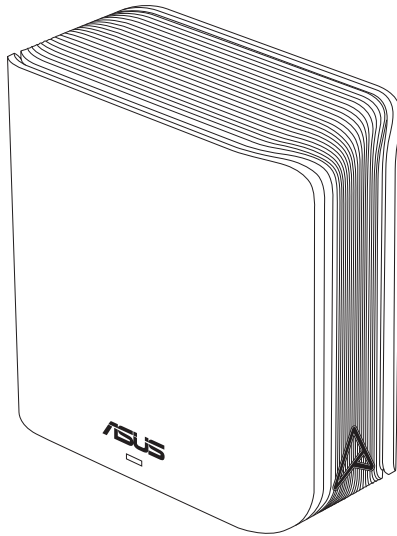


Manuale utente

ZenWiFi BD4

Router BE3600 Dual Band



I23951

Prima edizione

Agosto 2024

INFORMAZIONI SUL COPYRIGHT

Nessuna parte di questo manuale, compresi i prodotti e i software in esso descritti, può essere riprodotta, trasmessa, trascritta, archiviata in un sistema di recupero o tradotta in alcuna lingua, in alcuna forma e in alcun modo, fatta eccezione per la documentazione conservata dall'acquirente a scopi di backup, senza l'espressa autorizzazione scritta di ASUSTeK COMPUTER INC. ("ASUS").

ASUS FORNISCE QUESTO MANUALE "COSÌ COM'È" SENZA GARANZIA DI ALCUN TIPO, ESPLICITA O IMPLICITA, INCLUDENDO SENZA LIMITAZIONI LE GARANZIE O CONDIZIONI IMPLICITE DI COMMERCIALIZZABILITÀ O IDONEITÀ AD UN PARTICOLARE SCOPO. IN NESSUN CASO ASUS, I SUOI DIRIGENTI, FUNZIONARI, IMPIEGATI O DISTRIBUTORI SONO RESPONSABILI PER QUALSIASI DANNO INDIRETTO, PARTICOLARE, ACCIDENTALE O CONSEGUENTE (COMPRESI DANNI DERIVANTI DA PERDITA DI PROFITTO, PERDITA DI CONTRATTI, PERDITA D'USO O DI DATI, INTERRUZIONE DELL'ATTIVITÀ E SIMILI), ANCHE SE ASUS È STATA AVVISATA DELLA POSSIBILITÀ CHE TALI DANNI SI POSSANO VERIFICARE IN SEGUITO A QUALSIASI DIFETTO O ERRORE NEL PRESENTE MANUALE O NEL PRODOTTO.

I prodotti e nomi delle aziende che compaiono in questo manuale possono essere marchi registrati o diritti d'autore delle rispettive aziende, o meno, e sono usati a solo scopo identificativo o illustrativo, a beneficio dell'utente, senza alcuna intenzione di violazione dei diritti di alcun soggetto.

LE SPECIFICHE E LE INFORMAZIONI CONTENUTE IN QUESTO MANUALE SONO FORNITE A SOLO USO INFORMATIVO E SONO SOGGETTE A CAMBIAMENTI IN QUALSIASI MOMENTO, SENZA PREAVVISO, E NON POSSONO ESSERE INTERPRETATE COME UN IMPEGNO DA PARTE DI ASUS. ASUS NON SI ASSUME ALCUNA RESPONSABILITÀ E NON SI FA CARICO DI ALCUN ERRORE O INESATTEZZA CHE POSSA COMPARIRE IN QUESTO MANUALE COMPRESI I PRODOTTI E I SOFTWARE DESCRITTI AL SUO INTERNO.

Copyright © 2024 ASUSTeK Computer, Inc. Tutti i diritti riservati.

CONDIZIONI E LIMITI DI COPERTURA DELLA GARANZIA SUL PRODOTTO

Le condizioni di garanzia variano a seconda del tipo di prodotto e sono specificatamente indicate nel Certificato di Garanzia allegato a cui si fa espresso rinvio.

Inoltre la garanzia stessa non è valida in caso di danni o difetti dovuti ai seguenti fattori: (a) uso non idoneo, funzionamento o manutenzione impropri inclusi (senza limitazioni) e l'utilizzo del prodotto con una finalità diversa da quella conforme alle istruzioni fornite da ASUSTeK COMPUTER INC. in merito all'idoneità di utilizzo e alla manutenzione; (b) installazione o utilizzo del prodotto in modo non conforme agli standard tecnici o di sicurezza vigenti nell'Area Economica Europea e in Svizzera; (c) collegamento a rete di alimentazione con tensione non corretta; (d) utilizzo del prodotto con accessori di terzi, prodotti o dispositivi ausiliari o periferiche; (e) tentativo di riparazione effettuato da una qualunque terza parte diversa dai centri di assistenza ASUSTeK COMPUTER INC. autorizzati; (f) incidenti, fulmini, acqua, incendio o qualsiasi altra causa il cui controllo non dipenda da ASUSTeK COMPUTER INC.; (g) abuso, negligenza o uso commerciale.

La Garanzia non è valida per l'assistenza tecnica o il supporto per l'utilizzo del Prodotto in merito all'utilizzo dell'hardware o del software. L'assistenza e il supporto disponibili (se previsti) nonché le spese e gli altri termini relativi all'assistenza e al supporto (se previsti) verranno specificati nella documentazione destinata al cliente fornita a corredo del prodotto. È responsabilità dell'utente, prima ancora di richiedere l'assistenza, effettuare il backup dei contenuti presenti sul Prodotto, inclusi i dati archiviati o il software installato. ASUSTeK COMPUTER INC. non è in alcun modo responsabile per qualsiasi danno, perdita di programmi, dati o altre informazioni archiviate su qualsiasi supporto o parte del prodotto per il quale viene richiesta l'assistenza; ASUSTeK COMPUTER INC. non è in alcun modo responsabile delle conseguenze di tali danni o perdite, incluse quelle di attività, in caso di malfunzionamento di sistema, errori di programmi o perdite di dati. È responsabilità dell'utente, prima ancora di richiedere l'assistenza, eliminare eventuali funzioni, componenti, opzioni, modifiche e allegati non coperti dalla Garanzia prima di far pervenire il prodotto a un centro servizi ASUSTeK COMPUTER INC. ASUSTeK COMPUTER INC. non è in alcun modo responsabile di qualsiasi perdita o danno ai componenti sopra descritti. ASUSTeK COMPUTER INC. non è in alcun modo responsabile di eliminazioni, modifiche o alterazioni ai contenuti presenti sul Prodotto compresi eventuali dati o applicazioni prodotte durante le procedure di riparazione del Prodotto stesso. Il Prodotto verrà restituito all'utente con la configurazione originale di vendita, in base alle disponibilità di software a magazzino.

LIMITAZIONE DI RESPONSABILITÀ

Potrebbero verificarsi circostanze per le quali, a causa di difetti di componenti ASUS, o per altre ragioni, abbiate diritto a richiedere un risarcimento danni ad ASUS. In ciascuna di queste circostanze, a prescindere dai motivi per i quali si ha diritto al risarcimento danni, ASUS è responsabile per i danni alle persone (incluso il decesso), danni al patrimonio o alla proprietà privata; o qualsiasi altro danno reale e diretto risultante da omissione o mancata osservazione degli obblighi di legge previsti in questo Certificato di Garanzia, fino al prezzo contrattuale elencato per ogni prodotto e non oltre.

ASUS sarà solo responsabile o indennizzerà per perdite, danni o reclami su base contrattuale, extracontrattuale o di infrazione ai sensi del presente Certificato di Garanzia.

Questo limite si applica anche ai fornitori e rivenditori ASUS. Questo è il limite massimo per il quale ASUS, i suoi fornitori e il vostro rivenditore sono responsabili collettivamente.

IN NESSUN CASO ASUS È RESPONSABILE DI QUANTO SEGUE: (1) RICHIESTE DI TERZI PER DANNI DA VOI CAUSATI; (2) PERDITA O DANNEGGIAMENTO DEI VOSTRI DATI O DOCUMENTI O (3) QUALSIASI DANNO INDIRECTO, PARTICOLARE, ACCIDENTALE O CONSEGUENTE (COMPRESI DANNI DERIVANTI DA PERDITA DI PROFITTO, PERDITA DI CONTRATTI, PERDITA D'USO O DI DATI, INTERRUZIONE DELL' ATTIVITÀ E SIMILI) ANCHE SE ASUS, I SUOI DISTRIBUTORI E I VOSTRI RIVENDITORI SONO CONSAPEVOLI DELLA POSSIBILITÀ CHE TALI DANNI SI POSSANO VERIFICARE.

LICENZA SOFTWARE

I prodotti ASUS possono essere corredati da software, secondo la tipologia del prodotto. I software, abbinati ai prodotti, sono in versione "OEM": il software OEM viene concesso in licenza all'utente finale come parte integrante del prodotto; ciò significa che non può essere trasferito ad altri sistemi hardware e che, in caso di rottura, di furto o in ogni altra situazione che lo renda inutilizzabile anche la possibilità di utilizzare il prodotto OEM viene compromessa. Chiunque acquisti, unitamente al prodotto, un software OEM è tenuto ad osservare i termini e le condizioni del contratto di licenza, denominato "EULA" (End User Licence Agreement), tra il proprietario del software e l'utente finale e visualizzato a video durante l'installazione del software stesso. Si avvisa che l'accettazione da parte dell'utente delle condizioni dell'EULA ha luogo al momento dell'installazione del software stesso.

ASSISTENZA E SUPPORTO

Visitate il nostro sito all'indirizzo: <http://www.asus.com/it/support>

Indice

1	Conoscete il vostro router wireless	
1.1	Benvenuti!	7
1.2	Contenuto della confezione	7
1.3	Il vostro router wireless.....	8
1.4	Posizionamento del vostro router wireless	9
1.5	Requisiti per l'installazione.....	10
2	Per iniziare	
2.1	Configurazione del router	11
	A. Connessione cablata	12
	B. Connessione senza fili	13
2.2	Installazione rapida Internet (QIS) con auto-rilevamento...	15
2.3	Connessione alla vostra rete wireless	17
3	Configurare le impostazioni generali e avanzate	
3.1	Accedere all'interfaccia web	18
	3.1.1 Configurare le impostazioni di protezione della rete wireless	20
	3.1.2 Gestione dei client di rete	21
3.2	QoS adattativo.....	22
	3.2.1 Gestione della banda QoS	22
3.3	Amministrazione	25
	3.3.1 Modalità operativa.....	25
	3.3.2 Sistema.....	26
	3.3.3 Aggiornamento firmware	27
	3.3.4 Ripristina/Salva/Carica Impostazioni.....	27
3.4	AiProtection.....	28
	3.4.1 Protezione della rete	28
	3.4.2 Configurazione di Controllo Genitori.....	32

Indice

3.5	Firewall.....	35
3.5.1	Generale.....	35
3.5.2	Filtro URL.....	36
3.5.3	Filtro Parole Chiave	37
3.5.4	Packet Filter.....	38
3.6	IPv6.....	39
3.7	LAN.....	40
3.7.1	LAN IP	40
3.7.2	Server DHCP	41
3.7.3	Rotte.....	43
3.7.4	IPTV.....	44
3.8	Rete	45
3.8.1	Rete principale - Filtro MAC.....	45
3.8.2	Rete ospiti.....	47
3.8.2.1	Rete ospiti.....	47
3.8.2.2	Smart Home Master	49
3.9	Registro di sistema.....	53
3.10	Traffic Analyzer	54
3.11	WAN.....	55
3.11.1	Connessione ad Internet	55
3.11.2	WAN duale.....	58
3.11.3	Port Trigger.....	59
3.11.4	Virtual Server/Port Forwarding.....	61
3.11.5	DMZ.....	64
3.11.6	DDNS	65
3.11.7	NAT Passthrough.....	66
3.12	Wireless	67
3.12.1	WPS	67
3.12.2	Bridge	69

Indice

3.12.3	Impostazioni RADIUS.....	71
3.12.4	Professionale	72

4 Utility

4.1	Device Discovery	75
4.2	Firmware Restoration	75

5 Risoluzione dei problemi

5.1	Risoluzione dei problemi più comuni.....	77
5.2	Domande e risposte frequenti (FAQs)	80

Appendice

	Comunicazioni sulla sicurezza	98
	Servizio e supporto.....	100

1 Conoscete il vostro router wireless

1.1 Benvenuti!

Vi ringraziamo per aver acquistato il router senza fili ASUS ZenWiFi BD4.

Con un accento metallico nel colore del monogramma A sul chassis minimalista bianco, ZenWiFi BD4 è dotato di dual band da 2,4 GHz e 5 GHz per uno streaming HD wireless simultaneo senza pari; nei server Samba, UPnP AV e FTP per la condivisione di file 7 giorni su 7, 24 ore su 24. Il router inoltre è in grado di gestire fino a 300000 sessioni ed è stato progettato secondo la ASUS Green Network Technology per un risparmio di energia fino al 70%.

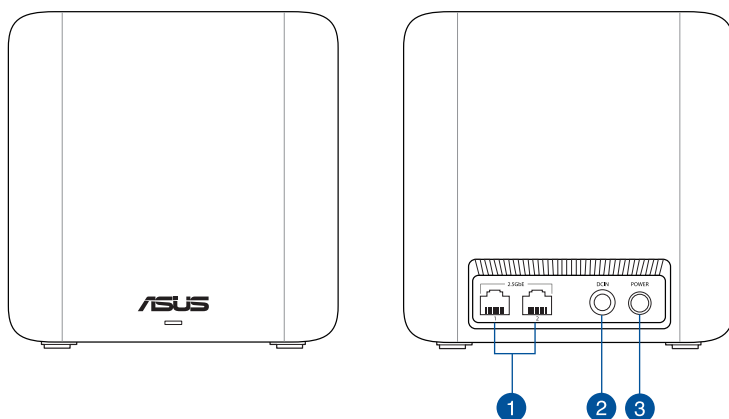
1.2 Contenuto della confezione

- Router wireless ZenWiFi BD4
- Cavo di rete Ethernet (RJ-45)
- Adattatore di alimentazione
- Guida rapida
- Certificato di garanzia

NOTE:

- Nel caso in cui uno di questi articoli sia danneggiato, o mancante, contattate ASUS per ottenere supporto. Fate riferimento alle *Servizio e Supporto* in fondo a questo manuale.
 - Conservate la confezione originale integra nel caso abbiate bisogno, in futuro, di servizi di garanzia come la riparazione o la sostituzione.
-

1.3 Il vostro router wireless



1 Porte 2.5GbE (Rilevamento automatico WAN/LAN)

Collegare un cavo di rete in queste porte per stabilire una connessione WAN/LAN da 2.5GbE.

2 Porta di alimentazione (DCIN)

Inserite l'alimentatore in dotazione in questo ingresso e collegate il router ad una sorgente di alimentazione.

3 Pulsante di accensione/spengimento

Premete questo pulsante per accendere o spegnere il sistema.

NOTE:

- Usate solamente l'adattatore di alimentazione che trovate nella confezione. L'utilizzo di altri adattatori potrebbe danneggiare il dispositivo.
- **Specifiche:**

Adattatore di alimentazione DC	Uscita alimentatore DC: +12V con corrente 1.5A		
Temperatura di esercizio	0~40°C	Archiviazione	0~70°C
Umidità di esercizio	50~90%	Archiviazione	20~90%

1.4 Posizionamento del vostro router wireless

Per ottenere una migliore trasmissione del segnale tra il router wireless e i dispositivi di rete connessi assicuratevi di:

- Posizionate il router wireless il più possibile al centro della vostra area per avere una copertura globale migliore.
- Tenete il router lontano da ostacoli di metallo e dalla luce solare diretta.
- Tenete lontano da dispositivi Wi-Fi (che supportino solo 802.11g o 20Mhz), periferiche per computer a 2.4Ghz, dispositivi Bluetooth, telefoni cordless, trasformatori, motori pesanti, luci fluorescenti, forni a microonde, frigoriferi o altre attrezzature industriali per prevenire interferenze sul segnale.
- Aggiornate sempre all'ultimo firmware disponibile. Scaricate l'ultimo firmware disponibile dal sito web ASUS: [**http://www.asus.com**](http://www.asus.com).

1.5 Requisiti per l'installazione

Per configurare la vostra rete wireless avete bisogno di un computer che abbia almeno le seguenti caratteristiche:

- Porta (LAN) Ethernet RJ-45 (10Base-T/100Base-TX/1000Base-TX)
- Connettività wireless IEEE 802.11a/b/g/n/ac/ax
- Protocollo TCP/IP installato sul sistema operativo
- Un browser Internet come Internet Explorer, Mozilla Firefox, Safari o Google Chrome

NOTE:

- Se il vostro computer non è dotato di connettività wireless potete installare un adattatore WLAN, compatibile con gli standard IEEE 802.11a/b/g/n/ac/ax, per connettervi alla rete wireless.
- Grazie alla tecnologia dual-band il vostro router wireless supporta simultaneamente i segnali wireless 2.4GHz e 5GHz. Questo permette, prima di tutto, di svolgere attività su Internet come navigazione o lettura/scrittura di email usando la banda a 2.4GHz e, allo stesso tempo, la trasmissione di file audio/video ad alta definizione (come filmati o musica) usando la banda a 5GHz.
- Alcuni dispositivi IEEE 802.11n che volete connettere alla rete potrebbero non essere compatibili con lo standard a 5GHz. Fate riferimento al manuale utente del dispositivo per le specifiche.
- Il cavo Ethernet RJ-45, usato per la connessione cablata, non deve essere lungo più di 100m.

IMPORTANTE!

- Alcuni adattatori Wi-Fi potrebbero avere problemi a connettersi agli access point Wi-Fi 802.11ax.
- Se incontrate questo problema assicuratevi di usare gli ultimi driver disponibili. Consultate il sito di supporto ufficiale del produttore per ottenere driver, aggiornamenti e ulteriori informazioni.
 - Realtek: <https://www.realtek.com/en/downloads>
 - Mediatek: <https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi>
 - Intel: <https://downloadcenter.intel.com/it/>

2 Per iniziare

2.1 Configurazione del router

IMPORTANTE!

- Per evitare possibili problemi di configurazione consigliamo di usare una connessione cablata durante la configurazione del router wireless.
 - Prima di configurare il vostro router wireless ASUS seguite questi semplici passaggi:
 - Se state sostituendo un router esistente scollegatelo dalla rete.
 - Scollegate i cavi che sono al momento collegati al modem. Se il modem ha una batteria supplementare rimuovete anche quella.
 - Riavviate il vostro modem e il computer (raccomandato).
-



AVVERTIMENTO!

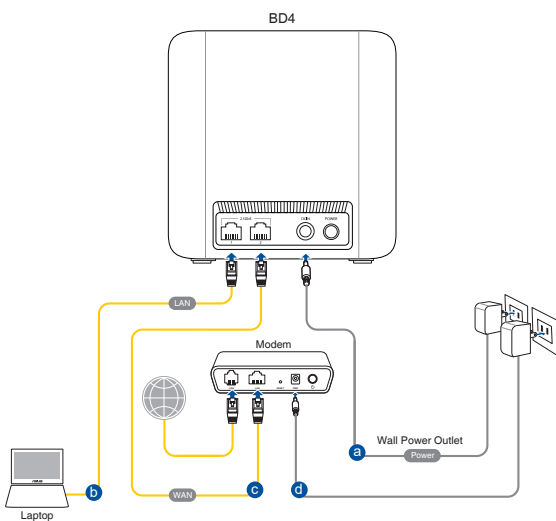
- Il cavo o i cavi di alimentazione devono essere inseriti a prese che sono dotate di un'adeguata messa a terra. Collegare l'apparecchio solo ad una presa vicina e facilmente accessibile.
 - Se l'adattatore è danneggiato non provare a ripararlo. Contattate un tecnico qualificato o il vostro rivenditore.
 - NON utilizzare cavi di alimentazione, accessori o periferiche danneggiate.
 - NON montate questo dispositivo ad un'altezza superiore a 2 metri.
 - Usa questo prodotto in ambienti la cui temperatura sia compresa tra 0°C (32°F) e 40°C (104°F).
-

A. Connessione cablata

NOTA: Potete usare un cavo dritto, o incrociato (crossover), per la connessione cablata del PC al router.

Per configurare il vostro router wireless tramite una connessione cablata:

1. Collegate il router ad una presa di corrente e accendetelo. Collegate un cavo di rete dal vostro computer ad una porta 2.5GbE del router.

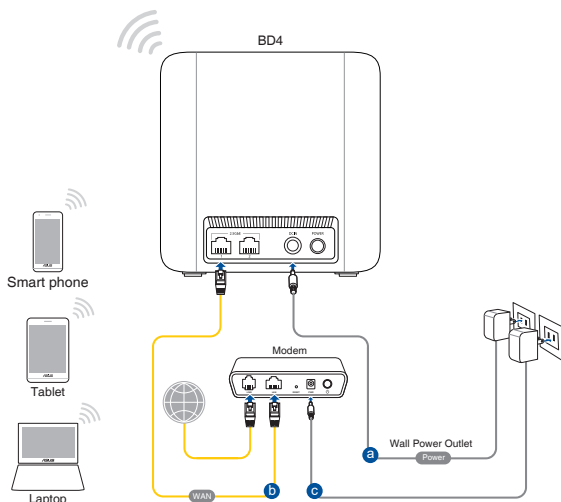


2. L'interfaccia web (GUI) si avvia automaticamente quando aprite un browser web. In caso contrario inserite <http://www.asusrouter.com> nella barra degli indirizzi.
3. Impostate una password per il vostro router per prevenire accessi non autorizzati.

B. Connessione senza fili

Per configurare il vostro router wireless tramite una connessione wireless:

1. Collegate il router ad una presa di corrente e accendetelo.



2. Stabilite la connessione alla rete senza fili con nome (SSID) che trovate sull'etichetta nella parte posteriore del router. Per una migliore sicurezza di rete modificate il SSID inserendo un nome unico e assegnate una password.

Nome rete Wi-Fi (SSID): ASUS_XX

* **XX** corrisponde alle ultime due cifre dell'indirizzo MAC 2.4GHz. Potete trovare l'indirizzo nell'etichetta sul retro del router.

3. Una volta eseguita la connessione l'interfaccia web (GUI) si avvia automaticamente quando aprite un browser web. In caso contrario inserite <http://www.asusrouter.com> nella barra degli indirizzi.

4. Impostate una password per il vostro router per prevenire accessi non autorizzati.
-

NOTE:

- Per maggiori informazioni sulla connessione ad una rete wireless fate riferimento al manuale fornito con il vostro adattatore WLAN.
 - Per sapere come configurare le impostazioni di sicurezza della vostra rete wireless fate riferimento alla sezione *3.1.1 Configurare le impostazioni di protezione della rete wireless* di questo manuale.
-

2.2 Installazione rapida Internet (QIS) con auto-rilevamento

L'installazione rapida Internet (QIS) vi aiuterà nella configurazione della vostra connessione a Internet.

NOTA: Prima di impostare la connessione ad Internet per la prima volta assicuratevi di aver premuto il pulsante di Reset per riportare il router wireless alle impostazioni predefinite di fabbrica.

Per usare l'auto-rilevamento dell'installazione rapida:

1. Avviate un browser web. Verrete reindirizzati ad ASUS Setup Wizard (Installazione rapida Internet o QIS). In caso contrario inserite <http://www.asusrouter.com> manualmente.
2. Il router è in grado di capire automaticamente se la connessione fornita dal vostro ISP è a **IP dinamico, PPPoE, PPTP** o **L2TP**. Inserite le informazioni necessarie per individuare il tipo di connessione fornita dal vostro ISP.

IMPORTANTE! Ottenete le informazioni necessarie sul tipo di connessione dal vostro ISP.

NOTE:



- Il rilevamento automatico dell'ISP viene attivato quando configurate il router wireless per la prima volta, o dopo aver resettato il router wireless alle impostazioni di fabbrica.
 - Se l'installazione rapida Internet (QIS) fallisse cliccate su **Manual setting (Impostazione manuale)** per configurare manualmente le impostazioni per la connessione ad Internet.
-
3. Impostate un nome della rete (SSID) e una chiave di sicurezza per le vostre reti wireless a WiFi 7 Network. Quando avete finito cliccate su **Apply (Applica)**.
 4. Nella pagina **Configurazione informazioni di accesso** cambiate la password di accesso per prevenire accessi non autorizzati al vostro router wireless.

NOTA: nome utente e la password del router wireless sono diversi dai SSID e dalle chiavi di sicurezza delle reti wireless WiFi 7. Il nome utente e la password del router wireless vi permettono di accedere all'interfaccia web del router per configurare le impostazioni del router. Il nome rete (SSID) delle reti WiFi 7 e le chiavi di sicurezza permettono ai dispositivi Wi-Fi di accedere e connettersi alle reti wireless WiFi 7.

2.3 Connessione alla vostra rete wireless

Dopo aver configurato correttamente il router wireless tramite l'Installazione rapida Internet (QIS) potete connettere il vostro computer, o altri dispositivi mobili, alla vostra rete wireless.

Per connettervi alla rete:

1. Sul vostro computer cliccate sull'icona di rete  nell'area di notifica per visualizzare le connessioni wireless disponibili.
2. Selezionate una rete wireless alla quale volete connettervi e cliccate su **Connect (Connetti)**.
3. Potrebbe essere richiesto l'inserimento di una chiave di sicurezza per connettersi ad una rete wireless protetta. Dopo averla inserita cliccate su **OK**.
4. Aspettate qualche secondo per permettere al computer di stabilire la connessione correttamente. A connessione avvenuta sarà visualizzato lo stato della connessione e l'icona di rete visualizzata sarà la seguente  per confermare la connessione.

NOTE:

- Fate riferimento ai capitoli successivi per maggiori dettagli su come configurare le diverse impostazioni della vostra rete wireless.
 - Fate riferimento al manuale utente del vostro dispositivo per sapere come connettervi correttamente alla vostra rete wireless.
-

3 Configurare le impostazioni generali e avanzate

3.1 Accedere all'interfaccia web

Il vostro router wireless ASUS dispone di un'interfaccia Web intuitiva, chiamata anche GUI (Graphical User Interface), che vi permette di configurare tutte le varie impostazioni disponibili tramite l'utilizzo di un browser Internet come, ad esempio, Internet Explorer, Mozilla Firefox, Safari o Google Chrome.

NOTA: Le caratteristiche possono variare in base alla versione del firmware installata sul router.

Per accedere all'interfaccia web GUI (Graphical User Interface):

1. Avviate il vostro browser e inserite, nella barra degli indirizzi, l'indirizzo standard del router: <http://www.asusrouter.com>.
2. Nella pagina di accesso inserite il nome utente e la password che avete impostato in *2.2 Installazione rapida Internet (QIS) con auto-rilevamento*.
3. Ora potete usare la GUI per configurare le varie impostazioni del vostro router wireless ASUS.

Pulsanti comandi veloci

The screenshot displays the ASUS ZenWiFi BD4 web interface. A red box highlights the top navigation bar containing 'Login' and 'Reboot' buttons. Another red box highlights the left sidebar menu, which includes 'Quick Internet Setup' (labeled as QIS), 'General', 'Network Map', 'AdMesh', 'Guest Network Pro', 'Parental Controls', 'QoS', 'Advanced Settings', 'Wireless', 'LAN', 'WAN', 'Amazon Alexa', 'IPv6', 'VPN', 'Firewall', 'Administration', 'System Log', and 'Network Tools'. A third red box highlights the top status bar showing 'Operation Mode: Mesh, Mesh, router' and 'Firmware Version: 3.0.0.64-102.5203'. The main content area shows 'Internet Status: Connected' with IP address '192.168.122.229' and DNS '8.8.8.8'. Below this is 'Security: WPA2/WPA3-Personal' and 'Clients: 1'. The 'System Status' panel on the right shows CPU usage for four cores (22%, 20%, 18%, 27%), RAM usage (60%), and Ethernet ports (2.5G, 1G, 3.0G). At the bottom, there is a footer with 'ASUS Support | Product Registration | Feedback | ESD' and '© 2024 ASUSTek Computer Inc. All rights reserved.'

QIS
(Installazione rapida Internet)

Pannello di navigazione

Barra delle informazioni

* L'immagine è solo di riferimento.

NOTA: Al primo accesso all'interfaccia web verrete indirizzati automaticamente all'installazione rapida Internet (QIS).

3.1.1 Configurare le impostazioni di protezione della rete wireless

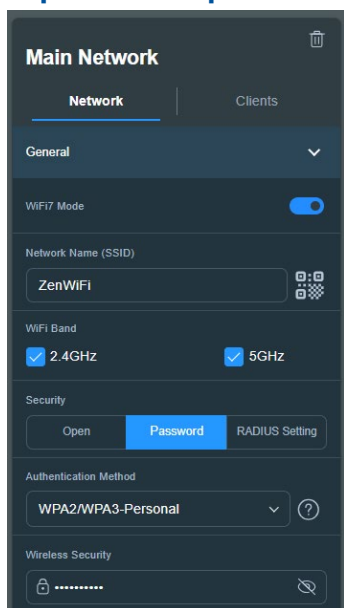
Per proteggere la vostra rete wireless dagli accessi non autorizzati dovete configurare le sue impostazioni di protezione.

Per configurare le impostazioni di protezione della rete wireless:

1. Dal pannello di navigazione andate su **General (Generale)** > **Network Map (Mappa di rete)**.
2. Selezionare la network e potete visualizzare le impostazioni di protezione come la visibilità del SSID, il livello di sicurezza e la cifratura.

NOTA: Avete la possibilità di configurare diverse impostazioni di sicurezza per le due diverse bande di frequenza 2.4GHz e 5GHz.

Impostazioni di protezione 2.4GHz/5GHz



3. Nel campo **Network Name (Nome della rete) (SSID)** inserite un nome unico da assegnare alla vostra rete wireless.
4. Dall'elenco **WEP Encryption (Cifratura WEP)** selezionate il metodo di cifratura che intendete usare per la vostra rete.

IMPORTANTE! Gli standard IEEE 802.11n/ac/ax impediscono l'uso di elevate velocità di trasferimento se utilizzate i metodi di cifratura WEP o WPA-TKIP. Se decidete di utilizzarli comunque la velocità della vostra rete sarà limitata allo standard IEEE 802.11g a 54 Mbps.

5. Inserite la vostra password di sicurezza.
6. Quando avete finito cliccate su **Apply (Applica)**.

3.1.2 Gestione dei client di rete



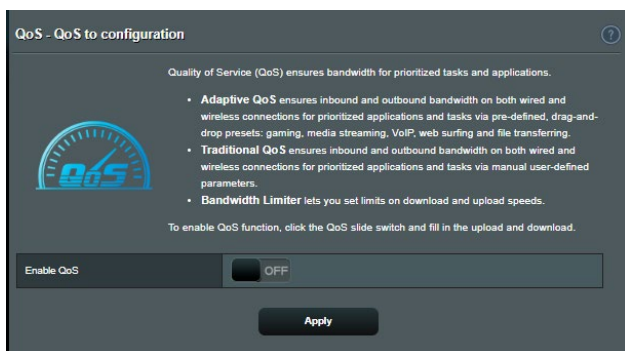
Per gestire i client della vostra rete:

1. Dal pannello di navigazione andate su **General (Generale) > Network Map (Mappa di rete)**.
2. Nella schermata **Network Map (Mappa di rete)** selezionate l'icona **Client status (Stato client)** per visualizzare le informazioni sui client della rete.
3. Per bloccare l'accesso di un client alla vostra rete selezionate il client e cliccate su **Block (Blocca)**.

3.2 QoS adattativo

3.2.1 Gestione della banda QoS

La funzione QoS (Quality of Service) vi permette di impostare la priorità e gestire il traffico di rete.



Per impostare la priorità di banda:

1. Dal pannello di navigazione andate su **General (Generale) > Adaptive QoS (QoS adattativo) > QoS**.
2. Spostate il cursore su **ON** per abilitare QoS. Specificate un valore per la banda in upload e download.

NOTA: Contattate il vostro ISP per ottenere i valori di banda disponibili con la vostra connessione.

3. Cliccate su **Apply (Applica)**.

NOTA: La tabella **User Specify Rule List (Regole Personalizzate)** contiene le impostazioni avanzate. Se dal menu in alto a destra scegliete **User-defined Priority (Priorità definite dall'utente)** potete impostare le priorità da assegnare successivamente ad applicazioni di rete o servizi di rete.

4. Selezionando la voce **User-defined QoS rules (Regole QoS definite dall'utente)** nell'elenco in alto a destra vedrete alcuni tra i servizi online più comuni: Web Surf (Navigazione web), HTTPS e File Transfer (Trasferimento file). Per aggiungere un

servizio compilate i campi **Source IP or MAC (Indirizzo IP o MAC sorgente)**, **Destination Port (Porta di destinazione)**, **Protocol (Protocollo)**, **Transferred (Trasferiti)** e **Priority (Priorità)** e, quando avete finito, cliccate su **Apply (Applica)**. Queste informazioni verranno aggiunte alla schermata delle regole QoS.

NOTE:

- Per inserire l'indirizzo IP o MAC sorgente potete:
 - a) Inserire un indirizzo IP specifico, come "192.168.122.1".
 - b) Inserire indirizzi IP appartenenti alla stessa subnet o allo stesso intervallo, come "192.168.123.*" o "192.168.*.*"
 - c) Inserire tutti gli indirizzi IP (*.**.*) o lasciare il campo vuoto.
 - d) Inserire l'indirizzo MAC. Un indirizzo MAC è composto da 6 coppie di cifre esadecimali, con ciascuna coppia separata da (:), per un totale di 12 cifre. Ad esempio: 12:34:56:aa:bc:ef
 - Nel campo porta sorgente e destinazione potete:
 - a) Inserire un numero di porta specifico, come "95".
 - b) Inserite un intervallo di porte, come "103:315", ">100" o "<65535".
 - La colonna **Transferred (Trasferiti)** contiene informazioni sul traffico upstream e downstream (ovvero il traffico in uscita e in entrata) per ogni sezione. In questa colonna potete impostare il limite di traffico (in KB) per un servizio specifico in modo da generare una priorità relativa ad un servizio assegnato ad una particolare porta. Per esempio, se due client, PC1 e PC2, stanno entrambi cercando di accedere ad Internet (porta 80), ma il PC1 ha già superato il limite di traffico, lo stesso PC1 avrà una priorità più bassa. Se non volete impostare il limite di traffico potete lasciare questo spazio vuoto.
-

5. Se dal menu in alto a destra scegliete **User-defined Priority (Priorità definite dall'utente)** potete impostare fino a 5 livelli di priorità, selezionabili successivamente nella pagina **user-defined QoS rules (Regole QoS definite dall'utente)** e assegnabili ad applicazioni di rete o dispositivi. Basandovi sui livelli di priorità potete usare i seguenti metodi per inviare pacchetti di dati:

- Cambiare l'ordine dei pacchetti di rete in uscita diretti verso Internet.
 - Nella tabella **Upload Bandwidth (Banda in Upload)** potete impostare i valori di **Minimum Reserved Bandwidth (Banda Minima Riservata)** e **Maximum Bandwidth Limit (Banda Massima Riservabile)** in modo da avere diverse applicazioni di rete ciascuna con il suo livello di priorità. La percentuale indica quanta banda è disponibile, in rapporto alla banda totale, per quella particolare applicazione di rete.
-

NOTE:

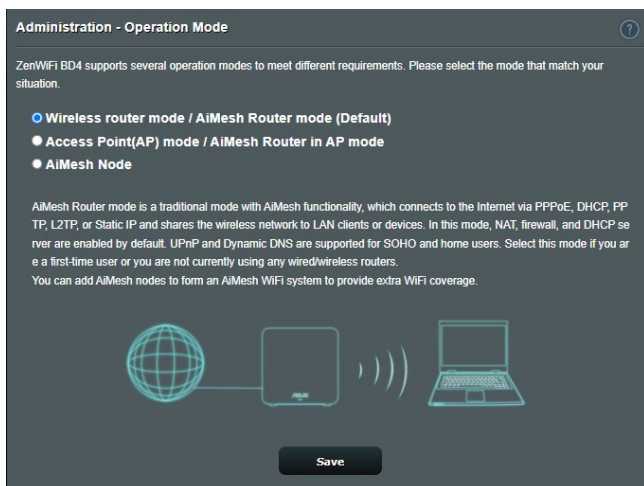
- I pacchetti con bassa priorità sono trascurati per favorire la trasmissione dei pacchetti ad alta priorità.
 - Nella tabella **Download Bandwidth (Banda in Download)** potete impostare i valori di **Maximum Bandwidth Limit (Banda Massima Riservabile)** per diverse applicazioni di rete e nell'ordine desiderato. Un pacchetto in uscita ad alta priorità genererà un pacchetto in entrata ad alta priorità.
 - Se non ci sono pacchetti inviati ad alta priorità la banda totale della connessione ad Internet sarà disponibile per i pacchetti a bassa priorità.
-
6. Impostate il pacchetto a priorità massima. Per assicurarvi un'esperienza di gioco online fluida potete impostare i pacchetti ACK, SYN e ICMP come pacchetti ad alta priorità.

NOTA: Assicuratevi di aver abilitato QoS prima di configurare i limiti di upload e download.

3.3 Amministrazione

3.3.1 Modalità operativa

La pagina Modalità operativa vi permette di scegliere la modalità appropriata necessaria per la vostra rete.



Per impostare la modalità operativa:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione)** e selezionate la scheda **Operation Mode (Modalità operativa)**.
2. Selezionate una delle seguenti modalità operative:
 - **Wireless router mode (default) (Modalità router wireless (predefinita)):** Nella modalità router wireless il router wireless si connette a Internet e fornisce accesso ad Internet a tutti i dispositivi presenti nella sua rete locale.
 - **Access Point mode (Modalità Access Point):** In questo modo il router, collegato ad una rete cablata, crea una nuova rete wireless.
 - **Nodo AiMesh:** Potete configurare ZenWiFi BD4 come nodo AiMesh per estendere la copertura Wi-Fi di un router AiMesh esistente.
3. Quando avete finito cliccate su **Save (Salva)**.

NOTA: Il router si riavvia automaticamente per cambiare la modalità.

3.3.2 Sistema

La pagina **Sistema** vi permette di configurare le impostazioni del vostro router wireless.

Per configurare le impostazioni di sistema:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione)** e selezionate la scheda **System (Sistema)**.
2. Potete configurare le seguenti impostazioni:
 - **Change router login password (Cambia le credenziali di accesso al router):** Potete cambiare la password e il nome utente del vostro router wireless inserendo un nuovo nome utente e una nuova password.
 - **WPS button behavior (Funzionamento pulsante WPS):** Il pulsante WPS presente sul router wireless può essere usato per attivare la funzione WPS (Wi-Fi Protected Setup).
 - **Time Zone (Fuso Orario):** Selezionate il corretto fuso orario per la vostra rete.
 - **NTP Server (Server NTP):** Il router wireless può ottenere informazioni da un server NTP (Network time Protocol) per regolare automaticamente data e ora.
 - **Enable Telnet (Abilita Telnet):** Selezionate **Yes (Sì)** per permettere le connessioni al router tramite il protocollo Telnet. Selezionate **No** per impedirlo.
 - **Authentication Method (Metodo d'autenticazione):** Potete scegliere HTTP, HTTPS o entrambi per un accesso al router sicuro.
 - **Enable Web Access from WAN (Abilita l'accesso all'interfaccia Web da Internet):** Selezionate **Yes (Sì)** per permettere la gestione del router tramite interfaccia Web anche dall'esterno della vostra rete. Selezionate **No** per impedirlo.
 - **Only allow specific IP (Indirizzi IP fidati):** Selezionate **Yes (Sì)** per creare un elenco di indirizzi IP ai quali permettere la gestione del router tramite interfaccia Web dall'esterno della vostra rete.
3. Cliccate su **Apply (Applica)**.

3.3.3 Aggiornamento firmware

NOTA: Scaricate l'ultimo firmware disponibile dal sito web ASUS:
<http://www.asus.com>.

Per aggiornare il firmware:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione)** e selezionate la **Firmware Upgrade (Aggiornamento firmware)**.
 2. Dalla pagina **Firmware Version (Versione del firmware)** cliccate su **Check (Controlla)** per cercare il file del firmware che avete appena scaricato.
 3. Cliccate su **Upload (Carica)** per aggiornare il firmware.
-

NOTE:

- Quando l'aggiornamento del firmware è completato aspettate qualche minuto per permettere al sistema di riavviarsi.
 - Se l'aggiornamento del firmware fallisce il router wireless entra automaticamente in modalità di recupero e il LED di alimentazione del pannello anteriore comincia a lampeggiare lentamente. Fate riferimento alla sezione *4.2 Firmware Restoration* per avere maggiori informazioni su come effettuare il recupero del firmware.
-

3.3.4 Ripristina/Salva/Carica Impostazioni

Per ripristinare/salvare/caricare le impostazioni del router wireless:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione)** e selezionate la **Restore/Save/Upload Setting (Impostazione Ripristina/Salva/Carica)**.
 2. Selezionate il processo che volete eseguire:
 - Cliccate su **Restore (Ripristina)** e poi su **OK** se volete ripristinare le impostazioni predefinite di fabbrica.
 - Cliccate su **Save setting (Salva impostazione)**, scegliete un percorso dove salvare il file e poi cliccate su **Save (Salva)** se volete salvare le impostazioni correnti del sistema.
 - Per ripristinare le impostazioni da un file salvato in precedenza cliccate su **Upload (Carica)**, selezionate il file e cliccate su **Open (Apri)**.
-

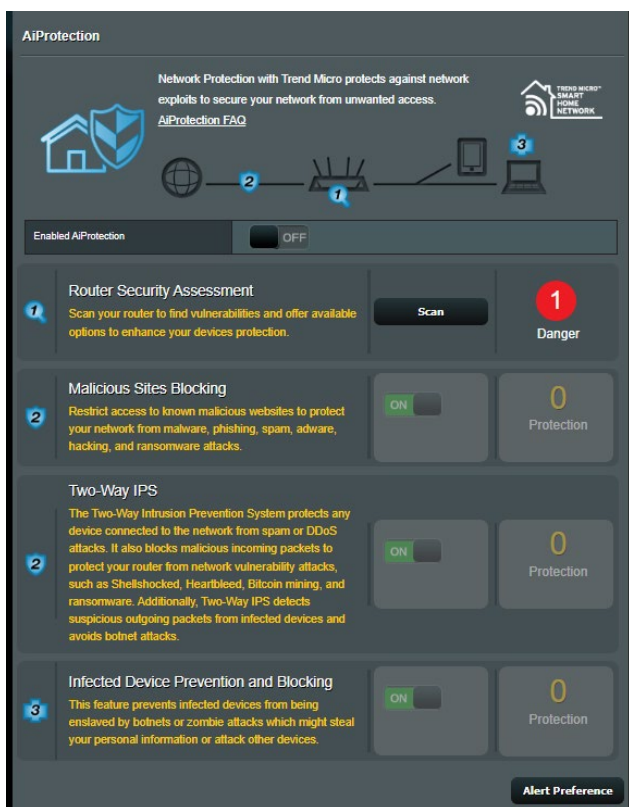
IMPORTANTE! Se ci fossero dei problemi aggiornate il firmware all'ultima versione e configurate le nuove impostazioni. **NON** ripristinate le impostazioni predefinite del router.

3.4 AiProtection

AiProtection fornisce monitoraggio in tempo reale per rilevare malware, spyware e accessi non autorizzati. Inoltre permette di filtrare siti web o app indesiderate e limitare l'accesso ad Internet ai dispositivi connessi per un determinato periodo di tempo.

3.4.1 Protezione della rete

Protezione della rete permette di proteggersi contro exploit di rete per impedire accessi non autorizzati.

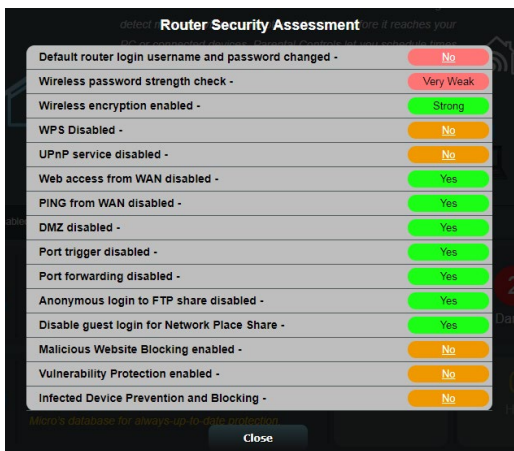


Configurazione di Network Protection (Protezione della rete)

Per configurare Protezione della rete:

1. Dal pannello di navigazione andate su **General (Generale)** > **AiProtection**.
2. Nella pagina principale di **AiProtection** cliccate su **Network Protection (Protezione della rete)**.
3. Nella scheda di **Network Protection** cliccate su **Scan (Scansione)**.

Una volta terminata la scansione verrete indirizzati alla pagina **Router Security Assessment (Valutazione della sicurezza del router)**.



IMPORTANTE! Le voci sicure vengono valutate con un **Yes (Sì)** nella pagina **Router Security Assessment (Valutazione della sicurezza del router)**. Al contrario le voci valutate con **No, Weak (Debole)** o **Very Weak (Molto debole)** devono essere configurate ulteriormente.

4. (Opzionale) Nella pagina **Router Security Assessment (Valutazione della sicurezza del router)** configurate manualmente le voci valutate con **No, Weak (Debole)** o **Very Weak (Molto debole)**. Per fare questo:
 - a. Cliccate su una voce.

NOTA: Quando cliccate su una voce verrete reindirizzati automaticamente alla pagina delle sue impostazioni.

- b. Configurate e applicate le modifiche necessarie, cliccate su **Apply (Applica)** quando avete finito.
 - c. Tornate alla pagina **Valutazione della sicurezza del router** e cliccate su **Close (Chiudi)** per uscire.
5. Per configurare automaticamente le opzioni di sicurezza cliccate su **Secure Your Router (Metti in sicurezza)**.
 6. Quando appare un messaggio di conferma cliccate su **OK**.

Blocco siti web malevoli

Questa funzione limita l'accesso ai siti web conosciuti, e dannosi, servendosi di un database cloud per una protezione sempre aggiornata.

NOTA: Questa funzione viene abilitata automaticamente se eseguite la **Router Weakness Scan (Scansione vulnerabilità del router)**.

Per abilitare Blocco siti web malevoli:

1. Dal pannello di navigazione andate su **General (Generale) > AiProtection**.
2. Nella pagina principale di **AiProtection** cliccate su **Network Protection (Protezione della rete)**.
3. Nel pannello di **Malicious Sites Blocking (Blocco siti web malevoli)** cliccate su **ON**.

IPS bidirezionale

IPS bidirezionale (Intrusion Prevention System) protegge il vostro router da attacchi di rete bloccando i pacchetti malevoli in ingresso e rilevando i pacchetti sospetti in uscita.

NOTA: Questa funzione viene abilitata automaticamente se eseguite la **Router Weakness Scan (Scansione vulnerabilità del router)**.

Per abilitare IPS bidirezionale:

1. Dal pannello di navigazione andate su **General (Generale)** > **AiProtection**.
2. Nella pagina principale di **AiProtection** cliccate su **Network Protection (Protezione della rete)**.
3. Nel pannello di **Two-Way IPS (IPS bidirezionale)** cliccate su **ON**.

Prevenzione e blocco di dispositivi infetti

Questa funzione impedisce ai dispositivi connessi infetti di diffondere informazioni personali, o informazioni di vulnerabilità, a soggetti esterni.

NOTA: Questa funzione viene abilitata automaticamente se eseguite la **Router Weakness Scan (Scansione vulnerabilità del router)**.

Per abilitare la prevenzione e il blocco di dispositivi infetti:

1. Dal pannello di navigazione andate su **General (Generale)** > **AiProtection**.
2. Nella pagina principale di **AiProtection** cliccate su **Network Protection (Protezione della rete)**.
3. Nel pannello di **Infected Device Prevention and Blocking (Prevenzione e blocco di dispositivi infetti)** cliccate su **ON**.

Per configurare Preferenze avvisi:

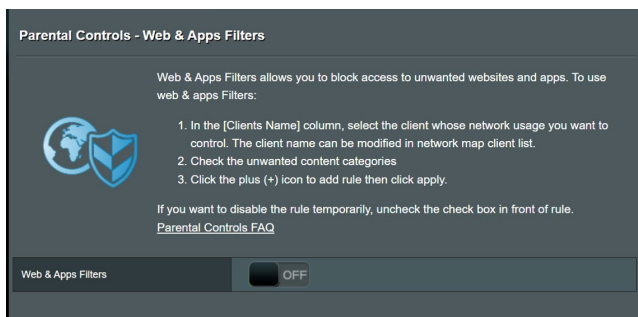
1. Nel pannello di **Infected Device Prevention and Blocking (Prevenzione e blocco di dispositivi infetti)** cliccate su **Alert Preference (Preferenze avvisi)**.
2. Selezionate o inserite il provider email, l'account email e la password quindi cliccate su **Apply (Applica)**.

3.4.2 Configurazione di Controllo Genitori

Controllo genitori permette di controllare l'orario di accesso ad Internet, o di impostare un tempo limite, per i clienti della rete.

Per accedere alla pagina principale di Controllo Genitori:

Dal pannello di navigazione andate su **General (Generale)** > **Parental Controls (Controllo Genitori)**.



Filtro web e app

Filtro web e app è una funzione di **Parental Controls (Controllo genitori)** e permette di impedire l'accesso a siti web e app non desiderate.

Per configurare Filtro web e app:

1. Dal pannello di navigazione andate su **General (Generale)** > **Parental Controls (Controllo Genitori)**.
2. Nel pannello di **Web & Apps Filters (Filtro web e app)** cliccate su **ON**.
3. Quando appare il messaggio con il contratto di licenza per l'utente finale (EULA) cliccate su **I agree (Accetto)** per continuare.
4. Nella colonna **Client List (Elenco client)** selezionate o inserite il nome del client.
5. Nella colonna **Content Category (Categoria di contenuti)** impostate il filtro per le quattro categorie principali: **Adulti, Chat e comunicazione, Trasferimento file e P2P e Intrattenimento**.
6. Cliccate su  per aggiungere il profilo del client.
7. Cliccate su Apply (Applica) per confermare le modifiche.

Parental Controls - Web & Apps Filters



Web & Apps Filters allows you to block access to unwanted websites and apps. To use web & apps Filters:

1. In the [Clients Name] column, select the client whose network usage you want to control. The client name can be modified in network map client list.
2. Check the unwanted content categories
3. Click the plus (+) icon to add rule then click apply.

If you want to disable the rule temporarily, uncheck the check box in front of rule.
[Parental Controls FAQ](#)

Web & Apps Filters ON

Client List (Max Limit : 64)

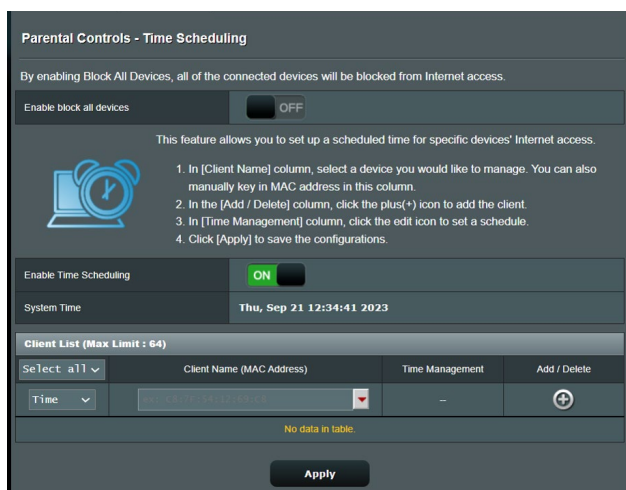
<input type="checkbox"/>	Client Name (MAC Address)	Content Category	Add / Delete
<input checked="" type="checkbox"/>	192.168.1.100	<ul style="list-style-type: none"><input type="checkbox"/> Adult Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature.<input type="checkbox"/> Instant Message and Communication Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites.<input type="checkbox"/> P2P and File Transfer By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission.<input type="checkbox"/> Streaming and Entertainment By blocking streaming and entertainment services you can limit the time your children spend online.	<input data-bbox="750 619 771 643" type="button" value="+"/>

No data in table.

Pianificazione temporale

Pianificazione temporale vi permette di impostare un limite di tempo per l'utilizzo della rete da parte di un client.

NOTA: Assicuratevi che l'ora di sistema sia sincronizzata con il server NTP.



Per configurare Pianificazione temporale:

1. Dal pannello di navigazione andate su **General (Generale)** > **Parental Controls (Controllo Genitori)** > **Time Scheduling (Pianificazione temporale)**.
2. Nel pannello di **Enable Time Scheduling (Abilita Pianificazione temporale)** cliccate su **ON**.
3. Nella colonna **Client Name (Nome client)** selezionate o inserite il nome del client.

NOTA: Potete anche inserire l'indirizzo MAC nella colonna **Client MAC Address (Indirizzo MAC client)**. Assicuratevi che il nome del client non contenga caratteri speciali o spazi perché potreste causare un malfunzionamento del router.

4. Cliccate su **+** per aggiungere il profilo del client.
5. Cliccate su **Apply (Applica)** per confermare le modifiche.

3.5 Firewall

Il router wireless può funzionare anche da firewall hardware per la vostra rete.

NOTA: La funzione Firewall è abilitata su tutti i router.

3.5.1 Generale

Firewall

General

Enable the firewall to protect your local area network against attacks from hackers. The firewall filters the incoming and outgoing packets based on the filter rules.
[DoS Protection FAQ](#)

Enable Firewall Yes No

Enable DoS protection Yes No

Logged packets type

Respond ICMP Echo (ping) Request from WAN Yes No

Basic Config

Enable IPv4 inbound firewall rules Yes No

Inbound Firewall Rules (Max Limit : 128)

Source IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="button" value="⊕"/>

No data in table.

IPv6 Firewall

All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.

You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified.
(2001::1111:2222:3333:64 for example)

Basic Config

Enable IPv6 Firewall Yes No

Famous Server List

Inbound Firewall Rules (Max Limit : 128)

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="button" value="⊕"/>

No data in table.

Per configurare le impostazioni di base del firewall:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Firewall > General (Generale)**.
2. Alla voce **Enable Firewall (Abilita Firewall)** selezionate **Yes (Sì)**.
3. Alla voce **Enable DoS protection (Abilita la protezione DoS)** selezionate **Yes (Sì)** se volete proteggere la vostra rete da

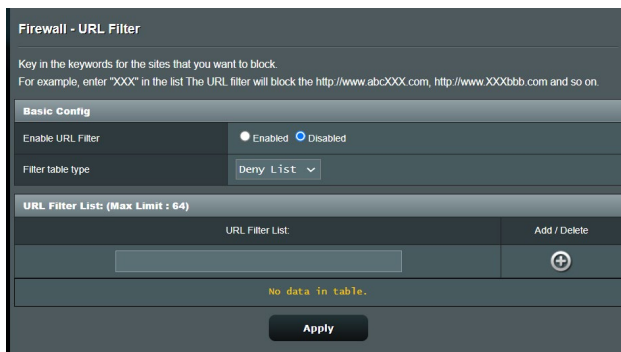
possibili attacchi DoS (Denial of Service) che possono peggiorare notevolmente le prestazioni del vostro router.

4. Potete anche controllare i pacchetti scambiati tra LAN (rete locale) e WAN (Internet). Alla voce **Logged packets type (Tipologia di pacchetti registrati)** selezionate **Dropped (Scartati)**, **Accepted (Accettati)** o **Both (Entrambi)**.
5. Cliccate su **Apply (Applica)**.


3.5.2 Filtro URL

Potete specificare parole chiave o indirizzi web per impedire l'accesso a URL specifici.

NOTA: Il filtro URL lavora sulle query DNS. Se un client ha già effettuato l'accesso ad un sito web, ad esempio `http://www.abcxxx.com`, potrà comunque visitare nuovamente il sito anche se il filtro lo impedirebbe (la cache DNS del sistema ricorda i siti visitati in precedenza in modo da non dover continuamente interrogare il server DNS). Per risolvere questo problema svuotate la cache DNS prima di impostare il filtro URL.

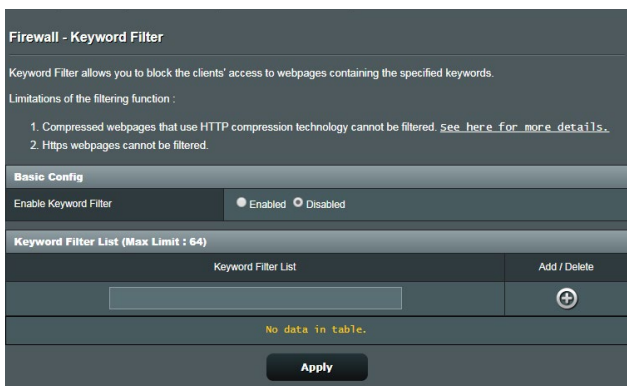


Per abilitare e configurare il filtro URL:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Firewall > URL filter (Filtro URL)**.
2. Alla voce **Enable URL Filter (Abilita filtro URL)** selezionate **Enabled (Abilitato)**.
3. Inserite un indirizzo Internet e cliccate sul pulsante  .
4. Cliccate su **Apply (Applica)**.

3.5.3 Filtro Parole Chiave

Il Filtro Parole Chiave blocca l'accesso alle pagine web contenenti le parole che inserite nell'elenco.



Per abilitare e configurare il Filtro Parole Chiave:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Firewall > Keyword Filter (Filtro parole chiave)**.
2. Alla voce Enable Keyword Filter (Abilita filtro parole chiave) selezionate **Enabled (Abilitato)**.
3. Inserite una parola o una frase e poi cliccate sul pulsante **Add (Aggiungi)**.
4. Cliccate su **Apply (Applica)**.

NOTE:

- Il Filtro Parole Chiave lavora sulle query DNS. Se un client ha già effettuato l'accesso ad un sito web, ad esempio <http://www.abcxxx.com>, potrà comunque visitare nuovamente il sito anche se il filtro lo impedirebbe (la cache DNS del sistema ricorda i siti visitati in precedenza in modo da non dover continuamente interrogare il server DNS). Per risolvere questo problema svuotate la cache DNS prima di impostare il Filtro Parole Chiave.
- Le pagine web compresse tramite la compressione HTTP non possono essere filtrate. Neanche le pagine HTTPS possono essere bloccate tramite il Filtro Parole Chiave.

3.5.4 Packet Filter

Il Packet Filter blocca i pacchetti diretti verso l'esterno della rete e limita l'accesso dei client di rete a servizi specifici come Telnet o FTP.

Firewall - Network Services Filter

The Network Services filter blocks the LAN to WAN packet exchanges and restricts devices from using specific network services. For example, if you do not want the device to use the Internet service, key in 80 in the destination port. The traffic that uses port 80 will be blocked (but https can not be blocked).
Leave the source IP field blank to apply this rule to all LAN devices.

Deny List Duration : During the scheduled duration, clients in the Deny List cannot use the specified network services. After the specified duration, all the clients in LAN can access the specified network services.

Allow List Duration : During the scheduled duration, clients in the Allow List can ONLY use the specified network

NOTE : If you set the subnet for the Allow List, IP addresses outside the subnet will not be able to access the Internet or any Internet service.

Network Services Filter

Enable Network Services Filter Yes No

Filter table type

Well-Known Applications

Date to Enable LAN to WAN Filter Mon Tue Wed Thu Fri

Time of Day to Enable LAN to WAN Filter : - :

Date to Enable LAN to WAN Filter Sat Sun

Time of Day to Enable LAN to WAN Filter : - :

Filtered ICMP packet types

Network Services Filter Table (Max Limit : 32)

Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
				TCP	

No data in table.

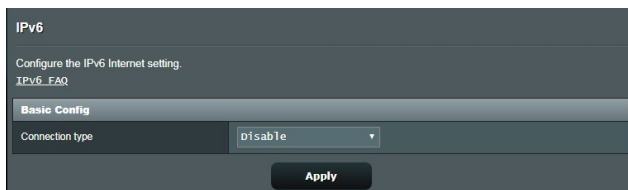
Apply

Per abilitare e configurare il Packet Filter:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione) > Network Service Filter (Packet Filter)**.
2. Alla voce **Enable Network Services Filter (Abilita Packet Filter)** selezionate **Yes (Sì)**.
3. Selezionate la modalità di filtraggio. **Deny (Nega)** blocca i servizi di rete selezionati. **Allow (Consenti)** limita l'accesso esclusivamente ai servizi selezionati.
4. Selezionate giorno e orario nei quali intendete attivare il filtro.
5. Per aggiungere un nuovo servizio da filtrare inserite IP sorgente, IP destinazione, porta/e e il protocollo. Cliccate sul pulsante .
6. Cliccate su **Apply (Applica)**.

3.6 IPv6

Il router wireless supporta il protocollo IPv6, un protocollo in grado di gestire molti più indirizzi del protocollo IPv4. Questo standard non è ancora disponibile in maniera molto diffusa. Chiedete informazioni al vostro ISP per sapere se IPv6 è effettivamente supportato.



Per configurare IPv6:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > IPv6**.
2. Selezionate il **Connection type (Tipo di connessione)** appropriato. Le opzioni di configurazione variano a seconda del tipo di connessione selezionata.
3. Inserite le impostazioni della LAN IPv6 e del server DNS.
4. Cliccate su **Apply (Applica)**.

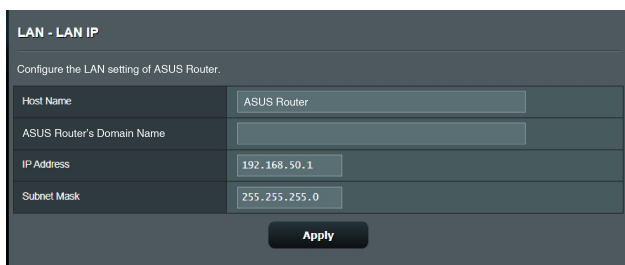
NOTA: Chiedete informazioni al vostro ISP per sapere se IPv6 è effettivamente supportato.

3.7 LAN

3.7.1 LAN IP

La schermata LAN IP permette di modificare le impostazioni LAN del router wireless.

NOTA: Qualsiasi cambiamento dell'IP LAN del vostro router avrà effetti automaticamente anche sulle impostazioni del server DHCP.



The screenshot shows the 'LAN - LAN IP' configuration page. At the top, it says 'Configure the LAN setting of ASUS Router.' Below this, there are four input fields: 'Host Name' with the value 'ASUS Router', 'ASUS Router's Domain Name' (empty), 'IP Address' with the value '192.168.50.1', and 'Subnet Mask' with the value '255.255.255.0'. At the bottom center, there is an 'Apply' button.

Per modificare le impostazioni LAN del router wireless:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **LAN** e selezionate la **LAN IP (IP LAN)**.
2. Potete modificare i campi **IP Address (Indirizzo IP)** e **Subnet Mask**.
3. Quando avete finito cliccate su **Apply (Applica)**.

3.7.2 Server DHCP

Il vostro router wireless usa il protocollo DHCP per assegnare indirizzi IP nella vostra rete automaticamente. Potete specificare l'intervallo di indirizzi IP e il tempo di rilascio per i client della vostra rete.

LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the DNS server IP and default gateway IP. ASUS Router supports up to 253 IP addresses for your local network.
Manually Assigned IP around the DHCP list FAQ

Basic Config

Enable the DHCP Server Yes No

ASUS Router's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

Advertise router's IP in addition to user-specified DNS Yes No

WINS Server

Manual Assignment

Enable Manual Assignment Yes No

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

No data in table.

Apply

Per configurare il server DHCP:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > LAN** e selezionate la **DHCP Server (Server DHCP)**.
2. Alla voce **Enable the DHCP Server (Abilita il server DHCP)** selezionate **Yes (Sì)**.
3. Nel campo **Domain Name (Nome del Dominio)** inserite un nome di dominio per il router wireless.

4. Nel campo **IP Pool Starting Address (Indirizzo IP iniziale)** inserite l'indirizzo IP iniziale dell'intervallo desiderato.
5. Nel campo **IP Pool Ending Address (Indirizzo IP finale)** inserite l'indirizzo IP finale dell'intervallo desiderato.
6. Nel campo **Lease Time (Tempo di rilascio)** specificate, in termini di secondi, la durata dell'assegnazione di un indirizzo IP. Una volta raggiunto il tempo di rilascio il server DHCP assegnerà al client un nuovo indirizzo IP.

NOTE:

- Raccomandiamo di utilizzare un indirizzo IP del formato 192.168.50.xxx (con xxx che può variare da 2 a 254) quando dovete scegliere un intervallo di indirizzi IP.
 - L'indirizzo IP iniziale non deve essere superiore all'indirizzo IP finale.
-
7. Nella sezione **DNS and WINS Server Setting (Impostazione server DNS e WINS)** inserite gli indirizzi IP dei server DNS e WINS se necessario.
 8. Il vostro router wireless è anche in grado di assegnare manualmente gli indirizzi IP ai dispositivi della rete. Alla voce **Enable Manual Assignment (Abilita assegnazione manuale)** selezionate **Yes (Sì)** per assegnare un indirizzo IP ad un indirizzo MAC specifico sulla rete. Potete specificare fino a 32 indirizzi MAC nell'elenco DHCP di assegnazione manuale degli indirizzi IP.

3.7.3 Rotte

Se la vostra rete usa uno o più router wireless potete configurare una tabella di routing in modo da condividere la stessa connessione ad Internet.

NOTA: Vi raccomandiamo di non modificare la tabella di routing predefinita a meno che non abbiate una conoscenza approfondita delle tabelle di routing.

LAN - Route

This function allows you to add routing rules into. It is useful if you connect several routers behind to share the same connection to the Internet.

Basic Config

Enable static routes Yes No


Static Route List (Max Limit : 32)

Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete
				LAN	+

No data in table.

Apply

Per configurare la tabella di routing:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > LAN > Route (Rotte)**.
2. Selezionate **Yes (Sì)** alla voce **Enable static routes (Abilita routing statico)**.
3. Nell'elenco **Static Route List (Rotte Statiche)** inserite le informazioni di rete degli altri access point o nodi. Cliccate sul pulsante **Add (Aggiungi)**  o **Delete (Elimina)**  per aggiungere o rimuovere un dispositivo dall'elenco.
4. Cliccate su **Apply (Applica)**.

3.7.4 IPTV

Il router wireless supporta la connessione a servizi IPTV tramite ISP o LAN. La scheda IPTV vi permette di configurare le varie impostazioni per i servizi IPTV, VoIP, multicasting e UDP. Contattate il vostro ISP per maggiori informazioni sui servizi disponibili con la vostra fornitura.

LAN - IPTV

To watch IPTV, the WAN port must be connected to the Internet. Please go to [WAN - Dual WAN](#) to confirm that WAN port is assigned to primary WAN.

LAN Port	
Select ISP Profile	None ▾
Choose IPTV STB Port	None ▾

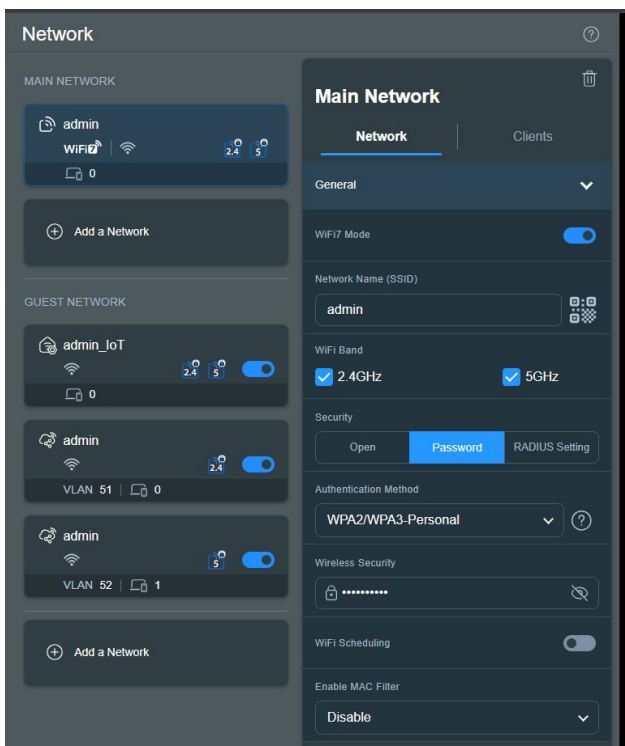
Special Applications	
Use DHCP routes	microsoft ▾
Enable multicast routing (IGMP Proxy)	Disable ▾
UDP Proxy (Udpxy)	0

Apply

3.8 Rete

3.8.1 Rete principale - Filtro MAC

Il Filtro MAC wireless fornisce controllo sui pacchetti trasmessi verso uno specifico indirizzo MAC (Media Access Control) presente nella vostra rete wireless.





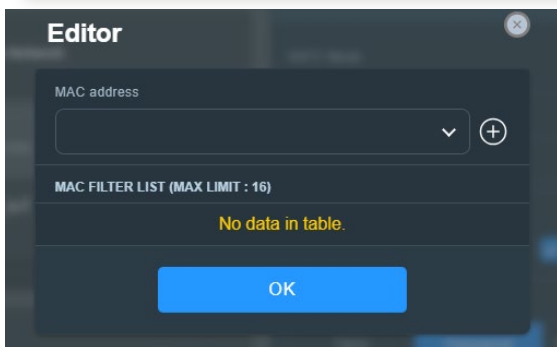
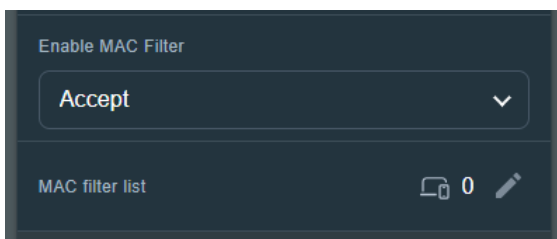
Per impostare il Filtro MAC wireless:

1. Dal pannello di navigazione andate su **General (Generali) > Network (Rete) > Main Network (Rete principale)** e seleziona il nome (SSID) della rete principale.
2. Nel menu **Enable MAC Filter (Abilita filtro MAC)** selezionate **Accept (Accetta)** o **Reject (Rifiuta)**.
 - Selezionate **Accept (Accetta)** per permettere agli indirizzi MAC nell'elenco di accedere alla rete wireless.

- Selezionate **Reject (Rifiuta)** per impedire agli indirizzi MAC nell'elenco di accedere alla rete wireless.

NOTA: Seleziona **Disabilita** se desideri disattivare **Abilita filtro MAC**.

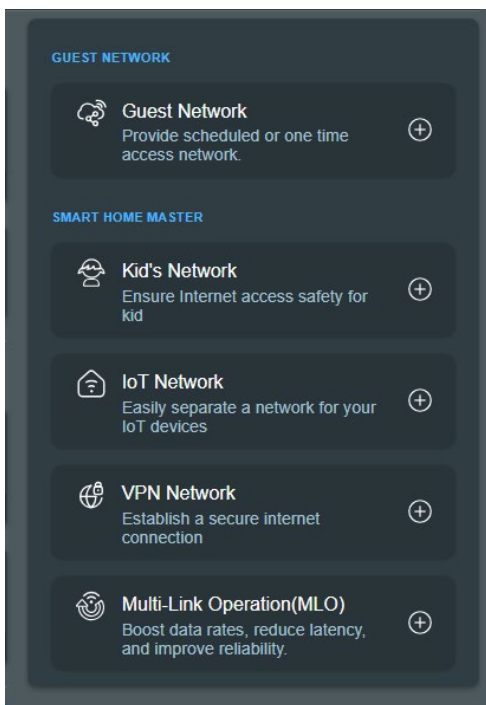
4. In Elenco filtro MAC, fare clic su  per accedere alla pagina **Editor**, quindi fare clic su  e digitare l'indirizzo MAC del dispositivo wireless.
5. Cliccate su **OK**.



3.8.2 Rete ospiti

3.8.2.1 Rete ospiti

Una Guest Network (Rete ospiti) fornisce ai visitatori temporanei una connessione ad Internet, tramite una rete diversa (SSID differente), senza fornire accesso alla vostra rete privata.



NOTA: ZenWiFi BD4 supporta fino a tre SSID nella rete Guest.

Per creare una Rete ospiti:

1. Dal pannello di navigazione andate su **General (Generale)** > **Network (Rete)** > **Guest Network (Rete ospiti)** > **Add a Network (Aggiungere una rete)**.
2. Selezionare **Guest Network (Rete ospiti)** e assegnare un nome alla rete temporanea nel campo **Network Name (Nome della rete) (SSID)**.

3. Selezionare un metodo di autenticazione in **Security (Sicurezza)**.
4. Specificare l'orario di accesso o scegliere **Scheduled (Programmato)** per aggiungere un profilo di programmazione online.
5. Selezionare la **WiFi Band (Banda WiFi)** per la rete ospite che si desidera creare.
6. Abilita o disabilita il **Bandwidth Limiter (Limitatore larghezza di banda)**.
7. Abilitare o disabilitare **Access Intranet (Accesso Intranet)**.
8. Quando avete finito cliccate su **Apply (Applica)**.

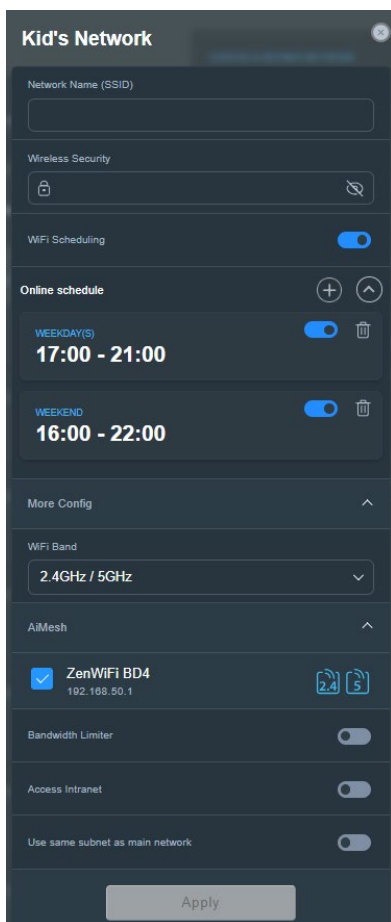
The screenshot shows the 'Guest Network' configuration page. At the top, there is a 'Network Name (SSID)' input field. Below it is the 'Security' section with an 'Open' button and a 'Password' input field. The 'WiFi Scheduling' section has a toggle switch turned on and two radio buttons: 'Scheduled' (unselected) and 'One Time Access' (selected). Under 'One Time Access', there are buttons for '30 mins', '1 hr(s)', '2 hr(s)' (highlighted in blue), '4 hr(s)', '6 hr(s)', and 'Custom'. A 'More Config' section with an upward arrow contains the 'WiFi Band' dropdown menu set to '2.4GHz / 5GHz'. Below that is the 'AiMesh' section with an upward arrow, showing 'ZenWiFi BD4' with IP '192.168.50.1' and icons for 2.4 and 5 GHz. At the bottom, there are three toggle switches: 'Bandwidth Limiter' (off), 'Access Intranet' (off), and 'Use same subnet as main network' (off). A large 'Apply' button is at the very bottom.

3.8.2.2 Smart Home Master

Smart Home Master è uno strumento potente e facile da usare per la segmentazione della rete. Semplifica il processo di creazione e gestione di scenari di sottoreti avanzati come la creazione di un SSID dedicato per i dispositivi dei bambini, la connessione a una VPN tramite una sottorete dedicata o persino la creazione di un SSID sicuro per tutti i dispositivi IoT.

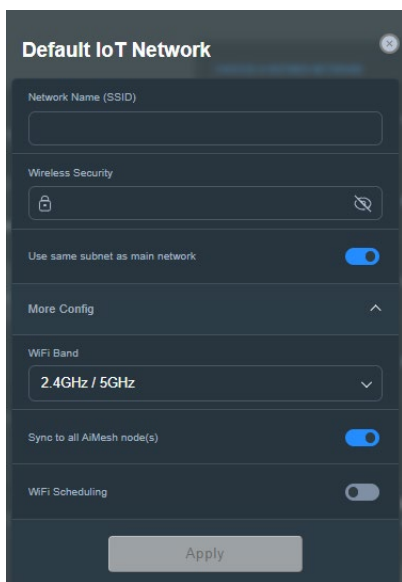
Creare una rete per bambini:

1. Dal pannello di navigazione andate su **General (Generale)** > **Network (Rete)** > **Guest Network (Rete ospiti)** > **Add a Network (Aggiungere una rete)**.
2. Selezionare **Kid's Network (Rete per bambini)** e assegnare un nome di rete e una chiave di sicurezza nei campi **Network Name (Nome della rete) (SSID)** e **Wireless Security (Sicurezza wireless)**.
3. Personalizzare l'orario di accesso a Internet nel campo **Online schedule (Programma online)**.
4. Selezionare la **WiFi Band (Banda WiFi)** per la rete del bambino che si desidera creare.
5. Abilita o disabilita il **Bandwidth Limiter (Limitatore larghezza di banda)**.
6. Abilitare o disabilitare **Access Intranet (Accesso Intranet)**.
7. Quando avete finito cliccate su **Apply (Applica)**.



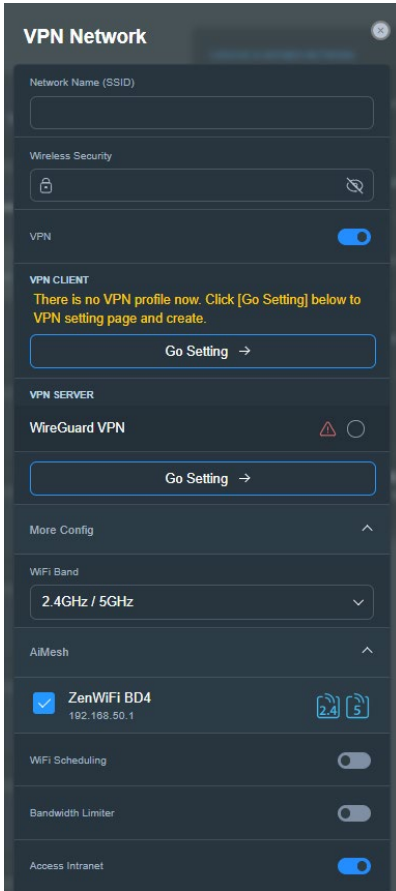
Per creare una Rete IoT:

1. Dal pannello di navigazione andate su **General (Generale)** > **Network (Rete)** > **Guest Network (Rete ospiti)** > **Add a Network (Aggiungere una rete)**.
2. Selezionare **IoT Network (Rete IoT)** e assegnare un nome di rete e una chiave di sicurezza nei campi **Network Name (Nome della rete) (SSID)** e **Wireless Security (Sicurezza wireless)**.
3. Selezionare la **WiFi Band (Banda WiFi)** per la Rete IoT che si desidera creare.
4. Personalizzate l'orario di accesso a Internet attivando la **WiFi Scheduling (programmazione del WiFi)**.
5. Quando avete finito cliccate su **Apply (Applica)**.



Per creare una Rete VPN:

1. Dal pannello di navigazione andate su **General (Generale)** > **Network (Rete)** > **Guest Network (Rete ospiti)** > **Add a Network (Aggiungere una rete)**.
2. Selezionare **VPN Network (Rete VPN)** e assegnare un nome di rete e una chiave di sicurezza nei campi **Network Name (Nome della rete) (SSID)** e **Wireless Security (Sicurezza wireless)**.
3. Se non è stato impostato un profilo VPN per il server VPN o il client VPN, fare clic su **Go Setting (Vai a impostazione)** per creare un profilo VPN.
4. Selezionare la **WiFi Band (Banda WiFi)** per la Rete VPN che si desidera creare.
5. Personalizzate l'orario di accesso a Internet attivando la **WiFi Scheduling (programmazione del WiFi)**.
6. Abilita o disabilita il **Bandwidth Limiter (Limitatore larghezza di banda)**.
7. Abilitare o disabilitare **Access Intranet (Accesso Intranet)**.
8. Quando avete finito cliccate su **Apply (Applica)**.



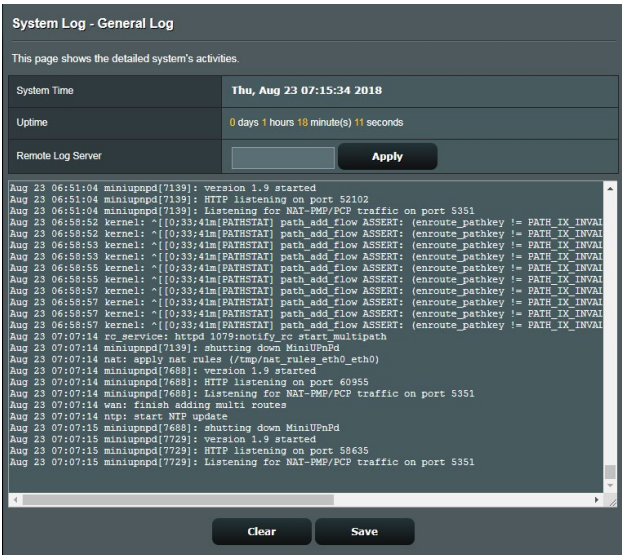
3.9 Registro di sistema

Il registro di sistema contiene la registrazione delle vostre attività di rete.

NOTA: Il registro di sistema viene cancellato quando il router viene riavviato o spento.

Per visualizzare il vostro registro di sistema:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > System Log (Registro di sistema)**.
2. Potete visualizzare le diverse attività di rete in una delle seguenti schede:
 - General Log (Registro generale)
 - Wireless Log (Registro wireless)
 - DHCP Leases (Lease DHCP)
 - IPv6
 - Routing Table (Tabella di routing)
 - Port Forwarding
 - Connessioni



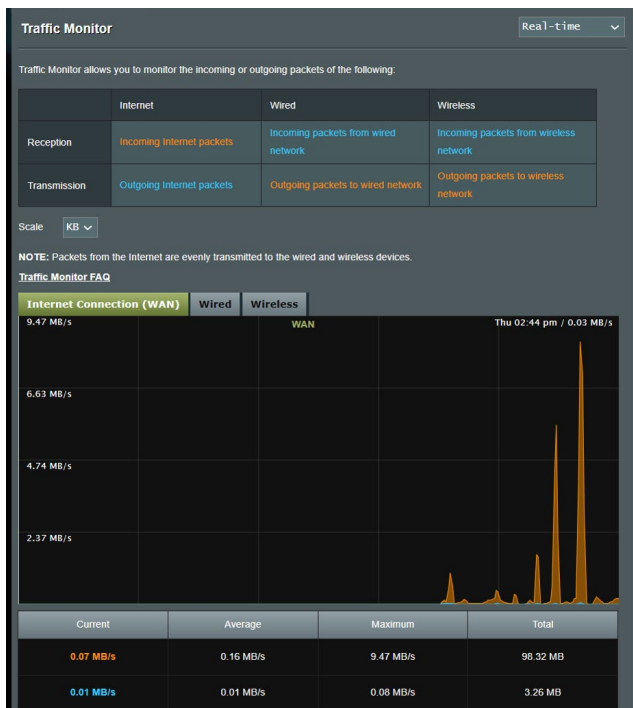
The screenshot displays the 'System Log - General Log' interface. At the top, it states 'This page shows the detailed system's activities.' Below this, there are fields for 'System Time' (Thu, Aug 23 07:15:34 2018) and 'Uptime' (0 days 7 hours 18 minutes(s) 11 seconds). A 'Remote Log Server' field is present with an 'Apply' button. The main area is a scrollable log window containing the following text:

```
Aug 23 06:51:04 minipppd[7139]: version 1.9 started
Aug 23 06:51:04 minipppd[7139]: HTTP listening on port 52102
Aug 23 06:51:04 minipppd[7139]: Listening for NAI-PMP/PCP traffic on port 5351
Aug 23 06:58:52 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:53 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:53 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:55 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:55 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 07:07:14 rc_service: httpd 1079:notify_rc start_multipath
Aug 23 07:07:14 minipppd[7139]: shutting down MiniUPnPd
Aug 23 07:07:14 ntp: apply ntp rules (/tmp/ntp_rules_etc0_eth0)
Aug 23 07:07:14 minipppd[7688]: version 1.9 started
Aug 23 07:07:14 minipppd[7688]: HTTP listening on port 60955
Aug 23 07:07:14 minipppd[7688]: Listening for NAI-PMP/PCP traffic on port 5351
Aug 23 07:07:14 wpa: finish adding multi courses
Aug 23 07:07:14 ntp: start NTP update
Aug 23 07:07:15 minipppd[7688]: shutting down MiniUPnPd
Aug 23 07:07:15 minipppd[7729]: version 1.9 started
Aug 23 07:07:15 minipppd[7729]: HTTP listening on port 58635
Aug 23 07:07:15 minipppd[7729]: Listening for NAI-PMP/PCP traffic on port 5351
```

At the bottom of the log window, there are 'Clear' and 'Save' buttons.

3.10 Traffic Analyzer

Il Traffic Monitor (Monitoraggio traffico) vi permette di accedere alle informazioni relative alla banda e all'utilizzo di Internet, connessione cablata e connessione wireless. Il monitoraggio è possibile in tempo reale o su base giornaliera. Se volete potete anche visualizzare il traffico delle ultime 24 ore.



NOTA: I pacchetti provenienti dalla rete Internet sono ugualmente trasmessi ai dispositivi della rete.

3.11 WAN

3.11.1 Connessione ad Internet

La schermata Connessione ad Internet vi permette di configurare le varie impostazioni per la connessione WAN.

WAN - Internet Connection

ASUS Router supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Configure the Ethernet WAN settings of ASUS Router.

Basic Config	
WAN Connection Type	Automatic IP ▾
Enable WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable NAT	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable UPnP <small>UPnP_EAQ</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable WAN Aggregation	<input type="radio"/> Yes <input checked="" type="radio"/> No <small>WAN Aggregation combines two network connections to increase your WAN speed up to 2Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports (ensure you use two cables with the same specification) WAN Aggregation FAQ</small>

WAN DNS Setting	
DNS Server	Default status : Get the DNS IP from your ISP automatically. Assign a DNS service to improve security, block advertisement and gain faster performance. Assign
Forward local domain queries to upstream DNS	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable DNS Rebind protection	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable DNSSEC support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Prevent client auto DoH	Auto ▾
DNS Privacy Protocol	None ▾

DHCP Option	
Class-identifier (Option 60)	<input type="text"/>
Client-identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID <input type="text"/>
Class-identifier (Option 60)	<input type="text"/>
Client-identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID <input type="text"/>

Account Settings	
Authentication	None ▾
PPP Echo Interval	<input type="text" value="6"/>
PPP Echo Max Failures	<input type="text" value="10"/>

Special Requirement from ISP	
Host Name	<input type="text"/>
MAC Address	<input type="text"/> MAC Clone
DHCP query frequency	Aggressive Mode ▾
Extend the TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No
Spoof LAN TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No

Apply

Per configurare le impostazioni della connessione WAN:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > WAN > Internet Connection (Connessione ad Internet)**.
2. Configurate le seguenti impostazioni. Quando avete finito cliccate su **Apply (Applica)**.
 - **Tipo di connessione WAN:** Scegliete il protocollo di connessione ad Internet in base alle indicazioni del vostro ISP. Le scelte sono le seguenti: **IP automatico, PPPoE, PPTP, L2TP** o **IP statico**. Contattate il vostro ISP nel caso in cui il vostro router non riuscisse ad ottenere un indirizzo IP valido o se non siete sicuri del tipo di connessione WAN.
 - **Abilita WAN:** Selezionate **Yes (Sì)** per permettere al router di accedere ad Internet. Selezionate **No** per impedirlo.
 - **Abilita NAT:** Il servizio NAT (Network Address Translation) prevede che un unico indirizzo IP pubblico (WAN) possa essere usato per condividere l'accesso ad Internet a diversi client presenti nella rete locale (LAN) assegnando a ciascuno di essi un indirizzo IP privato. L'indirizzo IP privato di ogni client della rete locale è salvato in una tabella di NAT ed è usato per instradare i pacchetti di dati in entrata.
 - **Abilita UPnP:** Il protocollo UPnP (Universal Plug and Play) permette a diversi dispositivi (come router, televisioni, sistemi stereo, console di gioco e telefoni cellulari) di essere controllati all'interno di una rete IP con, o senza, il bisogno di un controller centrale come potrebbe essere un gateway. UPnP connette PC di vario tipo fornendo funzionalità di rete per la configurazione remota e il trasferimento dati. Usando UPnP un nuovo dispositivo di rete viene rilevato automaticamente. Una volta collegati in rete i dispositivi possono essere configurati da remoto per supportare applicazioni P2P (peer-to-peer), gioco online, video conferenze e server proxy o web. A differenza del Port Forwarding, il quale richiede la configurazione manuale delle porte, UPnP configura automaticamente il router ad accettare le connessioni in ingresso e indirizzare le richieste ad un PC specifico sulla rete locale.

- **Abilita WAN Aggregation:** WAN Aggregation permette di combinare due connessioni di rete per raddoppiare la larghezza di banda WAN fino ad un massimo di 2 Gigabit. Collegare la porta WAN e la porta LAN 4 del router alla porta LAN del modem.
- **Connetti al Server DNS:** Ordina al router di ottenere automaticamente dall'ISP l'indirizzo IP del Server DNS. Un Server DNS è un'entità presente nella rete Internet che si occupa di tradurre gli indirizzi Internet nei corrispondenti indirizzi IP.
- **Autenticazione:** Questo campo potrebbe essere richiesto da alcuni ISP. Verificate con il vostro ISP e compilate questo campo se necessario.
- **Nome Host:** Questo campo vi permette di inserire un Nome Host per il vostro router. Di solito è un requisito speciale richiesto da alcuni ISP. Se il vostro ISP ha assegnato un Nome Host al vostro computer dovete inserirlo qui.
- **Indirizzo MAC:** L'indirizzo MAC (Media Access Control) è un codice identificativo unico per ogni interfaccia di rete. Alcuni ISP controllano gli indirizzi MAC dei dispositivi di rete che tentano di connettersi al loro servizio e rifiutano ogni richiesta proveniente da dispositivi di cui non sono a conoscenza. Per evitare problemi di questo tipo dovuti a indirizzi MAC non registrati potete:
 - Contattare il vostro ISP e aggiornare l'elenco degli indirizzi MAC associati al vostro servizio.
 - Clonare o modificare l'indirizzo MAC del vostro router ASUS in modo che sia uguale all'indirizzo MAC del vostro precedente router.

3.11.2 WAN duale

Dual WAN (WAN duale) permette di selezionare due connessioni ISP diverse per il router, una WAN primaria e una WAN secondaria.

Per configurare Dual WAN:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > WAN**.
2. Nel campo **Dual WAN (WAN duale)** spostate il cursore su **ON**.
3. Selezionate la **Primary WAN (WAN primaria)** e la **Secondary WAN (WAN secondaria)**. Sono disponibili due WAN/LAN da 2,5 GbE per le opzioni.
4. Selezionate tra le modalità **Fail Over** o **Load Balance (Bilanciamento del carico)**.
5. Cliccate su **Apply (Applica)**.

NOTA: Nelle domande frequenti (FAQ) sul sito di supporto ASUS <https://www.asus.com/it/support/FAQ/1011719/> potete trovare una spiegazione dettagliata che vi aiuterà ad usare questa funzione in modo adeguato.

The screenshot shows the 'WAN - Dual WAN' configuration page. At the top, there is a title 'WAN - Dual WAN' and a descriptive paragraph: 'ZenWiFi BD4 provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connections. [Dual WAN FAQ](#)'. Below this is a 'Basic Config' section with a toggle for 'Enable Dual WAN' set to 'OFF' and a dropdown for 'Primary WAN' set to 'WAN'. The 'Auto Network Detection' section includes a note: 'Detailed explanations are available on the [ASUS Support Site FAQ](#), which may help you use this function effectively.' It contains three rows: 'Detect Interval' set to 'Every 3 seconds', 'Internet Connection Diagnosis' with a note 'When the current WAN fails 2 continuous times, it is deemed a disconnection.', and 'Network Monitoring' with checkboxes for 'DNS Query' and 'Ping'. An 'Apply' button is at the bottom.

WAN - Dual WAN	
ZenWiFi BD4 provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connections. Dual WAN FAQ	
Basic Config	
Enable Dual WAN	<input type="checkbox"/> OFF
Primary WAN	WAN
Auto Network Detection	
Detailed explanations are available on the ASUS Support Site FAQ , which may help you use this function effectively.	
Detect Interval	Every 3 seconds
Internet Connection Diagnosis	When the current WAN fails 2 continuous times, it is deemed a disconnection.
Network Monitoring	<input type="checkbox"/> DNS Query <input type="checkbox"/> Ping
Apply	

3.11.3 Port Trigger

Il trigger di un intervallo di porte apre una porta in ingresso predeterminata per un periodo di tempo limitato quando un client della rete locale fa una richiesta di connessione in uscita relativamente ad una porta specifica. Il Port Trigger si usa nei seguenti casi:

- Diversi client della rete locale hanno bisogno di port forwarding per la stessa applicazione contemporaneamente.
- Un'applicazione richiede una specifica porta in ingresso diversa dalla porta in uscita.

WAN - Port Trigger

Port Trigger allows you to temporarily open data ports when LAN devices require unrestricted access to the Internet. There are two methods for opening incoming data ports: port forwarding and port trigger. Port forwarding opens the specified data ports all the time and devices must use static IP addresses. Port trigger only opens the incoming port when a LAN device requests access to the trigger port. Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows multiple devices to share a single open port and port trigger only allows one client at a time to access the open port.

[Port Trigger FAQ](#)

Basic Config

Enable Port Trigger Yes No

Well-Known Applications

Trigger Port List (Max Limit : 32)

Description	Trigger Port	Protocol	Incoming Port	Protocol	Delete
No data in table.					

Per configurare il Port Trigger:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > WAN > Port Trigger**.
2. Configurate le seguenti impostazioni. Quando avete finito cliccate su **Apply (Applica)**.
 - **Abilita Port Trigger:** Selezionate **Yes (Sì)** per abilitare il Port Trigger.
 - **Applicazioni Comuni:** Selezionate giochi e servizi web comuni da aggiungere all'elenco di Port Trigger.
 - **Descrizione:** Inserite un nome o una descrizione del servizio.
 - **Porta Trigger:** Specificate la porta trigger che intendete usare.
 - **Protocollo:** Selezionate il protocollo, TCP o UDP.

- **Porta in ingresso:** Inserite una porta in ingresso per ricevere traffico in ingresso da Internet.
-

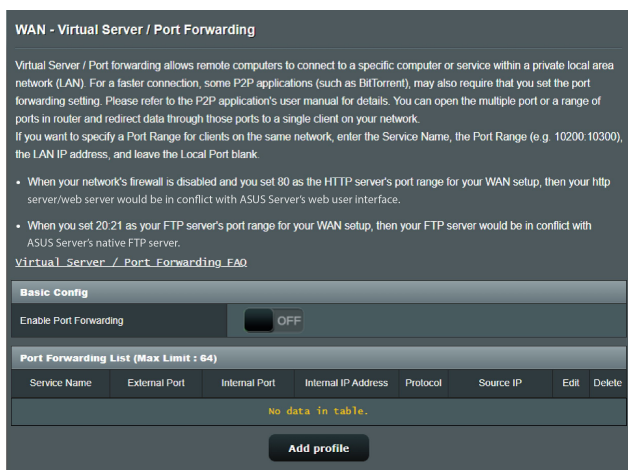
NOTE:

- Quando vi connettete ad un server IRC un PC client stabilisce una connessione in uscita usando l'intervallo di porte trigger 6666-7000. Il server IRC risponde verificando il nome utente e creando una nuova connessione verso il PC client usando una porta in ingresso.
 - Se il Port Trigger è disabilitato il router chiude la connessione perché non è in grado di stabilire quale PC stia richiedendo accesso al servizio IRC. Quando il Port Trigger è abilitato il router assegna una porta in ingresso al client per ricevere il traffico in ingresso. La porta in ingresso viene chiusa dopo che è passato un determinato periodo di tempo perché il router non è a conoscenza di quando l'applicazione è stata chiusa.
 - Il Port Triggering permette solo ad un client della rete di usare un particolare servizio tramite una particolare porta in un periodo di tempo specifico.
 - Non potete usare la stessa applicazione per attivare una porta in più di un PC allo stesso momento. La porta sarà inoltrata solamente all'ultimo client che ha mandato al router una richiesta di trigger.
-

3.11.4 Virtual Server/Port Forwarding

Il Port Forwarding è un metodo per dirigere il traffico di rete da Internet ad una porta specifica, o ad un intervallo specifico di porte, verso un client della vostra rete locale. Il servizio di Port Forwarding permette ai PC all'esterno della vostra rete locale di accedere a servizi specifici forniti da un PC all'interno della vostra rete locale.

NOTA: Quando il Port Forwarding è abilitato il router ASUS blocca il traffico non richiesto proveniente da Internet e permette l'ingresso solamente alle risposte relative alle richieste in uscita provenienti dalla LAN. Il client di rete non ha accesso direttamente a Internet e viceversa.



Per configurare il Port Forwarding:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > WAN > Virtual Server / Port Forwarding**.
2. Configurate le seguenti impostazioni. Quando avete finito selezionate **ON**.
 - **Abilita port forwarding:** Spostate il cursore su **ON** per abilitare il Port Forwarding.
 - **Servizi più comuni:** Selezionate il tipo di servizio al quale volete accedere.

- **Giochi più comuni:** Lista dei port forwarding standard per i giochi online più diffusi.
- **Porta server FTP:** Non assegnate i valori 20 e 21 al vostro server FTP perché andrebbe in conflitto con il server FTP nativo del router.
- **Nome del servizio:** Inserite il nome del servizio.
- **Intervallo porte:** Se volete specificare un intervallo di porte per i client della stessa rete inserite il nome del servizio, l'intervallo di porte (ad esempio 10200:10300), l'indirizzo IP della LAN, e lasciate vuoto il campo Porta locale. Questo campo accetta vari formati come, ad esempio, un intervallo di porte (300:350), porte singole (566,789) o misto (1015:1024,3021).

NOTE:

- Quando il firewall di rete è disabilitato e voi selezionate la porta 80 come predefinita per il vostro server HTTP lo stesso server andrà in conflitto con l'interfaccia web di gestione del router.
- Una rete utilizza il concetto di porta in modo da scambiare dati seguendo il principio che ogni porta sia assegnata ad un servizio ben preciso. Per esempio il servizio HTTP usa la porta 80. Ogni porta può essere usata per un solo servizio alla volta. Di conseguenza, se due PC tentano di accedere ai dati attraverso la stessa porta, il processo fallirà. Quindi, ad esempio, ecco perché non potete configurare il servizio di Port Forwarding sulla porta 100 contemporaneamente per due PC della stessa rete.

-
- **IP Locale:** Inserite l'indirizzo IP locale del client.

NOTA: Assicuratevi che il client disponga di un indirizzo IP statico per fare in modo che il port-forwarding funzioni correttamente. Fate riferimento alla sezione 3.8 LAN per maggiori informazioni.

- **Porta locale:** Inserite una porta specifica per ricevere i pacchetti inoltrati. Lasciate vuoto questo campo se volete che i pacchetti siano diretti al range specifico di porte.
- **Protocollo:** Selezionate il protocollo. Se non siete sicuri selezionate **BOTH (ENTRAMBI)**.

Per controllare che il Port Forwarding sia configurato correttamente:

- Assicuratevi che il vostro server, o l'applicazione, siano avviati e operativi.
- Avete bisogno di un client al di fuori della vostra rete LAN (Internet client). Questo client non deve essere connesso al router ASUS.
- Dall'Internet client usate l'indirizzo IP pubblico (WAN) del router per accedere al servizio. Se il port forwarding è stato configurato correttamente dovreste essere in grado di accedere ai file e alle applicazioni.

Differenze tra port trigger e port forwarding:

- Il Port Trigger funziona anche senza bisogno di inserire un indirizzo IP LAN specifico. A differenza del port forwarding, il quale richiede un indirizzo IP statico sulla LAN, il port trigger permette un reindirizzamento dinamico. Range di porte predeterminati sono configurati per accettare connessioni in ingresso per un breve periodo di tempo. Il port trigger permette a diversi computer di accedere a programmi che, normalmente, richiederebbero un port forwarding manuale per ogni client della rete.
- Il port trigger è più sicuro del port forwarding dal momento che le porte in ingresso non sono aperte in modo continuo. Le porte vengono aperte solamente quando l'applicazione stabilisce una connessione in uscita attraverso la porta di trigger.

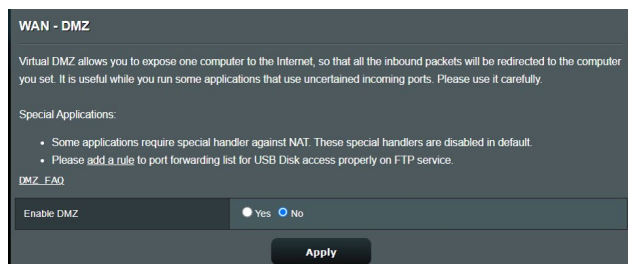
3.11.5 DMZ

Il servizio DMZ espone un client della rete direttamente ad Internet permettendogli di ricevere tutti i pacchetti in entrata diretti alla vostra rete locale.

Il traffico in ingresso, di solito, è diretto ad un client specifico della rete solamente se una regola di port-forwarding per una specifica porta è stata configurata sul router, altrimenti viene scartato. In una configurazione DMZ uno specifico client della rete riceve tutti i pacchetti in ingresso.

La configurazione DMZ è utile quando si ha bisogno di avere le porte in ingresso aperte verso l'esterno perché, ad esempio, si intende ospitare un server di dominio, web o email.

ATTENZIONE: L'apertura di tutte le porte in ingresso verso un client rende la rete locale vulnerabile agli attacchi dall'esterno. Siate quindi consapevoli dei rischi a cui andate incontro se decidete di usare il servizio DMZ.



Per configurare DMZ:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > WAN > DMZ**.
2. Configurate le seguenti impostazioni. Quando avete finito cliccate su **Apply (Applica)**.
 - **Indirizzo IP del client bersaglio:** Inserite l'indirizzo IP (relativo alla rete locale) del client per il quale volete attivare il servizio DMZ in modo da esporlo alla rete Internet. Assicuratevi che il client disponga di un indirizzo IP statico.

Per disabilitare DMZ:

1. Eliminate l'indirizzo IP del client dalla casella di testo **IP Address of Exposed Station (Indirizzo IP del client bersaglio)**.
2. Quando avete finito cliccate su **Apply (Applica)**.

3.11.6 DDNS

Configurando il servizio DNS dinamico (DDNS) avrete la possibilità di accedere al router dall'esterno della vostra rete. Potete scegliere di usare il servizio ASUS DDNS (incluso) oppure un altro servizio DDNS.

WAN - DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

If you cannot use ASUS DDNS services, please go to <https://iplookup.asus.com/nslookup.php> to reach your internet IP address to use this service.

The wireless router currently uses a private WAN IP address.
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.

The host name is successfully registered. You can use "[hostname].asuscomm.com" to access the service in home network from WAN. Use "[hostname].asuscomm.com" to remotely access your network.
Go to Advanced Settings > WAN to configure the port forwarding or DMZ settings to allow other WAN clients to remotely access your network.
If you want to remotely configure the wireless router, go to [here](#).

Enable the DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No
Server	WWW.ASUS.COM <input type="button" value="Deregister"/>
Host Name	A8878A175D4A6FD5402E68D6195D65EF7 <small>asuscomm.com</small>
DDNS Status	Active
DDNS Registration Result	Registration is successful.
HTTPS/SSL Certificate	<input type="radio"/> Free Certificate from Let's Encrypt <input type="radio"/> Import Your Own Certificate <input checked="" type="radio"/> None

Per configurare un DNS Dinamico:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > WAN > DDNS Dinamico**.
2. Configurate le seguenti impostazioni. Quando avete finito cliccate su **Apply (Applica)**.
 - **Enable the DDNS Client (Abilita il client DDNS):** Abilita l'accesso al router ASUS dall'esterno tramite nome DNS piuttosto che per indirizzo IP pubblico.
 - **Server and Host Name (Server e Nome Host):** Scegliete ASUS DDNS o un altro DDNS. Se volete usare ASUS DDNS inserite il Nome Host nel formato xxx.asuscomm.com (dove xxx è il vostro Nome Host).
 - Se volete usare un servizio DDNS diverso selezionatelo dall'elenco, cliccate su Free Trial (Prova gratuita) e registratevi online prima di usare il servizio. Compilate i campi Nome utente o Indirizzo email e Password o chiave DDNS.

- **Enable wildcard (Abilita wildcard):** Abilitate le wildcard (metacaratteri) se il vostro server DNS Dinamico lo richiede.

NOTE:

Il server DNS Dinamico non funzionerà nei seguenti casi:

- Quando il router usa come indirizzo pubblico (WAN) un indirizzo IP destinato alle reti private (192.168.x.x, 10.x.x.x, or 172.16.x.x) come indicato dalla scritta in giallo.
 - Il router si trova in una rete che usa NAT multipli.
-

3.11.7 NAT Passthrough

Il NAT Passthrough permette alla connessione VPN di passare attraverso i router e arrivare ai clienti di rete. Le modalità PPTP Passthrough, L2TP Passthrough, IPsec Passthrough e RTSP Passthrough sono abilitate di default.

Per abilitare / disabilitare le funzionalità NAT Passthrough andate su **Advanced Settings (Opzioni avanzate) > WAN > NAT Passthrough**. Quando avete finito cliccate su **Apply (Applica)**.

WAN - NAT Passthrough	
Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.	
PPTP Passthrough	Enable ▾
L2TP Passthrough	Enable ▾
IPsec Passthrough	Enable ▾
RTSP Passthrough	Enable ▾
H.323 Passthrough	Enable ▾
SIP Passthrough	Enable ▾
PPPoE Relay	Disable ▾
FTP ALG port	2021

Apply

3.12 Wireless

3.12.1 WPS

WPS (Wi-Fi Protected Setup) è uno standard di sicurezza wireless che vi permette di collegare facilmente i vostri dispositivi alla rete wireless. Potete configurare WPS tramite un codice PIN o con il pulsante WPS.

NOTA: Assicuratevi che i dispositivi supportino WPS.

Wireless - WPS

WPS (WiFi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS button.

Enable WPS	<input checked="" type="checkbox"/> ON
Current Frequency	2.4 GHz
Connection Status	Idle
Configured	<input checked="" type="checkbox"/> Enabled <small>Pressing the reset button resets the network name (SSID) and WPA encryption key.</small>
AP PIN Code	51246044

You can easily connect a WPS client to the network in either of these two ways:

- Method1: Click the WPS button on this interface (or press the physical WPS button on the router), then press the WPS button on the client's WLAN adapter and wait for about three minutes to make the connection.
- Method2: Start the client WPS process and get the client PIN code. Enter the client's PIN code on the Client PIN code field and click Start. Please check the user manual of your wireless client to see if it supports the WPS function. If your wireless client does not support the WPS function, you have to configure the wireless client manually and set the same network Name (SSID), and security settings as this router.

WPS Method: Push button Client PIN Code

Start

Per abilitare il WPS sulla vostra rete wireless:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Wireless > WPS**.
2. Nel campo **Enable WPS (Abilita WPS)** spostate il cursore su **ON**.
3. WPS utilizza la frequenza predefinita 2.4 GHz. Se volete cambiare la frequenza scegliendo 5 GHz spostate il cursore su **OFF**, cliccate su **Switch Frequency (Cambia frequenza)** e spostate nuovamente il cursore su **ON**.

NOTA: WPS supporta autenticazione tramite Open System, WPA-Personal e WPA2-Personal. WPS non supporta una rete wireless che usa una metodi di cifratura a chiave condivisa, WPA-Enterprise, WPA2-Enterprise e RADIUS.

4. Nel campo **WPS Method (Modalità WPS)** selezionate **Push Button (Premi Pulsante)** o **Client PIN Code (Codice PIN client)**. Se selezionate **Push Button (Premi Pulsante)** andate al passaggio 5. Se selezionate **Client PIN Code (Codice PIN client)** andate al passaggio 6.
5. Per impostare il WPS usando il pulsante WPS del router procedete nel modo seguente:
 - a. Cliccate su **Start (Avvia)** o premete il pulsante WPS che trovate nella parte posteriore del router wireless.
 - b. Premete il pulsante WPS sul vostro dispositivo wireless. Di solito questo pulsante è identificato dal logo WPS.

NOTA: Controllate il vostro dispositivo wireless, o il relativo manuale utente, per verificare la posizione del pulsante WPS.

- c. Il router wireless cercherà i dispositivi WPS disponibili. Se il router wireless non trova nessun dispositivo WPS entrerà in standby.
6. Per impostare il WPS usando il codice PIN client procedete nel modo seguente:
 - a. Individuate il codice PIN WPS sul manuale utente del vostro dispositivo wireless o sul dispositivo stesso.
 - b. Inserite il codice PIN client nella casella di testo relativa.
 - c. Cliccate su **Start (Avvia)** per dire al router di entrare in modalità rilevamento WPS. Gli indicatori LED del router lampeggiano velocemente per tre volte fino a quando la configurazione WPS è completata.

3.12.2 Bridge

La modalità Bridge, o WDS (Wireless Distribution System), permette al vostro router wireless di connettersi ad un altro access point wireless in maniera più o meno esclusiva impedendo ad altri dispositivi wireless, o stazioni, di connettersi al vostro router wireless ASUS. In alternativa, il router wireless, si può comportare come repeater wireless. In questo caso il router wireless ASUS comunicherà con un altro access point wireless e con altri dispositivi wireless (ibrido).

Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your ASUS Router to connect to an access point wirelessly. WDS may also be considered a repeater mode.

Note:

The function only support [Open System/NONE, Open System/WEF] security authentication method. To set up the corresponding authentication method, please select Legacy as your wireless mode first. [Click Here](#) to modify. Please refer to this [FAQ](#) for more details.

To enable WDS to extend the wireless signal, please follow these steps :

1. Select [WDS Only] or [Hybrid] mode and add MAC address of APs in Remote AP List.
2. Ensure that this wireless router and the AP you want to connect to use the same channel.
3. Key in the remote AP mac in the remote AP list and open the remote AP's WDS management interface, key in the this router's MAC address.
4. To get the best performance, please go to Advanced Settings > Wireless > General and assign the same channel bandwidth, control channel, and extension channel to every router in the network.

You are currently using the Auto channel bandwidth. [Click here](#) to modify.

You are currently using the Auto channel. [Click here](#) to modify.

Basic Config

2.4 GHz MAC	<input type="text" value="C8:7F:54:12:69:C8"/>
5 GHz MAC	<input type="text" value="C8:7F:54:12:69:CC"/>
Band	<input type="text" value="2.4 GHz"/>
AP Mode	<input type="text" value="AP Only"/>
Connect to APs in list	<input checked="" type="radio"/> Yes <input type="radio"/> No

Remote AP List (Max Limit : 4)

Remote AP List	Add / Delete
<input type="text" value=""/>	<input type="button" value="+"/>
No data in table.	

Per configurare il bridge wireless:


1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Wireless > WDS**.
2. Selezionate la banda di frequenza per il bridge wireless.
3. Nel campo **AP Mode (Modalità AP)** selezionate una delle seguenti opzioni:

- **AP Only (Solo WDS):** Disabilita la funzionalità Bridge Wireless.
- **WDS Only (Solo WDS):** Abilita la funzionalità Bridge Wireless ma impedisce agli altri dispositivi/stazioni di connettersi al router.
- **IBRIDO:** Abilita la funzionalità Bridge Wireless e permette ad altri dispositivi/stazioni wireless di connettersi al router.

NOTA: Nella modalità **IBRIDO** i dispositivi wireless connessi al router wireless ASUS riceveranno solamente metà della banda disponibile dell'Access Point.

4. Nel campo **Connect to APs in list (Connetti ad AP nell'elenco)** selezionate **Yes (Sì)** se volete connettervi ad un Access Point presente nell'elenco degli AP remoti.
5. Nel campo **Control Channel (Canale di controllo)** selezionate il canale operativo per il bridge wireless. Selezionate **Auto (Automatico)** per permettere al router di scegliere automaticamente il canale con la minore interferenza possibile.

NOTA: La disponibilità dei canali wireless varia in base al Paese o alla regione.

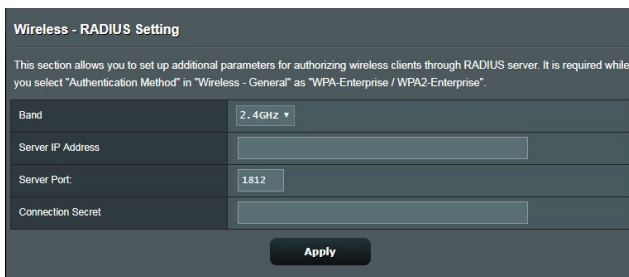
6. In **Elenco AP remoti** inserite un indirizzo MAC e cliccate sul pulsante **Add (Aggiungi)**  per inserire l'indirizzo MAC di altri Access Point disponibili.

NOTA: Ogni Access Point aggiunto alla lista deve essere configurato sullo stesso canale di controllo del router wireless ASUS.

7. Cliccate su **Apply (Applica)**.

3.12.3 Impostazioni RADIUS

Il servizio RADIUS (Remote Authentication Dial In User Service) fornisce un ulteriore livello di sicurezza nel caso si siano selezionate le modalità di autenticazione WPA-Enterprise, WPA2-Enterprise o Radius 802.1x.



Wireless - RADIUS Setting	
This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".	
Band	2.4GHz ▾
Server IP Address	<input type="text"/>
Server Port	1812
Connection Secret	<input type="text"/>
Apply	

Per configurare le impostazioni wireless RADIUS:

1. Assicuratevi che la modalità di autenticazione wireless del router sia impostata su WPA-Enterprise, WPA2-Enterprise o Radius with 802.1x.
2. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Wireless** e selezionate la scheda **RADIUS Setting (Impostazioni RADIUS)**.
3. Selezionate la frequenza.
4. Nel campo **Server IP Address (Indirizzo IP server)** inserite l'indirizzo IP del server RADIUS.
5. Nel campo **Connection Secret** inserite la password per accedere al server RADIUS.
6. Cliccate su **Apply (Applica)**.

3.12.4 Professionale

La schermata Professionale fornisce opzioni di configurazione avanzata.

NOTA: Vi raccomandiamo di utilizzare i valori predefiniti per questa pagina.

Wireless - Professional	
Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.	
Band	2.4 GHz
Enable Radio	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable wireless scheduler	<input checked="" type="radio"/> Yes <input type="radio"/> No
Set AP Isolated	<input checked="" type="radio"/> Yes <input type="radio"/> No
Roaming assistant	Enable Disconnect clients with RSSI lower than : -70 dBm
Bluetooth Coexistence	Disable
Enable IGMP Snooping	Enable
Multicast Rate(Mbps)	Auto
Preamble Type	Long
AMPDU RTS	Enable
RTS Threshold	2347
DTIM Interval	1
Beacon Interval	100
Enable TX Bursting	Enable
Enable WMM	Enable
Enable WMM No-Acknowledgement	Disable
Enable WMM APSD	Enable
Optimize AMPDU aggregation	Disable
Modulation Scheme	Up to MCS 11 (VHTroQAM/1024-QAM)
Airtime Fairness	Disable
Multi-User MIMO	Enable
OFDMA/802.11ax MU-MIMO	Disable
Explicit Beamforming	Enable
Universal Beamforming	Enable
Tx power adjustment	<input type="range"/> Performance
Apply	

Nella schermata **Professional (Professionale)** potete configurare le seguenti opzioni:

- **Band:** Selezionate la banda di frequenza.
- **Enable Radio (Abilita WiFi):** Selezionate **Yes (Sì)** per abilitare la rete wireless. Selezionate **No** per disabilitarla.

- **Enable wireless scheduler (Abilita programmatore wireless):** Potete selezionare un formato per l'orologio tra 24-ore o 12-ore. Il colore di una casella indica se in quell'ora la rete wireless è attiva o disattiva. Cliccate su ciascuna casella per modificare le impostazioni di ciascun ora della settimana, cliccate su **OK** quando avete finito.

Wireless - Professional

* Reminder: The System time zone is different from your locale setting.

Clock Format: 24-hour ▾ Allow Deny

Active Schedule

System Time: Thu, Aug 23 06:59:27 2018

Select All	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00 ~ 01							
01 ~ 02							
02 ~ 03							
03 ~ 04							
04 ~ 05							
05 ~ 06							
06 ~ 07							
07 ~ 08							
08 ~ 09							
09 ~ 10							
10 ~ 11							
11 ~ 12							
12 ~ 13							
13 ~ 14							
14 ~ 15							
15 ~ 16							
16 ~ 17							
17 ~ 18							
18 ~ 19							
19 ~ 20							
20 ~ 21							
21 ~ 22							
22 ~ 23							
23 ~ 24							

Cancel OK

- **Set AP isolated (Imposta Isolamento AP):** L'opzione **Imposta Isolamento AP** impedisce ai dispositivi wireless della vostra rete di comunicare tra di loro. Questa caratteristica è utile se molti dispositivi diversi accedono e lasciano la vostra rete di frequente. Selezionate **Yes (Sì)** per abilitare questa funzione, **No** per disabilitarla.
- **Multicast rate (Mbps) (Velocità multicast (Mbps)):** Selezionate la velocità del multicast o **Disable (Disabilita)** se volete impedire le trasmissioni singole simultanee.

- **Preamble Type (Tipo di preambolo):** Definisce quanto tempo deve spendere il router per il controllo CRC (Cyclic Redundancy Check). CRC è un metodo che si occupa di rilevare gli errori durante la trasmissione di dati. Selezionate **Short (Corto)** per una rete wireless molto frequentata con elevato traffico di rete. Selezionate **Long (Lungo)** se la vostra rete wireless è frequentata da dispositivi wireless datati.
- **RTS Threshold (Soglia RTS):** Un valore più basso di Soglia RTS (Request to Send) migliorerà la comunicazione wireless in una rete affollata e con elevato traffico di rete.
- **Intervallo DTIM:** L'intervallo DTIM (Delivery Traffic Indication Message) è l'intervallo di tempo che passa prima dell'invio di un segnale di risveglio, verso un dispositivo wireless che è in sospensione, per indicare che un pacchetto di dati sta aspettando per la consegna. Il valore standard è di 3 millisecondi.
- **Beacon Interval (Intervallo Beacon):** L'intervallo Beacon è il periodo di tempo che passa tra due segnali DTIM consecutivi. Il valore standard è di 100 millisecondi. Abbassate il valore dell'intervallo Beacon nel caso di rete wireless instabile o per dispositivi in roaming.
- **Enable TX Bursting (Abilita TX Burst):** Migliora la velocità di trasferimento tra il router wireless e i dispositivi 802.11g.
- **Enable WMM APSD (Abilita APSD WMM):** Abilitate la funzione APSD WMM (Wi-Fi Multimedia Automatic Power Save Delivery) per migliorare la gestione dell'energia, e della banda, nei confronti di dispositivi wireless compatibili. Selezionate **Disable (Disabilita)** per disattivare APSD WMM.

4 Utility

4.1 Device Discovery

Device Discovery è un'utility ASUS WLAN che vi permette di localizzare il router wireless ASUS e configurarne le impostazioni della rete wireless.

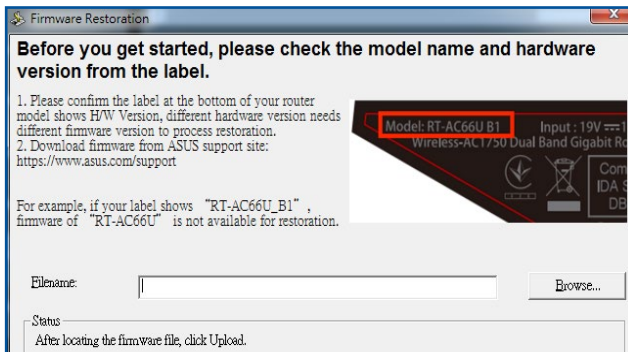
Per lanciare l'utility Device Discovery:

- Dal Desktop di Windows® cliccate su **Start > All Programs (Tutti i programmi) > ASUS Utility > ASUS Wireless Router > Device Discovery.**

NOTA: Quando impostate il router in modalità Access Point avete bisogno di usare Device Discovery per ottenere l'indirizzo IP del router.

4.2 Firmware Restoration

Firmware Restoration si usa su un router wireless ASUS quando l'aggiornamento del firmware è fallito. Questo carica il firmware che voi stessi specificate. L'intero processo può durare dai tre ai quattro minuti.



IMPORTANTE! Lanciate la modalità di recupero prima di eseguire l'utility Firmware Restoration.

NOTA: Questa caratteristica non è supportata in Mac OS.

Per lanciare la modalità di recupero e eseguire l'utility Firmware Restoration:

1. Scollegate il router dalla sorgente di alimentazione.
2. Tenete premuto il pulsante di reset che trovate sul pannello posteriore e, contemporaneamente, collegate il cavo di alimentazione. Rilasciate il pulsante di reset quando il LED di alimentazione sul pannello anteriore lampeggia lentamente. Questo indica che il router è in modalità di recupero.
3. Assegnate un indirizzo IP statico al vostro computer e usate le seguenti istruzioni per configurare le vostre impostazioni TCP/IP:

Indirizzo IP: 192.168.1.x

Maschera di sottorete: 255.255.255.0

4. Dal desktop cliccate su **Start > Tutti i programmi > ASUS Utility > Wireless Router > Firmware Restoration**.
5. Selezionate il file specifico e poi cliccate su **Upload (Carica)**.

NOTA: Questo non è un programma per l'aggiornamento del firmware e non può essere utilizzato su un router wireless ASUS funzionante. I normali aggiornamenti del firmware devono essere fatti attraverso l'interfaccia web. Fate riferimento al *Capitolo 3: Configurare le impostazioni generali e avanzate* per maggiori dettagli.

5 Risoluzione dei problemi

Questo capitolo fornisce soluzioni a vari problemi che potrebbero verificarsi durante il normale utilizzo del router. Se incontrate un problema che non è menzionato in questo capitolo visitate il sito di supporto ASUS al seguente indirizzo:

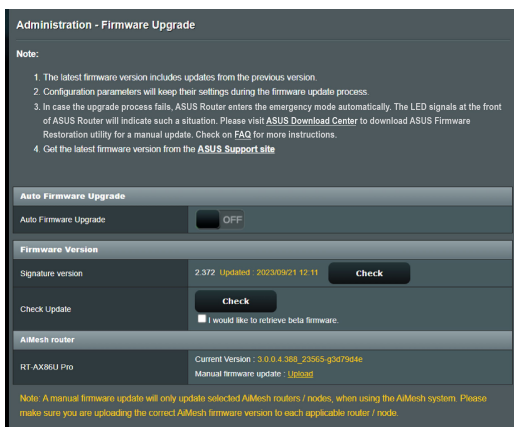
<https://www.asus.com/it/support> per avere maggiori informazioni e per ottenere i contatti del supporto tecnico ASUS.

5.1 Risoluzione dei problemi più comuni

Se andate incontro a problemi con il vostro router provate a seguire questi semplici passi prima di cercare altre soluzioni.

Aggiornate il firmware all'ultima versione.

1. Aprite l'interfaccia web. Andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione) > Firmware Upgrade (Aggiornamento firmware)**. Cliccate sul pulsante **Check (Controlla)** per verificare la presenza di aggiornamenti disponibili.



2. Se un nuovo firmware è disponibile visitate il sito: <https://www.asus.com/Networking/ZenWiFi BD4/HelpDesk/> per ottenere il firmware aggiornato.
3. Dalla pagina **Firmware Version (Versione del firmware)** cliccate su **Check (Controlla)** per cercare il file del firmware che avete appena scaricato.
4. Cliccate su **Upload (Carica)** per aggiornare il firmware.

Riavvio della rete:

1. Spegnete il modem.
2. Scollegate il modem dalla rete.
3. Spegnete il router e i computer.
4. Collegate il modem.
5. Accendete il modem e aspettate 2 minuti.
6. Accendete il router e aspettate 2 minuti.
7. Accendete i computer.

Controllate che le impostazioni wireless del vostro computer siano uguali a quelle del router.

- Quando collegate il vostro computer al router tramite rete wireless assicuratevi che il SSID, l'encryption method (metodo di cifratura) e la password siano corretti.

Assicuratevi che le vostre impostazioni di rete siano corrette.

- Ogni client sulla rete deve avere un indirizzo IP valido. ASUS raccomanda di usare il server DHCP del router wireless per assegnare automaticamente gli indirizzi IP ai computer della vostra rete.

- Alcuni fornitori di connessione dati via cavo potrebbero richiedere che l'indirizzo MAC del vostro computer sia registrato con il vostro utente prima di permettere la connessione. Potete visualizzare il vostro indirizzo MAC dall'interfaccia web andando su **Network Map > Clients** e posizionando il puntatore sul vostro dispositivo nella sezione **Client Status (Stato client)**.

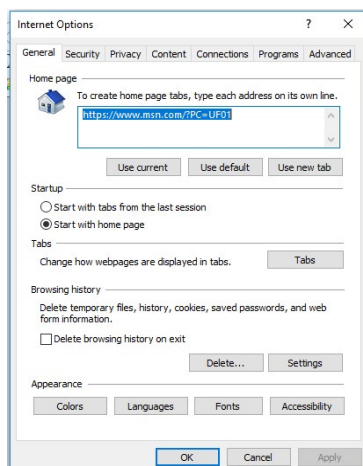


5.2 Domande e risposte frequenti (FAQs)

Impossibile accedere all'interfaccia web usando il browser Internet

- Se il vostro computer è collegato via cavo controllate accuratamente la connessione del cavo e lo stato dei LED come descritto nelle sezioni precedenti.
- Assicuratevi di usare le corrette informazioni di login. Assicuratevi che il tasto "BLOCCO MAIUSCOLE" sia disattivato quando inserite il nome utente e la password.
- Rimuovete i cookie e i file temporanei dal vostro browser. Per Internet Explorer la procedura standard per rimuovere i cookie e i file temporanei è la seguente:

1. Lanciate Internet Explorer e cliccate su **Strumenti** > **Opzioni Internet**.
2. Nella scheda **Generale**, nel riquadro **Cronologia esplorazioni** cliccate su **Elimina...**, selezionate le voci **File temporanei Internet e file di siti Web** e **Cookie e dati di siti Web**, e poi cliccate su **Elimina**.



NOTE:

- La procedura per la rimozione dei cookie e dei file temporanei potrebbe variare a seconda del browser utilizzato.
- Disabilitate il server proxy, le connessioni remote e configurate le impostazioni TCP/IP in modo da ottenere un indirizzo IP automaticamente. Per maggiori informazioni fate riferimento al *Capitolo 1* di questo manuale.
- Assicuratevi di usare cavi Ethernet CAT5 o CAT6.

Il client non riesce a stabilire una connessione wireless con il router.

NOTA: Se riscontrate dei problemi nel connettervi alla rete wireless a 5Ghz assicuratevi che il vostro dispositivo wireless sia in grado di supportare i 5Ghz o le reti dual-band.

- **Fuori portata:**
 - Avvicinate il router al client wireless.
- **Il server DHCP è stato disabilitato:**
 1. Aprite l'interfaccia web. Andate su **General (Generale) > Network Map (Mappa di rete) > Clients (Client)** e cercate il dispositivo che volete connettere al router.
 2. Se non riuscite a trovare il dispositivo nella **Network Map (Mappa di rete)** andate su **Advanced Settings (Impostazioni avanzate) > LAN > DHCP Server (Server DHCP)**, posizionatevi sul riquadro **Basic Config (Configurazione di base)** e selezionate **Yes (Sì)** all'opzione **Enable the DHCP Server (Abilita il server DHCP)**.

LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the DNS server IP and default gateway IP. ASUS Router supports up to 253 IP addresses for your local network.
Manually Assigned IP around the DHCP list FAQ

Basic Config

Enable the DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
ASUS Router's Domain Name	<input type="text"/>
IP Pool Starting Address	<input type="text" value="192.168.50.2"/>
IP Pool Ending Address	<input type="text" value="192.168.50.254"/>
Lease time	<input type="text" value="86400"/>
Default Gateway	<input type="text"/>

DNS and WINS Server Setting

DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>
Advertise router's IP in addition to user-specified DNS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WINS Server	<input type="text"/>

Manual Assignment

Enable Manual Assignment	<input type="radio"/> Yes <input checked="" type="radio"/> No
--------------------------	---

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

No data in table.

- Il nome della rete (SSID) non è visibile. Se il vostro dispositivo visualizza reti disponibili provenienti da altri router, ma non la rete del vostro router, andate su **Advanced Settings (Impostazioni avanzate) > Wireless > General (Generale)**, selezionate **No** alla voce **Hide SSID (Nascondi SSID)** e selezionate **Auto (Automatico)** alla voce **Control Channel (Canale di controllo)**.

Wireless - General

Set up the wireless related information below.

Enable Smart Connect	<input type="checkbox"/> OFF
Band	2.4 GHz
Network Name (SSID)	LIAD
Hide SSID	<input type="radio"/> Yes <input checked="" type="radio"/> No
Wireless Mode	Auto <input checked="" type="checkbox"/> Big Protection <input type="checkbox"/> Disable 11b
802.11ax / WiFi 6 mode	Enable <small>If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check FAQ.</small>
WiFi Agile Multiband	Disable
Target Wake Time	Disable
Channel bandwidth	20/40 MHz
Control Channel	Auto <small>Current Control Channel: 6</small>
Extension Channel	Auto
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	***** Weak
Group Key Rotation Interval	3600

Apply

- Se state usando un adattatore per la rete wireless assicuratevi che il canale che state usando sia conforme con i canali wireless disponibili nella vostra zona. Se così non fosse correggete il canale, la sua larghezza di banda e la modalità wireless.
- Se ancora non riuscite a connettervi al router in modalità wireless potete resettare il router alle impostazioni predefinite di fabbrica. Aprite l'interfaccia web, andate su **Administration (Amministrazione)**, selezionate la scheda **Restore/Save/Upload Setting (Impostazione Ripristina/Salva/Carica)** e cliccate sul pulsante **Restore (Ripristina)**.

Administration - Restore/Save/Upload Setting

This function allows you to save current settings of ASUS Router to a file, or load settings from a file.

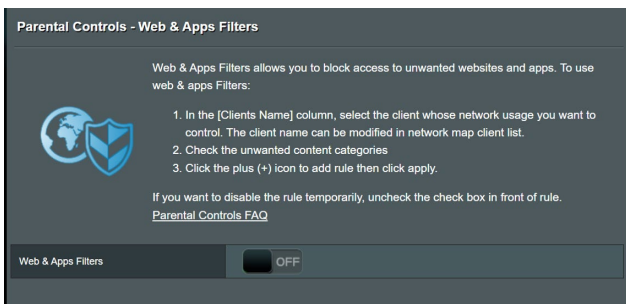
Factory default	Restore <input type="checkbox"/> Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer, and Web History.
Save setting	Save setting <input type="checkbox"/> Click on this checkbox if you want to share the config file for debugging. Since the original password in the config file will be removed, please do not import the file into your router. <input type="checkbox"/> Transfer ASUS DDNS name.
Restore setting	Upload

Nessun accesso a Internet.

- Verificate che il vostro router si possa connettere all'indirizzo IP pubblico (WAN) del vostro ISP. Per fare questo aprite l'interfaccia web e andate su **General (Generale) > Network Map (Mappa di rete)** e controllate la voce **Internet status (Stato Internet)**.
- Se il vostro router non riesce a raggiungere l'IP pubblico del vostro ISP provate a riavviare il router seguendo il procedimento consigliato nella sezione *Riavvio della rete* del paragrafo *Risoluzione dei problemi*.



- Il dispositivo è stato bloccato tramite la funzione Parental Control (Controllo Genitori). Andate sulla scheda **General (Generale) > Parental Controls (Controllo genitori)** e verificate se il dispositivo è presente nell'elenco. Se il dispositivo è nell'elenco **Client Name (Nome client)** rimuovete il dispositivo usando il pulsante **Delete (Elimina)** o modificate le impostazioni di **Time Management (Gestione tempo)**.



- Se ancora non avete accesso ad Internet provate a riavviare il computer e, in seguito, controllate il suo indirizzo IP di rete e l'indirizzo del gateway predefinito.

Avete dimenticato il nome della rete (SSID) o la chiave di protezione

- Impostate un nuovo SSID e una nuova chiave di protezione collegandovi al router tramite un cavo Ethernet. Aprite l'interfaccia web, andate su **Network Map (Mappa di rete)**, cliccate sull'icona del router, inserite un nuovo SSID e una nuova chiave di protezione e poi cliccate su **Apply (Applica)**.
- Ripristinate le impostazioni predefinite del router. Aprite l'interfaccia web, andate su **Administration (Amministrazione)**, selezionate la scheda **Restore/Save/Upload Setting (Impostazione Ripristina/Salva/Carica)** e cliccate sul pulsante **Restore (Ripristina)**.

Come faccio a ripristinare le impostazioni predefinite del router?

- Andate su **Administration (Amministrazione)**, selezionate la scheda **Restore/Save/Upload Setting (Impostazione Ripristina/Salva/Carica)** e cliccate sul pulsante **Restore (Ripristina)**.

Aggiornamento del firmware non riuscito.

Lanciate la modalità di recupero e eseguite l'utilità Firmware Restoration. Fate riferimento alla sezione *4.2 Firmware Restoration* per avere maggiori informazioni su come effettuare il recupero del firmware.

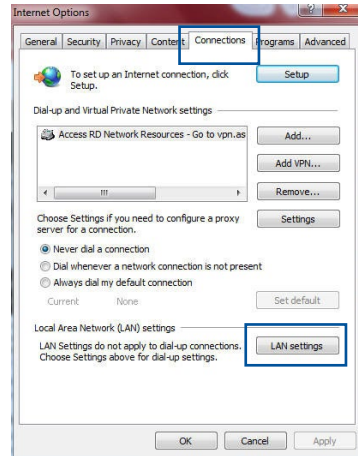
Impossibile accedere all'interfaccia web

Prima di procedere con la configurazione del router portate a termine i seguenti passaggi sul vostro computer e su eventuali altri computer presenti nella vostra rete.

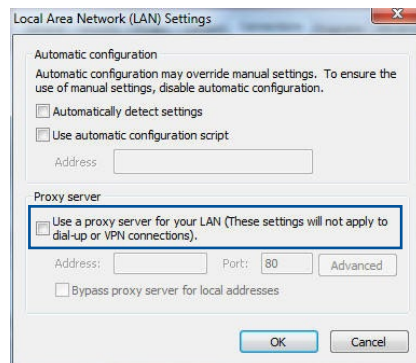
A. Disabilitate il server proxy (se abilitato).

Windows®

1. Cliccate su **Start > Internet Explorer** per aprire il browser.
2. Cliccate su **Tools (Strumenti) > Internet options (Opzioni Internet) > Connections (Connessioni)** e cliccate su **LAN settings (Impostazioni LAN)**.

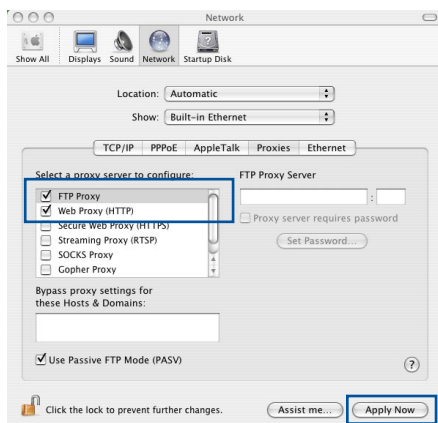


3. Dalla schermata di impostazioni della vostra LAN (Local Area Network) togliete la spunta da **Use a proxy server for your LAN (Utilizza un proxy server per le connessioni LAN)**.
4. Quando avete finito selezionate **OK**.



MAC OS

1. Dal vostro browser Safari cliccate su **Safari > Preferences (Preferenze) > Advanced (Avanzate) > Change Settings (Modifica Impostazioni)**.
2. Dal pannello **Network** togliete la spunta da **FTP Proxy (Proxy FTP)** e **Web Proxy (HTTP) (Proxy web (HTTP))**.
3. Quando avete finito selezionate **Apply Now (Applica)**.

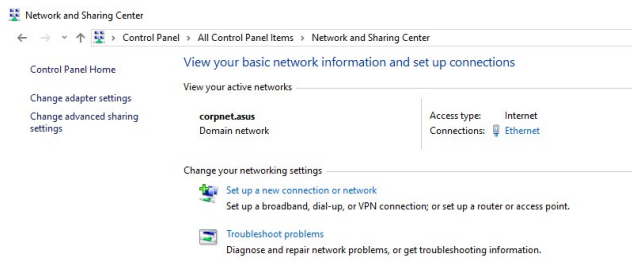


NOTA: Fate riferimento alla funzione *Aiuto* del vostro browser per dettagli su come disabilitare una connessione remota.

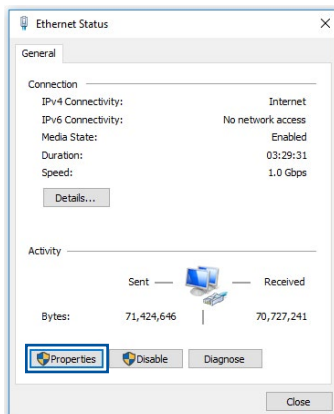
B. Configurare le impostazioni TCP/IP in modo da ottenere un indirizzo IP automaticamente.

Windows®

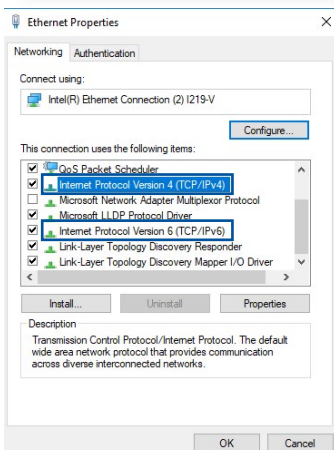
1. Cliccate su **Start > Control Panel (Pannello di controllo) > Network and Sharing Center (Centro connessioni di rete e condivisione)** quindi cliccate sulla connessione di rete per visualizzare la finestra di stato.



2. Cliccate su **Properties** (**Proprietà**) per visualizzare la finestra delle proprietà Ethernet.



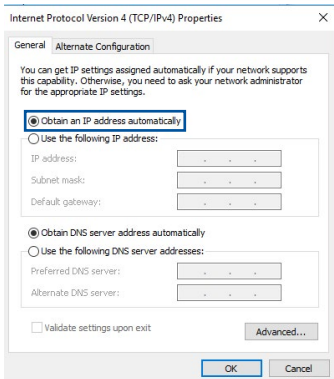
3. Selezionate **Protocollo Internet versione 4 (TCP/IPv4)** o **Internet Protocol Version 6 (TCP/IPv6)** (**Protocollo Internet versione 6 (TCP/IPv6)**) e poi cliccate su Proprietà.




4. Per ottenere automaticamente le impostazioni IPv4 selezionate **Otteni automaticamente un indirizzo IP**.

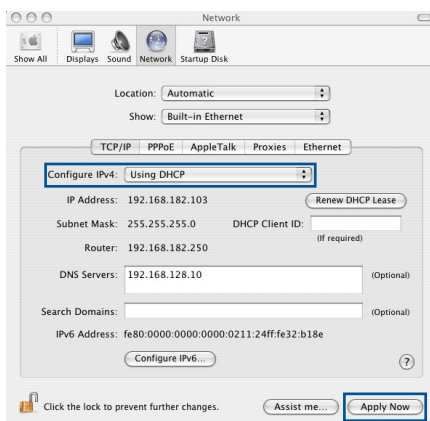
Per ottenere automaticamente le impostazioni IPv6 selezionate **Obtain an IPv6 address automatically (Ottieni automaticamente un indirizzo IPv6)**.

5. Quando avete finito selezionate **OK**.



MAC OS

1. Cliccate sull'icona della mela  sulla parte in alto a sinistra del vostro schermo.
2. Cliccate su **System Preferences (Preferenze di Sistema) > Network (Rete) > Configure... (Configura...)**.
3. Dal pannello **TCP/IP** selezionate **Using DHCP (Utilizzo di DHCP)** nell'elenco **Configure IPv4 (Configura IPv4)**.
4. Quando avete finito selezionate **Apply Now (Applica)**.

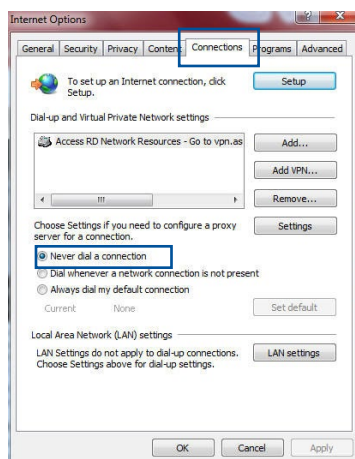


NOTA: Fate riferimento alle informazioni su aiuto e supporto del vostro sistema operativo per avere maggiori dettagli sulla configurazione delle impostazioni TCP/IP del vostro computer.

C. Disabilitate la connessione remota (se abilitata).

Windows®

1. Cliccate su **Start > Internet Explorer** per aprire il browser.
2. Cliccate su **Tools (Strumenti) > Internet options (Opzioni Internet) > Connections (Connessioni)**.
3. Selezionate la voce **Never dial a connection (Non utilizzare mai connessioni remote)**.
4. Quando avete finito selezionate **OK**.



NOTA: Fate riferimento alla sezione *Aiuto* del vostro browser per dettagli su come disabilitare una connessione remota.

Appendice

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that

any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent

access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the

Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies

to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

- 11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
- 12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Comunicazioni sulla sicurezza

Quando si utilizza questo prodotto, seguire sempre le precauzioni fondamentali di sicurezza, incluso, a titolo esemplificativo ma non esaustivo, quanto segue:



AVVERTIMENTO!

- Il cavo o i cavi di alimentazione devono essere inseriti a prese che sono dotate di un'adeguata messa a terra. Collegare l'apparecchio solo ad una presa vicina e facilmente accessibile.
 - Se l'adattatore è danneggiato non provare a ripararlo. Contattate un tecnico qualificato o il vostro rivenditore.
 - NON utilizzare cavi di alimentazione, accessori o periferiche danneggiate.
 - NON montate questo dispositivo ad un'altezza superiore a 2 metri.
 - Usa questo prodotto in ambienti la cui temperatura sia compresa tra 0°C (32°F) e 40°C (104°F).
 - Leggere le linee guida per l'uso e l'intervallo di temperature forniti prima di utilizzare il prodotto.
 - Prestare particolare attenzione alla sicurezza personale quando si utilizza questo dispositivo in aeroporti, ospedali, stazioni di servizio e officine professionali.
 - Interferenza del dispositivo medico: Mantenere una distanza minima di almeno 15 cm (6 pollici) tra i dispositivi medici impiantati e i prodotti ASUS per ridurre il rischio di interferenze.
 - Utilizzare i prodotti ASUS in buone condizioni di ricezione per ridurre al minimo il livello di radiazioni.
 - Tenere il dispositivo lontano dalla portata delle donne incinte e dal basso addome degli adolescenti.
 - NON utilizzare questo prodotto se si possono osservare difetti visibili o se è stato bagnato, danneggiato o modificato. Richiedere assistenza.
-



AVVERTIMENTO!

- Non collocare il dispositivo su superfici irregolari o instabili.
 - NON posizionare o far cadere oggetti sopra il prodotto. Evitare di esporre il prodotto a urti meccanici quali schiacciamento, piegatura, foratura o frantumazione.
 - NON smontare, aprire, mettere nel microonde, incenerire, dipingere o inserire oggetti estranei in questo prodotto.
 - Consulta l'etichetta indicante la potenza posta sul fondo del prodotto e assicurati che l'adattatore di alimentazione sia compatibile con tali valori.
 - Tenere il prodotto lontano dal fuoco e da fonti di calore.
 - NON esporre a liquidi, pioggia o umidità. NON utilizzare il prodotto durante i temporali.
 - Collegare i circuiti di uscita PoE di questo prodotto esclusivamente alle reti PoE, senza indirizzarli a strutture esterne.
 - Per prevenire il rischio di scosse elettriche scollega il cavo di alimentazione dalla presa di corrente prima di spostare il sistema.
 - Utilizzare solo accessori approvati dal produttore del dispositivo per funzionare con questo modello. L'uso di altri tipi di accessori potrebbe invalidare la garanzia o violare le normative e le leggi locali e potrebbe comportare rischi per la sicurezza. Contattare il rivenditore locale per la disponibilità degli accessori autorizzati.
 - L'uso di questo prodotto in modo non consigliato nelle istruzioni fornite potrebbe comportare il rischio di incendio o lesioni personali.
-

Servizio e supporto

Visita il nostro sito multi-lingua a <https://www.asus.com/support/>.

