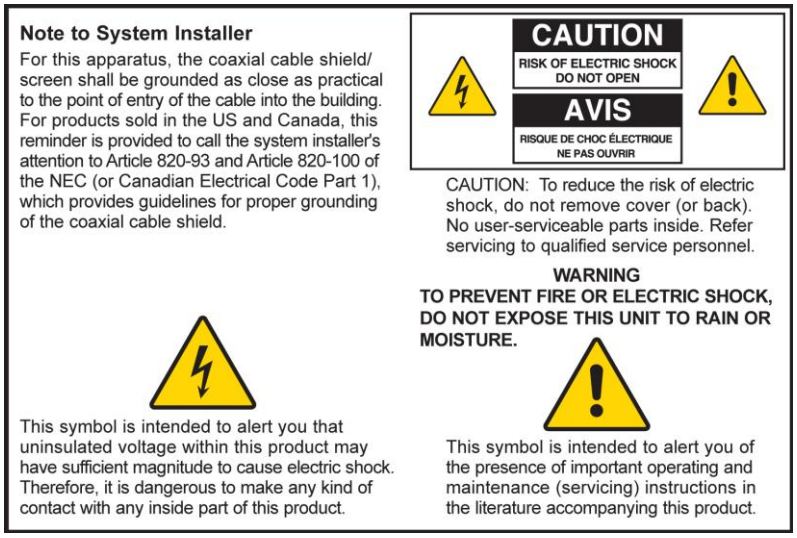
Guía de usuario para el gateway residencial inalámbrico con adaptador telefónico del modelo Cisco DPQ3925 8x4 DOCSIS 3.0

En este documento

INSTRUCCIONES IMPORTANTES DE SEGURIDAD

Aviso a los instaladores

Las instrucciones para las reparaciones que se proporcionan en este aviso son para uso exclusivo del personal de mantenimiento cualificado. Para disminuir el riesgo de descarga eléctrica, no realice ningún tipo de reparación que no se incluya en las instrucciones de funcionamiento a no ser que disponga de la cualificación necesaria para ello.



Notice à l'attention des installateurs de réseaux câblés

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

Mitteilung für CATV-Techniker

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

Mitteilung an den Systemtechniker

Für dieses Gerät muss der 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 Koaxial-kabelschirms festgehalten sind.

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

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

WARNUNG

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

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

Aviso a los instaladores de sistemas CATV

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

Nota para el instalador del sistema

En lo que se refiere a este aparato, el blindaje del cable 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.

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

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

ADVERTENCIA

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

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

20080814_Installer820_Intl

INSTRUCCIONES IMPORTANTES DE SEGURIDAD

1) Lea estas instrucciones.
2) Conserve estas instrucciones.
3) Tenga en cuenta todas las advertencias.
4) Siga todas las instrucciones.
5) No utilice este aparato cerca del agua.
6) Límpielo únicamente con un paño seco.
7) No obstruya los orificios de ventilación. Realice la instalación de acuerdo con las instrucciones del fabricante.
8) No lo instale cerca de fuentes de calor, tales como radiadores, salidas de aire caliente, estufas u otros aparatos (incluidos amplificadores) que generen calor.
9) No actúe en contra de las medidas de seguridad del enchufe polarizado o de conexión a tierra. Un enchufe polarizado cuenta con dos clavijas, una más ancha que la otra. Un enchufe de conexión a tierra tiene dos clavijas, más una tercera de conexión a tierra. La clavija ancha o la tercera clavija se incluye para su seguridad. Si el enchufe suministrado no encaja en la toma de corriente, póngase en contacto con un electricista para cambiar la toma de corriente obsoleta.
10) Evite pisar o apretar el cable de alimentación, especialmente en la zona del enchufe, en las tomas de corriente y en el punto por donde sale del aparato.
11) Utilice únicamente los acoplamientos y accesorios especificados por el fabricante.

12) Utilice únicamente con el carrito, la base, el trípode, la abrazadera o la mesa que especifica el fabricante o que se vende con el aparato. Cuando utilice un carrito, tenga cuidado al mover el conjunto de carrito/aparato para evitar lesiones producidas por un volcado.
13) Desconecte este aparato durante las tormentas eléctricas o cuando no tenga previsto utilizarlo durante periodos de tiempo prolongados.
14) Las reparaciones debe efectuarlas el personal de mantenimiento cualificado. Las reparaciones son necesarias cuando el aparato sufre algún tipo de daño como, por ejemplo, si el cable de alimentación o el enchufe se dañan, si se vierte líquido o caen objetos sobre el aparato, si éste ha estado expuesto a la lluvia o a la humedad, si no funciona correctamente o si ha caído.

Advertencia sobre la fuente de alimentación

La etiqueta de este producto indica la fuente de alimentación correcta para el producto. Conecte este producto únicamente a una toma de corriente eléctrica con el voltaje y la frecuencia que se indican en la etiqueta del producto. Si desconoce el tipo de suministro de alimentación de su casa o de la oficina, consulte al proveedor de servicios o a la compañía eléctrica de su zona.

La entrada de CA de la unidad debe resultar siempre accesible y manejable.

Conecte a tierra el producto

ADVERTENCIA: evite el peligro de descargas eléctricas e incendios. Si este producto se conecta a un cableado coaxial, asegúrese de que el sistema de cables esté conectado a tierra. La conexión a tierra proporciona un grado de protección contra las fluctuaciones de tensión y las cargas estáticas acumuladas.

Proteja el producto de los rayos

Además de desconectar la alimentación de CA de la toma de corriente de la pared, desconecte las entradas de señal.

Compruebe la fuente de alimentación con el indicador de encendido/apagado.

Aunque la luz de encendido/apagado no esté iluminada, es posible que el aparato siga conectado a la fuente de alimentación. La luz puede apagarse al desconectar el aparato, independientemente de si está enchufado a una fuente de alimentación de CA.

Elimine cualquier sobrecarga de la red principal de CA

ADVERTENCIA: evite el peligro de descargas eléctricas e incendios. No sobrecargue la red principal de CA, las tomas, los cables prolongadores o las tomas de corriente integrales. Para productos que funcionan con pilas u otras fuentes de alimentación, consulte las instrucciones de funcionamiento correspondientes.

Tratamiento de la batería recargable optativa

Este producto puede incluir una batería recargable de Litio-Ion para permitir el funcionamiento en modo de espera en caso de una interrupción en la alimentación de CA.

Tenga en cuenta la advertencia siguiente, siga las instrucciones de seguridad y eliminación de la batería que se ofrecen a continuación, y consulte las instrucciones que se incluyen en esta guía para el tratamiento, sustitución y eliminación de la batería.

ADVERTENCIA: existe peligro de explosión si la batería se trata de forma inadecuada o se sustituye incorrectamente. Sustitúyala únicamente por una batería del mismo tipo. No la desmonte ni intente recargarla fuera del equipo. No la aplaste ni perfore, no la arroje al fuego, no reduzca los contactos externos ni la exponga al agua o a otros líquidos. Deseche la batería conforme a las normativas locales y las instrucciones de su proveedor de servicios.

Seguridad de la batería

- Inserte las baterías correctamente. Puede existir peligro de explosión si las baterías no se insertan correctamente.
- No intente recargar las baterías “desechables” o “no reutilizables”.
- Siga las instrucciones que se facilitan para la carga de las baterías “recargables”.
- Sustituya las baterías por otras del mismo tipo o equivalentes a las recomendadas.
- No exponga las baterías a un calor excesivo (por ejemplo, a la luz directa del sol o al fuego).
- No exponga las baterías a temperaturas superiores a 100°C (212°F).

Eliminación de la batería

- Las baterías pueden contener sustancias perjudiciales para el medioambiente.
- Recicle o elimine las baterías conforme a las instrucciones proporcionadas por el fabricante y las normativas locales y nacionales sobre el reciclaje y la eliminación.

- Las baterías pueden contener perclorato, una sustancia reconocida como peligrosa, por lo que es posible que se requiera un tratamiento y una eliminación especial para este producto. Si desea más información sobre el perclorato y las prácticas recomendables para la gestión de sustancias que contienen perclorato, consulte www.dtsc.ca.gov/hazardouswaste/perchlorate

Proporcione ventilación y elija una ubicación

- Retire todo el material de embalaje antes de conectar el producto a la alimentación eléctrica.
- No coloque este aparato encima de la cama, el sofá, alfombras o superficies similares.
- No coloque este aparato encima de una superficie inestable.
- No instale este aparato en un lugar cerrado como una librería o una estantería, a menos que ofrezca ventilación suficiente.
- No coloque otros dispositivos de ocio (tales como reproductores de vídeo o DVD), lámparas, libros, floreros con líquido ni otros objetos encima de este producto.
- No obstruya los orificios de ventilación.

Proteja el producto contra la exposición a la humedad y los objetos extraños

ADVERTENCIA: evite el peligro de descargas eléctricas e incendios. No exponga el producto al goteo o rociado de líquidos, lluvia o humedad. No deben colocarse objetos que contengan líquido, tales como floreros, encima de este aparato.

ADVERTENCIA: evite el peligro de descargas eléctricas e incendios. Desenchufe este producto antes de limpiarlo. No utilice limpiadores líquidos ni en aerosol. No utilice un dispositivo de limpieza magnético/estático (aire comprimido) para limpiar este producto.

ADVERTENCIA: evite el peligro de descargas eléctricas e incendios. No inserte nunca objetos por los orificios de este producto. Los objetos extraños pueden provocar cortocircuitos que causen una descarga eléctrica o un incendio.

Advertencias sobre el mantenimiento

ADVERTENCIA: evite las descargas eléctricas. No abra la tapa de este producto. Abrir o quitar la tapa puede exponerle a voltajes peligrosos. Si abre la tapa, la garantía quedará anulada. Este producto no contiene partes que el usuario pueda reparar.

Compruebe la seguridad del producto

Al finalizar cualquier tarea de mantenimiento o reparación de este producto, el técnico de mantenimiento deberá realizar comprobaciones de seguridad para establecer el funcionamiento correcto del producto.

Proteja el producto al moverlo

Desconecte siempre la fuente de alimentación cuando mueva el aparato o conecte o desconecte los cables.

Aviso sobre los equipos telefónicos

Al utilizar los equipos telefónicos, siga siempre las precauciones de seguridad básicas para reducir el riesgo de incendio, descarga eléctrica y lesiones a las personas, incluidas las siguientes:

1. No utilice este producto cerca del agua, por ejemplo, cerca de una bañera, lavabos, fregadero o lavadero, en un sótano húmedo o cerca de una piscina.

2. Procure no utilizar el teléfono (excepto del tipo inalámbrico) durante una tormenta eléctrica, ya que el riesgo de descarga eléctrica es mayor debido a los rayos.

3. No utilice el teléfono para notificar una fuga de gas si este se encuentra cerca de la fuente de la fuga.

PRECAUCIÓN: para reducir el riesgo de incendios, utilice solamente un cable de línea de telecomunicaciones AWG n.º 26 o superior.

GUARDE ESTAS INSTRUCCIONES

20090915_Modem No Battery_Safety

Conformidad con la normativa FCC estadounidense

Este equipo se ha probado y **cumple** los límites de los dispositivos digitales de Clase B, de conformidad con la sección 15 de la normativa de la FCC (del inglés, *Federal Communications Commission*, Comisión Federal de Comunicaciones). Estos límites están diseñados para proporcionar una protección razonable contra interferencias en una instalación residencial. Este equipo genera, utiliza y puede irradiar energía de radiofrecuencia. Si no se instala y utiliza de acuerdo con las instrucciones, puede producir interferencias dañinas en las comunicaciones de radio. No obstante, no hay garantía de que no se produzcan interferencias en una instalación determinada. Si este equipo produce interferencias perjudiciales para la recepción de radio o televisión, lo que se puede comprobar apagando (OFF) y encendiendo (ON) el equipo, se recomienda al usuario que intente corregir las interferencias mediante una o varias de las siguientes medidas:

- Cambie de orientación o posición la antena receptora.
- Aumente la separación entre el equipo y el receptor.
- Conecte el equipo a una toma de corriente de un circuito distinto al que está conectado el receptor.
- Solicite ayuda al proveedor de servicios o a un técnico experto en radio y televisión.

Cualquier cambio o modificación no aprobada expresamente por Cisco Systems, Inc. puede anular el permiso del usuario para utilizar el equipo.

La información contenida en la sección de Declaración de conformidad con la FCC siguiente es un requisito de la FCC y su objetivo es proporcionarle información relativa a la aprobación de este dispositivo por parte de la FCC. *Los números de teléfono citados son exclusivamente para consultas sobre la FCC y no para cuestiones relacionadas con la conexión o el funcionamiento de este dispositivo. Póngase en contacto con su proveedor de servicios si tiene alguna duda con respecto al funcionamiento o la instalación de este dispositivo.*

FC Declaración de conformidad

Este dispositivo cumple con la sección 15 de la normativa FCC. El funcionamiento está sujeto a las dos condiciones siguientes: (1) que el dispositivo no produzca interferencias dañinas y (2) que el dispositivo acepte cualquier interferencia recibida, incluidas aquellas que produzcan un funcionamiento no deseado.

Gateway residencial DOCSIS
Modelo: DPQ3925
Fabricado por:
Cisco Systems, Inc.
5030 Sugarloaf Parkway
Lawrenceville, Georgia 30044 EE. UU.
Teléfono: (+1) 678-277-1120

Normativa EMI de Canadá

Este aparato digital de clase B cumple con el estándar canadiense ICES-003.

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

Frecuencias de doble banda por DFS (del inglés *Dynamic Frequency Selection*, selección de frecuencia dinámica)

Algunas configuraciones de este producto pueden funcionar en las bandas 5150-5250MHz y 5470-5725MHz. Si selecciona un canal en estos intervalos de frecuencias, el producto está limitado a funcionar en el interior únicamente según las instrucciones de la FCC. El uso de este producto en las frecuencias afectadas cuando se encuentre en el exterior no está en conformidad con la normativa y las pautas de la FCC.

Declaraciones de exposición a la RF

Nota: este transmisor no se debe colocar ni utilizar con ninguna otra antena o transmisor. Cuando instale y utilice este equipo, asegúrese de que haya una distancia mínima de 20 cm entre el radiador y su cuerpo.

US (Subida)

Este sistema ha sido evaluado para la exposición de las personas a la RF en relación con los límites ANSI C 95.1 (del inglés *American National Standards Institute*, Instituto de normas nacionales de Estados Unidos). La evaluación se basó en el boletín FCC OET 65C rev 01.01 de conformidad con la Sección 2.1091 y la Sección 15.27. Para mantener la conformidad, la distancia de separación mínima de la antena a cualquier persona debe ser de 20 cm.

Canadá

Este equipo cumple con las restricciones en materia de exposición a radiofrecuencia (RF) establecidas por la IC para un entorno no controlado. Este sistema ha sido evaluado para la exposición de las personas a la RF en relación con los límites del Código de salud 6 de Canadá (2009). La evaluación se basó en la evaluación según RSS-102 Rev 4. Para mantener la conformidad con la normativa, la distancia de separación mínima de la antena a cualquier persona debe ser de 20 cm.

UE

Este sistema ha sido evaluado para la exposición de las personas a la RF en relación con los límites ICNIRP (del inglés *International Commission on Non-Ionizing Radiation Protection*, Comisión internacional sobre la protección contra la radiación no ionizante). La evaluación se basó en el estándar de producto EN 50385 para demostrar la conformidad de las estaciones base para radios y terminales fijos de sistemas de telecomunicaciones inalámbricos con las restricciones básicas o los niveles de referencia relacionados con la exposición de personas a campos electromagnéticos de radiofrecuencia de 300 MHz a 40 GHz. La distancia de separación mínima de la antena a cualquier persona debe ser de 20 cm.

Australia

Este sistema se ha evaluado para la exposición a radiofrecuencia (RF) según la normativa australiana de la protección contra la radiación (Australian Radiation Protection) y según los límites establecidos por la ICNIRP. La distancia de separación mínima de la antena a cualquier persona debe ser de 20 cm.

20100527 FCC DomandIntl

Conformidad con la normativa CE

Declaración de conformidad con la directiva de la UE 1999/5/CE (Directiva RTTE)

Esta declaración solo es válida para configuraciones (combinaciones de software, firmware y hardware) admitidas o suministradas por Cisco Systems para su uso en la UE. El uso de software o firmware no admitido o suministrado por Cisco Systems puede dar lugar a que el equipo ya no ofrezca conformidad con los requisitos preceptivos.

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

Nota: la declaración de conformidad completa de este producto se encuentra en la sección Declaraciones de conformidad e información reglamentaria de la guía de instalación de hardware del producto correspondiente, que está disponible en Cisco.com.

Durante la evaluación del producto según los requisitos de la directiva 1999/5/CE, se han aplicado los siguientes estándares:

- Radio: EN 300 328
- EMC: EN 301 489-1 y EN 301 489-17
- Seguridad: EN 60950 y EN 50385

La marca CE y el identificador clase-2 están adheridos al producto y su embalaje. Este producto se ajusta a las siguientes directivas europeas:

 -1999/5/EC

Restricciones nacionales

Este producto solo se puede utilizar en interiores.

France

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

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

Italy

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

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

Latvia

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

2,4 GHz frekven?u joslas izmantošanai ?rpus telp?m nepieciešama at?auja no Elektronisko sakaru direkcijas. Vair?k inform?cijas: 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).

Antenas

Utilice únicamente la antena suministrada con el producto. 20090312 CE_Gateway

Introducción

Le damos la bienvenida al emocionante mundo de Internet de alta velocidad y servicio de telefonía de alta calidad. El nuevo gateway residencial inalámbrico con adaptador telefónico del modelo Cisco® DPQ3925 DOCSIS® 3.0 es un cable módem que cumple los estándares del sector en relación con la conectividad de datos de alta velocidad junto con un servicio de telefonía digital fiable. El gateway residencial DPQ3925 proporciona prestaciones de gateway de datos y voz, por cable (Ethernet) o inalámbrico, para conectar una variedad de dispositivos en el hogar o en una oficina pequeña. Además, admite el acceso de alta velocidad a servicios de datos y de voz altamente rentables, todo en un único dispositivo. Con un gateway residencial DPQ3925, podrá disfrutar aún más de Internet, de las comunicaciones en casa y en el trabajo, y de una mayor productividad personal.

En esta guía se proporcionan procedimientos y recomendaciones para la colocación, la instalación, la configuración, el funcionamiento y la resolución de problemas del gateway residencial DPQ3925, para el servicio de conexión a Internet de alta velocidad y telefonía digital en el hogar o la oficina. Consulte la sección correspondiente de esta guía para obtener la información específica necesaria para su situación. Póngase en contacto con su proveedor del servicios para obtener más información sobre la suscripción a estos servicios.

Ventajas y funciones

El nuevo gateway residencial DPQ3925 ofrece estas excelentes ventajas y funciones:

- De conformidad con los estándares DOCSIS 3.0, 2.0 y 1.x así como con las especificaciones de PacketCable™ y EuroPacketCable™ para ofrecer rendimiento y fiabilidad de gama alta
- Conectividad a Internet de banda ancha y alto rendimiento, para dinamizar su experiencia en línea
- Adaptador de voz incorporado de dos líneas para telefonía por cable.
- Cuatro puertos Ethernet 1000/100/10BASE-T para proporcionar conectividad con cable
- Punto de acceso inalámbrico 802.11n
- Incluye una o dos baterías internas optativas de Litio-Ion de tipo cartucho para proporcionar una alimentación de refuerzo práctica y de larga duración
- WPS (del inglés *Wi-Fi Protected Setup*, configuración Wi-Fi protegida), incluido un botón que activa WPS para una configuración inalámbrica simplificada y segura.
- Control parental configurable por el usuario, que bloquea el acceso a sitios de Internet no deseados
- La tecnología avanzada de firewall disuade a los piratas informáticos y protege el entorno doméstico contra los accesos no autorizados

- Un diseño compacto y atractivo que permite el funcionamiento vertical, horizontal o montado en la pared
- Codificación en colores de los puertos de interfaz y sus cables correspondientes, para simplificar la instalación y la configuración
- El etiquetado y comportamiento de los indicadores LED de conformidad con DOCSIS-5 proporcionan a usuarios y técnicos un método sencillo para comprobar el estado operativo, y actúan como herramienta de detección y solución de problemas
- Permite las actualizaciones de software automáticas de su proveedor de servicios

Contenido de la caja

Cuando reciba el gateway residencial inalámbrico, compruebe el equipo y los accesorios para verificar que la caja contenga todos los componentes en perfecto estado. La caja contiene los siguientes componentes:

Un gateway residencial DOCSIS DPQ3925

Batería de cartucho de Litio-Ion

Un cable Ethernet (CAT5/RJ-45)

Un CD-ROM

Si falta alguno de estos componentes o está dañado, solicite asistencia a su proveedor de servicios.

Notas:

- Si desea conectar un reproductor de vídeo, un DHCT (del inglés *Digital Home Communications Terminal*, terminal de comunicaciones doméstico digital) o descodificador o un televisor a la misma conexión de cable que el gateway residencial inalámbrico, necesitará un divisor de señal de cable optativo y cables coaxiales de radiofrecuencia (RF) estándar adicionales.
- Los cables y otros equipos necesarios para el servicio de telefonía deben adquirirse por separado. Póngase en contacto con el proveedor de servicios para obtener información acerca de los equipos y cables que necesita para el servicio de telefonía.

Descripción del panel frontal

El panel frontal del gateway residencial dispone de indicadores LED de estado que indican si está funcionando bien y en qué estado se encuentra. Consulte ***Funciones del indicador LED de estado del panel frontal*** (página 103) para obtener más información sobre las funciones del indicador LED de estado del panel frontal.

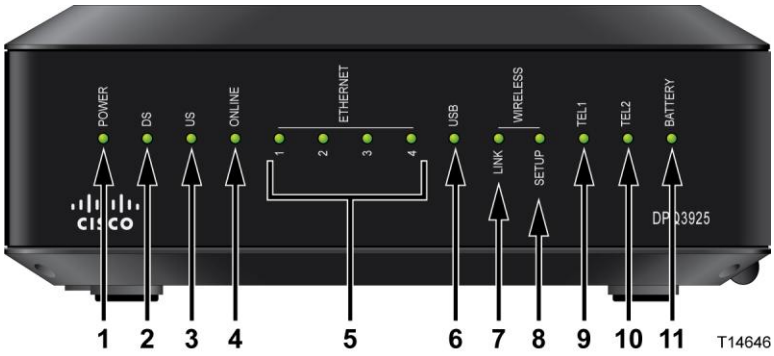


Imagen del modelo DPQ3925

1 **POWER** (Alimentación): (encendido) el gateway residencial inalámbrico recibe alimentación.

2 **DS** (Bajada): (encendido) el gateway residencial inalámbrico está recibiendo datos de la red por cable.

3 **US** (Subida): (encendido) el gateway residencial inalámbrico está enviando datos de la red por cable.

4 **ONLINE** (En línea): (encendido) el gateway residencial inalámbrico se ha registrado en la red y está completamente operativo.

5 **ETHERNET 1 - 4** (Ethernet 1-4): (encendido) hay un dispositivo conectado a uno de los puertos Ethernet. El parpadeo indica que se están transfiriendo datos a través de la conexión Ethernet.

6 **USB**—ON (USB, encendido), hay un dispositivo conectado al puerto USB. El parpadeo indica que se están transfiriendo datos a través de la conexión USB

7 **WIRELESS LINK** (Conexión inalámbrica): (encendido) el punto de acceso inalámbrico está operativo. El parpadeo indica que se están transfiriendo datos a través de la conexión inalámbrica. Si está apagado significa que el usuario ha desactivado el punto de acceso inalámbrico.

8 **WIRELESS SETUP** (Configuración inalámbrica): (apagado, estado normal) la configuración inalámbrica no está activa. El parpadeo indica que el usuario ha activado la configuración inalámbrica para agregar nuevos clientes inalámbricos a la red inalámbrica.

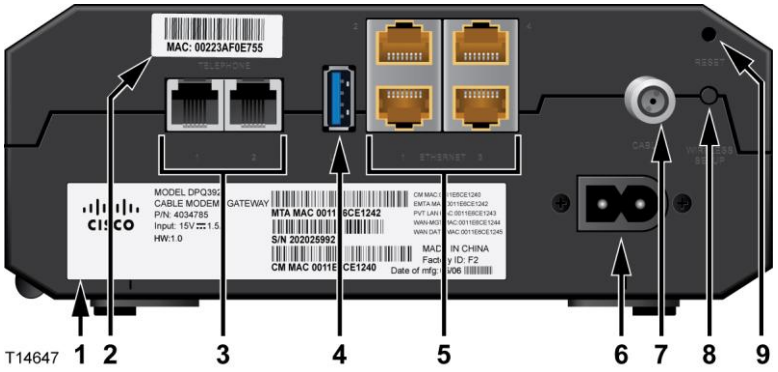
9 **TEL1** (Tel. 1): (encendido) indica que el servicio de telefonía está activado. Parpadea cuando la línea 1 está en uso. Si está apagado, indica que el servicio de telefonía no está activado para TEL 1 (Tel. 1).

10 **TEL2** (Tel. 2): (encendido) indica que el servicio de telefonía está activado. Parpadea cuando la línea 2 está en uso. Si está apagado, indica que el servicio de telefonía no está activado para TEL 2 (Tel. 2).

11 **BATTERY** (Batería): se ilumina cuando la batería está completamente cargada.

Descripción del panel posterior

En las ilustraciones siguientes se muestra la descripción y la función de los componentes del panel posterior del gateway residencial Cisco DPQ3925.



1 **LABEL** (Etiqueta): muestra información técnica relacionada con el gateway.

2 **MAC ADDRESS LABEL** (Etiqueta de dirección MAC): muestra la dirección MAC del gateway residencial.

3 **TELEPHONE 1 y 2**: puertos telefónicos RJ-11 para la conexión de los cables de telefonía residencial a teléfonos convencionales o máquinas de fax.

4 **USB**: conecta a los dispositivos clientes seleccionados.

5 **ETHERNET**: cuatro puertos Ethernet RJ-45 se conectan al puerto Ethernet del PC o la red doméstica.

6 **POWER** (Alimentación): conecta el gateway residencial al cable de alimentación de CA que se suministra con él.

> **PRECAUCIÓN:**
>
> **Evite dañar el equipo. Utilice únicamente el cable de alimentación que se proporciona con el gateway residencial.**

7 **CABLE**: el conector F se conecta a una señal de cable activa del proveedor de servicios.

8 **WIRELESS SETUP** (Configuración inalámbrica): si pulsa este botón, se iniciará la configuración inalámbrica en la que el usuario puede agregar a la red doméstica nuevos clientes inalámbricos compatibles con WPS™ (del inglés Wi-Fi Protected Setup, configuración Wi-Fi protegida).

9 **RESET** (Restablecer): al pulsar este interruptor durante un instante (1-2 segundos) se reinicia el EMTA. Si pulsa el interruptor durante más de diez segundos, primero se restauran todos los parámetros a los valores predeterminados y, a continuación, se reinicia el gateway.

> **PRECAUCIÓN:**
>
> **El botón Reset (Restablecer) solo se utiliza para fines de mantenimiento. No lo utilice a menos que se lo haya indicado su proveedor de servicios de cable o telefonía. Si lo hace, puede perder los parámetros del cable módem que haya seleccionado.**

¿Cuáles son los requisitos de sistema para el servicio a Internet?

Para comprobar si su gateway residencial funciona a pleno rendimiento con el servicio de acceso a Internet de alta velocidad, verifique si todos los dispositivos Internet de su sistema cumplen o sobrepasan los siguientes requisitos mínimos de hardware y software.

Nota: también necesitará una línea de entrada de cable activa y una conexión a Internet.

Requisitos del sistema mínimos para un PC

- PC con un procesador Pentium MMX 133 o superior
- 32 MB de RAM
- Software de navegador web
- Unidad de CD-ROM

Requisitos del sistema mínimos para un Macintosh

- MAC OS 7.5 o superior
- 32 MB de RAM

Requisitos del sistema mínimos para una conexión Ethernet

- PC con sistema operativo Microsoft Windows 2000 (o posterior) con el protocolo TCP/IP instalado, o bien un equipo Apple Macintosh con el protocolo TCP/IP instalado
- Una NIC (del inglés *Network Interface Card*, tarjeta de interfaz de red) Ethernet 10/100/1000BASE-T activa instalada

¿Cómo me suscribo a un servicio de conexión a Internet de alta velocidad y telefonía?

Antes de utilizar el gateway residencial, debe disponer de una cuenta de acceso a Internet de alta velocidad. Si no dispone de una cuenta de acceso a Internet de alta velocidad, deberá establecer una con su proveedor de servicios local. Seleccione una de las opciones de esta sección.

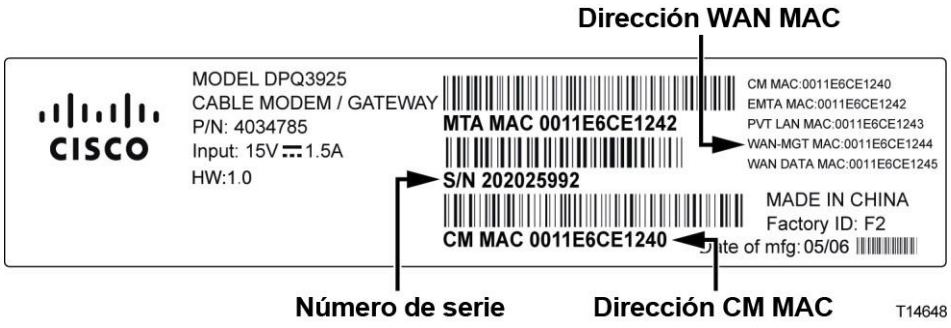
No tengo una cuenta de acceso a Internet de alta velocidad

Si *no* dispone de una cuenta de acceso a Internet de alta velocidad, el proveedor de servicios configurará su cuenta y se convertirá en su Proveedor de servicios de Internet (ISP). El acceso a Internet le permite enviar y recibir correo electrónico, acceder a la World Wide Web, y recibir otros servicios de Internet.

Deberá facilitar al proveedor de servicios la información siguiente:

- Número de serie del módem
- Dirección de control de acceso a los medios (MAC) del módem (CM MAC)
- Otros números de direcciones MAC necesarios

Estos números figuran en una etiqueta de código de barras adherida al gateway residencial. El número de serie consta de varios caracteres alfanuméricos precedidos de **S/N**. La dirección MAC consta de varios caracteres alfanuméricos precedidos de **CM MAC**. En la ilustración siguiente se muestra un ejemplo de etiqueta de código de barras.



Escriba estos números en el espacio que se proporciona aquí.

Número de serie _____

Dirección MAC _____

Ya tengo una cuenta de acceso a Internet de alta velocidad

Si ya tiene una cuenta de acceso a Internet de alta velocidad, facilite al proveedor de servicios el número de serie y la dirección MAC del gateway residencial. Consulte la información de número de serie y dirección MAC que se ha proporcionado anteriormente en esta sección.

Quiero utilizar el servidor de aplicaciones para el servicio de telefonía

También deberá establecer una cuenta telefónica con el proveedor de servicios local si desea utilizar el gateway residencial para el servicio de telefonía. Cuando se ponga en contacto con el proveedor de servicios, es posible que pueda transferir sus números de teléfono existentes, de lo contrario el proveedor de servicios de telefonía por cable le asignará un nuevo número de teléfono para cada línea telefónica activa actual o adicional. Analice estas opciones con su proveedor de servicios de telefonía.

¿Cuál es la mejor ubicación para el gateway residencial DOCSIS?

La ubicación idónea es aquella que ofrezca acceso a las tomas de corriente y otros dispositivos. Piense en la distribución de su hogar u oficina, y consulte a su proveedor de servicios para decidir cuál es la mejor ubicación para el gateway residencial. Lea detenidamente esta guía de usuario antes de decidir la ubicación del gateway residencial.

Tenga en cuenta las recomendaciones siguientes:

- Elija una ubicación cercana a su PC si también va a utilizar el gateway residencial para un servicio de acceso a Internet de alta velocidad.
- Elija una ubicación cercana a una conexión coaxial de RF existente para eliminar la necesidad de una toma coaxial RF adicional.
- Si utiliza solamente uno o dos aparatos telefónicos, coloque el gateway residencial junto a ellos.

  Nota: si utiliza el gateway residencial para proporcionar servicio a varios teléfonos, un técnico profesional puede conectar la unidad al cableado telefónico existente de la casa. Para minimizar los cambios a dicho cableado, es recomendable colocar el gateway residencial cerca de una toma telefónica existente.
- Elija una ubicación relativamente protegida de perturbaciones accidentales o daños potenciales, tales como armarios, sótanos u otras áreas protegidas.
- Elija una ubicación que ofrezca espacio suficiente para apartar los cables del módem sin tensarlos ni doblarlos.
- No debe restringirse la circulación de aire alrededor del gateway residencial.
- Lea detenidamente esta guía de usuario antes de instalar el gateway residencial.

¿Cómo se monta el módem en una pared? (Optativo)

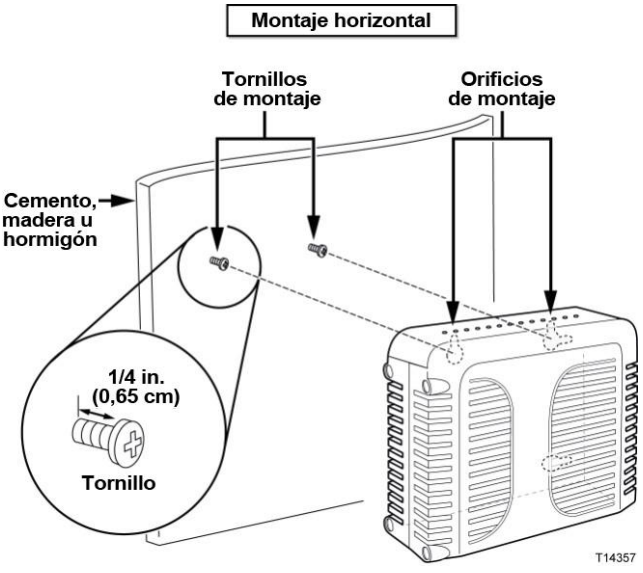
Para montar el gateway residencial en una pared, utilice dos anclajes de pared, dos tornillos y las ranuras de montaje de la unidad. El módem puede montarse de forma vertical u horizontal.

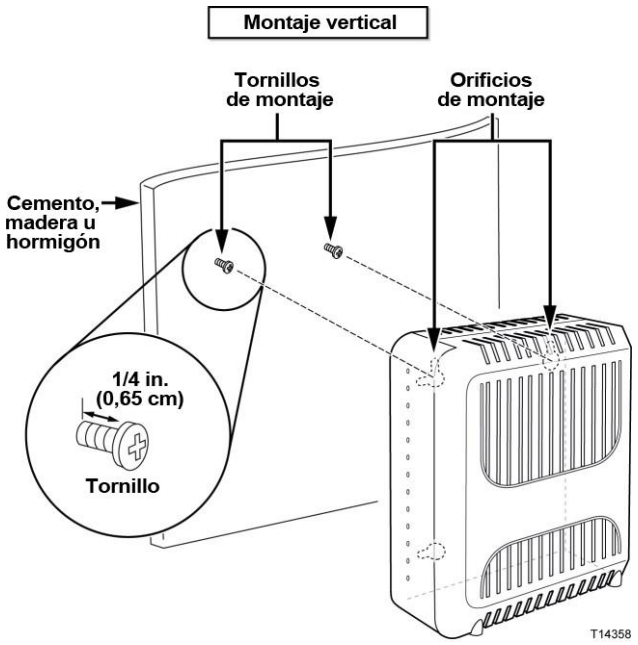
Antes de comenzar

Antes de comenzar, elija un lugar apropiado para el montaje. La pared puede ser de cemento, madera o panel de yeso (Pladur). La ubicación de montaje no debe estar obstruida por ninguno de sus lados, y los cables deben llegar al gateway residencial fácilmente y sin tensarlos. Deje espacio suficiente entre la base del gateway residencial y el suelo o estante que haya por debajo, para permitir el paso de los cables. Asimismo, deje los cables lo suficientemente sueltos como para que el gateway residencial pueda moverse para las tareas de mantenimiento sin desconectar los cables. Verifique también si dispone de los siguientes elementos:

- Dos anclajes de pared para tornillos n.º 8 x 1 pulgada
- Dos tornillos metálicos laminados de cabeza plana n.º 8 x 1 pulgada
- Taladro con una broca de 3/16 pulgadas para madera o albañilería, según la composición de la pared
- En las páginas siguientes se ofrece una copia de las ilustraciones del montaje en pared.

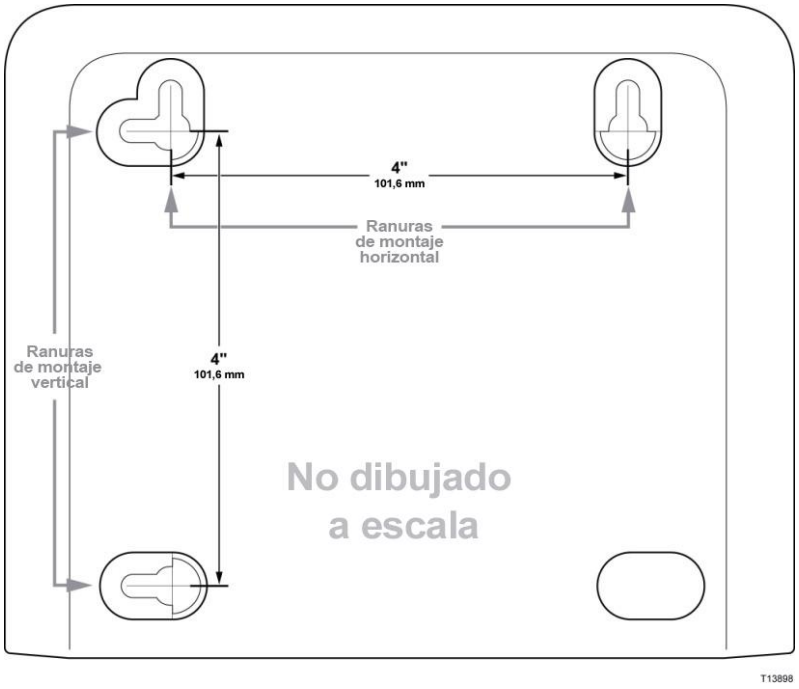
Monte el módem como se indica en una de las ilustraciones siguientes.





Ubicación y dimensiones de las ranuras de montaje en pared

En la ilustración siguiente se muestran la ubicación y las dimensiones de las ranuras de montaje en pared en la base del módem. Utilice la información de esta página como guía para montar el módem en la pared.



Montaje del gateway residencial en la pared

1. Con un taladro de broca de 3/16 pulgadas, perfore dos orificios a la misma altura y a una distancia de 10,16 cm entre sí.

   Nota: en el gráfico anterior se ilustra la ubicación de los orificios de montaje en la parte posterior del gateway residencial.

2. ¿Va a montar el gateway residencial en un panel de yeso o una superficie de hormigón en la que haya algún montante de madera?

   - Si la respuesta es **sí**, vaya al paso 3.
   - Si la respuesta es **no**, inserte los pernos de anclaje en la pared e instale en ellos los tornillos de montaje; deje un espacio de 0,64 cm aproximadamente entre la cabeza del tornillo y la pared. A continuación, vaya al paso 4.

3. Instale los tornillos de montaje en la pared; deje un espacio de 0,64 cm aproximadamente entre la cabeza del tornillo y la pared. A continuación, vaya al paso 4.
4. Compruebe que no haya cables conectados al gateway residencial.
5. Eleve el gateway residencial hasta su posición. Deslice el extremo grande de ambas ranuras de montaje (situadas en la parte posterior del gateway residencial) por encima de los tornillos de montaje y deslice el gateway residencial hacia abajo hasta que el extremo estrecho de la ranura en ojo de cerradura entre en contacto con el eje del tornillo.

   Importante: compruebe que los tornillos de montaje sujeten firmemente el gateway residencial antes de soltar la unidad.

¿Cuáles son los requisitos para el servicio de telefonía?

Número de dispositivos telefónicos

Los conectores telefónicos RJ-11 del gateway residencial pueden proporcionar servicio de telefonía a varios teléfonos, máquinas de fax y módems analógicos.

El número máximo de dispositivos telefónicos que se conectan a cada puerto RJ-11 está limitado por la carga de timbre total de los dispositivos telefónicos conectados. Muchos dispositivos telefónicos llevan la marca REN (del inglés *Ringer Equivalent Number*, número de equivalencia de dispositivo de llamada). Cada puerto telefónico del gateway residencial admite una carga máxima de 5 REN.

La suma de la carga REN de todos los dispositivos telefónicos conectados a cada puerto no puede superar 5 REN.

Tipos de dispositivos telefónicos

Puede utilizar dispositivos telefónicos que no llevan la etiqueta del número REN. Sin embargo, el número máximo de dispositivos telefónicos conectados no podrá calcularse con precisión. En el caso de dispositivos telefónicos sin etiquetas, se deberán conectar todos los dispositivos y se deberá realizar una prueba de la señal de llamada antes de agregar dispositivos adicionales. Si se conectan demasiados dispositivos telefónicos y la señal de llamada ya no se oye, deberá quitar los dispositivos telefónicos hasta que la señal funcione correctamente.

Los teléfonos, las máquinas de fax y otros dispositivos telefónicos deben utilizar las dos patillas centrales de los conectores RJ-11 para conectarse a los puertos telefónicos del gateway residencial. Algunos teléfonos utilizan otras patillas de los conectores RJ-11 y requieren el uso de adaptadores para funcionar.

Requisitos de marcación

Todos los teléfonos deben estar configurados para la marcación DTMF (del inglés *Dual-Tone Multifrequency*, multifrecuencia de doble tono). Los proveedores locales normalmente no permiten la marcación por pulsación.

Requisitos del cableado telefónico

El gateway residencial admite la conexión al cableado telefónico interior, así como la conexión directa a un teléfono o una máquina de fax. La distancia máxima desde la unidad hasta el dispositivo telefónico más lejano no debe ser superior a 300 metros. Utilice cables telefónicos de par trenzado de calibre 26 o superior.

Importante: la conexión a una red doméstica de cableado telefónico existente o nueva instalada permanentemente debe realizarla un instalador cualificado.

¿Cómo se conecta el gateway para el servicio de conexión a Internet y telefonía?

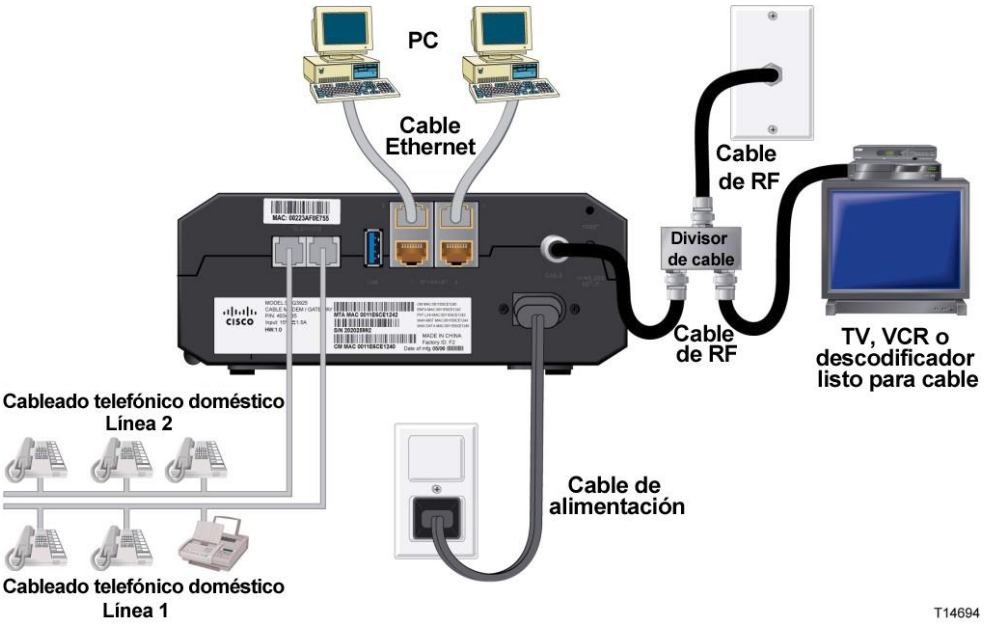
Puede utilizar el gateway residencial para proporcionar servicio telefónico y acceso a Internet. Además, puede compartir la conexión a Internet con otros dispositivos web de su casa u oficina. Compartir una conexión con varios dispositivos se denomina conexión en red.

Conexión e instalación de dispositivos de Internet

La instalación puede realizarla un profesional. Pida asistencia a su proveedor de servicios local.

Conexión de los dispositivos

En el diagrama siguiente se ilustra una de las diversas opciones disponibles para trabajar en red.



Conexión del gateway residencial para el servicio de datos de alta velocidad y telefonía

El siguiente procedimiento de instalación garantiza la configuración correcta del gateway residencial.

1 Elija una ubicación adecuada y segura para la instalación del gateway residencial (cerca de una fuente de alimentación, una conexión de cables activa, su PC si piensa utilizar la conexión a Internet de alta velocidad y las líneas de teléfono si piensa utilizar los servicios de VoIP).

ADVERTENCIA:

- **Para evitar daños personales, siga las instrucciones de instalación en el mismo orden que se indica.**
- **Para evitar posibles daños en el equipo, desconecte todos los demás servicios de telefonía antes de conectar el cable módem a los mismos cables.**
- **Los puertos telefónicos del gateway residencial pueden contener peligrosos voltajes eléctricos y dichos voltajes pueden también estar presentes en el cableado conectado, incluidos los cables Ethernet, los cables telefónicos y el cable coaxial.**
- **Los cables y las conexiones de telefonía deben estar aislados correctamente para evitar descargas eléctricas.**
- **Las conexiones telefónicas a una red doméstica de cableado telefónico instalada debe realizarlas un instalador cualificado. Es posible que el proveedor de servicios de telefonía ofrezca una instalación y conexión profesionales a la red doméstica de cableado telefónico. Este servicio puede estar sujeto a cargos adicionales.**
- **El cableado y las conexiones deben estar correctamente aislados para evitar descargas eléctricas.**
- **Desconecte la alimentación del gateway residencial antes de conectarlo con cualquier dispositivo.**

2 Apague su PC y otros dispositivos de trabajo en red; a continuación, desenchúfelos de la fuente de alimentación.

3 Conecte el cable coaxial de RF activo de su proveedor de servicios al conector coaxial con la etiqueta **CABLE** de la parte posterior del gateway residencial.

Nota: para conectar una TV, DHCT, descodificador o VCR desde la misma conexión de cable, deberá instalar un divisor de señal de cable (no incluido). Consulte siempre a su proveedor de servicios antes de utilizar un divisor, ya que puede degradar la señal.

4 Conecte su PC al gateway inalámbrico con cualquiera de los siguientes métodos.

- **Conexión Ethernet:** busque el cable Ethernet amarillo, conecte uno de sus extremos al puerto Ethernet de su PC y el otro extremo al puerto **ETHERNET** amarillo de la parte posterior del gateway inalámbrico.

  Nota: para instalar un número de dispositivos Ethernet mayor que los puertos suministrados en el gateway residencial, utilice un switch Ethernet multipuertos externo.

- **Inalámbrico:** asegúrese de que el dispositivo inalámbrico esté encendido. Deberá asociar el dispositivo inalámbrico al gateway inalámbrico una vez que éste último esté operativo. Siga las indicaciones suministradas con el dispositivo inalámbrico para la asociación a un punto de acceso inalámbrico.

  En la sección ***Configuración de los parámetros de conexión inalámbrica*** de esta guía de usuario (página 41) encontrará más información sobre la configuración predeterminada del gateway inalámbrico.

5 Conecte un extremo de un cable puente telefónico (no suministrado) a una toma telefónica de su casa o a un teléfono o una máquina de fax. A continuación, conecte el otro extremo al puerto **TELEPHONE** (teléfono) RJ-11 correspondiente situado en la parte posterior del gateway residencial. Los puertos telefónicos son de color gris claro y llevan las etiquetas 1/2 y 2, o 1 y 2 en función de la región geográfica en la que se utiliza el gateway residencial.

Notas:

- Asegúrese de conectar el servicio de telefonía al puerto RJ-11 correcto. Para un servicio de telefonía de una sola línea, conéctese al puerto 1/2 o 1.
- En Norteamérica, los gateways residenciales tienen una capacidad multilínea en el puerto telefónico RJ-11 con la etiqueta 1/2. La línea 1 se encuentra en las clavijas 3 y 4 del puerto 1/2 y la línea 2 se encuentra en las clavijas 2 y 5. En Europa, los gateways residenciales solo admiten una línea por puerto. La línea 1 se encuentra en el puerto 1 y la línea 2 en el puerto 2.
- Es posible que los teléfonos que requieren conectores eléctricos distintos de RJ-11 necesiten un adaptador externo (que se vende por separado).

6 Localice el cable de alimentación de CA suministrado con el gateway residencial. Inserte un extremo del cable de alimentación en el conector de CA de la parte posterior del gateway residencial. Enchufe el cable de alimentación de CA en una toma de CA para encender el gateway residencial. El gateway residencial realizará una búsqueda automática para localizar la red de datos de banda ancha e iniciar sesión en ella. Este proceso puede durar de 2 a 5 minutos. El módem estará listo para usar cuando los LED **POWER** (Alimentación), **DS**, **US** y **ONLINE** (En línea) del panel frontal del gateway residencial hayan dejado de parpadear y permanezcan encendidos de forma continua.

7 Enchufe y encienda su PC y demás dispositivos de la red doméstica. El indicador LED **LINK** (Enlace) del gateway residencial correspondiente a los dispositivos conectados debe estar encendido o parpadear.

8 Una vez que el gateway residencial esté en línea, casi todos los dispositivos Internet tendrán acceso inmediato a Internet.

Nota: si su PC no tiene acceso a Internet, consulte las ***Preguntas más frecuentes*** (en la página 97) para obtener más información sobre cómo configurar el PC para TCP/IP. Para los dispositivos Internet que no sean el PC, consulte la sección de configuración de dirección DHCP o IP de la guía de usuario o el manual de funcionamiento de los dispositivos.

¿Cómo se mantiene la batería?

El módem incluye una batería recargable de Litio-Ion para permitir el funcionamiento en modo de espera en caso de una interrupción en la alimentación de CA. Puede sustituir la batería sin necesidad de utilizar herramientas.

ADVERTENCIA:

Las baterías recargables de gran capacidad completamente cargadas deben manipularse con cuidado. Realice la sustitución sólo con la batería recomendada por el fabricante. No la desmonte ni intente recargarla fuera del sistema. La batería no se debe aplastar, perforar, arrojar al fuego para desecharse, acortar sus contactos externos, exponerse a altas temperaturas ni sumergirse en agua u otros líquidos. Deseche la batería conforme a las normativas locales y las instrucciones de su proveedor de servicios.

Carga de la batería

La batería comienza a cargarse automáticamente en cuanto se conecta el módem a la toma de alimentación de CA. La primera vez que conecta el módem, el indicador LED de estado **POWER** se ilumina.

Importante: la batería puede tardar hasta 24 horas en cargarse completamente.

Uso del módem sin batería

Si lo desea, puede utilizar el módem sin batería. Si necesita extraer la batería, siga el procedimiento que se describe en ***Extracción y sustitución de la batería*** (en la página 31).

Importante: si decide utilizar el módem sin batería, corre el riesgo de perder el servicio de telefonía en caso de interrupción en el suministro eléctrico.

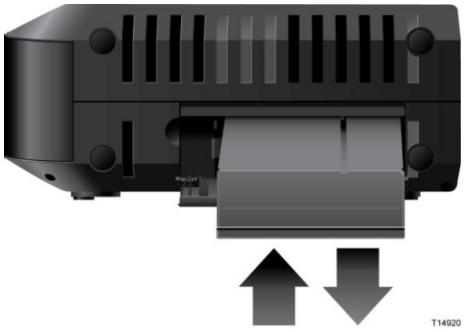
Sustitución de la batería

En circunstancias normales, la batería debería durar varios años. El indicador LED de estado **BATTERY** (Batería) se apaga para indicar que se debe sustituir la batería pronto. Póngase en contacto con su proveedor de servicios para obtener baterías de recambio y para solicitar instrucciones para su eliminación.

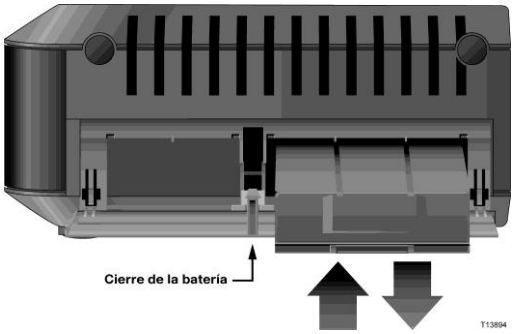
Nota: siga los pasos que se describen en ***Extracción y sustitución de la batería*** (en la página 31) para extraer y sustituir la batería.

Ubicación de la batería

Tal y como se muestra en las siguientes ilustraciones, el compartimento de la batería se sitúa en el panel del lado derecho de ambos tipos de alojamiento DPQ3925.



Tipo de alojamiento 1



Tipo de alojamiento 2

Pasos previos a la extracción y sustitución de la batería

Antes de extraer y sustituir la batería, consulte la siguiente información.

- Puede extraer y sustituir la batería sin desconectar la fuente de alimentación de CA.
- La batería puede tardar hasta 24 horas en cargarse por completo.
- Deseche la batería conforme a las normativas locales y las instrucciones de su proveedor de servicios.

Extracción y sustitución de la batería (tipo de alojamiento 1)

1. Abra la puerta de la batería accionando el cierre de la puerta de la batería situada en la parte lateral de la unidad.
2. Agarre la lengüeta de extracción de plástico de la batería y deslice con cuidado la batería hacia adelante para extraerla del compartimento.
3. Inserte una nueva batería en el compartimento.
4. Cierre la puerta del compartimento de la batería.

Extracción y sustitución de la batería (tipo de alojamiento 2)

1. Abra la puerta de la batería presionando la puerta donde se indica en la parte lateral de la unidad.
2. Deslice el desbloqueo de la batería gris dentro del compartimiento hacia arriba para liberar el cierre de la batería.
3. Agarre la lengüeta de extracción de plástico de la batería y deslice con cuidado la batería hacia adelante para extraerla del compartimento.
4. Inserte una nueva batería en el compartimento.

   Cierre la puerta del compartimento de la batería. El cierre de la batería se bloqueará automáticamente.

¿Cómo se configura el gateway residencial DOCSIS?

Para configurar el gateway residencial, primero debe acceder a las páginas de configuración de WebWizard. Esta sección contiene la información y los procedimientos detallados para acceder a las páginas de WebWizard y configurar el gateway residencial para que funcione correctamente. Esta sección también ofrece ejemplos y descripciones de cada página de configuración de WebWizard. Utilice las páginas de WebWizard para adaptar el gateway residencial a sus necesidades en lugar de usar los parámetros predeterminados. Las páginas de WebWizard de esta sección están organizadas en el orden indicado en la página **Setup** (Configuración).

Importante: las páginas de WebWizard y los ejemplos de esta sección se ofrecen solo a título informativo. Sus páginas pueden diferir de las páginas incluidas en esta guía. Las páginas mostradas en esta guía también representan los valores predeterminados del dispositivo.

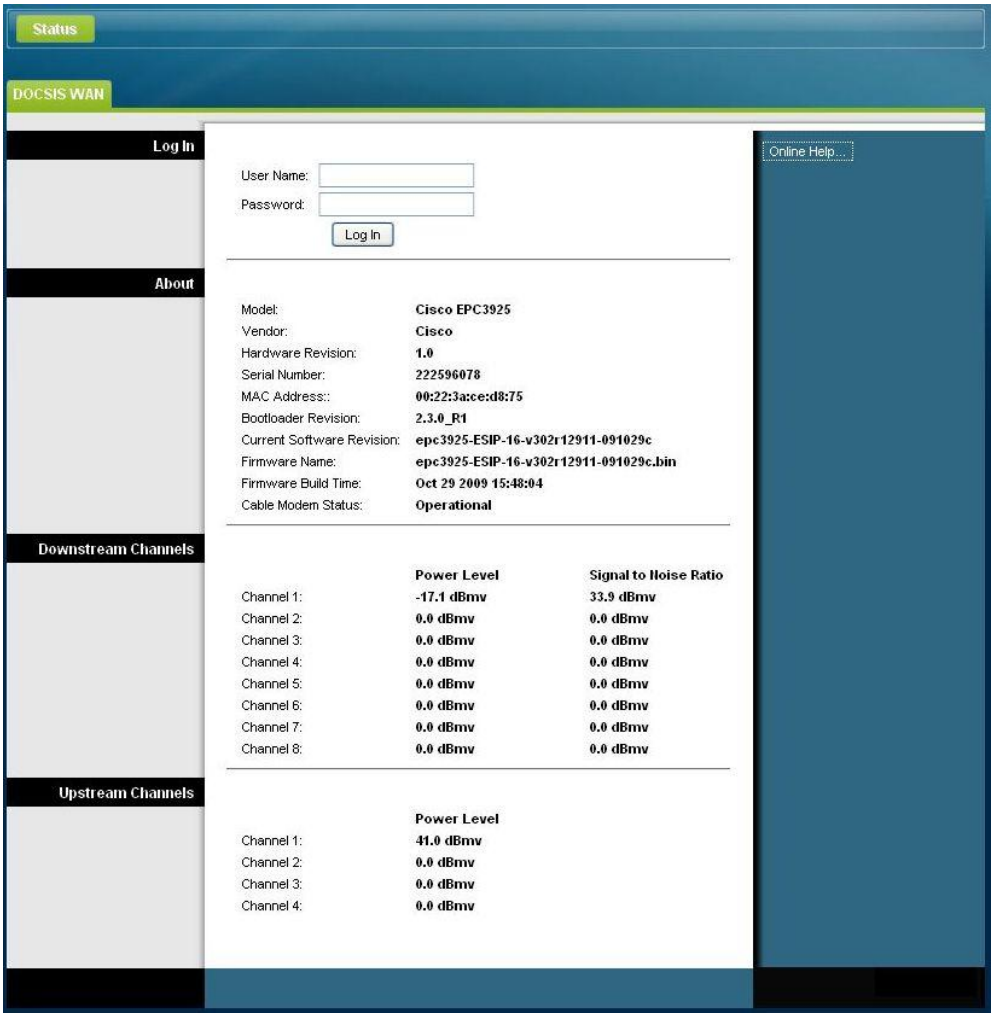
Nota: si no conoce los procedimientos de configuración de red detallados en esta sección, póngase en contacto con su proveedor de servicios antes de realizar cambios en los parámetros predeterminados del gateway residencial.

Conectarse al gateway por primera vez

La configuración predeterminada del gateway utiliza la dirección IP 192.168.0.1. Si ha conectado el gateway y ha configurado el equipo correctamente, siga los pasos que se describen a continuación para conectarse al gateway como administrador.

1 En su PC, abra el navegador web que prefiera.

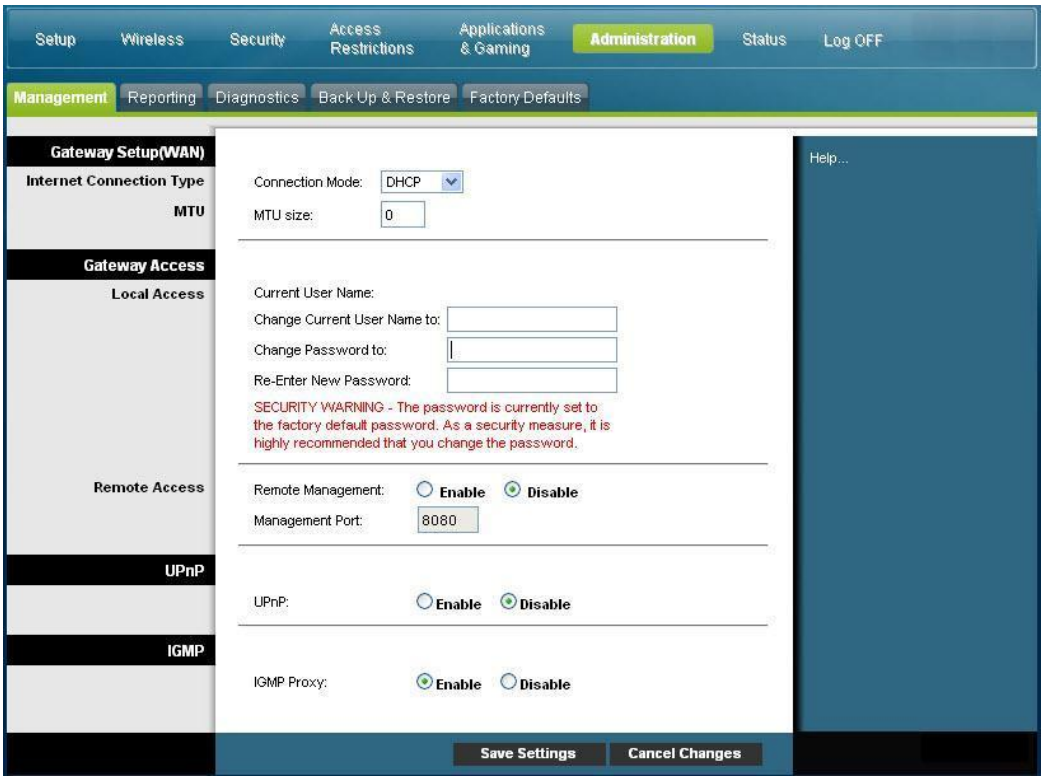
2 En el campo de dirección, introduzca la siguiente dirección IP: **192.168.0.1**. Se abrirá una página de inicio de sesión Status DOCSIS WAN (Estado de DOCSIS WAN) similar a la siguiente.



3 En la página Status DOCSIS WAN (Estado de DOCSIS WAN), deje en blanco los campos User Name (Nombre de usuario) y Password (Contraseña) y pulse **Log In** (Iniciar sesión). El gateway se abre con una página Administration Management (Administración > Gestión) en primer lugar. Puede utilizar la página Administration Management (Administración > Gestión) para cambiar su nombre de usuario y su contraseña.

Ya está conectado al gateway. Puede seleccionar cualquiera de las páginas web de configuración y gestión. Sin embargo, se le ha remitido a la página Administration Management (Administración > Gestión) como recordatorio para que configure una contraseña nueva.

Importante: le recomendamos que configure una nueva contraseña para protegerse de posibles ataques por Internet que busquen dispositivos que funcionen con nombres de usuario o contraseñas muy conocidos o predeterminados.



4 En la página Administration Management (Administración > Gestión), cree un nombre de usuario y una contraseña, y después pulse **Save Settings** (Guardar parámetros). Una vez guardados los parámetros de User Name (Nombre de usuario) y Password (Contraseña) en la página Administration Management (Administración > Gestión), se abre la página Setup Quick Setup (Configuración > Configuración rápida).

Importante: si lo prefiere, deje en blanco el campo de contraseña (valor predeterminado). Sin embargo, si no cambia su nombre de usuario y contraseña, será remitido a la página Administration Management (Administración > Gestión) cada vez que acceda al gateway. Esto sirve de recordatorio para configurar una contraseña personalizada.

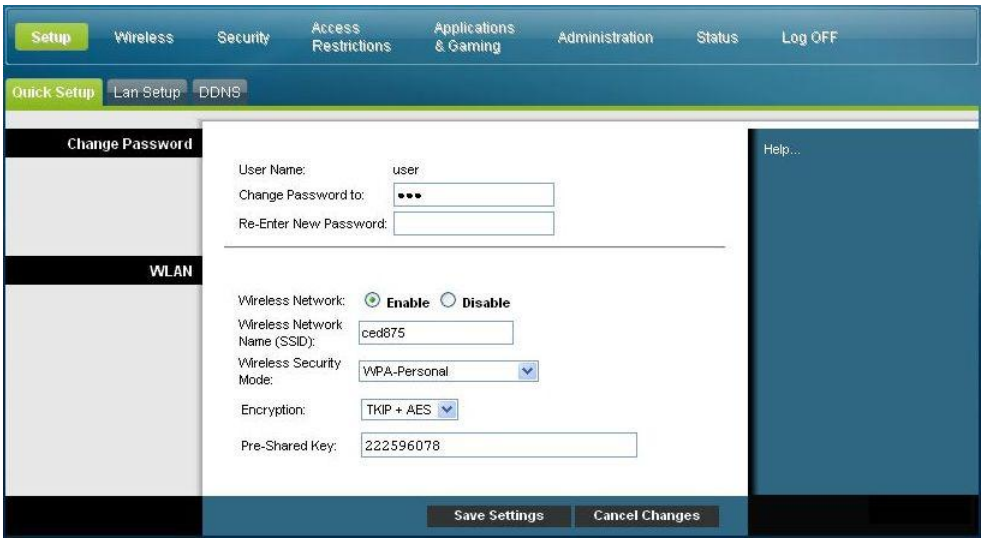
Una vez que haya personalizado su contraseña, los inicios de sesión posteriores le llevarán directamente a la página Setup Quick Setup (Configuración > Configuración rápida).

5 Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Setup > Quick Setup (Configuración > Configuración rápida)

La página Setup Quick Setup (Configuración > Configuración rápida) es la primera página que se abre una vez que se conecta al gateway. Puede utilizar los parámetros de esta página para cambiar de contraseña y configurar la WLAN.

Importante: los parámetros de esta página son exclusivos para su dispositivo. Si lo prefiere, no necesita modificar los parámetros de esta página. Estos parámetros predeterminados son lo único que necesita para utilizar una red inalámbrica segura.



Configuración de parámetros rápidos

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de red para el dispositivo. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Cambiar contraseña	**User Name (Nombre de usuario)** Muestra el nombre de usuario del operador conectado en ese momento. **Change Password to (Cambiar contraseña por)** Le permite cambiar la contraseña. **Re-Enter New Password (Volver a introducir nueva contraseña)** Le permite volver a introducir la nueva contraseña. Debe introducir la misma contraseña que la especificada en el campo **Change Password to (Cambiar contraseña por)**

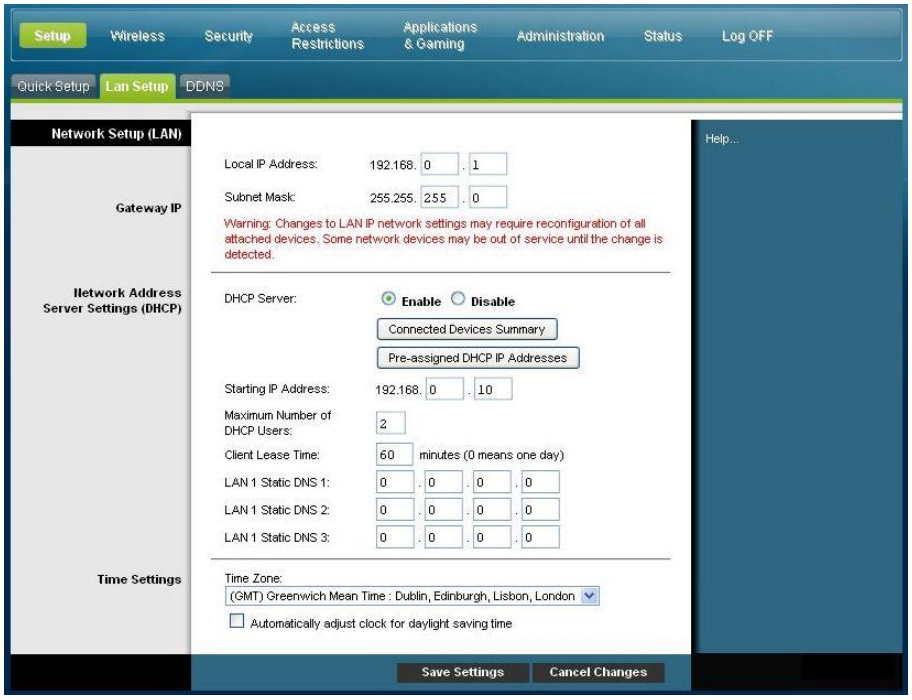
Sección	Descripción de campos
WLAN	**Wireless Network (Red inalámbrica)** Le permite activar o desactivar la red inalámbrica. Seleccione la opción deseada: ■ Enable (Activar) ■ Disable (Desactivar) **Wireless Network Name (SSID) (Nombre de la red inalámbrica, SSID)** Le permite introducir un nombre para la red inalámbrica o utilizar el valor predeterminado. El valor que introduzca aquí se verá en los PC y otros dispositivos clientes inalámbricos, como el nombre de la red inalámbrica. **Nota:** por lo general, el Identificador de conjunto de servicios (SSID) predeterminado es igual a los 6 últimos caracteres de la Dirección CM MAC. La Dirección CM MAC se encuentra en la etiqueta de clasificación adherida al gateway inalámbrico. **Wireless Security Mode (Modo de seguridad inalámbrica)** Le permite seleccionar un modo de seguridad inalámbrica para ayudarle a proteger su red. Si selecciona **Disable** (Desactivar), la red inalámbrica no estará protegida y cualquier dispositivo inalámbrico dentro del alcance podrá conectarse a ella. Consulte ***Seguridad inalámbrica*** (página 45) para ver una descripción detallada de los modos de seguridad inalámbrica. **Nota:** el modo de seguridad inalámbrica predeterminado es WPA (del inglés *Wi-Fi Protected Access*, acceso Wi-Fi protegido) o WPA2-Personal. **Encryption (Cifrado)** Le permite seleccionar un nivel de cifrado en función del modo de seguridad inalámbrica que elija. Consulte ***Seguridad inalámbrica*** (página 45) para ver una descripción detallada del cifrado. **Pre-Shared Key (Clave precompartida)** Es la clave precompartida del dispositivo. La clave puede constar de 8 a 63 caracteres. La clave precompartida predeterminada es igual al número de serie de 9 dígitos de su gateway. La Dirección CM MAC se encuentra en la etiqueta de clasificación adherida al gateway inalámbrico. **Nota: su proveedor de servicios puede proporcionarle una tarjeta de configuración inalámbrica con una información de SSID y de configuración de seguridad inalámbrica para su red doméstica distinta de la descrita anteriormente.**

Setup > Lan Setup (Configuración > Configuración Lan)

La página Setup Lan Setup (Configuración > Configuración Lan) le permite configurar los parámetros de la red de área local (LAN) de su hogar. Estos parámetros incluyen el intervalo de direcciones IP que definen a la propia LAN así como la forma de asignar (automáticamente por DHCP o manualmente) las direcciones a medida que se agreguen nuevos dispositivos a la red.

Importante: a menos que esté familiarizado con la administración de direcciones IP, le recomendamos que no cambie estos parámetros. Si modifica estos valores incorrectamente, puede perder el acceso a Internet.

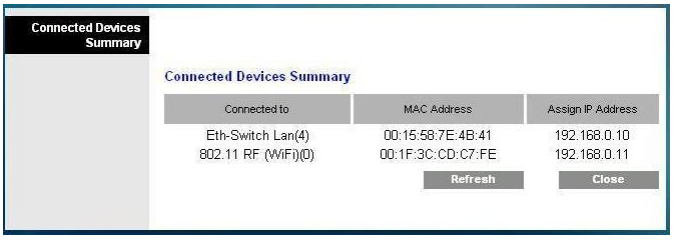
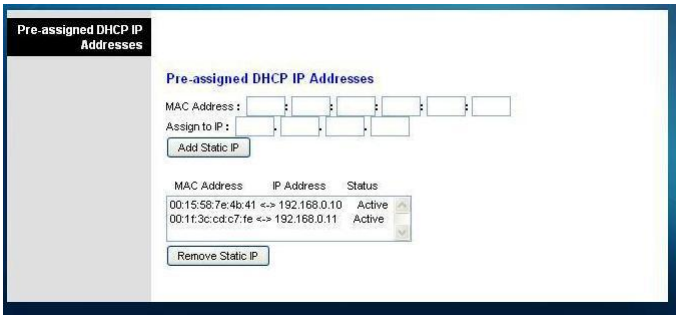
Seleccione la ficha **Lan Setup** (Configuración Lan) para abrir la página Setup Lan Setup (Configuración > Configuración Lan).



Configuración de los parámetros de red

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de red para el gateway residencial. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Configuración de la red (LAN) **Gateway IP (IP del gateway)**	**Local IP Address (Dirección IP local)** La dirección IP básica de la LAN doméstica privada. La dirección IP predeterminada de la LAN es 192.168.0.1. **Subnet Mask (Máscara de subred)** La máscara de subred de su LAN

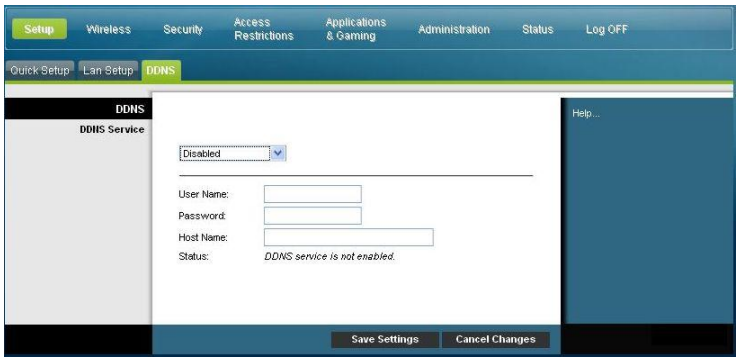
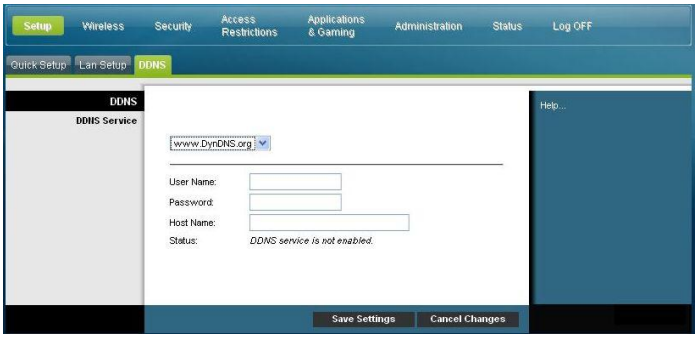
Sección	Descripción de campos
Network Address Server Settings (DHCP) (Parámetros de servidor de direcciones de red, DHCP)	**DHCP Server (Servidor DHCP)** Le permite activar o desactivar el servidor DHCP en el gateway residencial. El servidor DHCP se utiliza para asignar automáticamente las direcciones IP a los dispositivos cuando se acoplan a la red doméstica. ■ **Página Connected Devices Summary (Resumen de dispositivos conectados)** Pulse **Connected Devices Summary** (Resumen de dispositivos conectados) en la página Lan Setup (Configuración de Lan). Se abre la página Connected Devices Summary (Resumen de dispositivos conectados). Esta página es una ventana emergente que muestra la dirección MAC y la dirección IP de los dispositivos conectados al gateway residencial.  ■ **Página Pre-assigned DHCP IP Addresses (Direcciones IP DHCP preasignadas)** Pulse **Pre-assigned DHCP IP Addresses** (Direcciones IP DHCP preasignadas) en la página Lan Setup (Configuración de Lan). Se abre la página Pre-assigned DHCP IP Addresses (Direcciones IP DHCP preasignadas). Esta página le permite asignar una dirección IP específica a un PC u otro dispositivo cuando se solicita una dirección IP utilizando DHCP. Con esta función solo se pueden reservar direcciones dentro del intervalo del grupo de direcciones DHCP del gateway.  **Notas:** – El botón **Add Static IP** (Agregar IP estática) agrega la dirección IP estática a la lista de direcciones IP preasignadas. – El botón **Remove Static IP** (Quitar IP estática) quita la dirección IP estática de la lista de direcciones IP preasignadas.

Sección	Descripción de campos
	Starting IP Address (Dirección IP inicial) Muestra la dirección inicial que utiliza el servidor DHCP incorporado para distribuir las direcciones IP de LAN privada. Debido a que la dirección IP predeterminada del gateway es **192.168.0.1**, la dirección IP inicial debe ser **192.168.0.2** o superior, pero menor que **192.168.0.253**. La dirección IP inicial predeterminada es **192.168.0.10**.
	Maximum Number of DHCP Users (Número máximo de usuarios de DHCP) Introduzca el número máximo de usuarios a los que el servidor DHCP puede asignar direcciones IP para utilizar en la LAN. Este número no puede ser mayor que 254 menos la dirección IP inicial descrita anteriormente. **Client Lease Time (Tiempo de concesión del cliente)** El tiempo durante el cual permanece válida una dirección IP. Su PC y otros dispositivos que utilizan DHCP para obtener las direcciones IP renuevan automáticamente las concesiones de dirección IP. Si se deja caducar una concesión, la dirección IP volverá al grupo de direcciones IP disponibles que pueden ser asignadas por el servidor DHCP conforme se agreguen dispositivos nuevos a su red. El ajuste predeterminado es 60 minutos cuando el gateway está en línea. **LAN Static DNS (Domain Name Server) 1-3 (Servidor de nombres de dominio estático de LAN)** El PC u otros dispositivos clientes utilizan el servidor de nombres de dominio (DNS) para conocer la dirección IP pública asociada a una URL o la dirección de un sitio web basada en un nombre. Puede especificar manualmente los servidores DNS que deben utilizar los dispositivos de su red por las direcciones IP introducidas de esos servidores en estos campos. De lo contrario, el gateway reenviará la información del servidor DNCS de su proveedor de servicio automáticamente. El ajuste predeterminado es dejar estos campos en blanco.
Time Settings (Parámetros de hora)	**Time Zone (Zona horaria)** Permite seleccionar la zona horaria correspondiente a su ubicación. Si su ubicación aplica el horario de verano, seleccione **Automatically adjust clock for daylight saving time (Ajustar automáticamente el reloj para el horario de verano)**.

Setup (Configuración) > DDNS

El Servicio dinámico de nombres de dominios (DDNS) proporciona al gateway residencial (que puede tener una dirección IP variable) un nombre de host o URL que las aplicaciones de red pueden resolver mediante consultas a DNS estándar. El DDNS resulta útil cuando aloja su propio sitio web, servidor FTP u otro servidor detrás del dispositivo. Antes de utilizar esta función, debe suscribirse al servicio DDNS.

Seleccione la ficha **DDNS** para abrir la página Setup DDNS (Configuración DDNS).

Sección	Descripción de campos
DDNS Service (Servicio DDNS)	**Desactivación de DDNS** (configuración predeterminada) Para desactivar el DDNS, seleccione **Disabled** (Desactivado) de la lista desplegable y pulse **Save Settings** (Guardar parámetros).  **Activación de DDNS** **Nota:** para utilizar la función DDNS, primero debe configurar una cuenta y establecer una URL con www.DynDNS.org. La función DDNS no funcionará sin una cuenta válida. Para configurar una cuenta DDNS, abra el navegador e introduzca www.DynDNS.org en la barra de dirección. Siga las instrucciones que le ofrezca el sitio web para configurar una cuenta. Para activar el DDNS, siga estos pasos. **1** En la página DDNS, seleccione **www.DynDNS.org** como su servidor DDNS.  **2** Configure los campos siguientes: ■ User Name (Nombre de usuario) ■ Password (Contraseña) ■ Host Name (Nombre de host) **3** Pulse **Save Settings** (Guardar parámetros). El dispositivo avisará al servicio DDNS de la dirección IP (Internet) WAN cada vez que ésta cambie. **Importante:** el área Status (Estado) de la ventana mostrará el estado de la conexión del servicio DDNS.

Configuración de los parámetros de conexión inalámbrica

En esta sección se describen las opciones disponibles en las páginas Wireless (Inalámbrico), que puede utilizar para configurar los parámetros WAP para atender sus requisitos y necesidades específicos.

Wireless > Basic Settings (Inalámbrico > Configuración básica)

Configurar el gateway residencial para la comunicación inalámbrica le da la libertad de conectarse a Internet desde cualquier lugar dentro del alcance WAP sin tener que utilizar conexiones con cable. Seleccione la ficha **Basic Settings** (Configuración básica) para abrir la página Wireless Basic Settings (Inalámbrico > Configuración básica).

La página Wireless Basic Settings (Inalámbrico > Configuración básica) le permite elegir su modo de red inalámbrica y otras funciones básicas.

- Red inalámbrica: activar o desactivar
- Configuración de conexión inalámbrica: manual o Configuración Wi-Fi protegida (WPS)
- Modo de red
- Banda de radio
- Ancho de canal
- Canal estándar
- Nombre de la red inalámbrica (SSID)

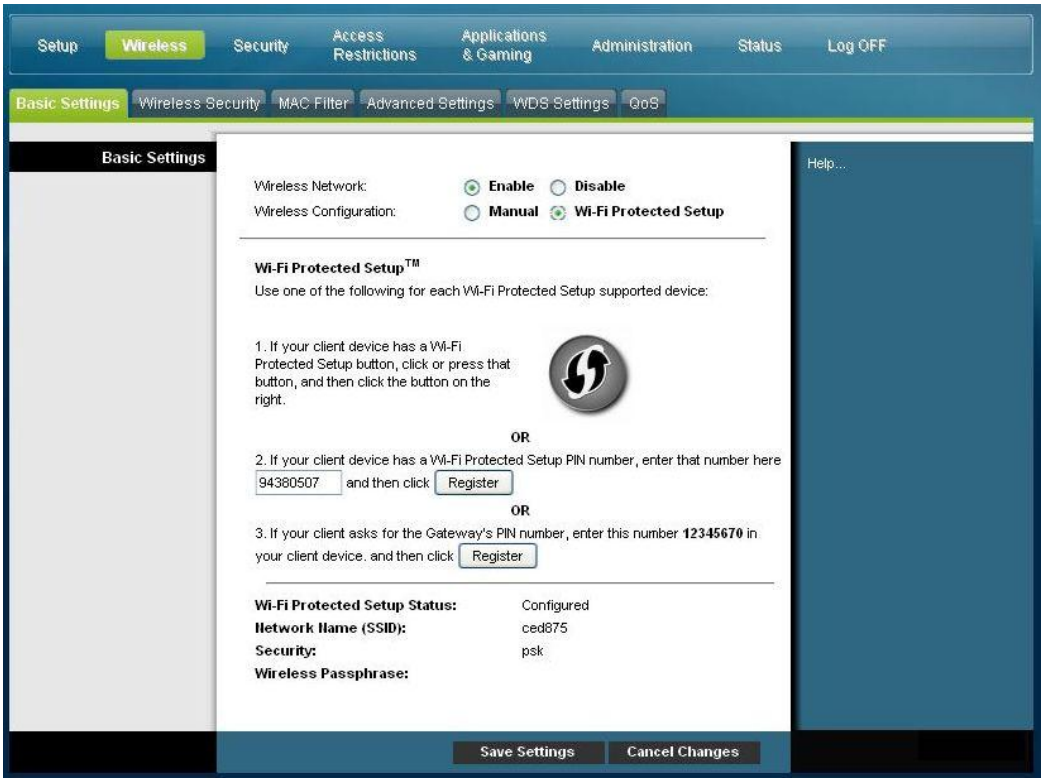
Wi-Fi Protected Setup (WPS) (Configuración Wi-Fi protegida, WPS)

Cuando selecciona WPS como configuración de la conexión inalámbrica, muchos de los parámetros están preconfigurados. WPS permite una configuración simplificada que permite conectar fácilmente nuevos dispositivos WPA a la red.

Importante: cuando utilice el modo WPS, no se admite WEP. Si es preciso utilizar el cifrado WEP, debe desactivarse la WPS estableciendo la configuración inalámbrica como **Manual**.

Nota: WPS es el ajuste predeterminado.

Ejemplo de configuración inalámbrica de Configuración Wi-Fi protegida



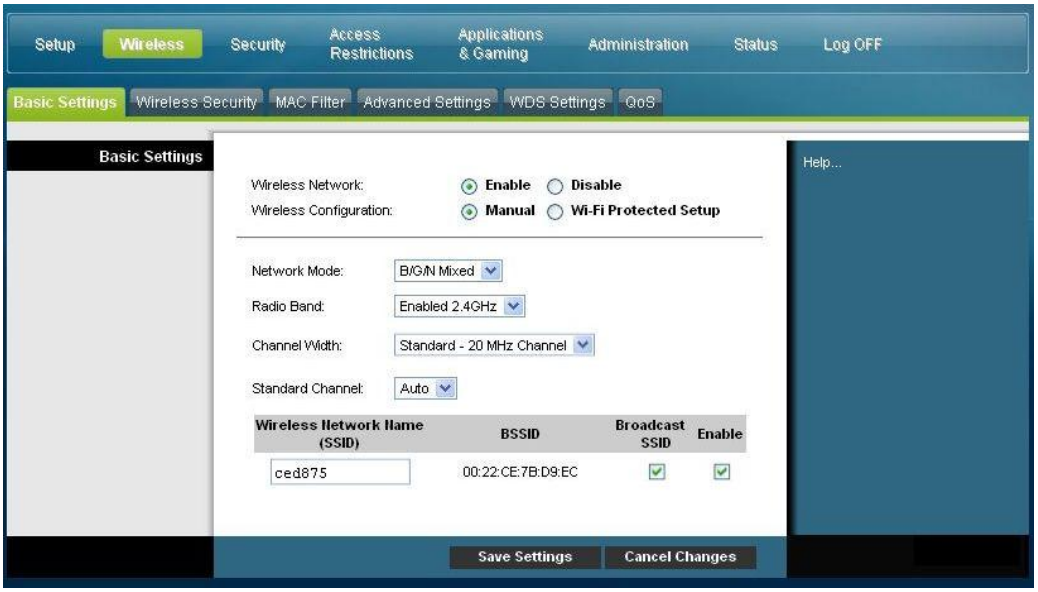
Descripción de la página de configuración inalámbrica Wi-Fi Protected Setup (Configuración Wi-Fi protegida)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros básicos de Wi-Fi Protected Setup (Configuración Wi-Fi protegida) para el gateway residencial. Cuando haya finalizado su selección, pulse **Save Settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Basic Settings (Configuración básica)	**Enable** (Activar) o **Disable** (Desactivar) la red inalámbrica **Wi-Fi Protected Setup (Configuración Wi-Fi protegida)** La función Configuración Wi-Fi protegida (WPS) configura automáticamente una red inalámbrica protegida mediante cifrado. Para utilizar WPS, deberá disponer de al menos un dispositivo que admita Configuración Wi-Fi protegida en la red. Después de haber configurado los dispositivos Wi-Fi, puede configurar manualmente otros dispositivos. **Configuración mediante el botón de WPS (opción 1)** Pulse el botón de configuración Wi-Fi protegida de la página Basic Wireless Settings (Inalámbrico > Configuración básica) o el botón del panel posterior del gateway para registrar un cliente inalámbrico con el gateway. Pulse el botón de software de configuración Wi-Fi protegida del lado del cliente al mismo tiempo que pulsa el botón de configuración Wi-Fi protegida en el gateway. La conexión se configurará automáticamente.

Sección	Descripción de campos
	Configuración de WPS mediante el PIN del adaptador Wi-Fi (opción 2) Esta es la opción más segura para registrar un cliente inalámbrico con el gateway. Necesitará el número PIN de la configuración Wi-Fi protegida, que se encuentra en la utilidad de configuración Wi-Fi protegida del cliente. Una vez que haya introducido el número PIN de la configuración Wi-Fi protegida del cliente, podrá conectarse al gateway. **Configuración de WPS mediante el PIN del gateway (opción 3)** Anote el número PIN de la configuración Wi-Fi protegida del gateway que se muestra en la página Wi-Fi Protected Setup (Configuración Wi-Fi protegida). Pulse el botón Register (Registrar) de la opción 3 y, con cualquier utilidad de configuración Wi-Fi protegida de cliente o Microsoft Vista, introduzca el número PIN de la configuración Wi-Fi protegida del gateway en el dispositivo cliente para completar el registro.

Ejemplo de página de configuración inalámbrica manual



Descripción de la página Wireless Basic Settings (Inalámbrico > Configuración básica)

Utilice las descripciones e instrucciones de la tabla siguiente para establecer manualmente la configuración básica de la comunicación inalámbrica del gateway residencial. Cuando haya finalizado su selección, pulse **Save Settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Basic Settings (Configuración básica)	**Wireless Network (Red inalámbrica)** **Enable** (Activar) o **Disable** (Desactivar) la red inalámbrica **Wireless Configuration (Configuración de conexión inalámbrica)** El valor predeterminado es **WPS**. Consulte ***Wi-Fi Protected Setup (WPS)*** (Configuración Wi-Fi protegida, WPS) (en la página 41) para obtener información adicional acerca del uso de WPS. Seleccione **Manual** para configurar manualmente la red con esta opción.
	Network Mode (Modo de red) Elija una de estas opciones para el modo de red: **G only (Solo G), B/G Mixed (B/G mezclados), B/G/N Mixed (B/G/N mezclados)** (valor predeterminado) **Importante:** cuando se selecciona TKIP authentication only (Solo autenticación TKIP), el modo de red B/G/N Mixed (B/G/N mezclado) no está disponible. **Radio Band (Banda de radio)** Seleccione **Enabled 2.4GHz (Activado 2.4 GHz)** (valor predeterminado) o **Enabled 5GHz (Activado 5 GHz).** **Nota:** algunos modelos no admiten la banda de radio 5GHz. **Channel Width (Ancho de canal)** Elija **Standard - 20 MHz Channel** (Canal estándar - 20 MHz) o **Wide 40 MHz Channel (Canal ancho 40 MHz)** **Standard Channel (Canal estándar)** Seleccione uno de los canales de la lista desplegable que se corresponda con su configuración de red. Todos los dispositivos de la red inalámbrica deben emitir en el mismo canal para establecer comunicación. Puede seleccionar **Auto** (valor predeterminado) para la selección automática de canales.

Sección	Descripción de campos
	Wireless Network Name (SSID) (Nombre de la red inalámbrica, SSID) SSID es el nombre de su red inalámbrica. La tecnología inalámbrica utiliza el SSID para diferenciar a su red de las demás redes inalámbricas de la zona. La longitud del SSID puede tener 32 caracteres como máximo. El SSID predeterminado suele ser los 6 últimos caracteres de la dirección CM MAC de la etiqueta de clasificación situada en la base de su gateway. Este SSID es un identificador exclusivo y no necesita modificarse a menos que usted quiera hacerlo. Su proveedor de servicios puede proporcionarle información sobre la configuración inalámbrica que requiera un SSID diferente. **BSSID** Muestra el Identificador de conjunto de servicios básicos (BSSID) de su red inalámbrica. El BSSID suele ser la dirección MAC del punto de acceso inalámbrico. **Nota:** ésta puede no ser la misma dirección MAC que la dirección CM MAC utilizada para determinar el SSID predeterminado. **Broadcast SSID (SSID de transmisión)** Cuando se marca esta casilla (valor predeterminado), el gateway transmite o anuncia su presencia a otros dispositivos inalámbricos. Los dispositivos clientes pueden detectar automáticamente el punto de acceso cuando se activa esta baliza. Anule la marca de esta casilla si quiere ocultar la red a los clientes inalámbricos. Si oculta su red, tendrá que configurar manualmente cada uno de sus dispositivos clientes inalámbricos. **Importante:** la casilla **Enable** (Activar) no está en uso actualmente y no repercute en el funcionamiento del gateway.

Wireless > Wireless Security (Inalámbrico > Seguridad inalámbrica)

La selección de un modo de seguridad inalámbrica ayuda a proteger la red. Si selecciona **Disable** (Desactivar), la red inalámbrica no estará protegida y cualquier dispositivo inalámbrico dentro del alcance podrá conectarse a ella.

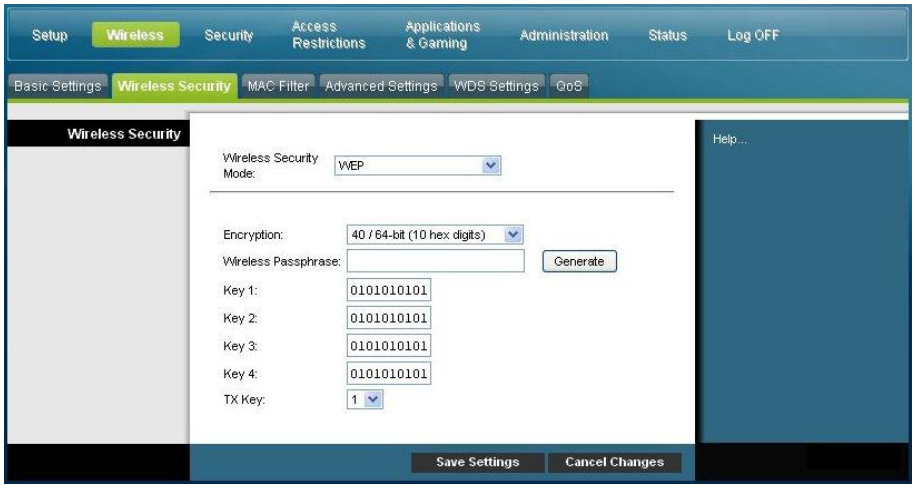
Para mantener alejados a los intrusos de su red inalámbrica, utilice la página Wireless Security (Seguridad inalámbrica) para configurar sus parámetros de seguridad incluido el modo de seguridad (nivel de cifrado), las claves de cifrado y otros parámetros de seguridad.

Seleccione la ficha **Wireless Security** (Seguridad inalámbrica) para abrir la página Wireless Security (Seguridad inalámbrica). La siguiente tabla muestra ejemplos de la página Wireless Security (Seguridad inalámbrica) con varios modos de seguridad inalámbrica seleccionados.

Descripción de la página Wireless Security (Seguridad inalámbrica)

Utilice las descripciones e instrucciones de la tabla siguiente para configurar la seguridad inalámbrica del gateway residencial. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Wireless Security (Seguridad inalámbrica)	**Wireless Security Mode (Modo de seguridad inalámbrica)** Elija una de estas opciones para el modo de seguridad: **WEP** El modo de seguridad Privacidad equivalente al cable (WEP) está definido en el estándar IEEE 802.11 original. Este modo ya no se recomienda debido a su débil protección de seguridad. Se recomienda encarecidamente a los usuarios que migren a WPA-Personal o WPA2-Personal. **Nota:** el modo WPS no admite WEP en este dispositivo.



Descripción de los campos

- **Encryption (Cifrado)** Seleccione un nivel de cifrado WEP, 40/64 bits (10 hex digits) [40/64 bits (10 dígitos hexadecimales)] o 128 bits (26 hex digits) [128 bits (26 dígitos hexadecimales)].
- **Wireless Passphrase (Frase de contraseña inalámbrica)** Para completar la configuración de seguridad inalámbrica, debe elegir una frase de contraseña inalámbrica que le sea fácil de recordar pero difícil de adivinar por otras personas. La primera vez que conecte un nuevo dispositivo inalámbrico a la red, es posible que tenga que introducir esta frase de contraseña en la sección de configuración adecuada del dispositivo conectado. Para aumentar la seguridad de su red, no facilite esta frase de contraseña a usuarios no autorizados. Introduzca una frase de letras y números con una longitud de entre 4 y 24 caracteres. A continuación, pulse Generate (Generar) para crear la frase de contraseña.
- **Key 1-4 (Clave 1-4)** Si desea introducir manualmente claves WEP, complete los campos proporcionados. La clave WEP puede incluir letras de la "A" a la "F" y números del "0" al "9". La longitud debe ser de 10 caracteres para cifrado de 64 bits o 26 caracteres para cifrado de 128 bits.
- **TX Key (Clave de transmisión)** Elija una clave de transmisión (TX) del 1 al 4. La clave TX es la que se utilizará para cifrar sus datos. Aunque se pueden crear cuatro claves, solo se utiliza una para cifrar los datos. Seleccione una de las cuatro claves para el cifrado WEP. Utilice la clave TX seleccionada para configurar los clientes inalámbricos.

Sección	Descripción de campos

WPA

Seguridad para redes personales: modos WPA o WPA2 Personal

Acceso protegido Wi-Fi (Wi-Fi Protected Access, WPA) es una tecnología inalámbrica más segura que WEP. WPA puede utilizarse para redes inalámbricas tanto empresariales (aplicaciones corporativas) como personales (red doméstica). Le recomendamos encarecidamente que seleccione WPA-Personal o bien WPA2-Personal como el modo de seguridad de su red doméstica, en función de cuál sea el modo admitido por el adaptador inalámbrico de su PC o clientes inalámbricos.

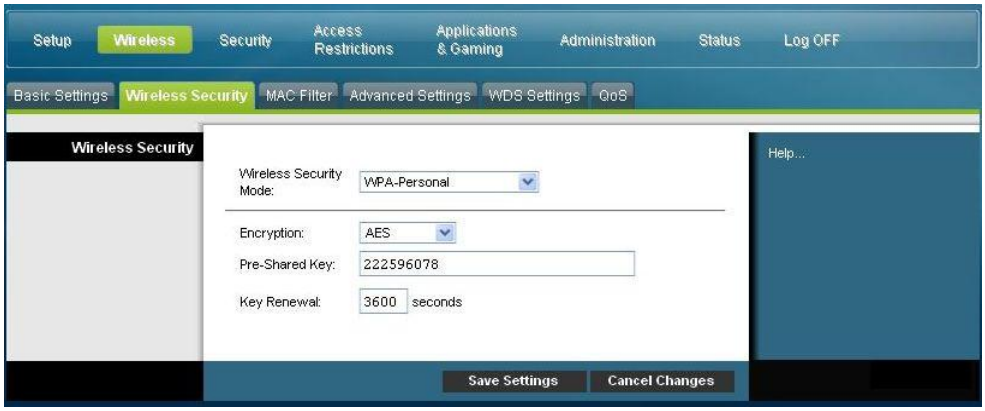
WPA-Personal (también llamada WPA-PSK o clave precompartida WPA), proporciona una red inalámbrica más segura que WEP. WPA-Personal introduce la autenticación de usuarios TKIP y unas claves de cifrado más potentes que WEP.

WPA2-Personal (también llamada WPA2-PSK o clave precompartida WPA2) proporciona la red inalámbrica basada en estándares más segura. WPA2-Personal incorpora el Estándar de cifrado avanzado (Advanced Encryption Standard, AES) para la transmisión de datos.

Nota: no todos los adaptadores inalámbricos admiten WPA2. WPA es compatible con una amplia variedad de dispositivos. Tanto si selecciona WPA o WPA2, asegúrese de utilizar una frase de contraseña segura. Una frase de contraseña segura es una cadena de caracteres aleatorios de al menos 21 caracteres de longitud.

Seleccione uno de los tres modos WPA o WPA2 Personal siguientes:

- **WPA-Personal**
- **WPA2-Personal**
- **WPA o WPA2-Personal**



Descripción de los campos

- **Encryption (Cifrado)** El valor predeterminado es TKIP+AES.
- **Pre-Shared Key (Clave precompartida)** Introduzca una clave de 8 a 63 caracteres.
- **Key Renewal (Renovación de claves)** Introduzca el período de renovación de claves, que indica al dispositivo la frecuencia con la que debe cambiar las claves de cifrado. El valor predeterminado es **3.600** segundos.

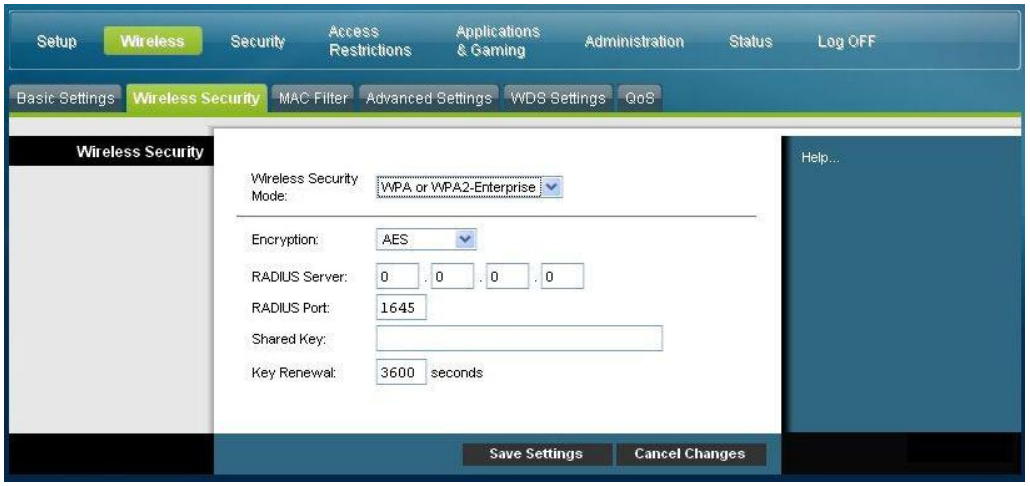
Sección	Descripción de campos

Seguridad para las redes empresariales: modos WPA-Enterprise

Esta opción incluye WPA que se utiliza en coordinación con un servidor RADIUS para la autenticación de usuarios (solo se debe utilizar si hay un servidor RADIUS conectado al dispositivo).

Seleccione uno de los tres modos WPA o WPA2 Enterprise siguientes:

- **WPA-Enterprise (WPA-Empresarial)**
- **WPA2-Enterprise (WPA2-Empresarial)**
- **WPA or WPA2-Enterprise (WPA o WPA2-Empresarial)**



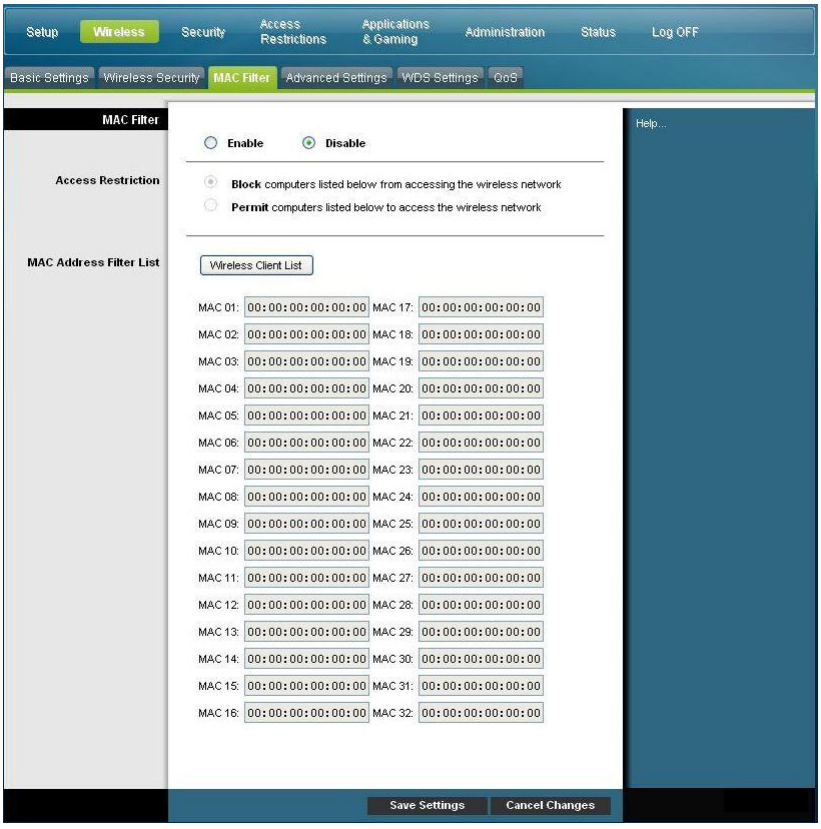
Descripción de los campos

- **Encryption (Cifrado)** El valor predeterminado es TKIP+AES.
- **RADIUS Server (Servidor RADIUS)** Introduzca la dirección IP del servidor RADIUS.
- **RADIUS Port (Puerto RADIUS)** Introduzca el número de puerto que utiliza el servidor RADIUS. El valor predeterminado es **1812**.
- **Shared Key (Clave compartida)** Introduzca la clave que utilizan el dispositivo y el servidor RADIUS.
- **Key Renewal (Renovación de claves)** Introduzca el período de renovación de claves, que indica al dispositivo la frecuencia con la que debe cambiar las claves de cifrado. El valor predeterminado es **3.600** segundos.

Wireless > MAC Filter (Inalámbrico > Filtro MAC)

La función filtro MAC se utiliza para permitir o bloquear el acceso a su LAN inalámbrica en función de la dirección MAC de los dispositivos clientes inalámbricos. La función filtro MAC, también llamada lista de accesos, puede utilizarse para ayudar a proteger su red inalámbrica contra el acceso de usuarios no autorizados.

Seleccione la ficha **MAC Filter** (Filtro MAC) para abrir la página Wireless MAC Filter (Inalámbrico > Filtro MAC).



Descripción de la página Wireless MAC Filter (Inalámbrico > Filtro MAC)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar el filtrado de direcciones MAC para la red inalámbrica de su gateway residencial. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
MAC Filter (Filtro MAC)	Puede elegir las opciones **Enable** (Activar) o **Disable** (Desactivar) para el filtrado MAC para el gateway residencial.

Sección	Descripción de campos
Access Restriction (Restricción de acceso)	**Access Restriction (Restricción de acceso)** Sirve para permitir o bloquear el acceso de los PC a la red inalámbrica. La elección que haga aquí afectará a las direcciones enumeradas en esta página. Elija una de las siguientes opciones: ■ Block computers listed below from accessing the wireless network (Bloquear el acceso a la red inalámbrica a los equipos siguientes) Seleccione esta opción para denegar el acceso a Internet a las direcciones MAC de los dispositivos que incluya en la tabla. Todas las demás direcciones MAC tendrán acceso a Internet. ■ Permit computers listed below access to the wireless network (Permitir el acceso a la red inalámbrica a los equipos siguientes) Seleccione esta opción para permitir el acceso a Internet solo a las direcciones MAC de los dispositivos que incluya en la tabla. Las direcciones MAC no incluidas en la tabla no tendrán acceso a Internet
MAC Address Filter List (Lista de filtros de direcciones MAC)	**MAC Address Filter List (Lista de filtros de direcciones MAC)** La lista de filtros de direcciones MAC muestra a los usuarios cuyo acceso inalámbrico desea controlar. Pulse **Wireless Client List** (Lista de clientes inalámbricos) para mostrar una lista de usuarios de la red por dirección MAC. En el menú desplegable Sort by (Ordenar por), puede ordenar la tabla por dirección IP, dirección MAC, estado, interfaz o nombre de cliente. Para ver la información más reciente, pulse el botón Refresh (Actualizar).

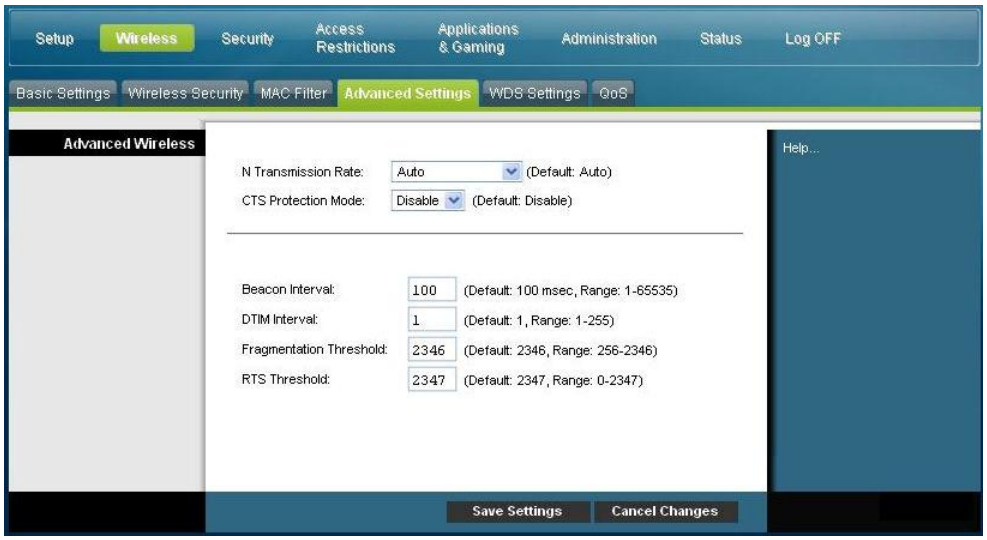
Wireless > Advanced Settings (Inalámbrico > Configuración avanzada)

La configuración inalámbrica avanzada agrega otra capa de seguridad a la red inalámbrica para su gateway residencial. Esta página se utiliza para configurar las funciones inalámbricas avanzadas. Solo un administrador experto debe ajustar esta configuración. Una configuración incorrecta puede reducir el rendimiento inalámbrico.

Seleccione la ficha **Advanced Settings** (Configuración avanzada) para abrir la página Wireless Advanced Settings (Inalámbrico > Configuración avanzada).

Utilice esta página para configurar las siguientes opciones:

- N Transmission Rate (Velocidad de transmisión N)
- CTS Protection Mode (Modo de protección CTS)
- Beacon Interval (Intervalo de baliza)
- DTM Interval (Intervalo DTM)
- Fragmentation Threshold (Umbral de fragmentación)
- RTS Threshold (Umbral RTS)



Descripción de la página Wireless Advanced Settings (Inalámbrico > Configuración avanzada)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de red para su gateway residencial. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

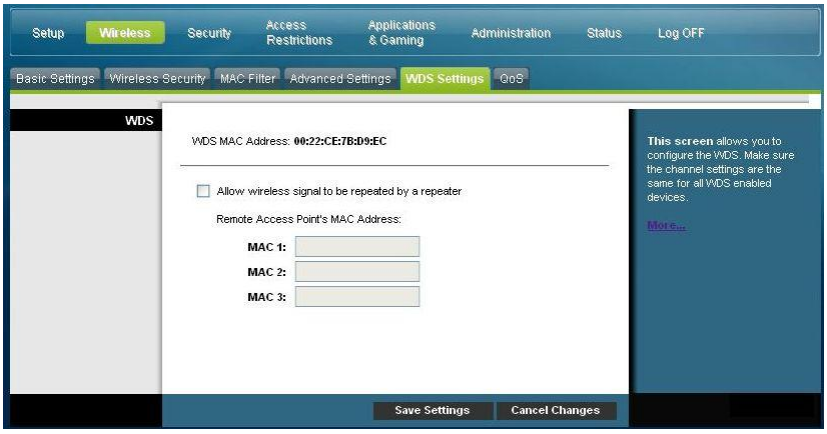
Sección	Descripción de campos
Advanced Wireless (Parámetros inalámbricos avanzados)	**N Transmission Rate (Velocidad de transmisión N)** La velocidad de transmisión de datos se debe establecer según la velocidad de la conexión en red N inalámbrica. Seleccione un valor de un intervalo de velocidades de transmisión o seleccione **Auto** para que el dispositivo utilice automáticamente la máxima velocidad de transferencia de datos posible y active la función Auto-Fallback (Reserva automática). Auto-Fallback (Reserva automática) negocia la mejor conexión posible entre el dispositivo y un cliente inalámbrico. El valor predeterminado es **Auto**. Elija una de las siguientes opciones para la velocidad de transmisión: ■ Auto (Automático) (valor predeterminado) ■ Use Legacy Rate (Utilizar velocidad anterior) ■ 0: 6,5 o 13,5 Mbps ■ 1: 13 o 27 Mbps ■ 2: 19,5 o 40,5 Mbps ■ 3: 26 o 54 Mbps ■ 4: 39 o 81 Mbps ■ 5: 52 o 108 Mbps ■ 6: 58,5 o 121,5 Mbps ■ 7: 65 o 135 Mbps ■ 8: 13 o 27 Mbps ■ 9: 26 o 54 Mbps ■ 10: 39 o 81 Mbps ■ 11: 52 o 108 Mbps ■ 12: 78 o 162 Mbps ■ 13: 104 o 216 Mbps ■ 14: 117 o 243 Mbps ■ 15: 130 o 270 Mbps
	CTS Protection Mode (Modo de protección CTS) El modo de protección Listo para emitir (Clear-To-Send, CTS) potencia la capacidad del dispositivo de detectar todas las transmisiones inalámbricas, pero puede disminuir notablemente el rendimiento. Seleccione **Auto** para utilizar esta función cuando sea necesario, cuando los productos Wireless-N/G no puedan transmitir al dispositivo en un entorno con mucho tráfico 802.11b. Seleccione **Disable** (Desactivar) para desactivar esta función de forma permanente.
	Beacon Interval (Intervalo de baliza) Este valor indica el intervalo de frecuencia de la baliza. Una baliza es un paquete difundido por el dispositivo para sincronizar la red inalámbrica. (Predeterminado: 100 ms, intervalo: de 20 a 1000)

Sección	Descripción de campos
	DTIM Interval (Intervalo DTIM) El Mensaje indicador de tráfico de transmisiones (Delivery Traffic Indication Message, DTIM) indica el intervalo entre las transmisiones de difusión/multidifusión. El campo DTIM es un campo de cuenta atrás que informa a los clientes de la siguiente ventana para recibir los mensajes de difusión y multidifusión. Una vez que el dispositivo haya almacenado en el búfer los mensajes de difusión o multidifusión para los clientes asociados, envía el siguiente DTIM con un valor de intervalo DTIM. Sus clientes reciben las balizas y se activan para recibir los mensajes de difusión y multidifusión. (Valor predeterminado: 1, intervalo: de 1 a 255)
	Fragmentation Threshold (Umbral de fragmentación) El umbral de fragmentación especifica el tamaño máximo de un paquete antes de fragmentar los datos en varios paquetes. Si experimenta una tasa alta de errores de paquete, puede aumentar ligeramente el umbral de fragmentación. Si establece un umbral de fragmentación demasiado bajo, se puede reducir el rendimiento de la red. Solo se recomiendan reducciones mínimas del valor predeterminado. En la mayoría de los casos, debe permanecer en su valor predeterminado de 2.346.
	RTS Threshold (Umbral RTS) El umbral RTS determina el tamaño de paquete por encima del cual se debe invocar el mecanismo listo para enviar/listo para emitir (RTS/CTS). Si detecta un flujo de datos irregular, se recomienda efectuar solo una reducción mínima del valor predeterminado, 2.346. Si un paquete de red es más pequeño que el tamaño de umbral RTS predefinido, el mecanismo RTS/CTS no se activará. El dispositivo envía tramas RTS (del inglés *Request to Send*, petición de envío) a una determinada estación de recepción y negocia el envío de una trama de datos. Después de recibir una petición de envío, la estación inalámbrica responde con una trama CTS para confirmar el inicio de la transmisión. El valor del umbral RTS debe permanecer en su valor predeterminado de 2.347.

Wireless > WDS Settings (Inalámbrico > Configuración WDS)

La página Wireless Distribution System (WDS) Settings (Configuración del sistema de distribución inalámbrica, WDS) le permite ampliar la cobertura de su red inalámbrica mediante la instalación de repetidores de señal. Asegúrese de que los parámetros de canal sean los mismos para todos los dispositivos WDS.

Seleccione la ficha **Advanced Settings** (Configuración avanzada) para abrir la página Wireless WDS Settings (Inalámbrico > Configuración WDS). Utilice esta página para configurar los parámetros WDS.



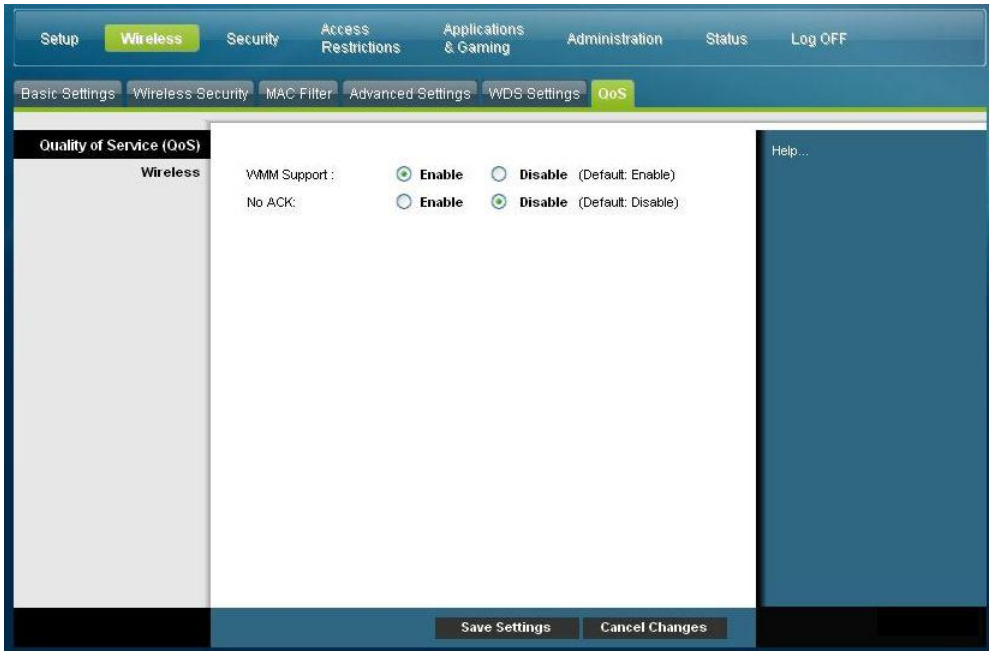
Descripción de la página Wireless WDS Settings (Inalámbrico > Configuración WDS)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de red para su gateway residencial. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
WDS	**WDS MAC Address (Dirección MAC de WDS)** Muestra la dirección MAC de WDS (o BSSID) del punto de acceso del gateway
	Allow Wireless Signal To Be Repeated by a Repeater (Permitir que el repetidor repita la señal inalámbrica) Marque esta casilla para permitir que un cliente inalámbrico se conecte a un repetidor y dirija el tráfico entre el cliente inalámbrico y un repetidor. Se permite un máximo de 3 repetidores.
	Remote Access Point's MAC Address (MAC 1 through 3) (Dirección MAC 1 a 3 del punto de acceso remoto) Utilice los tres campos (MAC 1, 2 y 3) para introducir la dirección MAC de los repetidores.

Wireless > QoS (Inalámbrico > Calidad de servicio)

La calidad de servicio (del inglés *Quality of Service*, QoS) garantiza un servicio óptimo para tipos de tráfico de red de alta prioridad, que pueden consistir en aplicaciones exigentes y en tiempo real, como las videoconferencias. Los parámetros QoS le permiten especificar las prioridades para distintos tipos de tráfico. El tráfico de menor prioridad se ralentizará para permitir un mayor rendimiento o un menor retraso del tráfico de alta prioridad. Seleccione la ficha **QoS** (Calidad de servicio) para abrir la página Wireless QoS (Inalámbrico > QoS).



Descripción de la página Wireless QoS (Inalámbrico > Calidad de servicio)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar cada parámetro QoS. Cuando haya finalizado su selección, pulse **Save Settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Quality of Service (QoS) (Calidad de servicio)	
Wireless (Inalámbrico)	**WMM Support (Compatibilidad con WMM)** Si los clientes inalámbricos admiten WMM (del inglés *Wi-Fi Multimedia*, multimedia por Wi-Fi), la activación de esta opción significa que el tráfico multimedia y de voz tendrá mayor prioridad que otro tipo de tráfico. Seleccione la opción deseada: ■ **Enable (Activar)**, (valor predeterminado) ■ **Disable (Desactivar)**

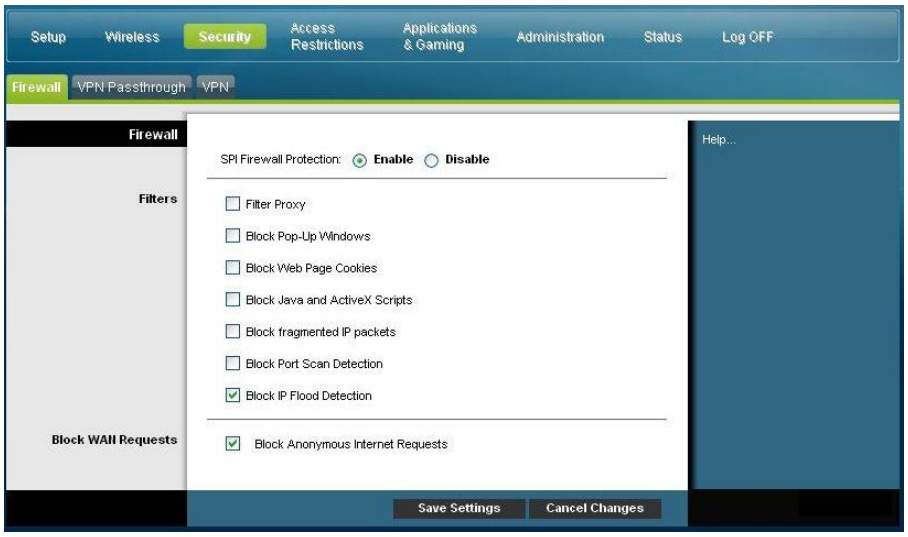
Sección	Descripción de campos
	No ACK (Sin acuse de recibo) Le permite activar o desactivar NO ACK (Sin acuse de recibo). Esta función se recomienda para los servicios de datos en los que la transmisión es importante y la pérdida de paquetes es en cierta medida tolerable. Si selecciona **Disable** (Desactivar), se devuelve un paquete de acuse de recibo por cada paquete recibido. Esto proporciona una transmisión más fiable, pero aumenta la carga de tráfico, lo que reduce el rendimiento. Seleccione la opción deseada: ■ **Enable (Activar)** ■ **Disable (Desactivar)**, (valor predeterminado)

Configuración de seguridad

Security (Seguridad) > Firewall

La tecnología avanzada de firewall disuade a los piratas y protege el entorno doméstico contra los accesos no autorizados Utilice esta página para configurar un firewall capaz de filtrar los distintos tipos de tráfico no deseado en la red local del gateway.

Seleccione la ficha **Firewall** para abrir la página Security Firewall (Firewall de seguridad).



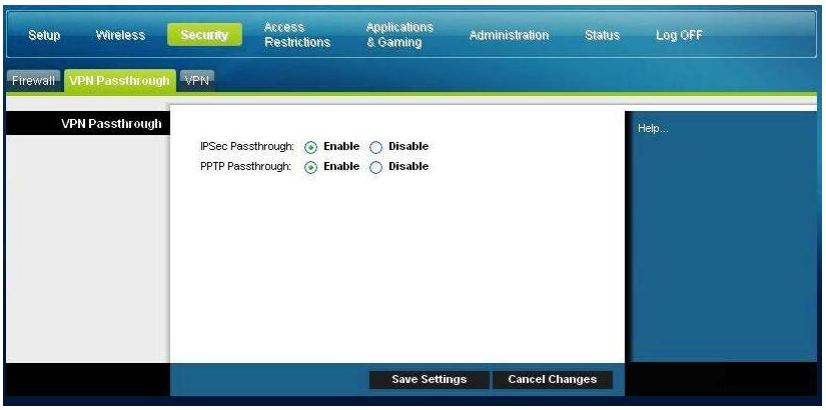
Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de red para su gateway residencial. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Firewall	**SPI Firewall Protection (Protección de firewall SPI)** SPI Firewall Protection (Protección de firewall SPI) bloquea los ataques de Denegación de servicio (Denial of Service, DoS). Un ataque DoS no intenta robar datos ni dañar los PC, pero sobrecarga la conexión a Internet para que no se pueda usar. Seleccione la opción deseada: ■ **Enable (Activar)**, (valor predeterminado) ■ **Disable (Desactivar)**

Sección	Descripción de campos
Filters (Filtros)	**Filter Proxy (Proxy de filtro)** Activa/desactiva el filtro de servidores proxy. Si los usuarios locales tienen acceso a servidores proxy de WAN, podrían eludir los filtros de contenido y acceder a los sitios web bloqueados por el dispositivo. Si selecciona la función Filter Proxy (Proxy de filtro), ésta bloqueará el acceso a los servidores proxy de WAN. **Block Pop-Up Windows (Bloquear ventanas emergentes)** Activa o desactiva las ventanas emergentes. Algunas de las aplicaciones más utilizadas emplean ventanas emergentes como parte de la aplicación. Si desactiva las ventanas emergentes, puede obstaculizar el funcionamiento de algunas de estas aplicaciones. **Block Web Page Cookies (Bloquear cookies de páginas web)** Activa/desactiva el bloqueo de cookies. Esta función filtra el depósito no deseado de cookies de Internet en los dispositivos de su red local privada. Las cookies son archivos informáticos que contienen información personal o datos de comportamiento de navegación en Web. **Block Java and ActiveX Scripts (Bloquear Java y scripts ActiveX)** Activa/desactiva los subprogramas Java y los scripts ActiveX. Esta función ayuda a proteger los dispositivos de su red privada contra los subprogramas Java molestos o malintencionados que se envían, sin haberse solicitado, desde Internet a los dispositivos de su red privada. Estos subprogramas se ejecutan automáticamente cuando el PC los recibe. Java es un lenguaje de programación para sitios web. Si selecciona la función Filter Java Applets (Filtrar subprogramas Java), es posible que no obtenga acceso a los sitios de Internet creados con este lenguaje de programación. Esta función también ayuda a proteger los dispositivos de su red privada contra los controles ActiveX molestos o malintencionados que se envían, sin haberse solicitado, desde Internet a los dispositivos de su red privada. Estos controles ActiveX se ejecutan automáticamente cuando el PC los recibe. **Block fragmented IP packets (Bloquear paquetes IP fragmentados)** Activa o desactiva el filtrado de paquetes IP fragmentados. Esta función ayuda a proteger su red local privada contra los ataques de denegación de servicio basados en Internet. **Block Port Scan Detection (Bloquear detección de análisis de puerto)** Activa o desactiva la respuesta del gateway a los análisis de puertos basados en Internet. Esta función está diseñada para proteger su red local privada contra los piratas basados en Internet que intentan obtener acceso no solicitado a su red mediante la detección de puertos IP abiertos en el gateway. **Block IP Flood Detection (Bloquear la detección de inundación de IP** [marcada - opción predeterminada]**)** Bloquea los dispositivos malintencionados que intentan inundar los dispositivos o las redes con paquetes de difusión ilegales. También se conoce como "tormenta de difusión".
Block WAN Requests (Bloquear solicitudes WAN)	**Block Anonymous Internet Requests (Bloquear las peticiones de Internet anónimas** [marcada - opción predeterminada]**)** Active esta función para evitar que su red sea detectada por otros usuarios de Internet. La función Block Anonymous Internet Requests (Bloquear las peticiones de Internet anónimas) también oculta sus puertos de red. Ambas opciones dificultan la entrada de usuarios externos a la red.

Security > VPN Passthrough (Seguridad > Paso a través de VPN)

Utilice esta página para configurar la compatibilidad con la red privada virtual (Virtual Private Network, VPN). Activar estos parámetros en esta página permite que los túneles VPN que utilizan protocolos IPsec o PPTP pasen a través del firewall del gateway. Seleccione la ficha **VPN Passthrough** (Paso a través de VPN) para abrir la página Security VPN Passthrough (Seguridad > Paso a través de VPN).



Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de red para su gateway residencial. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
VPN Passthrough (Paso a través de VPN)	**IPSec Passthrough (Paso a través de IPSec)** Activa/desactiva la Seguridad de protocolo de Internet (Internet Protocol Security, IPsec). IPSec es un conjunto de protocolos utilizados para implantar el intercambio seguro de paquetes en la capa IP. Si activa IPSec Passthrough (Paso a través de IPSec), las aplicaciones que utilicen IPsec pueden pasar a través del firewall. Para desactivar IPSec Passthrough (Paso a través de IPSec), seleccione **Disable** (Desactivar). Seleccione la opción deseada: ■ **Enable (Activar)**, (valor predeterminado) ■ **Disable (Desactivar)**
	PPTP Passthrough (Paso a través de PPTP) Activa/desactiva el Protocolo de tunelación punto a punto (Point-to-Point Tunneling Protocol, PPTP). PPTP permite la tunelación del Protocolo punto a punto (Point-to-Point Protocol, PPP) a través de una red IP. Si activa el paso a través de PPTP, las aplicaciones que utilizan el protocolo PTP pueden pasar a través del firewall. Para desactivar PPTP Passthrough (Paso a través de PPTP) seleccione **Disable** (Desactivar). Seleccione la opción deseada: ■ **Enable(Activar)**, (valor predeterminado) ■ **Disable (Desactivar)**

Security (Seguridad) > VPN

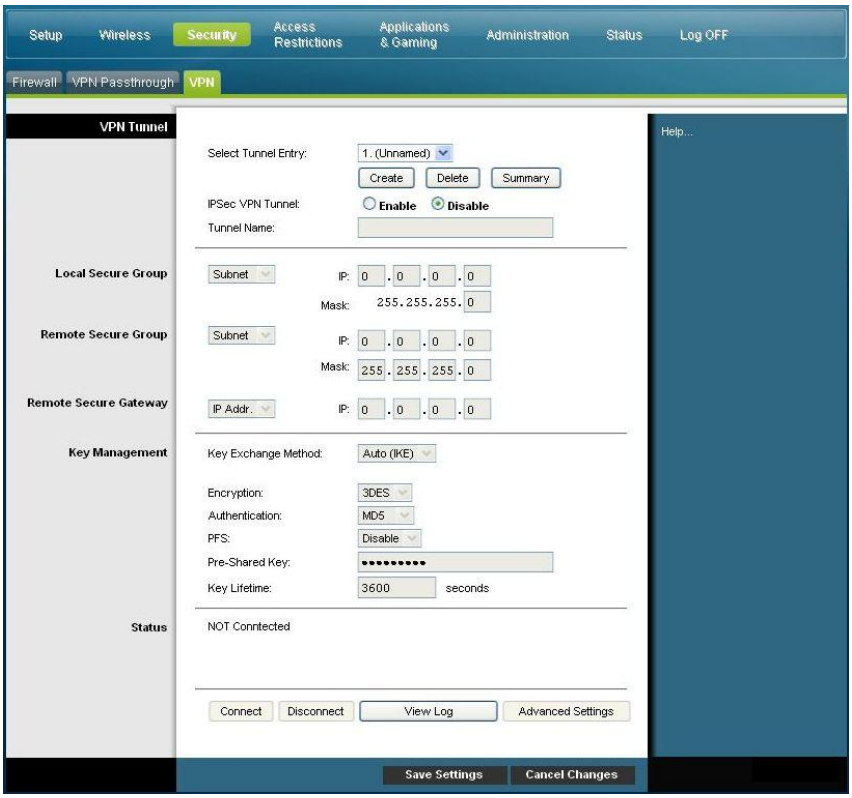
Una red privada virtual (Virtual Private Network, VPN) es una conexión entre dos puntos terminales de redes diferentes que permite el envío de datos privados de forma segura a través de redes públicas u otras redes privadas. Esto se consigue mediante la creación de un "túnel VPN". Un túnel VPN conecta los dos PC o redes y permite transmitir los datos por Internet como si fuera una red privada. El túnel VPN utiliza IPsec para cifrar los datos enviados entre los dos puntos terminales y encapsula los datos dentro de una trama Ethernet/IP normal, permitiendo que los datos pasen entre las redes de forma segura y sin incidentes.

Una VPN proporciona una opción rentable y más segura que utilizar una línea privada, especial y arrendada para una red privada. Mediante el uso de las técnicas de cifrado y autenticación estándar del sector, una VPN de IPsec crea una conexión segura que funciona como si estuviera directamente conectado a su red privada local.

Por ejemplo, una VPN permite a los usuarios estar en casa y conectarse a la red corporativa de su empresa y recibir una dirección IP en su red privada, exactamente igual que si estuvieran en su despacho conectados a la LAN corporativa.

Seleccione la ficha **VPN** para abrir la página Setup VPN (Configuración VPN).

Utilice esta página para configurar la VPN para su gateway residencial.



Descripción de la página Security > VPN Tunnel (Seguridad > Túnel VPN)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de túnel VPN para su gateway. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
VPN Tunnel (Túnel VPN)	**Select Tunnel Entry (Seleccionar entrada de túnel)** Le permite mostrar una lista de los túneles VPN creados **Botón Create (Crear)** Pulse este botón para crear una entrada de túnel. **Botón Delete (Eliminar)** Pulse este botón para eliminar todos los parámetros del túnel seleccionado. **Botón Summary (Resumen)** Pulse este botón para mostrar los parámetros y el estado de todos los túneles activados **IPSec VPN Tunnel (Túnel VPN IPSec)** Le permite activar o desactivar el Protocolo de seguridad de Internet (Internet Security Protocol) para el túnel VPN. **Tunnel Name (Nombre del túnel)** Introduzca el nombre del túnel.
Local Secure Group (Grupo seguro local)	Seleccione los usuarios LAN locales que pueden utilizar el túnel VPN. Puede ser una única dirección IP o una subred. Tenga en cuenta que el grupo seguro local debe coincidir con el grupo seguro remoto del gateway remoto. **IP** Introduzca la dirección IP de la red local. **Mask (Máscara)** Si selecciona la opción Subnet (Subred), introduzca la máscara para determinar la dirección IP en la red local.
Remote Secure Group (Grupo seguro remoto)	Seleccione los usuarios LAN remotos detrás del gateway remoto que pueden utilizar el túnel VPN. Puede ser una única dirección IP, una subred o varias direcciones. Si se establece "Any" (Cualquiera), el gateway se encarga de responder y acepta las peticiones de cualquier usuario remoto. Tenga en cuenta que el grupo seguro remoto debe coincidir con el grupo seguro local del gateway remoto. **IP** Introduzca la dirección IP de la red remota. **Mask (Máscara)** Si selecciona la opción Subnet (Subred), introduzca la máscara para determinar la dirección IP en la red remota.

Sección	Descripción de campos
Remote Secure Gateway (Gateway seguro remoto)	Seleccione la opción deseada, **IP Addr.** (Dirección IP), **Any** (Cualquiera) o **FQDN**. Si el gateway remoto tiene una dirección IP dinámica, seleccione **Any** (Cualquiera) o **FQDN**. Si selecciona **Any** (Cualquiera), el gateway aceptará peticiones de cualquier dirección IP. **FQDN** Si selecciona **FQDN**, introduzca el nombre de dominio del gateway remoto para que el gateway pueda localizar una dirección IP actual que esté utilizando DDNS. **IP** La dirección IP de este campo debe coincidir con la dirección IP (WAN o Internet) pública del gateway remoto al otro extremo de este túnel.
Key Management (Gestión de claves)	**Key Exchange Method (Método de intercambio de claves)** El gateway admite la gestión de claves automática y manual. Si se selecciona la gestión automática de claves, se utilizan protocolos IKE (del inglés *Internet Key Exchange*, intercambio de claves por Internet) para negociar el material de clave para SA (del inglés *Security Association*, asociación de seguridad). Si se selecciona la gestión manual de claves, no se necesita ninguna negociación de claves. Básicamente, la gestión manual de claves se utiliza en pequeños entornos estáticos para fines de identificación y resolución de problemas. Tenga en cuenta que ambos extremos deben utilizar el mismo método de gestión de claves.

Sección	Descripción de campos
Key Management (Gestión de claves) (continuación)	Seleccione una de las siguientes opciones para el método de intercambio de claves: ■ **Auto (IKE) (IKE automático)** – **Encryption (Cifrado):** el método de cifrado determina la longitud de la clave que se utilice para cifrar/descifrar los paquetes ESP. Observe que ambos extremos deben utilizar el mismo método. – **Authentication (Autenticación):** el método de autenticación valida los paquetes de Carga útil de seguridad encapsulada (Encapsulating Security Payload, ESP). Seleccione **MD5** o **SHA**. Observe que ambos extremos (extremos VPN) deben utilizar el mismo método. ▪ MD5: algoritmo de hashing unidireccional que produce un resumen de 128 bits. ▪ SHA: algoritmo de hashing unidireccional que produce un resumen de 160 bits. – **Perfect Forward Secrecy (Confidencialidad directa perfecta, PFS)**: si se activa PFS, la negociación IKE de fase 2 generará material de claves nuevo para el cifrado y la autenticación del tráfico IP. Tenga en cuenta que ambos extremos deben tener PFS activado. – **Pre-Shared Key (Clave precompartida):** IKE utiliza la clave precompartida para autenticar el punto IKE remoto. Este campo acepta valores de caracteres y hexadecimales, p. ej., "My_@123" ó "0x4d795f40313233". Tenga en cuenta que ambos extremos deben utilizar la misma clave precompartida. – **Key Lifetime (Duración de clave):** esta campo especifica la duración de la clave generada por IKE. Si caduca el tiempo especificado, se volverá a negociar una nueva clave automáticamente. La vida útil de la clave puede oscilar entre 300 y 100.000.000 segundos. La duración predeterminada es de **3.600** segundos. ■ **Manual** – **Encryption (Cifrado):** el método de cifrado determina la longitud de la clave que se utilice para cifrar/descifrar los paquetes ESP. Observe que ambos extremos deben utilizar el mismo método. – **Encryption Key (Clave de cifrado):** este campo especifica la clave que se utilizará para cifrar y descifrar el tráfico IP. Se aceptan caracteres y valores hexadecimales. Tenga en cuenta que ambos extremos deben utilizar la misma clave de cifrado. – **Authentication (Autenticación):** el método de autenticación valida los paquetes de Carga útil de seguridad encapsulada (Encapsulating Security Payload, ESP). Seleccione MD5 o SHA. Observe que ambos extremos (extremos VPN) deben utilizar el mismo método. ▪ MD5: algoritmo de hashing unidireccional que produce un resumen de 128 bits. ▪ SHA: algoritmo de hashing unidireccional que produce un resumen de 160 bits. – **Authentication Key (Clave de autenticación):** este campo especifica la clave que se utilizará para autenticar el tráfico IP. Se aceptan caracteres y valores hexadecimales. Tenga en cuenta que ambos extremos deben utilizar la misma clave de autenticación.

Sección	Descripción de campos
	– **Inbound SPI/Outbound SPI (SPI entrante/SPI saliente):** el Índice de parámetros de seguridad (Security Parameter Index, SPI) figura en el encabezado de la ESP. Esto permite al destinatario seleccionar la SA bajo la que se deberá procesar el paquete. El SPI es un valor de 32 bits. Se aceptan valores decimales y hexadecimales. p. ej., "987654321" ó "0x3ade68b1". Cada túnel debe tener un SPI entrante y un SPI saliente exclusivos. Dos túneles no pueden compartir el mismo SPI. Tenga en cuenta que el SPI entrante debe coincidir con el SPI saliente del gateway remoto y viceversa.
Status (Estado)	Este campo muestra el estado de conexión del túnel seleccionado. El estado puede ser **Connected** (Conectado) o **Disconnected** (Desconectado).
Botones	**Connect (Conectar)** Haga clic en este botón para establecer una conexión para el túnel VPN actual. Si ha realizado algún cambio, pulse **Save Settings** (Guardar parámetros) para aplicarlo primero. **Disconnect (Desconectar)** Haga clic en este botón para interrumpir una conexión para el túnel VPN actual. **View Log (Ver registro)** Haga clic en este botón para ver el registro VPN en el que se muestra información detallada sobre cada túnel establecido. **Advanced Settings (Parámetros avanzados)** Si el método de intercambio de claves es Auto (IKE), este botón proporciona acceso a otros parámetros relacionados con IKE. Pulse este botón si el gateway no puede establecer un túnel VPN al gateway remoto, y asegúrese de que la configuración avanzada coincida con la del gateway remoto. ■ **Phase 1 - Operation Mode (Fase 1 - Modo de operación)** Seleccione el método adecuado para el extremo VPN remoto. – **Main (Principal):** el modo principal es más lento pero también más seguro. – **Aggressive (Agresivo):** el modo agresivo es más rápido pero menos seguro. ■ **Local Identity (Identidad local)** Seleccione la opción deseada para hacer coincidir el parámetro de identidad remota en el otro extremo del túnel. – Local IP Address (Dirección IP local): la dirección IP (Internet) de la WAN. – Name (Nombre): el nombre del dominio. ■ **Remote Identity (Identidad remota)** Seleccione la opción deseada para hacer coincidir el parámetro de identidad local en el otro extremo del túnel. – Local IP Address (Dirección IP local): la dirección IP (Internet) de la WAN del extremo VPN remoto. – Name (Nombre): el nombre de dominio del extremo VPN remoto. ■ **Encryption (Cifrado)** Se trata del algoritmo de cifrado que se utiliza para la SA IKE. Debe coincidir con el parámetro que se utiliza en el otro extremo del túnel.

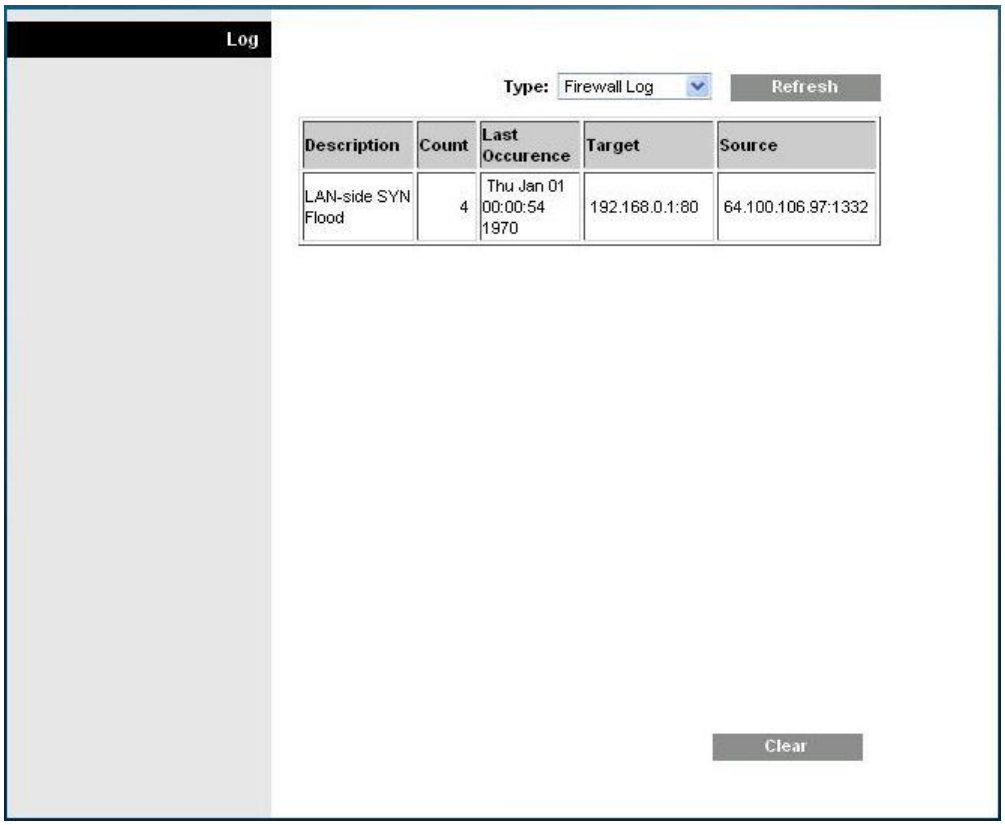
View Log (Ver registro)

La página Security VPN View Log (Seguridad > VPN > Ver registro) muestra los eventos capturados por el firewall. En el registro se muestran los elementos siguientes:

- Descripción del evento
- Número de eventos que han tenido lugar
- Última vez que se ha producido un evento
- Direcciones de destino y origen

Desde esta página puede ver los registros siguientes:

- Access log (Registro de acceso)
- Firewall log (Registro de firewall)
- VPN log (Registro de VPN)
- Parental Control log (Registro de control parental)



Pulse **Clear** (Borrar) para borrar los datos del registro.

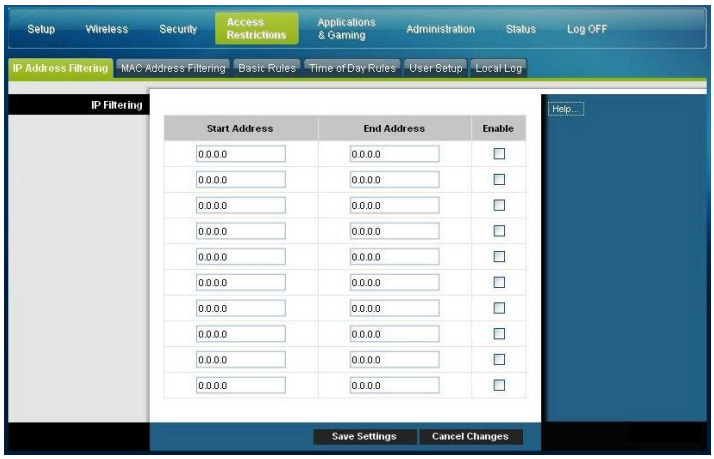
Control del acceso al gateway

Access Restrictions > IP Address Filtering (Restricciones de acceso > Filtrado de direcciones IP)

Utilice esta página para configurar los filtros de direcciones IP. Estos filtros bloquean el acceso a Internet a un intervalo de direcciones IP.

Nota: si no conoce los procedimientos de configuración de red detallados en esta sección, póngase en contacto con su proveedor de servicio antes de realizar cambios en los parámetros de configuración avanzados predeterminados de filtrado de IP del gateway residencial.

Seleccione la ficha **IP Address Filtering** (Filtrado de direcciones IP) para abrir la página Access Restrictions IP Address Filtering (Restricciones de acceso > Filtrado de direcciones IP). Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.



Access Restrictions > MAC Address Filtering (Restricciones de acceso > Filtrado de direcciones MAC)

Utilice esta página para configurar los filtros de direcciones MAC. Estos filtros le permiten permitir o bloquear el acceso a Internet a un intervalo de direcciones MAC en función de la dirección MAC.

Nota: si no conoce los procedimientos de configuración de red detallados en esta sección, póngase en contacto con su proveedor de servicio antes de realizar cambios en los parámetros de configuración avanzados predeterminados de filtrado de IP del gateway residencial.

Seleccione la ficha **MAC Address Filtering** (Filtrado de direcciones MAC) para abrir la página Access Restrictions MAC Address Filtering (Restricciones de acceso > Filtrado de direcciones MAC).

El menú desplegable **Block/Pass** (Bloquear/Permitir) le permite bloquear o permitir el acceso a Internet a las direcciones MAC de los dispositivos incluidos en la tabla de filtros de direcciones MAC. En la siguiente tabla se describe la función del menú desplegable **Block/Pass** (Bloquear/Permitir). Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Nombre del campo	Descripción
MAC Filtering (Filtrado de MAC)	**Block Listed (Bloquear enumeradas) (valor predeterminado)** Seleccione **Block Listed** (Bloquear enumeradas) para denegar el acceso a Internet a las direcciones MAC de los dispositivos incluidos en la tabla. Todas las demás direcciones MAC tendrán acceso a Internet.
	Pass Listed (Permitir enumeradas) Seleccione **Pass Listed** (Permitir enumeradas) para permitir el acceso a Internet solo a las direcciones MAC de los dispositivos incluidos en la tabla. Las direcciones MAC *no* incluidas en la tabla no tendrán acceso a Internet.

Teclas de función

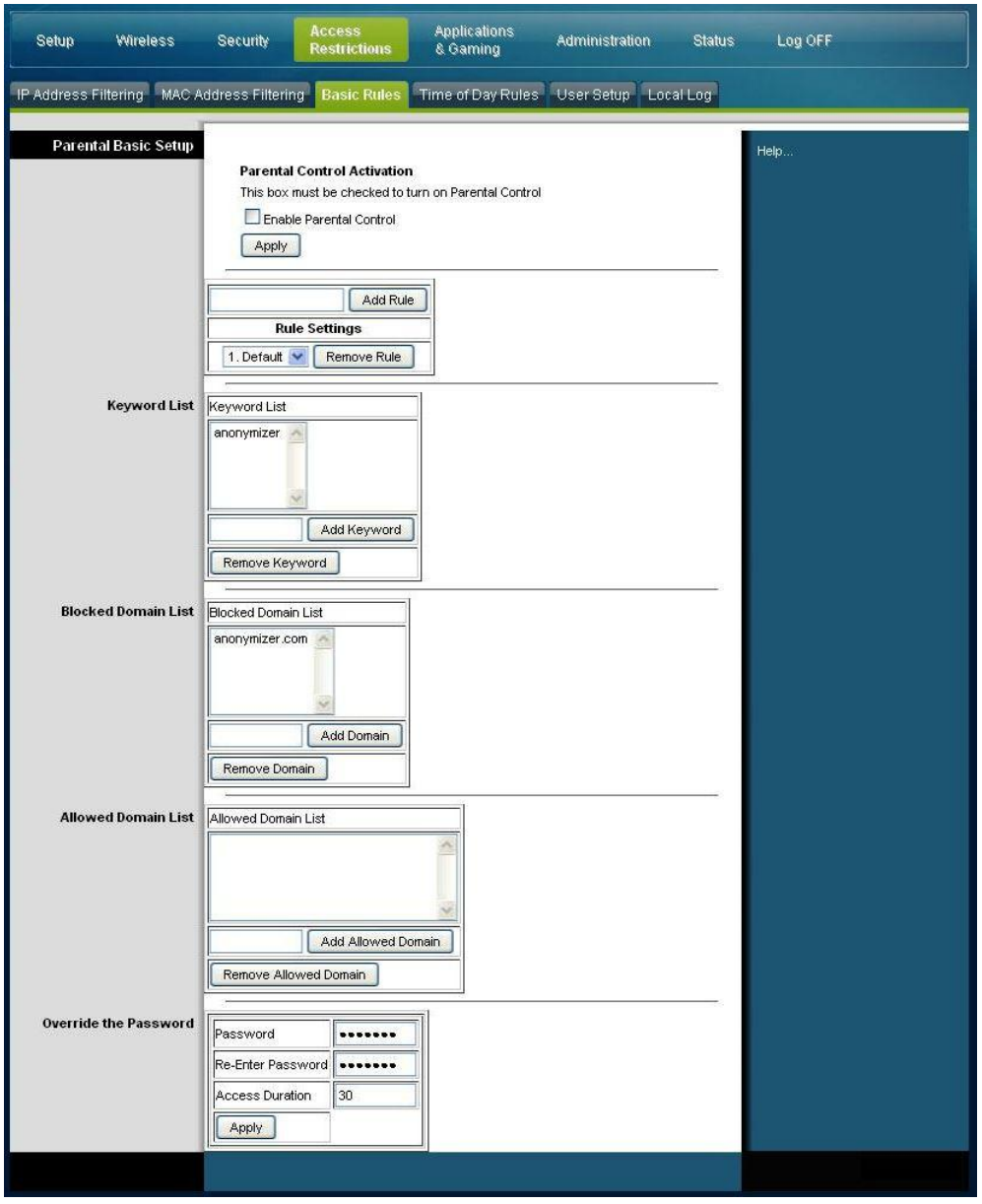
Las siguientes teclas de función aparecen en la página Advanced Settings - MAC Address Filtering (Configuración avanzada - Filtrado de direcciones MAC).

Tecla	Descripción
Apply (Aplicar)	Guarda los valores introducidos en los campos sin cerrar la página.
Add MAC Address (Agregar dirección MAC)	Permite guardar la dirección MAC introducida en el campo de texto asociado.
Remove MAC Address (Quitar dirección MAC)	Elimina la dirección MAC seleccionada.
Clear All (Borrar todo)	Elimina todas las direcciones MAC definidas.

Access Restrictions > Basic Rules (Restricciones de acceso > Normas básicas)

Las restricciones de acceso le permiten bloquear o permitir determinados tipos de uso y tráfico de Internet, como el acceso a Internet, aplicaciones designadas, sitios web y tráfico entrante durante días y horas específicos. La página Access Restrictions > Basic Rules (Restricciones de acceso > Normas básicas) le permite configurar controles parentales en el gateway residencial y supervisar a las personas que disponen de autorización para definir los controles parentales.

Seleccione la ficha **Basic Rules** (Normas básicas) para abrir la página Access Restrictions > Basic Rules (Restricciones de acceso > Normas básicas).



Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de red para el gateway residencial. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Parental Control Basic Setup (Configuración básica del control parental)	**Parental Control Activation (Activación del control parental)** Permite activar o desactivar los controles parentales. Para activar los controles parentales, active la casilla **Enable Parental Control** (Activar control parental) y pulse **Apply** (Aplicar). Para desactivar los controles parentales, desactive la casilla **Enable Parental Control** (Activar control parental) y pulse **Apply** (Aplicar). **Add Rule (Agregar norma)** Agrega y guarda una nueva norma a la lista de normas de contenido. **Remove Rule (Quitar norma)** Quita la norma seleccionada de la lista de normas de contenido.
Keyword List (Lista de palabras clave)	**Keyword List (Lista de palabras clave)** Permite crear una lista de palabras clave. El gateway bloqueará los intentos de acceder a una dirección URL que contenga cualquiera de las palabras clave de la lista. **Add/Remove Keyword (Agregar/quitar palabra clave)** Permite agregar palabras clave nuevas a la lista o eliminar de ésta las palabras clave seleccionadas.
Blocked Domain List (Lista de dominios bloqueados)	**Blocked Domain List (Lista de dominios bloqueados)** Permite crear una lista de dominios a los que el gateway debe bloquear el acceso. El gateway bloqueará los intentos de acceder a cualquiera de los dominios de esta lista. **Add/Remove Domain (Agregar/quitar dominio)** Permite agregar dominios nuevos a la lista o eliminar de ésta los dominios seleccionados.
Allowed Domain List (Lista de dominios permitidos)	**Allowed Domain List (Lista de dominios permitidos)** Permite crear una lista de dominios a los que el gateway autoriza el acceso. **Add/Remove Allowed Domain (Agregar/quitar dominio permitido)** Permite agregar dominios nuevos a la lista o eliminar de ésta los dominios seleccionados.

Sección	Descripción de campos
Override the Password (Anular contraseña)	**Password (Contraseña)** Permite crear una contraseña para sustituir temporalmente las restricciones de acceso del usuario a un sitio de Internet bloqueado. **Re-Enter Password (Volver a introducir contraseña)** Repita la contraseña para confirmar la contraseña de sustitución del campo anterior. **Access Duration (Duración de acceso)** Permite designar una cantidad de tiempo en minutos durante los cuales la contraseña de sustitución permitirá el acceso temporal a un sitio de Internet bloqueado. **Apply (Aplicar)** Guarda todas las adiciones, las modificaciones y los cambios.

Para utilizar el bloqueo de palabras clave y dominios

El bloqueo de palabras clave o dominios le permite restringir el acceso a sitios de Internet mediante el bloqueo del acceso a esos sitios basado en una cadena de palabras o texto contenido en las direcciones URL utilizadas para acceder a esos sitios de Internet.

El bloqueo de dominios le permite restringir el acceso a sitios web basándose en el nombre de dominio del sitio. El nombre de dominio es la parte de la URL que antecede la conocida extensión .COM, .ORG o .GOV.

El bloqueo de palabras clave le permite bloquear el acceso a sitios de Internet basándose en una cadena de palabras clave o texto que esté presente en cualquier lugar de la URL, no solo en el nombre de dominio.

Nota: la función de bloqueo de dominios bloquea el acceso a cualquier dominio de la lista de dominios. También bloquea los dominios que contengan alguna parte que coincida exactamente con las entradas de la lista.

Por ejemplo, si introduce **ejemplo.com** como dominio, se bloquearán todos los sitios que contengan "ejemplo.com". Por lo general, no conviene incluir "www." en un nombre de dominio porque de esa manera se limita el bloqueo exclusivamente al sitio que coincida exactamente con ese nombre de dominio. Por ejemplo, si introduce www.ejemplo.com en la lista, solo se bloqueará el sitio que coincida exactamente con ese nombre. Por consiguiente, si no incluye "www.", se bloquearán todos los sitios dentro de "ejemplo.com" y asociados con éste.

Block Access to Websites (Bloquear acceso a sitios web)

Si desea bloquear el acceso a sitios web, utilice la **Blocked Domain List** (Lista de dominios bloqueados) o la **Keyword List** (Lista de palabras clave)

Para utilizar la **Blocked Domain List** (Lista de dominios bloqueados), introduzca las URL o los nombres de dominio de los sitios web que desea bloquear.

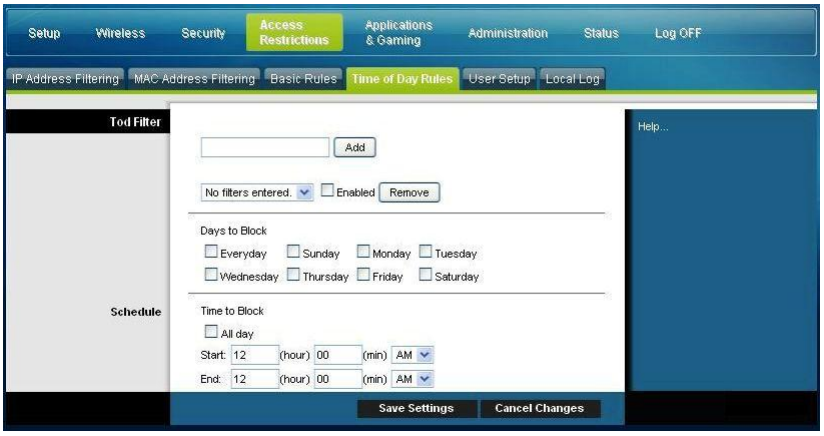
Utilice la **Keyword List** (Lista de palabras clave) para introducir las palabras clave que desea bloquear. Si alguna de las palabras clave aparece en la URL de un sitio web, se bloqueará el acceso a dicho sitio. Tenga presente que solo se comprueba la URL, no el contenido de cada página web.

Access Restrictions > Time of Day Rules (Restricciones de acceso > Normas de hora del día)

Utilice la página Access Restrictions > Time of Day Rules (Restricciones de acceso > Normas de hora del día) para configurar los filtros de acceso a la Web para bloquear todo el tráfico de Internet entre los dispositivos de red indicados, basándose en el día de la semana y la hora del día que seleccione.

Seleccione la ficha **Time of Day Rules** (Normas de hora del día) para abrir la página Access Restrictions > Time of Day Rules (Restricciones de acceso > Normas de hora del día). La siguiente ilustración es un ejemplo de la página Access Restrictions > Time of Day Rules (Restricciones de acceso > Normas de hora del día).

Nota: el gateway residencial utiliza el reloj de hora del día de la red que gestiona su proveedor de servicios de datos. El reloj de hora del día debe ser preciso y representar la hora del día en su zona horaria para que esta característica funcione correctamente. Compruebe que las páginas Status (Estado) y Set Time (Establecer hora) reflejen la hora del día correcta. Si no reflejan la hora del día correcta, póngase en contacto con su proveedor de servicios de datos. También puede ajustar estos parámetros para que tengan en cuenta la diferencia.



Descripción de la página Access Restrictions > Time of Day Rules (Restricciones de acceso > Normas de hora del día)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de red para su gateway residencial. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Tod Filter (Filtro hora del día)	**Add (Agregar)** Permite agregar un nuevo filtro o norma de acceso de hora del día. Introduzca el nombre del filtro y pulse la tecla **Add** (Agregar) para agregar el filtro a la lista. Las normas de hora del día se utilizan para restringir el acceso a Internet según el día y la hora. **Remove (Quitar)** Quita el filtro seleccionado de la lista de filtros de hora del día.
Schedule (Programación)	**Days to Block (Bloquear días)** Le permite controlar el acceso basándose en los días de la semana. **Time to Block (Bloquear hora)** Le permite controlar el acceso basándose en la hora del día.

Access Restrictions > User Setup (Restricciones de acceso > Configuración de usuario)

Utilice la página Access Restrictions > User Setup (Restricciones de acceso > Configuración de usuario) para configurar cuentas y perfiles de usuario adicionales para los miembros de la familia. Pueden asignarse niveles personalizados de acceso a Internet a cada perfil, según lo definan las normas de acceso asignadas al perfil de usuario.

Importante: estas cuentas adicionales no otorgan acceso administrativo al gateway.

Nota: una vez que haya definido y activado los perfiles de usuario, los usuarios deberán iniciar sesión cada vez que deseen acceder a Internet. El usuario puede conectarse cuando aparezca la pantalla emergente de conexión en su navegador web. El usuario debe introducir su nombre de usuario y contraseña correctos para obtener el acceso a Internet.

Seleccione la ficha **User Setup** (Configuración de usuario) para abrir la página Access Restrictions > User Setup (Restricciones de acceso > Configuración de usuario).

Descripción de la página Access Restrictions > User Setup (Restricciones de acceso > Configuración de usuario)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de usuario para su gateway residencial. Cuando haya finalizado su selección, pulse **Save Settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
User Configure (Parámetros de usuario)	**Add User (Agregar usuario)** Permite agregar un nuevo perfil de usuario. Introduzca el nombre del usuario y pulse la tecla **Add User** (Agregar usuario) para agregar el usuario a la lista. **User Settings (Configuración de usuario)** Le permite editar un perfil de usuario mediante el menú desplegable correspondiente. El menú desplegable le permite abrir el perfil que desea editar. Los nombres de usuario y las contraseñas distinguen entre mayúsculas y minúsculas. Asegúrese de activar la casilla **Enable** (Activar) para activar el perfil de usuario. Si un perfil no está activo, ese usuario no tendrá acceso a Internet. Para quitar un perfil de usuario, utilice el menú desplegable para seleccionar el usuario que va a quitar y pulse el botón **Remove User** (Quitar usuario). **Password (Contraseña)** Introduzca en este campo la contraseña del usuario seleccionado. Los usuarios deben introducir su nombre de usuario y contraseña cada vez que utilicen Internet. Los nombres de usuario y las contraseñas distinguen entre mayúsculas y minúsculas. **Nota:** el gateway residencial autorizará el acceso a Internet a los usuarios de acuerdo con las normas seleccionadas en esta página para cada usuario. **Re-Enter Password (Volver a introducir contraseña)** Repita la contraseña para confirmar la contraseña del campo anterior. **Trusted User (Usuario de confianza)** Active esta casilla si el usuario seleccionado se va a designar como usuario de confianza. Los usuarios de confianza no están sujetos a las normas de acceso a Internet. **Content Rule (Norma de contenido)** Seleccione la norma de contenido para el perfil de usuario actual. Primero se deben definir las normas de contenido en la página Rules Configuration (Configuración de normas). Para acceder a la página de configuración de normas, pulse la ficha "Basic Rules" (Normas básicas) de esta página. **Time Access Rule (Norma de acceso por hora)** Seleccione la norma de acceso por hora para el perfil de usuario actual. Primero se deben definir las normas de hora de acceso en la página Time of Day Rules (Normas de hora del día). Para acceder a la página Time of Day Rules (Normas de hora del día) pulse la ficha "Time of Day Rules" (Normas de hora del día) de esta página. **Session Duration (Duración de sesión)** 1.440 minutos [valor predeterminado cuando se crea un usuario. De lo contrario, es 0 (cero)]. Introduzca la cantidad de tiempo en minutos que el usuario podrá acceder a Internet a partir de la hora en que se conecte con su nombre de usuario y contraseña. **Nota:** defina la duración de sesión como 0 (cero) para evitar que se agote el tiempo de espera de la sesión.

Sección	Descripción de campos
	Inactivity Time (Tiempo de inactividad) 60 minutos [valor predeterminado cuando se crea un usuario. De lo contrario, es 0 (cero)]. Introduzca la cantidad de tiempo durante una sesión de usuario en la que no hay actividad de acceso a Internet, lo que indica que el usuario ya no está en línea. Si se activa el temporizador de inactividad, la sesión de usuario se cerrará automáticamente. Para volver a obtener acceso a Internet, el usuario debe conectarse nuevamente con su nombre de usuario y contraseña. **Nota:** establezca el valor del tiempo de inactividad como 0 (cero) para evitar que se agote el tiempo de espera de la sesión.

Access Restrictions > Local Log (Restricciones de acceso > Registro local)

Esta página permite realizar un seguimiento, por usuario, de los intentos de ese usuario de acceder a los sitios de Internet restringidos. Desde esta página también puede ver los eventos capturados por la función de información de eventos de control parental.

Seleccione la ficha **Local Log** (Registro local) para abrir la página Access Restrictions > Local Log (Restricciones de acceso > Registro local).

La siguiente ilustración es un ejemplo de la página Access Restrictions > Local Log (Restricciones de acceso > Registro local).

Sección	Descripción de campos
Local Log (Registro local) **Parental Control - Event Log (Control parental - Registro de eventos)**	**Last Occurence (Último intento)** Muestra la hora del intento más reciente de acceder a un sitio de Internet restringido. **Action (Acción)** Muestra la acción emprendida por el sistema. **Target (Destino)** Muestra la dirección URL del sitio restringido. **User (Usuario)** Muestra el usuario que intentó acceder a un sitio restringido. **Source (Origen)** Muestra la dirección IP del PC que se utilizó para intentar acceder al sitio web restringido.

Configuración de aplicaciones y juegos

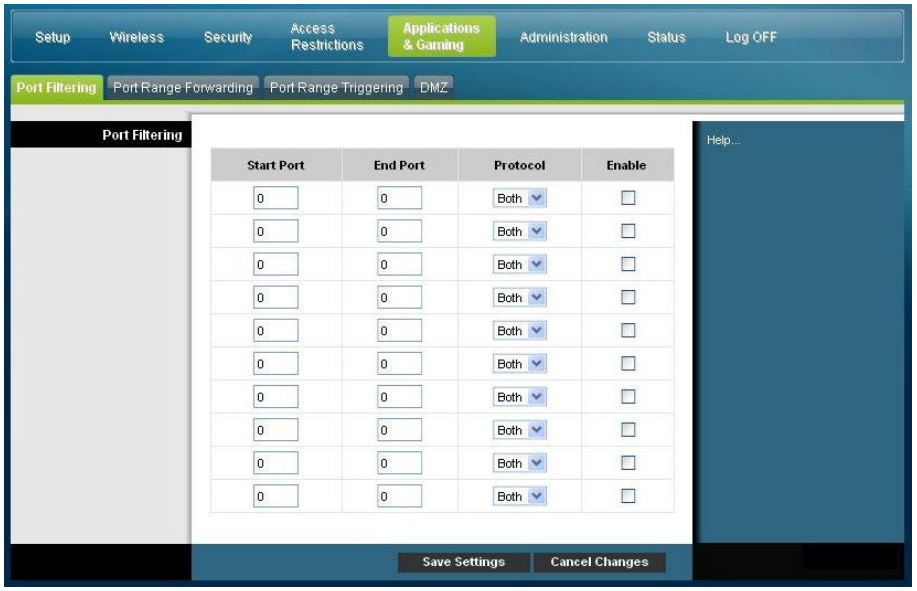
Información general

Casi todas las aplicaciones de Internet más conocidas son compatibles con los gateways de capas de aplicación (Application Layer Gateways, ALG). Los ALG ajustan automáticamente el firewall del gateway para permitir el paso de datos sin hacer ajustes personalizados. Le recomendamos que pruebe su aplicación antes de hacer cambios en esta sección.

Applications & Gaming > Port Filtering (Aplicaciones y juegos > Filtrado de puertos)

Utilice esta ventana para configurar los filtros de puertos de protocolo de control de transmisión (transmission control protocol, TCP) y protocolo de datagramas de usuario (user datagram protocol, UDP). Estos filtros impiden que un intervalo de puertos TCP/UDP acceda a Internet. También puede impedir que los PC envíen tráfico TCP/UDP saliente a la WAN sobre números de puerto IP específicos. Este filtro no es específico para una dirección IP o MAC. El sistema bloquea los intervalos de puertos específicos para todos los PC.

Seleccione la ficha **Port Filtering** (Filtrado de puertos) para abrir la página Applications & Gaming > Port Filtering (Aplicaciones y juegos > Filtrado de puertos).



Descripción de la página Applications & Gaming > Port Filtering (Aplicaciones y juegos > Filtrado de puertos)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar el filtrado de puertos para las funciones de aplicaciones y juegos utilizadas en su gateway residencial. Marque la casilla **Enable** (Activar) para activar el reenvío de puertos para la aplicación correspondiente. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Port Filtering (Filtrado de puertos)	**Start Port (Puerto inicial):** Inicio del intervalo de puertos. Introduzca el inicio del intervalo de números de puerto (puertos externos) que utiliza el servidor o la aplicación web. Consulte la documentación de software de la aplicación web para obtener más información.
	End Port (Puerto final): Final del intervalo de puertos. Introduzca el final del intervalo de números de puerto (puertos externos) que utiliza el servidor o la aplicación web. Consulte la documentación de software de la aplicación web para obtener más información.
	Protocol (Protocolo) Seleccione uno de los siguientes protocolos: ■ **TCP** ■ **UDP** ■ **Ambos**
	Enable (Activar): Marque esta casilla para activar el filtrado de los puertos indicados.

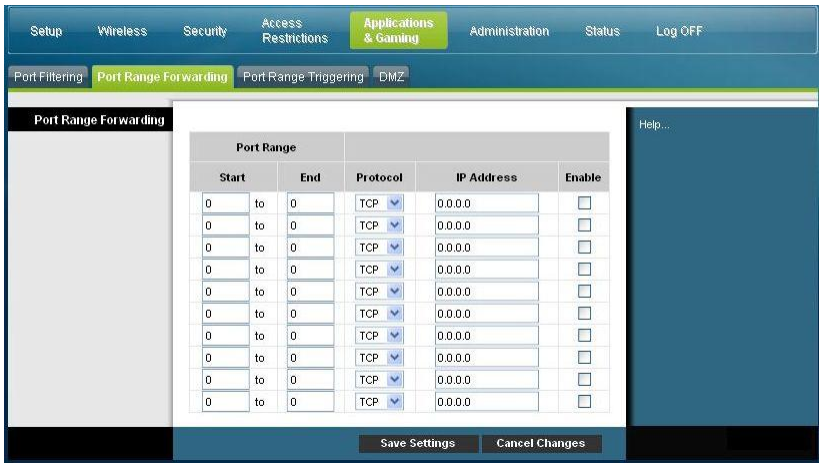
Applications & Gaming > Port Range Forwarding (Aplicaciones y juegos > Reenvío de intervalos de puertos)

Importante: el gateway normalmente implementa una función llamada Port Translation (Traducción de puerto). La traducción de puerto supervisa los puertos que están utilizando sus PC u otros dispositivos conectados a su LAN. Esta supervisión proporciona un nivel de seguridad adicional al que ofrece el firewall. Sin embargo, algunas aplicaciones exigen que el gateway utilice determinados puertos para conectarse a Internet.

Utilice Port Range Forwarding (Reenvío de intervalos de puertos) para reenviar los puertos desde la Internet pública a direcciones IP específicas de su red local. Seleccione la ficha **Port Range Forwarding** (Reenvío de intervalos de puertos) para abrir la página Applications & Gaming > Port Range Forwarding (Aplicaciones y juegos > Reenvío de intervalos de puertos).

Para el puerto inicial y final, seleccione un puerto del intervalo 49152 - 65535 recomendado. Tenga en cuenta que los puertos utilizados son específicos de cada programa, por lo cual debe comprobar aquellos cuyo reenvío exige el programa. Escriba el número de puerto o intervalo en ambas casillas. En la casilla de la dirección IP, escriba el nombre de la dirección IP del PC que se incluirá.

Nota: Port Range Forwarding (Reenvío de intervalos de puertos) expone de forma continua los puertos seleccionados a la Internet pública. Eso significa que el firewall del gateway ya no está activo en esos puertos. El dispositivo con la dirección IP de reenvío puede quedar expuesto a los ataques de piratas durante el reenvío del intervalo de puertos.



Descripción de la página Applications & Gaming > Port Range Forwarding (Aplicaciones y juegos > Reenvío de intervalos de puertos)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de reenvío de intervalos de puertos para su gateway residencial. Seleccione activar para cada uno. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

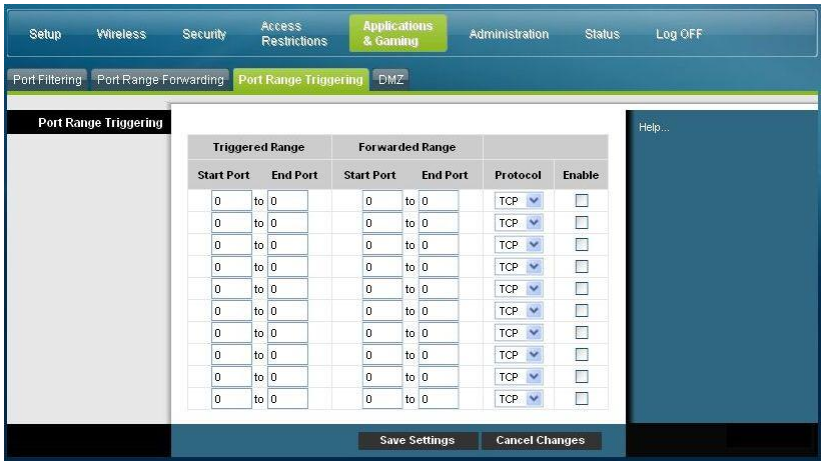
Sección	Descripción de campos
Port Range Forwarding (Reenvío de intervalos de puertos)	**Start (Inicio)** Para el puerto inicial, seleccione un puerto del intervalo 49152 - 65535 recomendado. Tenga en cuenta que los puertos utilizados son específicos de cada programa, por lo cual debe comprobar aquellos cuyo reenvío exige el programa.
	End (Final) Para el puerto final, seleccione un puerto del intervalo 49152 - 65535 recomendado. Tenga en cuenta que los puertos utilizados son específicos de cada programa, por lo cual debe comprobar aquellos cuyo reenvío exige el programa.

Sección	Descripción de campos
	Protocol (Protocolo) Seleccione uno de los siguientes protocolos: ■ TCP ■ UDP ■ Ambos
	IP Address (Dirección IP) Introduzca la dirección IP del equipo que se incluirá.
	Enable (Activar) Marque esta casilla para activar el reenvío de puertos para los puertos y direcciones IP que se indique.

Applications & Gaming > Port Range Triggering (Aplicaciones y juegos > Desencadenado de intervalos de puertos)

El desencadenado de intervalos de puertos es una manera dinámica de reenviar los puertos a uno de los PC de la LAN que los necesite en un momento determinado. Ese momento es cuando se ejecuta una aplicación específica que realiza algún evento que activa el router. Este evento debe ser un acceso saliente de un intervalo de puertos dado.

Seleccione la ficha **Port Range Triggering** (Desencadenado de intervalos de puertos) para abrir la página Applications & Gaming > Port Range Triggering (Aplicaciones y juegos > Desencadenado de intervalos de puertos).



Descripción de la página Applications & Gaming > Port Range Triggering (Aplicaciones y juegos > Desencadenado de intervalos de puertos)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de desencadenado de intervalos de puertos para el gateway residencial. Seleccione Activar para cada uno. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

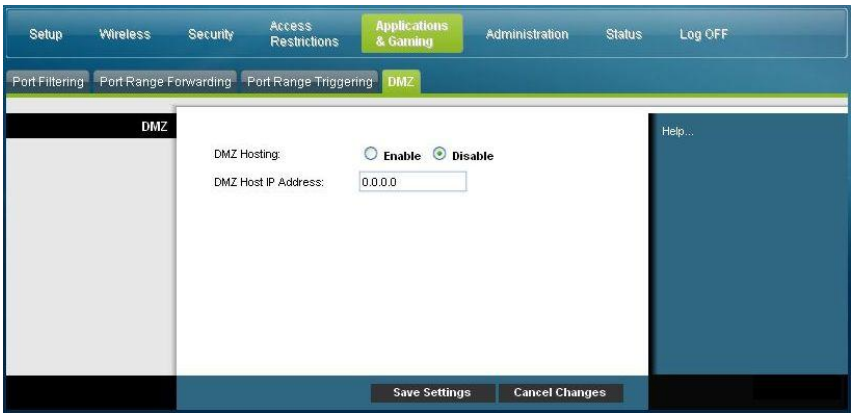
Sección	Descripción de campos
Port Range Triggering (Desencadenado de intervalos de puertos)	
Triggered Range (Intervalo desencadenado)	**Start Port (Puerto inicial)** Para el puerto inicial, seleccione un puerto del intervalo 49152 - 65535 recomendado. Tenga en cuenta que los puertos utilizados son específicos de cada programa, por lo cual debe comprobar aquellos cuyo reenvío exige el programa.
	End Port (Puerto final) Para el puerto final, seleccione un puerto del intervalo 49152 - 65535 recomendado. Tenga en cuenta que los puertos utilizados son específicos de cada programa, por lo cual debe comprobar aquellos cuyo reenvío exige el programa.
Forwarded Range (Intervalo reenviado)	**Start Port (Puerto inicial)** Para el puerto inicial, seleccione un puerto del intervalo 49152 - 65535 recomendado. Tenga en cuenta que los puertos utilizados son específicos de cada programa, por lo cual debe comprobar aquellos cuyo reenvío exige el programa.
	End Port (Puerto final) Para el puerto final, seleccione un puerto del intervalo 49152 - 65535 recomendado. Tenga en cuenta que los puertos utilizados son específicos de cada programa, por lo cual debe comprobar aquellos cuyo reenvío exige el programa.
	Protocol (Protocolo) Seleccione uno de los siguientes protocolos: ■ TCP ■ UDP ■ Ambos
	Enable (Activar) Marque la casilla Enable (Activar) para activar el reenvío de puertos para la aplicación correspondiente.

Applications and Gaming > DMZ (Aplicaciones y juegos > DMZ)

Utilice esta página para configurar una dirección IP cuyos puertos estén directamente expuestos a la Internet pública o a la Red de área amplia (Wide Area Network, WAN). El alojamiento de Zona desmilitarizada (Demilitarized Zone, DMZ) se conoce comúnmente como "host expuesto" y le permite especificar un destinatario de tráfico WAN que la Traducción de direcciones de red (Network Address Translation, NAT) no puede traducir a un PC local conocido.

Por lo general, los DMZ los utilizan las empresas que quieren alojar su propio servidor de Internet. DMZ permite colocar una dirección IP en el lado de Internet del firewall del gateway, mientras las demás permanecen protegidas tras el firewall.

El DMZ permite que un dispositivo esté accesible directamente al tráfico de Internet, como un servidor web (HTTP), un servidor FTP, un servidor SMTP (correo electrónico) y un servidor de sistemas de nombres de dominio (DNS). Seleccione la ficha **DMZ** para abrir la página Applications and Gaming > DMZ (Aplicaciones y juegos > DMZ).



Descripción de la página Applications and Gaming > DMZ (Aplicaciones y juegos > DMZ)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de desencadenado de intervalos de puertos para el gateway residencial. Seleccione Activar para cada dirección IP del host DMZ. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

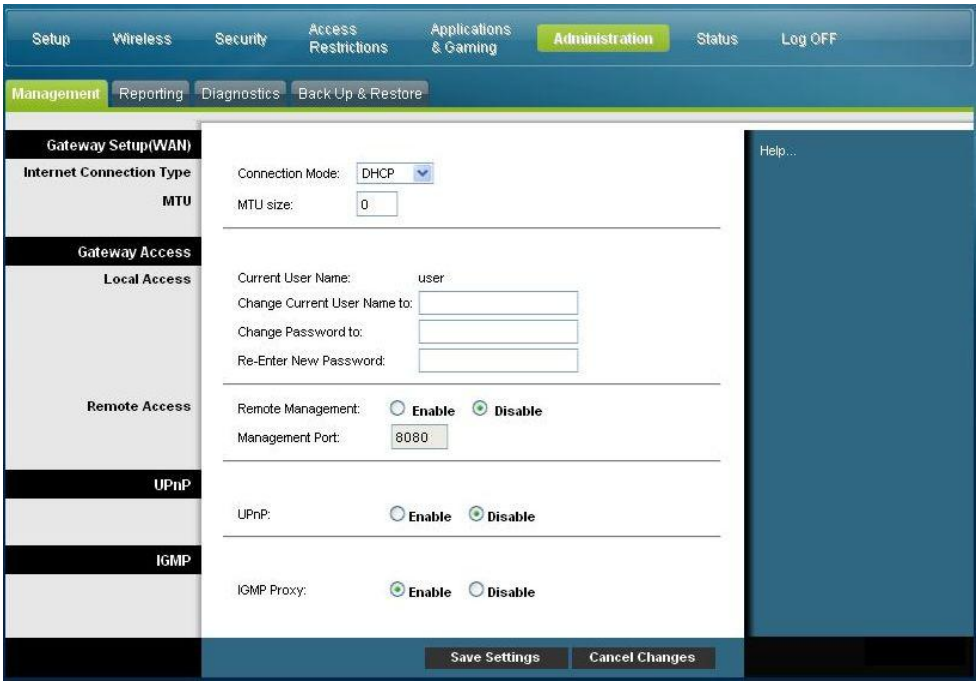
Sección	Descripción de campos
DMZ	**DMZ Hosting (Asignación de DMZ)** Seleccione la opción deseada: ■ **Enable (Activar)** ■ **Disable (Desactivar)**, (valor predeterminado)
	DMZ Host IP Address (Dirección IP de asignación de DMZ) DMZ permite que una dirección IP esté desprotegida mientras las demás permanecen protegidas. Introduzca la dirección IP del PC que quiere exponer a Internet en este campo.

Gestión del gateway

Administration > Management (Administración > Gestión)

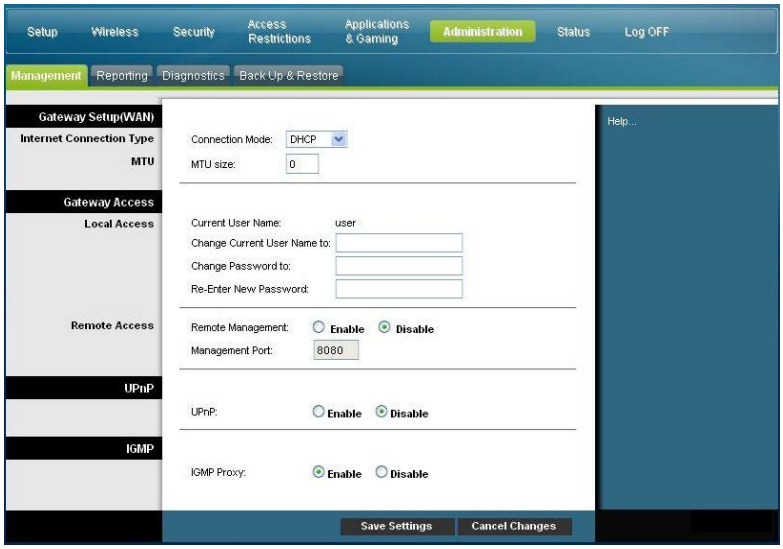
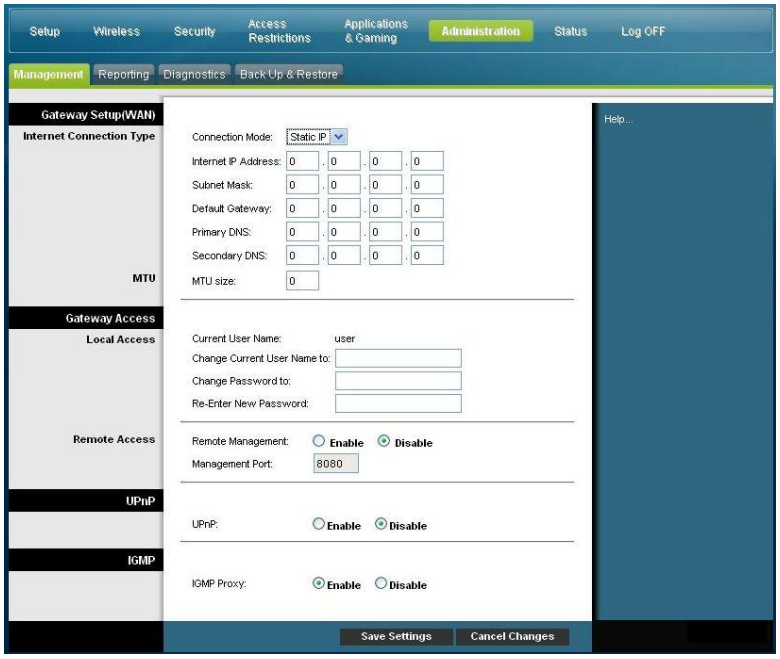
La pantalla Administration > Management (Administración > Gestión) permite que el administrador de la red administre determinadas funciones de acceso y seguridad del gateway. Seleccione la ficha **Management** (Gestión) para abrir la página Administration > Management (Administración > Gestión).

Importante: la página siguiente se abre cuando el modo de conexión es **DHCP** (valor predeterminado). La página que se abre cuando se selecciona **Static IP** (IP estática) se muestra y describe más adelante en esta misma sección.



Descripción de la página Administration > Management (Administración > Gestión)

Utilice las descripciones e instrucciones de la siguiente tabla para configurar la administración y gestión del gateway residencial cuando se selecciona el modo de conexión DHCP o IP estática. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Campo	Descripción
Gateway Setup (WAN) (Configuración del gateway [WAN])	**Connection Mode (Modo de conexión)** Este parámetro le permite determinar la manera en que la WAN (o la interfaz del gateway con Internet) obtiene su dirección IP. **DHCP** (valor predeterminado)
Internet Connection Type (Tipo de conexión a Internet)	Permite que el gateway obtenga automáticamente una dirección IP pública.  **Static IP (IP estática)** Le permite especificar la dirección IP de la WAN y la información del servidor correspondiente como los valores estáticos o fijos que se utilizarán siempre que el gateway esté en línea 

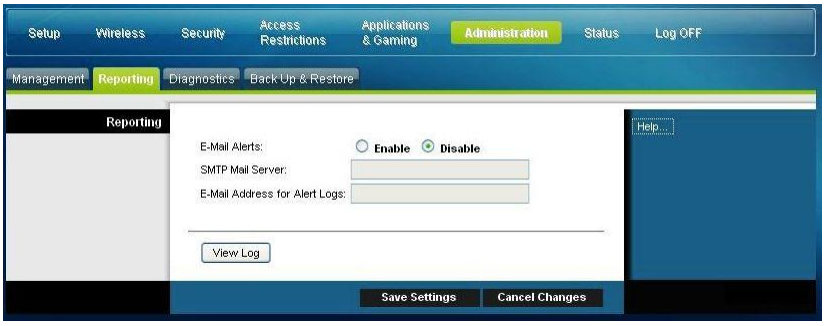
Campo	Descripción
	Internet IP Address (Dirección IP de Internet) Introduzca la dirección IP del gateway (como se ve desde Internet). **Subnet Mask (Máscara de subred)** Introduzca la máscara de subred del gateway (como se ve desde Internet, incluido su proveedor de servicio). **Default Gateway (Gateway predeterminado)** Introduzca el gateway predeterminado del servidor del proveedor de servicio. **Primary DNS (DNS principal)** Introduzca las direcciones IP del servidor de nombres de dominio principal proporcionado por su proveedor de servicios. Este campo es obligatorio. **Secondary DNS (DNS secundario)** Introduzca las direcciones IP del servidor de nombres de dominio secundario proporcionado por su proveedor de servicios. Este campo es optativo.
MTU	**MTU size (Tamaño MTU)** MTU es la unidad de transmisión máxima. El tamaño de MTU especifica el tamaño de paquete máximo permitido para transmitir por Internet. . Valor predeterminado = 0 (1.500 bytes)
Gateway Access (Acceso al gateway)	**Current User Name (Nombre de usuario actual)** Identifica al usuario conectado en un momento determinado.
Local Access (Acceso local)	**Change Current User Name to (Cambiar nombre de usuario actual a)** Este campo le permite cambiar su nombre de usuario. Para cambiar su nombre de usuario, introduzca el nuevo nombre de usuario en este campo y pulse **Save Settings** (Guardar parámetros) para aplicar el cambio. **Nota:** el nombre de usuario predeterminado es un campo en blanco. **Change Password to (Cambiar contraseña por)** Este campo le permite cambiar su contraseña. Para cambiar su contraseña, introduzca la contraseña nueva en este campo. A continuación, repita su contraseña nueva en el campo **Re-Enter New Password** (Volver a introducir nueva contraseña) y pulse **Save Settings** (Guardar parámetros) para aplicar el cambio. **Nota:** la contraseña predeterminada es un campo en blanco.

Campo	Descripción
	Re-Enter New Password (Volver a introducir nueva contraseña) Le permite volver a introducir la nueva contraseña. Debe introducir la misma contraseña que la introducida en el campo **Change Password to (Cambiar contraseña por).** Una vez que haya introducido nuevamente la contraseña nueva, pulse **Save Settings** para aplicar el cambio.
Remote Access (Acceso remoto)	**Remote Management (Gestión remota)** Le permite activar o desactivar la gestión remota. Esta función le permite acceder y gestionar los parámetros de su gateway desde Internet cuando esté fuera de casa. Para permitir el acceso remoto, seleccione **Enable** (Activar). De lo contrario, mantenga el valor predeterminado, **Disable** (Desactivar). El protocolo HTTP es obligatorio para la gestión remota. Para acceder al dispositivo de forma remota, introduzca https://xxx.xxx.xxx.xxx:8080 (las "x" representan la dirección IP de Internet pública del dispositivo, y 8080 representa el puerto indicado) en el campo **Address** (Dirección) de su navegador web. **Management Port (Puerto de gestión)** Introduzca el número de puerto que se abrirá al acceso exterior. El valor predeterminado es 8080. Este puerto debe utilizarse cuando establezca una conexión remota.
UPnP	**UPnP** El sistema Universal Plug and Play (UPnP) permite a Windows XP y Vista configurar automáticamente el gateway para varias aplicaciones de Internet, como juegos y videoconferencias. Si desea utilizar UPnP, mantenga el valor predeterminado, **Enable** (Activar). De lo contrario, seleccione **Disable** (Desactivar).
IGMP	**IGMP Proxy (Proxy de IGMP)** El protocolo multidifusión de grupo de Internet (Internet Group Multicast Protocol, IGMP) se utiliza para establecer la pertenencia a un grupo de multidifusión y se suele emplear para aplicaciones de transmisión de multidifusión. Por ejemplo, puede tener televisión por protocolo de Internet (Internet Protocol Television, IPTV) con varios descodificadores en la misma red local. Estos descodificadores ejecutan distintas transmisiones de vídeo al mismo tiempo, de modo que debe utilizar la función IGMP del router. El reenvío (proxy) por IGMP es un sistema que mejora la multidifusión de los clientes del lado LAN. Si los clientes admiten esta opción, mantenga el valor predeterminado, **Enable** (Activar). De lo contrario, seleccione **Disable** (Desactivar).

Administration > Reporting (Administración > Informes)

Los informes de administración le permiten enviar por correo electrónico diversas actividades de sistema a su dirección de correo electrónico.

Seleccione la ficha **Reporting** (Informes) para abrir la página Administration > Reporting (Administración > Informes).



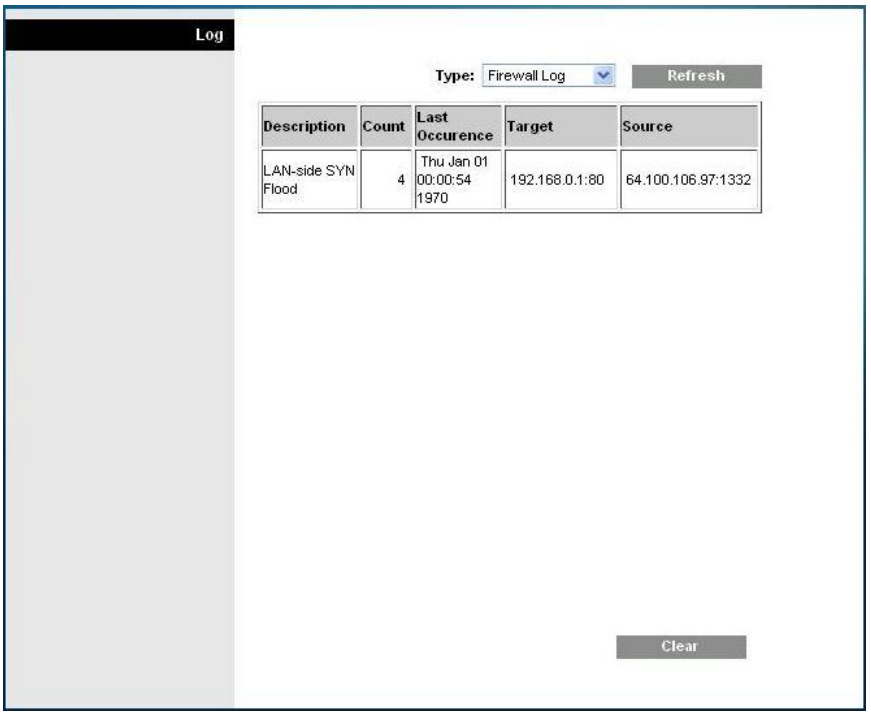
Utilice las descripciones e instrucciones de la siguiente tabla para configurar la función de informes en el gateway. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Reporting (Informes)	**E-Mail Alerts (Alertas de correo electrónico)** Si está activada esta función, se enviará un correo electrónico de inmediato cuando se detecten eventos notificables. Para utilizar esta función, deberá proporcionar la información necesaria sobre la dirección de correo electrónico.
	SMTP Mail Server (Servidor de correo SMTP) Introduzca la dirección (nombre de dominio) o la dirección IP del servidor SMTP (del inglés *Simple Mail Transport Protocol*, protocolo simple de transferencia de correo) que utiliza para el correo electrónico saliente.
	E-Mail Address for Alert Logs (Dirección de correo electrónico para registros de alertas) Introduzca la dirección de correo electrónico que debe recibir los registros.

View Log (Ver registro)

Para ver los registros, lleve a cabo los pasos siguientes.

1 Pulse **View Log** (Ver registro). Se abre una nueva ventana con la página de datos del registro.



2 Para ver un registro determinado, seleccione una de las siguientes opciones del menú desplegable Type (Tipo):

- All (Todos)
- Access Log (Registro de acceso)
- Firewall Log (Registro de firewall)
- VPN Log (Registro de VPN)

3 Una vez que hayan aparecido los datos del registro, utilice una de las siguientes opciones:

- Pulse el botón **Page Refresh** (Actualizar) para actualizar el registro.
- Pulse el botón **Clear** (Borrar) para borrar toda la información del registro actual.
- Pulse el botón **Previous Page** (Atrás) para volver a la información previamente visualizada.
- Pulse el botón **Next Page** (Siguiente) para ver la siguiente sección del registro, si está disponible.

Administration > Diagnostics (Administración > Diagnóstico)

El diagnóstico de administración le permite comprobar el estado de su conexión a Internet mediante una prueba de Ping.

Seleccione la ficha **Diagnostics** (Diagnóstico) para abrir la página Administration > Diagnostics (Administración > Diagnóstico).

Utilice las descripciones e instrucciones de la siguiente tabla para configurar los parámetros de la función diagnóstico para su gateway. Cuando haya finalizado su selección, pulse **Save settings** (Guardar parámetros) para aplicar los cambios o **Cancel Changes** (Cancelar cambios) para cancelarlos.

Sección	Descripción de campos
Ping Test (Prueba de ping)	
Ping Test Parameters (Parámetros de prueba de ping)	**Ping Target IP (IP de destino de ping)** Introduzca la dirección IP a la que desea hacer un ping. **Ping Size (Tamaño de ping)** Tamaño del paquete que desea utilizar. **Number of Pings (Número de pings)** Número de veces que desea realizar un ping del dispositivo de destino. **Ping Interval (Intervalo de ping)** Período de tiempo (en milisegundos) entre cada ping. **Ping Timeout (Tiempo de espera de ping)** Período de tiempo de espera (en milisegundos) deseado. Si no se recibe respuesta en este período Ping, la prueba de ping se considera errónea.

Sección	Descripción de campos
	Start Test (Iniciar prueba) Para iniciar una prueba, lleve a cabo los pasos siguientes. **1** Pulse **Start Test** (Iniciar prueba) para iniciar la prueba. Se abre una nueva página con un resumen de los resultados de la prueba. **2** Pulse **Save Settings** (Guardar parámetros) para guardar los resultados de la prueba, o pulse **Cancel Changes** (Cancelar cambios) para cancelar la prueba.

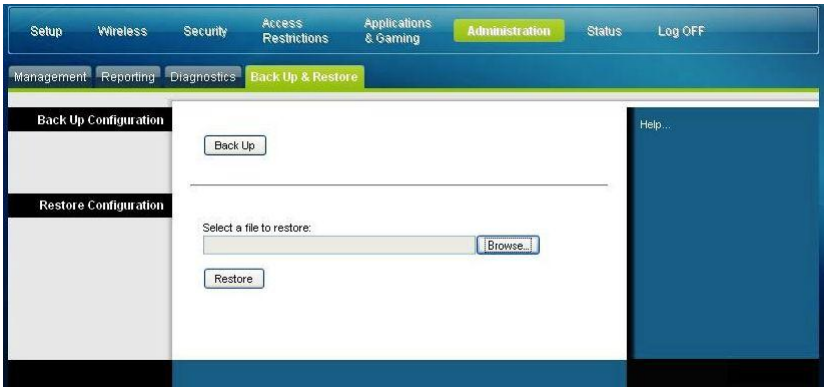
Administration > Backup & Restore (Administración > Copia de seguridad y restauración)

Administration > Backup & Restore (Administración > Copia de seguridad y restauración) le permite hacer una copia de seguridad de la configuración del gateway y guardarla en su equipo. Puede utilizar este archivo para restaurar una configuración guardada anteriormente para el gateway.

Seleccione la ficha **Backup & Restore** (Copia de seguridad y restauración) para abrir la página Administration > Backup & Restore (Administración > Copia de seguridad y restauración).

PRECAUCIÓN:

Al cargar un archivo de configuración se destruirán (sobrescribirán) todos los parámetros existentes.



Sección	Descripción de campos
Back Up Configuration (Copia de seguridad de la configuración)	Utilice la función de copia de seguridad de la configuración para guardar una copia de la configuración actual y guardar el archivo en el PC. Pulse **Back Up** (Copia de seguridad) para iniciar la descarga.
Restore Configuration (Restaurar configuración)	Utilice la función de restauración de la configuración para restaurar un archivo de configuración guardado previamente. Pulse **Browse** (Examinar) para seleccionar el archivo de configuración y, a continuación, pulse **Restore** (Restaurar) para cargar el archivo de configuración en el dispositivo.

Administration > Factory Defaults (Administración > Parámetros predeterminados)

La página Administration > Factory Defaults (Administración > Parámetros predeterminados) le permite restaurar la configuración a los parámetros predeterminados. Seleccione la ficha **Factory Defaults** (Valores predeterminados) para abrir la página Administration > Factory Defaults (Administración > Parámetros predeterminados).

PRECAUCIÓN:

Si restaura los valores predeterminados, el gateway perderá todos los parámetros que haya introducido. Antes de restablecer el gateway a los valores predeterminados, escriba todos sus parámetros personalizados. Tras restablecer los parámetros predeterminados, deberá volver a introducir todos los valores de configuración personalizados.

Restauración de los parámetros predeterminados

Para restaurar los valores predeterminados, pulse **Restore Factory Defaults** (Restaurar valores predeterminados) para restablecer todos los parámetros de la configuración a sus valores predeterminados. Los parámetros que haya guardado se perderán al restaurar los parámetros predeterminados.

Supervisión del estado del gateway

En esta sección se describen las opciones disponibles en la ficha Status (Estado) que puede utilizar para supervisar el estado del gateway residencial y realizar un diagnóstico del dispositivo y de la red.

Status > Gateway (Estado > gateway)

La página Status > Gateway (Estado > gateway) muestra información sobre el gateway y sus parámetros actuales. La información que aparece en pantalla varía según el tipo de conexión a Internet que utilice.

Seleccione la ficha **Gateway** (gateway) para abrir la pantalla de estado del gateway. Pulse **Refresh** (Actualizar) para actualizar los datos que aparecen en pantalla.

Utilice las descripciones de la siguiente tabla para revisar el estado de su gateway y su conexión a Internet.

Sección	Descripción de campos
Gateway Information (Información del gateway)	**Firmware Version (Versión del firmware)** Número de versión del firmware. **MAC Address (CM MAC Address) [Dirección MAC (Dirección CM MAC)]** Dirección alfanumérica exclusiva para la interfaz coaxial del Cablemodem que se utiliza para conectar al CMTS (del inglés *Cable Modem Termination System*, sistema de terminación de Cablemodem) en el terminal principal. Una dirección de Control de acceso a los medios (Media access control, MAC) es una dirección de hardware que identifica de forma exclusiva a cada nodo de una red. **Current Time (Hora actual)** Se muestra la hora, basada en la zona horaria que se haya seleccionado en la página Basic Setup (Configuración básica).

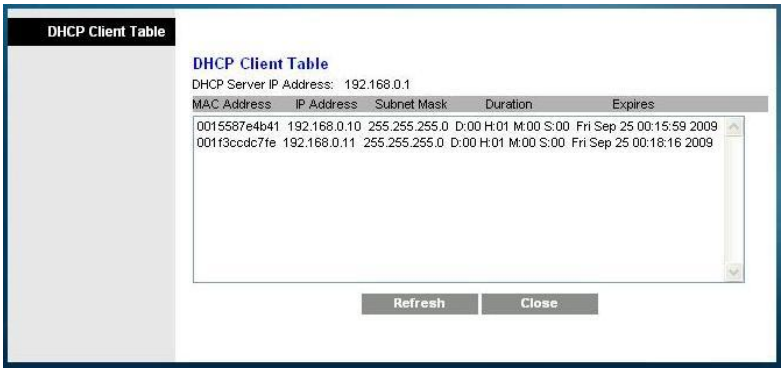
Sección	Descripción de campos
Internet Connection (Conexión a Internet)	**IP Address (Dirección IP)** Muestra la dirección IP de la interfaz WAN. Esta dirección se asigna al gateway cuando está en línea. **Subnet Mask (Máscara de subred)** Muestra la máscara de subred del puerto WAN. Su ISP asigna automáticamente esta dirección al puerto WAN salvo cuando se ha configurado una dirección IP estática. **Default Gateway (Gateway predeterminado)** Dirección IP del gateway predeterminado del ISP **DNS1-3** Direcciones IP del DNS que actualmente utiliza el gateway. **WINS** Direcciones IP del WINS que actualmente utiliza el gateway.

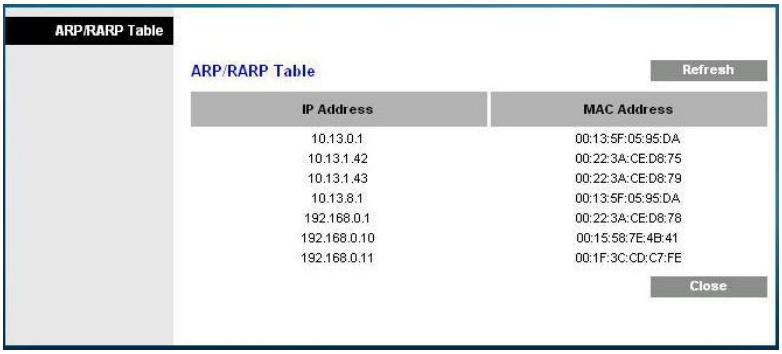
Status > Local Network (Estado > Red local)

La página Status > Local Network (Estado > Red local) muestra información sobre el estado de la red de área local.

Seleccione la ficha **Local Network** (Red local) para abrir la página Status > Local Network (Estado > Red local). Pulse **Refresh** (Actualizar) para actualizar los datos de la página.

Utilice las descripciones de la siguiente tabla para revisar el estado de su gateway y su conexión a Internet.

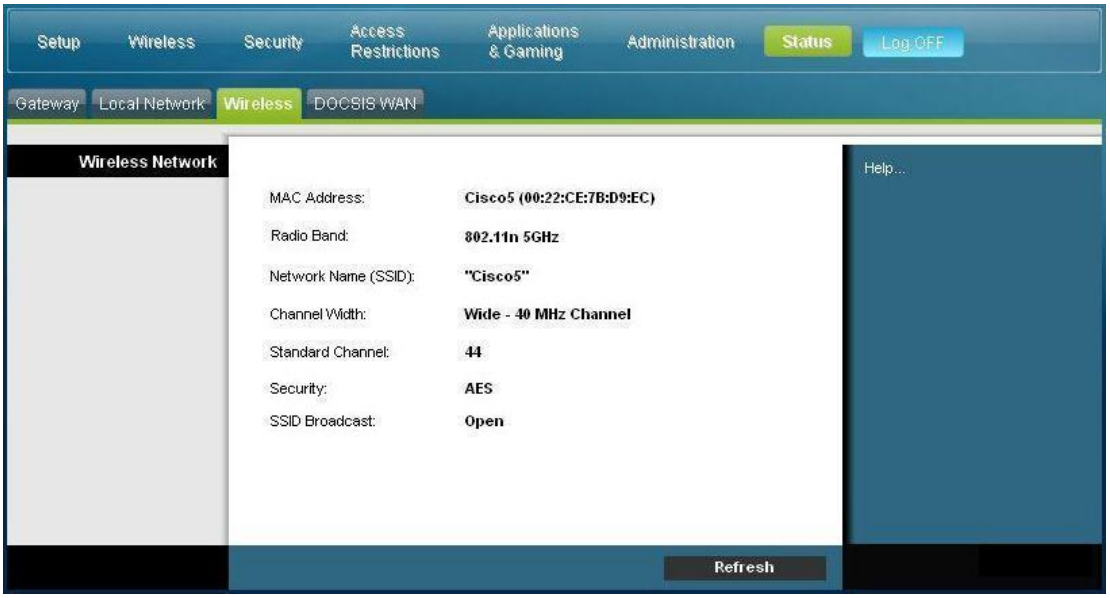
Sección	Descripción de campos
Local Network **(Red local)**	**MAC Address (Dirección MAC)** Dirección alfanumérica exclusiva de la red doméstica LAN privada. Una dirección MAC es una dirección de hardware que identifica de forma exclusiva a cada nodo de una red. **IP Address (Dirección IP)** Muestra la dirección IP de la subred LAN. **Subnet Mask (Máscara de subred)** Muestra la máscara de subred de su LAN. **DHCP Server (Servidor DHCP)** Muestra el estado de su servidor DHCP local (activado o desactivado). **Starting IP Address (Dirección IP inicial)** Muestra el comienzo del intervalo de direcciones IP que utiliza el servidor DHCP en su gateway. **End IP Address (Dirección IP final)** Muestra el final del intervalo de direcciones IP que utiliza el servidor DHCP.
DHCP Client Table (Tabla de clientes DHCP)	Haga clic en **DHCP Client Table** (Tabla de clientes DHCP) para mostrar los dispositivos conectados a la LAN que han recibido direcciones IP del servidor DHCP del gateway. En la página DHCP Client Table (Tabla de clientes DHCP) verá una lista de los clientes DHCP (PC y otros dispositivos de red) con la siguiente información: Client Host Names (Nombres de hosts de clientes), IP Addresses (Direcciones IP), MAC Addresses (Direcciones MAC) y el período de tiempo antes de que caduquen sus direcciones IP asignadas. Para recuperar la información más reciente, pulse **Refresh** (Actualizar). Para salir de esta página y volver a la página Local Network (Red local), pulse **Close** (Cerrar). La siguiente ilustración muestra un ejemplo de la tabla de clientes DHCP. 

Sección	Descripción de campos
ARP/RARP Table (Tabla ARP/RARP)	Pulse **ARP/RARP Table** (Tabla ARP/RARP) para ver una lista completa de los dispositivos conectados a su red. Para recuperar la información más reciente, pulse **Refresh** (Actualizar). Para salir de esta página y volver a la página Local Network (Red local), pulse **Close** (Cerrar). La siguiente ilustración muestra un ejemplo de la tabla de clientes ARP/RARP. 

Status > Wireless (Estado > Inalámbrico)

La página Status > Wireless (Estado > Inalámbrico) muestra información básica sobre la red inalámbrica del gateway.

Seleccione la ficha **Wireless** (Inalámbrico) para abrir la página Status > Wireless (Estado > Inalámbrico). Pulse **Refresh** (Actualizar) para actualizar los datos de la página.



Descripción de la página Status > Wireless (Estado > Inalámbrico).

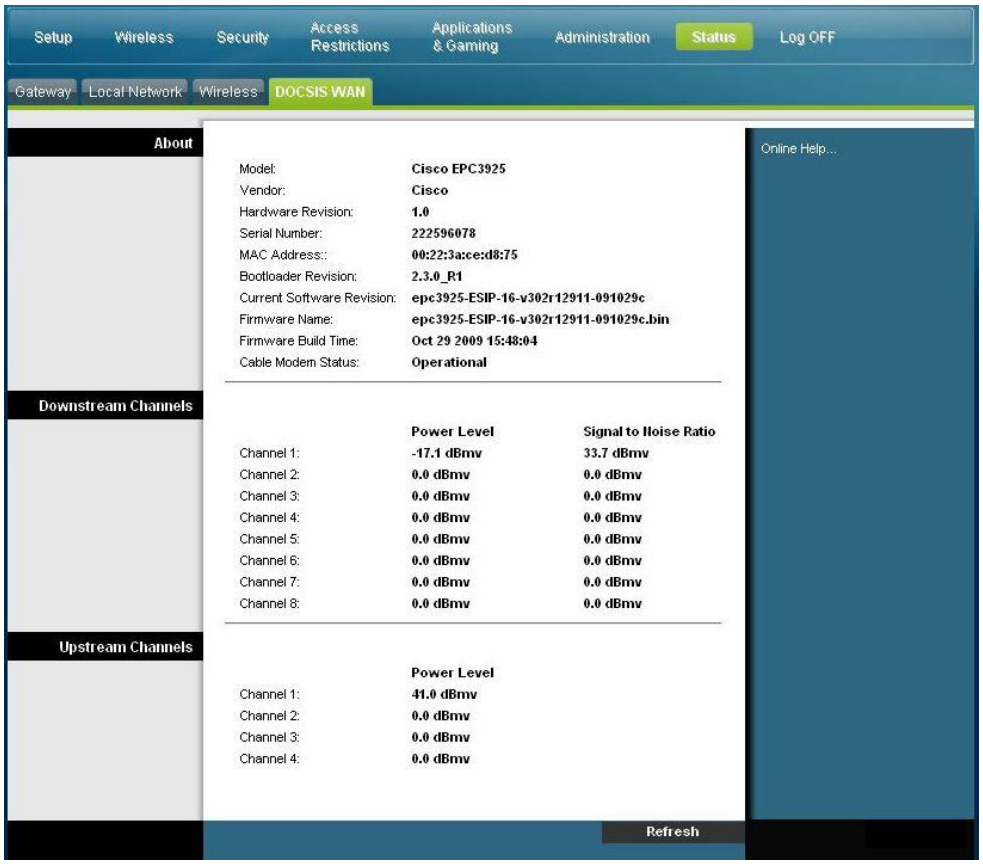
Utilice la tabla siguiente para revisar el estado de su red inalámbrica.

Sección	Descripción de campos
Wireless Network (Red inalámbrica)	**MAC Address (Dirección MAC)** Muestra la dirección MAC del punto de acceso inalámbrico local de su gateway. **Radio Band (Banda de radio)** Muestra una de las siguientes frecuencias de banda de radio actualmente operativas: ■ 2.4 GHz ■ 5 GHz ■ 2.4 y 5 GHz **Nota:** no todos los productos admiten la banda de radio de 5 GHz. **Newtwork Name (SSID) (Nombre de la red, SSID)** Muestra el nombre o el identificador del conjunto de servicios (Service Set Identifier, SSID) de su punto de acceso inalámbrico. **Channel Width (Ancho de canal)** Muestra el parámetro de ancho de banda de canal seleccionado en la página Basic Wireless Settings (Configuración inalámbrica básica) **Wide Channel (Canal ancho)** Muestra el parámetro de canal ancho seleccionado en la página Basic Wireless Settings (Configuración inalámbrica básica). **Standard Channel (Canal estándar)** Muestra el parámetro de canal estándar seleccionado en la página Basic Wireless Settings (Configuración inalámbrica básica). **Security (Seguridad)** Muestra el método de seguridad que utiliza su red inalámbrica. **SSID Broadcast (Difusión SSID)** Muestra el estado de la función de difusión SSID del gateway.

Status > DOCSIS WAN (Estado > DOCSIS WAN)

El estado DOCSIS WAN muestra información sobre el sistema de su cable módem.

Seleccione la ficha **DOCSIS WAN** para abrir la página Status > DOCSIS WAN (Estado > DOCSIS WAN).



Descripción de la página Status > DOCSIS WAN (Estado > DOCSIS WAN)

Utilice las descripciones de la siguiente tabla para revisar el estado de su red DOCSIS WAN.

Sección	Descripción de campos
About	**Model (Modelo)**
(Acerca de)	Muestra el nombre del gateway residencial.
	Vendor (Fabricante)
	Muestra el nombre del fabricante del gateway residencial.
	Hardware Revision (Revisión del hardware)
	Muestra la revisión del diseño del circuito impreso.
	Serial Number (Número de serie)
	Muestra la serie exclusiva del gateway residencial.

Sección	Descripción de campos
	MAC Address (CM MAC Address) [Dirección MAC (Dirección CM MAC)] Muestra la dirección CM MAC. La dirección CM MAC es una dirección alfanumérica exclusiva para la interfaz coaxial del cable módem, que se utiliza para conectarse al CMTS del terminal principal. Una dirección MAC es una dirección de hardware que identifica de forma exclusiva a cada nodo de una red.
	Bootloader Revision (Revisión del bootloader) Muestra la versión del código de revisión de arranque.
	Current Software Revision (Revisión actual del software) Muestra la versión de revisión del firmware.
	Firmware Name (Nombre del firmware) Muestra el nombre del firmware.
	Firmware Build Time (Hora de compilación del firmware) Muestra la fecha y hora de creación del firmware.
	Cable Modem Status (Estado del cable módem) Muestra uno de los posibles estados actuales del gateway.
Downstream Channels (Canales de bajada)	**Channels 1-8 (Canales 1-8)** Muestra el nivel de potencia y el ratio señal/ruido de los canales de bajada activos.
Upstream Channels (Canales de subida)	**Channels 1-4 (Canales 1-4)** Muestra el nivel de potencia de los canales de subida activos.

Preguntas más frecuentes

P. ¿Cómo se configura el protocolo TCP/IP?

R. Para configurar el protocolo TCP/IP, necesita tener instalado en su sistema una tarjeta de interfaz de red Ethernet con el protocolo de comunicaciones TCP/IP. TCP/IP es un protocolo de comunicaciones que se utiliza para acceder a Internet. En esta sección se incluyen instrucciones para configurar TCP/IP en sus dispositivos Internet para que funcionen con el gateway residencial en entornos de Microsoft Windows o Macintosh.

El protocolo TCP/IP en un entorno de Microsoft Windows es diferente para cada sistema operativo. Siga las instrucciones de esta sección correspondientes a su sistema operativo.

Configuración de TCP/IP en sistemas con Windows 2000

1. Haga clic en **Start** (Inicio), seleccione **Settings** (Configuración) y elija **Network and Dial-up Connections** (Conexiones de red y acceso telefónico).
2. Haga doble clic en el icono **Local Area Connection** (Conexión de área local) en la ventana Network and Dial-up Connections (Conexiones de red y acceso telefónico).
3. Haga clic en **Properties** (Propiedades) en la ventana Local Area Connection Status (Estado de conexión de área local).
4. Haga clic en **Internet Protocol (TCP/IP)** [Protocolo de Internet (TCP/IP)] en la ventana Local Area Connection Properties (Propiedades de conexión de área local) y después haga clic en **Properties** (Propiedades).
5. Seleccione tanto **Obtain an IP address automatically** (Obtener una dirección IP automáticamente) como **Obtain DNS server address automatically** (Obtener la dirección del servidor DNS automáticamente) en la ventana Internet Protocol (TCP/IP) Properties [Propiedades del protocolo TCP/IP] y, a continuación, haga clic en **OK** (Aceptar).
6. Haga clic en **Yes** (Sí) para reiniciar su equipo cuando se abra la ventana Local Network (Red local). Se reiniciará el equipo. El protocolo TCP/IP ya está configurado en su PC y los dispositivos Ethernet están listos para utilizarse.
7. Pruebe el acceso a Internet. Si no puede acceder a Internet, pida asistencia a su proveedor de servicios.

Configuración de TCP/IP en sistemas con Windows XP

1. Haga clic en **Start** (Inicio) y, en función de la configuración de su menú Inicio, elija una de las siguientes opciones:
   - Si utiliza el menú de inicio predeterminado de Windows XP, seleccione **Connect to** (Conectar a), elija **Show all connections** (Mostrar todas las conexiones) y, a continuación, vaya al paso 2.
   - Si utiliza el menú de inicio clásico de Windows XP, seleccione **Settings** (Configuración), elija **Network Connections** (Conexiones de red), haga clic en **Local Area Connection** (Conexión de área local) y, a continuación, vaya al paso 3.

2 Haga doble clic en el icono **Local Area Connection** (Conexión de área local) en la sección LAN o Internet de alta velocidad de la ventana Network Connections (Conexiones de red).

3 Haga clic en **Properties** (Propiedades) en la ventana Local Area Connection Status (Estado de conexión de área local).

4 Haga clic en **Internet Protocol (TCP/IP)** (Procolo Internet [TCP/IP]) y, a continuación, en **Properties** (Propiedades) de la ventana **Local Area Connection Properties** (Propiedades de conexión de área local).

5 Seleccione tanto **Obtain an IP address automatically** (Obtener una dirección IP automáticamente) como **Obtain DNS server address automatically** (Obtener la dirección del servidor DNS automáticamente) en la ventana Internet Protocol (TCP/IP) Properties [Propiedades del protocolo TCP/IP] y, a continuación, haga clic en **OK** (Aceptar).

6 Haga clic en **Yes** (Sí) para reiniciar su equipo cuando se abra la ventana Local Network (Red local). Se reiniciará el equipo. El protocolo TCP/IP ya está configurado en su PC y los dispositivos Ethernet están listos para utilizarse.

7 Pruebe el acceso a Internet. Si no puede acceder a Internet, pida asistencia a su proveedor de servicios.

Configuración de TCP/IP en sistemas Macintosh

1 Haga clic en el icono **Apple** en la esquina superior izquierda de Finder (Buscador). Desplácese hasta **Control Panels** (Paneles de control) y, a continuación, haga clic en **TCP/IP**.

2 Pulse **Edit** (Editar) en Finder (Buscador) en la parte superior de la página. Desplácese hasta la parte inferior del menú y, a continuación, haga clic en **User Mode** (Modo de usuario).

3 Haga clic en **Advanced** (Avanzado) en la ventana User Mode (Modo de usuario) y, a continuación, haga clic en **OK** (Aceptar).

4 Haga clic en las flechas de selección arriba y abajo situadas a la derecha de la sección Connect Via (Conectarse vía) de la ventana TCP/IP y, a continuación, haga clic en **Using DHCP Server** (Con servidor DHCP).

5 Haga clic en **Options** (Opciones) en la ventana TCP/IP y, a continuación, en **Active** (Activo) en la ventana TCP/IP Options (Opciones de TCP/IP).

Nota: asegúrese de que la opción **Load only when needed** (Cargar solo cuando sea necesario) esté *desactivada*.

6 Compruebe si la opción **Use 802.3** (Utilizar 802.3) situada en la esquina superior derecha de la ventana TCP/IP está desactivada. Si la opción está marcada, desactívela y, a continuación, haga clic en **Info** (Información) en la esquina inferior izquierda.

7 ¿Hay alguna dirección de hardware en esta ventana?

- Si es que **sí**, haga clic en **OK** (Aceptar). Para cerrar la ventana TCP/IP Control Panel (Panel de control TCP/IP), haga clic en **File** (Archivo) y, a continuación, desplácese y haga clic en **Close** (Cerrar). Ha finalizado este procedimiento.
- Si es que **no**, debe apagar su Macintosh.

8 Con el equipo apagado, pulse de forma simultánea y mantenga pulsadas las teclas **Command (Apple)** (Comando), **Option** (Opción), **P** y **R** del teclado. Manteniendo pulsadas esas teclas, encienda el Macintosh pero no suelte las teclas hasta oír el sonido de Apple por lo menos tres veces; a continuación, suelte las teclas y deje que se reinicie el equipo.

9 Cuando el equipo se haya reiniciado por completo, repita los pasos del 1 al 7 para comprobar que todos los parámetros TCP/IP sean correctos. Si su equipo aún no tiene una dirección de hardware, pida ayuda a su distribuidor autorizado de Apple o al centro de asistencia técnica de Apple.

P. ¿Cómo renuevo la dirección IP en mi PC?

R. Si su PC no puede acceder a Internet una vez que el gateway residencial esté en línea, es posible que el PC no haya renovado su dirección IP. Siga las instrucciones de esta sección que correspondan a su sistema operativo para renovar la dirección IP de su PC.

Renovación de la dirección IP en los sistemas Windows 95, 98, 98SE y ME

1 Pulse **Start** (Inicio) y, a continuación, pulse **Run** (Ejecutar) para abrir la ventana Run (Ejecutar).

2 Escriba **winipcfg** en el campo Open (Abrir) y pulse **OK** (Aceptar) para ejecutar el comando winipcfg. Se abre la ventana IP Configuration (Configuración de IP).

3 Haga clic en la flecha abajo a la derecha del campo superior y seleccione el adaptador Ethernet instalado en el PC. La ventana IP Configuration (Configuración de IP) muestra la información del adaptador Ethernet.

4 Pulse **Release** (Liberar) y, a continuación, pulse **Renew** (Renovar). La ventana IP Configuration (Configuración de IP) muestra una nueva dirección IP.

5 Pulse **OK** (Aceptar) para cerrar la ventana IP Configuration (Configuración de IP); ha finalizado este procedimiento.

Nota: si no puede acceder a Internet, solicite asistencia a su proveedor de servicios.

Renovación de la dirección IP en los sistemas Windows NT, 2000 o XP

1 Haga clic en **Start** (Inicio) y, a continuación, en **Run** (Ejecutar). Se abrirá la ventana Run (Ejecutar).

2 Escriba **cmd** en el campo Open (Abrir) y haga clic en **OK** (Aceptar). Se abrirá una ventana con un indicador de comando.

3 Escriba **ipconfig/release** en el indicador C:/ y pulse **Enter** (Intro). El sistema liberará la dirección IP.

4 Escriba **ipconfig/renew** en el indicador C:/ y pulse **Enter** (Intro). El sistema mostrará una nueva dirección IP.

5 Haga clic en la **X** en la esquina superior derecha de la ventana para cerrar la ventana Command Prompt (Indicador de comando). Ha finalizado este procedimiento.

Nota: si no puede acceder a Internet, pida ayuda a su proveedor de servicios.

P. ¿Qué ocurre si no estoy abonado a la televisión por cable?

R. Si la TV por cable está disponible en su zona, los servicios de datos pueden estar disponibles con o sin abonarse a un servicio de TV por cable. Pida información completa a su proveedor de servicios local sobre los servicios por cable, incluido el acceso a Internet de alta velocidad.

P. ¿Qué debo hacer para solicitar la instalación?

R. Llame a su proveedor de servicios y pregunte por la instalación profesional. Una instalación profesional le garantiza una conexión correcta por cable al módem y a su PC, así como la configuración adecuada de todos los parámetros de hardware y software. Pida más información sobre la instalación a su proveedor de servicios.

P. ¿Cómo se conecta el gateway residencial al PC?

R. El gateway residencial se conecta al PC mediante una conexión inalámbrica o a través del puerto Ethernet 10/100/1000BASE-T del PC. Si quiere utilizar una interfaz Ethernet, solicite las tarjetas Ethernet disponibles en su establecimiento local informático o de suministros de oficinas, o bien a su proveedor de servicios. Para obtener el mejor rendimiento de una conexión Ethernet, el PC debe estar equipado con una tarjeta Gigabit Ethernet.

P. Una vez que el gateway residencial esté conectado, ¿cómo se accede a Internet?

R. Su proveedor de servicios local se convierte en su proveedor de servicios de Internet (ISP). Éste ofrece una amplia gama de servicios, incluidos los de correo electrónico, chat, noticias e información. Su proveedor de servicios le proporcionará el software necesario.

P. ¿Puedo ver la televisión y navegar por Internet al mismo tiempo?

R. Por supuesto. Si está abonado al servicio de televisión por cable, puede ver la tele y utilizar el gateway residencial al mismo tiempo al conectar el televisor y el gateway residencial a la red de cable mediante un divisor de señal de cable opcional.

Problemas más frecuentes

No entiendo los indicadores de estado del panel frontal.

Consulte ***Funciones del indicador LED de estado del panel frontal*** (página 103), para obtener más información sobre la operación y las funciones de los indicadores LED de estado del panel frontal.

El gateway residencial no registra una conexión Ethernet.

- Compruebe si su PC tiene tarjeta Ethernet y asegúrese de que el software del controlador Ethernet está correctamente instalado. Si compra e instala una tarjeta Ethernet, siga estrictamente las instrucciones de instalación.
- Compruebe el estado de las luces indicadoras de estado del panel frontal.

El gateway residencial no registra una conexión Ethernet después de conectarse a un hub.

Si está conectando varios PC al gateway residencial, primero debe conectar el módem al puerto de enlace ascendente del hub con el cable cruzado correcto. El LED LINK (Enlace) del switch se iluminará de forma continua.

El gateway residencial no registra una conexión por cable.

- El módem funciona con un cable coaxial de RF estándar de 75 ohmios. Si utiliza un cable diferente, su gateway residencial no funcionará correctamente. Póngase en contacto con su proveedor de servicios de cable para determinar si está utilizando el cable correcto.
- La tarjeta NIC o la interfaz USB puede estar averiada. Consulte la información sobre detección y resolución de problemas de la documentación de la tarjeta NIC o la interfaz USB.

Sugerencias para mejorar el rendimiento

Comprobar y corregir

Si el gateway residencial no funciona según lo previsto, estas sugerencias pueden resultar útiles. Si necesita más ayuda, póngase en contacto con su proveedor de servicios.

- Compruebe que el enchufe de alimentación de CA de su gateway residencial esté insertado correctamente en una toma de corriente eléctrica.
- Compruebe que el cable de alimentación de CA del gateway residencial no esté enchufado a una toma eléctrica controlada por un interruptor de pared. Si un interruptor de pared controla la toma eléctrica, asegúrese de que está en la posición de **encendido**.
- Compruebe que el indicador LED de estado **ONLINE** (En línea) del panel frontal del gateway residencial esté iluminado.
- Compruebe que el servicio por cable esté activo y admita el servicio de bidireccional.
- Compruebe que todos los cables estén correctamente conectados y que sean los cables correctos.
- Compruebe que su TCP/IP esté correctamente instalado y configurado, si utiliza la conexión Ethernet.
- Compruebe que ha llamado a su proveedor de servicios y que le ha proporcionado el número de serie y la dirección MAC del gateway residencial.
- Si utiliza un divisor de señal de cable para poder conectar el gateway residencial a otros dispositivos, quite el divisor y reconecte los cables para que el gateway residencial esté conectado directamente a la entrada de cable. Si el gateway residencial ahora funciona correctamente, es posible que el divisor de señal de cable esté dañado y deba sustituirse por otro.
- Para obtener el mejor rendimiento de una conexión Ethernet, el PC debe estar equipado con una tarjeta Gigabit Ethernet.

Funciones del indicador LED de estado del panel frontal

Encendido inicial, calibración y registro (con aplicación de alimentación de CA)

En el siguiente cuadro se muestra la secuencia de pasos y el aspecto correspondiente de los indicadores de estado LED del panel frontal del gateway residencial durante el encendido inicial, la calibración y el registro en la red cuando se aplica la alimentación de CA al gateway residencial. Utilice este cuadro para detectar y solucionar cualquier problema con el proceso de encendido inicial, calibración y registro del gateway residencial.

Nota: cuando el gateway residencial finaliza el paso 11 (Registro telefónico finalizado), el módem pasa inmediatamente al funcionamiento normal. Consulte ***Operaciones normales (con alimentación AC)*** (página 105).

Indicadores de estado LED del panel frontal durante el encendido inicial, la calibración y el registro							
		Paso 1: registro de datos de alta velocidad					
Paso:		**1**	**2**	**3**	**4**	**5**	**6**
Indicador del panel frontal		**Self Test (Auto-diagnóstico)**	**Análisis de flujo descendente**	**Bloqueo de señal de flujo descendente**	**Determinación de intervalos**	**Solicitud de dirección IP**	**Solicitar archivo de suministro de datos de alta velocidad**
1	POWER (alimentación)	Encendido	Encendido	Encendido	Encendido	Encendido	Encendido
2	DS (Bajada)	Encendido	Parpadeante	Encendido	Encendido	Encendido	Encendido
3	US (Subida)	Encendido	Apagado	Apagado	Parpadeante	Encendido	Encendido
4	ONLINE (En línea)	Encendido	Apagado	Apagado	Apagado	Apagado	Parpadeante
5	ETHERNET 1-4	Encendido	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante
6	USB	Encendido	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante
7	WIRELESS LINK (Conexión inalámbrica)	Apagado	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante
8	WIRELESS SETUP (Conexión inalámbrica)	Apagado	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante
9	TEL 1 (Tel. 1)	Encendido	Apagado	Apagado	Apagado	Apagado	Apagado
10	TEL 2 (Tel. 2)	Encendido	Apagado	Apagado	Apagado	Apagado	Apagado
11	BATTERY (BATERÍA)	Encendido	Apagado	Apagado	Apagado	Apagado	Apagado

Indicadores de estado LED del panel frontal durante el encendido inicial, la calibración y el registro						
Paso 2: registro telefónico						
Paso		**7**	**8**	**9**	**10**	**11**
Indicador del panel frontal		**Registro de red de datos finalizado**	**Solicitud de dirección IP telefónica**	**Solicitar archivo de suministro de telefonía**	**Reinicio del servicio de voz**	**Registro telefónico finalizado**
1	POWER	Encendido	Encendido	Encendido	Encendido	Encendido
2	DS (Bajada)	Encendido	Encendido	Encendido	Encendido	Encendido
3	US (Subida)	Encendido	Encendido	Encendido	Encendido	Encendido
4	ONLINE (En línea)	Encendido	Encendido	Encendido	Encendido	Encendido
5	ETHERNET 1 – 4	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante
6	USB	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante
7	WIRELESS LINK (Conexión inalámbrica)	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante	Encendido o parpadeante
8	WIRELESS SETUP (Conexión inalámbrica)	Apagado	Apagado	Apagado	Encendido o parpadeante	Encendido o parpadeante
9	TEL 1 (Tel. 1)	Apagado	Parpadeante	Apagado	Parpadeante	Encendido
10	TEL 2 (Tel. 2)	Apagado	Apagado	Parpadeante	Parpadeante	Encendido
11	BATTERY (BATERÍA)	Apagado	Apagado	Apagado`	Apagado	Apagado

Operaciones normales (con alimentación AC)

En el siguiente cuadro se muestra el aspecto de los indicadores de estado LED del panel frontal del gateway residencial durante las operaciones normales cuando se aplica alimentación de CA al gateway.

Indicadores de estado LED del panel frontal durante condiciones normales		
Indicador del panel frontal		**Operaciones normales**
1	POWER	Encendido
2	DS (Bajada)	Encendido
3	US (Subida)	Encendido
4	ONLINE (En línea)	Encendido
5	ETHERNET 1 - 4	■ Encendido: solo se ha conectado un dispositivo al puerto Ethernet y no se produce intercambio de datos con el módem. ■ Parpadea: solo hay conectado un dispositivo Ethernet y hay transferencia de datos entre el equipo de la ubicación del CPE y el gateway residencial inalámbrico. ■ Apagado: no hay dispositivos conectados a los puertos Ethernet.
6	USB	■ Encendido: solo hay conectado un dispositivo al puerto Ethernet y no hay intercambio de datos con el módem. ■ Parpadea: solo hay conectado un dispositivo Ethernet y hay transferencia de datos entre el equipo de la ubicación del consumidor (consumer premise equipment, CPE) y el gateway residencial inalámbrico. ■ Apagado: no hay dispositivos conectados a los puertos USB.
7	WIRELESS LINK (Conexión inalámbrica)	■ Encendido: el punto de acceso inalámbrico está activado y en funcionamiento. ■ Parpadea: se está produciendo la transferencia de datos entre el CPE y el gateway residencial inalámbrico. ■ Apagado: el usuario ha desactivado el punto de acceso inalámbrico.
8	WIRELESS SETUP (Conexión inalámbrica)	■ Apagado: la configuración inalámbrica no está activa. ■ Parpadea: la configuración inalámbrica está activa para agregar nuevos clientes inalámbricos a la red inalámbrica.
9	TEL 1 (Tel. 1)	■ Encendido: está activado el servicio de telefonía. ■ Parpadea: la línea 1 está en uso.
10	TEL 2 (Tel. 2)	■ Encendido: está activado el servicio de telefonía. ■ Parpadea: la línea 2 está en uso.
11	BATTERY (BATERÍA)	■ Encendido: la batería está cargada. ■ Parpadea: el nivel de la batería es bajo. ■ Apagado: no hay batería en la unidad.

Condiciones especiales

En el siguiente cuadro se describe el aspecto de los indicadores de estado LED del panel frontal del cable módem durante condiciones especiales para mostrar que se le ha denegado el acceso a la red.

Indicadores de estado LED del panel frontal durante condiciones especiales		
Indicador del panel frontal		**Acceso a la red denegado**
1	POWER	Parpadeo lento 1 vez por segundo
2	DS (Bajada)	Parpadeo lento 1 vez por segundo
3	US (Subida)	Parpadeo lento 1 vez por segundo
4	ONLINE (En línea)	Parpadeo lento 1 vez por segundo
5	ETHERNET 1 – 4	Parpadeo lento 1 vez por segundo
6	USB	Parpadeo lento 1 vez por segundo
7	WIRELESS LINK (Conexión inalámbrica)	Parpadeo lento 1 vez por segundo
8	WIRELESS SETUP (Conexión inalámbrica)	Parpadeo lento 1 vez por segundo
9	TEL 1 (Tel. 1)	Apagado
10	TEL 2 (Tel. 2)	Apagado
11	BATTERY (BATERÍA)	Encendido

Avisos

Marcas comerciales

Cisco y el logotipo Cisco son marcas comerciales o marcas comerciales registradas de Cisco y/o sus filiales en EE.UU. y otros países. Puede consultar una lista de las marcas comerciales de Cisco en **www.cisco.com/go/trademarks**.

DOCSIS es una marca registrada de Cable Television Laboratories, Inc.
PacketCable es una marca comercial de Cable Television Laboratories, Inc.
La marca Wi-Fi Protected Setup pertenece a Wi-Fi Alliance. Wi-Fi Protected Setup es una marca comercial de Wi-Fi Alliance

Las marcas comerciales de otros fabricantes mencionadas en este documento pertenecen a sus respectivos propietarios.

El uso de la palabra partner no implica la existencia de una relación entre Cisco y cualquier otra empresa. (1009R)

Renuncia de responsabilidad

Cisco Systems, Inc. no se hace responsable de los errores u omisiones que puedan aparecer en esta guía. Nos reservamos el derecho a modificar esta guía sin previo aviso.

El máximo rendimiento inalámbrico se deriva de las especificaciones del estándar IEEE 802.11. El rendimiento real puede variar, incluida una menor capacidad de red inalámbrica, la velocidad de transmisión de datos, el intervalo y la cobertura. El rendimiento depende de numerosos factores, condiciones y variables, entre otras: la distancia desde el punto de acceso, el volumen del tráfico de red, los materiales y el tipo de fabricación, el sistema operativo utilizado, la combinación de productos inalámbricos empleados, las interferencias y otras condiciones adversas.

Aviso de copyright de la documentación

La información que se ofrece en el presente documento está sujeta a cambios sin previo aviso. No podrá reproducirse ninguna parte de este documento de ninguna forma sin la autorización expresa por escrito de Cisco Systems, Inc.

Utilización del software y firmware

El software descrito en este documento está protegido por la ley de propiedad intelectual y se proporciona en virtud de un contrato de licencia. Solo podrá utilizar o copiar este software de conformidad con las condiciones de su contrato de licencia.

El firmware de este equipo está protegido por la ley de propiedad intelectual. Solo podrá utilizar el firmware en el equipo en el cual se suministre. Se prohíbe la reproducción o distribución de este firmware, o de cualquier parte del mismo, sin nuestro consentimiento expreso por escrito.

Información

Si tiene alguna pregunta

Si tiene alguna pregunta técnica, llame a Cisco Services para solicitar asistencia. Siga las opciones del menú para hablar con un ingeniero de mantenimiento.

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

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

Mayo de 2012 Part number 4039566 Rev C