview

Most well-known Internet applications are supported by Application Layer Gateways (ALGs). ALGs automatically adjust the gateway firewall to allow data to pass without making any custom settings. We recommend that you test your application before making changes in this section.

Applications & Gaming > Port Filtering

Use this window 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. 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.

Select the **Port Filtering** tab to open the Applications & Gaming 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"/>
0	0	Both	<input type="checkbox"/>

Applications and Gaming Port Filtering Page Description

Use the descriptions and instructions in the following table to configure the port filtering for applications and gaming features used on your residential gateway. Click the **Enable** checkbox to enable port forwarding for the relevant application. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
Port Filtering	<p>Start Port:</p> <p>This is the beginning of the port range. Enter the beginning of the range of port numbers (external ports) used by the server or Internet application. Check with the software documentation of the Internet application for more information if necessary.</p>
	<p>End Port:</p> <p>This is the end of the port range. Enter the end of the range of port numbers (external ports) used by the server or Internet application. Check with the software documentation of the Internet application for more information if necessary.</p>
	<p>Protocol</p> <p>Select one of the following protocols:</p> <ul style="list-style-type: none"> ■ TCP ■ UDP ■ Both
	<p>Enable:</p> <p>Check this box to enable filtering on the specified ports.</p>

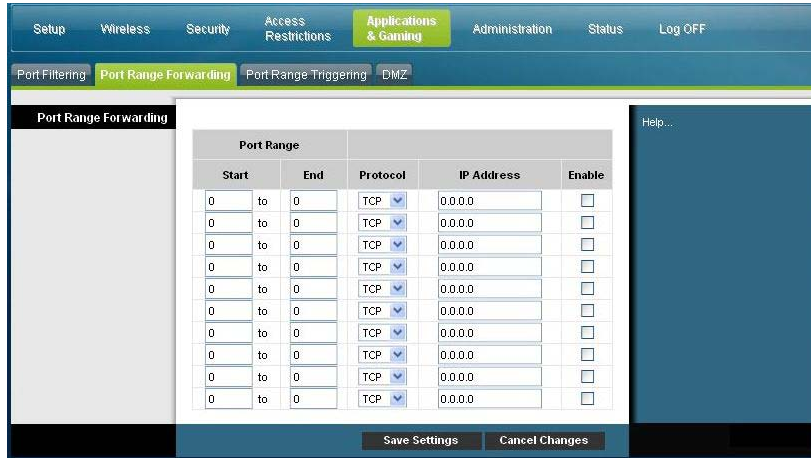
Applications & Gaming > Port Range Forwarding

Important: The gateway normally implements a feature called Port Translation. Port Translation monitors what ports are actually being used by your PCs or other devices on your LAN. This monitoring provides an added level of security beyond what the firewall provides. However, there are some applications that require the gateway to use specific ports to connect over the Internet.

Use Port Range Forwarding to forward ports from the public Internet to specific IP addresses in your local network. Select the **Port Range Forwarding** tab to open the Applications & Gaming Port Range Forwarding page.

For the Start and End Port, select a port from the recommended 49152 - 65535 range. Keep in mind that ports used are program specific so check which ones the program requires to be forwarded. Type the port number or range in both boxes. In the IP Address box type the name of the computer's IP address to which this is to apply.

Note: Port Range Forwarding continually exposes the selected ports to the public Internet. This means that the gateway's firewall is no longer active on these ports. The device with the forwarding IP address can be exposed to hacker attacks while the port range is being forwarded.



Applications and Gaming Port Range Forward Page Description

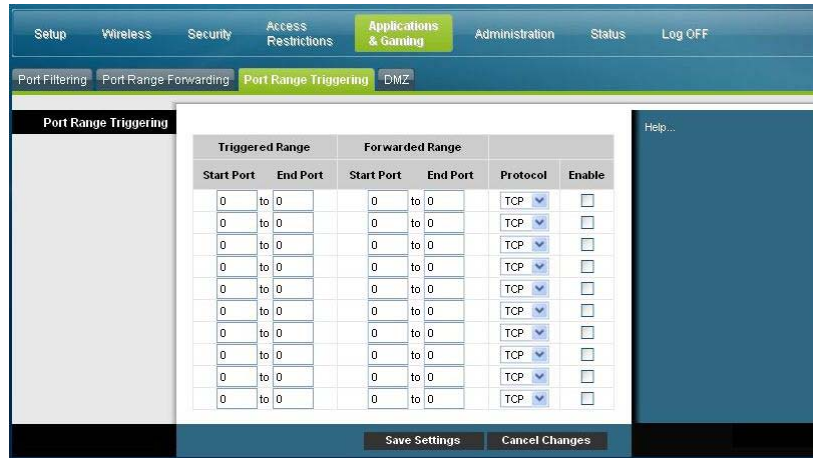
Use the descriptions and instructions in the following table to configure the port range forwarding for the residential gateway. Select enable for each. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
Port Range Forwarding Start	For the Start port, select a port from the recommended 49152 - 65535 range. Keep in mind that ports used are program specific so check which ones the program requires to be forwarded.
End	For the End port, select a port from the recommended 49152 - 65535 range. Keep in mind that ports used are program specific so check which ones the program requires to be forwarded.
Protocol	Select one of the following protocols: <ul style="list-style-type: none"> ■ TCP ■ UDP ■ Both
IP Address	Enter the computer's IP address to which this is to apply.
Enable	Check this box to enable port forwarding for the specified ports and IP addresses.

Applications & Gaming > Port Range Triggering

Port range triggering is a way to dynamically forward ports to a LAN PC that needs them at a particular time. That particular time is when it runs a certain application that performs some event that trigger the router. This event must be an outbound access of a particular port range.

Select the **Port Range Triggering** tab to open the Applications & Gaming Port Range Triggering page.



Applications and Gaming Port Range Triggering Page Description

Use the descriptions and instructions in the following table to configure the port range triggering for the residential gateway. Select enable for each. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
Port Range Triggering	
Triggered Range	Start Port For the Start port, select a port from the recommended 49152 - 65535 range. Keep in mind that ports used are program specific so check which ones the program requires to be forwarded.
	End Port For the End port, select a port from the recommended 49152 - 65535 range. Keep in mind that ports used are program specific so check which ones the program requires to be forwarded.
Forwarded Range	Start Port For the Start port, select a port from the recommended 49152 - 65535 range. Keep in mind that ports used are program specific so check which ones the program requires to be forwarded.

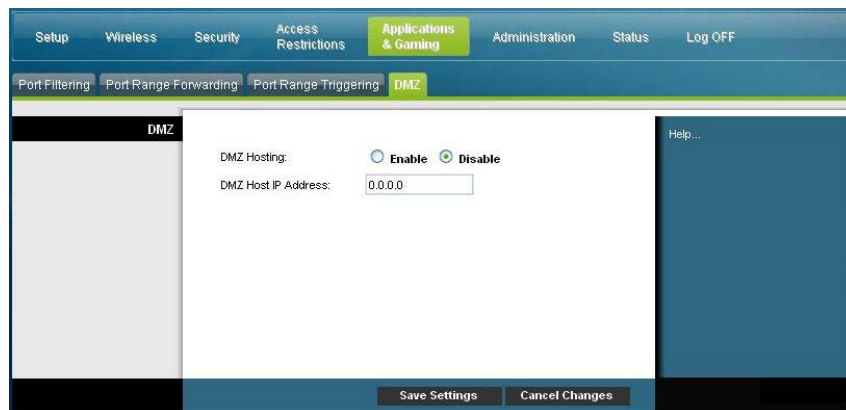
Section	Field Description
	<p>End Port</p> <p>For the End port, select a port from the recommended 49152 - 65535 range. Keep in mind that ports used are program specific so check which ones the program requires to be forwarded.</p>
	<p>Protocol</p> <p>Select one of the following protocols:</p> <ul style="list-style-type: none"> ■ TCP ■ UDP ■ Both
	<p>Enable</p> <p>Click the Enable checkbox to enable port range triggering for the relevant application.</p>

Applications & Gaming > DMZ

Use this page to configure an IP address whose ports are directly exposed to the public Internet or to the Wide Area Network (WAN). Demilitarized Zone (DMZ) hosting is commonly referred to as "exposed host," and allows you to specify a recipient of WAN traffic that Network Address Translation (NAT) is unable to translate to a known local PC.

A DMZ is typically used by a company that wants to host its own Internet server. DMZ allows one IP address to be placed on the Internet side of the gateway firewall while others remain protected behind the firewall.

The DMZ allows a device to be directly accessible to Internet traffic, such as a web (HTTP) server, an FTP server, an SMTP (e-mail) server, and a domain name system (DNS) server. Select the **DMZ** tab to open the Applications & Gaming DMZ page.



Applications and Gaming DMZ Page Description

Use the descriptions and instructions in the following table to configure the port range triggering for the residential gateway. Select enable for each DMZ Host IP address. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
DMZ	DMZ Hosting Select the desired option: <ul style="list-style-type: none">■ Enable■ Disable (factory default)
	DMZ Host IP Address DMZ allows one IP address to be unprotected while others remain protected. Enter the IP address of the computer you want to expose to the Internet in this field.

Manage the Gateway

Administration > Management

The Administration Management page allows the network's administrator to manage specific gateway functions for access and security. Select the **Management** tab to open the Administration Management page.

Important: The following page displays when **DHCP** (factory default) is the Connection Mode. The page that displays when **Static IP** is selected is shown and described later in this section.

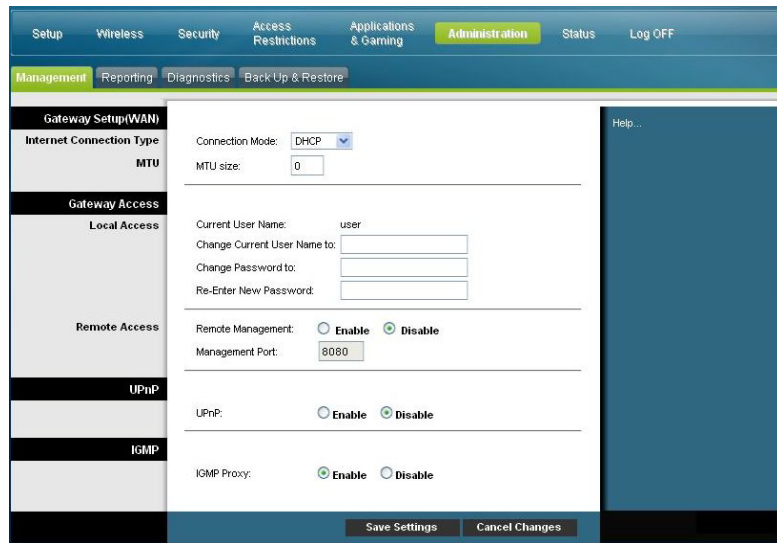
The screenshot displays the Administration Management page for Gateway Setup (WAN). The page is organized into several sections:

- Navigation:** Top tabs include Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration (selected), Status, and Log OFF. Sub-tabs under Administration include Management (selected), Reporting, Diagnostics, and Back Up & Restore.
- Gateway Setup (WAN):**
 - Internet Connection Type:** Connection Mode is set to DHCP (dropdown), and MTU size is 0 (input field).
 - Gateway Access:**
 - Local Access:** Current User Name is 'user'. Fields for 'Change Current User Name to:', 'Change Password to:', and 'Re-Enter New Password:' are present.
 - Remote Access:** Remote Management is set to 'Disable' (radio button). Management Port is 8080 (input field).
 - UPnP:** UPnP is set to 'Disable' (radio button).
 - IGMP:** IGMP Proxy is set to 'Enable' (radio button).
- Buttons:** 'Save Settings' and 'Cancel Changes' buttons are located at the bottom of the configuration area.
- Help:** A 'Help...' link is visible on the right side of the page.

Administration Management Page Description

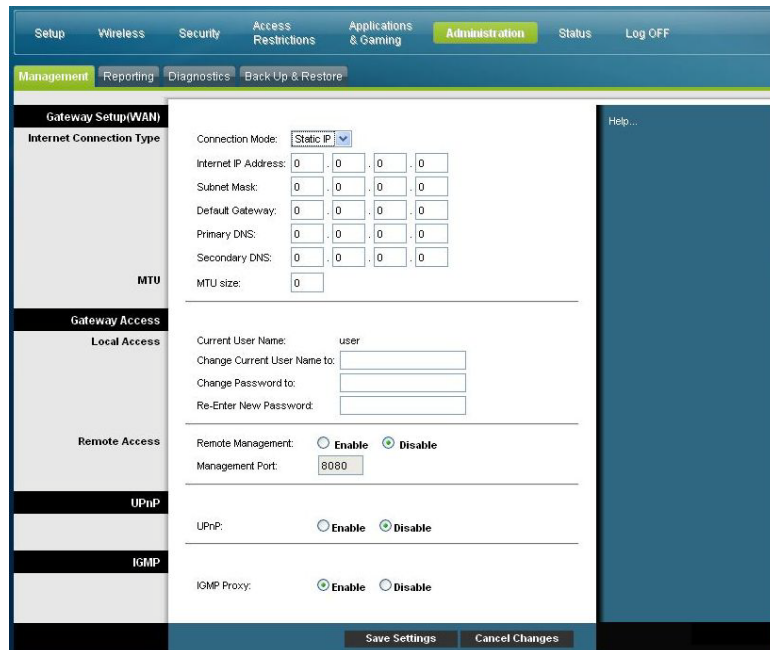
Use the descriptions and instructions in the following table to configure the administration management for the residential gateway when DHCP or Static IP connection mode is selected. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Field	Description
Gateway Setup (WAN)	Connection Mode This setting allows you to determine how the WAN (or gateway interface to the Internet) obtains its IP address.
Internet Connection Type	DHCP (factory default) Allows the gateway to obtain a public IP address automatically



Static IP

Allows you to specify the WAN IP address and corresponding server information as static or fixed values that will be used whenever the gateway goes online



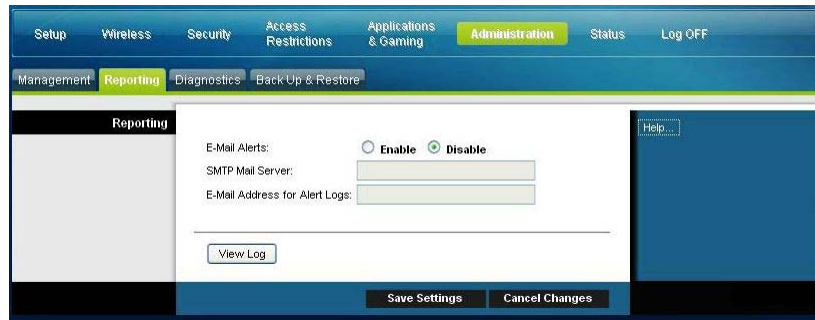
Field	Description
	<p>Internet IP Address</p> <p>Enter the gateway's IP address (as seen from the Internet)</p> <p>Subnet Mask</p> <p>Enter the gateway's subnet mask (as seen from the Internet, including your service provider)</p> <p>Default Gateway</p> <p>Enter the default gateway of the service provider's server</p> <p>Primary DNS</p> <p>Enter the primary domain name server IP address(es) provided by your service provider. This is required.</p> <p>Secondary DNS</p> <p>Enter the secondary domain name server IP address(es) provided by your service provider. This is optional.</p>
MTU	<p>MTU size</p> <p>MTU is the Maximum Transmission Unit. The MTU size specifies the largest packet size permitted for Internet transmission. . The factory default = 0 (1500 bytes)</p>
Gateway Access	<p>Current User Name</p>
Local Access	<p>Identifies the currently logged in user</p> <p>Change Current User Name to</p> <p>This field allows you to change your user name. If you want to change your user name, enter your new user name in this field and click Save Settings to apply the change.</p> <p>Note: The factory default user name is a blank field.</p> <p>Change Password to</p> <p>This field allows you to change your password. If you want to change your password, enter your new password in this field. Then, re-enter your new password in the Re-Enter New Password field and click Save Settings to apply the change.</p> <p>Note: The factory default password is a blank field.</p> <p>Re-Enter New Password</p> <p>Allows you to re-enter the new password. You must enter the same password as the one entered in the previous field Change Password to. After you re-enter your new password, click Save Settings to apply the change.</p>

Field	Description
Remote Access	<p data-bbox="602 268 862 296">Remote Management</p> <p data-bbox="602 317 1383 575">Allows you to enable to disable remote management. This feature allows you to access and manage your gateway settings from the Internet when you are away from home. To allow remote access, select Enable. Otherwise, keep the default setting, as Disable. The protocol HTTP is required for remote management. To remotely access the device, enter https://xxx.xxx.xxx.xxx:8080 (the x's represent the device's public Internet IP address, and 8080 represents the specified port) in your web browser's Address field.</p> <p data-bbox="602 596 818 623">Management Port</p> <p data-bbox="602 644 1383 737">Enter the port number that will be open to outside access. The factory default setting is 8080. This port must be used when you establish a remote connection.</p>
UPnP	<p data-bbox="602 758 672 785">UPnP</p> <p data-bbox="602 806 1383 940">Universal Plug and Play (UPnP) allows Windows XP and Vista to automatically configure the Gateway for various Internet applications, such as gaming and videoconferencing. If you want to use UPnP, keep the default, Enable. Otherwise, select Disable.</p>
IGMP	<p data-bbox="602 961 753 989">IGMP Proxy</p> <p data-bbox="602 1010 1383 1234">Internet Group Multicast Protocol (IGMP) is used to establish membership in a multicast group and is commonly used for multicast streaming applications. For example, you may have Internet Protocol Television (IPTV) with multiple set-top boxes on the same local network. These set-top boxes have different video streams running simultaneously, so you should use the IGMP feature of the Router.</p> <p data-bbox="602 1255 1383 1352">IGMP forwarding (proxying) is a system that improves multicasting for LAN-side clients. If the clients support this option, keep the default, Enable. Otherwise, select Disable.</p>

Administration > Reporting

Administration reporting allows you to email various system activities to your email address.

Select the **Reporting** tab to open the Administration Reporting page.



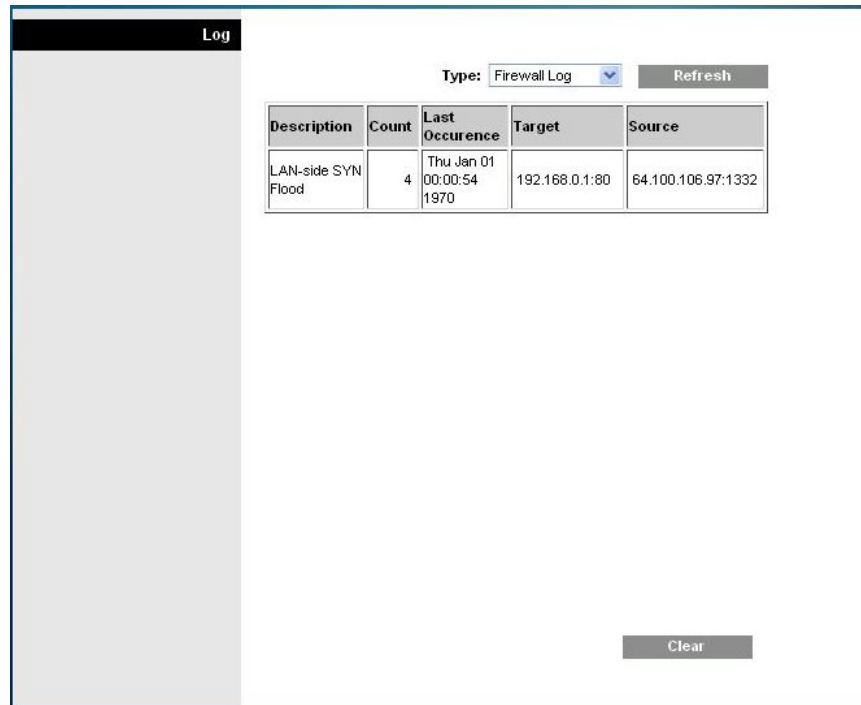
Use the descriptions and instructions in the following table to configure the reporting feature on the gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

Section	Field Description
Reporting	E-Mail Alerts If enabled, an e-mail will be sent immediately if any reportable events are detected. To use this feature, provide the necessary e-mail address information.
	SMTP Mail Server Enter the address (domain name) or IP address of the Simple Mail Transport Protocol (SMTP) server you use for outgoing e-mail.
	E-Mail Address for Alert Logs Enter the e-mail address that should receive the logs.

View Log

To view the logs, complete the following steps.

- 1 Click **View Log**. A new window opens with the log data page.

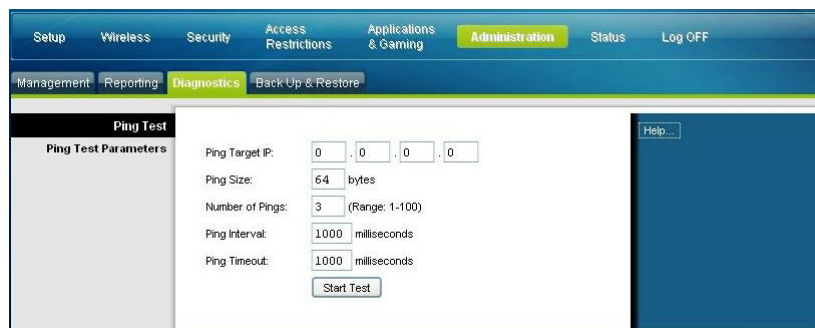


- 2 To view a particular log, select one of the following options from the Type drop-down menu:
 - All
 - Access Log
 - Firewall Log
 - VPN Log
- 3 After the log data is displayed, use one of the following options:
 - Click the **Page Refresh** button to update the log.
 - Click the **Clear** button to clear all the information in the current log.
 - Click the **Previous Page** button to go back to the information previously displayed.
 - Click the **Next Page** button to see the next section of the log, if available.

Administration > Diagnostics

Administration diagnostics allow you to check the status of your Internet connection by using a Ping test.

Select the **Diagnostics** tab to open the Administration Diagnostics page.




Use the descriptions and instructions in the following table to configure the diagnostics feature on the gateway. After you make your selections, click **Save Settings** to apply your changes or **Cancel Changes** to cancel.

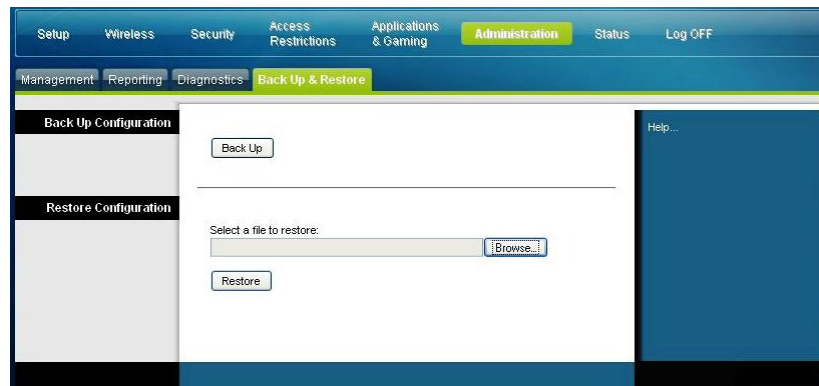
Section	Field Description
Ping Test	
Ping Test Parameters	<p>Ping Target IP The IP address that you want to ping</p> <p>Ping Size The size of the packet you want to use</p> <p>Number of Pings The number of times you wish to ping the target device</p> <p>Ping Interval The time period (milliseconds) between each ping</p> <p>Ping Timeout The desired time period (milliseconds) of the timeout. If no response is received within this ping period, the ping test is considered a failure</p> <p>Start Test To start a test, complete the following steps.</p> <ol style="list-style-type: none"> 1 Click Start Test to begin the text. A new page opens and displays a summary of the test results. 2 Click the Save Settings to save the test results or click Cancel Changes to cancel the test.

Administration > Backup & Restore

Administration Backup & Restore allows you to back up you configuration of the Gateway and store it on your computer. You can use this file to restore a previously saved configuration for your Gateway.

Select the **Back Up & Restore** tab to open the Administration Back Up & Restore page.

 **CAUTION:**
Restoring a configuration file will destroy (overwrite) all of the existing settings.



Section	Field Description
Back Up Configuration	Use the Back Up Configuration feature to save a copy of the current configuration and store the file on your computer. Click Back Up to start the download.
Restore Configuration	Use the Restore Configuration feature to restore a previously saved configuration file. Click Browse to select the configuration file, and then click Restore to load the configuration file to the device.

Administration > Factory Defaults

The Administration Factory Defaults page allows you to restore the configuration to its factory default settings. Select the **Factory Defaults** tab to open the Administration Factory Defaults page.



CAUTION:

If you restore the factory defaults, the gateway will lose all of the settings you have entered. Before you reset the gateway to its factory default settings, write down all of your custom settings. After the defaults have been restored, you will have to re-enter all of your configuration settings.



Restore Factory Defaults

To restore factory defaults, click **Restore Factory Defaults** to reset all configuration settings to their default values. Any settings you have saved will be lost when the default settings are restored.

Monitor Gateway Status

This section describes the options available under the Status tab that you can use to monitor the status of the residential gateway and to perform diagnostics on the device and the network.

Status > Gateway

The Gateway Status page displays information about the gateway and its current settings. The on-screen information varies depending on the Internet Connection type you use.

Select the **Gateway** tab to open the Status Gateway screen. Click **Refresh** to update the data displayed on-screen.



Use the descriptions in the following table to review the status of your gateway and your Internet connection.

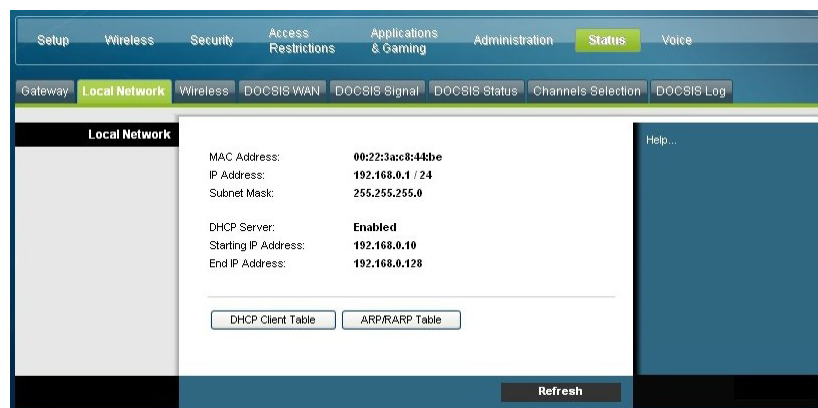
Section	Field Description
Gateway Information	Firmware Version The version number of the firmware.
	MAC Address (CM MAC Address) A unique alphanumeric address for the cable modem coaxial interface, which is used to connect to the cable modem termination system (CMTS) at the headend. A media access control (MAC) address is a hardware address that uniquely identifies each node of a network.
	Current Time The time, based on the time zone selected on the Basic Setup page is displayed.

Section	Field Description
Internet Connection	IP Address
	Displays the IP address of the WAN interface. This address is assigned to the gateway when it goes online.
	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.
	Default Gateway
	The IP address of the ISP's Default Gateway.
DNS1-3	The DNS IP addresses currently used by the gateway.
	WINS
	The WINS IP address currently used by the gateway.

Status > Local Network

The Local Network Status page displays information about the status of the local area network.

Select the **Local Network** tab to open the Status Local Network page. Click **Refresh** to update the data on the page.



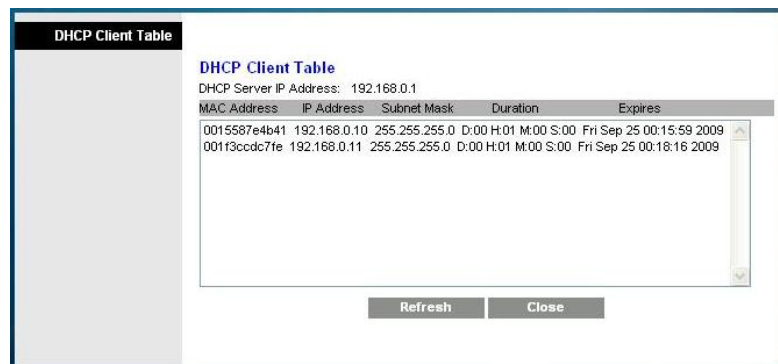
Use the following table to review the status of your gateway and your Internet connection.

Section	Field Description
Local Network	MAC Address
	A unique alphanumeric address for the private LAN home network. A MAC address is a hardware address that uniquely identifies each node of a network.

Section	Field Description
	<p>IP Address</p> <p>Displays the IP address for the LAN subnet</p> <p>Subnet Mask</p> <p>Displays the subnet mask for your LAN</p> <p>DHCP Server</p> <p>Displays the status of your local DHCP server (Enabled or Disabled)</p> <p>Starting IP Address</p> <p>Displays the beginning of the range of IP addresses used by the DHCP server in your gateway</p> <p>End IP Address</p> <p>Displays the end of the range of IP addresses used by the DHCP server</p>

DHCP Client Table Click **DHCP Client Table** to show which devices are attached to your LAN that have been issued IP addresses by the DHCP server in the gateway. On the DHCP Client Table page, you will see a list of DHCP clients (computers and other network devices) with the following information: Client Host Names, IP Addresses, MAC Addresses, and the length of time before their assigned IP addresses expire. To retrieve the most up-to-date information, click **Refresh**. To exit this page and return to the Local Network page, click **Close**.

The following illustration shows an example of the DHCP Client Table.



ARP/RARP Table Click **ARP/RARP Table** to see a complete list of all devices that are connected to your network. To retrieve the most up-to-date information, click **Refresh**. To exit this page and return to the Local Network page, click **Close**.

The following illustration shows an example of the ARP/RARP Table.

ARP/RARP Table		Refresh
IP Address	MAC Address	
10.13.0.1	00:13:5F:05:95:DA	
10.13.1.42	00:22:3A:CE:D8:75	
10.13.1.43	00:22:3A:CE:D8:79	
10.13.8.1	00:13:5F:05:95:DA	
192.168.0.1	00:22:3A:CE:D8:78	
192.168.0.10	00:15:58:7E:4B:41	
192.168.0.11	00:1F:3C:CD:C7:FE	
		Close

Status > Wireless

The Wireless Network Status page displays basic information about the wireless network of the gateway.

Select the **Wireless** tab to open the Status Wireless page. Click **Refresh** to update the data on the page.



Status Wireless Page Description

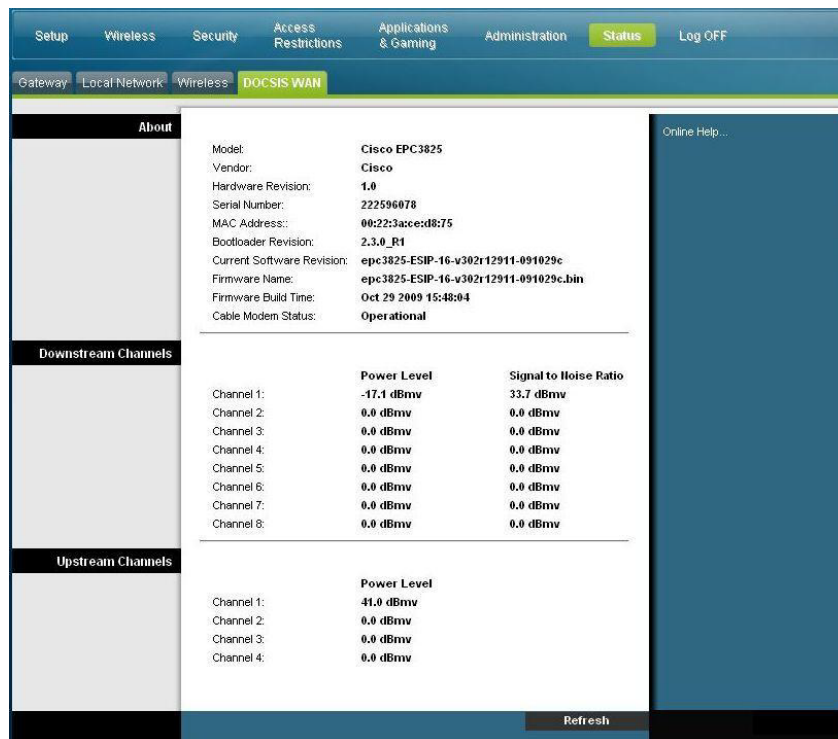
Use the following table to review the status of your wireless network.

Section	Field Description
Wireless Network	<p data-bbox="599 447 773 472">MAC Address</p> <p data-bbox="599 485 1382 548">Displays the MAC Address of your gateway's local wireless access point</p> <p data-bbox="599 569 740 594">Radio Band</p> <p data-bbox="599 606 1365 669">Displays one of the following radio band frequencies currently in operation:</p> <ul data-bbox="599 690 813 821" style="list-style-type: none"> <li data-bbox="599 690 740 716">■ 2.4 GHz <li data-bbox="599 737 721 762">■ 5 GHz <li data-bbox="599 783 813 808">■ 2.4 and 5 GHz <p data-bbox="599 837 1227 863">Note: Not all products support the 5 GHz radio band.</p> <p data-bbox="599 884 873 909">Network Name (SSID)</p> <p data-bbox="599 921 1365 984">Displays the name or service set identifier (SSID) of your wireless access point</p> <p data-bbox="599 1005 786 1031">Channel Width</p> <p data-bbox="599 1043 1312 1106">Displays the channel bandwidth setting selected on the Basic Wireless Settings page</p> <p data-bbox="599 1127 773 1152">Wide Channel</p> <p data-bbox="599 1165 1360 1228">Displays the Wide Channel setting selected on the Basic Wireless Settings page</p> <p data-bbox="599 1249 818 1274">Standard Channel</p> <p data-bbox="599 1287 1297 1350">Displays the Standard Channel setting selected on the Basic Wireless Settings page</p> <p data-bbox="599 1371 699 1396">Security</p> <p data-bbox="599 1409 1312 1434">Displays the security method used by your wireless network</p> <p data-bbox="599 1455 789 1480">SSID Broadcast</p> <p data-bbox="599 1493 1292 1518">Displays the status of the gateway's SSID Broadcast feature</p>

Status > DOCSIS WAN

DOCSIS WAN Status displays information about the system of your cable modem.

Select the **DOCSIS WAN** tab to open the Status DOCSIS WAN page.



DOCSIS WAN Page Description

Use the descriptions in the following table to review the status of your DOCSIS WAN network.

Section	Field Description
About	Model
	Displays the name of the residential gateway
	Vendor
	Displays the manufacturer of the residential gateway
	Hardware Revision
Displays the revision of the circuit board design	
About	Serial Number
	Displays the unique serial of the residential gateway

Monitor Gateway Status

Section	Field Description
	MAC Address (CM MAC Address) Displays the CM MAC Address. The CM MAC Address is a unique alphanumeric address for the cable modem coaxial interface, which is used to connect to the CMTS at the headend. A MAC address is a hardware address that uniquely identifies each node of a network.
	Bootloader Revision Displays the boot revision code version
	Current Software Revision Displays the revision version of the firmware
	Firmware Name Displays the name of the firmware
	Firmware Build Time Displays the date and time the firmware was built
	Cable Modem Status Displays one of the possible current states of the gateway
Downstream Channels	Channels 1-8 Displays the power level and the signal to noise ratio of the active downstream channels
Upstream Channels	Channels 1-4 Displays the power level of the active upstream channels

Frequently Asked Questions

Q. How Do I Configure TCP/IP Protocol?

A. 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 2000 Systems

- 1 Click **Start**, select **Settings**, and choose **Network and Dial-up Connections**.
- 2 Double-click the **Local Area Connection** icon in the Network and Dial-up Connections window.
- 3 Click **Properties** in the Local Area Connection Status window.
- 4 Click **Internet Protocol (TCP/IP)** in the Local Area Connection Properties window, and then click **Properties**.
- 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 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.

Frequently Asked Questions

- 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 page. 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.

Q. How Do I Renew the IP Address on My PC?

A. 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 95, 98, 98SE, and ME Systems

- 1 Click **Start**, and then click **Run** to open the Run window.
- 2 Type **wiipcfg** in the Open field, and click **OK** to execute the winipcfg command. The IP Configuration window opens.
- 3 Click the down arrow to the right of the top field, and select the Ethernet adapter that is installed on your PC. The IP Configuration window displays the Ethernet adapter information.
- 4 Click **Release**, and then click **Renew**. The IP Configuration window displays a new IP address.
- 5 Click **OK** to close the IP Configuration 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 Windows NT, 2000, or 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.

Q. What if I don't subscribe to cable TV?

A. 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.

Q. How do I arrange for installation?

A. Call your service provider to inquire about professional installation. A professional installation ensures proper cable connection to the modem 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.

Frequently Asked Questions

Q. How does the residential gateway connect to my computer?

A. The residential gateway connects to the PC using a wireless connection or the 10/100/1000BASE-T Ethernet port on your PC. If you want to use an 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.

Q. After my residential gateway is connected, how do I access the Internet?

A. 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.

Q. Can I watch TV and surf the Internet at the same time?

A. 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.

Common Troubleshooting Issues

I don't understand the front panel status indicators

See *Front Panel LED Status Indicator Functions* (on page 96), for more detailed information on front panel LED status indicator operation and function.

The residential gateway does not register an Ethernet connection

- 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 modem 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 modem 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 cable service provider to determine whether you are using the correct cable.
- Your NIC card or USB interface may be malfunctioning. Refer to the troubleshooting information in the NIC or USB documentation.

Tips for Improved Performance

Check and Correct

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.
- Verify that your TCP/IP is properly installed and configured if you are using the Ethernet connection.
- 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.
- For best performance over an Ethernet connection, your PC should be equipped with a Gigabit Ethernet card.

Front Panel LED Status Indicator Functions

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 6 (Request High-Speed Data Provisioning File), the modem proceeds immediately to Normal Operations. See *Normal Operations (AC Power applied)* (on page 98).

		High Speed Data Registration					
		1	2	3	4	5	6
Step:		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	ETHERNET1-4	On	On or Blinking	On or Blinking	On or Blinking	On or Blinking	On or Blinking
6	USB	On	On or Blinking	On or Blinking	On or Blinking	On or Blinking	On or Blinking
7	WIRELESS LINK	Off	On or Blinking	On or Blinking	On or Blinking	On or Blinking	On or Blinking
8	WIRELESS SETUP	Off	On or Blinking	On or Blinking	On or Blinking	On or Blinking	On or Blinking

Front Panel LED Status Indicators During Initial Power Up, Calibration, and Registration		
High Speed Data Registration (continued)		
Step		7
Front Panel Indicator		Data Network Registration Complete
1	POWER	On
2	DS	On
3	US	On
4	ONLINE	On
5	ETHERNET 1 - 4	On or Blinking
6	USB	On or Blinking
7	WIRELESS LINK	On or Blinking
8	WIRELESS SETUP	Off

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	ETHERNET 1 - 4	<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 modem ■ Blinks - When only one 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	USB	<ul style="list-style-type: none"> ■ On - When a single device is connected to the USB port and no data is being sent to or from the modem ■ Blinks - When only one USB 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 USB ports
7	WIRELESS LINK	<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 by the user
8	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

Special Conditions

The following chart describes the appearance of the cable modem 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	Slow Blinking 1 time per second
2	DS	Slow Blinking 1 time per second
3	US	Slow Blinking 1 time per second
4	ONLINE	Slow Blinking 1 time per second
5	ETHERNET 1 - 44	Slow Blinking 1 time per second
6	USB	Slow Blinking 1 time per second
7	WIRELESS LINK	Slow Blinking 1 time per second
8	WIRELESS SETUP	Slow Blinking 1 time per second

Notices

Trademarks

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

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

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

Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this guide. We reserve the right to change this guide at any time without notice.

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

Documentation Copyright Notice

Information in this document is subject to change without notice. No part of this document may be reproduced in any form without the express written permission of Cisco Systems, Inc.

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.

For Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer. Use the following table to find the center in your area.

Region	Assistance Centers	Telephone and Fax Numbers
North America South America Central America	Atlanta, Georgia United States	<p>Technical Support</p> <p>For <i>Digital Broadband Delivery System</i> products only, call:</p> <ul style="list-style-type: none"> ■ Toll-free: 1-866-787-3866 ■ Local: 770-236-2200 ■ Fax: 770-236-2488 <p>For all products <i>other than</i> Digital Broadband Delivery System, call:</p> <ul style="list-style-type: none"> ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 ■ Fax: 770-236-2306 <p>Customer Service</p> <ul style="list-style-type: none"> ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 ■ Fax: 770-236-5477
Europe	European Technical Assistance Center (EuTAC), Belgium	Telephone: 32-56-445-197 or 32-56-445-155 Fax: 32-56-445-061
Asia-Pacific	Hong Kong, China	Telephone: 011-852-2588-4745 Fax: 011-852-2588-3139
Australia	Sydney, Australia	Telephone: 011-61-2-8446-5394 Fax: 011-61-2-8446-8015
Japan	Tokyo, Japan	Telephone: 011-81-3-5322-2067 Fax: 011-81-3-5322-1311



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

678.277.1000
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.

© 2010 Cisco and/or its affiliates. All rights reserved.
October 2010

Printed in United States of America
Part Number 4021196 Rev B