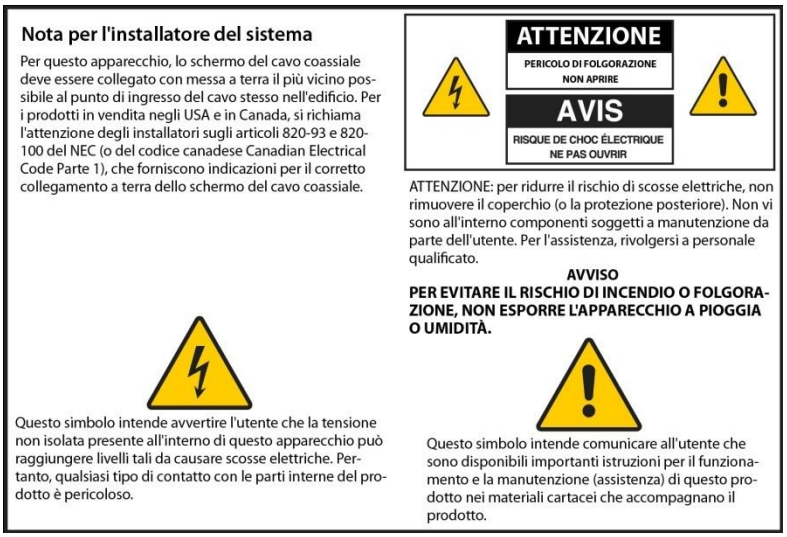
Gateway Wireless Cisco residenziale modello DPC3925 e EPC3925 8x4 DOCSIS 3.0 con guida utente integrata per adattatore vocale digitale

Indice

IMPORTANTI ISTRUZIONI SULLA SICUREZZA

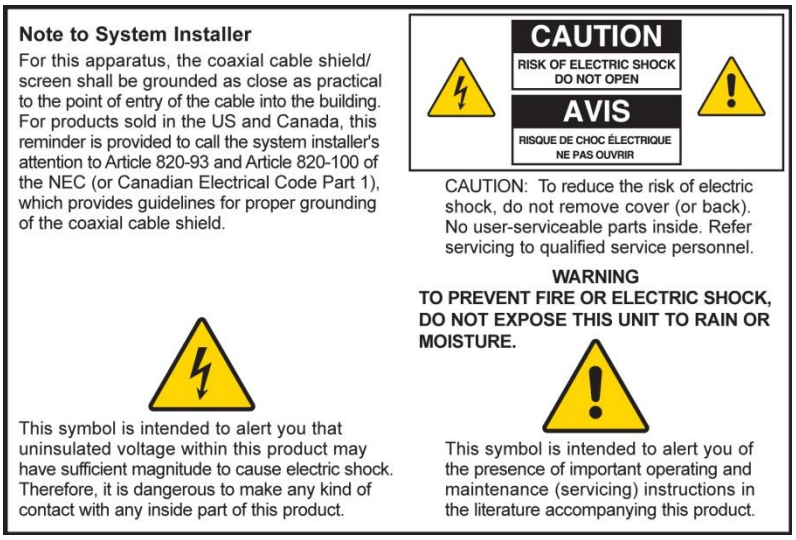
Avvertenze di installazione

Le procedure di manutenzione contenute in questo documento sono rivolte esclusivamente al personale di assistenza qualificato. Per evitare il rischio di scosse elettriche, non eseguire alcuna operazione di manutenzione diversa da quelle contenute nelle istruzioni, eccetto per gli utenti qualificati.



Notice to Installers

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



Notice à l'attention des installateurs de réseaux câblés

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

Mitteilung für CATV-Techniker

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

Mitteilung an den Systemtechniker

Für dieses Gerät muss der 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

IMPORTANTI ISTRUZIONI SULLA SICUREZZA

1) Leggere le istruzioni.
2) Conservare le istruzioni.
3) Osservare tutte le avvertenze.
4) Seguire tutte le istruzioni.
5) Non utilizzare l'apparecchio vicino all'acqua.
6) Pulire soltanto con un panno asciutto.
7) Non ostruire le aperture di ventilazione. Eseguire l'installazione seguendo le istruzioni del produttore.
8) Non installare l'apparecchio vicino a fonti di calore quali caloriferi, bocchette di aria calda, stufe o altre apparecchiature (compresi amplificatori) che emettono calore.
9) Utilizzare la spina polarizzata o di messa a terra come misura di sicurezza. Una spina polarizzata presenta due poli di dimensioni differenti. Una spina con la messa a terra presenta due poli più un terzo per la messa a terra. Il polo più largo o il terzo polo sono forniti come misura di sicurezza. Se non si possiede una presa adatta a tale spina, rivolgersi a un elettricista e sostituire la presa inutilizzabile.
10) Evitare di calpestare o schiacciare il cavo di alimentazione, in particolar modo per quanto riguarda le spine, le prese femmina e i punti nei quali questi componenti fuoriescono dall'apparecchio.
11) Collegare o fissare unicamente gli accessori specificati dal produttore.

12) Utilizzare solo carrelli, supporti, treppiedi, staffe o sostegni consigliati dal produttore o forniti in dotazione con l'apparecchio. Quando viene utilizzato un carrello, usare cautela durante lo spostamento dell'apparecchio per evitare infortuni dovuti al ribaltamento.
13) Scollegare l'apparecchio dalla presa di corrente durante i temporali o in caso di lunghi periodi di inattività.
14) Per l'assistenza, rivolgersi a personale qualificato. L'assistenza si rende necessaria per qualsiasi tipo di danno all'apparecchio e al cavo di alimentazione, nel caso vi penetrino liquidi o altri oggetti, nel caso venga esposto a pioggia o umidità oppure nel caso di funzionamento non regolare o di cadute.

Avvertenze sulla fonte di alimentazione

Il prodotto è dotato di un'etichetta con l'indicazione della fonte di alimentazione da utilizzare. Utilizzare il prodotto solo se risulta collegato ad una presa elettrica avente tensione e frequenza corrispondenti a quelle indicate sulla targhetta. In caso di dubbio circa la fonte di alimentazione da utilizzare, a casa o in ufficio, rivolgersi al provider di servizi o all'assistenza tecnica di zona.

L'ingresso c.a. dell'apparecchio deve rimanere costantemente accessibile ed utilizzabile.

Messa a terra

ATTENZIONE: evitare scosse e rischi di incendio! Se l'apparecchio viene collegato ad un cavo coassiale, verificare che l'impianto sia messo a terra (a massa). La messa a terra costituisce una protezione dai picchi di sovratensione e dalle cariche statiche.

Proteggere l'apparecchio dai fulmini

Scollegare l'alimentazione c.a. dalla presa a muro e gli ingressi di segnale.

Verificare la fonte di alimentazione indicata dalla spia luminosa On/Off

Anche se la spia on/off è spenta, l'apparecchio potrebbe essere collegato alla fonte di alimentazione. La spia si spegne quando l'apparecchio viene spento, indipendentemente dal fatto che la spina sia ancora collegata ad una fonte di alimentazione.

Eliminare i sovraccarichi di rete c.a.

ATTENZIONE: evitare scosse e rischi di incendio! Evitare il sovraccarico di reti c.a., prese, prolunghe e riduttori. Per le apparecchiature con alimentazione a batteria o sorgenti di potenza di altro tipo, consultare le relative istruzioni d'uso.

Prevedere una circolazione d'aria adeguata e sistemare in una postazione idonea

- Prima di alimentare elettricamente il prodotto, togliere tutto il materiale d'imballaggio.
- Non appoggiare l'apparecchio sulla superficie del letto, del divano o simile.
- Non posizionare l'apparecchio su una superficie instabile.
- Non sistemare l'apparecchio in luogo chiuso quale una libreria o un rack a meno che la ventilazione non sia adeguata.
- Non appoggiare lettori (tipo VCR o DVD), lampade, libri, vasi contenenti liquido o altri oggetti sull'apparecchio.
- Non ostruire le aperture di ventilazione.

Proteggere da esposizione all'umidità o a corpi estranei.

ATTENZIONE: evitare scosse e rischi di incendio! Non esporre il prodotto a spruzzi o gocce di liquido, pioggia o umidità. Evitare di appoggiare sull'apparecchio qualsiasi oggetto contenente liquidi, quali vasi o altro.

ATTENZIONE: evitare scosse e rischi di incendio! Staccare la spina prima di procedere alla pulizia dell'apparecchio. Non usare detergenti liquidi o spray. Non usare sistemi di pulizia a carica magnetica/statica (spolverini o stracci) sull'apparecchio.

ATTENZIONE: evitare scosse e rischi di incendio! Evitare di introdurre nell'apparecchio qualsiasi oggetto attraverso le aperture. I corpi estranei possono provocare cortocircuiti con rischio di elettrocuzione o incendio.

Avvertenze per l'uso

ATTENZIONE: evitare scosse elettriche! Non aprire il coperchio dell'apparecchio. L'apertura o la rimozione del coperchio può esporre l'utente a tensioni pericolose. L'apertura del coperchio farà decadere automaticamente la garanzia. L'apparecchio non contiene componenti sostituibili o riparabili dall'utente.

Verificare le condizioni di sicurezza del prodotto

Dopo aver completato qualsiasi operazione di assistenza o manutenzione, il tecnico deve eseguire i controlli di sicurezza previsti per stabilire se l'apparecchio è in condizioni operative di sicurezza.

Proteggere l'apparecchio in caso di trasporto

Scollegare sempre la fonte di alimentazione in caso di spostamento dell'apparecchio oppure nel collegare o scollegare cavi.

Avvertenza sulle apparecchiature elettroniche

Durante l'uso dell'apparecchio telefonico osservare sempre le principali precauzioni di sicurezza per contenere il rischio di incendi, scosse elettriche e lesioni personali, compreso quanto segue:

1. Non utilizzare l'apparecchio in prossimità di acqua, ad esempio, vicino ad una vasca da bagno, al lavandino della cucina o del bagno, su superficie bagnata o in prossimità di una piscina.

2. Evitare di usare un qualsiasi telefono (se non di tipo cordless) in caso di temporale in quanto vi è la remota possibilità di folgorazione da fulmine.

3. Non usare il telefono per denunciare una fuoriuscita di gas in prossimità della medesima.

ATTENZIONE: per ridurre il rischio di incendi, usare esclusivamente un cavo di linea tipo 26 AWG o di dimensioni maggiori.

CONSERVARE QUESTE ISTRUZIONI

20090915_Modem No Battery_Safety

Conformità alla normative FCC USA

Questo apparecchio è stato testato ed è risultato conforme **ai** limiti previsti per i dispositivi digitali di Classe B, in conformità alla Parte 15 delle norme FCC. Tali requisiti sono stati stabiliti al fine di garantire la protezione adeguata da interferenze dannose nell'ambito di un'installazione domestica. L'apparecchio genera, utilizza e può irradiare radiofrequenze. In caso di installazione ed uso non conformi alle istruzioni, può generare interferenze dannose per le comunicazioni radio. Tuttavia, non si garantisce che tali interferenze non possano avere luogo in determinate installazioni. Qualora il dispositivo dovesse provocare interferenze nella ricezione radiotelevisiva, cosa che si può verificare spegnendo e riaccendendo l'apparecchio, si consiglia di eliminare l'interferenza in uno dei seguenti modi:

- **Riorientare o riposizionare l'antenna ricevente.**
- **Aumentare la distanza tra l'apparecchio e la base.**
- **Collegare l'apparecchio a una presa su un circuito elettrico diverso da quello utilizzato per la base.**
- **Consultare il provider di servizi oppure un tecnico radiotelevisivo esperto a scopo di consulenza.**

Qualsiasi modifica o alterazione non espressamente approvata da Cisco Systems, Inc., può invalidare il diritto dell'utente all'uso dell'apparecchio.

Le informazioni incluse nel seguente paragrafo Dichiarazione di conformità delle FCC hanno lo scopo di fornire all'utente tutte le indicazioni relative all'omologazione FCC del presente apparecchio. *I numeri telefonici elencati si riferiscono unicamente a richieste relative alle FCC e non per porre domande relative al collegamento o al funzionamento dell'apparecchio. Contattare il provider di servizi locale per qualsiasi domanda in merito al funzionamento o all'installazione dell'apparecchio.*

FC Dichiarazione di Conformità

Questo dispositivo è conforme alla Parte 15 delle norme FCC. Il funzionamento è soggetto alle seguenti due condizioni: (1) l'apparecchio non può generare frequenze pericolose e (2) deve accettare qualsiasi interferenza ricevuta, compresa quella che ne può provocare l'attivazione non richiesta.

Gateway residenziale DOCSIS
Modello: DPC3925/EPC3925
Produttore:
Cisco Systems, Inc.
5030 Sugarloaf Parkway
Lawrenceville, Georgia 30044 USA
Telefono: +1 770-236-1077

Soggetto a norme EMI, Canada.

Questo apparecchio digitale di Classe B è conforme alle norme canadesi ICES-003.

Questo apparecchio digitale di classe (B) è conforme alle norme canadesi NMB-003.

Selezione di frequenze dinamica (DFS) Frequenze a doppia banda

Alcune configurazioni dell'apparecchio possono funzionare con bande comprese tra 5150-5250 MHz e 5470-5725 MHz. Selezionando un canale con queste gamme di frequenza, l'uso

dell'apparecchio viene limitato al funzionamento unicamente in interni, come da normativa FCC. L'uso dell'apparecchio sulle frequenze interessate in esterni non è conforme alle norme e ai principi FCC.

Esposizione a radiazioni

Nota: questo trasmettitore non deve essere collocato o utilizzato insieme ad altre antenne o altri trasmettitori. L'apparecchio deve essere installato e azionato ad una distanza minima di 20 cm (7,9 pollici) tra la sorgente di emissione ed il corpo dell'utente.

US

Il sistema è stato esaminato per valutare l'esposizione a RF per gli utenti in riferimento ai limiti previsti dalle norme ANSI C 95,1 (American National Standards Institute). La valutazione si basa sulle indicazioni fornite alle norme FCC OET Bulletin 65C rev 01.01, Parte 2.1091 e Parte 15.27. La distanza minima tra l'antenna e un utente generico deve essere pari a 20 cm (7,9 pollici) per rispetto alle norme.

Canada

Il sistema è stato esaminato per valutare l'esposizione a RF per gli utenti in riferimento ai limiti previsti dalle norme ANSI C 95.1 (American National Standards Institute). La valutazione si basa sulle indicazioni delle RSS-102 Rev 2. La distanza minima tra l'antenna e un utente generico deve essere pari a 20 cm (7,9 pollici) per rispetto alle norme.

UE

Il sistema è stato esaminato per valutare l'esposizione a RF per gli utenti in riferimento ai limiti previsti dalle norme ICNIRP (International Commission on Non-Ionizing Radiation Protection). La valutazione si basa sulle specifiche del prodotto EN 50385, allo scopo di dimostrare la conformità delle stazioni radio di base e dei terminali fissi per i sistemi di telecomunicazione wireless soggetti a restrizioni di base o a livelli di riferimento in merito all'esposizione degli utenti ai campi magnetici generati dalle radiofrequenze da 300 MHz a 40 GHz. La distanza minima tra l'antenna e un utente generico deve essere pari a 20 cm (7,9 pollici).

Australia

Il sistema è stato esaminato per valutare l'esposizione a RF come indicato nelle norme australiane per la protezione dalle radiazioni e in riferimento ai limiti previsti dalle norme ICNIRP (International Commission on Non-Ionizing Radiation Protection). La distanza minima tra l'antenna e un utente generico deve essere pari a 20 cm (7,9 pollici).

20091016 FCC DomandIntl

Conformità CE

Dichiarazione di conformità alla Direttiva UE 1999/5/EC (Direttiva R&TTE)

La presente dichiarazione è valida unicamente per le configurazioni (combinazione di software, firmware e hardware) supportate o fornite da Cisco Systems e utilizzabili entro i confini dell'UE. L'utilizzo di software o firmware non supportati o forniti da Cisco Systems potrebbe compromettere la conformità dell'apparecchio con i requisiti della normativa.

Български [Bulgarian]	Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/EC.
Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-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 dichiarazione di conformità relativa al presente apparecchio è contenuta nella sezione Dichiarazioni di conformità e informazioni sulla normativa, inclusa nella guida di

installazione dell'apparecchio, anche disponibile sul sito Cisco.com.

Per la valutazione del prodotto in base ai requisiti della direttiva europea 1999/5/EC sono stati applicati gli standard seguenti:

- **Radio: EN 300 328**
- **EMC: EN 301 489-1 e EN 301 489-17**
- **Sicurezza: EN 60950 e EN 50385**

Il marchio CE e l'identificativo di classe 2 sono apposti sul prodotto e sulla relativa confezione. Il prodotto è conforme alle direttive europee:

 -1999/5/EC

Restrizioni valide nei singoli Paesi

L'apparecchio è destinato unicamente per l'uso in interni.

Francia

Per 2,4 GHz, la potenza in uscita è limitata a 10 mW EIRP quando il prodotto viene utilizzato in esterni nella banda 2454 - 2483,5 MHz. Non sono previste restrizioni in caso di utilizzo in altre zone della banda 2,4 GHz. Visitare il sito Web http://www.arcep.fr/ per ulteriori informazioni.

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.

Italia

L'apparecchio è conforme alle specifiche di Interfacce Radio Nazionali e rispetta il Piano nazionale di ripartizione delle frequenze in Italia. Se l'apparecchio wireless LAN viene utilizzato al di fuori della residenza dell'utente occorre ottenere un'autorizzazione generale. Visitare il sito http://www.comunicazioni.it/it/ per ulteriori informazioni.

Questo prodotto è conforme alle specifiche di Interfacce 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 un'autorizzazione generale. Consultare il sito http://www.comunicazioni.it/it/ per ulteriori informazioni.

Lettonia

L'uso all'aperto nella banda a 2,4 GHz richiede l'autorizzazione dell'organismo di controllo delle comunicazioni elettroniche. Visitare il sito Web http://www.esd.lv per ulteriori informazioni.

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

Nota: i limiti stabiliti per la potenza di uscita massima sono specificati in EIRP. È possibile calcolare il livello di EIRP di un dispositivo sommando il guadagno dell'antenna utilizzata

(specificato in dBi) alla potenza di uscita disponibile in corrispondenza del connettore (specificata in dBm).

Antenne

Utilizzare solo l'antenna fornita con il prodotto. 20090312 CE_Gateway

Introduzione

Benvenuto nell'affascinante mondo di Internet ad alta velocità e dei servizi di telefonia digitale alta qualità. Il nuovo Gateway Wireless Cisco® residenziale, modello DPC3925 DOCSIS® 3.0 o EPC3925 EuroDOCSIS™ con adattatore vocale digitale incorporato è un modem via cavo conforme alle normative industriali che regolano la connettività per la trasmissione dati ad alta velocità abbinata ad un servizio di telefonia digitale affidabile. I gateway residenziali DPC3925 e EPC3925 abbinano le caratteristiche di trasmissione dati, voce e gateway cablati (Ethernet) o wireless per connettere una serie di dispositivi domestici o per piccoli uffici e supportano un accesso dati ad alta velocità combinato a servizi vocali convenienti ed affidabili, il tutto con un unico dispositivo. Utilizzando un gateway residenziale DPC3925 o EPC3925, il traffico vocale ad uso privato e commerciale ne trarrà certamente notevoli vantaggi, aumentando, al contempo, la produttività.

La presente guida contiene procedure e raccomandazioni per l'ubicazione, l'installazione, la configurazione, l'uso e la diagnostica dei dispositivi gateway ad uso residenziale DPC3925 e EPC3925 per l'suo di Internet ad alta velocità ed i servizi di telefonia ad uso privato o commerciale. Consultare la sezione relativa all'argomento specifico per maggiori informazioni. Contattare il provider di servizi per ulteriori informazioni relative ai contratti per i servizi.

Vantaggi e caratteristiche

I nuovi gateway ad uso residenziale DPC3925 e EPC3925 offrono i vantaggi e le caratteristiche seguenti:

- Conformità con DOCSIS 3.0, 2.0 e 1.x con specifiche PacketCable™ e EuroPacketCable™ per le massime prestazioni e affidabilità.
- Connettività Internet a banda larga ad alte prestazioni per potenziare la navigazione
- Adattatore vocale digitale incorporato a doppia linea per servizi di telefonia cablati.
- Quattro porte Ethernet 1000/100/10BASE-T per connettività cablata.
- Punti di accesso wireless 802.11n
- Wi-Fi Protected Setup (WPS), con pulsante di attivazione del WPS per una configurazione wireless semplice e sicura.
- Il Controllo genitori configurabile dall'utente blocca l'accesso a siti Internet indesiderati.

- La tecnologia firewall d'avanguardia ostacola le intrusioni e protegge la rete domestica da accessi indesiderati.

- Il design compatto ne permette l'installazione verticale, orizzontale o a parete.
- Le porte di interfaccia con codice colore e i cavi corrispondenti semplificano l'installazione e la configurazione.
- Le spie LED conformi al protocollo DOCSIS-5 garantiscono all'utente e ai tecnici di assistenza un sistema semplice per il controllo dello stato operativo e per la diagnostica.
- Il sistema è in grado di ricevere automaticamente gli aggiornamenti software tramite il provider di servizi.

Contenuto della confezione

Quando si riceve il gateway ad uso domestico, controllare apparecchiatura e accessori per verificare che la confezione sia completa e che i singoli componenti non siano danneggiati. La confezione contiene i seguenti componenti:

Uno dei modelli di Gateway residenziale DOCSIS (DPC3925 o EPC3925):

Un adattatore di corrente (per i modelli con fonte di alimentazione esterna)

Un cavo Ethernet (CAT5/RJ-45)

Un CD-ROM

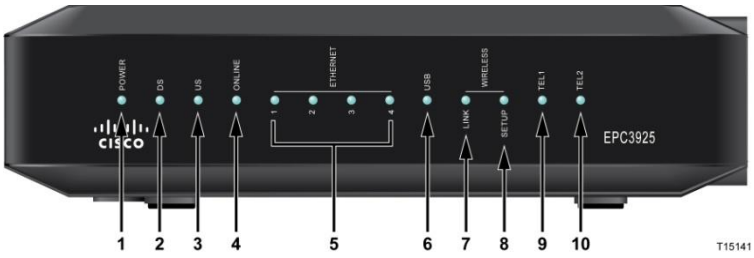
Se uno dei componenti elencati risulta mancante o danneggiato, contattare il provider di servizi.

Note:

- Occorre avere uno splitter di segnale e cavi coassiali comuni RF supplementari per collegare un VCR, un terminale Digital Home Communications Terminal (DHCT), un decoder, o la TV allo stesso collegamento via cavo usato per il gateway residenziale wireless.
- I cavi e le altre apparecchiature occorrenti per il servizio di telefonia devono essere acquistate separatamente. Consultare il provider di servizi per verificare le apparecchiature e i cavi che occorrono per i servizi di telefonia.

Descrizione pannello anteriore

Il pannello anteriore del gateway ad uso residenziale è dotato di LED indicatori di stato che indicano le prestazioni di funzionamento e lo stato dell'apparecchio. Vedere ***Funzioni degli indicatori di stato a LED del pannello anteriore*** (a pagina 130), per ulteriori informazioni sulle funzioni dei LED indicatori di stato del pannello anteriore.



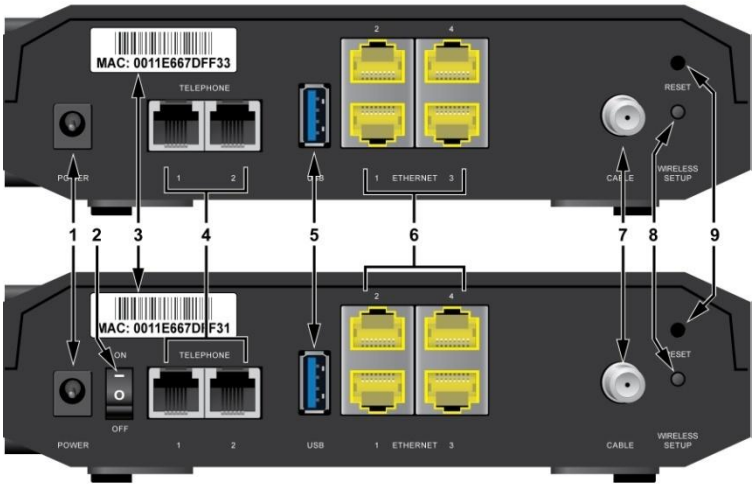
La figura mostra il modello EPC3925

1. **POWER —** ACCESO, il gateway residenziale wireless è alimentato
2. **DS —** ACCESO, il gateway residenziale wireless riceve i dati dalla rete via cavo
3. **US —** ACCESO, il gateway residenziale wireless riceve i dati dalla rete via cavo
4. **ONLINE —** ACCESO, il gateway residenziale wireless è registrato in rete e funziona normalmente
5. **ETHERNET 1 - 4 —** ACCESO, un dispositivo è collegato alle porte Ethernet. LAMPEGGIO, indica che i dati sono in corso di trasferimento tramite collegamento Ethernet
6. **USB —** ACCESO (acceso), un dispositivo è collegato alla porta USB. LAMPEGGIO, indica che i dati sono in corso di trasferimento tramite collegamento USB
7. **WIRELESS LINK —** ACCESO, il punto di accesso Wireless è attivo. Il led LAMPEGGIANTE, indica che i dati sono in corso di trasferimento tramite collegamento wirelessIl led SPENTO indica che il punto di accesso wireless è stato disabilitato dall'utente.
8. **WIRELESS SETUP —** SPENTO (condizione normale) configurazione wireless non attiva. Il led LAMPEGGIANTE indica che l'utente ha attivato la configurazione wireless per aggiungere altri clienti alla rete wireless
9. **TEL1 —** Il led ACCESO indica che il servizio di telefonia è abilitato. Lampeggia quando la linea 1 è utilizzata. Il led SPENTO indica che il servizio di telefonia per TEL 1 non è abilitato
10. **TEL2 —** Il led ACCESO indica che il servizio di telefonia è abilitato. Lampeggia quando la linea 2 è utilizzata. Il led SPENTO indica che il servizio di telefonia per TEL 2 non è abilitato

Descrizione pannello posteriore

Di seguito vengono illustrate e descritte le funzioni dei componenti posti sul pannello posteriore del gateway residenziale Cisco EPC3925.

Model DPC3925



Model EPC3925

T14517

1 **POWER**—Collega il gateway residenziale all'adattatore di potenza c.a. fornito con il dispositivo.

> **ATTENZIONE:**
>
> **Attenzione a non danneggiare l'apparecchio. Utilizzare esclusivamente l'alimentazione prevista per l'apparecchio.**

2 **INTERRUTTORE ON/OFF (solo per il mercato europeo)**—Permette di accendere il gateway residenziale senza scollegare il cavo di alimentazione

3 **ETICHETTA INDIRIZZI MAC** —Mostra l'indirizzo MAC del gateway residenziale

4 **TELEFONO 1 e 2**—Porte del telefono RJ-11 per collegare il circuito di telefonia domestica a telefoni o fax di tipo tradizionale

5 **USB**—Per il collegamento ai dispositivi utente

6 **ETHERNET**—Quattro porte Ethernet RJ-45 per il collegamento alla porta Ethernet del PC o della rete domestica

7 **CAVO**—Connettore F per il collegamento ad un segnale via cavo attivo fornito dal provider di servizi

8 **WIRELESS SETUP** (configurazione wireless)—Premendo il pulsante l'utente può aggiungere nuovi clienti wireless Wi-Fi Protected Setup (WPS) idonei alla rete domestica.

9 **RESET**—Una breve pressione di questo interruttore (1-2 secondi) avvia il reboot di EMTA. Se l'interruttore viene premuto più a lungo, verranno ripristinate le configurazioni di default previste dal costruttore e poi verrà avviato il reboot del gateway

ATTENZIONE:

Il tasto Reset deve essere usato esclusivamente a scopo di manutenzione. Non utilizzarlo se non specificamente richiesto per telefono o via cavo dal provider di servizi. In caso contrario, si potrebbero perdere le impostazioni selezionate per il modem via cavo.

Requisiti di sistema per collegamento Internet

Per garantire un corretto funzionamento del gateway residenziale per il servizio Internet ad alta velocità, controllare che tutti i dispositivi Internet del sistema a cui è collegato siano conformi ai seguenti requisiti minimi, oppure abbiano requisiti superiori, rispetto a quanto previsto per l'hardware ed il software.

Nota: è inoltre necessario disporre di una linea di ingresso via cavo attiva e di connessione Internet

Requisiti minimi di sistema per il PC

- Processore Pentium MMX 133 o di livello superiore
- 32 MB di RAM
- Browser Web
- Lettore CD-ROM

Requisiti minimi di sistema per Macintosh

- Mac OS: 7.5 o successivo
- 32 MB di RAM

Requisiti di sistema per connessione Ethernet

- PC con sistema operativo Microsoft Windows 2000 (o versione successiva) con protocollo TCP/IP installato, oppure computer Apple Macintosh con protocollo TCP/IP installato
- Scheda di interfaccia di rete Ethernet 10/100/1000BASE-T attiva installata

Modalità di adesione al servizio Internet ad alta velocità e al servizio telefonico

Per utilizzare il gateway residenziale è necessario disporre di un account di accesso Internet ad alta velocità. Per operare con Internet ad alta velocità occorre prima sottoscrivere un account con il provider di servizi locale. Selezionare una delle opzioni incluse in questa sezione.

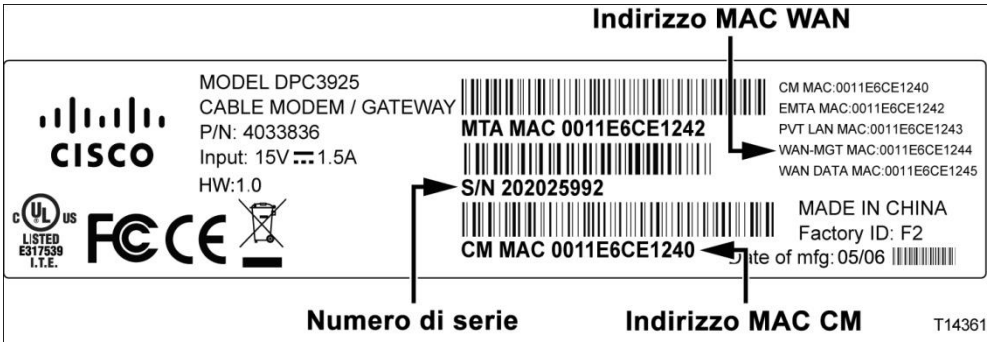
Non ho un account per l'accesso ad Internet ad alta velocità

Se *non* si ha un account con accesso ad Internet ad alta velocità, richiederlo al provider di servizi che diventerà il provider di servizi Internet (ISP) dell'utente. L'accesso ad Internet permette di inviare e ricevere e-mail, accedere al World Wide Web ed usufruire di altri servizi Internet.

Si devono fornire al provider di servizi le seguenti informazioni:

- Numero di serie del modem
- Indirizzo Media Access Control (MAC) del modem (CM MAC)
- Gli altri numeri di indirizzo MAC richiesti

Tali numeri sono inclusi su una etichetta con codice a barre apposta al gateway residenziale. Il numero di serie è composto da vari caratteri alfanumerici preceduti dalla sigla **S/N**. L'indirizzo MAC è composto da vari caratteri alfanumerici preceduti dalla sigla CM **MAC**. L'illustrazione seguente mostra un esempio di etichetta con codice a barre.



Scrivere i numeri nello spazio sottostante.

Numero di serie _____

Indirizzo MAC _____

Ho un account per l'accesso ad internet ad alta velocità

Se si dispone già di un account di accesso ad Internet ad alta velocità, è necessario fornire al provider di servizi il numero di serie e l'indirizzo MAC del gateway residenziale. Vedere le informazioni relative al numero di serie e all'indirizzo MAC riportate in precedenza nella presente sezione.

Come usare il server dell'applicazione per il servizio telefonico

Per utilizzare il gateway ad uso residenziale per il servizio telefonico occorre aver sottoscritto un contratto telefonico con il provider di servizi locale. Quando si contatta il proprio provider di servizi, si devono poter trasferire i numeri telefonici esistenti, oppure il provider del servizio di telefonia via cavo assegnerà un nuovo numero telefonico per ogni linea in uso o per ogni linea supplementare attiva. Verificare queste opzioni con il propri provider di servizi telefonici.

Postazione ideale per il Gateway DOCSIS residenziale

La postazione ideale per il gateway residenziale è il punto in cui è possibile accedere alle prese e ad altri dispositivi. Facendo riferimento alla configurazione di casa o dell'ufficio, consultare il proprio provider di servizi per individuare la postazione ideale per collocare il gateway residenziale. Leggere attentamente la presente guida utente prima di decidere dove sistemare il gateway.

Tener conto dei seguenti suggerimenti:

- Selezionare una postazione vicina al computer se si desidera usare il gateway anche per il servizio Internet ad alta velocità.
- Selezionare una postazione vicina ad un collegamento coassiale RF esistente per evitare di installare un'ulteriore presa coassiale RF.
- Selezionare una postazione in cui il gateway sia vicino all'apparecchio telefonico se si utilizzano solo uno o due dispositivi telefonici.

  Nota: per utilizzare il gateway allo scopo di fornire servizi a diversi telefoni, contattare un tecnico qualificato per collegare il gateway alla rete telefonica domestica esistente. Per ridurre al minimo le modifiche alla rete telefonica domestica, posizionare il gateway in prossimità di una presa telefonica esistente.
- Scegliere una postazione sufficientemente riparata da disturbi o danni accidentali, quali un armadio, il seminterrato o altra zona protetta.
- Selezionare una postazione in cui vi sia spazio sufficiente a prevedere un percorso cavi in uscita dal modem senza doverli tirare eccessivamente o arricciarli.
- L'ambiente di installazione deve garantire una buona circolazione dell'aria.
- Leggere la guida utente con attenzione prima di montare il gateway.

Montaggio del modem a parete (opzionale)

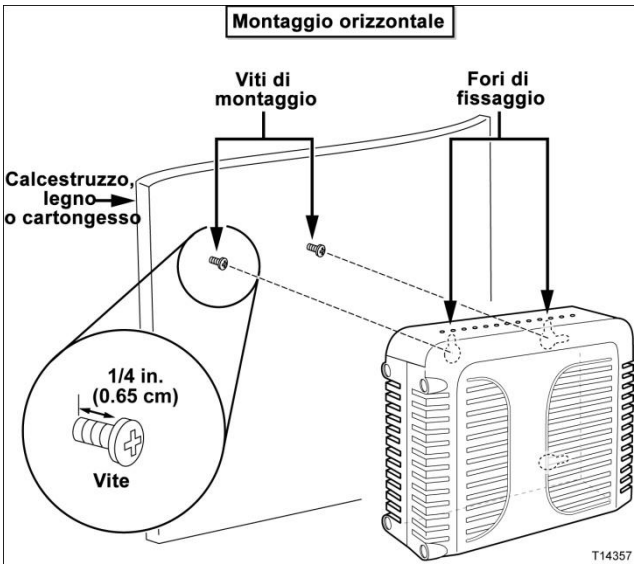
Il gateway ad uso residenziale può essere montato a parete utilizzando due staffe, due viti e gli slot nel dispositivo. Il modem può essere montato in orizzontale o in verticale.

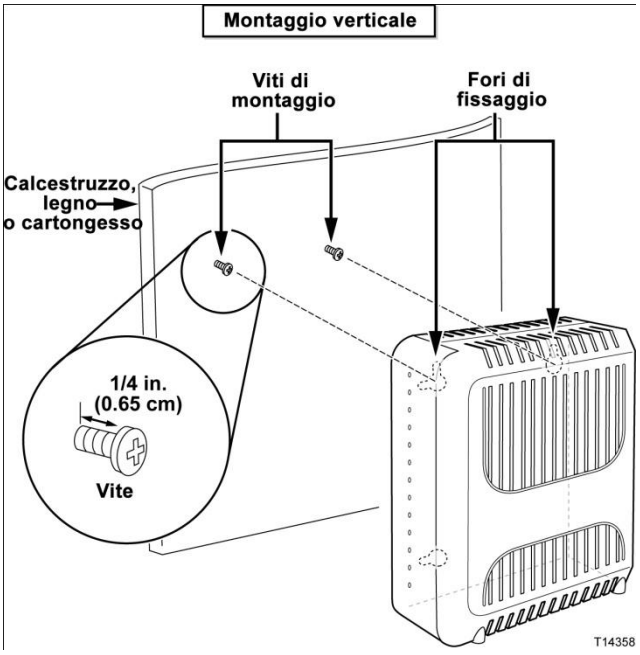
Operazioni preliminari

Prima di iniziare, selezionare una postazione di montaggio opportuna. La parete può essere in cemento, legno o in cartongesso. La postazione di montaggio deve essere libera da ingombri laterali e i cavi devono poter raggiungere il gateway facilmente senza tirarli. Lasciare uno spazio sufficiente tra il fondo del gateway e il pavimento o la superficie sottostante per aver accesso ai cavi. Inoltre lasciare una lunghezza sufficiente a consentire di smontare il gateway a scopo di manutenzione senza dover staccare i cavi. Verificare inoltre di avere a disposizione quanto segue:

- Due staffe a parete con viti da 8 x 1"
- Due viti metalliche a testa cilindrica da 8 x 1"
- Usare una punta di trapano da 3/16" per superfici in legno o in muratura, secondo la parete da forare
- Nelle pagine seguenti sono riportate le illustrazioni per il montaggio a parete

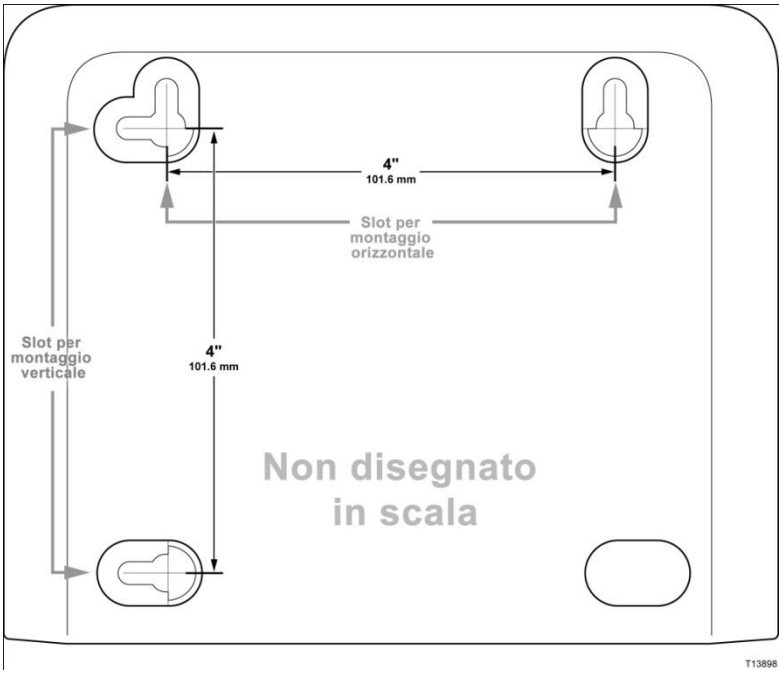
Montare il modem come illustrato nelle figure seguenti.





Posizione e dimensioni degli slot per il montaggio a parete

Le illustrazioni seguenti mostrano la posizione e le dimensioni degli slot sul fondo del modem per il montaggio a parete. Utilizzare le informazioni contenute in queste pagine come guida per il montaggio del modem a parete.



Montaggio del Gateway residenziale a parete

1. Usare una punta di trapano da 3/16" ed eseguire due fori alla stessa altezza, a distanza di 4 in l'uno rispetto all'altro.

   Nota: la grafica precedente, illustra la posizione dei fori di montaggio sul retro del gateway.

2. Il gateway viene montato su una superficie in cartongesso o in cemento dove è presente una piccola stecca in legno?
   - **In tal caso,** passare al punto 3.
   - In **caso contrario**, inserire le staffe di ancoraggio nella parete e montare le viti di fissaggio nelle staffe lasciando una luce pari a circa 1/4" tra la testa della vite e la parete. Quindi, passare al punto 4.
3. Montare le viti di fissaggio nella parete; lasciare una luce pari a circa 1/4" tra la testa della vite e la parete. Quindi, passare al punto 4.
4. Controllare che nessuno dei cavi o dei fili sia collegato al gateway.
5. Sollevare il gateway sino a portarlo nella posizione desiderata. Far scivolare l'estremità più larga dei due slot di montaggio (posti sul retro del gateway) sulle viti di fissaggio, quindi far scivolare verso il basso il gateway sino a portare l'estremità più stretta degli slot a contatto con il gambo della vite.

Importante: verificare che le viti di fissaggio siano in grado di sostenere il gateway in modo sicuro prima di lasciarlo andare.

Requisiti per l'impianto telefonico

Numero di dispositivi telefonici

I connettori telefonici RJ-11 presenti sul gateway supportano ciascuno il servizio a vari telefoni, fax e modem analogici.

Il numero massimo di dispositivi telefonici collegati ad ogni porta RJ-11 é limitato dal carico di chiamate dei dispositivi collegati. Molti dispositivi sono contrassegnati con un codice Ringer Equivalent Number (REN). Le singole porte telefoniche del gateway residenziale possono supportare un carico sino a 5 REN.

La somma del carico REN di tutti i dispositivi telefonici collegati ad ogni porta non deve superare 5 REN.

Tipi di dispositivi telefonici

Si possono usare dispositivi telefonici non codificati con un numero REN, ma il numero massimo di dispositivi telefonici collegati non può essere calcolato con precisione. Per i dispositivi telefonici non codificati, collegare prima ogni apparecchio quindi verificare il segnale di chiamata prima di aggiungere altri dispositivi. Se il numero di apparecchi telefonici collegati è eccessivo e non si riesce a sentire il segnale di chiamata, eliminarli progressivamente sino ad ottenere nuovamente il segnale.

Telefoni, fax e altri dispositivi telefonici utilizzano i 2 pin centrali dei connettori RJ-11 per il collegamento alle porte telefoniche del gateway residenziale. Alcuni telefoni usano altri pin dei connettori RJ-11, e per utilizzarli è necessario ricorrere ad appositi adattatori.

Requisiti di chiamata

Tutti i telefoni devono utilizzare la modalità di chiamata DTMF. In genere le chiamate a impulsi non sono abilitate dal provider locale.

Requisiti di cablaggio telefonico

Il gateway residenziale supporta il collegamento alla rete telefonica interna oppure può essere collegato direttamente al telefono e al fax. La distanza massima del gruppo dal dispositivo telefonico più lontano non deve superare 300 m (1000 ft). Usare una cavo telefonico n. 26 o di dimensione maggiore con doppini intrecciati.

Importante: il collegamento ad una rete telefonica domestica permanente deve essere eseguito da un tecnico qualificato.

Procedure di collegamento del Gateway a Internet e al servizio telefonico

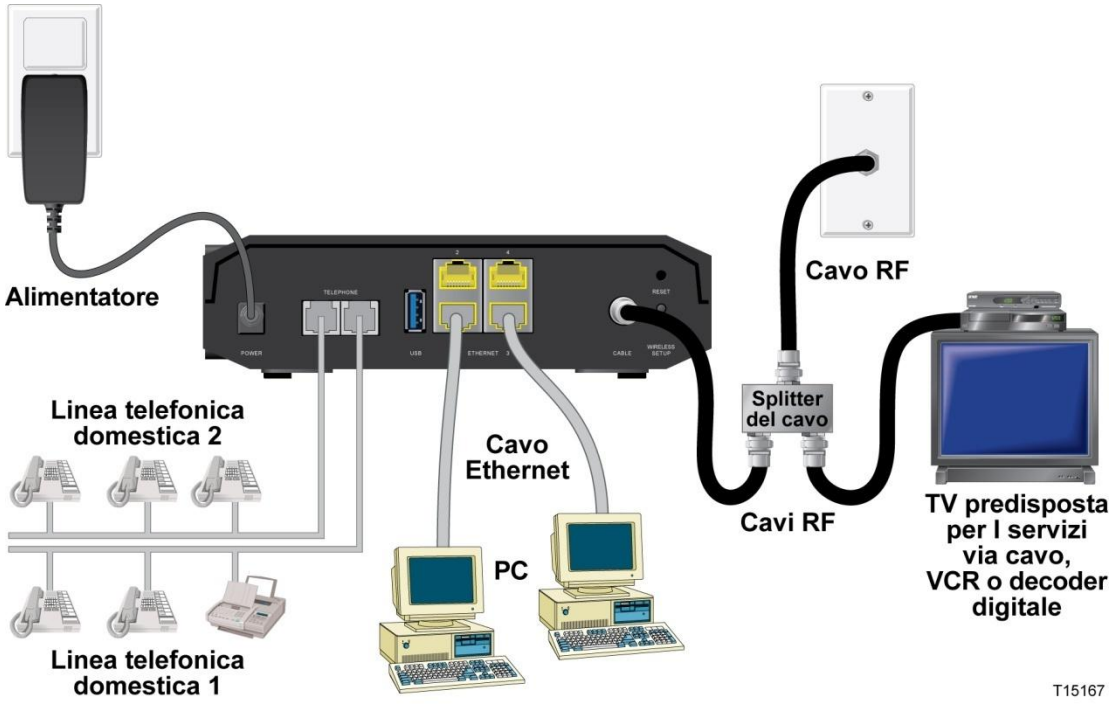
Il Gateway residenziale può essere usato sia per servizi telefonici che per il collegamento a Internet, che può essere condiviso con altri dispositivi Internet presenti in casa o in ufficio. La condivisione di un collegamento tra vari dispositivi viene definito collegamento in rete.

Collegamento e installazione di dispositivi Internet

L'installazione dev'essere eseguita in modo professionale. Rivolgersi al proprio provider di servizi per ricevere assistenza.

Collegamento dei dispositivi

Lo schema seguente illustra le varie opzioni di collegamento in rete disponibili all'utente.



Collegamento del Gateway residenziale per servizi di trasferimento dati ad alta velocità o telefonici

La procedura di montaggio illustrata di seguito permette eseguire correttamente l'impostazione e la configurazione del gateway.

1 Selezionare una postazione adatta e sicura per installare il gateway (vicino a una fonte di alimentazione, a un collegamento via cavo attivo, al PC se si utilizza Internet ad alta velocità, e alle linee telefoniche se si usa un VoIP).

AVVISO:

- Per evitare lesioni personali, seguire le istruzioni di installazione nell'ordine esatto in cui vengono fornite.
- Per evitare danni alle apparecchiature, scollegare qualsiasi altro servizio telefonico prima di collegare il modem via cavo alla rete.
- Sulle porte telefoniche del gateway residenziale possono essere presenti tensioni pericolose, così come su altri circuiti collegati, comprese le reti Ethernet, telefonica e sul cavo coassiale.
- Isolare opportunamente i cablaggi e i collegamenti telefonici per evitare il rischio di elettrocuzione.
- Il collegamento ad una rete telefonica domestica deve essere eseguito da un tecnico qualificato. Il provider di servizi telefonici via cavo potrebbe eventualmente fornire tecnici specializzati per l'installazione e il collegamento alla rete telefonica domestica. Si tratta normalmente di un servizio a pagamento.
- Isolare opportunamente i cablaggi e i collegamenti per evitare il rischio di elettrocuzione.
- Scollegare l'alimentazione dal gateway residenziale prima di provare a collegare qualsiasi dispositivo.

2 Spegnere il PC e qualsiasi altro dispositivo in rete, quindi staccare la spina dalla fonte di alimentazione.

3 Collegare il cavo coassiale RF attivo fornito dal proprio provider di servizi al connettore coassiale denominato **CABLE (cavo)** sul retro del gateway residenziale.

Nota: per collegare TV, DHCT, decoder o VCR provenienti dal medesimo collegamento via cavo, occorre montare uno splitter di segnale (non compreso). Prima di utilizzare uno splitter, consultare sempre il proprio provider di servizi, in quanto il segnale potrebbe risultare degradato.

4 Collegare il PC al gateway residenziale mediante uno dei metodi illustrati di seguito.

- **Collegamento Ethernet:** individuare il cavo giallo Ethernet, collegare una estremità del medesimo alla porta Ethernet del PC e collegare l'altra estremità alla porta gialla **ETHERNET** posta sul retro del gateway residenziale.

  Nota: per installare un numero maggiore di dispositivi Ethernet rispetto alle porte previste sul gateway residenziale, utilizzare un adattatore esterno a porte multiple Ethernet.
- **Wireless:** verificare che il dispositivo wireless sia alimentato. Il dispositivo wireless deve essere associato al gateway wireless quando il gateway è operativo. Seguire le istruzioni fornite con il dispositivo wireless per collegarlo a un punto di accesso dedicato.

  Per ulteriori informazioni circa la configurazione predefinita del gateway wireless, consultare la sezione ***Configurazione delle impostazioni wireless*** (pag. 50) di questa guida.

5 Collegare una estremità del ponticello telefonico (non compreso) a una presa telefonica domestica oppure a un telefono o fax. Collegare poi l'altra estremità del ponticello alla porta **TELEFONO** RJ-11 prevista sul retro del gateway residenziale. Le porte telefoniche sono di color grigio chiaro e identificate dai numeri 1/2 e 2 oppure 1 e 2 a seconda della nazione in cui viene utilizzato il gateway residenziale.

Note:

- Verificare che il servizio telefonico sia collegato alla porta RJ-11 corretta. Per linee telefoniche singole, collegarsi alla porta 1/2 o 1.
- Per il Nord America, i gateway residenziali supportano linee multiple sulla porta telefonica RJ-11 identificata 1/2. La linea 1 è sui pin 3 e 4 della porta 1/2, e la linea 2 è supportata sui pin 2 e 5. In Europa, i gateway ad uso residenziale supportato una sola linea per porta. La linea 1 è sulla porta 1 e la linea 2 è sulla porta 2.
- I telefoni che necessitano di connettori elettrici diversi dal tipo RJ-11 possono utilizzare un adattatore esterno (venduto separatamente).

6 Individuare il cavo di potenza c.a. fornito con il gateway residenziale. Inserire una estremità del cavo di potenza nel connettore c.a. sul retro del gateway residenziale. Collegare quindi il cavo di potenza c.a. in una presa c.a. per alimentare il gateway residenziale. Il gateway eseguirà una ricerca automatica per individuare e accedere alla rete dati a banda larga. Questa operazione può

richiedere da 2 a 5 minuti. Il modem sarà pronto per l'uso quando i LED **POWER**, **DS**, **US** e **ONLINE** sul pannello anteriore del gateway residenziale smetteranno di lampeggiare per rimanere accesi in modo permanente.

7 Inserire e accendere il PC e gli altri dispositivi di rete domestica. I LED **LINK** sul gateway corrispondenti ai dispositivi collegati dovranno essere accesi o lampeggiare.

8 Quando il gateway residenziale è collegato, praticamente tutti i dispositivi Internet avranno accesso immediato.

Nota: se il PC non può accedere a Internet consultare la sezione ***FAQ (domande frequenti)*** (pag. 123) per le informazioni relative alla configurazione del PC per TCP/IP. Per dispositivi Internet diversi dal PC, consultare la sezione di configurazione indirizzi DHCP o IP relativa a tali dispositivi nella Guida utente o nel Manuale d'uso.

Procedure di configurazione del Gateway DOCSIS ad uso residenziale

Per configurare il gateway residenziale accedere innanzitutto alle pagine di configurazione WebWizard. La sezione fornisce istruzioni e procedure dettagliate per l'accesso alle pagine WebWizard e per la configurazione del gateway residenziale tali da consentirne il corretto funzionamento. La sezione contiene anche esempi e descrizioni delle singole pagine di configurazione WebWizard. Utilizzare le pagine WebWizard per personalizzare il gateway secondo le proprie esigenze invece delle impostazioni predefinite. Le pagine WebWizard contenute nella presente sezione sono organizzate secondo l'ordine descritto nella pagina **Configurazione**.

Importante: le pagine WebWizard e gli esempi contenuti in questa sezione sono riportati esclusivamente a scopo illustrativo. Le pagine utente possono ovviamente essere diverse da quelle contenute nella guida. Le pagine illustrate in questa guida mostrano anche i valori predefinit impostati per il dispositivo.

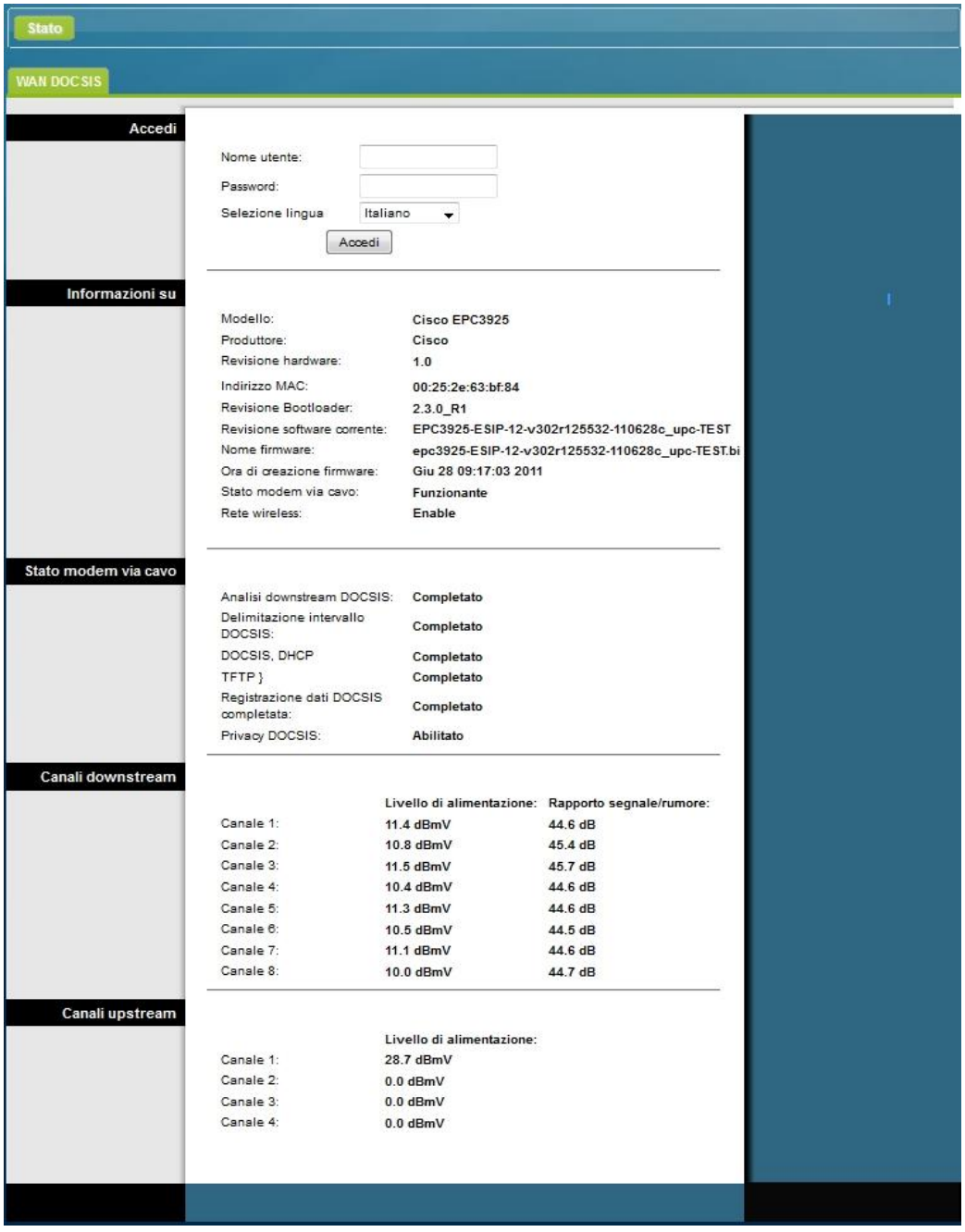
Nota: se non si ha familiarità con le procedure di configurazione di rete riportate in questa sezione, contattare il provider di servizi prima di provare a modificare qualsiasi impostazione predefinita del gateway residenziale.

Primo accesso al gateway

La configurazione predefinita del gateway usa l'indirizzo IP 192,168.0,1. Se il gateway è stato collegato correttamente e se anche il computer è stato configurato in modo corretto, seguire la procedura illustrata di seguito per accedere al gateway come amministratore.

1 Dal PC, lanciare il browser web preferito.

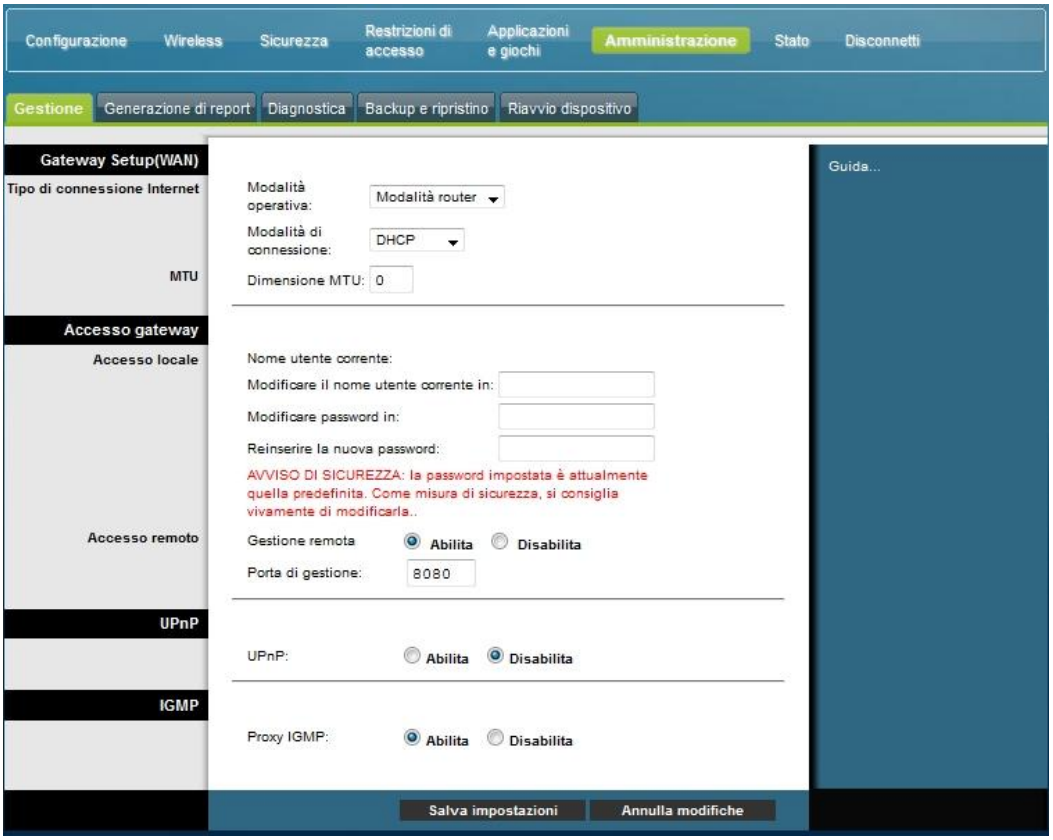
2 Nel campo indirizzi, inserire il seguente indirizzo IP: **192.168.0.1**. Si apre una pagina di stato di log-in DOCSIS WAN simile alla pagina seguente.



3 Sulla pagina di stato DOCSIS WAN lasciare vuoto il campo Nome utente e Password e fare clic su **Accedi**. Il gateway si apre con una pagina iniziale Amministrazione > Gestione. Si può utilizzare la pagina Amministrazione > Gestione per modificare Nome utente e Password.

A questo punto il l'accesso è stato effettuato. Si può scegliere qualsiasi pagina web relativa a impostazioni e gestione. Tuttavia, l'accesso è stato eseguito in modalità di amministrazione per ricordare all'utente di impostare una nuova password.

Importante: si raccomanda l'uso di una nuova password per impedire qualsiasi accesso fraudolento da Internet alla ricerca di dispositivi funzionanti con password e/o nome utente comunemente noti o predefiniti.



4 Dalla pagina Amministrazione > Gestione creare un nuovo Nome utente e Password, quindi fare clic su **Salva Impostazioni**. Dopo aver salvato le impostazioni per il nuovo Nome utente e Password nella pagina, viene visualizzata la pagina Configurazione > Quick Setup (Installazione rapida).

Importante: è possibile lasciare vuoto il campo della password (valore predefinito). Tuttavia, se non si modificano Nome utente e Password, si aprirà la pagina Administration Management tutte le volte che si effettuerà l'accesso al gateway. Si tratta di un modo per ricordare all'utente di impostare una password personalizzata.

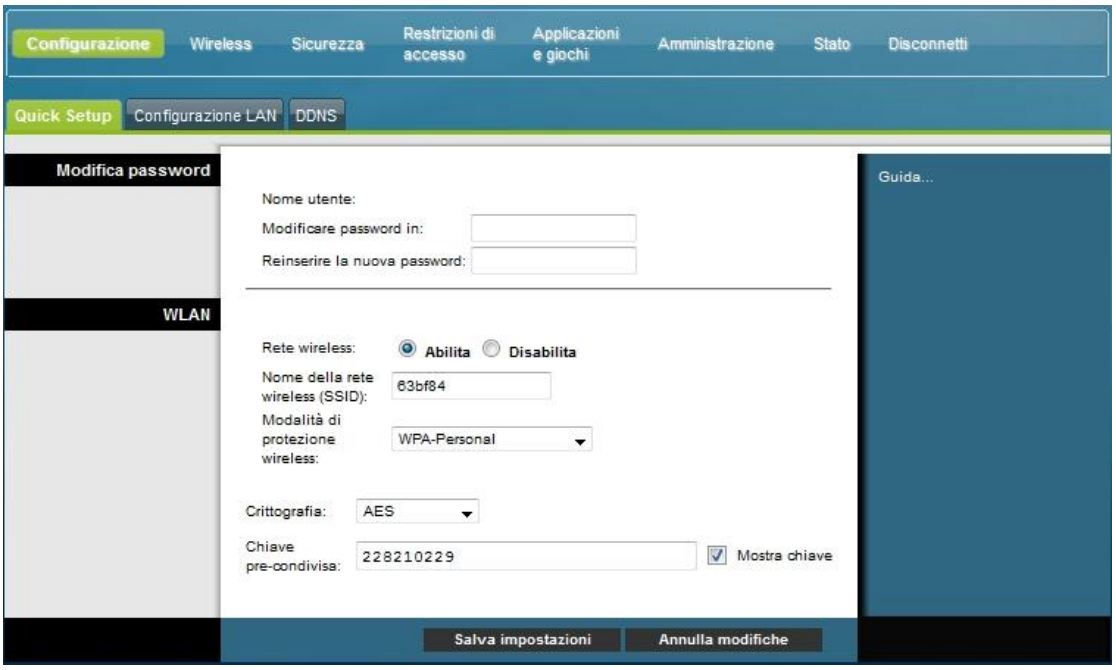
Dopo aver modificato la Password, i log-in successivi portano direttamente alla pagina Configurazione Installazione rapida.

5 Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Configurazione > Quick Setup (Installazione rapida)

La pagina Configurazione > Quick Setup (Installazione rapida) è la prima pagina che si apre dopo aver effettuato il log-in al gateway. Si possono usare le impostazioni di questa pagina per modificare la password e per le configurazioni WLAN.

Importante: le impostazioni di questa pagina sono abbinate esclusivamente a questo dispositivo utente. Se selezionate, non sarà necessario eseguire altre modifiche alle impostazioni di questa pagina. Queste impostazioni predefinite garantiranno un utilizzo sicuro della rete wireless.



Configurazione delle Impostazioni rapide

Utilizzare le descrizioni e seguire le istruzioni riportate nella tabella seguente per configurare le impostazioni di rete del dispositivo. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva Impostazioni** per attivare la modifiche oppure **Annulla Modifiche** per annullarle.

Sezione	Descrizione campo
Modifica password	**Nome utente** Viene visualizzato il nome utente dell'operatore attualmente collegato. **Modificare password in** Consente di modificare la propria password. **Reinserire la nuova password** Consente di reinserire la nuova password, che deve corrispondere a quella immessa nel campo **Modificare password in**.

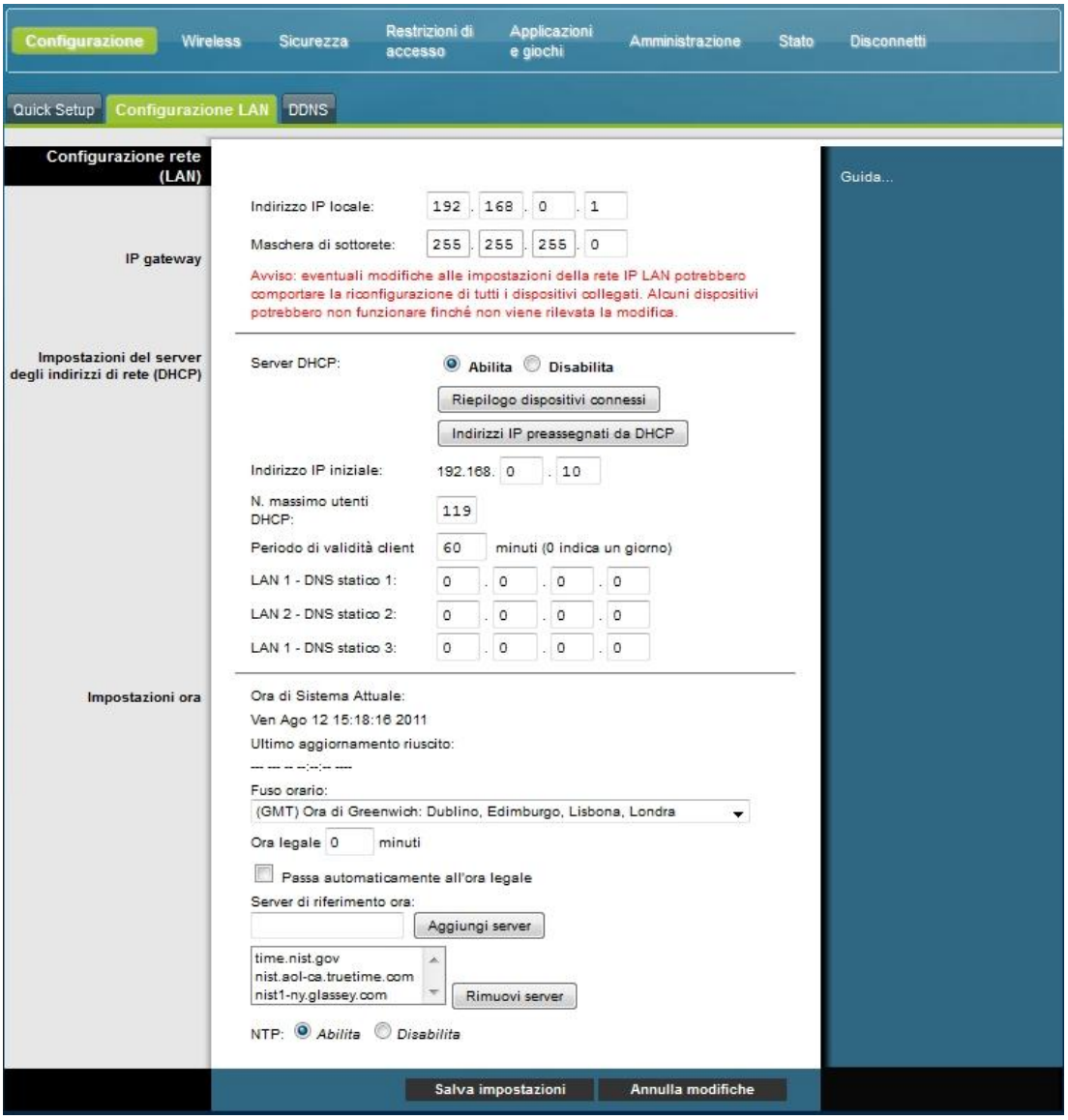
Sezione	Descrizione campo
WLAN	**Rete wireless** Consente di abilitare o disabilitare la rete wireless. Selezionare l'opzione desiderata: ■ **Abilita** ■ **Disabilita** **Nome della rete wireless (SSID)** Permette di inserire un nome per la rete wireless o di utilizzare il valore di default. Il valore immesso sarà visibile su tutti i computer e altri dispositivi client wireless, così come il nome della rete wireless. **Nota:** il codice identificativo Service Set Identifier (SSID) predefinito solitamente è composto dagli ultimi 6 caratteri dell'indirizzo CM MAC L'indirizzo CM MAC si trova sull'etichetta con i valori nominali apposta sul gateway wireless. **Modalità di protezione wireless** Permette di selezionare una modalità di sicurezza wireless per la protezione della rete utente. Se si seleziona **Disabilita** la rete wireless non sarà protetta e tutti i dispositivi nelle vicinanze potranno connettersi. Vedere la sezione ***Sicurezza wireless*** (pag. 55) per una descrizione dettagliata delle modalità di sicurezza wireless. **Nota:** la modalità di sicurezza wireless predefinita è WPA oppure WPA2-Personal. **Crittografia** Permette di selezionare un livello di crittografia basato sulla modalità di sicurezza wireless selezionata. Vedere la sezione ***Sicurezza wireless*** (pag. 55) per una descrizione dettagliata della crittografia. **Chiave precondivisa** Chiave precondivisa per il dispositivo. La chiave può contenere da 8 a 63 caratteri. La chiave precondivisa predefinita è composta dalle 9 cifre del numero di serie del gateway. Il numero di serie si trova sull'etichetta con i valori nominali, apposta sul gateway wireless. **Nota:** il service provider può eventualmente fornire una scheda con configurazione wireless contenente l'identificativo SSID e le informazioni di sicurezza della configurazione wireless relative alla rete domestica e che possono essere diverse da quanto sopra descritto.

Configurazione > Configurazione LAN

La pagina Configurazione Configurazione LAN permette di configurare le impostazioni di rete Local Area Network (LAN) domestiche. Tali impostazioni comprendono la gamma di indirizzi IP che definiscono la rete LAN in sé nonché come vengono assegnati gli indirizzi (in automatico con DHCP o manuale) dei nuovi dispositivi eventualmente aggiunti alla rete.

Importante: a meno che l'utente non sia esperto nel gestire gli indirizzi IP, si raccomanda di non modificare tali impostazioni. Se i valori vengono modificati è possibile perdere l'accesso a Internet.

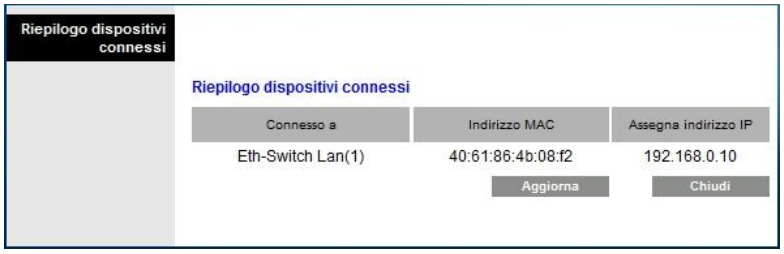
Selezionare la scheda **Configurazione LAN** per aprire la pagina Configurazione LAN.



Configurazione delle impostazioni di rete

Utilizzare le descrizioni e seguire le istruzioni riportate nella tabella seguente per configurare le impostazioni di rete del gateway residenziale. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva Impostazioni** per attivare la modifiche oppure **Annulla Modifiche** per annullarle.

Sezione	Descrizione campo
Configurazione rete (LAN) **IP gateway**	**Indirizzo IP locale** Indirizzo IP di base della LAN domestica privata. Il valore di default dell'indirizzo LAN IP è 192,168.0,1. **Maschera di sottorete** Maschera di sottorete della rete LAN
Impostazioni del server degli indirizzi di rete (DHCP)	**Server DHCP** Consente di abilitare o disabilitare il server DHCP del gateway residenziale. Il server DHCP viene usato per assegnare automaticamente gli indirizzi IP ai dispositivi collegati di volta in volta alla rete domestica.

Sezione	Descrizione campo
Impostazioni del server degli indirizzi di rete (DHCP)	**Server DHCP** ■ Pagina riassuntiva dei dispositivi collegati Fare clic su **Riepilogo dispositivi connessi** nella pagina di Configurazione LAN. Si aprirà la pagina Riepilogo dispositivi connessi. La pagina si presenta come finestra di popup che mostra gli indirizzi MAC e gli indirizzi IP dei dispositivi collegati al gateway residenziale.  ■ Pagina Indirizzi IP preassegnati da DHCP Fare clic su **Indirizzi IP preassegnati da DHCP** nella pagina di Configurazione LAN. Si aprirà la pagina Indirizzi IP preassegnati da DHCP La pagina permette di assegnare un indirizzo IP specifico a un PC o un altro dispositivo che richieda un indirizzo IP mediante DHCP. La funzione permette di riservare solo gli indirizzi compresi nell'intervallo del DHCP disponibili per il gateway.  **Note:** – Il pulsante **Aggiungi IP statico** permette di aggiungere indirizzi IP statici all'elenco degli indirizzi IP preassegnati. – Il pulsante **Rimuovi IP statico** permette di aggiungere indirizzi IP statici all'elenco degli indirizzi IP preassegnati.

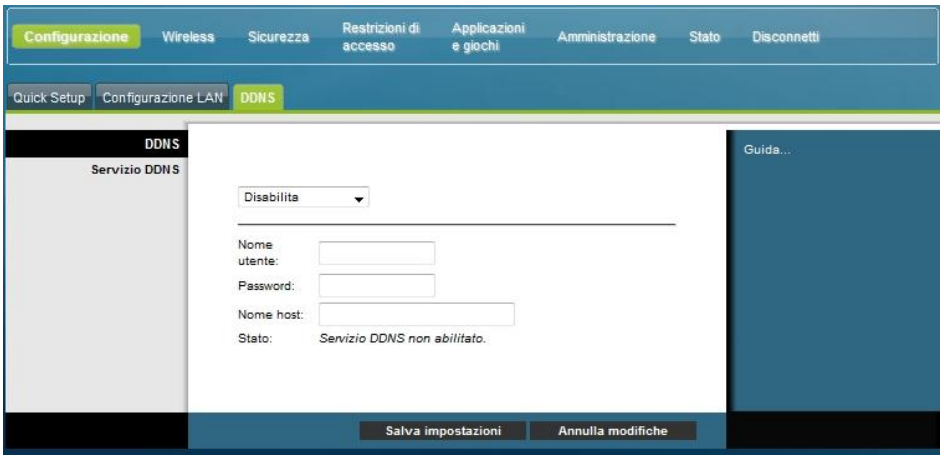
Sezione	Descrizione campo
	Indirizzo IP iniziale Mostra l'indirizzo iniziale usato dal server DHCP incorporato per distribuire indirizzi LAN IP privati. Poiché l'indirizzo IP predefinito del gateway è **192.168.0.1**, l'indirizzo IP iniziale deve essere **192.168.0.2** o superiore, ma inferiore a **192.168.0.253**. L'indirizzo IP iniziale predefinito è **192.168.0.10.N. massimo utenti DHCP** Inserire il numero massimo di utenti a cui il server DHCP può assegnare indirizzi IP da usare nella rete LAN. Tale numero non può essere maggiore di 254 meno l'indirizzo IP iniziale sopra descritto. **Durata lease del client** La voce Durata lease del client corrisponde alla durata di validità dell'indirizzo IP. Gli indirizzi di lease IP vengono automaticamente rinnovati tramite il PC utente e tutti gli altri dispositivi che usano DHCP per ottenere indirizzi IP. In caso di scadenza del leasing, l'indirizzo IP ritorna agli indirizzi IP disponibili che possono essere assegnati dal server DHCP come nuovi indirizzi da aggiungere alla rete. L'impostazione predefinita del tempo impostato è di 60 minuti con gateway collegato. **DNS statico LAN (Domain Name Server) 1-3** Il DNS viene usato dal PC o da altri dispositivi utente per individuare l'indirizzo IP pubblico associato a un URL o l'indirizzo in base al nome di un sito Web. È possibile specificare manualmente quali server DNS i dispositivi di rete devono usare inserendo gli indirizzi IP di tali server in questi campi. In caso contrario, il gateway invia automaticamente le informazioni del server DNCS provenienti dal provider di servizi. Per impostazione predefinita questi campi non vengono compilati.
Impostazioni ora	**Fuso orario** Selezionare il fuso orario per la propria località. Se nella propria zona viene utilizzata l'ora legale, selezionare **Passa automaticamente all'ora legale.**

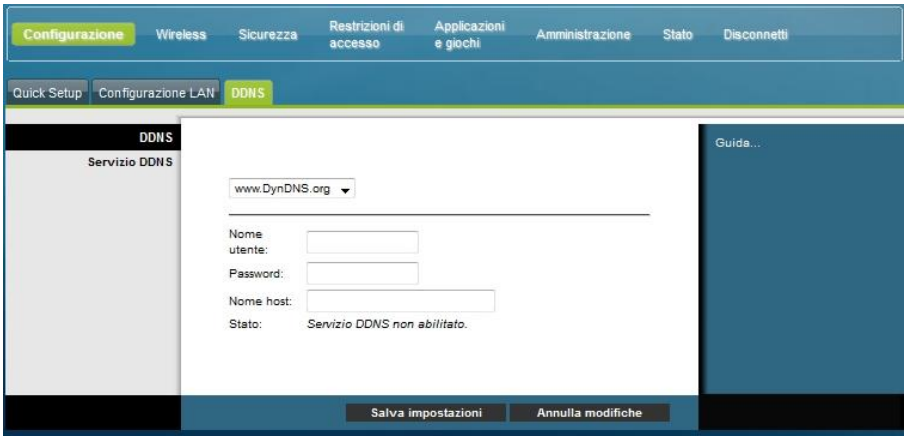
Configurazione > DDNS

L'opzione Dynamic Domain Name Service (DDNS) fornisce al gateway residenziale (che può avere un indirizzo IP modificato) un nome host o un URL risolvibile con applicazioni di rete tramite ricerca standard DNS. L'opzione DDNS si rivela particolarmente utile per l'hosting del proprio sito Web, di un server FTP o di altri

server gestiti dal dispositivo. Prima di usare questa opzione occorre registrarsi per il servizio DDNS.

Selezionare la scheda **DDNS** per aprire la pagina di configurazione DDNS.

Sezione	Descrizione campo
Servizio DDNS	**Disabilitazione DDNS** (Impostazioni predefinite) Per disabilitare il servizio DDNS, selezionare **Disabilita** dall'elenco a discesa e fare clic su **Salva impostazioni**.  **Abilitazione DDNS** **Nota:** per usare l'opzione DDNS occorre prima impostare un account e definire un URL con www.DynDNS.org. L'opzione DDNS non funziona senza un account valido. Per impostare un account DDNS, aprire il browser e inserire www.DynDNS.org nella barra degli indirizzi. Seguire le istruzioni del sito Web per impostare un account.

Sezione	Descrizione campo
Servizio DDNS	Per abilitare DDNS, procedere come segue. **1** Dalla pagina DDNS, selezionare **www.DynDNS.org** come proprio server DDNS.  **2** Configurare i seguenti campi: ■ Nome utente ■ Password ■ Nome host **3** Fare clic su **Salva impostazioni**. Il dispositivo comunicherà al servizio DDNS l'indirizzo IP WAN (Internet) corrente, qualora tale indirizzo venga modificato. **Importante:** l'area Stato della finestra visualizza ora lo stato del collegamento del servizio DDNS.

Configurazione delle impostazioni wireless

Questa sezione descrive le opzioni disponibili dalle pagine Wireless che si possono usare per configurare i parametri del WAP secondo le esigenze specifiche.

Wireless - Impostazioni wireless di base

Configurando il proprio gateway residenziale per la comunicazione wireless è possibile collegarsi a Internet da qualsiasi postazione nel range del WAP senza dover usare collegamenti cablati. Selezionare la scheda **Impostazioni di base** per aprire la pagina Impostazioni wireless di base.

La pagina Impostazioni wireless di base permette di selezionare la modalità di rete wireless e altre funzioni di base.

- Rete wireless: Abilita o Disabilita
- Configurazione wireless: impostazione Manuale o Wi-Fi Protected Setup (WPS)
- Modalità di rete
- Banda radio
- Ampiezza canale
- Canale standard
- Nome della rete wireless (SSID)

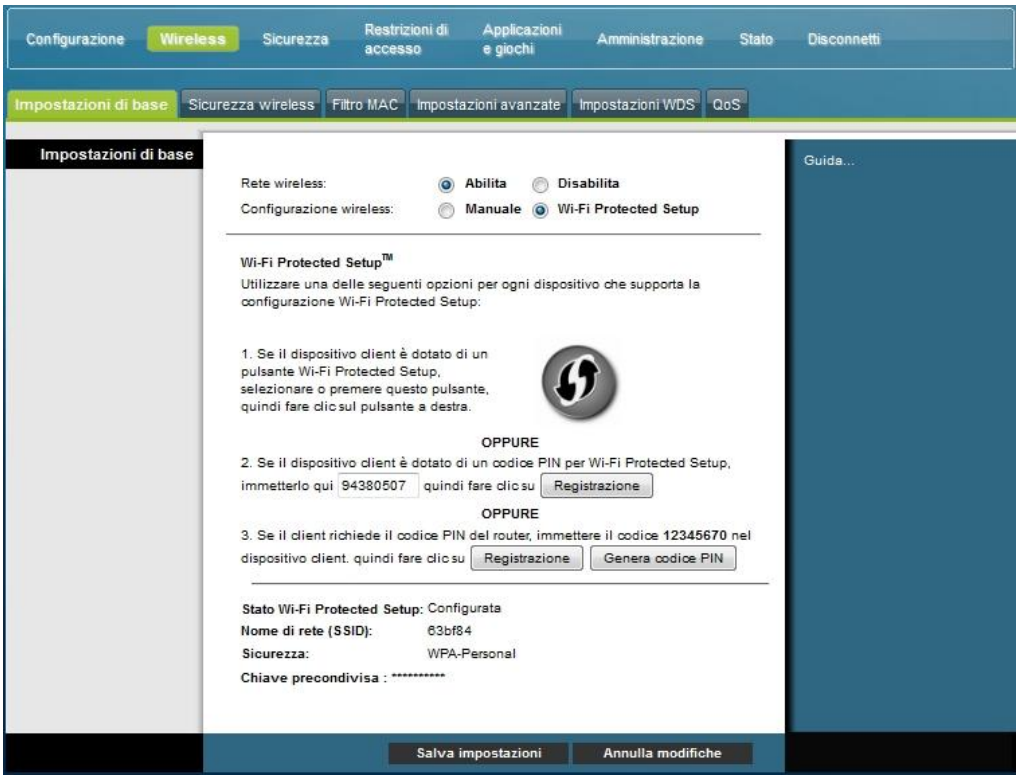
Wi-Fi Protected Setup (WPS)

Selezionando Wi-Fi Protected Setup (WPS) come configurazione wireless molte impostazioni risulteranno preconfigurate. La modalità WPS permette di eseguire una configurazione semplificata che consente di collegare alla rete nuovi dispositivi abilitati WPA.

Importante: se si usa la modalità WPS, il WEP non è supportato. Per usare il crittogramma WEP occorre disabilitare WPS, impostando la configurazione wireless su **Manuale**.

Nota: WPS è l'impostazione predefinita.

Esempio di configurazione wireless Wi-Fi Protected Setup

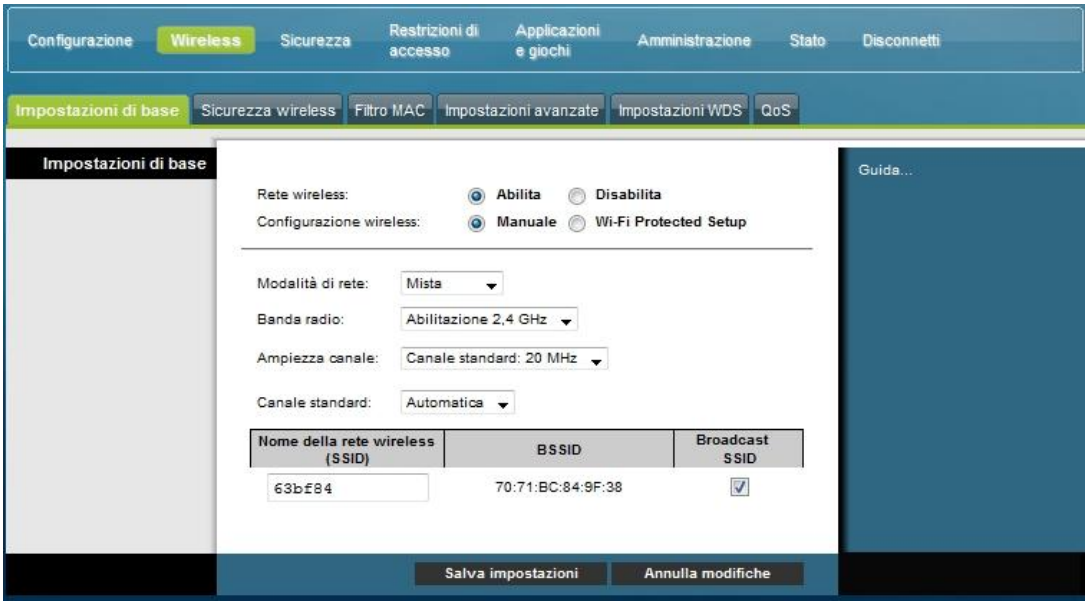


Descrizione della pagina di configurazione wireless Wi-Fi Protected Setup

Utilizzare le descrizioni e seguire le istruzioni riportate nella tabella seguente per configurare l'opzione Wi-Fi Protected Setup del gateway residenziale. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Impostazioni di base	**Abilita** o **Disabilita** la rete wireless **Configurazione Wi-Fi Protected Setup** La funzione Wi-Fi Protected Setup consente di configurare automaticamente una rete wireless protetta mediante crittografia. Per utilizzare tale funzione, è necessario disporre di almeno un altro dispositivo che supporti la modalità Wi-Fi Protected Setup all'interno della rete. Dopo aver configurato i dispositivi compatibili con la funzione Wi-Fi Protected Setup, è possibile configurare manualmente altri dispositivi. **Wi-Fi Protected Setup (Opzione 1)** Per registrare un client wireless sul gateway, premere il pulsante Wi-Fi Protected Setup sulla pagina Impostazioni wireless di base oppure il tasto sul pannello posteriore del gateway. Premere il pulsante software Wi-Fi Protected Setup sul client contemporaneamente al pulsante Wi-Fi Protected Setup sul gateway. La connessione verrà configurata automaticamente.
	Wi-Fi Protected Setup mediante codice PIN dell'adattatore Wi-Fi (Opzione 2) Questa è l'opzione che offre maggiore protezione per registrare il client wireless con il gateway. L'utente deve fornire il proprio codice PIN Wi-Fi Protected Setup, reperibile nell'utilità Wi-Fi Protected Setup del client. Dopo aver immesso il codice PIN Wi-Fi Protected Setup del client, l'utente è in grado di connettersi al gateway. **Wi-Fi Protected Setup mediante codice PIN del gateway (Opzione 3)** Notare che il codice PIN del Wi-Fi Protected Setup viene visualizzato sulla pagina Wi-Fi Protected Setup. Fare clic sul tasto Register (registra) dell' Opzione 3. Usando una qualsiasi utility client di Wi-Fi Protected Setup o di Microsoft Vista, inserire il codice PIN Wi-Fi Protected Setup del gateway nel dispositivo client per completare la registrazione.

Esempio di pagina di configurazione wireless manuale



Descrizione della pagina Impostazioni wireless di base

Utilizzare le descrizioni e seguire le istruzioni riportate nella tabella seguente per configurare le impostazioni di base per la comunicazione wireless del gateway residenziale. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Impostazioni di base	**Rete wireless** **Abilita** o **Disabilita** la rete wireless **Configurazione wireless** L'impostazione predefinita è **WPS**. Vedere *Wi-Fi Protected Setup (WPS)* (pag. 38) per ulteriori informazioni sull'uso del WPS. Selezionare **Manuale** per impostare manualmente la rete utente mediante questa opzione.
	Modalità di rete Selezionare una di queste opzioni per la modalità di rete: **Solo G, B/G mista, B/G/N mista** (impostazioni predefinite) **Importante:** selezionando la sola autenticazione TKIP, la modalità di rete B/G/N mista non è disponibile.

Sezione	Descrizione campo
	Banda radio Selezionare **Abilitazione 2,4 GHz** (valore predefinito) o **Abilitazione 5 GHz** **Nota:** la banda radio 5 GHz potrebbe non essere supportata in alcuni modelli. **Ampiezza canale** Selezionare **Canale standard: 20 MHz** o **Canale ampio: 40 MHz** **Canale standard** Selezionare dal menu a discesa un canale che corrisponda alle proprie impostazioni di rete. Tutti i dispositivi collegati alla rete wireless devono trasmettere sullo stesso canale per poter comunicare. Per la selezione automatica del canali selezionare **Auto** (valore predefinito).
	Nome di rete wireless (SSID) Il nome della rete wireless utente è SSID. La sigla SSID viene utilizzata dalla tecnologia wireless per identificare la rete utente da altre reti presenti nella zona. La sigla SSID può contenere fino a 32 caratteri. Il valore SSID predefinito in genere è composto dagli ultimi 6 caratteri dell'indirizzo CM MAC, che si trova sull'etichetta apposta sul fondo del gateway. La sigla SSID è un codice identificativo unico e non deve essere modificato se non per espressa volontà dell'utente. Il provider di servizi dell'utente potrà fornire tutte le informazioni di configurazione wireless per la richiesta di un identificativo SSID diverso. **BSSID** Visualizza il Basic Service Set Identifier (BSSID) della rete wireless utente. In genere il BSSID è l'indirizzo MAC del punto di accesso wireless. **Nota:** potrebbe non trattarsi dello stesso indirizzo MAC CM utilizzato per determinare il SSID predefinito. **Broadcast SSID** Se la casella reca il segno di spunta (impostazione predefinita), il gateway trasmette l'identificativo o avverte della presenza di altri dispositivi wireless. Se questo beacon è abilitato, i dispositivi client possono individuare automaticamente il punto di accesso. Per nascondere la propria rete ad altri client wireless, eliminare il segno di spunta dalla casella. Nascondendo la rete, si dovranno configurare manualmente i singoli dispositivi client wireless della rete. **Importante:** la casella di spunta **Abilita** non è attualmente in uso e non influisce in alcun modo sul funzionamento del gateway.

Wireless > Sicurezza wireless

La selezione di una modalità di sicurezza wireless consente di proteggere la rete. Se si seleziona **Disabilita,** la rete wireless non sarà protetta e tutti i dispositivi nelle vicinanze potranno connettersi.

Per evitare intrusioni nella propria rete wireless, usare la pagina Sicurezza wireless per configurare i propri parametri di sicurezza, compresa la modalità di sicurezza (livello di crittografia), le chiavi di crittografia e le altre impostazioni di sicurezza.

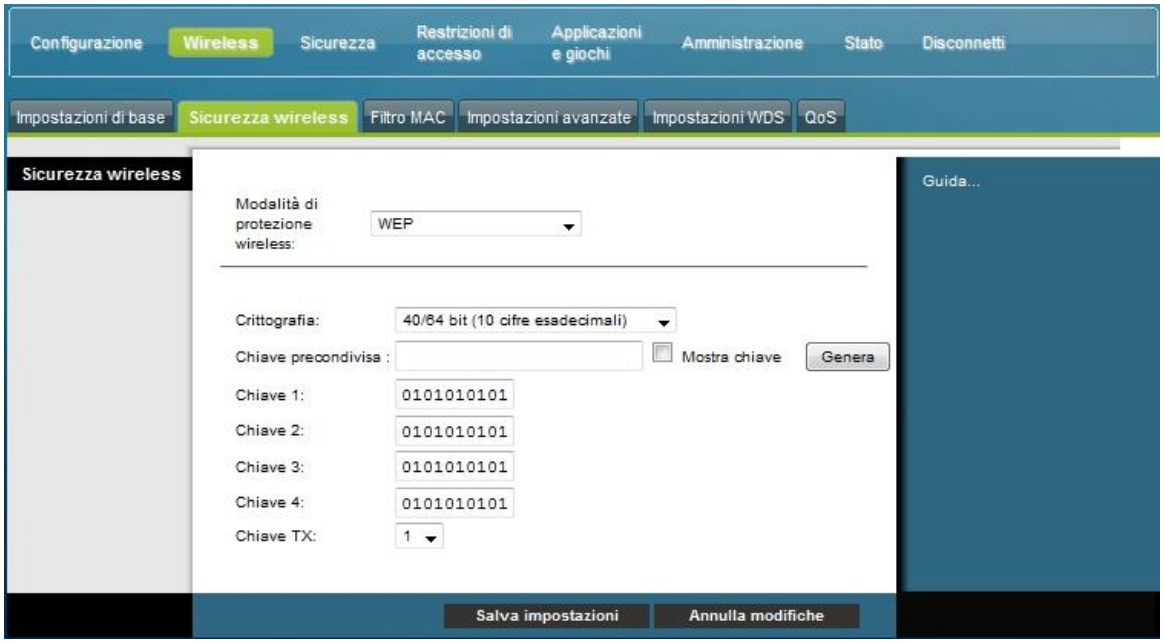
Selezionare la scheda **Sicurezza wireless** per aprire la relativa pagina. La tabella seguente illustra alcuni esempi della pagina di Sicurezza wireless con varie modalità di sicurezza wireless selezionate.

Descrizione della pagina Sicurezza wireless

Utilizzare le descrizioni e seguire le istruzioni riportate nella tabella seguente per configurare la sicurezza wireless del gateway residenziale Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo

Sezione	Descrizione campo
Sicurezza wireless	**Modalità di protezione wireless** Selezionare una di queste opzioni per la modalità sicurezza: **WEP** La modalità di sicurezza Wired Equivalent Privacy (WEP) viene definita nelle norme originali IEEE 802.11. Tale modalità non viene più consigliata in quanto fornisce una protezione insufficiente. Si consiglia perciò di eseguire la migrazione verso WPA-Personal o WPA2-Personal. **Nota:** la modalità WPS non supporta il WEP per questo dispositivo.



Descrizioni campo

- **Crittografia.** Selezionare un livello di crittografia WEP: 40/64 bit (10 cifre esadecimali) o 104/128 bit (26 cifre esadecimali).
- **Chiave precondivisa.** Per completare la configurazione della sicurezza wireless, è necessario scegliere una chiave precondivisa facile da ricordare e difficile da indovinare per altri utenti. Quando si collega un nuovo dispositivo wireless alla rete per la prima volta, potrebbe essere necessario immettere la chiave nella sezione di configurazione appropriata all'interno del dispositivo connesso. Per migliorare la sicurezza di rete, non divulgare la chiave a utenti non autorizzati. Immettere una frase composta da lettere e/o numeri con una lunghezza compresa tra 4 e 24 cifre. Quindi, fare clic su **Genera** per creare la chiave.
- **Chiave 1-4.** Se si desidera immettere le chiavi WEP manualmente, compilare i campi forniti. Ogni chiave WEP può contenere lettere dalla A alla F e numeri da 0 a 9. La chiave deve contenere un massimo di 10 caratteri per la crittografia a 40/64 bit o 26 caratteri per la crittografia a 104/128 bit.
- **Chiave TX.** Scegliere una chiave di trasmissione (TX) da 1 a 4. La chiave TX è la chiave che verrà usata per crittografare i dati utente. Anche se si possono creare quattro chiavi, una sola di esse verrà usata per crittografare i dati. Selezionare una delle quattro chiavi per la crittografia del WEP. Usare la chiave TX selezionata per configurare i client wireless.

Sezione	Descrizione campo

WPA

Sicurezza per le reti private – Modalità privata WPA o WPA2

Accesso Wi-Fi protetto (WPA) rappresenta una tecnologia wireless più sicura rispetto al WEP. Il WPA può essere usato da reti wireless di imprese (applicazioni aziendali) e private (reti domestiche). Si raccomanda caldamente di selezionare la modalità di sicurezza WPA-Personal o WPA2-Personal per le reti domestiche, a seconda della modalità supportata dall'adattatore wireless presente nel PC utente o nei wireless clients.

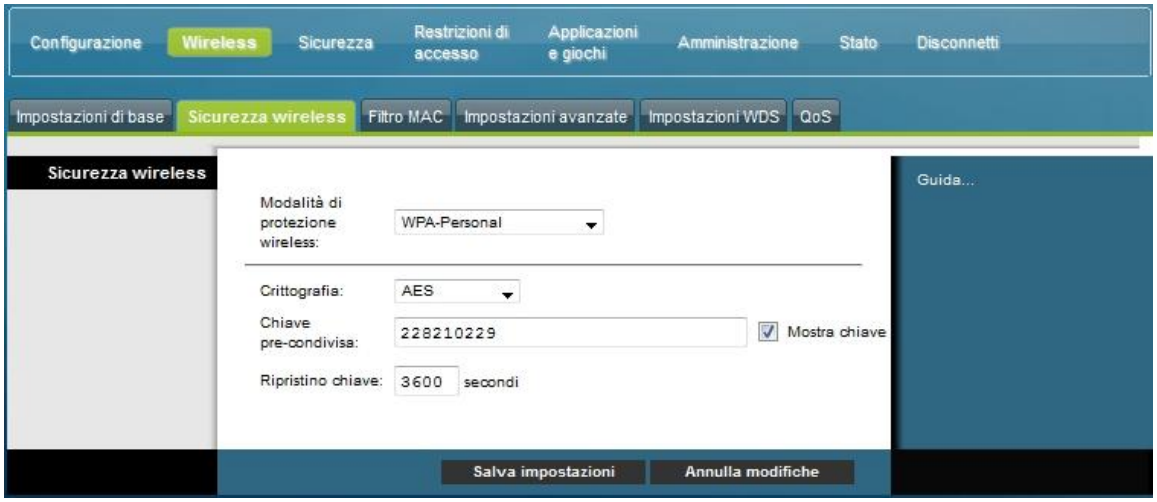
La modalità WPA-Personal (cioè WPA-PSK o chiave WPA pre-condivisa), consente di avere a disposizione una rete wireless più sicura del WEP. La modalità WPA-Personal introduce il metodo di autenticazione utente TKIP ed è caratterizzata da un chiavi di crittografia di livello superiore rispetto al WEP.

La modalità WPA2-Personal (cioè WPA2-PSK o chiave WPA2 precondivisa) consente di avere a disposizione una rete wireless standardizzata della massima sicurezza. La modalità WPA2-Personal è conforme agli standard AES (Advanced Encryption Standard) di trasmissione dati.

Nota: non tutti gli adattatori wireless supportano la modalità WPA2. La modalità WPA è supportata da una vasta serie di dispositivi. Indipendentemente dall'utilizzo di WPA o WPA2, accertarsi che il livello di sicurezza della chiave sia alto. Una chiave sicura si compone di una stringa di caratteri casuali, contenente 21 caratteri.

Selezionare una delle seguenti modalità WPA o WPA2 private:

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



Descrizioni campo

- **Crittografia.** L'impostazione predefinita è TKIP+AES.
- **Chiave pre-condivisa.** Immettere una chiave compresa tra 8 e 63 caratteri.
- **Ripristino chiave**. Immettere un intervallo di ripristino chiave per specificare la frequenza con cui si desidera che il dispositivo modifichi le chiavi di crittografia. L'impostazione predefinita è **3600** secondi.

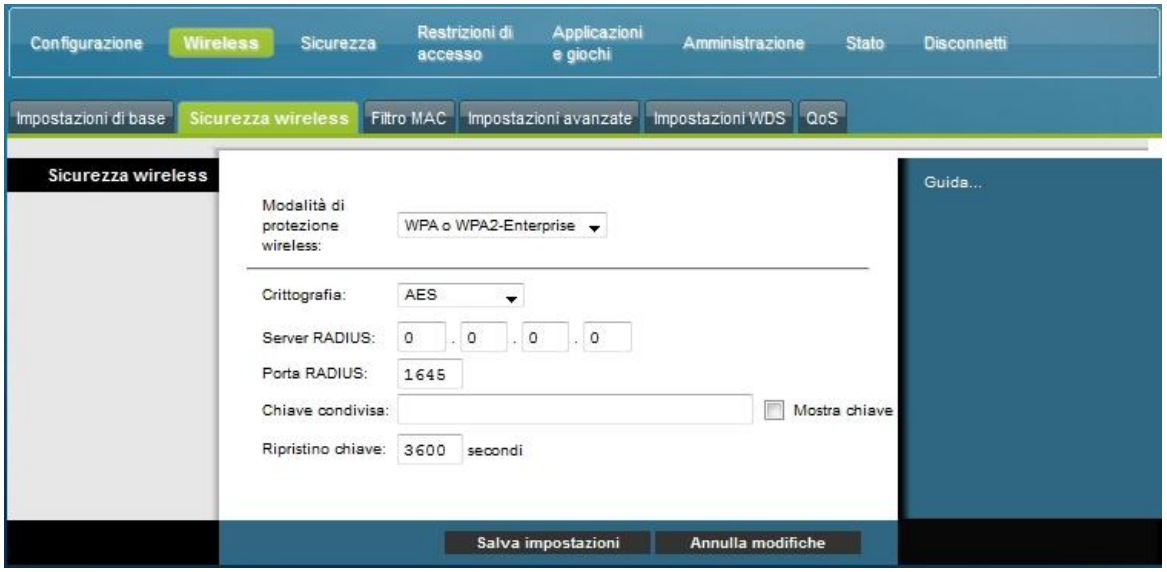
Sezione	Descrizione campo

Reti Security for Enterprise - Modalità WPA-Enterprise

Questa modalità sfrutta il protocollo WPA in associazione a un server RADIUS per l'autenticazione del client. (Deve essere utilizzata solo quando al dispositivo è collegato un server RADIUS.)

Selezionare uno dei tre seguenti modi WPA o WPA2-Enterprise

- **WPA-Enterprise**
- **WPA2-Enterprise**
- **WPA o WPA2-Enterprise**



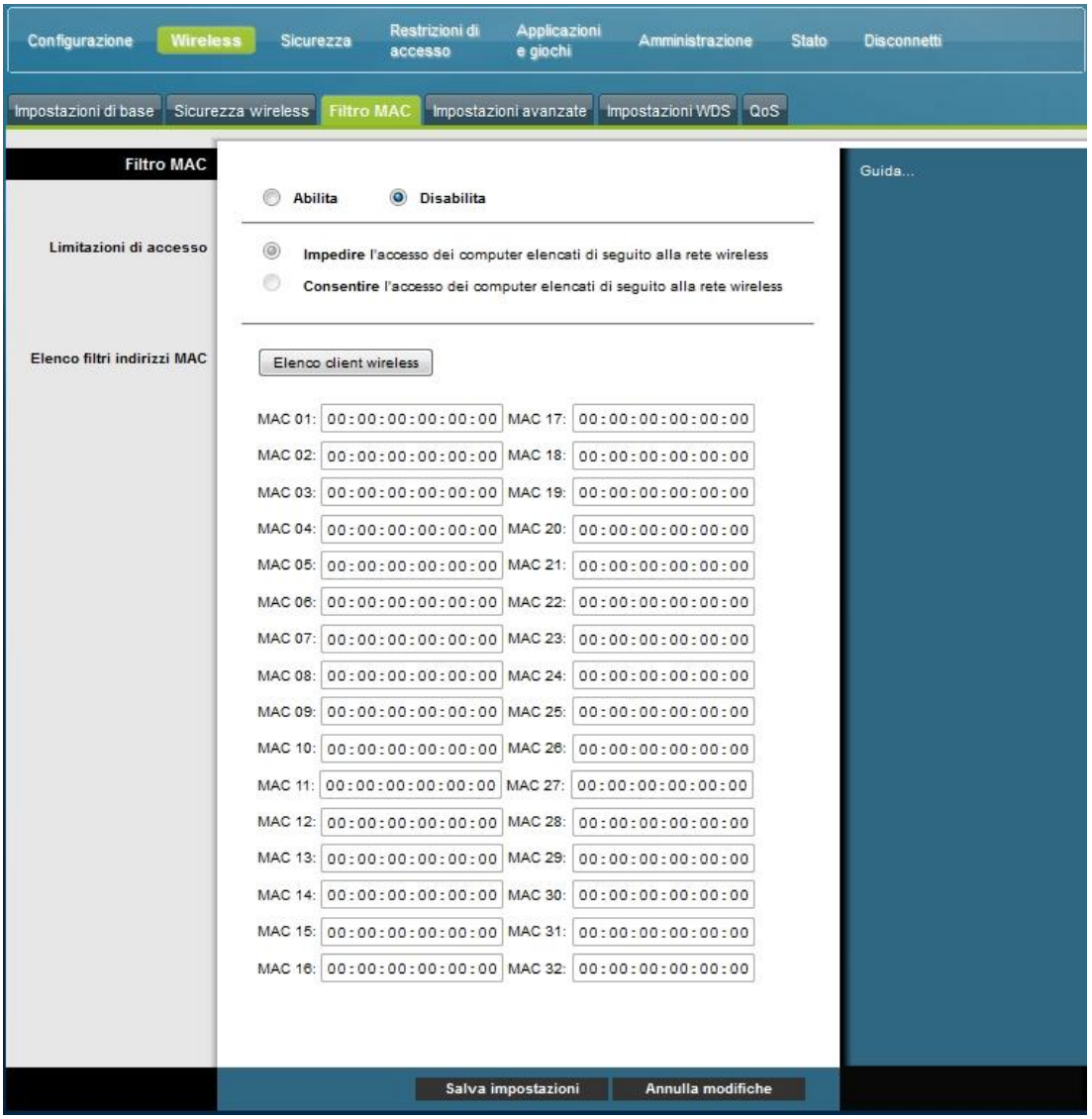
Descrizioni campo

- **Crittografia.** L'impostazione predefinita è TKIP+AES.
- **Server RADIUS.** Immettere l'indirizzo IP del server RADIUS.
- **Porta RADIUS.** Immettere il numero della porta utilizzata dal server RADIUS. L'impostazione predefinita è 1812.
- **Chiave condivisa.** Immettere la chiave utilizzata dal dispositivo e dal server RADIUS.
- **Ripristino chiave.** Immettere un intervallo di ripristino della chiave per specificare la frequenza con cui si desidera che il dispositivo modifichi le chiavi di crittografia. L'impostazione predefinita è **3600** secondi.

Scheda Wireless - Filtro MAC

La funzione filtro Filtro MAC viene utilizzata per consentire o impedire l'accesso alla rete wireless LAN in base all'indirizzo MAC dei dispositivi client wireless. La funzione Filtro MAC, anche nota come lista di accesso, viene utilizzata per consentire o impedire l'accesso alla rete wireless agli utenti non autorizzati.

Selezionare il tasto **Filtro MAC** per aprire la pagina Wireless Filtro MAC.



Descrizione pagina Wireless Filtro MAC

Usare le descrizioni e le istruzioni della seguente tabella per configurare il filtro indirizzi MAC per la rete wireless del gateway residenziale di appartenenza. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Filtro MAC	Permette di scegliere tra le opzioni **Abilita** o **Disabilita** il filtro MAC per il gateway residenziale
Restrizioni di accesso	**Restrizioni di accesso** Vengono utilizzate per consentire o impedire ai computer l'accesso alla rete wireless. La scelta influenza gli indirizzi elencati in questa pagina. Selezionare una delle opzioni seguenti: ■ Impedisci accesso alla rete wireless ai computer elencati di seguito Selezionare questa opzione per negare l'accesso a Internet agli indirizzi MAC dei dispositivi elencati nella tabella. A tutti gli altri indirizzi MAC verrà consentito l'accesso a Internet. ■ Consenti accesso alla rete wireless ai computer elencati di seguito. Selezionare questa opzione per consentire l'accesso a Internet solo agli indirizzi MAC dei dispositivi elencati nella tabella. A tutti gli indirizzi MAC non elencati nella tabella verrà negato l'accesso a Internet.
Elenco filtri indirizzi MAC	**Elenco filtri indirizzi MAC** L'utilizzo degli indirizzi MAC consente di visualizzare un elenco degli utenti dei quali si desidera controllare l'accesso wireless. Per visualizzare l'elenco degli utenti di rete in base agli indirizzi MAC, fare clic sul pulsante **Elenco client wireless**. Nel menu a discesa Ordina per è possibile ordinare la tabella per indirizzo IP, indirizzo MAC, Stato, Interfaccia o Nome client. Per visualizzare le informazioni più aggiornate, fare clic sul pulsante Aggiorna.

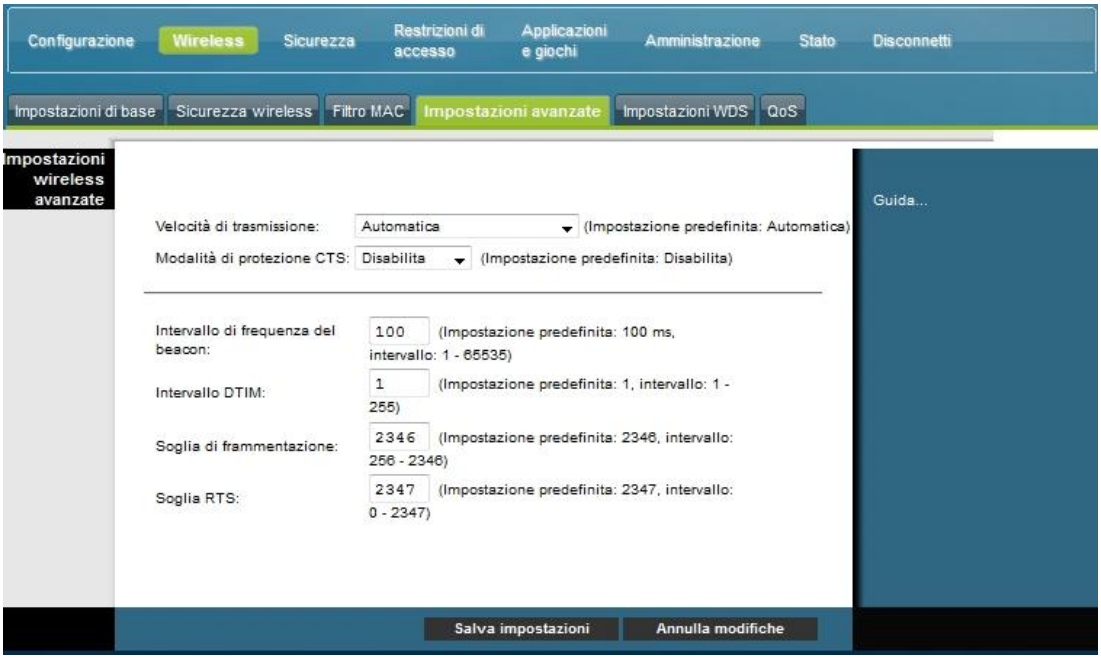
Wireless > Impostazioni avanzate

La funzione Impostazioni avanzate wireless aggiunge un ulteriore livello di sicurezza alla rete wireless per il gateway residenziale. Questa pagina consente di configurare le funzioni wireless avanzate. La regolazione di queste impostazioni sono riservate esclusivamente a un amministratore esperto. Eventuali impostazioni errate possono compromettere le prestazioni wireless.

Selezionare la scheda **Impostazioni avanzate** per aprire la pagina Impostazioni wireless avanzate.

Usare questa pagina per configurare le seguenti opzioni:

- Velocità di trasmissione N
- Modalità di protezione CTS
- Intervallo di frequenza del beacon
- Intervallo DTM
- Soglia di frammentazione
- Soglia RTS



Descrizione pagina Impostazioni wireless avanzate

Usare le descrizioni e le istruzioni della tabella seguente per configurare le impostazioni avanzate wireless per il gateway residenziale. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Impostazioni wireless avanzate	**Velocità di trasmissione N** La velocità di trasmissione dei dati deve essere impostata in base alla velocità della rete Wireless-N. Selezionare tra varie velocità di trasmissione, oppure selezionare l'impostazione **Auto** per consentire al dispositivo di utilizzare automaticamente la massima velocità dei dati possibile e abilitare la funzione di fallback automatico. Il fallback automatico consente di negoziare la migliore velocità di connessione tra il dispositivo e il client wireless. L'impostazione predefinita è **Auto**. Scegliere una delle seguenti opzioni per la velocità di trasmissione: ■ Auto (impostazione predefinita) ■ Utilizza velocità legacy ■ 0: 6,5 Mbps o 13,5 Mbps ■ 1: 13 Mbps o 27 Mbps ■ 2: 19,5 Mbps o 40,5 Mbps ■ 3: 26 Mbps o 54 Mbps ■ 4: 39 Mbps o 81 Mbps ■ 5: 52 Mbps o 108 Mbps ■ 6: 58,5 Mbps o 121,5 Mbps ■ 7: 65 Mbps o 135 Mbps ■ 8: 13 Mbps o 27 Mbps ■ 9: 26 Mbps o 54 Mbps ■ 10: 39 Mbps o 81 Mbps ■ 11: 52 Mbps o 108 Mbps ■ 12: 78 Mbps o 162 Mbps ■ 13: 104 Mbps o 216 Mbps ■ 14:117 Mbps o 243 Mbps ■ 15: 130 Mbps o 270 Mbps
	Modalità di protezione CTS La modalità di protezione CTS (Clear-To-Send) aumenta la capacità del dispositivo di catturare tutte le trasmissioni wireless, ma comporta una drastica diminuzione delle prestazioni. Selezionare **Auto** per usare questa funzione quando necessario, quando i prodotti Wireless-N/G non possono trasmettere al dispositivo in ambiente con traffico pesante 802,11b. Per disattivarla, selezionare **Disabilita**.

Sezione	Descrizione campo
	Intervallo di frequenza del beacon Questo valore indica l'intervallo di frequenza del beacon. Il beacon è un pacchetto trasmesso dal dispositivo per sincronizzare la rete wireless. (Impostazione predefinita: 100 ms, intervallo: 20 - 1000)
	Intervallo DTIM Il messaggio Delivery Traffic Indication Message (DTIM) indica l'intervallo tra le trasmissioni Broadcasts/Multicast. Il campo DTIM viene utilizzato per eseguire il conto alla rovescia per indicare ai client la disponibilità della successiva finestra di ascolto di messaggi broadcast e multicast. Dopo aver archiviato in un buffer di memoria i messaggi broadcast o multicast per i client associati, il dispositivo invia il DTIM successivo con un valore di intervallo DTIM. In questo modo, i client ricevono il beacon e si preparano a ricevere i messaggi broadcast e multicast. (Impostazione predefinita: 1, intervallo: 1 - 255)
	Soglia di frammentazione Soglia di frammentazione: specifica la dimensione massima di un pacchetto oltre la quale i dati verranno frammentati in più pacchetti. Se si riscontra una percentuale elevata di errori relativi ai pacchetti, è possibile aumentare leggermente la soglia di frammentazione. Impostando la soglia di frammentazione su un valore troppo basso, le prestazioni della rete possono risultare insoddisfacenti. Si consiglia di ridurre solo leggermente il valore predefinito. Nella maggior parte dei casi, questo valore deve essere mantenuto sull'impostazione predefinita 2346.
	Soglia RTS La soglia RTS determina a quale dimensione di pacchetto oltre la quale si invoca il meccanismo pronto per l'invio/autorizza l'invio (RTS/CTS). Se si verifica un flusso irregolare dei dati, è consigliabile ridurre solo leggermente il valore predefinito 2346. Se la dimensione di un pacchetto di rete è inferiore alla soglia RTS impostata, il meccanismo RTS o CTS non viene abilitato. Il dispositivo invia frame RTS (Request to Send) a una particolare stazione ricevente e negozia l'invio di un frame di dati. Dopo aver ricevuto la richiesta RTS, la stazione wireless risponde con un frame CTS (Clear to Send) che autorizza a iniziare la trasmissione. Il valore della soglia RTS dovrebbe rimanere impostato sull'impostazione predefinita 2347.

Wireless > Impostazioni WDS

La pagina WDS (Wireless Distribution System) consente di ampliare la copertura della rete wireless tramite i ripetitori di segnali. Accertarsi che le impostazioni del canale siano le stesse per tutti i dispositivi per cui è abilitato il sistema WDS.

Selezionare il tasto **Impostazioni WDS** per aprire la pagina impostazioni wireless. Usare questa pagina per configurare le impostazioni WDS.

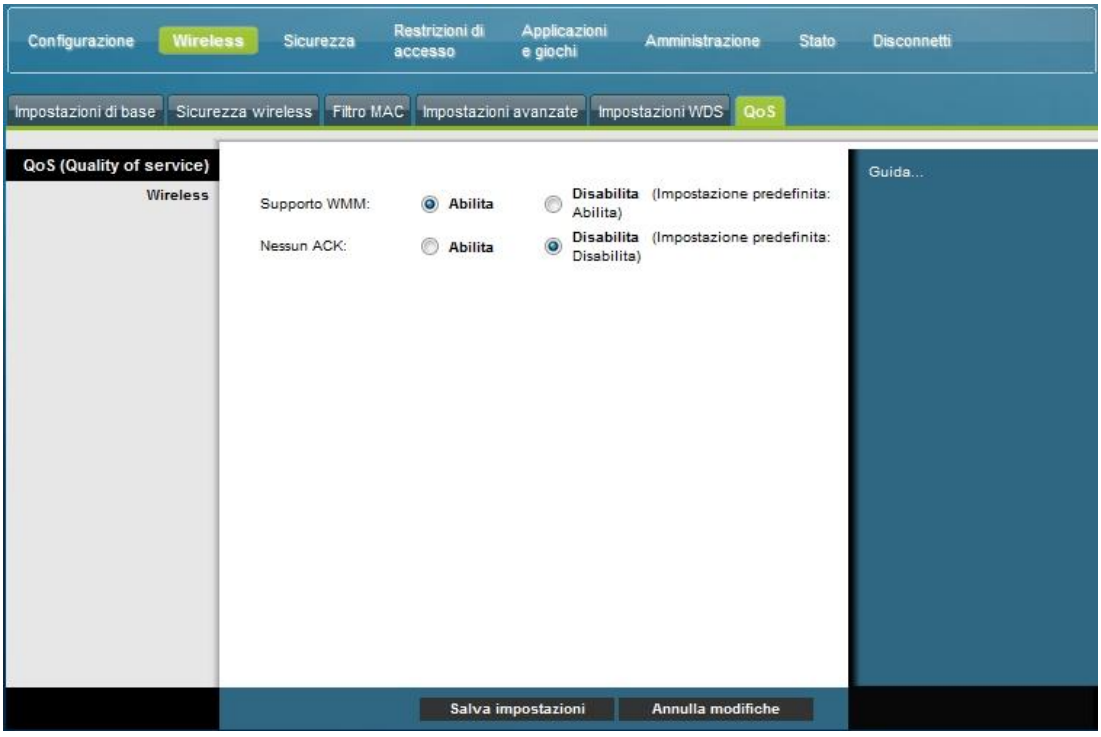
Descrizione pagina impostazioni WDS Wireless

Usare le descrizioni e le istruzioni della tabella seguente per configurare le impostazioni sistema distribuzione wireless per il gateway residenziale. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
WDS	**Indirizzo MAC del WDS** Visualizza l'indirizzo WDS MAC (o BSSID) del punto di accesso al gateway
	Consenti ripetizione del segnale wireless a un ripetitore Spuntare questa casella per consentire al client wireless di collegarsi a un ripetitore e avviare il traffico tra il client wireless e il ripetitore. Sono consentiti un massimo di 3 ripetitori.
	Indirizzo MAC del punto di accesso remoto (da MAC 1a 3) Usa i tre campi (MAC 1, 2, e 3) per immettere l'indirizzo MAC dei ripetitori

Wireless > QoS

QoS (Quality of Service) garantisce un servizio migliore alle tipologie di traffico di rete ad alta priorità, che possono richiedere applicazioni sofisticate e in tempo reale, come la videoconferenza. Le impostazioni QoS consentono di specificare le priorità per tipi diversi di traffico. Il traffico con priorità più bassa viene rallentato per consentire un trasferimento dei dati più veloce e un ritardo minore per il traffico ad alta priorità. Selezionare il tasto **QoS** per aprire la pagina Wireless QoS.



Descrizione pagina Wireless QoS

Usare le descrizioni e le istruzioni della tabella seguente per configurare ciascuna impostazione QoS. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

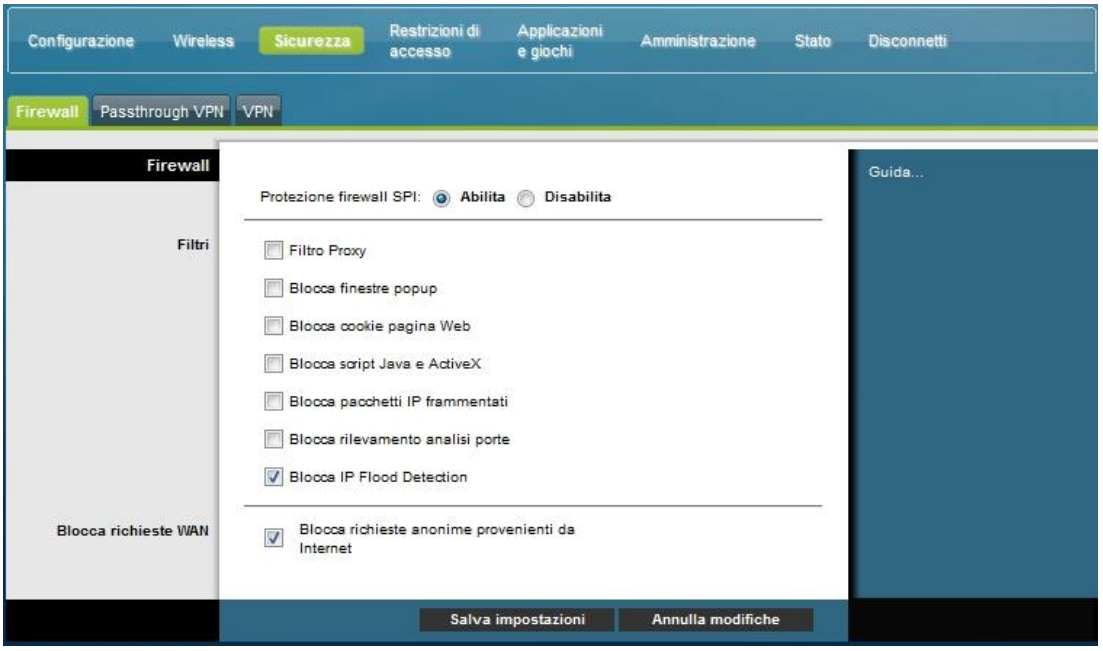
Sezione	Descrizione campo
QoS (Quality of Service)	**Supporto WMM** Se WMM (Wi-Fi Multimedia) è supportato dai client wireless, abilitando questa funzione il traffico vocale e multimedia avrà la priorità nei confronti di altro traffico. Selezionare l'opzione desiderata: ■ **Abilita (impostazione predefinita)** ■ **Disabilita**
	Nessun ACK Consente di abilitare o disabilitare Nessun ACK. Funzione consigliata per servizi dati per i quali la trasmissione è importante e la perdita di pacchetti è tollerabile fino a un certo punto. Se si seleziona **Disabilita**, per ogni pacchetto ricevuto viene restituito un pacchetto di conferma. Ciò consente una trasmissione più affidabile, ma aumenta il volume di traffico e diminuisce le prestazioni. Selezionare l'opzione desiderata: ■ **Abilita** ■ **Disabilita (impostazione predefinita)**

Configurazione della sicurezza

Sicurezza > Firewall

La tecnologia avanzata firewall protegge la rete dagli hacker e dagli accessi non autorizzati. Usare questa pagina per configurare un firewall in grado di filtrare vari tipi di traffico indesiderato sulla rete locale del gateway.

Selezionare il tasto **Firewall** per aprire la pagina Sicurezza Firewall.



Usare le descrizioni e le istruzioni della tabella seguente per configurare il firewall per il gateway residenziale. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

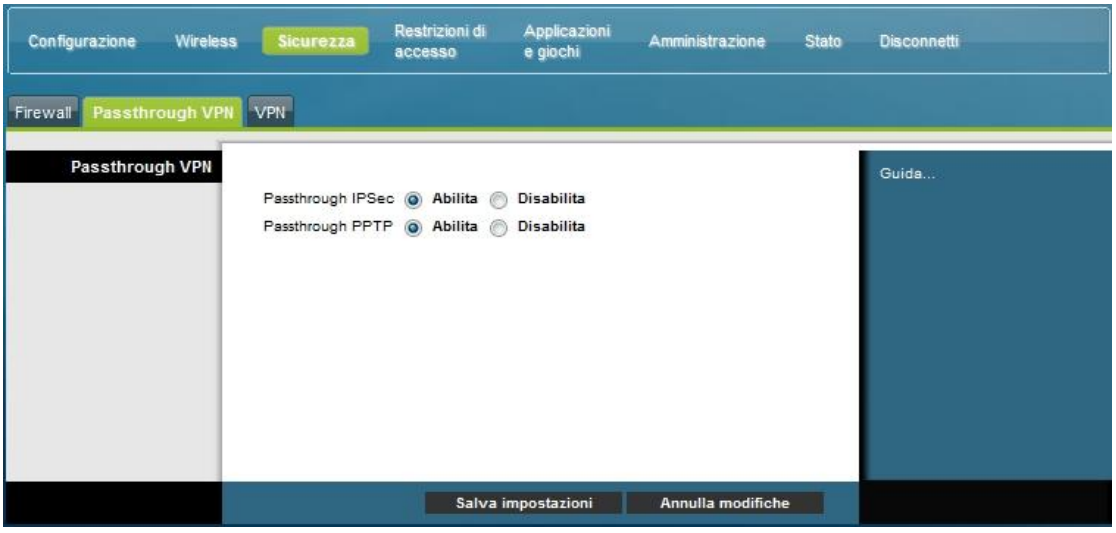
Sezione	Descrizione campo
Firewall	**Protezione firewall SPI** La funzione Protezione firewall SPI blocca gli attacchi DoS (Denial of Service). Un attacco DoS non tenta di rubare i dati o danneggiare i computer, ma sovraccarica la connessione Internet in modo da non poterla più utilizzare. Selezionare l'opzione desiderata: ■ **Abilita (impostazione predefinita)** ■ **Disabilita**

Sezione	Descrizione campo
Filtri	**Filtro Proxy** Abilita/disabilita Filtro Proxy. Se gli utenti locali accedono ai server proxy WAN, sono in grado di eludere i filtri e di accedere ai siti Internet bloccati dal dispositivo. Se si seleziona la funzione Filtro Proxy, verrà bloccato l'accesso a qualsiasi server proxy WAN. **Blocca finestre popup** Abilita/disabilita finestre popup. In alcune applicazioni comunemente utilizzate si usano finestre di popup come parte dell'applicazione. Se si disabilita le finestre popup, si può interferire con alcune di queste applicazioni. **Blocca cookie pagina Web** Abilita/disabilita blocco cookie. Questa funzione filtra i cookie indesiderati in arrivo da Internet verso i dispositivi della rete locale privata. I cookie sono file di computer che contengono dati personali o dati di surfing del Web. **Blocca script Java e ActiveX** Abilita/disabilita java applet e ActiveX scripts. Questa funzione protegge i dispositivi della rete privata da irritanti o malintenzionate applet Java inviate via internet senza essere state richieste ai dispositivi della rete privata. Queste applet vengono eseguite automaticamente al ricevimento da parte di un PC. Java è un linguaggio di programmazione per siti Web. Se si seleziona la funzione Filtro Applet Java, si corre il rischio di non poter accedere ai siti Internet creati usando questo linguaggio di programmazione. Questa funzione protegge inoltre i dispositivi della rete privata da irritanti o malintenzionate Java applets inviate via internet senza essere state richieste ai dispositivi della rete privata. Questi controlli ActiveX vengono eseguiti automaticamente al ricevimento da parte di un PC. **Blocca pacchetti IP frammentati** Abilita/disabilita il filtraggio di pacchetti IP frammentati. Questa funzione protegge la rete locale privata da attacchi al diniego di servizio. **Blocca rilevamento analisi porte** Abilita/disabilita la risposta del gateway alle analisi porte da Internet. Protegge la rete locale privata dagli hacker di internet che tentano di accedere alla rete rilevando porte IP aperte sul gateway. **Blocca IP Flood Detection** (controllato – impostazione predefinita) Blocca i dispositivi fraudolenti che tentano di ingolfare i dispositivi o le reti con pacchetti trasmessi illegali. Anche noti come “broadcast storm.”(diluvio trasmesso)

Sezione	Descrizione campo
Blocca richieste WAN	**Blocca richieste anonime provenienti da Internet** (controllato – impostazione predefinita) Abilitare questa funzione per evitare che la rete venga rilevata da altri utenti Internet, ad esempio con un comando ping. Anche la funzione Blocco richieste Internet anonime consente di nascondere le porte di rete. Queste due funzioni rendono più difficile agli utenti esterni l'accesso alla rete.

Sicurezza > Passthrough VPN

Usare questa pagina per configurare il supporto Virtual Private Network (VPN) . Abilitando le impostazioni di questa pagina consente ai tunnel VPN che usano i protocolli IPsec o PPTP di superare il firewall del gateway. Selezionare il tasto **Passthrough VPN** per aprire la pagina Sicurezza Passthrough VPN.



Usare le descrizioni e le istruzioni della tabella seguente per configurare il passthrough VPN per il gateway residenziale. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Passthrough VPN	**Passthrough IPSec** Abilita/disabilita Internet Protocol Security (IPsec). IPSec (Internet Protocol Security) è una suite di protocolli utilizzati per implementare lo scambio sicuro di pacchetti a livello IP. Abilitando IPSec Passthrough, le applicazioni che usano IPsec (IP Security) possono superare il firewall. Per disabilitare l'impostazione Passthrough IPSec, selezionare **Disabilita.** Selezionare l'opzione desiderata: ■ **Abilita (impostazione predefinita)** ■ **Disabilita**
	Passthrough PPTP Abilita/disabilita il protocollo PPTP (Point-to-Point Tunneling Protocol). PPTP consente al protocollo Point-to-Point Protocol (PPP) di accede tramite tunnel ad una rete IP. Abilitando il passthrough PPTP, le applicazioni che usano il protocollo Point to Point Tunneling Protocol (PPTP) possono superare il firewall. Per disabilitare PPTP Passthrough selezionare **Disabilita**. Selezionare l'opzione desiderata: ■ **Abilita (impostazione predefinita)** ■ **Disabilita**

Sicurezza > VPN

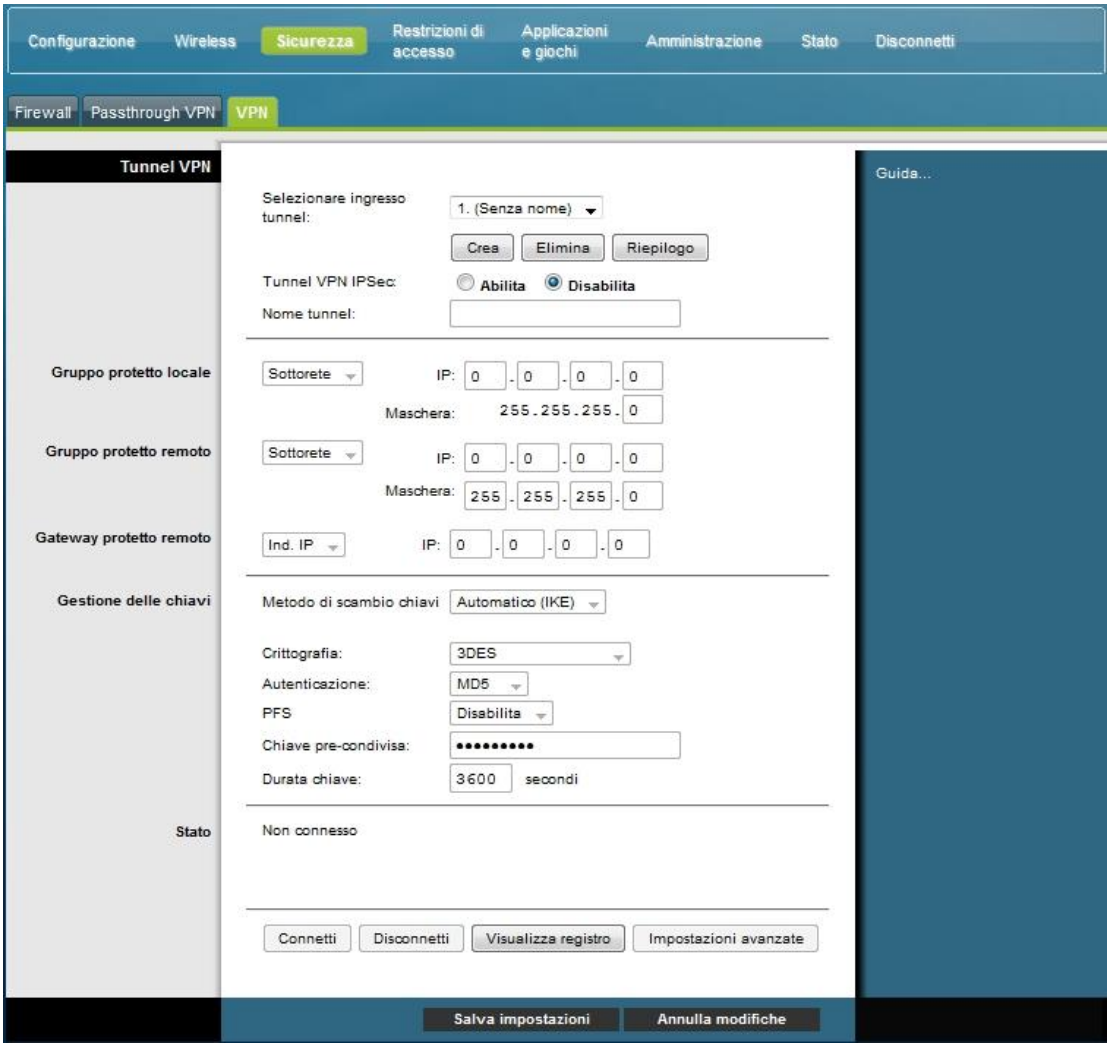
La rete Virtual Private Network (VPN) è il collegamento tra due endpoint di reti differenti che permette l'invio sicuro di dati privati tramite le reti pubbliche o altre reti private. Si realizza creando un tunnel VPN. Il tunnel VPN collega i due PC o le due reti e consente la trasmissione dati tramite Internet come se fosse una rete privata. Il tunnel VPN usa IPsec per crittare i dati scambiati tra i due endpoint e inserirli in un ambiente Ethernet/IP standard, consentendo il passaggio dei dati tra reti in modo sicuro e senza problemi.

VPN è un'alternativa conveniente e più sicura rispetto a una linea privata dedicata in noleggio per reti private. Con l'uso di un linguaggio crittografico di riferimento e debite tecniche di autenticazione, IPsec VPN crea un collegamento sicuro che funziona come se l'utente fosse collegato direttamente alla rete locale privata.

Esempio: la VPN consente agli utenti di collegarsi da casa alla rete aziendale per ricevere indirizzi IP sulla rete privata come se fossero in ufficio collegati alla LAN aziendale.

Selezionare il tasto **VPN** per aprire la pagina Sicurezza VPN.

Usare questa pagina per configurare la VPN per il gateway residenziale.



Descrizione pagina Sicurezza tunnel VPN

Usare le descrizioni e le istruzioni della tabella seguente per configurare il tunnel VPN per il gateway. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Tunnel VPN	**Selezionare ingresso tunnel** Permette di visualizzare l'elenco di tunnel VPN creati **Pulsante Crea** Fare clic su questo pulsante per creare un nuovo tunnel. **Pulsante Elimina** Fare clic su questo pulsante per eliminare tutte le impostazioni del tunnel selezionato. **Pulsante Riepilogo** Fare clic su questo pulsante per visualizzare le impostazioni e lo stato di tutti i tunnel abilitati **Tunnel VPN IPSec** Consente di abilitare o disabilitare il protocollo Internet Security Protocol per il tunnel VPN **Nome tunnel** Digitare il nome del tunnel
Gruppo protetto locale	Selezionare gli utenti della rete LAN che possono utilizzare questo tunnel VPN. È possibile specificare un singolo indirizzo IP o una sottorete. Tenere presente che il gruppo sicuro locale deve corrispondere al gruppo sicuro remoto del gateway. **IP** Immettere l'indirizzo IP della rete locale. **Maschera** Se viene selezionata l'opzione Sottorete, immettere la maschera per determinare gli indirizzi IP nella rete locale.
Gruppo sicuro remoto	Selezionare gli utenti della rete LAN remota dietro al gateway remoto autorizzati a utilizzare il tunnel VPN. È possibile specificare un singolo indirizzo IP, una sottorete o qualsiasi indirizzo. Se è impostato "Qualsiasi", il gateway funziona come dispositivo di risposta e accetta richieste da qualsiasi utente remoto. Tenere presente che il gruppo sicuro remoto deve corrispondere al gruppo sicuro locale del gateway. **IP** Immettere l'indirizzo IP della rete remota. **Maschera** Se viene selezionata l'opzione Sottorete, immettere la maschera per determinare gli indirizzi IP nella rete remota.

Sezione	Descrizione campo
Gateway protetto remoto	Selezionare l'opzione desiderata, **Ind. IP**, **Qualsiasi** o **FQDN**. Se il gateway remoto dispone di un indirizzo IP dinamico, selezionare **Qualsiasi** o **FQDN**. Se è selezionato **Qualsiasi**, il gateway accetterà richieste provenienti da qualsiasi indirizzo IP. **FQDN** Se è selezionato **FQDN**, immettere il nome di dominio del gateway remoto, affinché il gateway possa individuare un indirizzo IP corrente utilizzando il sistema DDNS. **IP** L'indirizzo IP in questo campo deve corrispondere all'indirizzo IP pubblico (WAN o Internet) del gateway remoto all'altra estremità del tunnel.
Gestione delle chiavi	**Metodo di scambio chiavi** Il gateway supporta sia la gestione della chiave automatica che quella manuale. Quando viene selezionata la gestione della chiave automatica, il key material per la SA (Security Association) viene negoziato utilizzando i protocolli IKE (Internet Key Exchange). Se si sceglie la gestione manuale, la negoziazione delle chiavi non è richiesta. Sostanzialmente, la gestione della chiave manuale viene utilizzata in piccoli ambienti statici o per la risoluzione di problemi. Tenere presente che entrambe le parti devono utilizzare lo stesso metodo di gestione della chiave. Selezionare una delle seguenti opzioni per il metodo di scambio chiavi: ■ Automatico (IKE) – **Crittografia:** il metodo di crittografia determina la lunghezza delle chiavi utilizzate per crittografare o decrittografare i pacchetti ESP. Tenere presente che entrambe le parti devono utilizzare lo stesso metodo. – **Autenticazione:** il metodo di Autenticazione consente di autenticare i pacchetti ESP (Encapsulating Security Payload). Selezionare **MD5** o **SHA**. Tenere presente che entrambe le parti (endpoint VPN) devono utilizzare lo stesso metodo. ▪ MD5: algoritmo di hashing unidirezionale che produce digest a 128 bit. ▪ SHA: algoritmo di hashing unidirezionale che produce digest a 160 bit. – **PFS (Perfect Forward Secrecy)**: se è abilitata l'opzione PFS, la negoziazione IKE fase 2 genera nuovo key material per la cifratura e l'autenticazione del traffico IP. Tenere presente che l'opzione PFS deve essere abilitata in entrambe le parti. – **Chiave pre-condivisa:** la negoziazione IKE utilizza la chiave precondivisa per autenticare il peer IKE remoto. In questo campo è possibile immettere sia caratteri che valori esadecimali, ad esempi \My_@123\ oppure \0x4d795f40313233\. Tenere presente che entrambe le parti devono utilizzare la stessa chiave precondivisa. – **Durata chiave**: questo campo specifica la durata della chiave generata tramite IKE. Raggiunta la scadenza, viene rinegoziata automaticamente una nuova chiave. È possibile immettere un valore compreso tra 300 e 100.000.000 secondi. Il valore predefinito è **3600** secondi.

Sezione	Descrizione campo
Gestione delle chiavi (continua)	■ Manuale – **Crittografia:** il metodo di crittografia determina la lunghezza delle chiavi utilizzate per crittografare o decrittografare i pacchetti ESP. Tenere presente che entrambe le parti devono utilizzare lo stesso metodo. – **Chiave di crittografia**: in questo campo è indicata la chiave da utilizzare per crittografare e decrittare il traffico IP. È possibile immettere sia lettere che valori esadecimali. Tenere presente che entrambe le parti devono utilizzare la stessa chiave di cifratura. – **Autenticazione**: il metodo di Autenticazione consente di autenticare i pacchetti ESP (Encapsulating Security Payload). Selezionare MD5 o SHA. Tenere presente che entrambe le parti (endpoint VPN) devono utilizzare lo stesso metodo. ▪ MD5: algoritmo di hashing unidirezionale che produce digest a 128 bit. ▪ SHA: algoritmo di hashing unidirezionale che produce digest a 160 bit. – **Chiave di autenticazione:** in questo campo è indicata la chiave da utilizzare per autenticare il traffico IP. È possibile immettere sia lettere che valori esadecimali. Tenere presente che entrambe le parti devono utilizzare la stessa chiave di autenticazione. – **SPI in entrata o SPI in uscita**: l'indice SPI (Security Parameter Index) è riportato nell'intestazione ESP e consente al destinatario di selezionare l'algoritmo SA da utilizzare per l'elaborazione del pacchetto. L'indice SPI è un valore a 32 bit. Sono accettabili sia valori decimali che esadecimali: ad esempio, "987654321" o "0x3ade68b1". Ogni tunnel deve avere un SPI in entrata e un SPI in uscita univoco. Due tunnel non possono condividere lo stesso indice SPI. Tenere presente che l'SPI in entrata deve corrispondere all'SPI in uscita del gateway remoto e viceversa.
Stato	In questo campo è visualizzato lo stato di connessione del tunnel selezionato, ossia **connesso** o **disconnesso**.

Sezione	Descrizione campo
Pulsanti	**Connetti** Fare clic su questo pulsante per stabilire una connessione per il tunnel VPN corrente. Se sono state apportate modifiche, fare clic sul pulsante **Salva impostazioni** per applicarle. **Disconnetti** Fare clic su questo pulsante per interrompere una connessione per il tunnel VPN corrente. **Visualizza registro** Fare clic su questo pulsante per visualizzare il registro VPN, che contiene i dettagli relativi a ogni tunnel creato. **Impostazioni avanzate** Se il metodo di scambio chiavi è impostato su Automatico (IKE), consentirà l'accesso alle impostazioni aggiuntive relative a IKE. Fare clic su questo pulsante se il gateway non è in grado di creare un tunnel VPN con il gateway remoto, quindi accertarsi che le impostazioni avanzate corrispondano a quelle del gateway remoto. ■ Fase 1 -Modalità operativa Selezionare il metodo appropriato per l'endpoint VPN remoto. – **Principale**: la modalità Principale è più lenta ma offre maggiore protezione. – **Aggressiva**: la modalità Aggressiva è più veloce ma offre una protezione minore. ■ Identità locale Selezionare l'opzione desiderata corrispondente all'impostazione della Identità remota all'altra estremità del tunnel. – Indirizzo IP locale: indirizzo IP (Internet) WAN – Nome: nome dominio ■ Identità remota Selezionare l'opzione desiderata corrispondente all'impostazione della Identità locale all'altra estremità del tunnel. – Indirizzo IP locale: indirizzo IP (Internet) WAN dell'endpoint VPN remoto – Nome: nome di dominio dell'endpoint VPN remoto. ■ Crittografia Questo è l'algoritmo di crittografia utilizzato per l'algoritmo SA IKE. Deve corrispondere all'impostazione utilizzata all'altra estremità del tunnel.

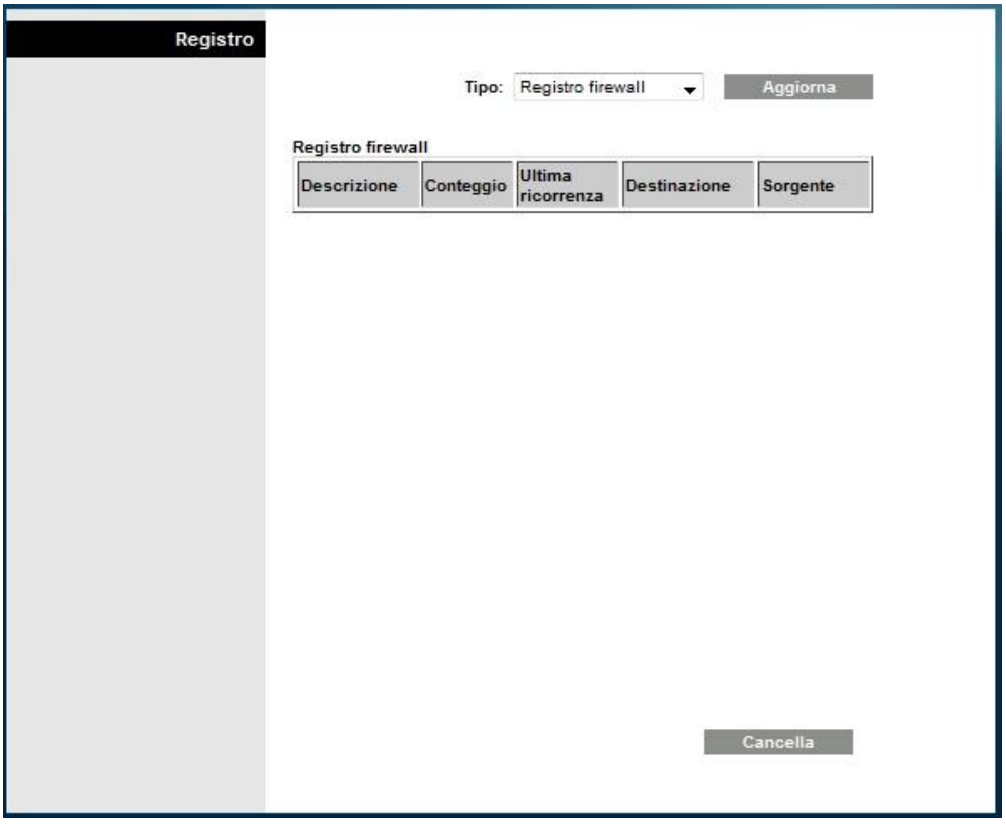
Visualizza registro

La pagina Sicurezza VPN > Visualizza registro mostra gli eventi recepiti dal firewall. Il registro visualizza i seguenti elementi:

- Descrizione dell'evento
- Numero di eventi occorsi
- Ultimo evento occorso
- Indirizzi di provenienza e di destinazione

Registri visualizzabili da questa pagina:

- Registro accessi
- Registro firewall
- Registro VPN
- Registro controllo genitori



Fare clic su **Cancella** per cancellare tutti i dati dal registro.

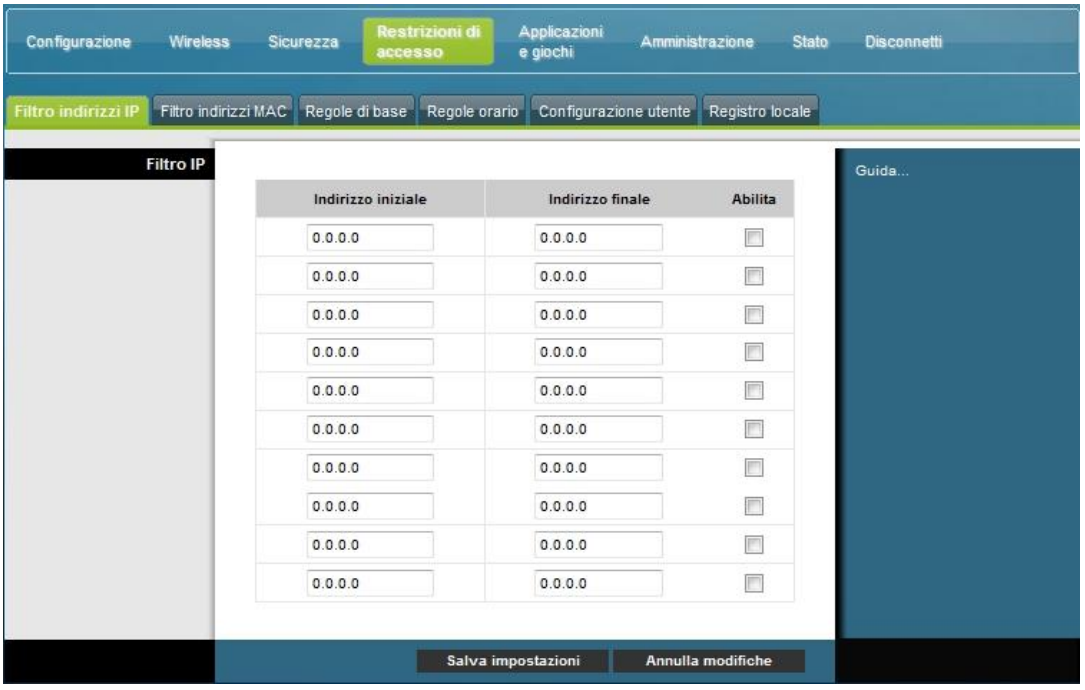
Controllo accesso al Gateway

Scheda Restrizioni di accesso > Filtro indirizzi IP

Utilizzare la pagina Restrizioni accesso > Filtro IP per configurare i filtri di indirizzi IP che consentono di impedire l'accesso a Internet a un intervallo di indirizzi IP.

Nota: se non si ha familiarità con le impostazioni avanzate riportate in questa sezione, contattare il provider di servizi prima di provare a modificare eventuali impostazioni di filtro IP avanzate predefinite del gateway residenziale wireless.

Selezionare il tasto **Filtro indirizzi IP** per aprire la pagina Restrizioni di accesso > Filtro indirizzi IP. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

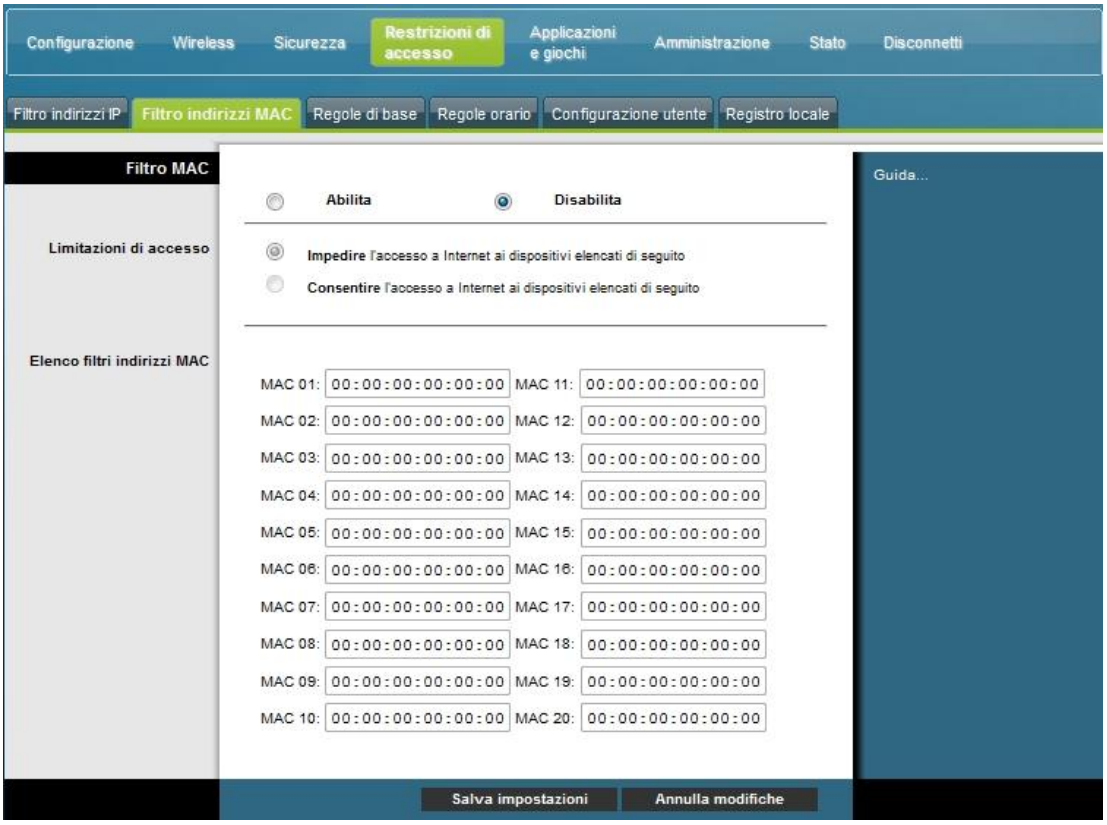


Restrizioni di accesso > Filtro indirizzi MAC

Utilizzare la pagina Restrizioni accesso > Filtro MAC per configurare i filtri di indirizzi MAC che consentono di autorizzare o bloccare l'accesso a un intervallo di indirizzi MAC a Internet in funzione dell'indirizzo MAC.

Nota: se non si ha familiarità con le impostazioni avanzate riportate in questa sezione, contattare il provider di servizi prima di provare a modificare eventuali impostazioni di filtro IP avanzate predefinite del gateway residenziale wireless.

Selezionare il tasto **Filtro indirizzi MAC** per aprire la pagina Restrizioni di accesso > Filtro indirizzi MAC.



Il menu a discesa Blocca/Consenti permette di bloccare o autorizzare l'accesso a Internet degli indirizzi MAC dei dispositivi elencati nella tabella Filtri indirizzi MAC. La tabella di seguito descrive la funzione del menu a discesa Blocca/Consenti. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Nome campo	Descrizione
Filtro MAC	**Impedire l'accesso a Internet ai dispositivi elencati di seguito (impostazione predefinita)** Selezionare **Impedire l'accesso a Internet ai dispositivi elencati di seguito** per negare l'accesso a Internet agli indirizzi MAC dei dispositivi elencati nella tabella. A tutti gli altri indirizzi MAC verrà consentito l'accesso a Internet.
	Consentire l'accesso a Internet ai dispositivi elencati di seguito Selezionare **Consentire l'accesso a Internet ai dispositivi elencati di seguito** per consentire l'accesso a Internet solo agli indirizzi MAC dei dispositivi elencati nella tabella. A tutti gli indirizzi MAC *non* elencati nella tabella verrà negato l'accesso a Internet.

Tasti funzione

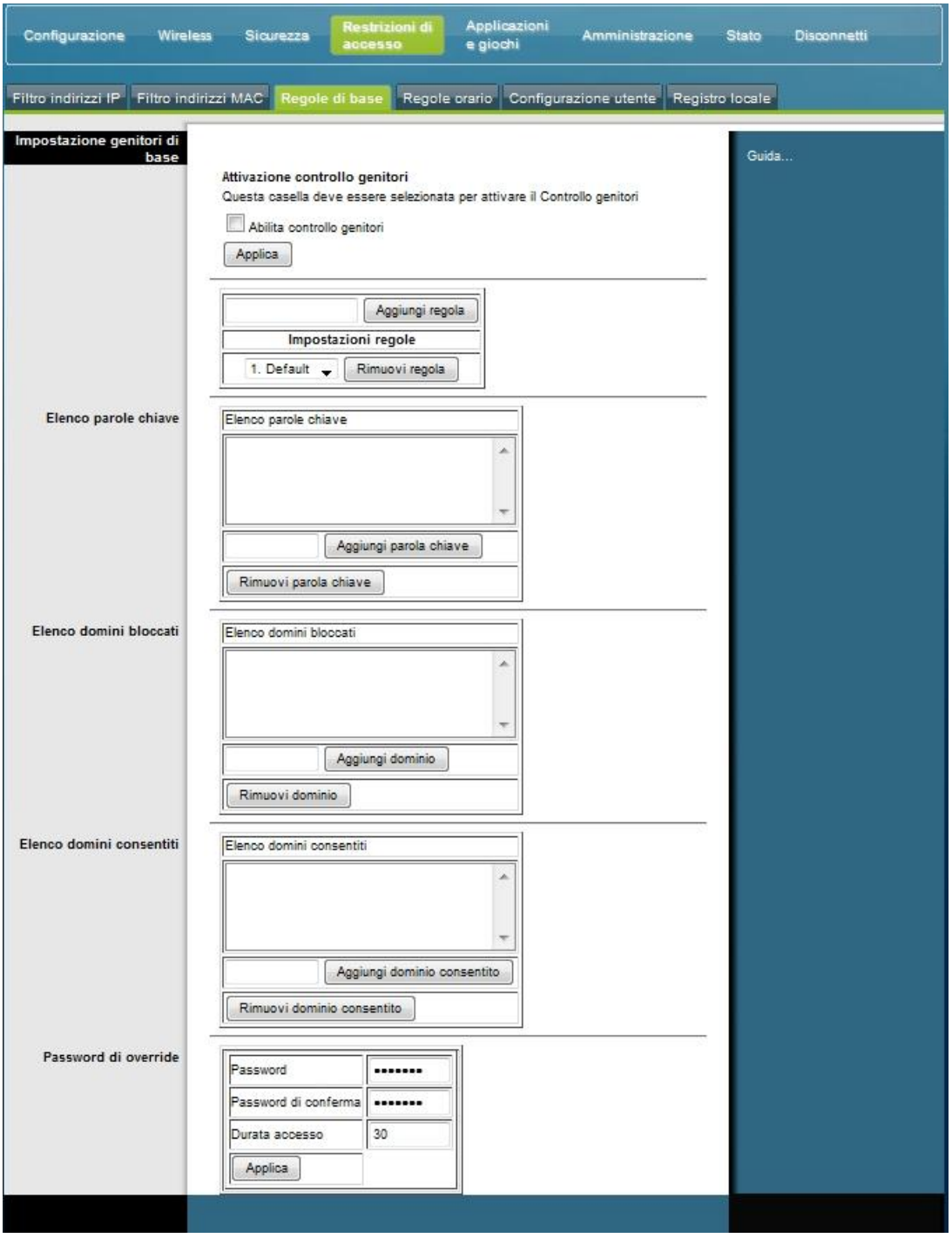
I seguenti tasti funzione compaiono nella pagina Impostazioni avanzate - Filtro indirizzi MAC .

Chiave	Descrizione
Applica	Salva i valori inseriti nei campi senza chiusura di pagina
Aggiungi indirizzo MAC	Consente di salvare l'indirizzo MAC immesso nel campo di testo associato.
Rimuovi indirizzo MAC	Consente di rimuovere l'indirizzo MAC selezionato.
Cancella tutto	Consente di rimuovere tutti gli indirizzi MAC definiti.

Scheda Restrizioni di accesso > Regole di base

Le restrizioni all'accesso consentono di impedire o autorizzare tipi specifici di utilizzo e traffico Internet, tra cui: accesso a Internet, applicazioni designate, siti Web e traffico in entrata secondo giorni e orari stabiliti. La pagina delle regole di base per le restrizioni di accesso permette di configurare il controllo genitori sul gateway residenziale e di monitorare gli individui autorizzati a impostare il controllo genitori.

Selezionare il tasto **Regole di base** per aprire la pagina regole di base per le restrizioni di accesso.



Usare le descrizioni e le istruzioni della tabella seguente per configurare le regole di base per le restrizioni di accesso relative al gateway residenziale. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Impostazione genitori di base	**Abilita controllo genitori** Permette di abilitare o disabilitare il controllo genitori. Per abilitare il controllo genitori, selezionare la casella **Abilita Controllo genitori** e fare clic su **Appica**. Per disabilitare il controllo genitori, deselezionare la casella **Abilita controllo genitori** e fare clic su **Applica**. **Aggiungi regola** Consente di aggiungere e salvare una nuova regola nell'elenco Regola contenuto **Rimuovi regola** Permette di rimuovere la regola selezionata dall'elenco Regola contenuto
Elenco parole chiave	**Elenco parole chiave** Permette di creare l'elenco delle parole chiave. Il gateway impedisce i tentativi di accesso agli URL contenenti le parole chiave di questo elenco **Aggiungi/rimuovi parola chiave** Consente di aggiungere nuove parole chiave all'elenco o di rimuovere dall'elenco parole chiave selezionate
Elenco domini bloccati	**Elenco domini bloccati** Consente di creare la lista di domini a cui il gateway deve impedire l'accesso. Il gateway blocca i tentativi di accesso ai domini della lista **Aggiungi/rimuovi dominio** Consente di aggiungere nuove parole chiave all'elenco o di rimuovere dall'elenco i domini selezionati

Sezione	Descrizione campo
Elenco domini consentiti	**Elenco domini consentiti** Permette di creare un elenco di domini ai quali il gateway consente l'accesso **Aggiungi/rimuovi dominio consentito** Consente di aggiungere nuove parole chiave all'elenco o di rimuovere dall'elenco i domini selezionati
Password di override	**Password** Permette di creare la password per neutralizzare temporaneamente le restrizioni di accesso utente a un sito Internet bloccato **Conferma password** Riscrivere la stessa password per confermare la password di override nel campo precedente **Durata accesso** Permette di designare un periodo di tempo in minuti durante il quale la password di override consente l'accesso temporaneo a un sito Internet ristretto **Applica** Salva tutte le aggiunte e le modifiche

Per usare il Blocco per parola chiave e Blocco per dominio

Il Blocco per parola chiave e il Blocco per dominio permettono di limitare l'accesso a siti Internet impedendo l'accesso ai siti sulla base di una parola o una stringa di testo contenuta negli URL di accesso a tali siti.

Il Blocco per dominio consente di limitare l'accesso ai siti Web sulla base del nome di dominio del sito. Il nome di dominio è la parte di URL che precede la tipica estensione .COM, .ORG o .GOV.

Il Blocco per parola chiave consente di impedire l'accesso a siti Internet sulla base di parole chiave o stringhe di testo presenti in qualsiasi punto di un URL, non solo nel nome dominio.

Nota: la funzione Blocco per dominio blocca l'accesso a qualsiasi dominio dell'Elenco domini. La funzione blocca anche i domini le cui parti contengono voci identiche nell'elenco.

Esempio: se si digita **example.com** come dominio, saranno bloccati i siti contenenti “example.com”. Di norma si tralascia “www.” nel Nome di dominio, poiché può limitare il blocco soltanto al sito che corrisponde esattamente a quel Nome di dominio. Esempio: se si digita www.example.com nella lista, verrà bloccato soltanto il sito "www.example.com". Tralasciando “www.”, verranno invece bloccati tutti i siti compresi in “example.com” e ad esso associati.

Blocca l'accesso ai siti web

Per bloccare l'accesso ai siti web, usare **Elenco domini bloccati** o **Elenco parole chiave**

Per usare **Elenco domini bloccati**, digitare gli URL o i nomi di dominio dei siti Web da bloccare.

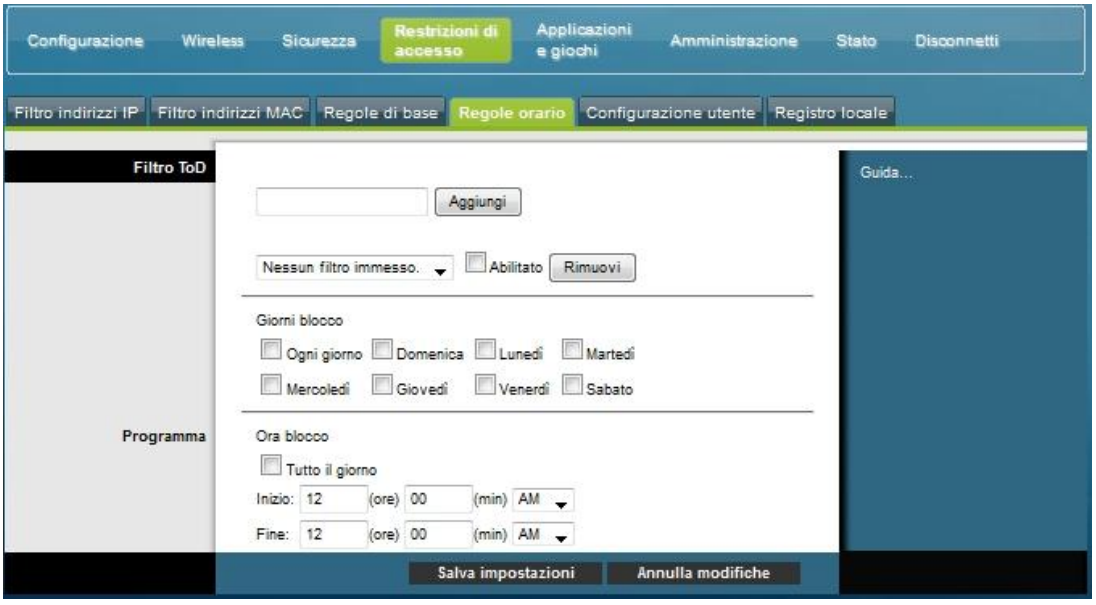
Usare **Elenco parole chiave** per inserire le parole chiave da bloccare. In questo modo verrà bloccato l'accesso ai siti Web il cui URL contiene una delle parole chiave. Tenere presente che viene controllato solo l'URL, non il contenuto di ciascuna pagina Web.

Scheda Restrizioni di accesso > Regole orario

Usare la pagina Restrizioni di accesso > Regole orario per configurare filtri di accesso ai siti Web che consentono di bloccare tutto il traffico Internet da e verso dispositivi di rete specifici impostando il giorno della settimana e l'orario giornaliero secondo le preferenze dell'utente.

Selezionare il tasto **Regole orario** per aprire la pagina Restrizioni di acesso > Regole orario. La seguente illustrazione è un esempio della pagina Restrizioni di acesso > Regole orario.

Nota: il gateway residenziale usa l'orario dell'orologio di rete gestito dal provider di servizi. Per utilizzare correttamente la funzione, l'ora deve essere precisa e rappresenta l'orario del giorno nel fuso orario di appartenenza. Verificare che le pagine di Stato e Imposta ora corrispondano con precisione all'ora del giorno. Altrimenti, contattare il provider di servizi. Si possono anche regolare le impostazioni per correggere la differenza.



Descrizione della pagina Restrizioni di accesso > Regole orario

Usare le descrizioni e le istruzioni della tabella seguente per configurare le regole orario per il gateway residenziale. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Filtro ToD	**Aggiungi ToD** Consente di aggiungere un nuovo filtro o regola di accesso per l'orario giornaliero. Inserire il nome del filtro e fare clic sul tasto **Aggiungi** per aggiungere il filtro all'elenco. Le regole dell'orario giornaliero servono per limitare l'accesso Internet in base al giorno e all'ora. **Rimuovi** Consente di rimuovere il filtro selezionato dall'elenco Filtro ToD (orario giornaliero)

Sezione	Descrizione campo
Programma	**Giorni blocco**
	Permette di controllare l'accesso in base ai giorni della settimana
	Ora blocco
	Consente di controllare l'accesso in base all'ora del giorno

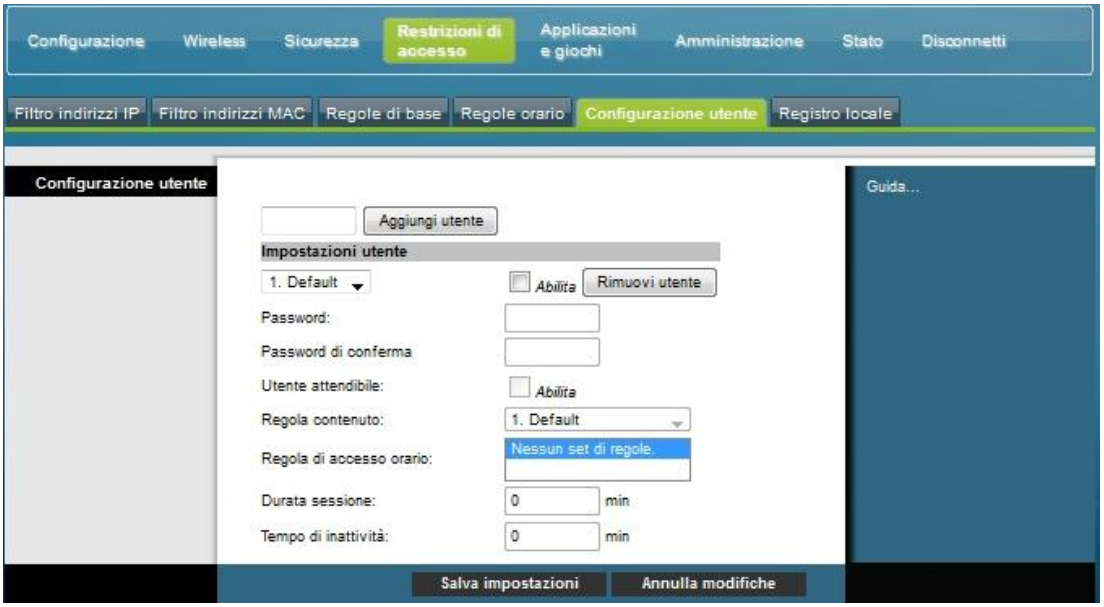
Scheda Restrizioni di accesso > Impostazione utente

Usare la pagina impostazioni utente restrizioni di accesso per impostare conti aggiuntivi e profili utente membri nuclei famigliari. A ciascun profilo si possono assegnare livelli personalizzati di accesso Internet secondo quanto definito dalle regole di accesso assegnate al profilo utente in questione.

Importante: i conti aggiuntivi non concedono l'accesso amministrativo al gateway.

Nota: alla definizione e abilitazione dei profili utente, ciascun utente deve firmare ogni volta che intende accedere a Internet. L'utente può firmare quando compare la schermata popup di invito alla firma sul Web browser di appartenenza. Per accedere a Internet l'utente deve digitare il suo nome utente e la sua password.

Selezionare il tasto **Configurazione utente** per aprire la pagina Restrizioni di accesso > Configurazione utente.



Descrizione della pagina Restrizioni di accesso > Configurazione utente

Usare le descrizioni e le istruzioni della tabella seguente per configurare la configurazione utente per il gateway residenziale. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Configura-zione utente	**Aggiungi utente** Permette di aggiungere un nuovo profilo utente. Inserire il nome del filtro e fare clic sul tasto **Aggiungi** per aggiungere l'utente all'elenco. **Impostazioni utente** Permette di editare il profilo utente mediante menu a discesa. Il menu a discesa consente di richiamare il profilo su cui intervenire. I nomi utenti e le password sono Maiuscolo/minuscolo. Controllare la casella **Abilita** per attivare il profilo utente. Se il profilo non è attivo, l'utente non ha accesso a Internet. Per rimuovere il profilo utente, usare il menu a discesa che consente di selezionare l'utente da rimuovere e fare clic sul pulsante **Rimuovi utente**. **Password** Inserire la password utente scelta in questo campo. Ciascun utente deve digitare il suo nome utente e password ogni volta che vuole entrare in Internet. I nomi utenti e le password sono Maiuscolo/minuscolo. **Nota:** il gateway residenziale consente a ciascun utente di accedere a Internet, fatta salva 'osservanza delle regole selezionate sulla pagina per l'utente in questione.

Sezione	Descrizione campo
	Ripetere la password Ripetere la stessa password per conferma della password nel campo precedente. **Utente attendibile** Spuntare la casella se l'utente selezionato è da designare come utente attendibile. Gli utenti attendibili non sono soggetti alle regole di accesso a Internet. **Regola contenuto** Selezionare la regola contenuto per profilo utente corrente. Le regole contenuto devono prima essere definite andando alla pagina configurazione regole. Si accede alla pagina configurazione regole facendo clic sul tasto regole di base su questa pagina. **Regola di accesso orario** Selezionare la regola di accesso orario per profilo utente corrente. Le regole accesso orario devono prima essere definite andando alla pagina regole ora del giorno. Si accede alla pagina regole ora del giorno facendo clic sul tasto "Regole orario" su questa pagina. **Durata sessione** 1440 minuti [impostazione predefinita a creazione di utente. Altrimenti è uguale a 0 (zero)]. Inserire il tempo in minuti di accesso concesso all'utente Internet a partire dal momento della firma con Nome utente e Password. **Nota:** impostare durata sessione a 0 (zero) per evitare timeout sessione. **Tempo di inattività** 60 minuti [impostazione predefinita a creazione di utente. Altrimenti è uguale a 0 (zero)]. Inserire il tempo di inattività accesso Internet durante la sessione utente, che denota che l'utente non è più online. All'intervento del timer di inattività la sessione utente viene chiusa automaticamente. Per tornare ad avere accesso a Internet, l'utente deve nuovamente immettere il nome utente e la password. **Nota:** impostare il valore tempo di inattività a 0 (zero) per evitare timeout sessione.

Scheda Restrizioni di accesso > Registro locale

Questa pagina consente di rintracciare, per ogni utente, i tentativi di accesso ai siti Internet soggetti a restrizioni. In questa pagina si possono anche visualizzare gli eventi registrati dalla funzione controllo genitori.

Selezionare il tasto **Registro locale** per aprire la pagina Restrizioni di accesso > Registro locale.

L'illustrazione di seguito è un esempio della pagina Restrizioni di accesso > Registro locale.

Sezione	Descrizione campo
Registro locale	**Ultima ricorrenza**
Controllo genitori: registro eventi	Visualizza l'ora del tentativo di accesso più recente ai siti Internet soggetti a restrizioni
	Azione
	Visualizza l'azione del sistema
	Destinazione
	Visualizza URL del sito soggetto a restrizioni
	Utente
	Visualizza l'utente che ha tentato di accedere a un sito soggetto a restrizioni
	Sorgente
	Visualizza l'indirizzo IP del PC in uso al momento del tentativo di accesso un sito Web soggetto a restrizioni

Configurazione applicazioni e giochi

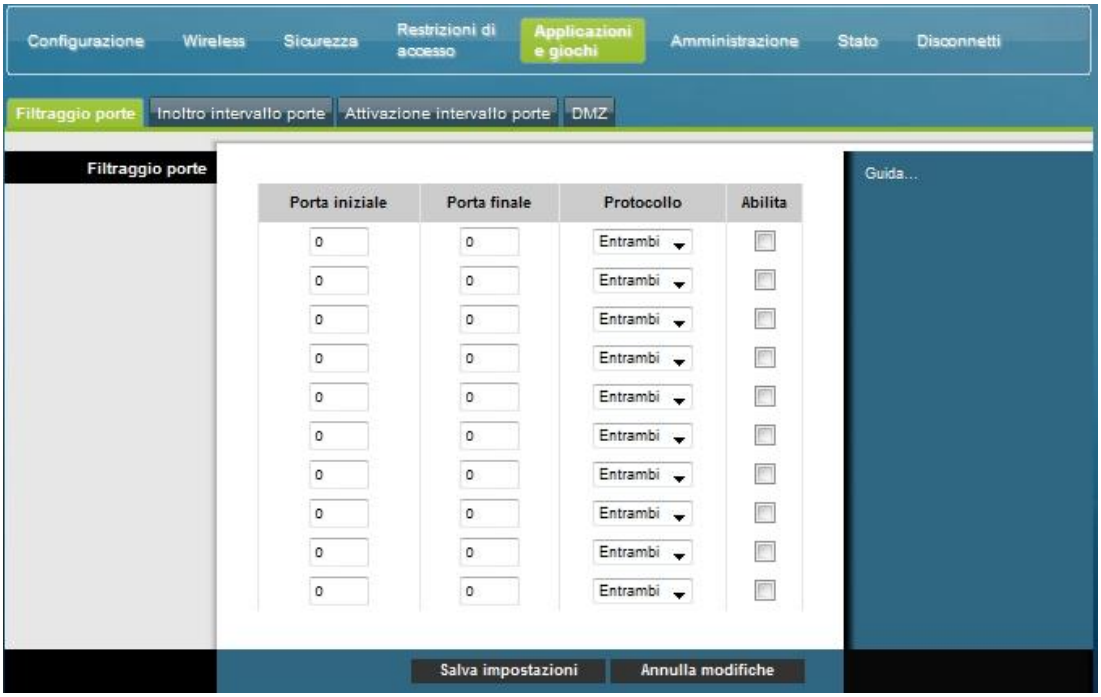
Panoramica

La maggior parte delle più note applicazioni Internet sono supportate dai protocolli ALG (Application Layer Gateway). I protocolli ALG regolano automaticamente il gateway del firewall per consentire il passaggio dati senza eseguire impostazioni personalizzate. Si consiglia di testare l'applicazione prima di apportare modifiche in questa sezione.

Applicazion e giochi > Filtro porte

Usare questa finestra per configurare i filtri delle porte TCP e UDP che consentono di impedire l'accesso a Internet a un intervallo di porte TCP/UDP. È possibile inoltre impedire ai computer di inviare traffico TCP/UDP in uscita alla rete WAN su numeri di porta IP specifici. Questo filtro non è specifico per indirizzo IP o indirizzo MAC. Il sistema blocca gli intervalli di porte specificati per tutti i computer.

Selezionare il tasto **Filtro porte** per aprire la pagina Applicazioni e giochi > Filtro porte.



Descrizione della pagina Applicazioni e giochi > Filtro porte

Usare le descrizioni e istruzioni della tabella per configurare il filtro porte per applicazioni e funzioni giochi in uso sul gateway residenziale. Selezionare la casella di controllo **Abilita** per attivare l'inoltro porte per l'applicazione desiderata. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Filtro porte	**Porta iniziale:** Rappresenta il valore iniziale dell'intervallo porte Inserire l'inizio dell'intervallo dei numeri di porta (porte esterne) utilizzati dal server o dall'applicazione Internet. Per eventuali ulteriori informazioni, consultare la documentazione del software dell'applicazione Internet.
	Porta finale: Rappresenta il valore finale dell'intervallo porte. Inserire la fine dell'intervallo dei numeri di porta (porte esterne) utilizzati dal server o dall'applicazione Internet. Per eventuali ulteriori informazioni, consultare la documentazione del software dell'applicazione Internet.
	Protocollo Selezionare uno dei seguenti protocolli: ■ TCP ■ UDP ■ Entrambi
	Abilita: Spuntare questa casella per abilitare il filtro sulle porte specificate.

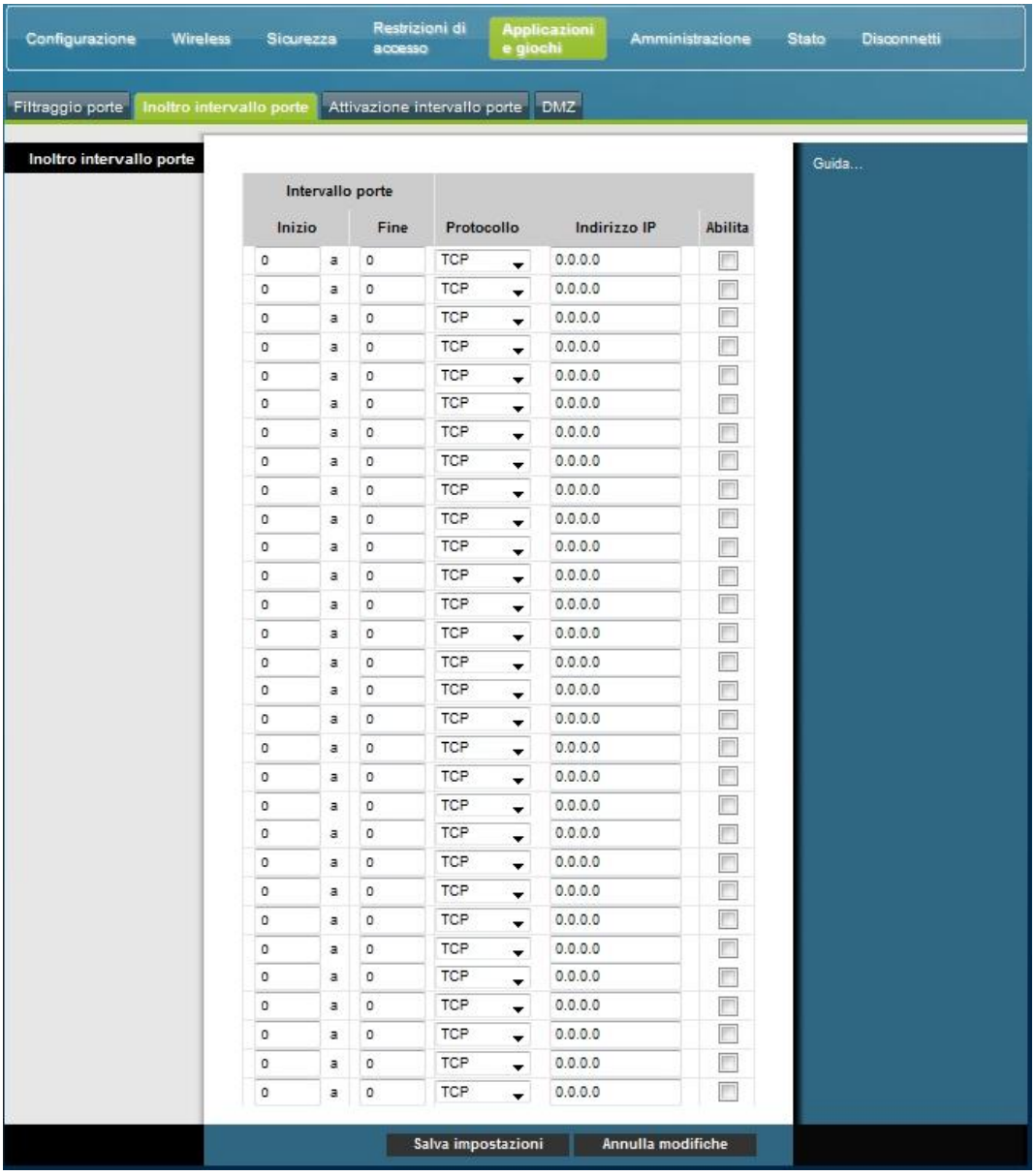
Applicazioni e giochi > Inoltro intervallo porte

Importante: di norma il gateway implementa una funzione nota come Traduzione di porta. La traduzione di porta monitora le porte usate dai PC o altri dispositivi del LAN. Questo monitoraggio garantisce un livello aggiuntivo di sicurezza oltre a quello di firewall. Per alcune applicazioni il gateway deve usare porte specifiche per il collegamento a Internet.

Usare Inoltro intervallo porte per inoltrare le porte da indirizzi Internet pubblici a indirizzi IP specifici della rete locale. Selezionare il tasto **Inoltro intervallo porte** per aprire la pagina invio intervallo porta Applicazioni e giochi.

Per la porta iniziale e finale selezionare una porta dall'intervallo raccomandato 49152 - 65535. Notare che le porte usate sono specifiche di programma, quindi occorre controllare quali devono essere inviate in base al programma. Digitare il numero di porta o l'intervallo in ambedue le caselle. Nella casella indirizzo IP digitare il nome dell'indirizzo IP del computer di competenza.

Nota: Inoltro intervallo porte espone continuamente le porte selezionate alla rete Internet pubblica. Quindi il firewall del gateway non è più attivo su queste porte. Il dispositivo con l'indirizzo IP di invio può essere esposto ad attacchi da parte degli hacker durante l'invio dell'intervallo di porta.



Descrizione della pagina Applicazioni e giochi > Inoltro intervallo porte

Usare le descrizioni e le istruzioni della tabella seguente per configurare l'intervallo porte relativo al gateway residenziale. Selezionare l'abilitazione per ogni porta. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Inoltro intervallo porte	**Inizio** Per la Porta iniziale, selezionare una porta dall'intervallo raccomandato 49152 - 65535. Notare che le porte usate sono specifiche di programma, quindi occorre controllare quali devono essere inviate in base al programma.
	Fine Per la Porta finale, selezionare una porta dall'intervallo raccomandato 49152 - 65535. Notare che le porte usate sono specifiche di programma, quindi occorre controllare quali devono essere inviate in base al programma.
	Protocollo Selezionare uno dei seguenti protocolli: ■ **TCP** ■ **UDP** ■ **Entrambi**
	Indirizzo IP Inserire l'indirizzo IP del computer di competenza.
	Abilita Spuntare questa casella per abilitare l'Inoltro porte per le porte e gli indirizzi IP specificati.

Applicazioni e giochi > Attivazione intervallo porte

L'attivazione intervallo porta effettua l'invio dinamico delle porte al PC di LAN che le richiede in un momento particolare. Il momento particolare è quando l'applicazione in esecuzione svolge un compito tale da attiva re il router. Il compito deve essere un accesso in uscita di un particolare intervallo porta.

Selezionare il tasto **Attivazione intervallo porte** per aprire la pagina Applicazioni e giochi > Attivazione intervallo porte

Descrizione della pagina Applicazioni e giochi > Attivazione intervallo porte

Usare le descrizioni e le istruzioni della tabella seguente per configurare l'attivazione intervallo porte relativo al gateway residenziale. Selezionare l'abilitazione per ogni porta. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Attivazione intervallo porte	
Intervallo di attivazione	**Porta iniziale** Per la porta iniziale selezionare una porta dall'intervallo raccomandato 49152 - 65535. Notare che le porte usate sono specifiche di programma, quindi occorre controllare quali devono essere inviate in base al programma.
	Porta finale Per la porta finale selezionare una porta dall'intervallo raccomandato 49152 - 65535. Notare che le porte usate sono specifiche di programma, quindi occorre controllare quali devono essere inviate in base al programma.

Sezione	Descrizione campo
Intervallo di inoltro	**Porta iniziale** Per la porta iniziale selezionare una porta dall'intervallo raccomandato 49152 - 65535. Notare che le porte usate sono specifiche di programma, quindi occorre controllare quali devono essere inviate in base al programma.
	Porta finale Per la porta finale selezionare una porta dall'intervallo raccomandato 49152 - 65535. Notare che le porte usate sono specifiche di programma, quindi occorre controllare quali devono essere inviate in base al programma.
	Protocollo Selezionare uno dei seguenti protocolli: ■ **TCP** ■ **UDP** ■ **Entrambi**
	Abilita Selezionare la casella di controllo Abilita per attivare l'attivazione intervallo porte per l'applicazione desiderata.

Applicazioni e giochi > DMZ

Usare questa pagina per configurare l'indirizzo IP con porte direttamente esposte alla rete Internet pubblica o alla WAN (Wide Area Network). Un hosting DMZ (Demilitarized Zone -zona demilitarizzata), anche noto come "host esposto", consente di specificare i riceventi di traffico WAN che il NAT (Network address Translation) non è in grado di trasferire a un PC locale noto.

Un DMZ serve tipicamente alle aziende per avere come host il loro server Internet. Il DMZ permette di inserire un indirizzo IP sulla piattaforma Internet del firewall del gateway, mentre gli altri indirizzi restano protetti dietro il firewall.

La funzione DMZ consente l'accesso diretto al traffico Internet di dispositivi quali server Web (HTTP), server FTP, server SMTP (e-mail) e server DNS (Domain Name System). Selezionare il tasto **DMZ** per aprire la pagina Applicazioni e giochi > DMZ.

Descrizione della pagina Applicazioni e giochi > DMZ

Usare le descrizioni e le istruzioni della tabella seguente per configurare l'attivazione intervallo porte relativo al gateway residenziale. Selezionare abilita per ciascun indirizzo IP host DMZ. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

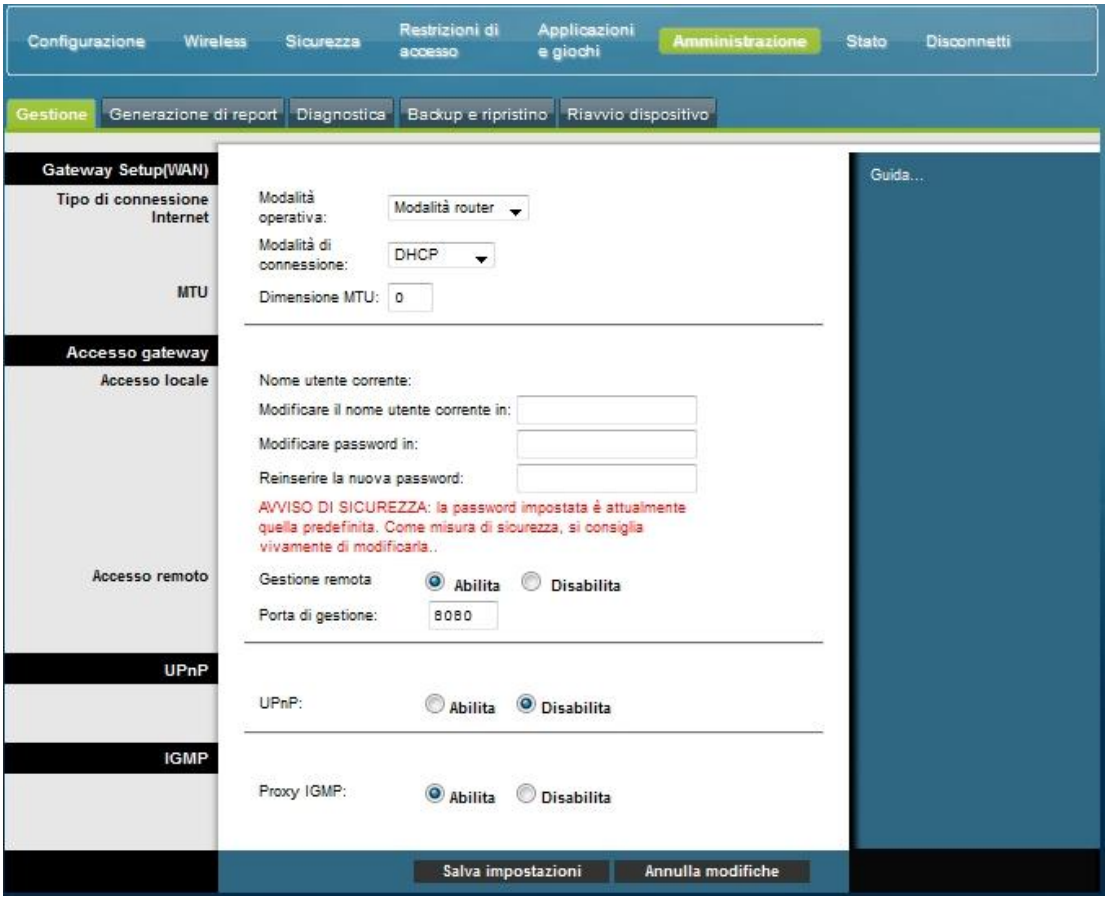
Sezione	Descrizione campo
DMZ	**Hosting DMZ** Selezionare l'opzione desiderata: ■ **Abilita** ■ **Disabilita (impostazione predefinita)**
	Indirizzo IP dell'host DMZ La funzione DMZ consente a un indirizzo IP di restare scoperto mentre gli altri rimangono protetti. Immettere l'indirizzo IP del computer che si desidera rendere visibile.

Gestione Gateway

Amministrazione > Gestione

La pagina Amministrazione > Gestione consente all'amministratore di rete di gestire funzioni specifiche di accesso e protezione. Selezionare il tasto **Gestione** per aprire la pagina Amministrazione > Gestione.

Importante: la pagina seguente viene visualizzata quando **DHCP** (impostazione predefinita) è in Modalità di connessione. La pagina visualizzata selezionando **IP statico** è illustrata e descritta più avanti in questa sezione.

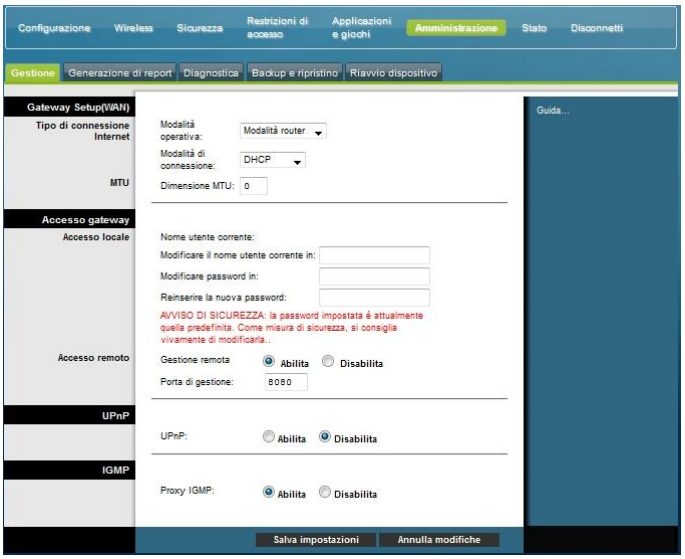
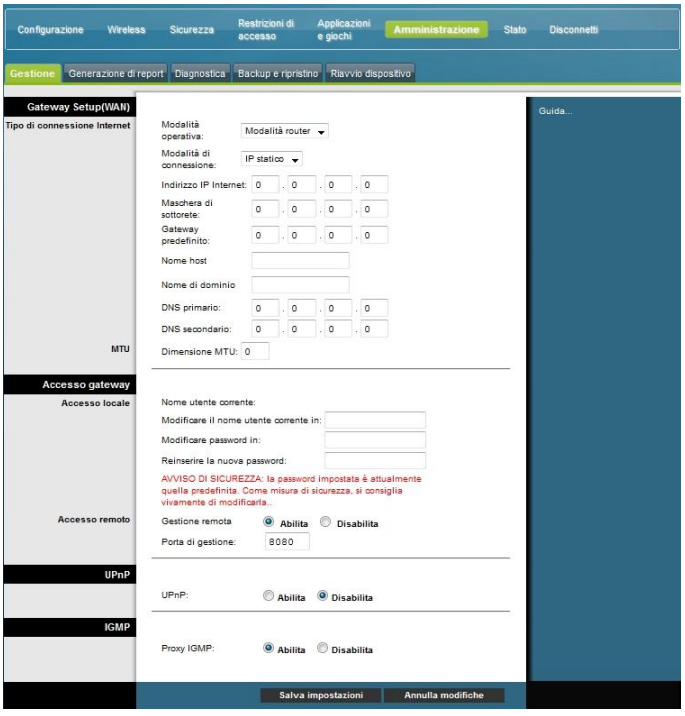


Descrizione pagina Amministrazione > Gestione

Usare le descrizioni e istruzioni della tabella per configurare la gesione dell'amministrazione del gateway residenziale quando si seleziona la modalità di connessione DHCP o IP statico. Dopo aver selezionato le opzioni desiderate, fare clic

su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Campo	Descrizione

Campo	Descrizione
Gateway Setup (WAN) **Tipo di connessione Internet**	**Modalità di connessione** Questa impostazione consente di determinare come il WAN (o interfaccia gateway verso Internet) ottiene l'indirizzo IP. **DHCP** (impostazione predefinita) Consente al gateway di ottenere automaticamente l'indirizzo IP pubblico  **IP statico** Permette di specificare l'indirizzo IP WAN e i corrispondenti dati di server come valori statici o fissi da usare con il gateway on-line 

Campo	Descrizione
	Indirizzo IP Internet
	Immettere l'indirizzo IP del gateway (come visualizzato su Internet)
	Maschera di sottorete
	Inserire la maschera di sottorete del gateway (come visualizzato su Internet, compreso il provider di servizi).
	Gateway predefinito
	Impostare il gateway predefinito del server del provider di servizi
	DNS primario
	Immettere l'indirizzo o gli indirizzi IP del DNS primario fornito dal provider di servizi. Questo dato è obbligatorio.
	DNS secondario
	Immettere l'indirizzo o gli indirizzi IP del DNS secondario fornito dal provider di servizi. Questo dato è facoltativo.
MTU	**Dimensione MTU**
	MTU è l'acronimo di Maximum Transmission Unit (unità massima di trasmissione) La dimensione della MTU specifica la dimensione massima del pacchetto che può essere trasmesso via Internet. . Valore predefinito = 0 (1500 byte)
Accesso gateway	
Accesso locale	**Nome utente corrente**
	Identifica l'utente attualmente collegato
	Modificare il nome utente corrente in
	Questo campo consente di modificare il proprio nome utente. Se si desidera modificare il proprio nome utente, immettere il nuovo nome

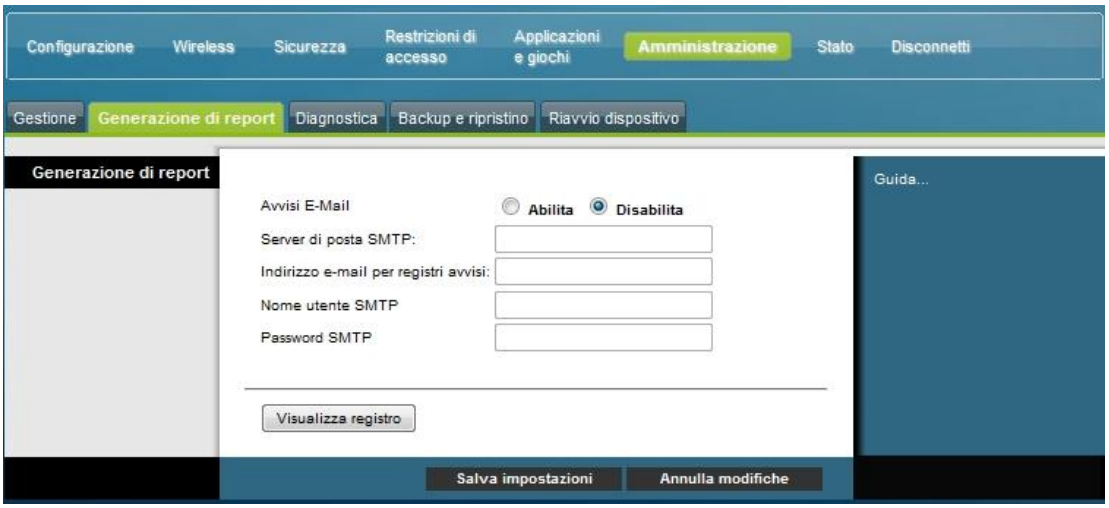
Campo	Descrizione
	utente in questo campo e fare clic su **Salva impostazioni** per applicare la modifica. **Nota:** il nome utente predefinito è un campo vuoto. **Modificare password in** Questo campo consente di modificare la propria password. Per modificare la propria password, immettere la nuova password in questo campo. Quindi, ripetere la nuova password nel campo **Reinserire la nuova password** e fare clic su **Salva impostazioni** per applicare la modifica. **Nota:** la password predefinita è un campo vuoto. **Reinserire la nuova password** Consente di ripetere l'immissione della nuova password. La password inserita in questo campo deve corrispondere a quella del campo precedente **Modifica password**. Dopo aver inserito nuovamente la nuova password, fare clic su **Salva impostazioni** per applicare la modifica.
Accesso remoto	**Gestione remota** Consente di abilitare e disabilitare la gestione remota. Questa funzionalità consente di accedere e gestire le proprie impostazioni del gateway da Internet quando ci si trova fuori casa. Per consentire l'accesso remoto, selezionare **Abilita**. Altrimenti, mantenere l'impostazione predefinita **Disabilta**. Per la gestione remota è richiesto il protocollo HTTP. Per l'accesso remoto al dispositivo, immettere l'indirizzo https://xxx.xxx.xxx.xxx:8080 (le x rappresentano l'indirizzo IP Internet del dispositivo, mentre 8080 rappresenta la porta specificata) nel campo **Indirizzo** del browser web. **Porta di gestione** Immettere il numero della porta che sarà aperta per l'accesso dall'esterno. L'impostazione predefinita è 8080. Questa porta deve essere utilizzata quando si stabilisce una connessione remota.
UPnP	**UPnP** Il servizio UPnP (Universal Plug and Play) consente a Windows XP e Vista di configurare il gateway per varie applicazioni Internet, ad esempio giochi on-line e videoconferenze. Per utilizzare UPnP, mantenere l'impostazione predefinita, **Abilita**. Altrimenti, selezionare **Disabilita**.

Campo	Descrizione
IGMP	**Proxy IGMP** Il protocollo IGMP (Internet Group Multicast Protocol) viene utilizzato per stabilire l'appartenenza a un gruppo multicast e viene generalmente utilizzato per le applicazioni di trasmissione multicast. Ad esempio, è possibile che sulla stessa rete locale sia disponibile il servizio di IPTV (Internet Protocol Television) con più caselle di configurazione, ognuna con diversi flussi stream simultanei; in tal caso è necessario utilizzare la funzione IGMP del router. Inoltro IGMP (proxy) è un sistema che migliora la trasmissione multicasting ai client su reti LAN. Se i client supportano questa opzione, mantenere l'impostazione predefinita, **Abilita**. Altrimenti, selezionare **Disabilita.**

Amministrazione > Generazione di report

La pagina Amministrazione > Generazione di report consente l'invio di e-mail relative alle diverse attività del sistema al proprio indirizzo e-mail.

Selezionare la scheda **Generazione di report** per aprire la pagina Amministrazione > Generazione di report



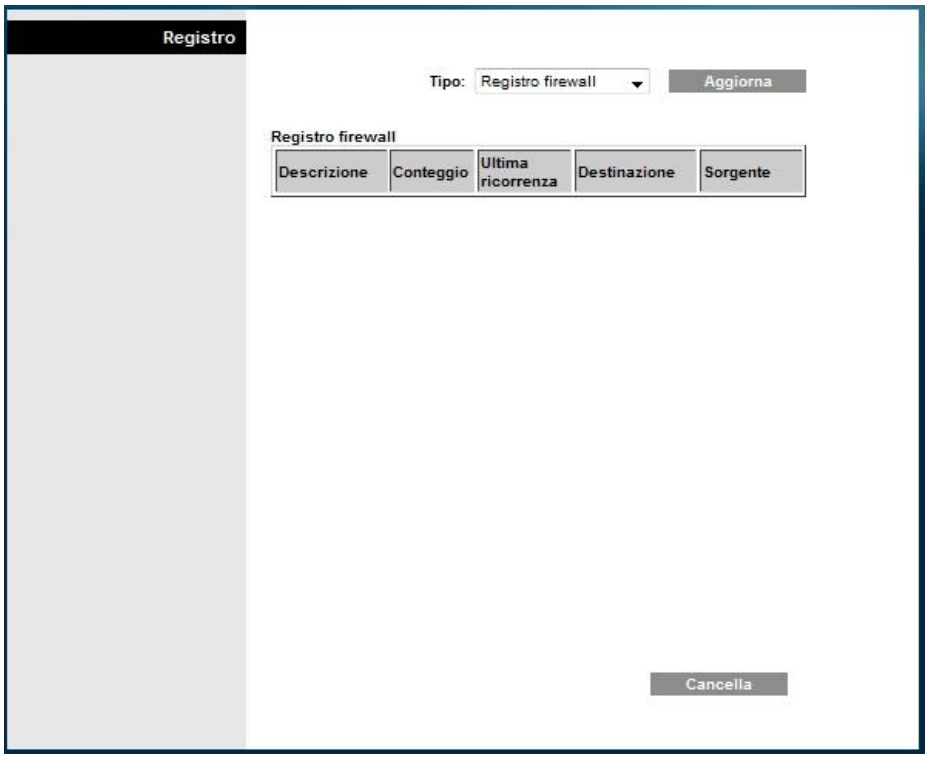
Utilizzare le descrizioni e seguire le istruzioni riportate nella tabella seguente per configurare la funzione di generazione di report sul gateway. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Generazione di report	**Avvisi E-Mail** Se questa opzione è attivata, viene inviato immediatamente un messaggio e-mail qualora venga rilevato un evento oggetto di interesse. Per utilizzare questa funzione, fornire le informazioni necessarie sull'indirizzo e-mail.
	Server di posta SMTP Immettere l'indirizzo (nome di dominio) o l'indirizzo IP del server SMTP (Simple Mail Transport Protocol) utilizzato per i messaggi e-
	Indirizzo e-mail per registri avvisi Immettere l'indirizzo e-mail che deve ricevere i registri.

Visualizza registro

Per visualizzare i registri, eseguire le seguenti operazioni.

1 Fare clic su **Visualizza registro**. Si apre una nuova finestra con la pagina dati del registro.



2 Per visualizzare un particolare registro, selezionare una delle opzioni presenti nel menu a tendina Tipo:

- Tutti
- Registro accessi
- Registro firewall
- Registro VPN

3 Dopo aver visualizzato i dati del registro, selezionare una delle seguenti opzioni:

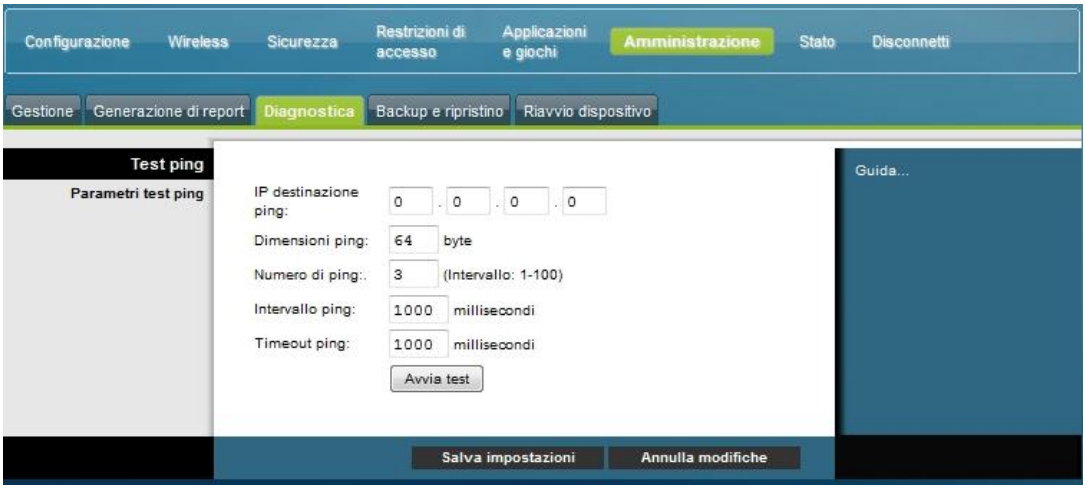
- Fare clic sul pulsante **Aggiorna pagina** per aggiornare il registro.
- Fare clic sul pulsante **Cancella** per cancellare tutte le informazioni contenute nel registro corrente.
- Fare clic sul pulsante **Pagina precedente** per tornare alle informazioni visualizzate precedentemente.

- Fare clic sul pulsante **Pagina successiva** per visualizzare la sezione successiva del registro, se disponibile.

Amministrazione > Diagnostica

Amministrazione > Diagnostica consente di verificare lo stato della propria connessione Internet utilizzando il test Ping.

Selezionare la scheda **Diagnostica** per aprire la pagina Amministrazione Diagnostica.



Utilizzare le descrizioni e seguire le istruzioni riportate nella tabella seguente per configurare la funzione di diagnostica sul gateway. Dopo aver selezionato le opzioni desiderate, fare clic su **Salva impostazioni** per confermare le variazioni oppure su **Annulla modifiche** per annullarle.

Sezione	Descrizione campo
Test ping	
Parametri test ping	**IP destinazione ping** Immettere l'indirizzo IP per il quale si desidera effettuare il ping. **Dimensioni ping** Immettere la dimensione del pacchetto da utilizzare.

Sezione	Descrizione campo
	Numero di ping Specificare quante volte si desidera effettuare il test ping sul dispositivo di destinazione. **Intervallo ping** Immettere l'intervallo di tempo (millisecondi) tra ogni test ping. **Timeout ping** Immettere l'intervallo di tempo desiderato (millisecondi) per il timeout. Se entro tale intervallo non si riceve alcuna risposta, il test ping viene considerato non riuscito.
	Avvia test Per avviare il test, eseguire le seguenti operazioni. **1** Fare clic su **Avvia Test** per avviare il test. Si apre una nuova pagina contenente un riassunto dei risultati del test. **2** Fare clic su **Salva impostazioni** per salvare i risultati del test o su **Annulla modifiche** per annullare il test.

Amministrazione > Backup e ripristino

Amministrazione > Backup e ripristino consente di effettuare una copia di sicurezza della configurazione del Gateway e di salvarla sul proprio computer. Questo file può essere utilizzato per ripristinare una configurazione precedentemente salvata per il proprio Gateway.

Selezionare la scheda **Backup e ripristino** per aprire la pagina Amministrazione Backup e Ripristino.

ATTENZIONE:

Il caricamento di un file di configurazione cancella (sovrascrive) tutte le impostazioni esistenti.

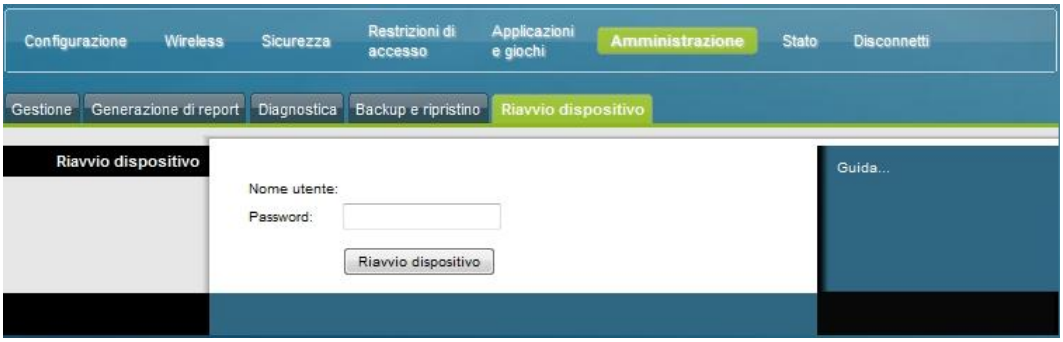
Sezione	Descrizione campo
Backup configurazione	Utilizzare la funzione Backup configurazione per effettuare una copia dell'attuale configurazione e salvare il file sul proprio computer. Fare clic sul pulsante **Backup** per avviare il download.
Ripristino configurazione	Utilizzare la funzione Ripristino configurazione per ripristinare un file di configurazione precedentemente salvato. Fare clic su **Browse** (Sfoglia) per selezionare il file di configurazione e, quindi, su **Ripristina** per caricare il file di configurazione sul dispositivo.

Amministrazione > Impostazioni predefinite

La pagina Impostazioni predefinite consente di ripristinare le impostazioni predefinite della configurazione del router. Selezionare la scheda **Impostazioni predefinite** per aprire la pagina Amministrazione > Impostazioni predefinite.

ATTENZIONE:

Ripristinando le impostazioni predefinite, il gateway perderà tutte le impostazioni precedentemente effettuate. Prima di ripristinare i valori predefiniti sul dispositivo, annotare tutte le impostazioni personalizzate. Dopo il ripristino dei valori predefiniti, è necessario immettere nuovamente tutte le impostazioni di configurazione.



Ripristina impostazioni predefinite

Per ripristinare le impostazioni predefinite, fare clic su **Ripristina impostazioni predefinite** per riportare tutte le impostazioni relative alla configurazione ai valori predefiniti. Il ripristino delle impostazioni predefinite provoca la perdita di quelle personalizzate.

Monitoraggio stato Gateway

Questa sezione descrive le opzioni contenute nella scheda Stato e utilizzabili per monitorare lo stato del gateway residenziale e per effettuare la diagnostica del dispositivo e della rete.

Stato > Gateway

La pagina Stato > Gateway visualizza informazioni sul gateway e sulle relative impostazioni correnti. Le informazioni visualizzate variano a seconda del tipo di connessione Internet utilizzata.

Selezionare la scheda **Gateway** per aprire la schermata Stato Gateway. Fare clic su **Aggiorna** per aggiornare i dati visualizzati sullo schermo.

Utilizzare le descrizioni riportate nella tabella seguente per visualizzare lo stato del proprio gateway e della connessione a Internet.

Sezione	Descrizione campo
Informazioni gateway	**Versione firmware** Numero della versione del firmware.

Sezione	Descrizione campo
	Indirizzo MAC Indirizzo alfanumerico univoco per l'interfaccia coassiale del modem via cavo, utilizzato per il collegamento al terminale del modem via cavo (CMTS) in corrispondenza della centralina di distribuzione. Un indirizzo MAC è un indirizzo hardware che identifica in modo univoco ciascun nodo della rete. **Ora attuale** Viene visualizzata l'ora in base al fuso orario selezionato nella schermata Configurazione di base.
Connessione Internet	**Indirizzo IP** Viene visualizzato l'indirizzo IP dell'interfaccia WAN. Questo indirizzo viene assegnato al gateway quando si collega on-line. **Maschera di sottorete** Viene visualizzata la maschera di sottorete della porta WAN dell'utente. Questo indirizzo viene assegnato in modo automatico alla porta WAN dell'utente dal proprio ISP, eccetto nel caso in cui sia stato impostato un indirizzo IP statico. **Gateway predefinito** Indirizzo IP del gateway predefinito da ISP. **DNS 1-3** Indirizzi IP DNS attualmente utilizzati dal gateway. **WINS** Indirizzo IP WINS attualmente utilizzato dal gateway.

Stato > Rete locale

La pagina Stato > Rete locale visualizza informazioni sullo stato della rete locale.

Selezionare la scheda **Rete locale** per aprire la pagina Stato Rete locale. Fare clic su **Aggiorna** per aggiornare i dati nella pagina.

Utilizzare la tabella seguente per visualizzare lo stato del proprio gateway e della connessione a Internet.

Sezione	Descrizione campo
Rete locale	**Indirizzo MAC** Indirizzo alfanumerico univoco assegnato alla rete domestica LAN privata. Un indirizzo MAC è un indirizzo hardware che identifica in modo univoco ciascun nodo della rete. **Indirizzo IP** Visualizza l'indirizzo IP della subnet LAN. **Maschera di sottorete** Visualizza la maschera di sottorete della LAN dell'utente. **Server DHCP** Visualizza lo stato del server DHCP locale (Abilitato o Disabilitato) **Indirizzo IP iniziale** Viene visualizzato il valore iniziale dell'intervallo di indirizzi IP utilizzato dal server DHCP sul gateway. **Indirizzo IP finale** Viene indicato il valore finale dell'intervallo di indirizzi IP utilizzato dal server DHCP.
Tabella client DHCP	Fare clic su **Tabella client DHCP** per visualizzare i dispositivi collegati alla propria LAN ai quali sono stati assegnati gli indirizzi IP

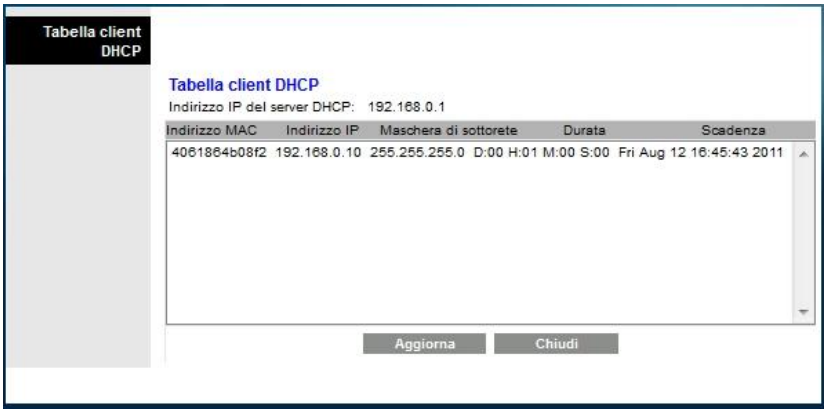
Sezione	Descrizione campo
	dal server DHCP sul gateway. Nella schermata Tabella client DHCP, viene visualizzato un elenco dei client DHCP (PC e altri dispositivi di rete) contenente le seguenti informazioni: nomi dei client, indirizzi IP, indirizzi MAC e l'intervallo temporale di assegnazione degli indirizzi IP. Per ottenere le informazioni più aggiornate, fare clic su **Aggiorna**.Per uscire da questa schermata e tornare alla schermata **Rete locale**, quindi, fare clic su **Chiudi.** L'illustrazione che segue mostra un esempio di Tabella client DHCP. 

Tabella ARP o RARP	Fare clic su **Tabella ARP/RARP** per visualizzare l'elenco completo di tutti i dispositivi collegati alla propria rete. Per ottenere le informazioni più aggiornate, fare clic su **Aggiorna**. Per uscire da questa schermata e tornare alla schermata **Rete locale**, quindi, fare clic su **Chiudi.** L'illustrazione che segue mostra un esempio di Tabella ARP/RARP. 

Stato > Wireless

La pagina Stato > Rete wireless visualizza le informazioni di base sullo stato della rete wireless del gateway.

Selezionare la scheda **Wireless** per aprire la pagina Stato Wireless. Fare clic su **Aggiorna** per aggiornare i dati nella pagina.

Descrizione della pagina Stato Wireless

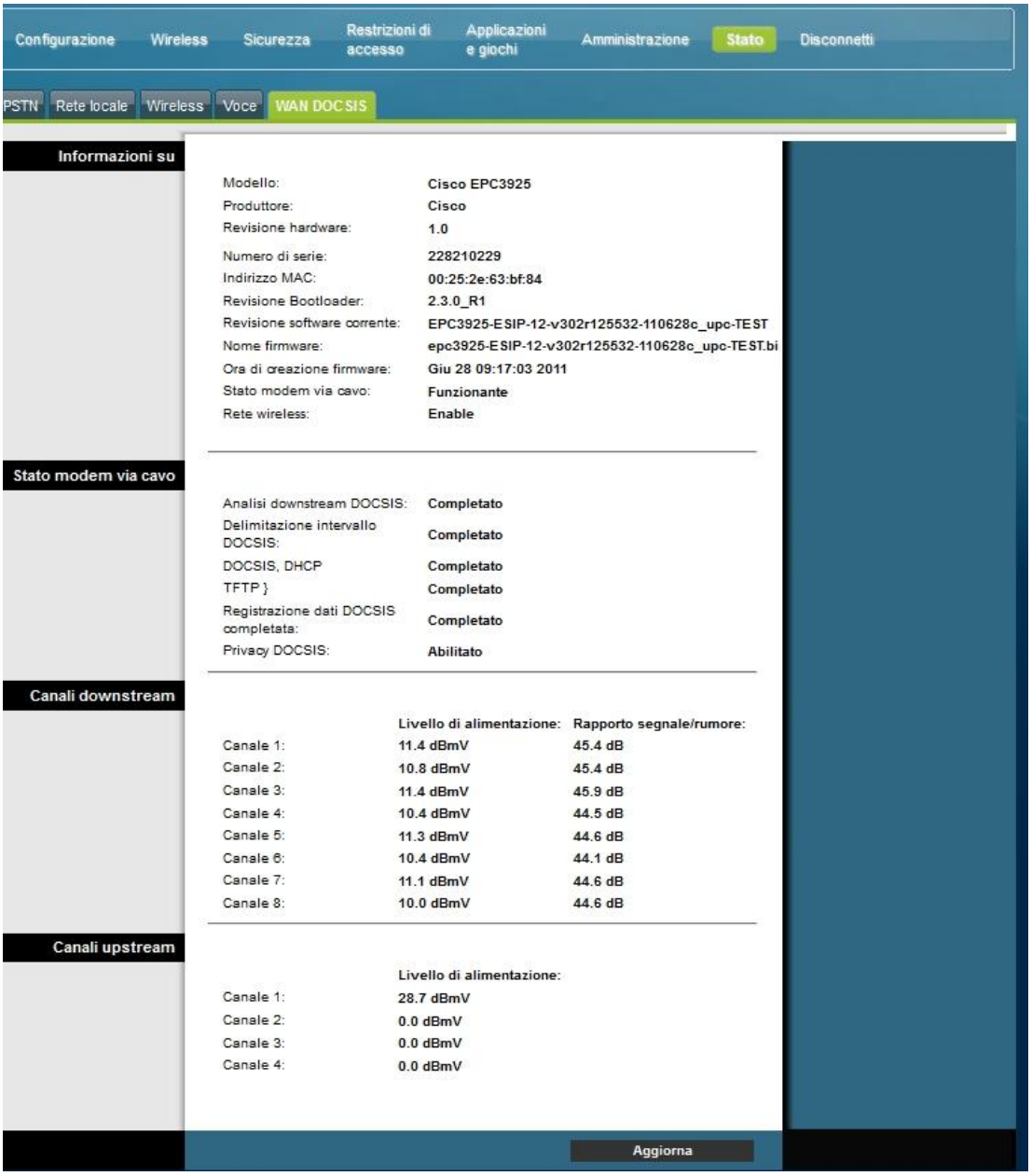
Utilizzare la tabella seguente per visualizzare lo stato della propria rete wireless.

Sezione	Descrizione campo
Rete wireless	**Indirizzo MAC** Visualizza l'indirizzo MAC del punto di accesso wireless locale al gateway **Banda radio** Visualizza una delle seguenti bande di frequenza radio attualmente in uso: ■ **2,4 GHz** ■ **5 GHz** ■ **2,4 e 5 GHz** **Nota:** non tutti i prodotti supportano la banda radio a 5 GHz. **Nome di rete (SSID)** Visualizza il nome o l'identificativo del servizio (SSID) del punto di accesso alla rete wireless **Ampiezza canale** Visualizza la larghezza di banda del canale impostata, selezionata sulla pagina Impostazioni wireless di base **Canale ampio** Visualizza l'impostazione Canale ampio selezionata sulla pagina Impostazioni wireless di base **Canale standard** Visualizza l'impostazione Canale standard selezionata sulla pagina Impostazioni wireless di base **Sicurezza** Viene visualizzato il metodo di protezione utilizzato dalla rete wireless **Broadcast SSID** Visualizza lo stato della funzione Broadcast SSID del gateway

Stato > WAN DOCSIS

Stato DOCSIS WAN visualizza informazioni sul sistema del modem via cavo.

Selezionare la scheda **WAN DOCSIS** per aprire la pagina Stato WAN DOCSIS.



Descrizione della pagina WAN DOCSIS

Utilizzare le descrizioni riportate nella tabella seguente per visualizzare lo stato della propria rete WAN DOCSIS.

Sezione	Descrizione campo
informazioni su	**Modello** Visualizza il nome del gateway residenziale
	Produttore Visualizza il produttore del gateway residenziale
	Revisione hardware Visualizza la revisione del progetto della scheda del circuito
	Numero di serie Visualizza il numero di serie univoco del gateway residenziale
	Indirizzo MAC (Indirizzo CM MAC) Visualizza l'indirizzo MAC della porta CM. L'indirizzo CM MAC è un indirizzo alfanumerico univoco per l'interfaccia coassiale dl modem via cavo, utilizzato per il collegamento al CMTS in corrispondenza della centralina di distribuzione. Un indirizzo MAC è un indirizzo hardware che identifica in modo univoco ciascun nodo della rete.
	Revisione bootloader: Visualizza la versione del codice di revisione del bootloader
	Revisione software attuale Visualizza la versione della revisione del firmware
	Nome firmware Visualizza il nome del firmware
	Ora di creazione firmware Visualizza la data e ora di creazione del firmware
	Stato modem via cavo Visualizza i possibili stati correnti del gateway
Canali downstream	**Canali 1-8** Visualizza il livello di potenza e il rapporto segnale/rumore dei canali downstream attivi

Sezione	Descrizione campo
Canali upstream	**Canali 1-4** Visualizza il livello di potenza dei canali upstream attivi

Domande frequenti

D: Come posso configurare il protocollo TCP/IP?

R. Per configurare il protocollo TCP/IP è necessario disporre di una scheda di interfaccia di rete Ethernet (NIC) con protocollo di comunicazione TCP/IP installato sul proprio sistema. Il TCP/IP è un protocollo di comunicazione utilizzato per l'accesso a Internet. Questa sezione contiene le istruzioni per la configurazione del TCP/IP sui propri dispositivi Internet per il funzionamento con il gateway residenziale in ambiente Microsoft Windows o Macintosh.

Il protocollo TCP/IP in ambiente Microsoft Windows è diverso per ogni sistema operativo. Seguire le istruzioni contenute in questa sezione relative al proprio sistema operativo.

Configurazione TCP/IP sui sistemi con Windows 2000

1. Fare clic su **Start**, selezionare **Impostazioni** e successivamente **Rete e connessioni remote**.
2. Fare doppio clic sull'icona **Connessione alla rete locale** nella finestra.
3. Fare clic su **Proprietà** nella finestra Stato della connessione alla rete locale.
4. Fare clic su **Protocollo Internet (TCP/IP)** nella finestra Proprietà connessione alla rete locale e fare clic su **Proprietà**.
5. Selezionare sia **Ottieni automaticamente un indirizzo IP** e **Ottieni automaticamente indirizzo server DNS** nella finestra Proprietà di Protocollo Internet (TCP/IP) e quindi fare clic su **OK**.
6. Fare clic su **Sì** per riavviare il computer quando si apre la finestra Rete locale. Il computer si riavvia. Il protocollo TCP/IP è ora configurato sul PC e i dispositivi Ethernet sono pronti per l'uso.
7. Tentare di accedere a Internet. Se non risulta possibile accedere a Internet, rivolgersi al provider di servizi per ricevere assistenza.

Configurazione TCP/IP sui sistemi con Windows XP

1. Fare clic su **Start** e, in funzione della configurazione del menu Start, selezionare una delle seguenti opzioni:
   - Se si sceglie di utilizzare il Menu di avvio predefinito di Windows XP, selezionare **Collegamento a**, selezionare **Mostra tutte le connessioni** e passare alla fase 2.

- Se si sceglie di utilizzare il Menu di avvio classico di Windows XP, selezionare **Impostazioni**, selezionare **Connessioni di rete**, fare clic su **Connessione alla rete locale** e passare alla fase 3.

2. Fare doppio clic sull'icona **Connessione alla rete locale** nella sezione LAN o Internet ad alta velocità della finestra Connessioni di rete.
3. Fare clic su **Proprietà** nella finestra Stato della connessione alla rete locale.
4. Fare clic su **Protocollo Internet (TCP/IP)** e poi su **Proprietà** nella finestra Proprietà connessione alla rete locale.
5. Selezionare sia **Ottieni automaticamente un indirizzo IP** e **Ottieni automaticamente indirizzo server DNS** nella finestra Proprietà di Protocollo Internet (TCP/IP) e quindi fare clic su **OK**.
6. Fare clic su **Sì** per riavviare il computer quando si apre la finestra Rete locale. Il computer si riavvia. Il protocollo TCP/IP è ora configurato sul PC e i dispositivi Ethernet sono pronti per l'uso.
7. Tentare di accedere a Internet. Se non risulta possibile accedere a Internet, rivolgersi al provider di servizi per ricevere assistenza.

Configurazione TCP/IP sui sistemi Macintosh

1. Fare clic sull'icona **Apple** nell'angolo superiore del Finder. Scorrere fino a **Pannelli di controllo** e fare clic su **TCP/IP**.
2. Fare clic su **Modifica** sul Finder nella parte superiore della pagina. Scorrere il menu verso il basso e fare clic su **Modalità utente**.
3. Fare clic su **Avanzata** nella finestra Modalità utente e quindi su **OK**.
4. Fare clic sulle frecce Su/Giù situate a destra della sezione Connetti tramite della finestra TCP/IP e quindi fare clic su **Utilizza server DHCP**.
5. Fare clic su **Opzioni** nella finestra TCP/IP e quindi su **Attiva** nella finestra Opzioni TCP/IP.

   Nota: Verificare che **l'opzione Carica solo quando necessario** *non sia selezionata*.
6. Verificare che l'opzione **Usa 802.3** situata nell'angolo superiore destro della finestra TCP/IP non sia selezionata. Nel caso in cui questa opzione sia selezionata, togliere il segno di spunta e fare clic su **Info** nell'angolo inferiore sinistro.
7. In questa finestra è presente un Indirizzo hardware?
   - Se **sì**, fare clic su **OK**. Per chiudere il Pannello di controllo TCP/IP, fare clic su **File** e quindi scorrere verso il basso per fare clic su **Chiudi**. La procedura è stata completata.

- Se **no**, è necessario spegnere il Macintosh.

8 Con il computer spento, mantenere premuti contemporaneamente i tasti **Comando (Apple)**, **Opzione**, **P** e **R** sulla tastiera. Tenendo premuti questi tasti, accendere il Macintosh senza rilasciare i tasti fino a quando il cicalino Apple non suona per almeno tre volte, dopodiché rilasciare i tasti e consentire al computer di riavviarsi.

9 Dopo che il computer si è completamente riavviato, ripetere le fasi da 1 a 7 per verificare che tutte le impostazioni TCP/IP siano corrette. Se il computer non dispone ancora di un indirizzo hardware, rivolgersi al rivenditore Apple o al centro di assistenza tecnica Apple per ricevere assistenza.

D: Come posso aggiornare l'indirizzo IP sul mio PC?

R. Se il PC non riesce ad accedere a Internet dopo che il gateway residenziale è collegato online, è possibile che il PC non abbia aggiornato il proprio indirizzo IP. Seguire le istruzioni contenute nella presente sezione relative al proprio sistema operativo per aggiornare l'indirizzo IP del PC.

Aggiornamento dell'indirizzo IP sui sistemi Windows 95, 98, 98SE e ME

1 Fare clic su **Start** e quindi su **Esegui** per aprire la finestra Esegui.

2 Digitare **winipcfg** nel campo Apri e fare clic su **OK** per eseguire il comando winipcfg. Si apre la finestra Configurazione IP.

3 Fare clic sulla freccia giù a destra del campo superiore e selezionare l'adattatore Ethernet installato sul PC. La finestra Configurazione IP visualizza le informazioni relative all'adattatore Ethernet.

4 Fare clic su **Rilascio** e quindi fare clic su **Aggiorna**. La finestra Configurazione IP visualizza un nuovo indirizzo IP.

5 Fare clic su **OK** per chiudere la finestra Configurazione IP: la procedura è stata completata.

Nota: se non risulta possibile accedere a Internet, rivolgersi al provider di servizi per ricevere assistenza.

Aggiornamento dell'indirizzo IP sui sistemi Windows NT, 2000 e XP

1 Fare clic su **Start** e quindi su **Esegui**. Si apre la finestra Esegui.

2 Digitare **cmd** nel campo Apri e fare clic su **OK**. Si apre una finestra contenente il prompt dei comandi.

3 Digitare **ipconfig/release** al prompt C:/ e premere **Invio**. Il sistema rilascia l'indirizzo IP.

4 Digitare **ipconfig/renew** al prompt C:/ prompt e premere **Invio**. Il sistema rilascia un nuovo indirizzo IP.

5 Fare clic sulla **X** nell'angolo superiore destro della finestra per chiudere la finestra Prompt dei comandi. La procedura è stata completata.

Nota: se non risulta possibile accedere a Internet, rivolgersi al provider per assistenza.

D: Cosa succede se non mi abbono alla TV via cavo?

R. Se nell'area è disponibile la TV via cavo, il servizio dati può essere reso disponibile sottoscrivendo o meno l'abbonamento alla TV via cavo. Rivolgersi al provider di servizi locale per avere informazioni sui servizi via cavo, incluso l'accesso a Internet ad alta velocità.

D: Cosa devo fare per l'installazione?

R. Rivolgersi al provider dei servizi per richiedere l'intervento di un installatore professionista. Un'installazione eseguita da un professionista garantisce il corretto collegamento del cavo al modem e al PC e la corretta configurazione di tutte le impostazioni hardware e software. Per ulteriori informazioni sull'installazione, rivolgersi al provider di servizi.

D: Come fa il gateway residenziale a collegarsi al mio computer?

R. Il gateway residenziale si collega al PC utilizzando una connessione wireless o la porta Ethernet 10/100/1000BASE-T del computer. Se si desidera utilizzare un'interfaccia Ethernet, le schede Ethernet sono disponibili presso il rivenditore locale di PC o prodotti per l'ufficio oppure presso il provider di servizi. Per ottimizzare le prestazioni con una connessione Ethernet, il PC dovrebbe essere dotato di una scheda Gigabit Ethernet.

D: Dopo che il mio gateway residenziale si è collegato, cosa devo fare per accedere a Internet?

R. Il provider di servizi locale diventa Internet Service Provider (ISP). Essi offrono un'ampia gamma di servizi tra cui e-mail, chat, news e servizi di informazione. Il provider di servizi fornirà tutto il software necessario.

D: Posso guardare la TV e navigare contemporaneamente su Internet?

R. Assolutamente sì! Sottoscrivendo un abbonamento al servizio di televisione via cavo, è possibile guardare la TV e utilizzare contemporaneamente il gateway residenziale collegando il televisore e il gateway residenziale alla rete mediante uno splitter di segnale via cavo opzionale.

Risoluzione dei problemi più comuni

Non capisco le funzioni degli indicatori di stato sul pannello anteriore

Vedere ***Funzioni degli indicatori di stato a LED del pannello anteriore*** (a pagina 130), per maggiori informazioni sul funzionamento e le funzioni degli indicatori di stato a LED del pannello anteriore.

Il gateway residenziale non rileva la connessione Ethernet

- Verificare che il computer sia dotato di una scheda Ethernet e che il driver software Ethernet sia correttamente installato. In caso di acquisto e installazione di una scheda Ethernet, seguire attentamente le istruzioni per l'installazione.
- Controllare lo stato degli indicatori luminosi di stato del pannello anteriore.

Il gateway residenziale non rileva alcuna connessione Ethernet dopo il collegamento a un hub

In caso di collegamento di più PC al gateway residenziale, occorre collegare prima il modem alla porta uplink dell'hub utilizzando il cavo incrociato corretto. Il LED LINK dell'hub rimane acceso.

Il gateway residenziale non rileva il collegamento via cavo

- Il modem funziona con un cavo coassiale RF standard da 75 ohm. Se viene utilizzato un cavo differente, il gateway residenziale non funzionerà correttamente. Rivolgersi al provider dei servizi via cavo per capire se si sta utilizzando il cavo giusto.
- La scheda NIC o l'interfaccia USB potrebbero essere difettose. Vedere le informazioni per la risoluzione dei problemi nella documentazione NIC o USB.

Suggerimenti per ottimizzare le prestazioni

Controllo e correggi

Se il gateway residenziale non funziona nel modo previsto, potrebbero essere utili i seguenti suggerimenti. Per maggiore assistenza, rivolgersi al provider di servizi.

- Verificare che la spina dell'alimentatore AC del gateway residenziale sia correttamente inserita nella presa di alimentazione.
- Verificare che il cavo di alimentazione AC del gateway residenziale non sia inserito in una presa elettrica controllata da un interruttore a parete. Nel caso in cui la presa elettrica sia controllata da un interruttore a parete, verificare che questo sia in posizione **ON**.
- Verificare che l'indicatore di stato a LED **ONLINE** sul pannello anteriore del gateway residenziale sia acceso.
- Verificare che il servizio via cavo sia attivo e che supporti il servizio bidirezionale.
- Verificare che tutti i cavi siano correttamente collegati e che siano del tipo giusto.
- Verificare che il TCP/IP sia correttamente installato e configurato nel caso in cui si utilizzi una connessione Ethernet.
- Verificare di aver contattato il provider di servizi fornendogli il numero di serie e l'indirizzo MAC del gateway residenziale.
- Nel caso in cui si stia utilizzando uno splitter di segnale via cavo per collegare il gateway residenziale ad altri servizi, rimuovere lo splitter e ricollegare i cavi in modo che il gateway residenziale sia collegato direttamente all'ingresso del cavo. Se il gateway residenziale funziona adesso nel modo coretto, è probabile che lo splitter di segnale via cavo sia difettoso e che debba essere sostituito.
- Per ottimizzare le prestazioni con una connessione Ethernet, il PC dovrebbe essere dotato di una scheda Gigabit Ethernet.

Funzioni degli indicatori di stato a LED del pannello anteriore

Avviamento iniziale, calibrazione e registrazione (con alimentazione c.a.)

La tabella seguente illustra le fasi e il corrispondente aspetto degli indicatori di stato a LED del pannello anteriore del gateway residenziale durante l'avviamento iniziale, la calibrazione e la registrazione in rete con l'alimentazione c.a. inserita. Utilizzare questa tabella per risolvere i problemi che dovessero eventualmente verificarsi durante i processi di avviamento iniziale, calibrazione e registrazione del gateway residenziale.

Nota: dopo che il gateway residenziale ha completato la fase 11 (Registrazione telefono completata), il modem passa immediatamente a Funzionamento normale. Vedere ***Funzionamento in condizioni normali (con alimentazione c.a.)*** (a pagina 108).

Indicatori di stato a LED del pannello anteriore durante le fasi di avviamento iniziale, calibrazione e registrazione							
		Parte 1, Registrazione dati ad alta velocità					
Fase:		**1**	**2**	**3**	**4**	**5**	**6**
Indicatore pannello anteriore		**Autotest**	**Analisi downstream**	**Blocco segnale downstream**	**Intervallo**	**Richiesta Indirizzo IP**	**Richiesta file provisioning di dati ad alta velocità**
1	ALIMENTAZIONE	On	On	On	On	On	On
2	DS	On	Lampeggiante	On	On	On	On
3	US	On	Off	Off	Lampeggiante	On	On
4	ONLINE	On	Off	Off	Off	Off	Lampeggiante
5	ETHERNET 1-4	On	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante
6	USB	On	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante
7	CONNESSIONE WIRELESS	Off	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante
8	CONFIGURAZIONE WIRELESS	Off	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante
9	TEL 1	On	Off	Off	Off	Off	Off
10	TEL 2	On	Off	Off	Off	Off	Off

Indicatori di stato a LED del pannello anteriore durante le fasi di avviamento iniziale, calibrazione e registrazione						
Parte 2, Registrazione telefono						
Fase		**7**	**8**	**9**	**10**	**11**
Indicatore pannello anteriore		**Registrazione dati di rete completata**	**Richiesta indirizzo IP telefono**	**Richiesta file provisioning telefono**	**Riavvio servizi vocali**	**Registrazione telefono completata**
1	ALIMENTAZIONE	On	On	On	On	On
2	DS	On	On	On	On	On
3	US	On	On	On	On	On
4	ONLINE	On	On	On	On	On
5	ETHERNET 1 - 4	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante
6	USB	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante
7	CONNESSIONE WIRELESS	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante	On o lampeggiante
8	CONFIGURAZIONE WIRELESS	Off	Off	Off	On o lampeggiante	On o lampeggiante
9	TEL 1	Off	Lampeggiante	Off	Lampeggiante	On
10	TEL 2	Off	Off	Lampeggiante	Lampeggiante	On

Funzionamento in condizioni normali (con alimentazione c.a.)

La tabella seguente illustra l'aspetto degli indicatori di stato a LED del pannello anteriore del gateway residenziale durante il funzionamento in condizioni normali quando l'alimentazione c.a. è inserita.

Indicatori di stato a LED del pannello anteriore in condizioni di normale funzionamento

Indicatore pannello anteriore		Funzionamento in condizioni normali
1	ALIMENTA-ZIONE	On
2	DS	On
3	US	On
4	ONLINE	On
5	ETHERNET 1 - 4	■ **On -** Quando un singolo dispositivo è collegato alla porta Ethernet e non vi è alcuna trasmissione di dati da o verso il modem ■ **Lampeggiante -** Quando è collegato un solo dispositivo Ethernet e vi è trasmissione di dati tra l'apparecchio presso l'abitazione dell'utente (CPE) e il gateway residenziale wireless ■ **Off -** Quando alle porte Ethernet non è collegato alcun dispositivo
6	USB	■ **On -** Quando un singolo dispositivo è collegato alla porta USB e non vi è alcuna trasmissione di dati da o verso il modem ■ **Lampeggiante -** Quando è collegato un solo dispositivo USB e vi è trasmissione di dati tra l'apparecchio presso l'abitazione dell'utente (CPE) e il gateway residenziale wireless ■ **Off -** Quando alle porte USB non è collegato alcun dispositivo
7	CONNESSIO-NE WIRELESS	■ **On -** Quando il punto di accesso wireless è abilitato e funzionante ■ **Lampeggiante** - Durante la trasmissione di dati tra il CPE e il gateway residenziale wireless ■ **Off -** Quando il punto di accesso wireless è disabilitato dall'utente
8	CONFIGURA-ZIONE WIRELESS	■ **Off -** Quando la configurazione wireless non è attiva ■ **Lampeggiante -** Quando la configurazione wireless è attiva e pronta ad accogliere nuovi clienti wireless sulla rete
9	TEL 1	■ **On -** Quando i servizi telefonici sono abilitati ■ **Lampeggiante -** Quando la linea 1 è in uso

10	TEL 2	■ **On -** Quando i servizi telefonici sono abilitati ■ **Lampeggiante -** Quando la linea 2 è in uso

Condizioni speciali

La tabella seguente illustra l'aspetto degli indicatori di stato a LED posti sul pannello anteriore del modem via cavo per indicare quando viene negato l'accesso alla rete.

Indicatori di stato a LED del pannello anteriore in condizioni speciali

Indicatore pannello anteriore		**Accesso alla rete negato**
1	ALIMENTA-ZIONE	Lampeggio lento 1 volta al secondo
2	DS	Lampeggio lento 1 volta al secondo
3	US	Lampeggio lento 1 volta al secondo
4	ONLINE	Lampeggio lento 1 volta al secondo
5	ETHERNET 1 - 4	Lampeggio lento 1 volta al secondo
6	USB	Lampeggio lento 1 volta al secondo
7	CONNESSIO-NE WIRELESS	Lampeggio lento 1 volta al secondo
8	CONFIGURA-ZIONE WIRELESS	Lampeggio lento 1 volta al secondo
9	TEL 1	Off
10	TEL 2	Off

Avvertenze

Marchi registrati

Cisco e il logo Cisco sono marchi o marchi registrati di Cisco e/o dei relativi affiliati negli Stati Uniti e in altri paesi. Un elenco dei marchi commerciali Cisco è reperibile all'indirizzo **www.cisco.com/go/trademarks**.
DOCSIS è un marchio registrato di Cable Television Laboratories, Inc.
EuroDOCSIS, EuroPacketCable e PacketCable sono marchi commerciali di Cable Television Laboratories, Inc.

I marchi commerciali di terze parti citati sono proprietà dei rispettivi titolari. L'uso del termine partner non implica una relazione di partnership tra Cisco ed eventuali altre aziende. (1009R)

Declinazione di responsabilità

Cisco Systems, Inc. non si assume alcuna responsabilità per errori od omissioni eventualmente presenti in questa guida. Si riserva inoltre il diritto di apportare modifiche alla presente guida in qualsiasi momento e senza preavviso.

Nota sul copyright della documentazione

Le informazioni contenute in questo documento sono soggette a modifiche senza preavviso. È vietata la riproduzione in qualsiasi forma di qualsiasi parte del presente documento senza l'espressa autorizzazione scritta di Cisco Systems, Inc.

Utilizzo di Software e Firmware

Il software descritto in questo documento è protetto dalla legge sul copyright e viene fornito al cliente nell'ambito di un accordo di licenza. L'utilizzo e la copia di questo software sono consentiti esclusivamente in accordo coi termini dell'accordo di licenza.

Il firmware contenuto in questo apparecchio è protetto dalla legge sul copyright. Detto firmware può essere utilizzato esclusivamente nell'apparecchio su cui è installato. Qualsiasi riproduzione o distribuzione di questo firmware, o di una qualsiasi parte di esso, senza la nostra espressa autorizzazione scritta, è vietata.

Per informazioni

Per ulteriori informazioni

Per qualsiasi problema tecnico, rivolgersi al servizio assistenza clienti di Cisco. Seguire le opzioni del menu per parlare con un tecnico del servizio assistenza.

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

+1 678 277-1120
+1 800 722-2009
www.cisco.com

Settembre 2011 Codice prodotto 4041326 Revisione A