



Guida Utente

Router XB432V Dual-Band Wi-Fi 7 GPON



Contents

Informazioni su questa guida.....	1
Chapter 1. Conoscere il router GPON.....	3
1. 1. Panoramica del prodotto.....	4
1. 2. Aspetto.....	5
1. 2. 1.Pannello frontale.....	5
1. 2. 2.Il pannello posteriore.....	7
Chapter 2. Collegamento dell'hardware	9
2. 1. Posizione del router GPON.....	10
2. 2. Collegare il router GPON.....	10
Chapter 3. Accedere al router GPON	14
Chapter 4. VoIP	18
4. 1. Collegamento del telefono.....	19
4. 2. Rubrica Telefonica.....	19
4. 2. 1.Rubrica Telefonica.....	19
4. 2. 2.Chiamate di emergenza.....	20
4. 3. Log Telefonate.....	21
4. 4. Blocchi di chiamata.....	22
4. 4. 1.DND (Non disturbare).....	22
4. 4. 2.Blocco di alcune chiamate.....	22
4. 4. 3.Vietare Telefonate in uscita.....	23
Chapter 5. Personalizzare le impostazioni di rete	25
5. 1. Configurare le impostazioni LAN.....	26
5. 1. 1.Modifica dell'indirizzo IP della LAN.....	26
5. 1. 2.Utilizzare il router come server DHCP.....	26
5. 1. 3.Riserva Indirizzi IP LAN.....	27
5. 2. Impostazione account del servizio DNS dinamico.....	28
5. 3. Creare Route Statiche.....	29
5. 4. Impostazioni RIP.....	31
5. 5. Impostazioni Wireless specifiche.....	32
5. 5. 1.Modificare le Impostazioni Wireless di base.....	32

5. 5. 2.	Impostazioni Wireless avanzate	36
5. 5. 3.	Visualizza le informazioni wireless	38
5. 6.	Schedulazione Wireless	39
5. 7.	Utilizzare WPS per la connessione wireless.....	40
Chapter 6. Impostazioni USB		42
6. 1.	Accesso al dispositivo di archiviazione USB	43
6. 1. 1.	Accesso al dispositivo USB in locale	43
6. 1. 2.	Accesso remoto al dispositivo USB.....	44
6. 1. 3.	Personalizzare le impostazioni di accesso	46
6. 2.	Condivisione Media.....	48
6. 3.	Impostazioni 3G/4G.....	50
Chapter 7. Rete Ospiti.....		52
7. 1.	Creare una rete per gli ospiti	53
7. 2.	Customizzare le opzioni della Rete Ospiti.....	53
Chapter 8. NAT Forwarding.....		54
8. 1.	ALG	55
8. 2.	Impostazione dei servizi pubblici sulla Rete Locale tramite Virtual Server	55
8. 3.	Aprire le porte in modo dinamico con il Port Triggering	57
8. 4.	Liberate le app dalla Restrizione Porte mediante DMZ	59
8. 5.	Per far funzionare senza problemi i giochi online di Xbox con UPnP	60
Chapter 9. Parental Control		62
Chapter 10.QoS.....		67
Chapter 11.Sicurezza		71
11. 1.	Firewall e Protezione DoS	72
11. 2.	Filtro Servizi	73
11. 3.	Controllo Accessi.....	74
11. 4.	IP e MAC Binding	76
Chapter 12.VPN Server&Client.....		78
12. 1.	Utilizzo OpenVPN per accedere alla rete domestica	79
12. 2.	Utilizzo VPN PPTP per accedere alla rete domestica.....	80
12. 3.	Utilizzo VPN IPSec per accedere alla rete domestica	84
12. 4.	Connessioni VPN	93

Chapter 13. Gestione del router GPON.....	94
13. 1. Impostare l'ora del sistema.....	95
13. 2. Controllo del LED.....	96
13. 3. Test Connettività Internet.....	96
13. 4. Aggiornare il firmware.....	97
13. 5. Backup e ripristino delle impostazioni di configurazione.....	98
13. 6. Riavvia il router GPON.....	99
13. 7. Amministrazione.....	100
13. 7. 1. Modificare la password di accesso.....	100
13. 7. 2. Gestione locale.....	101
13. 7. 3. Gestione remota.....	102
13. 7. 4. HTTP Referer Head Check.....	103
13. 7. 5. Ping ICMP.....	103
13. 7. 6. ID Sessione.....	104
13. 8. Log di Sistema.....	104
13. 9. Monitorare le statistiche del traffico Internet.....	106
FAQ	108

Informazioni su questa guida

Questa guida è un complemento della Guida rapida all'installazione.

Questa guida fornisce informazioni dettagliate su ciascuna funzione e illustra il modo in cui configurare tali funzioni in base alle proprie esigenze.

Nota: Le funzioni disponibili nel router possono variare in base alla versione software. Tutte le immagini, i passaggi e le descrizioni di questa guida sono solo esempi e potrebbero non rispecchiare l'esperienza effettiva del router.

Convenzioni

In questa guida si utilizzano le seguenti convenzioni:

Convenzione	Descrizione
<u>Sottolineato</u>	Le parole o le frasi sottolineate sono collegamenti ipertestuali. È possibile fare clic per reindirizzare a un sito web o a una sezione specifica.
Verde	I contenuti da enfatizzare e i testi della pagina web sono in verde, compresi i menu, le voci, i pulsanti, ecc.
>	Le strutture dei menu mostrano il percorso per caricare la pagina corrispondente. Ad esempio, Avanzate > Wireless > WDS significa che la pagina della funzione WDS si trova nel menu Wireless della scheda Avanzate.
🚩 Nota:	Ignorare questo tipo di nota potrebbe causare un malfunzionamento o danni al dispositivo.
🔗 Suggerimenti:	Indica informazioni importanti che aiutano a utilizzare meglio il dispositivo.
simboli sulla pagina web	<ul style="list-style-type: none">👉 Fare clic per modificare la voce corrispondente.🗑️ Fare clic per eliminare la voce corrispondente.📍 Fare clic per attivare o disattivare la voce corrispondente.🔍 Fare clic per visualizzare ulteriori informazioni sugli elementi della pagina.

Per saperne di più

La Guida rapida all'installazione si trova dove si trova questa guida o all'interno della confezione del router.

*Le velocità massime del segnale wireless sono le velocità fisiche derivate dallo standard IEEE.

Specifiche 802.11. L'effettivo throughput dei dati wireless e la copertura wireless non sono garantiti e variano in base a 1) fattori ambientali, tra cui materiali edilizi, oggetti fisici e ostacoli, 2) condizioni della rete, tra cui interferenze locali, volume e densità del traffico, ubicazione del prodotto, complessità della rete e overhead della rete e 3)

limitazioni del client, tra cui prestazioni nominali, ubicazione, connessione, qualità e condizioni del client.

*L'uso del Wi-Fi 6 (802.11ax) e di funzioni quali OFDMA, MU-MIMO, 1024-QAM e HT160 richiede che anche i client supportino le funzioni corrispondenti.

*Il risparmio energetico della batteria dei client richiede che i client supportino anche lo standard Wi-Fi 802.11ax. L'effettiva riduzione di potenza può variare in base alle condizioni di rete, alle limitazioni dei client e ai fattori ambientali.

*L'uso di WPA3 richiede che anche i client supportino la funzione corrispondente.

*Questo router potrebbe non supportare tutte le funzioni obbligatorie come ratificato nella bozza 3.0 della specifica IEEE 802.11ax.

*Potrebbero essere necessari ulteriori aggiornamenti del software per la disponibilità delle funzioni.

Capitolo 1

Conoscere il router GPON

Questo capitolo introduce le funzioni del router GPON e ne illustra l'aspetto. Il capitolo contiene le seguenti sezioni:

- [Panoramica del prodotto](#)
- [Aspetto](#)

1. 1. Panoramica del prodotto

Il router GPON di TP-Link è un dispositivo combinato di connessione di rete cablata/wireless con ONT GPON ad alta velocità, router NAT, switch a 4 porte e access point wireless, che riduce il problema della configurazione e fa risparmiare spazio.

Con una velocità di accesso downstream e upstream estremamente elevata, il router offre un'esperienza di navigazione senza precedenti.

Grazie alle porte Ethernet e alle antenne, il router fornisce accesso cablato e wireless a più computer e dispositivi mobili.

Con varie caratteristiche e funzioni, il router è lo strumento perfetto per le reti domestiche o aziendali.

Caratteristiche principali:

1. Porte Gigabit Ethernet ad alta velocità: Il router GPON è dotato di quattro porte Gigabit Ethernet, che consentono di collegare più dispositivi con connessioni cablate veloci e stabili. Godetevi uno streaming fluido, giochi online senza ritardi e trasferimenti di file efficienti.
2. Tecnologia Wi-Fi 802.11ax: Sperimentate una velocità wireless fulminea con la più recente tecnologia Wi-Fi 802.11ax. Collegate smartphone, tablet e altri dispositivi wireless per usufruire dell'accesso a Internet ad alta velocità in tutta la casa o l'ufficio.
3. Supporto Voice over IP (VoIP): Il router GPON supporta la tecnologia Voice over IP, che consente di utilizzare servizi telefonici basati su Internet. Godetevi una comunicazione vocale chiara e affidabile via Internet, eliminando la necessità di linee telefoniche tradizionali.
4. Firewall e funzioni di sicurezza integrati: La sicurezza della vostra rete è la nostra massima priorità. Il router GPON è dotato di una robusta protezione firewall integrata, che mantiene i vostri dati al sicuro da accessi non autorizzati e intrusi. Le funzioni di sicurezza avanzate, come la crittografia WPA3 e il Filtro degli indirizzi MAC, forniscono ulteriori livelli di protezione.
5. Configurazione semplice e interfaccia utente intuitiva: L'installazione del router GPON è rapida e senza problemi. La guida all'installazione, facile da seguire, vi permetterà di essere operativi in pochissimo tempo. L'interfaccia utente basata sul web è intuitiva e facile da usare e consente di configurare facilmente le impostazioni, monitorare l'utilizzo della rete e gestire i dispositivi collegati.

Il nostro router GPON vanta un design elegante e compatto, che gli consente di integrarsi perfettamente in qualsiasi ambiente domestico o di ufficio. Gli indicatori LED sul pannello frontale forniscono rapidi aggiornamenti visivi sullo stato, assicurando un facile monitoraggio e la risoluzione dei problemi.

Siamo certi che il nostro router GPON soddisferà le vostre esigenze di rete e fornirà una connessione internet affidabile. Per istruzioni dettagliate sull'installazione, la configurazione e le funzioni avanzate, consultare il presente manuale d'uso.

Nota: l'aspetto del prodotto è puramente illustrativo e potrebbe essere diverso da quello del vostro dispositivo.

1.2. Aspetto

1.2.1. Pannello frontale



I LED del router GPON (visti dall'alto verso il basso) si trovano sul pannello frontale. È possibile verificare lo stato di funzionamento del router GPON seguendo la tabella di spiegazione dei LED.

Spiegazione dei LED

LED	Stato	Indicazione
⏻ (PWP)	Blu Fisso	Il sistema si sta avviando o si è avviato con successo.
	Blu Lampeggiante	Il sistema si sta riavviando o il firmware è in fase di aggiornamento. Non scollegare o spegnere il router.
	Spento	L'alimentazione è spenta.

Spiegazione dei LED

LED	Stato	Indicazione
Φ (Fiber)	Blu Fisso	Il router è registrato presso Wind3.
	Blu Lampeggiante	Il router sta cercando di registrarsi con Wind3.
	Spento	Il dispositivo non rileva il collegamento GPON.
	Rosso Fisso	Il router non è in grado di trasmettere il segnale ottico.
⊙ (Internet)	Blu Fisso	La connessione a Internet è disponibile.
	Blu Lampeggiante	L'autenticazione è in corso.
	Rosso solido	L'autenticazione è fallita.
	Spento	Non c'è connessione a Internet o il router funziona in modalità Bridge.
□ (LAN)	Blu Fisso	Un dispositivo è collegato alla porta LAN.
	Blu Lampeggiante	La porta LAN sta trasmettendo o ricevendo dati.
	Spento	Nessun dispositivo è collegato alla porta LAN.
📶 (WIFI)	Blu Fisso	Almeno un'interfaccia radio è abilitata.
	Blu Lampeggiante lento	L'accoppiamento WPS è in corso.
	Blu Lampeggiante Veloce	I dati vengono trasmessi o ricevuti.
	Spento	Entrambe le interfacce radio 2.4 GHz e 5 GHz sono disattivate.
☎ (TELEFONO)	Blu Fisso	L'account SIP è stato registrato con successo.
	Blu Lampeggiante lento	Il telefono è agganciato e ci sono messaggi vocali.
	Blu Lampeggiante Veloce	Il telefono squilla.
	Rosso Fisso	Tutti gli account configurati e abilitati non sono registrati.
	Errore lampeggiante (1s Blu Fisso/ 1s rosso fisso)	Uno dei due account configurati non è registrato.
	Spento	Non vi è alcuna configurazione SIP.

Spiegazione dei LED

LED	Stato	Indicazione
 (USB)	Blu Fisso	Il dispositivo USB è pronto per l'uso.
	Blu Lampeggiante	È in corso l'identificazione di un nuovo dispositivo USB o il trasferimento di dati.
	Spento	Nessun dispositivo USB è collegato alla porta USB.

■ **Nota:** Se il LED GPON è spento, verificare prima la connessione a Internet. Per ulteriori informazioni su come effettuare correttamente la connessione a Internet, consultare la sezione [Collegare il router GPON](#). Se la connessione è già stata effettuata correttamente, contattare Wind3 per verificare che il servizio Internet sia disponibile.

1. 2. 2. Il pannello posteriore



Le seguenti parti (viste dall'alto verso il basso) si trovano sul pannello posteriore.

Spiegazione delle porte e dei pulsanti

Articolo	Descrizione
Wi-Fi	Premere il pulsante per attivare o disattivare il Wi-Fi 2.4GHz e 5GHz.
WPS	Premere il pulsante per avviare la sincronizzazione WPS.
TEL1, TEL2	Per collegare il telefono analogico al router GPON. Si noti che è possibile collegare al massimo due porte (una a Phone1 e l'altra a Phone2). Una porta telefonica per i servizi Voice over IP (VoIP). Questa porta consente di collegare un dispositivo telefonico al router e di effettuare chiamate via Internet.

Articolo	Descrizione
LAN1, LAN2, 2.5G LAN3, 2.5G WAN	Per collegare il router GPON al PC o ad altri dispositivi di rete Ethernet. Questo router GPON include 2 porte LAN/Ethernet, indicate come LAN1, LAN2, una porta LAN 2.5G e 1 porta WAN 2.5G. Queste porte vengono utilizzate per collegare dispositivi come computer, console di gioco o smart TV tramite cavi Ethernet per una connessione Internet via cavo.
USB	Per il collegamento a un dispositivo di archiviazione dati USB.
ON/OFF	L'interruttore per l'alimentazione. Premerlo per accendere o spegnere il router.
POWER	Per collegare il router alla presa di corrente tramite l'adattatore di corrente in dotazione.
FIBER	Per collegare il router GPON a Internet. Collegare la porta allo splitter tramite un cavo in fibra. Per maggiori dettagli, consultare la sezione Conoscere il router GPON . Questa porta serve a collegare il router GPON al cavo in fibra ottica fornito dal provider di servizi Internet. È utilizzata per la connettività Internet a banda larga.
RESET	Tenere premuto questo pulsante per almeno 5 secondi finché tutti i LED non lampeggiano per ripristinare le impostazioni di fabbrica del router.

Capitolo 2

Collegamento dell'hardware

Questo capitolo contiene le seguenti sezioni:

- [Posizione del router GPON](#)
- [Collegare il router GPON](#)

2.1. Posizione del router GPON

Con il router GPON, è possibile accedere alla rete da qualsiasi punto della copertura della rete wireless. Tuttavia, la potenza e la copertura del segnale wireless variano a seconda dell'ambiente in cui si trova il router GPON. Molti ostacoli possono limitare la portata del segnale wireless, ad esempio strutture in cemento armato e muri spessi.

Per la vostra sicurezza e per le migliori prestazioni del Wi-Fi, vi preghiamo di:

- Non collocare il router GPON in un luogo esposto all'umidità o al calore eccessivo.
- Tenere lontano dalle forti radiazioni elettromagnetiche e dai dispositivi sensibili alle radiazioni elettromagnetiche.
- Collocare il router GPON in una posizione in cui possa essere collegato ai vari dispositivi e a una fonte di alimentazione.
- Assicurarsi che i cavi e il cavo di alimentazione siano posizionati in modo da non creare rischi di inciampo.

 Suggerimenti: Il router GPON può essere collocato su una mensola o su un tavolo.

In genere, il router viene collocato su una superficie orizzontale, ad esempio su una mensola o un tavolo. L'altezza di installazione non deve superare i 2 metri.

2.2. Collegare il router GPON

1. Per collegare il router GPON, procedere come segue.

Metodo 1: attraverso la porta FIBRA (PON)

Collegare la linea in fibra e l'adattatore di alimentazione. La presa elettrica deve essere installata vicino al dispositivo e deve essere facilmente accessibile.

- a. Collegare un'estremità del cavo in fibra ottica alla porta in fibra ottica (solitamente contrassegnata con "FIBRA" o "PON") del router GPON.
- b. Collegare l'altra estremità del cavo in fibra ottica al terminale di rete ottico (ONT) fornito dalWind3. Questo dispositivo converte il segnale in fibra ottica in una connessione Ethernet.
- c. Inserire l'adattatore di alimentazione nel router GPON e collegarlo a una presa di corrente. Assicurarsi che il router riceva l'alimentazione e si accenda. Attendere che il router si avvii completamente, il che può richiedere uno o due minuti.



3 Verificare che il collegamento hardware sia corretto controllando i seguenti LED.
 ⏻ Potenza: Acceso
 ⚡ GPON: accesso o lampeggiante

Metodo 2: tramite la porta WAN Ethernet

- Individuare la porta Ethernet WAN del router. È etichettata come "WAN" e ha un colore diverso rispetto alle porte LAN.
- Prendete il cavo Ethernet e collegatene un'estremità alla porta Ethernet WAN del router.
- Collegare l'altra estremità del cavo Ethernet alla porta Ethernet del modem. Di solito è contrassegnata dalla dicitura "WAN".
- Collegare l'adattatore di alimentazione al router e inserirlo in una presa di corrente. Lasciate che il router si avvii per qualche istante e stabilisca una connessione con il modem.

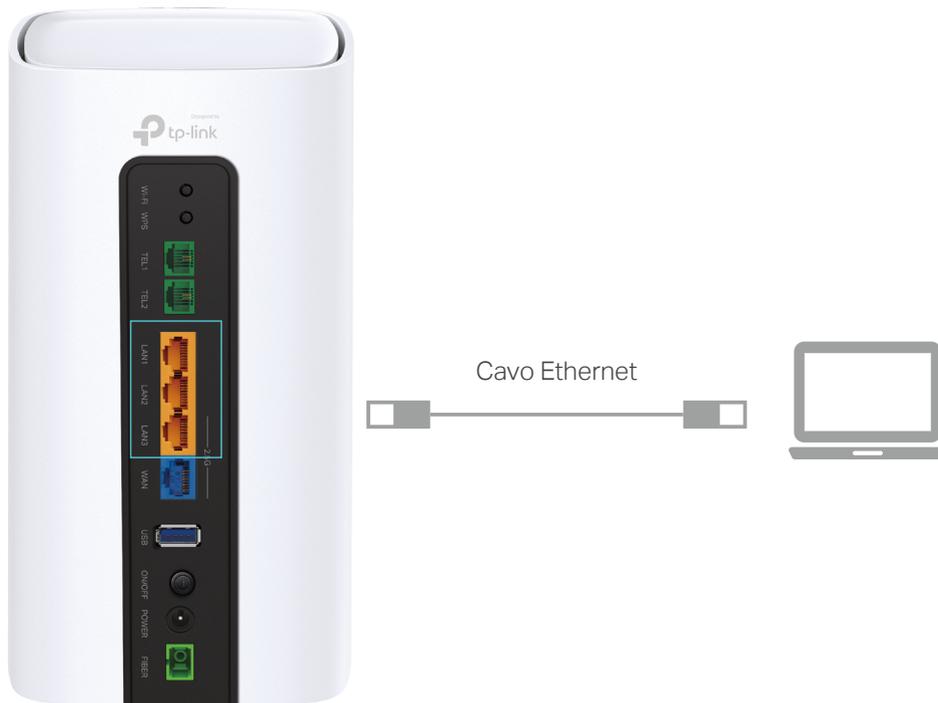


3 Verificare che il collegamento hardware sia corretto controllando i seguenti LED.
 ⏻ Potenza: Acceso
 ⚡ GPON: accesso o lampeggiante

2. Collegare il computer al router GPON.

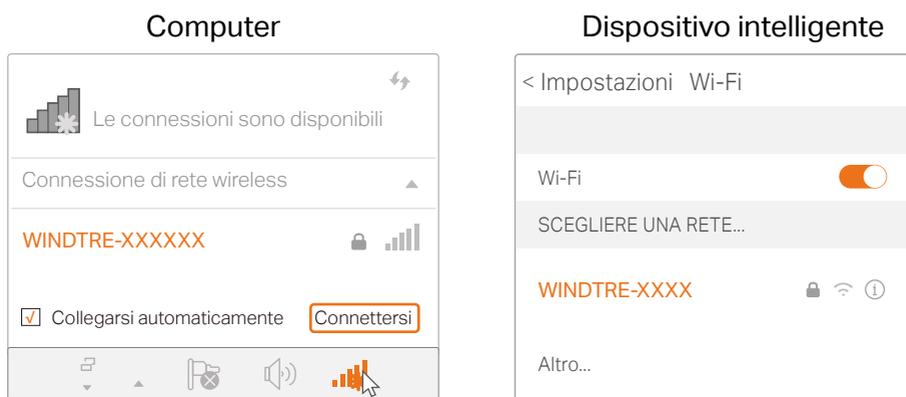
Metodo 1: via cavo

Collegare la porta Ethernet del computer alla porta LAN del router GPON tramite il cavo Ethernet.



Metodo 2: in modalità wireless

Per connettersi in modalità wireless, utilizzare l'SSID (nome di rete wireless) e la password wireless di default, stampati sull'etichetta del prodotto del router GPON.



Metodo 3: Utilizzare il pulsante WPS

I dispositivi wireless che supportano il WPS, tra cui telefoni e tablet Android e la maggior parte delle schede di rete USB, possono essere collegati al router con questo metodo. (Il WPS non è supportato dai dispositivi iOS).

Nota:

La funzione WPS non può essere configurata se la funzione wireless del router è disattivata. Inoltre, la funzione WPS sarà disabilitata se la crittografia wireless è WEP o Enterprise. Prima di configurare la funzione WPS, accertarsi che la funzione wireless sia abilitata e che sia configurata con la crittografia appropriata.

- 1) Toccare l'icona WPS sullo schermo del dispositivo.
- 2) Premere immediatamente il pulsante WPS sul router GPON.
- 3) Il LED WPS lampeggia per circa due minuti durante il processo WPS.
- 4) Quando il LED WPS è acceso, il dispositivo client si è collegato correttamente al router GPON.



Buon divertimento! Il router GPON è ora collegato. Dovreste avere accesso a Internet sul vostro dispositivo cablato e, se avete configurato il Wi-Fi, anche i dispositivi wireless possono connettersi. Godetevi la vostra connessione Internet veloce e affidabile.

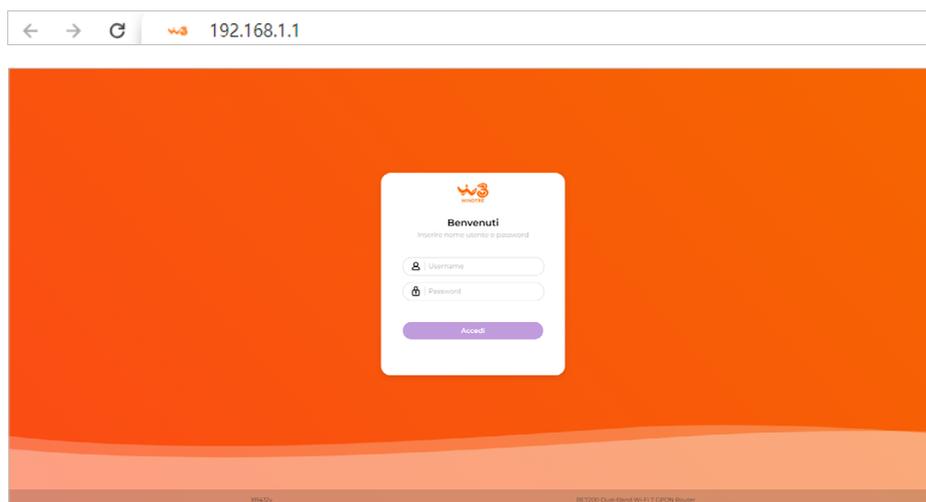
Capitolo 3

Accedere al router GPON

Grazie a un'utility basata sul Web, è facile configurare e gestire il router. L'utility basata sul Web può essere utilizzata su qualsiasi sistema operativo Windows, Mac OS o UNIX con un browser Web, come Microsoft Internet Explorer, Mozilla Firefox o Apple Safari.

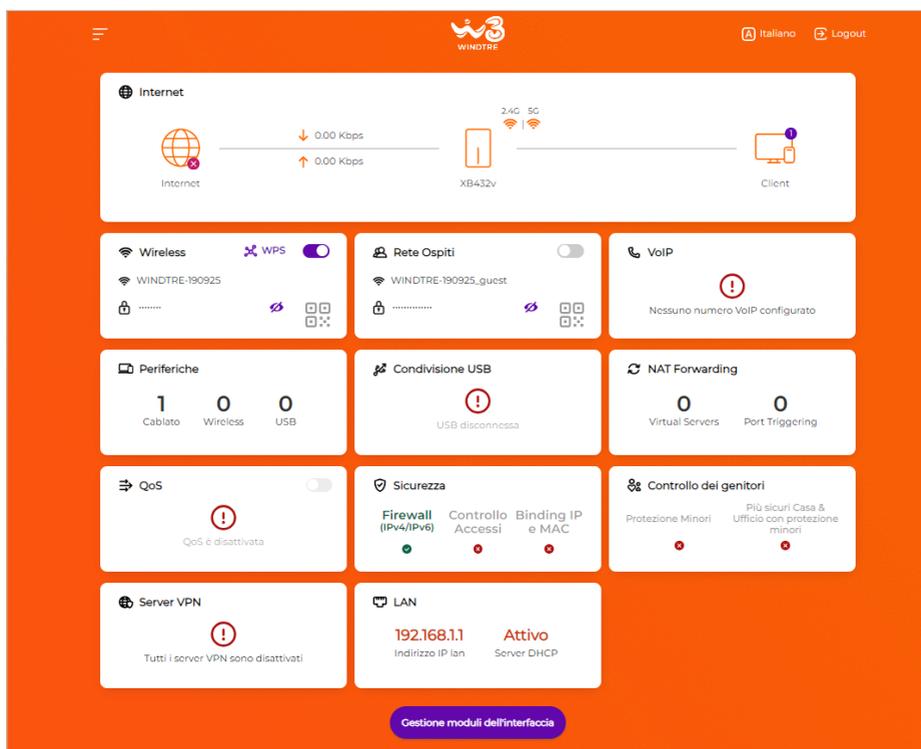
Seguite la procedura seguente per accedere al router.

1. Impostare il protocollo TCP/IP in modalità **Otteni automaticamente un indirizzo IP** sul computer.
2. Visitate <http://192.168.1.1>, e inserite il nome utente e la password stampati sull'etichetta del prodotto nella parte inferiore del router per iniziare.



Nota: Se la finestra di login non appare, consultare la sezione [FAQ](#).

3. Una volta effettuato l'accesso, si viene indirizzati alla pagina Dashboard, che serve come punto di partenza per personalizzare e gestire l'ambiente di rete in base alle proprie preferenze. La Dashboard presenta le principali opzioni di stato e di configurazione in modo intuitivo e facile da usare, consentendo di regolare facilmente le impostazioni di rete in base alle proprie esigenze.



Panoramica delle caratteristiche principali:

- **Riepilogo stato della rete:** visualizzato in alto o in una sezione visibile, fornisce una panoramica dello stato attuale della connessione di rete, compresa la connettività Internet, lo stato della rete locale (LAN) ed eventualmente la potenza del segnale wireless, fornendo un'istantanea dello stato di salute della rete.
- **Modulo impostazioni rapide:** La Dashboard dispone di un modulo per le impostazioni rapide o di uso frequente, che consente di accedere e regolare rapidamente le configurazioni di rete essenziali come il nome Wi-Fi (SSID), la password, il tipo di crittografia e altro ancora, senza dover navigare in menu complessi.
- **Gestione personalizzata dei moduli:** Per soddisfare le diverse esigenze degli utenti, il Dashboard supporta layout di moduli personalizzabili. È possibile aggiungere, rimuovere o riorganizzare i moduli funzionali della pagina, compresi i controlli dei genitori, le reti ospiti, la gestione dei dispositivi e così via, per adattare l'interfaccia alle proprie preferenze personali.
- **Gestione dei dispositivi:** Nel modulo di gestione dei dispositivi, è possibile visualizzare un elenco di tutti i dispositivi attualmente connessi al router, compresi i nomi dei

dispositivi, gli indirizzi MAC, gli indirizzi IP e altro ancora. Inoltre, è possibile applicare limiti di velocità, bloccare l'accesso a Internet o eseguire altre azioni su dispositivi specifici per gestire efficacemente le autorizzazioni di accesso alla rete.

- **Accesso alle Impostazioni Avanzate:** Per gli utenti che necessitano di configurazioni più approfondite, la pagina Dashboard offre punti di accesso alle Impostazioni Avanzate, come le impostazioni di rete, le impostazioni di sicurezza, le configurazioni di routing e altro ancora, soddisfacendo le esigenze degli utenti esperti.

Suggerimenti per il funzionamento:

- **Esplorare e familiarizzare:** Quando si utilizza per la prima volta il Dashboard, è necessario dedicare un po' di tempo a sfogliare i vari moduli e a comprenderne le funzioni e i metodi di utilizzo.
- **Regolazione in base alle esigenze:** Adattate il layout dei moduli e le impostazioni del Dashboard alle vostre esigenze specifiche, rendendo la gestione più comoda ed efficiente.
- **Rimanere al sicuro:** Quando si modificano le impostazioni di rete, assicurarsi di ricordare informazioni importanti come le nuove password Wi-Fi e controllare regolarmente l'elenco dei dispositivi per evitare accessi non autorizzati.

Utilizzando appieno le funzionalità della pagina Dashboard, è possibile gestire e ottimizzare senza sforzo l'ambiente di rete, godendo di un'esperienza online più fluida e sicura.

Capitolo 4

VoIP

Questo capitolo spiega come effettuare chiamate telefoniche via Internet. È possibile che non sia possibile configurare il VoIP quando si utilizzano determinati modelli; contattare Wind3 per assistenza.

- [Collegamento del telefono](#)
- [Rubrica Telefonica](#)
- [Log Telefonate](#)
- [Blocchi di chiamata](#)

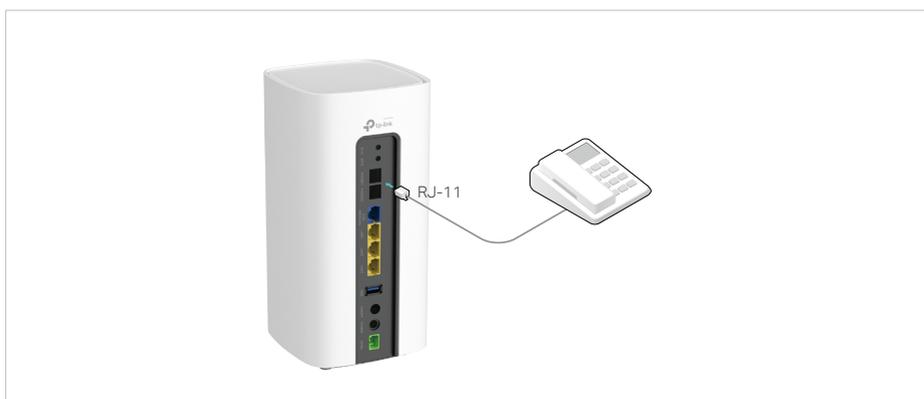
4. 1. Collegamento del telefono

Se si intende utilizzare la funzione VoIP del router GPON, collegare il telefono alla porta telefonica del router. Per il collegamento potrebbe essere necessario un cavo telefonico RJ11. In questo modo sarà possibile effettuare chiamate telefoniche utilizzando la connessione Internet.

Collegare il telefono alle porte RJ11 del pannello posteriore. Si noti che è possibile collegare al massimo due porte (una per il telefono 1 e l'altra per il telefono 2).

Per collegare il telefono alla porta telefonica del router, procedere come segue.

1. Individuare le porte telefoniche sul router GPON. Sono etichettate come "Tel1" e "Tel2". La porta è una presa telefonica standard.
2. Collegare un'estremità di un cavo telefonico alla porta telefonica del router GPON.
3. Collegare l'altra estremità del cavo telefonico al telefono stesso. Cercare una porta sul telefono con l'etichetta "Line" o "Tel."



4. Assicurarsi che il cavo sia collegato saldamente sia al router GPON che al telefono.
5. Una volta collegato il telefono, si dovrebbe sentire un tono di chiamata che indica che è stato configurato correttamente. Per verificare il corretto funzionamento del telefono, effettuare una chiamata.

4. 2. Rubrica Telefonica

È possibile memorizzare tutti i contatti sul router GPON, avere una rubrica telefonica, impostare numeri di chiamata rapida per alcuni contatti e attivare le chiamate di emergenza.

4. 2. 1. Rubrica Telefonica

Per avere una rubrica telefonica sul router GPON, procedere come segue.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.

2. Andare in **Avanzate > VoIP > Rubrica Telefonica**. Fare clic su **Aggiungi** per inserire le informazioni di un nuovo contatto.

Rubrica Telefonica

⊕ Aggiungi ⊖ Elimina Tutto

Nome	Numero Telefono	Numero velocità chiamata	Modifica
--	--	--	--

Nome:

Cognome:

Numero Telefonico Privato:

Numero Telefonico Lavoro:

Numero Telefonico Mobile:

Tipo Numero Chiamata Rapida:

Numero Chiamata Rapida:

3. È possibile impostare un numero di chiamata rapida per determinati numeri. La funzione di chiamata rapida consente di raggiungere l'interlocutore desiderato componendo un numero ridotto di tasti anziché un numero telefonico lungo.
4. Fare clic su **OK** per salvare le impostazioni.

4.2.2. Chiamate di emergenza

Voglio farlo:

Fare in modo che il mio telefono chiami automaticamente un contatto specifico quando il ricevitore viene sollevato ma non viene eseguita alcuna operazione entro un certo periodo di tempo. In questo modo gli anziani, i bambini, i pazienti o le donne incinte possono inviare segnali di aiuto in caso di emergenza.

Come posso farlo?

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Accedere a **Avanzate > VoIP > Rubrica telefonica**.

3. Abilitare il numero di emergenza.
4. **No Operation time**: impostare il tempo di attesa del telefono prima della composizione automatica del primo numero.)
5. **Numero Emergenza**: Impostare il numero da raggiungere automaticamente. Se è stato impostato più di un numero, il router GPON chiamerà automaticamente il successivo se il precedente non riceve risposta.
6. Fare clic su **Salva** per rendere effettive le impostazioni.

Fatto!

D'ora in poi, se si solleva il telefono ma non si compone entro il tempo di non funzionamento, il telefono chiamerà automaticamente il numero di emergenza!

4.3. Log Telefonate

Voglio farlo:

Disporre di un elenco di chiamate che registra informazioni dettagliate sulle chiamate in entrata e in uscita sul router GPON.

Come posso farlo?

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > VoIP > Log Telefonate**.

Data/Ora	Tipo	Durata (hh:mm:ss)	Numero/Contatti	Numero Dispositivo	Dispositivo Telefonico	Elimina
----------	------	-------------------	-----------------	--------------------	------------------------	---------

3. Abilitare **Log Telefonate**.

Fatto! D'ora in poi, tutte le chiamate in entrata e in uscita saranno registrate qui. Se si dispone di una rubrica telefonica, il nome del contatto viene visualizzato nell'elenco delle chiamate.

4.4. Blocchi di chiamata

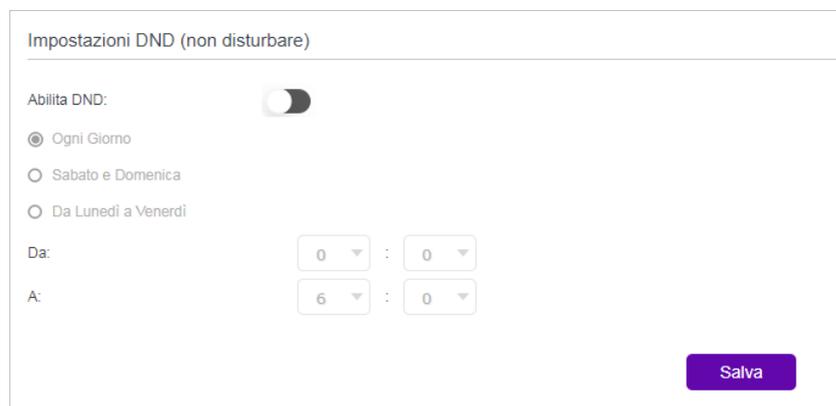
Quando non si desidera ricevere o comporre chiamate, utilizzare le funzioni di blocco delle chiamate. Questa parte è composta da tre funzioni: Non disturbare, Blocca alcune chiamate e Impedisci di comporre.

4.4.1. DND (Non disturbare)

Voglio farlo: Non far squillare il telefono in un determinato periodo di tempo.

Come posso farlo? 1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.

2. Accedere a **Avanzate > VoIP > DND (non disturbare)**.



3. Abilita **DND**.

4. Impostare i giorni in cui il DND è abilitato.

5. Fare clic su **Salva** per rendere effettive le impostazioni.

Fatto! In questo lasso di tempo, non squillerà alcun telefono, ma tutte le chiamate in arrivo saranno registrate nel Log Telefonate. Godetevi la vostra tranquillità e, quando tornate, controllate il Log Telefonate per vedere cosa vi siete persi.

4.4.2. Blocco di alcune chiamate

Voglio farlo: Blocco di alcune chiamate, ad esempio quelle anonime o quelle dei venditori fastidiosi.

Come posso farlo?

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Accedere a **Avanzate > VoIP > DND e Telefonate Bloccate**.
3. Fare clic su **Aggiungi** in corrispondenza di **Telefonata in Entrata**.

4. Selezionare il Numero Specifico e inserire il numero di telefono da bloccare nel campo **Numero**, oppure **Numero anonimo** per bloccare tutte le chiamate sconosciute.

5. Fare clic su **OK** per rendere effettive le impostazioni.

Fatto!

Ora il router GPON utilizzerà le informazioni immesse per bloccare le telefonate.

4.4.3. Vietare Telefonate in uscita

Voglio farlo:

Impedire al router GPON di comporre un certo tipo di numeri. **Ad esempio**, chiamare un cellulare tramite il mio numero di telefono costa molto, quindi non voglio che nessuno chiami un cellulare utilizzando il mio numero di telefono.

Come posso farlo?

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Accedere a **Avanzate > VoIP > DND e blocco chiamate**.
3. Fare clic su **Aggiungi** in corrispondenza di **Telefonate in Uscita**.

Telefonata Bloccata

Telefonate in Entrata

Telefonate in Uscita

Numero	Modifica	Tipo Chiamata o Prefisso	Modifica
--	--	--	--

4. Selezionare dall'elenco a discesa il **tipo di chiamata** che si desidera bloccare. Se si seleziona **Chiamata con prefisso numero specifico**, aggiungere il prefisso del numero di telefono nel campo Prefisso numero.

Telefonata Bloccata

Telefonate in Entrata

Telefonate in Uscita

Numero	Modifica	Tipo Chiamata o Prefisso	Modifica
--	--	--	--

Tipo Telefonata:

Mobile

Cancella OK

5. Fare clic su **OK** per rendere effettive le impostazioni.

Fatto!

Ora il router GPON impedirà la composizione di tutti i telefoni cellulari.

Inoltre:

Il tipo di numero può variare a seconda delle circostanze. È inoltre possibile impostare il prefisso scegliendo **Chiamate con prefisso numero specifico**. Quando si imposta un prefisso, tutti i numeri con questo prefisso non possono essere chiamati.

Capitolo 5

Personalizzare le impostazioni di rete

Questo capitolo illustra come modificare le impostazioni di default o regolare la configurazione di base del router GPON utilizzando la pagina di gestione web.

Contiene le seguenti sezioni:

- [Configurare le impostazioni LAN](#)
- [Impostazione account del servizio DNS dinamico](#)
- [Creare Route Statiche](#)
- [Impostazioni RIP](#)
- [Impostazioni Wireless specifiche](#)
- [Schedulazione Wireless](#)
- [Utilizzare WPS per la connessione wireless](#)

5.1. Configurare le impostazioni LAN

5.1.1. Modifica dell'indirizzo IP della LAN

Il router GPON è preimpostato con un IP LAN di default 192.168.1.1, che è possibile utilizzare per accedere alla pagina di gestione web. L'indirizzo IP LAN, insieme alla Subnet Mask, definisce anche la sottorete in cui si trovano i dispositivi collegati. Se l'indirizzo IP è in conflitto con un altro dispositivo della rete locale o se la rete richiede una sottorete IP specifica, è possibile modificarlo.

Per modificare l'indirizzo IP, procedere come segue.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Accedere alla pagina **Avanzate > Rete > Impostazioni LAN** e selezionare **IPv4**.

Server DHCP		IPv4 IPv6
Indirizzo MAC:	20:24:04:19:09:25	
Indirizzo IP:	192 . 168 . 1 . 1	
Subnet Mask:	255.255.255.0	
IGMP Snooping:	<input checked="" type="checkbox"/> Abilita	
Secondo IP:	<input type="checkbox"/> Abilita	

3. Inserire un nuovo **indirizzo IP** adatto alle proprie esigenze.
4. Selezionare la **Subnet Mask** dall'elenco a discesa. La Subnet Mask, insieme all'indirizzo IP, identifica la sottorete IP locale.
5. Mantenere lo **IGMP Snooping** abilitato di default. Lo IGMP Snooping è il processo di ascolto del traffico di rete IGMP (Internet Group Management Protocol). Questa funzione impedisce agli host di una rete locale di ricevere il traffico di un gruppo multicast a cui non hanno aderito esplicitamente.
6. È possibile configurare il **Secondo IP** e la **Subnet Mask** del router per l'interfaccia LAN, attraverso la quale è possibile accedere alla pagina di gestione web.
7. Mantenere le altre impostazioni come quelle di default.
8. Fare clic su **Salva** per rendere effettive le impostazioni.

5.1.2. Utilizzare il router come server DHCP

È possibile configurare il router in modo che agisca come server DHCP per assegnare gli indirizzi IP ai suoi client. Per utilizzare la funzione di server DHCP del router, è necessario configurare tutti i computer della LAN in modo che ottengano automaticamente un indirizzo IP.

Per configurare il server DHCP, procedere come segue.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Accedere alla pagina [Avanzate > Rete > Impostazioni LAN](#) e selezionare **IPv4**.

DHCP: **Abilita**

Server DHCP DHCP Relay

Pool Indirizzi IP: 192 . 168 . 1 . 2 - 192 . 168 . 1 . 254

Durata Indirizzo: 1440 minuti (1-2880. Il valore di default è 120).

Default Gateway: 192 . 168 . 1 . 1 (opzionale)

Dominio di Default: (opzionale)

DNS Primario: 192 . 168 . 1 . 1 (opzionale)

DNS Secondario: 0 . 0 . 0 . 0 (opzionale)

Salva

3. Abilitare la funzione **DHCP** e selezionare **Server DHCP**.
4. Specificare il **pool di indirizzi IP**; l'indirizzo iniziale e quello finale devono trovarsi nella stessa sottorete con LAN IP. Il router assegnerà ai suoi clienti gli indirizzi compresi in questo intervallo specificato. Di default, il range va da 192.168.1.2 a 192.168.1.249.
5. Inserire una durata nel campo **Durata Indirizzo**. La **Durata Indirizzo** è il periodo di tempo in cui un client DHCP può concedere il suo indirizzo IP dinamico corrente assegnato dal router. Alla scadenza dell'indirizzo IP dinamico, all'utente verrà assegnato automaticamente un nuovo indirizzo IP dinamico.
6. Mantenere le altre impostazioni come quelle di default e fare clic su **Salva**.

📌 **Note:**

1. Il router può essere configurato per funzionare come **DHCP Relay**. Un relay DHCP è un computer che inoltra i dati DHCP tra i computer che richiedono indirizzi IP e il server DHCP che assegna gli indirizzi. Ogni interfaccia del dispositivo può essere configurata come relay DHCP. Se è abilitato, le richieste DHCP dei PC locali saranno inoltrate al server DHCP che funziona sul lato WAN.
2. È inoltre possibile assegnare indirizzi IP all'interno di un intervallo specifico a dispositivi dello stesso tipo utilizzando la funzione **Condition Pool**. Ad esempio, è possibile assegnare indirizzi IP nel range (da 192.168.0.50 a 192.168.0.80) ai dispositivi della telecamera, facilitando così la gestione della rete. Abilitare la funzione DHCP e configurare i parametri in base alla propria situazione nella pagina [Avanzate > Rete > Impostazioni LAN](#).

5.1.3. Riserva Indirizzi IP LAN

È possibile visualizzare e aggiungere un indirizzo riservato per un client. Quando si specifica un indirizzo IP per un dispositivo della LAN, questo riceverà sempre lo stesso indirizzo IP quando accederà al server DHCP. Se nella LAN sono presenti dispositivi che richiedono indirizzi IP permanenti, configurare a tal fine la funzione di prenotazione degli indirizzi sul router.

Seguire la procedura seguente per riservare un indirizzo IP per i dispositivi.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Accedere alla pagina **Avanzate > Rete > Impostazioni LAN** e selezionare **IPv4**.
3. Scorrere fino alla sezione **Riserva Indirizzi** e fare clic su **Aggiungi** per aggiungere un indirizzo IP riservato per il dispositivo.

The screenshot shows the 'Riserva Indirizzi' configuration page. At the top right, there are buttons for '+ Aggiungi' and '- Elimina'. Below is a table with the following structure:

<input type="checkbox"/>	Indirizzo MAC	IP Riservato	Abilita	Modifica
--	--	--	--	--

Below the table, there are input fields for 'Indirizzo MAC' and 'IP Riservato', a 'Scansiona' button, a checked checkbox for 'Abilita questa voce', and 'Cancella' and 'OK' buttons.

4. Inserire l'**indirizzo MAC** del dispositivo per il quale si desidera riservare l'indirizzo IP.
5. Specificare l'**indirizzo IP** che verrà riservato dal router.
6. Selezionare la casella di controllo **Abilita questa voce** e fare clic su **OK** per rendere effettive le impostazioni.

5.2. Impostazione account del servizio DNS dinamico

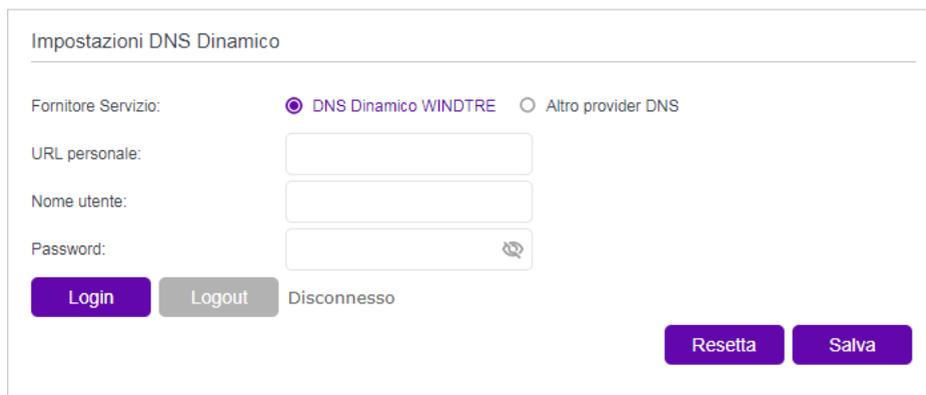
Wind3 generalmente assegna al router un indirizzo IP dinamico, che può essere utilizzato per accedere al router da remoto. Tuttavia, l'indirizzo IP può cambiare in qualsiasi momento e non si sa quando cambia. In questo caso, potreste aver bisogno della funzione DDNS (Dynamic Domain Name Server) del router per consentire a voi e ai vostri amici di accedere al router e ai server locali (FTP, HTTP, ecc.) utilizzando un nome di dominio, senza dover controllare e ricordare l'indirizzo IP.

📌 **Nota:** Il DDNS non funziona se Wind3 assegna al router un indirizzo IP WAN privato (ad esempio 192.168.1.x).

Per impostare il DDNS, seguire le istruzioni riportate di seguito:

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Rete > DNS Dinamico**.
3. Selezionare il **fornitore di servizi** (DNS Dinamico WINDTRE/DNS dinamico definito dall'utente).

4. Accedere con il proprio account DDNS, selezionare un provider di servizi. Inserire il nome utente, la password e il nome di dominio dell'account (ad esempio lisa.ddns.net).



Impostazioni DNS Dinamico

Fornitore Servizio: DNS Dinamico WINDTRE Altro provider DNS

URL personale:

Nome utente:

Password: 

Disconnesso

5. Fare clic su **Accedi** e **Salva**.

 **Suggerimento:** Se si desidera utilizzare un nuovo account DDNS, effettuare prima il logout e poi il login con il nuovo account.

5.3. Creare Route Statiche

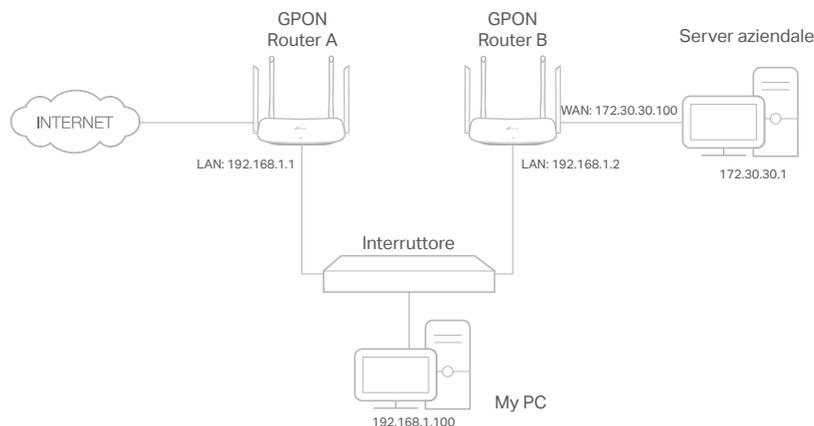
Una route statica è un percorso predeterminato che le informazioni di rete devono percorrere per raggiungere un host o una rete specifici. I dati da un punto a un altro seguiranno sempre lo stesso percorso, indipendentemente da altre considerazioni. Il normale utilizzo di Internet non richiede la configurazione di questa impostazione.

Voglio farlo:

Visitare più reti e più server contemporaneamente. **Ad esempio**, in un piccolo ufficio, il mio PC può navigare in Internet attraverso il router GPON A, ma voglio anche visitare il server della mia azienda.

Ora ho uno switch e un altro router B GPON.

Collegare i dispositivi come mostrato nell'immagine seguente, in modo da stabilire la connessione fisica tra il mio PC e il server della mia azienda. Per navigare in Internet e visitare contemporaneamente la rete aziendale, devo configurare il routing statico.



Come posso farlo?

1. Assicurarsi che i router utilizzino indirizzi IP LAN diversi sulla stessa subnet. Disattivare la funzione DHCP del router GPON B.
2. Visitare il sito <http://192.168.1.1> e accedere con la password impostata per il Router GPON A.
3. Andare in **Avanzate > Rete > Routing Statico**.
4. Fare clic su **Aggiungi** per aggiungere una nuova voce di routing statico. Completare le impostazioni in base alle spiegazioni seguenti:

IPv4 | IPv6

+ Aggiungi - Elimina

☐	ID	Rete di Destinazione	Subnet Mask	Gateway	Abilita	Modifica
--	--	--	--	--	--	--

IP di Destinazione:

Subnet Mask:

Gateway:

Interfaccia:

Abilita questa voce

- **Rete di Destinazione:** L'indirizzo IP di destinazione che si desidera assegnare a una route statica. Questo indirizzo IP non può trovarsi nella stessa sottorete dell'IP WAN o dell'IP LAN del router A. Nell'esempio, l'indirizzo IP di destinazione è l'indirizzo IP della rete aziendale, per cui si inserisce 172.30.30.1.
- **Subnet Mask:** Determina la rete di destinazione con l'indirizzo IP di destinazione. Se la destinazione è un singolo

indirizzo IP, inserire 255.255.255.255; altrimenti, inserire la Subnet Mask dell' IP di rete corrispondente. Nell'esempio, la rete di destinazione è un singolo IP, quindi si inserisce 255.255.255.255.

- **Gateway:** L'indirizzo IP del dispositivo gateway a cui verranno inviati i pacchetti di dati. Questo indirizzo IP deve trovarsi nella stessa sottorete dell'IP del router che invia i dati. Nell'esempio, i pacchetti di dati saranno inviati alla porta LAN del Router B e poi al Server, quindi il gateway di default deve essere 192.168.1.2.
 - **Interface:** Determinata dalla porta (WAN/LAN) che invia i pacchetti di dati. Nell'esempio, i dati vengono inviati al gateway attraverso la porta LAN del router A, quindi si deve selezionare **LAN**.
5. Selezionare la casella di controllo **Abilita questa voce** per abilitarla.
 6. Fare clic su **OK** per rendere effettive le impostazioni.

Fatto!

Aprire un browser web sul PC. Immettere l'indirizzo IP del server aziendale per visitare la rete aziendale.

5.4. Impostazioni RIP

Per attivare il RIP per l'interfaccia WAN, selezionare la versione e l'operazione RIP desiderata e spuntare il riquadro "Abilita". Per interrompere il RIP sull'interfaccia WAN, deselezionare la casella di controllo 'Abilita'. Fare clic sul pulsante 'Salva' per avviare/arrestare RIP e salvare la configurazione.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Rete > Impostazioni RIP**.
3. Configurare le impostazioni RIP.

Impostazioni RIP

Per attivare RIP per l'interfaccia WAN, seleziona la versione e l'operazione RIP desiderati e spunta la casella 'Abilitato'. Per interrompere RIP sull'interfaccia WAN, deseleziona la casella "Abilitato". Fai clic sul pulsante "Salva" per avviare/interrompere RIP e salvare la configurazione.

NOTA: RIP non può essere configurato sull'interfaccia WAN con NAT abilitato.

Autenticazione MD5: Abilita

MD5 Key ID 0:

MD5 Key ID 1:

[Salva](#)

Interfaccia	Versione	AcceptRA	SendRA	Abilitato	RipngEnabled	Modifica
--	--	--	--	--	--	--

- **Autenticazione MD5** - Abilita l'autenticazione MD5 per migliorare la sicurezza dei pacchetti rip RA.
- **MD5 Key ID 0** - Impostazione del valore dell'MD5 Key ID 0.
- **MD5 Key ID 1** - Impostazione del valore dell'MD5 Key ID 1.
- **Interfaccia** - Il nome dell'interfaccia WAN della voce della tabella delle regole RIP utilizzata.
- **Versione** - La versione RIP (RIPv1/RIPv2) della voce della tabella delle regole RIP utilizzata.
- **AcceptRA** - Abilitare per fare in modo che la voce della regola RIP possa accettare il Router Advertisement.
- **SendRA** - Abilitare per fare in modo che la voce della regola RIP possa inviare il Router Advertisement.
- **Abilitato** - Abilitato per rendere attiva la voce della regola RIP per IPv4.
- **RipngAbilitad** - Abilitarlo per rendere attiva la voce della regola RIP per IPv6, nota anche come Ripng.
- **Modifica** - Fare clic qui per modificare la voce della regola RIP.

5.5. Impostazioni Wireless specifiche

5.5.1. Modificare le Impostazioni Wireless di base

Il nome della rete wireless (SSID) e la password del router GPON e l'opzione di sicurezza sono preimpostati in fabbrica. L'SSID e la password preimpostati sono riportati

sull'etichetta del prodotto. È possibile personalizzare le Impostazioni Wireless in base alle proprie esigenze.

Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.

➤ **Per attivare o disattivare la funzione wireless:**

1. Andare in **Avanzate > Wireless > Impostazioni Wireless**.
2. La **radio wireless** è abilitata di default. Se si desidera disattivare la funzione wireless del router, è sufficiente deselezionare le caselle di controllo **Abilita**. In questo caso, tutte le Impostazioni Wireless non saranno più valide.

➤ **Per modificare il nome della rete wireless (SSID) e la password wireless:**

1. Andare in **Avanzate > Wireless > Impostazioni Wireless**.
2. Inserire un nuovo SSID (32 caratteri al massimo) nel campo **Nome Rete Wireless (SSID)** e una nuova password nel campo **Password** e fare clic su **Salva**. L'SSID e la password sono sensibili alle maiuscole e alle minuscole.

📌 **Nota:** Se si utilizza un dispositivo wireless per modificare le Impostazioni Wireless, si verrà disconnessi dopo l'entrata in vigore delle nuove impostazioni. Annotare il nuovo SSID e la nuova password per un uso futuro.

➤ **Per nascondere l'SSID:**

1. Andare in **Avanzate > Wireless > Impostazioni Wireless**.
2. Selezionare **Nascondi SSID** e l'SSID non verrà trasmesso. L'SSID non verrà visualizzato sui dispositivi wireless quando si esegue la scansione delle reti wireless locali e si deve unire manualmente alla rete.

➤ **Per cambiare la modalità o il canale:**

1. Andare in **Avanzate > Wireless > Impostazioni Wireless**.

Impostazioni Wireless

OFDMA:

TWT:

BSS Color:

Wireless Radio: Abilita

Nome Rete Wireless (SSID): SSID nascosto

Sicurezza:

Password:
Basso Medio Alto

Potenza Trasmissiva: Basso Medio Alto

Avanzate

Modalità 2.4 GHz:

Canale 2.4 GHz:

Ampiezza Canale 2.4 GHz:

Modalità 5GHz:

Canale 5GHz:

Ampiezza Canale 5 GHz:

Salva

2. Selezionare la modalità o il canale della rete wireless e fare clic su **Salva** per rendere effettive le impostazioni.

Modalità: Selezionare la modalità di trasmissione desiderata.

- 802.11a Only / 802.11b Only / 802.11g Only / 802.11n Only / 802.11ac Only / 802.11ax Only: Selezionare se si utilizzano solo client wireless 802.11a/11n/11b/11g/11ac/11ax.
- 802.11a/n mixed: selezionare se si utilizza un mix di client wireless 802.11a e 11n.
- 802.11a/n/ac mixed: selezionare se si utilizza un mix di client wireless 802.11a, 11n e 11ac.
- 802.11a/n/ac/ax mixed: selezionare se si utilizza un mix di client wireless 802.11a, 11n, 11ac e 11ax.
- 802.11a/n/ac/ax/be mixed: selezionare se si utilizza un mix di client wireless 802.11a, 11n, 11ac, 11ax e 11be.
- 802.11b/g mixed: selezionare se si utilizza un mix di client wireless 802.11b e 11g.
- 802.11b/g/n mixed: selezionare se si utilizza un mix di client wireless 802.11b, 11g e 11n.
- 802.11b/g/n/ax mixed: selezionare se si utilizza un mix di client wireless 802.11b, 11g, 11n e 11ax.

- **802.11b/g/n/ax/be mixed:** selezionare se si utilizza un mix di client wireless 802.11b, 11g, 11n, 11ax e 11be.

📌 **Nota:** Quando si seleziona la modalità 802.11n Only, solo le stazioni wireless 802.11n possono collegarsi al router. Si consiglia vivamente di selezionare 802.11b/g/n mixed (per 2.4GHz) e 802.1 a/n/ac/ax mixed (per 5GHz), e tutte le stazioni wireless 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac e 802.11ax possono collegarsi al router.

Canale: Selezionare il canale che si desidera utilizzare dall'elenco a discesa. Questo campo determina la frequenza operativa utilizzata. Non è necessario cambiare il canale wireless a meno che non si notino problemi di interferenza con un altro access point vicino.

Ampiezza Canale: selezionare l'ampiezza del canale dall'elenco a discesa. L'impostazione di default è **Auto**, che consente di regolare automaticamente l'ampiezza del canale per i clienti.

Potenza Trasmissiva: selezionare Bassa, Media o Alta per specificare la potenza di trasmissione dei dati. L'impostazione di default e consigliata è **Alta**.

➤ **Per modificare l'opzione di sicurezza:**

1. Accedere a **Avanzate > Wireless > Impostazioni Wireless**.

2. Selezionare un'opzione dall'elenco a discesa **Sicurezza** e configurare i relativi parametri. Il router offre cinque opzioni: **Nessuna sicurezza**, **WPA2-PSK[AES]**, **WPA2-PSK[AES]+WPA3-Personal**, **WPA3-Personal**, **WPA2-Enterprise**. WPA3 utilizza lo standard più recente e il livello di sicurezza è il più elevato. Si consiglia di non modificare le impostazioni di default se non necessario.

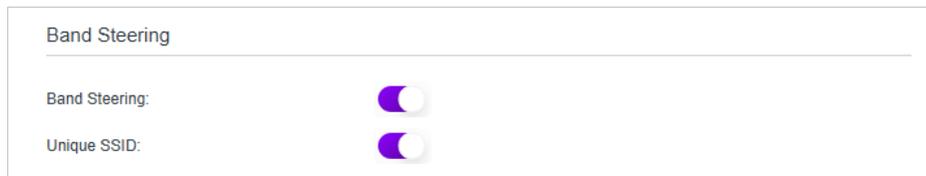
3. Fare clic su **Salva** per rendere effettive le impostazioni.

➤ **Per abilitare il roaming di rete:**

Il roaming di rete aiuta i dispositivi a scegliere un AP migliore in base alle condizioni reali per bilanciare le richieste di rete.

1. Accedere a **Avanzate > Wireless > Impostazioni Wireless**.

2. Individuare la sezione **Band Steering**, selezionare la casella di controllo **Abilita** per rendere effettive le impostazioni.



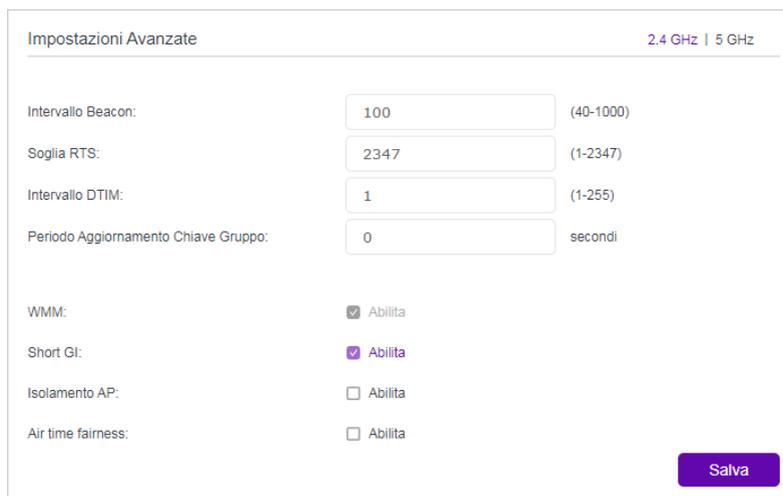
5.5.2. Impostazioni Wireless avanzate

Le Impostazioni Wireless avanzate sono destinate a coloro che desiderano maggiori controlli sulla rete. Per configurare il router è possibile seguire le istruzioni riportate di seguito.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare su **Avanzate > Wireless > Impostazioni Avanzate**.

➤ **Per modificare le Impostazioni Avanzate di base:**

Individuare la sezione **Impostazioni Avanzate** e configurare le Impostazioni Avanzate in base alla spiegazione riportata di seguito, quindi fare clic su **Salva**.



Impostazioni Avanzate		2.4 GHz 5 GHz
Intervallo Beacon:	<input type="text" value="100"/>	(40-1000)
Soglia RTS:	<input type="text" value="2347"/>	(1-2347)
Intervallo DTIM:	<input type="text" value="1"/>	(1-255)
Periodo Aggiornamento Chiave Gruppo:	<input type="text" value="0"/>	secondi
WMM:	<input checked="" type="checkbox"/> Abilita	
Short GI:	<input checked="" type="checkbox"/> Abilita	
Isolamento AP:	<input type="checkbox"/> Abilita	
Air time fairness:	<input type="checkbox"/> Abilita	

- **Intervallo beacon:** Inserire un valore compreso tra 40 e 1000 in millisecondi per determinare la durata della trasmissione dei pacchetti beacon da parte del router per sincronizzare la rete wireless. Il valore di default è 100 millisecondi.
- **Soglia RTS:** Inserire un valore compreso tra 1 e 2347 per determinare la dimensione del pacchetto di trasmissione dei dati attraverso il router. Di default, la dimensione della soglia RTS (Request to Send) è 2347. Se la dimensione del pacchetto è superiore alla soglia preimpostata, il router invia frame Request to Send a una particolare stazione ricevente e negozia l'invio di un frame di dati, altrimenti il pacchetto viene inviato immediatamente.

- **Intervallo DTIM:** Inserire un valore compreso tra 1 e 255 per determinare il range DTIM (Delivery Traffic Indication Message). 1 indica che il range DTIM è uguale al range Beacon.
- **Periodo Aggiornamento Chiave Gruppo:** Inserire il numero di secondi per controllare il range di tempo per il rinnovo automatico della chiave di crittografia. L'impostazione di default è 0, che indica l'assenza di rinnovo della chiave.
- **WMM:** questa funzione garantisce la trasmissione preferenziale dei pacchetti con messaggi ad alta priorità. Il WMM è abilitato obbligatoriamente in modalità 802.11n o 802.11ac.
- **Short GI:** Questa funzione è attivata di default ed è consigliata per aumentare la capacità dei dati riducendo il tempo del GI (Guard Interval).
- **Isolamento AP:** Selezionare questa casella di controllo per attivare la funzione Isolamento AP, che consente di confinare e limitare l'interazione tra dispositivi wireless della rete, pur potendo accedere a Internet.
- **Air time fairness:** Selezionare questa casella di controllo per abilitare la funzione ATF (Airtime Fairness) che consente di ottimizzare il throughput di ciascun flusso. Lo scheduler del traffico ATF utilizza gli obiettivi di tempo airtime fairness per target per bilanciare l'uso del airtime fairness tra le destinazioni del flusso.

Nota: Se non si ha familiarità con le impostazioni di cui sopra, si consiglia vivamente di mantenere le impostazioni di default, altrimenti le prestazioni della rete wireless potrebbero risultare inferiori.

➤ **Per attivare o disattivare la funzione WPS:**

WPS (Wi-Fi Protected Setup) offre un approccio più semplice per impostare una connessione Wi-Fi protetta. Questa funzione è attiva di default, ma se non ne avete bisogno, deselezionate la casella di controllo **Abilita WPS**.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare su **Avanzate > Wireless > WPS**.

PIN del Router

Altri dispositivi possono connettersi al router usando il PIN WPS del router.

PIN del Router:

PIN Corrente:

Impostazioni WPS

Abilita WPS:

Seleziona un metodo di setup:

Tasto Push (Consigliato)

Premi il tasto fisico WPS sul router o fai clic sul tasto Connetti qui sotto.

Codice PIN

5.5.3. Visualizza le informazioni wireless

➤ **Per visualizzare le impostazioni dettagliate della rete wireless:**

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Accedere alla pagina **Avanzate** > **Stato**. Troverete il pannello **Wireless**.
3. Fare clic su **2.4GHz** o **5GHz** per visualizzare i dettagli wireless.

Wireless  2.4 GHz | 5 GHz

Nome Rete:	WINDTRE-190925
Wireless Radio:	Accesso
Modalità:	802.11b/g/n/ax/be mix
Ampiezza Canale:	Auto(40MHz)
Canale:	Auto(9)
Indirizzo MAC:	20:24:04:19:09:25

🔗 **Suggerimento:** È possibile visualizzare i dettagli del wireless anche facendo clic sull'icona del router in **Dashboard** > **Internet**.

➤ **Per visualizzare le informazioni dettagliate dei client wireless connessi:**

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare alla pagina **Avanzate > Wireless > Statistiche**.
3. È possibile visualizzare le informazioni dettagliate dei client wireless, tra cui il tipo di connessione e l'opzione di sicurezza, nonché i pacchetti trasmessi.

Dispositivi Wireless Online

 **Aggiorna**

ID	Nome	Indirizzo MAC	Tipo Connessione	Sicurezza	Intensità Segnale	Pacchetti Ricevuti	Pacchetti Inviati
--	--	--	--	--	--	--	--

 **Suggerimento:** È possibile visualizzare i dettagli wireless anche facendo clic sull'icona dei client wireless in **Base > Mappa di rete**.



5. 6. Schedulazione Wireless

È possibile disattivare automaticamente le reti wireless quando non è necessaria la connessione wireless.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Wireless > Schedulazione Wireless**.
3. Abilitare la funzione **Schedulazione Wireless**.

Schedulazione Wireless

Abilita Schedulazione Wireless:

	Dom.	Lun.	Mar.	Mer.	Gio.	Ven.	Sab.
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							
24:00							

WLAN Spento

Ripristino Salva

4. Fare clic su **Aggiungi** per impostare l'ora di spegnimento wireless e fare clic su **Salva** per rendere effettive le impostazioni.

Note:

1. Prima di utilizzare questa funzione, accertarsi che l'ora del router sia corretta. Per ulteriori informazioni, fare riferimento a [Impostare l'ora del sistema](#).
2. Il LED wireless si spegne se la rete wireless corrispondente è disattivata.
3. La rete wireless si accenderà automaticamente dopo il periodo di tempo impostato.

5. 7. Utilizzare WPS per la connessione wireless

È possibile utilizzare il WPS (Wi-Fi Protected Setup) per aggiungere un nuovo dispositivo wireless alla rete esistente in modo rapido e semplice.

Metodo 1: Utilizzare il pulsante WPS

Utilizzare questo metodo se il dispositivo client dispone di un pulsante WPS.

1. Premere il pulsante WiFi/WPS del router.
2. Premere direttamente il pulsante WPS del dispositivo client.
3. Il LED WPS lampeggia per circa 2 minuti durante il processo WPS.

4. Quando il LED WPS è acceso, il dispositivo client si è collegato correttamente al router.

Metodo 2: utilizzare il pulsante "Connetti" nella pagina di gestione web

Utilizzare questo metodo se il dispositivo client dispone di un pulsante WPS.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare alla pagina [Avanzate](#) > [Wireless](#) > [WPS](#).

3. Fare clic su [Connetti](#) nella pagina.
4. Premere direttamente il pulsante WPS del dispositivo client.
5. Il LED WPS del router lampeggia per circa 2 minuti durante il processo WPS.
6. Quando il LED WPS è acceso, il dispositivo client si è collegato correttamente al router.

Metodo 3: Inserire il PIN del dispositivo client sul router

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in [Avanzate](#) > [Wireless](#) > [WPS](#) e fare clic su Numero PIN.
3. Immettere il [PIN del cliente](#).

4. Fare quindi clic sul pulsante [Connetti](#).
5. [Il dispositivo è stato aggiunto con successo!](#) o un'informazione simile apparirà sulla pagina web, il che significa che il dispositivo client si è collegato con successo al router.

Capitolo 6

Impostazioni USB

Questo capitolo descrive come utilizzare le porte USB per condividere file e contenuti multimediali dai dispositivi di archiviazione USB sulla rete domestica a livello locale o da remoto tramite Internet. Il router GPON supporta unità flash e dischi rigidi esterni USB.

Contiene le seguenti sezioni:

- [Accesso al dispositivo di archiviazione USB](#)
- [Condivisione Media](#)
- [Impostazioni 3G/4G](#)

6. 1. Accesso al dispositivo di archiviazione USB

Inserite il dispositivo di archiviazione USB nella porta USB del router GPON e accedete ai file memorizzati localmente o da remoto.

🔗 Suggestioni:

- Se si utilizzano hub USB, assicurarsi che al router GPON non siano collegati più di 4 dispositivi.
- Se il dispositivo di archiviazione USB richiede l'uso di un'alimentazione esterna, accertarsi che l'alimentazione esterna sia stata collegata.
- Se si utilizza un hard drive USB, assicurarsi che il suo file system sia FAT32, exFat, NTFS o HFS+.
- Prima di scollegare fisicamente un dispositivo USB dal router, rimuoverlo in modo sicuro per evitare danni ai dati: Andare su [Avanzate](#) > [Impostazioni USB](#) > [Impostazioni Dispositivo](#) e fare clic su [Rimuovi](#).

6. 1. 1. Accesso al dispositivo USB in locale

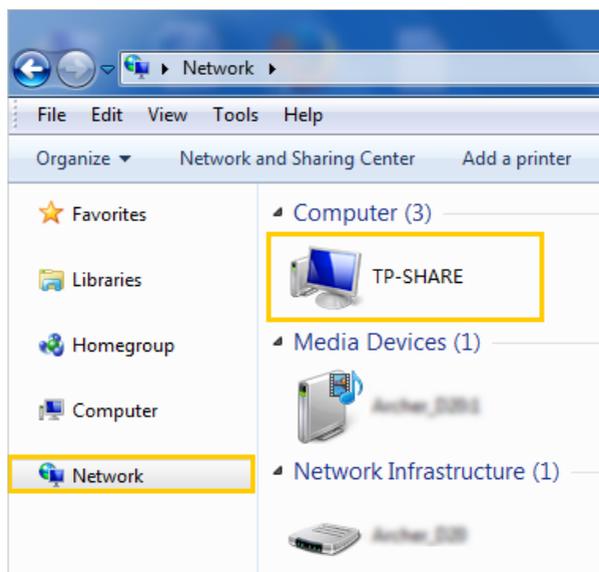
Inserire il dispositivo di archiviazione USB nella porta USB del router GPON e fare riferimento alla seguente tabella per accedere ai file memorizzati sul dispositivo di archiviazione USB.

Computer Windows

- **Metodo 1:**

Accedere a [Computer](#) > [Rete](#), quindi fare clic sul nome del server di rete (TP- SHARE di default) nella sezione [Computer](#).

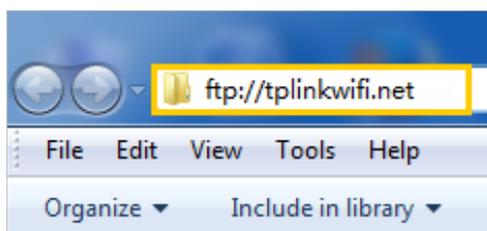
📌 Nota: Le operazioni nei diversi sistemi sono simili. Prendiamo come esempio Windows 7.



Computer Windows

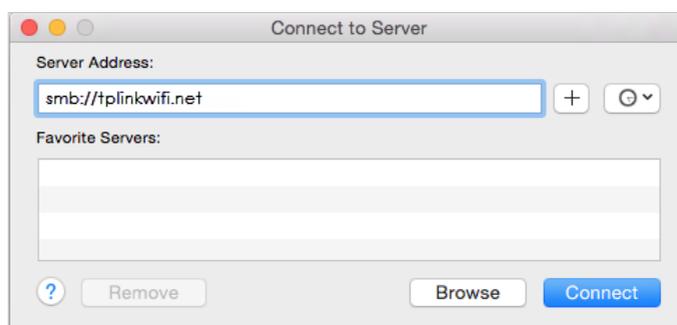
- **Metodo 2:**

Aprire **Windows Explorer** (o andare su **Computer**) e digitare l'indirizzo del server `\\tplinkwifi.net` o `ftp://tplinkwifi.net` nella barra degli indirizzi, quindi premere **Invio**.



Mac

- 1) Selezionare **Vai > Connetti al server**.
- 2) Digita l'indirizzo del server `smb://tplinkwifi.net`.
- 3) Fai clic su **Connetti**.



- 4) Quando viene richiesto, selezionare la casella di opzione **Ospite**. (Se sono stati impostati un nome utente e una password per impedire l'accesso anonimo ai dischi USB, è necessario selezionare la casella di opzione **Utente registrato**). Per sapere come impostare un account per l'accesso, consultare la sezione [Per Impostare l'autenticazione per la sicurezza dei dati](#)).

Tablet

Utilizzare un'applicazione di terze parti per la gestione dei file di rete.

☞ **Suggerimento:** È possibile accedere al dispositivo di archiviazione USB anche utilizzando il nome del server di rete/media come indirizzo del server. Per ulteriori informazioni, consultare la sezione [Per Personalizzare l'indirizzo del dispositivo di archiviazione USB](#).

6. 1. 2. Accesso remoto al dispositivo USB

È possibile accedere al disco USB al di fuori della rete locale. Ad esempio, è possibile:

- Condividere foto e altri file di grandi dimensioni con i vostri amici senza dover accedere a (e pagare) un sito di condivisione di foto o un sistema di posta elettronica.
- Procurarsi un backup sicuro dei materiali per una presentazione.
- Rimuovere di tanto in tanto i file sulla scheda di memoria della fotocamera durante il viaggio.

Nota: Se Wind3 assegna un indirizzo IP WAN privato (come 192.168.x.x o 10.x.x.x), non è possibile utilizzare questa funzione perché gli indirizzi privati non vengono instradati su Internet.

Per configurare le impostazioni di accesso remoto, procedere come segue.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate** > **Impostazioni USB** > **Condivisione Accesso** > **Impostazioni Condivisione**.
3. Selezionare la casella di controllo **FTP**, quindi fare clic su **Salva**.

Impostazione Condivisione

Nome Rete/Server Multimediale:

Abilita	Metodo Accesso	Indirizzo Accesso	Porta
<input checked="" type="checkbox"/>	Server Multimediale	--	--
<input checked="" type="checkbox"/>	Neighborhood Rete	\\XB432v	--
<input checked="" type="checkbox"/>	FTP	ftp://192.168.1.1:21	<input type="text" value="21"/>
<input type="checkbox"/>	FTP(via Internet)	ftp://0.0.0.0:21	21
<input checked="" type="checkbox"/>	HTTP	http://192.168.1.1:8082	<input type="text" value="8082"/>
<input type="checkbox"/>	HTTP (via Internet)	http://0.0.0.0:8082	8082
<input checked="" type="checkbox"/>	HTTPS	https://192.168.1.1:8443	<input type="text" value="8443"/>
<input type="checkbox"/>	HTTPS (via Internet)	https://0.0.0.0:8443	8443

4. Per accedere al disco USB da remoto, fare riferimento alla seguente tabella.

Computer	<p>1) Aprire Windows Explorer (o andare su Computer, solo per gli utenti Windows) o aprire un browser web.</p> <p>2) Digitare l'indirizzo del server nella barra degli indirizzi: Digitare ftp://<indirizzo IP WAN del router>:<numero di porta> (ad esempio ftp://59.40.2.243:21). Se è stato specificato il nome di dominio del router, è possibile digitare anche ftp://<nome di dominio>:<numerodiporta> (adesempio ftp://MyDomainName:21).</p> <div data-bbox="644 527 1136 753" data-label="Image"> </div> <p>3) Premere Invio sulla tastiera.</p> <p>4) Accedere con il nome utente e la password impostati in Per impostare l'autenticazione per la sicurezza dei dati.</p> <p><i>Suggerimenti:</i> È inoltre possibile accedere al disco USB tramite un'applicazione di terze parti per la gestione dei file di rete, che può riprendere i trasferimenti di file interrotti.</p>
	Tablet

Suggerimenti: Fare clic su [Impostazione account del servizio DNS dinamico](#) per imparare a impostare un nome di dominio per il router.

6.1.3. Personalizzare le impostazioni di accesso

Di default, tutti i client di rete possono accedere a tutte le cartelle del disco USB. È possibile personalizzare le impostazioni di condivisione impostando un account di condivisione, condividendo contenuti specifici e impostando un nuovo indirizzo di condivisione nella pagina di gestione web del router.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in [Avanzate](#) > [Impostazioni USB](#) > [Condivisione Accesso](#) > [Impostazioni Condivisione](#).

- **Per Personalizzare l'indirizzo del dispositivo di archiviazione USB**

È possibile personalizzare il nome del server e utilizzarlo per accedere al dispositivo di archiviazione USB.

1. Nella sessione [Impostazioni Condivisione](#), accertarsi che sia selezionata l'opzione [Server Multimediale](#) e inserire un [Nome Rete/Server Multimediale](#) a piacere, ad esempio [MyShare](#), quindi fare clic su [Salva](#).

Impostazione Condivisione

Nome Rete/Server Multimediale:

Abilita	Metodo Accesso	Indirizzo Accesso	Porta
<input checked="" type="checkbox"/>	Server Multimediale	--	--
<input checked="" type="checkbox"/>	Neighborhood Rete	\\XB432v	--
<input checked="" type="checkbox"/>	FTP	ftp://192.168.1.1:21	<input type="text" value="21"/>
<input checked="" type="checkbox"/>	FTP(via Internet)	ftp://0.0.0.0:21	21
<input checked="" type="checkbox"/>	HTTP	http://192.168.1.1:8082	<input type="text" value="8082"/>
<input checked="" type="checkbox"/>	HTTP (via Internet)	http://0.0.0.0:8082	8082
<input checked="" type="checkbox"/>	HTTPS	https://192.168.1.1:8443	<input type="text" value="8443"/>
<input checked="" type="checkbox"/>	HTTPS (via Internet)	https://0.0.0.0:8443	8443

2. Ora è possibile accedere al dispositivo di archiviazione USB visitando **\\MyShare** (per Windows) o **smb://MyShare** (per Mac).

- **Per Impostare l'autenticazione per la sicurezza dei dati**

È possibile impostare l'autenticazione per il dispositivo di archiviazione USB in modo che i clienti di rete debbano inserire nome utente e password quando accedono al dispositivo di archiviazione USB.

1. Nella sezione **Condivisione Account**, attivare **Usa un Nuovo Account**.

Condivisione Account

Per condividere dei contenuti serve un account di condisione. Puoi usare l'account di login o crearne uno nuovo.

Account: Usa Account di Default
 Usa un Nuovo Account

Username:

Password:

Conferma Password:

2. Modificare l'account di accesso. Il nome utente e la password sono entrambi **admin** per l'account amministratore di default e entrambi **visit** per l'account visitatore di

default. L'accesso come utente L'amministratore può leggere e modificare le cartelle condivise, mentre i visitatori possono solo leggere le cartelle condivise.

Condivisione Cartella

Condividi Tutto:

Abilita Autenticazione:

[Aggiorna](#)

ID	Nome Cartella	Percorso Cartella	Nome Volume
--	--	--	--

Note:

1. Per gli utenti Windows, non impostare il nome utente di condivisione come il nome utente di Windows. In caso contrario, il meccanismo delle credenziali di Windows potrebbe causare i seguenti problemi:
 - Se la password di condivisione è uguale a quella di Windows, l'autenticazione non funzionerà perché Windows utilizzerà automaticamente le informazioni del suo account per l'accesso USB.
 - Se la password di condivisione è diversa da quella di Windows, quest'ultimo non sarà in grado di ricordare le credenziali e sarà sempre necessario inserire la password di condivisione per l'accesso USB.
2. A causa del meccanismo delle credenziali di Windows, potrebbe essere impossibile accedere al disco USB dopo aver modificato le impostazioni di autenticazione. Uscire da Windows e riprovare ad accedere. In alternativa, è possibile modificare l'indirizzo del disco USB facendo riferimento a [Per Personalizzare l'indirizzo del dispositivo di archiviazione USB](#).

6.2. Condivisione Media

La funzione di **condivisione multimediale** consente di visualizzare le foto, riprodurre la musica e guardare i filmati memorizzati sul dispositivo di archiviazione USB direttamente dai dispositivi che supportano DLNA, come computer, tablet e PS2/3/4.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Impostazioni USB > Condivisione Accesso > Impostazioni Condivisione**.
3. Abilitare il **Server Multimediale**.

Impostazione Condivisione

Nome Rete/Server Multimediale:

Abilita	Metodo Accesso	Indirizzo Accesso	Porta
<input checked="" type="checkbox"/>	Server Multimediale	--	--
<input checked="" type="checkbox"/>	Neighborhood Rete	\\XB432v	--
<input checked="" type="checkbox"/>	FTP	ftp://192.168.1.1:21	<input type="text" value="21"/>
<input type="checkbox"/>	FTP (via Internet)	ftp://0.0.0.0:21	21
<input checked="" type="checkbox"/>	HTTP	http://192.168.1.1:8082	<input type="text" value="8082"/>
<input type="checkbox"/>	HTTP (via Internet)	http://0.0.0.0:8082	8082
<input checked="" type="checkbox"/>	HTTPS	https://192.168.1.1:8443	<input type="text" value="8443"/>
<input type="checkbox"/>	HTTPS (via Internet)	https://0.0.0.0:8443	8443

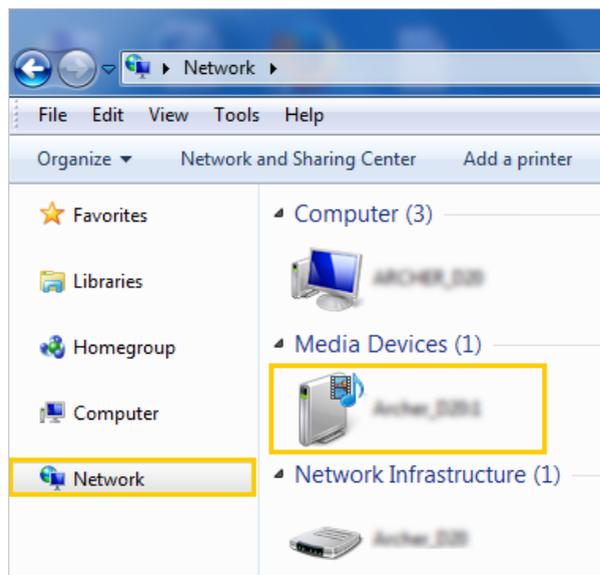
4. Quando il dispositivo di archiviazione USB è inserito nel router, i dispositivi supportati da DLNA (come il computer e il pad) collegati al router possono rilevare e riprodurre i file multimediali contenuti nei dispositivi di archiviazione USB.

5. Per istruzioni dettagliate, consultare la tabella seguente.

- Andare in **Computer > Rete**, quindi fare clic sul nome del Server Multimediale (**numero di modello condiviso** di default) nella sezione **Dispositivi multimediali**.

Nota: Prendiamo come esempio Windows 7.

Computer Windows



Tablet

- Utilizzare un lettore di terze parti con supporto DLNA.

6.3. Impostazioni 3G/4G

Time Machine esegue il backup di tutti i file del computer Mac su un dispositivo di archiviazione USB collegato al router.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare su **Avanzate > Impostazioni USB > Impostazioni 3G/4G**.

The screenshot shows the 'Impostazioni 3G/4G' configuration page. It features several sections: a main configuration area with a checked checkbox 'Abilita 3G/4G come soluzione di backup per accesso a Internet', fields for 'Modem USB 3G/4G' (Scollegato), 'Stato PIN' (Sconosciuto), and 'ISP Mobile' (Other); a manual configuration section with a checked checkbox 'Imposta manualmente Dial Number, APN, Username e Password', and fields for 'Dial Number' (*99#), 'APN' (internet.it), 'Username' (optional), 'Password' (optional), 'Modalità Connessione' (Sempre Attiva), 'Max Idle Time' (15 minuti), and 'Tipo Autenticazione' (PAP); an 'Avanzate' section with 'Dimensione MTU (in byte)' (1480) and 'Intervallo Richiesta Echo' (30 secondi); and checkboxes for 'Usa il seguente Indirizzo IP' and 'Usa i Seguenti Server DNS'. At the bottom, there are 'Connetti', 'Disconnetti', and 'Salva' buttons.

3. Spuntare la casella di controllo per abilitare il 3G/4G come soluzione di backup per l'accesso a Internet.

4. Spuntare la casella di controllo per impostare manualmente **Dial Number**, **APN**, **Username** e **password**.

▀ **Nota:** Le seguenti Impostazioni Avanzate vengono visualizzate solo se si attiva il 3G/4G come soluzione di backup per l'accesso a Internet.

5. Fare clic su **Salva**.

Capitolo 7

Rete Ospiti

Questa funzione consente di fornire l'accesso Wi-Fi agli ospiti senza rivelare la rete principale. Quando si hanno ospiti in casa, in appartamento o sul posto di lavoro, è possibile creare una Rete Ospiti per loro. Inoltre, è possibile personalizzare le opzioni della Rete Ospiti per garantire la sicurezza e la privacy della rete.

Contiene le seguenti sezioni:

- [Creare una rete per gli ospiti](#)
- [Customizzare le opzioni della Rete Ospiti](#)

7.1. Creare una rete per gli ospiti

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Wireless > Rete Ospiti**.
3. Creare una Rete Ospiti secondo le necessità.
 - 1) Spuntare la casella di controllo **Abilita** per la rete wireless.
 - 2) Personalizzare l'SSID. Non selezionare **SSID nascosto** se non si vuole che gli ospiti inseriscano manualmente l'SSID per accedere alla rete degli ospiti.
 - 3) Selezionare il tipo di **Sicurezza** e personalizzare la propria password. Se si seleziona **Nessuna Sicurezza**, non è necessaria alcuna password per accedere alla Rete Ospiti.

Guest Network

Guest SSID: Abilita

Nome Rete Wireless (SSID): SSID nascosto

Sicurezza:

Password:
 Basso Medio Alto

Vedersi: Consenti agli ospiti di vedersi fra loro

Salva

4. Fare clic su **Salva**. Ora i vostri ospiti possono accedere alla Rete Ospiti utilizzando l'SSID e la password che avete impostato!

🔗 **Suggerimento:** Per visualizzare le informazioni sulla Rete Ospiti, accedere a **Dashboard** e individuare la sezione **Wi-Fi Ospiti**. È possibile attivare o disattivare comodamente la funzione di Rete Ospiti.

7.2. Customizzare le opzioni della Rete Ospiti

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Wireless > Rete Ospiti**.
3. Personalizzare le opzioni della Rete Ospiti in base alle proprie esigenze.
4. **Consenti agli ospiti di vedersi fra loro**.
5. Selezionare questa casella di controllo se si desidera consentire ai client wireless della Rete Ospiti di comunicare tra loro con metodi quali Reti Vicine e Ping.
6. Fare clic su **Salva**. Ora è possibile garantire la sicurezza e la privacy della rete!

Capitolo 8

NAT Forwarding

La funzione NAT (Network Address Translation) del router GPON fa sì che i dispositivi della LAN utilizzino lo stesso indirizzo IP pubblico per comunicare con i dispositivi su Internet, proteggendo così la rete locale e nascondendo gli indirizzi IP dei dispositivi. Tuttavia, comporta anche il problema che un host esterno non può comunicare inizialmente con un dispositivo specifico della rete locale.

Con la funzione di forwarding, il router GPON può penetrare l'isolamento del NAT e consentire ai dispositivi su Internet di comunicare in modo iniziatico con i dispositivi sulla rete locale, realizzando così alcune funzioni speciali.

Il router TP-Link GPON supporta quattro regole di inoltro. Se sono impostate due o più regole, la priorità di implementazione da alta a bassa è Port Forwarding, Port Triggering, UPnP e DMZ.

Contiene le seguenti sezioni:

- [ALG](#)
- [Impostazione dei servizi pubblici sulla Rete Locale tramite Virtual Server](#)
- [Aprire le porte in modo dinamico con il Port Triggering](#)
- [Liberate le app dalla Restrizione Porte mediante DMZ](#)
- [Per far funzionare senza problemi i giochi online di Xbox con UPnP](#)

8.1. ALG

ALG permette di personalizzare i filtri NAT (Network Address Translation) da collegare al gateway per supportare la traduzione di indirizzi e porte per determinati protocolli "controllo/dati" del livello applicazione come FTP, TFTP, H323 ecc. Si consiglia di mantenere le impostazioni di default.

Potrebbe essere necessario disabilitare SIP ALG quando si utilizzano applicazioni voce e video per creare e accettare una chiamata attraverso il router, poiché alcune applicazioni di comunicazione voce e video non funzionano bene con SIP ALG.

Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON. Andare su **Avanzate** > **NAT Forwarding** > **Application Layer Gateway (ALG)**.

Application Layer Gateway (ALG)	
PPTP Pass-through:	<input checked="" type="checkbox"/> Abilita
L2TP Pass-through:	<input checked="" type="checkbox"/> Abilita
IPSec Pass-through:	<input checked="" type="checkbox"/> Abilita
FTP ALG:	<input checked="" type="checkbox"/> Abilita
TFTP ALG:	<input checked="" type="checkbox"/> Abilita
H323 ALG:	<input type="checkbox"/> Abilita
RTSP ALG:	<input checked="" type="checkbox"/> Abilita
SIP ALG:	<input type="checkbox"/> Abilita

Salva

8.2. Impostazione dei servizi pubblici sulla Rete Locale tramite Virtual Server

I server virtuali sono utilizzati per impostare servizi pubblici sulla rete locale. Un server virtuale è definito come una porta esterna e tutte le richieste provenienti da Internet a questa porta esterna saranno reindirizzate a un computer designato, che deve essere configurato con un indirizzo IP statico o riservato. Quando si crea un server sulla rete locale e si desidera condividerlo su Internet, i server virtuali possono realizzare il servizio e fornirlo agli utenti di Internet.

La tabella visualizza i parametri rilevanti del server virtuale. Per impostare una regola del server virtuale:

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate** > **NAT Forwarding** > **Virtual Server** e fare clic su **Aggiungi**.
3. Selezionare un nome di interfaccia dall'elenco a discesa.

Virtual Server

+ Aggiungi - Elimina

<input type="checkbox"/>	ID	Tipo Servizio	Porta Esterna	IP Interno	Porta Interna	Protocollo	Stato	Modifica
--	--	--	--	--	--	--	--	--

Nota: il server virtuale può essere configurato solo quando è disponibile un'interfaccia. Se la porta esterna è già utilizzata per la gestione remota o CWMP, Virtual Server non avrà effetto.

Nome Interfaccia:

Tipo di servizio: **Vedi Applicazioni Esistenti**

Porta Esterna: (XX-XX o XX)

IP interno:

Porta Interna: (XX o Vuoto, 1-65535)

Protocollo:

Controllo Accessi:

Solo questi indirizzi IP

+ Aggiungi un nuovo IP

/

Tutti

Abilita questa voce

Cancel

4. Fare clic su **Vedi Applicazioni Esistenti** per selezionare un servizio dall'elenco e inserire automaticamente il numero di porta appropriato nei campi **Porta Esterna** e **Porta Interna**. Se il servizio non è presente nell'elenco, inserite il numero di porta esterna (ad esempio 21) o un intervallo di porte (ad esempio 21-25). Lasciare vuota la Porta interna se è uguale alla Porta esterna o inserire un numero di porta specifico (ad es. 21) se la Porta esterna è una porta singola. L'immagine seguente prende come esempio l'applicazione **FTP**.

Virtual Server

+ Aggiungi - Elimina

<input type="checkbox"/>	ID	Tipo Servizio	Porta Esterna	IP Interno	Porta Interna	Protocollo	Stato	Modifica
--	--	--	--	--	--	--	--	--

Nota: il server virtuale può essere configurato solo quando è disponibile un'interfaccia. Se la porta esterna è già utilizzata per la gestione remota o CWMP, Virtual Server non avrà effetto.

Nome Interfaccia:

Tipo di servizio: Vedi Applicazioni Esistenti

Porta Esterna: (XX-XX o XX)

IP interno:

Porta Interna: (XX o Vuoto, 1-65535)

Protocollo:

Controllo Accessi:

Solo questi indirizzi IP

Aggiungi un nuovo IP

/ -

Tutti

Abilita questa voce

Cancella OK

5. Inserire l'indirizzo IP del computer che esegue l'applicazione del servizio nel campo IP interno.
6. Selezionare un protocollo per l'applicazione del servizio: TCP, UDP o TUTTO dall'elenco a discesa Protocollo.
7. Selezionare **Abilita questa voce**.
8. Fare clic su **OK**.

Suggestioni:

- Se si desidera disattivare questa voce, fare clic sull'icona della lampadina.
- Si consiglia di mantenere le impostazioni di default di Porta interna e Protocollo se non si è sicuri di quale porta o protocollo utilizzare.
- Se il dispositivo host locale ospita più di un tipo di servizi disponibili, è necessario creare una regola per ciascun servizio. Si noti che la porta esterna NON deve essere sovrapposta.

8.3. Aprire le porte in modo dinamico con il Port Triggering

Il Port Triggering può specificare una porta triggering e le porte esterne corrispondenti. Quando un host della rete locale avvia una connessione alla porta triggering, tutte le porte esterne vengono aperte per le connessioni successive. Il router può registrare l'indirizzo IP dell'host. Quando i dati provenienti da Internet ritornano alle porte esterne, il router può inoltrarli all'host corrispondente. Il Port Triggering si applica principalmente

a giochi online, VoIP, lettori video e applicazioni comuni, tra cui MSN Gaming Zone, Dialpad e Quick Time 4, ecc.

Seguire la procedura seguente per configurare le regole di Port Triggering:

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > NAT Forwarding > Port Triggering** e fare clic su **Aggiungi**.

Port Triggering

+ Aggiungi - Elimina

<input type="checkbox"/>	ID	Applicazione	Porta Triggering	Protocollo Triggering	Porta Esterna	Protocollo Esterno	Stato	Modifica
--	--	--	--	--	--	--	--	--

Nome Interfaccia:

Applicazione: **Vedi Applicazioni Esistenti**

Port Triggering: (XX)

Protocollo Triggering:

Porta Esterna: (XX o XX-XX o XX,XX-XX)

Protocollo Esterno:

Abilita questa voce

Cancella **OK**

3. Fare clic su **Vedi Applicazioni Esistenti** e selezionare l'applicazione desiderata. La **Porta Triggering**, il **Protocollo Triggering** e la **Porta Esterna** verranno compilati automaticamente. L'immagine seguente prende come esempio l'applicazione **MSN Gaming Zone**.

Port Triggering

+ Aggiungi - Elimina

<input type="checkbox"/>	ID	Applicazione	Porta Triggering	Protocollo Triggering	Porta Esterna	Protocollo Esterno	Stato	Modifica
--	--	--	--	--	--	--	--	--

Nome Interfaccia:

Applicazione: Vedi Applicazioni Esistenti

Port Triggering: (XX)

Protocollo Triggering:

Porta Esterna: (XX o XX-XX o XX,XX-XX)

Protocollo Esterno:

Abilita questa voce

Cancella OK

4. Fare clic su **OK**.

Port Triggering

+ Add - Delete

<input type="checkbox"/>	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
<input type="checkbox"/>	1	MSN Gaming Zone	47624	TCP or UDP	2300-2400, 28800-29000	TCP or UDP	💡	✎ 🗑️

Suggerimenti:

- È possibile aggiungere più regole di attivazione delle porte in base alle esigenze della rete.
- Le porte di attivazione non possono essere sovrapposte.
- Se l'applicazione desiderata non è presente nell'elenco delle Applicazioni esistenti, inserire i parametri manualmente. È necessario verificare prima le porte esterne utilizzate dall'applicazione e inserirle nel campo **Porta Esterna** secondo il formato visualizzato nella pagina.

8. 4. Liberate le app dalla Restrizione Porte mediante DMZ

Quando un PC viene impostato come host DMZ (Demilitarized Zone) sulla rete locale, è totalmente esposto a Internet e può realizzare una comunicazione bidirezionale illimitata tra host interni e host esterni. L'host DMZ diventa un server virtuale con tutte le porte aperte. Quando non si sa quali porte aprire in alcune applicazioni speciali, come le telecamere IP e i software di database, è possibile impostare il PC come host DMZ.

Nota: Quando la DMZ è attivata, l'host DMZ è totalmente esposto a Internet, il che può comportare alcuni potenziali rischi per la sicurezza. Se la DMZ non è in uso, si prega di disattivarla in tempo.

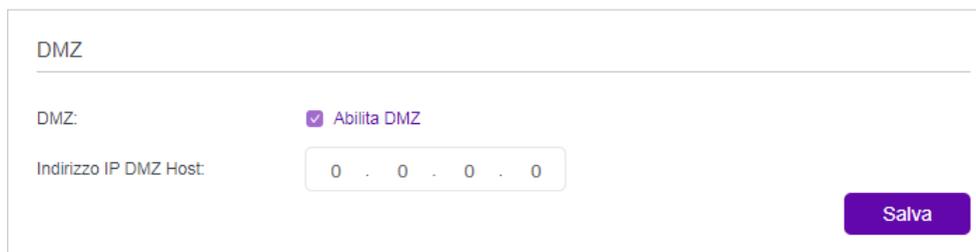
Voglio farlo:

Il PC di casa può partecipare al gioco online su Internet senza limitazioni di porta.

Ad esempio, a causa di una restrizione delle porte, quando si gioca online è possibile accedere normalmente, ma non è possibile unirsi a una squadra con altri giocatori. Per risolvere questo problema, impostare il PC come host DMZ con tutte le porte aperte.

Come posso farlo?

1. Assegnare al PC un indirizzo IP statico, ad esempio 192.168.1.100.
2. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
3. Andare su **Avanzate > NAT Forwarding > DMZ** e spuntare per abilitare la DMZ.
4. Inserire manualmente l'indirizzo IP del PC 192.168.1.100 nel campo **Indirizzo IP host DMZ**.



5. Fare clic su **Salva**.

Fatto!

La configurazione è completata. Avete impostato il vostro PC come host DMZ e ora potete creare una squadra per giocare con altri giocatori.

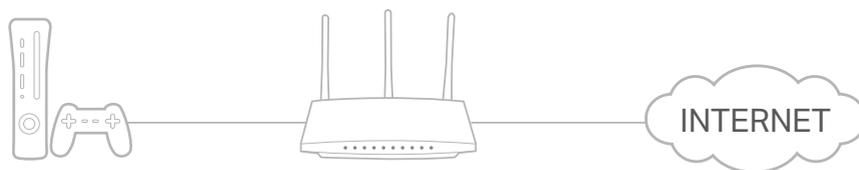
8. 5. Per far funzionare senza problemi i giochi online di Xbox con UPnP

Il protocollo UPnP (Universal Plug and Play) consente alle applicazioni o ai dispositivi host di trovare automaticamente il dispositivo NAT front-end e di inviargli la richiesta di aprire le porte corrispondenti. Con l'UPnP abilitato, le applicazioni o i dispositivi host sulla rete locale e su Internet possono comunicare liberamente tra loro, realizzando così la connessione continua della rete. Potrebbe essere necessario abilitare l'UPnP se si desidera utilizzare applicazioni per giochi multiplayer, connessioni peer-to-peer, comunicazioni in tempo reale (come VoIP o videoconferenze) o assistenza remota, ecc.

🔗 Suggestioni:

- UPnP è abilitato di default in questo router.
- Solo le applicazioni che supportano il protocollo UPnP possono utilizzare questa funzione.
- La funzione UPnP richiede il supporto del sistema operativo (ad esempio, Windows Vista/ Windows 7/ Windows 8, ecc. Alcuni sistemi operativi devono installare i componenti UPnP).

Ad esempio, quando si collega la Xbox al router collegato a Internet per giocare online, l'UPnP invierà al router la richiesta di aprire le porte corrispondenti per consentire la trasmissione dei dati seguenti che penetrano il NAT. Pertanto, è possibile giocare online con la Xbox senza problemi.



Se necessario, è possibile seguire la procedura per modificare lo stato di UPnP.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare su **Avanzate** > **NAT Forwarding** > **UPnP** e attivare o disattivare in base alle proprie esigenze.

UPnP

UPnP:

Elenco Servizi UPnP

Numero Client: 0 [Aggiorna](#)

ID	Descrizione Servizio	Porta Esterna	Protocollo	Indirizzo IP Interno	Porta Interna
--	--	--	--	--	--

Capitolo 9

Parental Control

Questa funzione consente di bloccare i siti web inappropriati, espliciti e dannosi e di controllare l'accesso a siti web specifici in un determinato momento.

Voglio farlo:

Controllare i tipi di siti web che i miei figli o altri utenti della rete domestica possono visitare e l'orario in cui possono accedere a Internet.

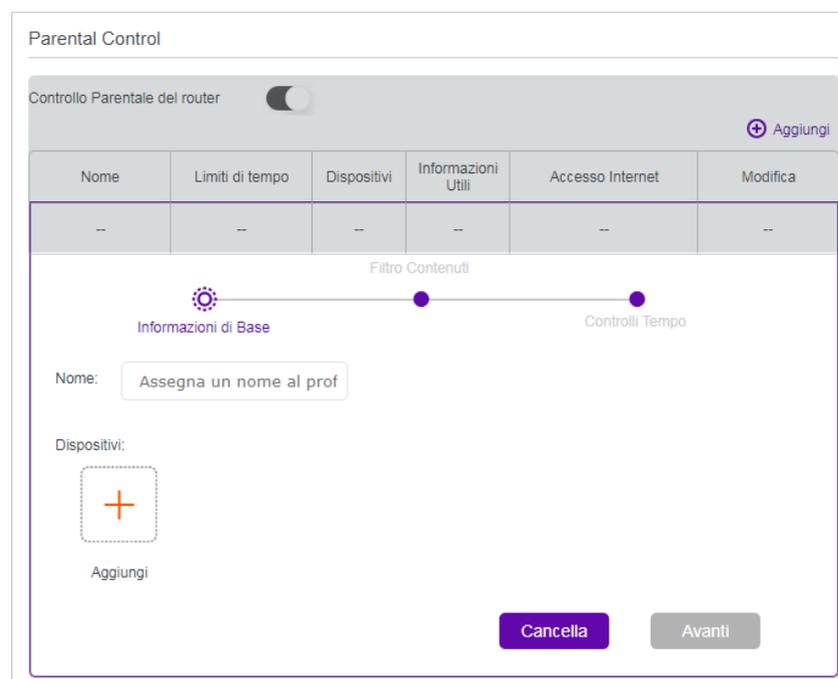
Ad esempio, voglio consentire ai dispositivi dei miei figli (ad esempio un computer o un tablet) di accedere solo a www.tp-link.com e Wikipedia.org dalle 18:00 (6 PM) alle 22:00 (10 PM) nei giorni feriali e non in altri orari.

Come posso farlo?

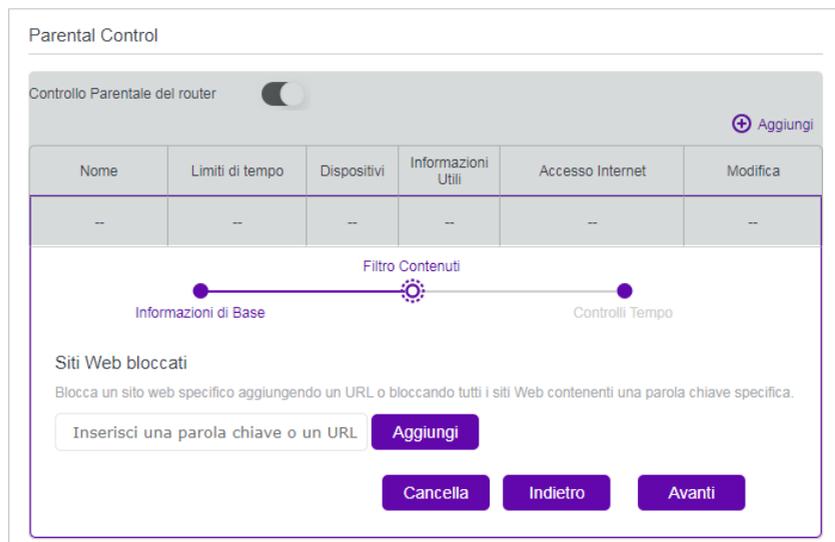
1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare a **Home > Parental Control** o **Avanzate > Parental Control**.



3. Fare clic su **Aggiungi**, quindi inserire manualmente il **Nome**. Fare clic su **Aggiungi** e specificare i dispositivi appartenenti al membro della famiglia. Fare clic su **Avanti**.



4. Selezionare un livello di filtro in base all'età del membro della famiglia. I contenuti bloccati saranno visualizzati nell'elenco Filtro contenuti. Fare clic su **Avanti**.



5. (Facoltativo) Eliminare le voci dall'elenco Filtro Contenuti, aggiungere voci dall'elenco Categorie disponibili o fare clic su Aggiungi una nuova parola chiave per aggiungere una parola chiave del filtro (ad esempio, "Facebook") o un URL.
6. Attivare Limiti di tempo da lunedì a venerdì e sabato e domenica, quindi impostare il tempo giornaliero consentito per l'accesso a Internet. Abilitare Riposo Notturno nelle notti scolastiche (da domenica a giovedì) e nei fine settimana (venerdì e sabato), quindi impostare il periodo di tempo in cui i dispositivi del profilo non possono accedere a Internet.

Parental Control

Controllo Parentale del router + Aggiungi

Nome	Limiti di tempo	Dispositivi	Informazioni Utili	Accesso Internet	Modifica
--	--	--	--	--	--

Filtro Contenuti

Informazioni di Base Controlli Tempo

Giorni della settimana Lun Mar Mer Giov Ven Sab Dom

Limiti di tempo
Imposta limiti di tempo giornalieri per il tempo totale trascorso online.

Giorni della settimana Abilita 20

30Min 80

Fine settimana Abilita 20

30Min 80

Riposo Notturno
Imposta un periodo di tempo durante il quale questo profilo non può accedere a Internet.

Giorni della settimana Abilita Da 10 : 00 PM A 06 : 00 AM

Fine settimana Abilita Da 10 : 00 PM A 06 : 00 AM

7. Fare clic su **Salva**.

Fatto!

Ora potete controllare l'accesso a Internet dei vostri figli secondo le vostre esigenze.

Suggerimenti:

- Per monitorare l'uso di Internet di un membro della famiglia:
1. Trovare il profilo del membro della famiglia, quindi fare clic sull'icona **Approfondimenti**.
 2. Nella pagina **5 Più Visitati**, selezionare un giorno degli ultimi 7 giorni per controllare il tempo trascorso online e i siti web più visitati. Se necessario, è possibile bloccare i siti web.
 3. Nella pagina **Storico Bloccati**, selezionare un giorno degli ultimi 7 giorni per controllare la cronologia dei siti web bloccati. Se necessario, è possibile **sbloccare i siti web** e fare clic su Siti web bloccati per visualizzarli.

Parental Control

Controllo Parentale del router  + Aggiungi

Nome	Limiti di tempo	Dispositivi	Informazioni Utili	Accesso Internet	Modifica
123	2o	0			 

5 più visitati
Storico bloccato
^

Oggi v



- Per sospendere o riprendere l'accesso a Internet di un membro della famiglia: Individuare il profilo del familiare, quindi fare clic sull'icona **Pausa/Play**.

Parental Control

Controllo Parentale del router  + Aggiungi

Nome	Limiti di tempo	Dispositivi	Informazioni Utili	Accesso Internet	Modifica
123	2o	0		 In pausa	 

Capitolo 10

QoS

Questa funzione consente di specificare la priorità del traffico e di ridurre al minimo l'impatto della congestione della rete.

Questo capitolo contiene le seguenti sezioni:

Il router GPON consente di configurare il QoS (Quality of Service) per ottimizzare il throughput e le prestazioni nella gestione del traffico wireless differenziato, come VoIP (VoiceoverIP), altri tipi di audio, video, media in streaming e dati IP tradizionali.

Per configurare il QoS sui router GPON, è necessario impostare i parametri delle code di trasmissione per i diversi tipi di traffico wireless. Nell'uso normale, si consiglia di mantenere i valori di default per i router GPON.

Questa funzione aiuta il router GPON ad allocare l'ampiezza di banda upstream per migliorare le prestazioni complessive della rete.

Per impostare il QoS per la rete:

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare su **Avanzate > QoS**.
3. Abilitare **QoS**.

QoS

QoS: Abilita

Ampiezza di Banda Upload: Mbps

IPTV QoS: Abilita

VoIP QoS: Abilita

Avanzate

Alto 60%

Medio 30%

Basso 10%

Salva

4. Immettere l'**Ampiezza di Banda Upload** totale fornita da Wind3.
5. (Facoltativo) Abilitare **IPTV QoS** o **VoIP QoS**, quindi impostare la priorità e l'ampiezza di banda riservata del traffico IPTV o VoIP.

The screenshot shows the 'QoS' configuration page. At the top, there is a 'QoS' section with a checked checkbox labeled 'Abilita'. Below this, there is a field for 'Ampiezza di Banda Upload' with a dropdown menu set to 'Mbps'. Further down, there are two more checked checkboxes labeled 'IPTV QoS:' and 'VoIP QoS:'. A red box highlights these two checkboxes. Below these is an 'Avanzate' section with an upward-pointing arrow icon. Under 'Avanzate', there are three sliders for 'Alto', 'Medio', and 'Basso' priorities, with values of 60%, 30%, and 10% respectively. A 'Salva' button is located at the bottom right.

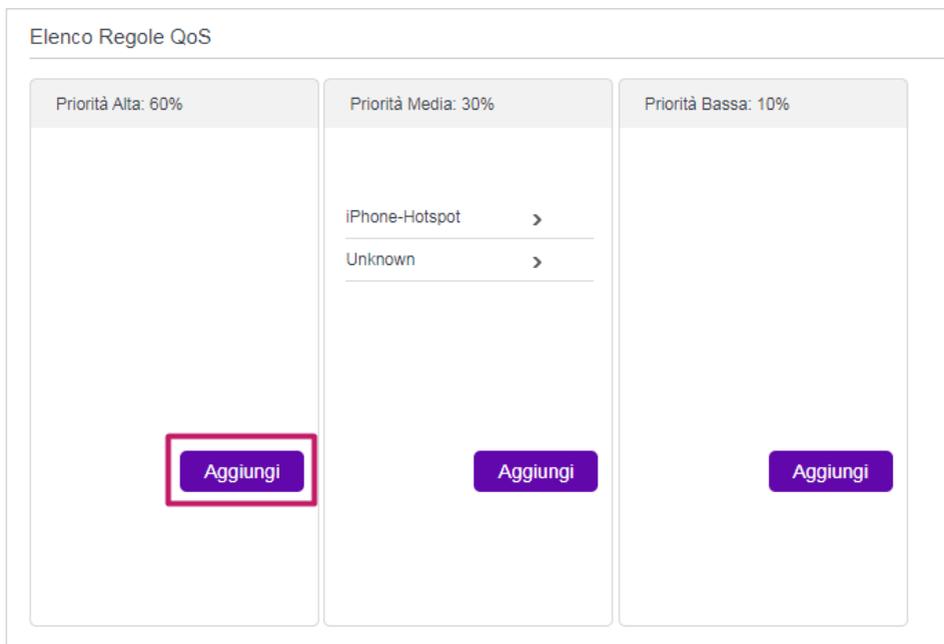
6. (Facoltativo) Fare clic su **Avanzate** e disporre i cursori per impostare la percentuale di ampiezza di banda di ciascuna priorità.

This screenshot is similar to the previous one, but the 'Avanzate' section is expanded. The 'Avanzate' icon is now highlighted with a red box. The sliders for 'Alto', 'Medio', and 'Basso' are visible, showing the same 60%, 30%, and 10% values. The 'Salva' button remains at the bottom right.

7. Fare clic su **Salva** per rendere effettive le impostazioni.

Per impostare il QoS per un dispositivo specifico:

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il dispositivo mesh.
2. Andare su **Avanzate > QoS**.
3. Nella tabella **Elenco Regole QoS**, scegliere una sezione di priorità e fare clic su **Aggiungi**.



4. Nella finestra Regola QoS, fare clic su **Scansiona** e su  per scegliere un dispositivo, quindi fare clic su **OK** per aggiungerlo alla regola.



ID	Nome Dispositivo	Indirizzo IP	Indirizzo MAC	Operazione
1	Unknown			

Capitolo 11

Sicurezza

Questo capitolo spiega come proteggere la rete domestica da utenti non autorizzati implementando funzioni di sicurezza di rete. È possibile bloccare o consentire l'accesso alla rete wireless a specifici dispositivi client utilizzando il filtro MAC o il controllo degli accessi per le reti cablate e wireless, oppure prevenire gli attacchi ARP e spoofing ARP utilizzando il IP & MAC Binding.

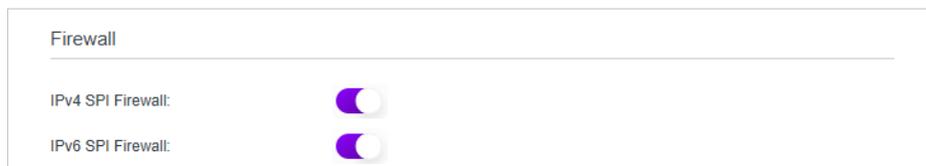
Questo capitolo contiene le seguenti sezioni:

- [Firewall e Protezione DoS](#)
- [Filtro Servizi](#)
- [Controllo Accessi](#)
- [IP e MAC Binding](#)

11. 1. Firewall e Protezione DoS

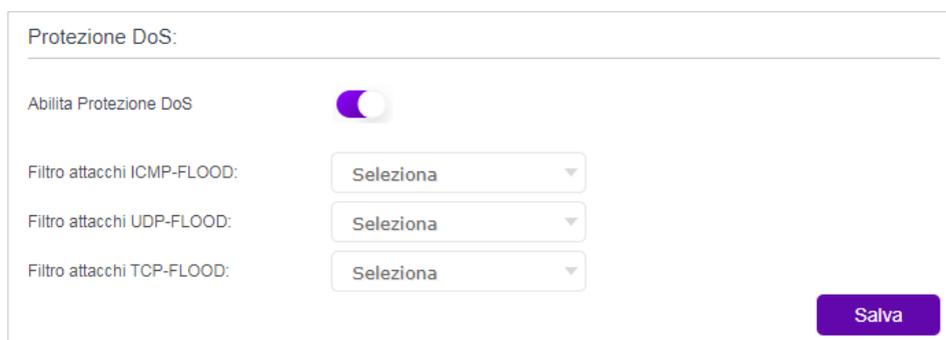
Il Firewall SPI (Stateful Packet Inspection) e la Protezione DoS (Denial of Service) proteggono il router dagli attacchi informatici.

Il Firewall SPI può prevenire gli attacchi informatici e convalidare il traffico che passa attraverso il router in base al protocollo. Questa funzione è abilitata di default e si consiglia di mantenere le impostazioni di default.



Protezione DoS può proteggere la rete domestica dagli attacchi DoS che inondano la rete di richieste server. Per configurare la protezione DoS, procedere come segue.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Sicurezza > DDoS**.



3. Abilitare la **Abilita Protezione DoS**.
4. Impostare il livello di protezione (**Basso**, **Medio** o **Alto**) per il **Filtro attacchi ICMP-FLOOD**, il **Filtro attacchi UDP-FLOOD** e il **Filtro attacchi TCP-FLOOD**.
 - **Filtro attacchi ICMP-FLOOD** - Abilitare per prevenire attacchi ICMP (Internet Control Message Protocol) flood.
 - **Filtro attacchi UDP-FLOOD** - Abilitare per prevenire attacchi UDP (User Datagram Protocol) flood.
 - **Filtro attacchi TCP-FLOOD** - Abilita per prevenire attacchi TCP (Transmission Control Protocol) flood.
5. Fare clic su **Salva**.

🔗 Suggerimenti:

1. Il livello di protezione si basa sul numero di pacchetti di traffico. È possibile specificare il livello in **Impostazioni Livello Protezione DoS**.

Impostazioni Livello Protezione DoS

Livello Protezione ICMP-FLOOD:	Basso:	<input type="text" value="3600"/>	(5-3600) Pacchetti/Sec
	Medio:	<input type="text" value="2400"/>	(5-3600) Pacchetti/Sec
	Alto:	<input type="text" value="1200"/>	(5-3600) Pacchetti/Sec
Livello Protezione UDP-FLOOD:	Basso:	<input type="text" value="3600"/>	(5-3600) Pacchetti/Sec
	Medio:	<input type="text" value="2400"/>	(5-3600) Pacchetti/Sec
	Alto:	<input type="text" value="1200"/>	(5-3600) Pacchetti/Sec
Livello Protezione TCP-SYN-FLOOD:	Basso:	<input type="text" value="3600"/>	(5-3600) Pacchetti/Sec
	Medio:	<input type="text" value="2400"/>	(5-3600) Pacchetti/Sec
	Alto:	<input type="text" value="1200"/>	(5-3600) Pacchetti/Sec

2. La protezione viene attivata immediatamente quando il numero di pacchetti supera il valore di soglia preimpostato e l'host nocivo viene visualizzato nella [Lista Host DoS Bloccati](#).

Lista Host DoS bloccati

Numero Host:0 [Aggiorna](#) [Elimina](#)

<input type="checkbox"/>	ID	Indirizzo IP	Indirizzo MAC
--	--	--	--

11. 2. Filtro Servizi

Con il filtro dei servizi, è possibile impedire a determinati utenti di accedere al servizio specificato e persino bloccare completamente l'accesso a Internet.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in [Avanzate](#) > [Sicurezza](#) > [Filtro Servizi](#) e attivare il [Filtro Servizi](#).

Filtro Servizi

Filtro Servizi:

3. Fare clic su [Aggiungi](#).

4. Selezionate un **Tipo Servizio** dall'elenco a discesa e i quattro campi seguenti verranno compilati automaticamente. Se il tipo di servizio desiderato non è presente nell'elenco, selezionare **Personalizzato** e inserire le informazioni manualmente.
5. Specificare gli indirizzi IP a cui applicare questa regola di Filtro.
6. Fare clic su **OK** per rendere effettive le impostazioni.

11.3. Controllo Accessi

Il controllo degli accessi serve a bloccare o consentire l'accesso alla rete (via cavo o wireless) a specifici dispositivi client in base a un elenco di dispositivi bloccati (Blacklist) o a un elenco di dispositivi autorizzati (Whitelist).

Voglio farlo: Bloccare o consentire a specifici dispositivi client di accedere alla mia rete (via cavo o wireless).

Come posso farlo?

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Sicurezza > Controllo Accessi** e attivare il **Controllo Accessi**.

3. Selezionare la modalità di accesso per bloccare (consigliato) o autorizza l'accesso del dispositivo alla rete.

Per bloccare uno o più dispositivi specifici:

- 1) Selezionare **Nega l'accesso alle periferiche elencate** e fare clic su **Salva**.

Modalità di funzionamento

Modalità di funzionamento: Nega l'accesso alle periferiche elencate
 Permetti l'accesso alle periferiche elencate

Salva

- 2) Selezionare il dispositivo o i dispositivi da bloccare nella tabella **Periferiche online** (oppure fare clic su **Aggiungi** sotto **Elenco periferiche** e inserire manualmente il **Nome Dispositivo** e l'**Indirizzo MAC**).
- 3) Fare clic su **Blocca** sopra la tabella **Periferiche online**. I dispositivi selezionati verranno aggiunti automaticamente alla **Elenco periferiche**.

Elenco periferiche

+ Aggiungi - Elimina

<input type="checkbox"/>	ID	Nome Dispositivo	Indirizzo MAC	Modifica
--	--	--	--	--

Nome Dispositivo: **Scansiona**

Indirizzo MAC: **Cancella** **OK**

Periferiche online

↻ Aggiorna 🔒 Blocca

<input type="checkbox"/>	ID	Nome Dispositivo	Indirizzo IP	Indirizzo MAC	Tipo Connessione
<input type="checkbox"/>	1	Unknown	██████	██████	Cablato

Per consentire uno specifico dispositivo:

- 1) Selezionare **Permetti l'accesso alle periferiche elencate** e fare clic su **Salva**.

Modalità di funzionamento

Modalità di funzionamento: Nega l'accesso alle periferiche elencate
 Permetti l'accesso alle periferiche elencate

Salva

- 2) Fare clic su **Aggiungi** nella sezione **Elenco periferiche**.

Elenco periferiche

+ Aggiungi - Elimina

<input type="checkbox"/>	ID	Nome Dispositivo	Indirizzo MAC	Modifica
--	--	--	--	--

Nome Dispositivo: Scansiona

Indirizzo MAC: Cancella OK

Periferiche online

↻ Aggiorna

<input type="checkbox"/>	ID	Nome Dispositivo	Indirizzo IP	Indirizzo MAC	Tipo Connessione
<input type="checkbox"/>	1	Unknown	---	---	Cablato

- 3) Inserire il **Nome Dispositivo** e l'**Indirizzo MAC**. (È possibile copiare e incollare le informazioni dalla tabella **Periferiche online** se il dispositivo è collegato alla rete).
- 4) Fare clic su **OK**.

Fatto!

Ora è possibile bloccare o consentire l'accesso di specifici dispositivi client alla rete (via cavo o wireless) mediante **Elenco periferiche**.

11.4. IP e MAC Binding

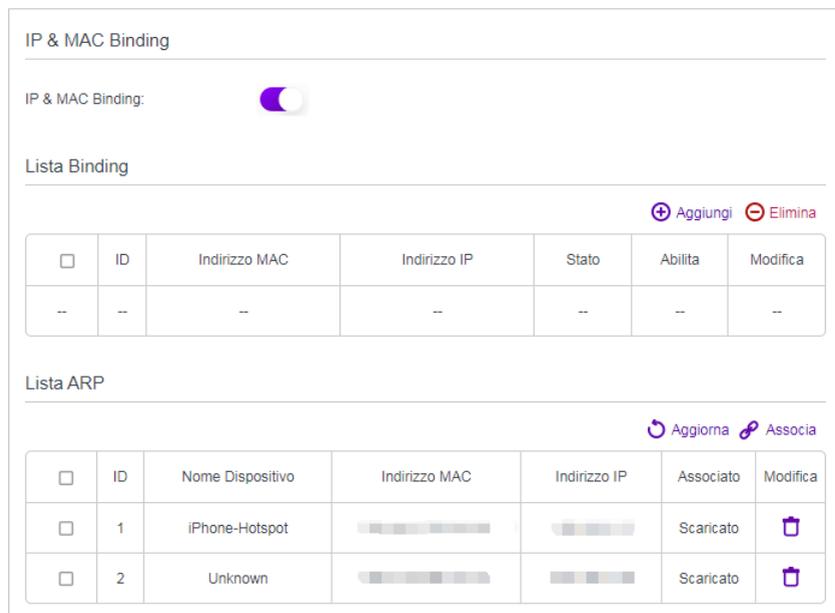
Il IP & MAC Binding, ovvero il binding ARP (Address Resolution Protocol), viene utilizzato per associare l'indirizzo IP di un dispositivo di rete al suo indirizzo MAC. In questo modo si previene lo spoofing ARP e altri attacchi ARP, negando l'accesso alla rete a un dispositivo con un indirizzo IP corrispondente nell'elenco di binding, ma con un indirizzo MAC non riconosciuto.

Voglio farlo:

Prevenire gli attacchi ARP spoofing e ARP.

Come posso farlo?

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate** > **Sicurezza** > **IP & MAC Binding** e abilitare **IP & MAC Binding**.



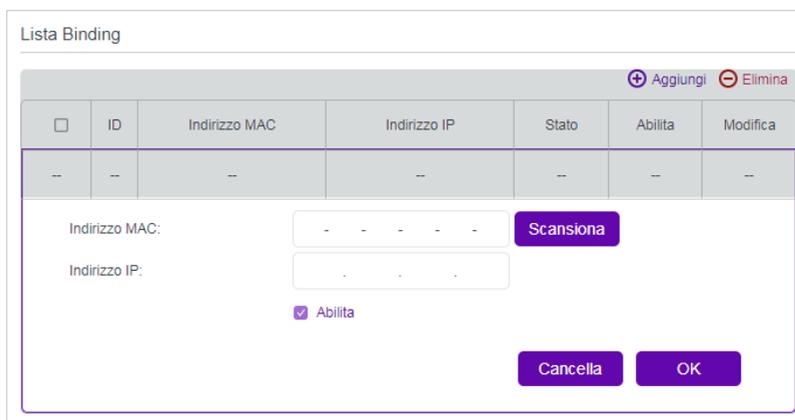
3. Associare i dispositivi in base alle proprie esigenze.

Per eseguire il binding dei dispositivi collegati:

- 1) Selezionare il dispositivo o i dispositivi da associare nell'**Lista ARP**.
- 2) Fare clic su **Bind** per aggiungerlo all'**Lista Binding**.

Per collegare il dispositivo non connesso:

- 1) Fare clic su **Aggiungi** nella sezione **Lista Binding**.



- 2) Inserire l'**Indirizzo MAC** e l'**Indirizzo IP** che si desidera associare.
- 3) Selezionare la casella di controllo **Abilita** per abilitare la voce e fare clic su **OK**.

Fatto!

Godetevi Internet senza preoccuparvi di ARP spoofing e attacchi ARP.

Capitolo 12

VPN Server&Client

Il router offre diversi modi per impostare le connessioni VPN:

Il **server VPN** consente ai dispositivi remoti di accedere alla rete domestica in modo sicuro attraverso Internet. Il router supporta tre tipi di server VPN:

OpenVPN è un po' complesso ma con una maggiore sicurezza e stabilità, adatto ad ambienti ristretti come la rete del campus e l'intranet aziendale.

La **VPN PPTP** è facile da usare con il software VPN integrato di computer e dispositivi mobili, ma è vulnerabile e può essere bloccata da alcuni ISP.

La **VPN L2TP/IPSec** è più sicura ma più lenta della VPN PPTP e può avere problemi a superare i firewall.

VPN Client consente ai dispositivi della rete domestica di accedere ai server VPN remoti, senza la necessità di installare il software VPN su ogni dispositivo.

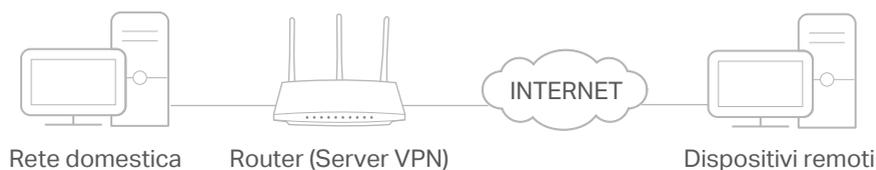
Questo capitolo contiene le seguenti sezioni:

- [Utilizzo OpenVPN per accedere alla rete domestica](#)
- [Utilizzo VPN PPTP per accedere alla rete domestica](#)
- [Utilizzo VPN IPSec per accedere alla rete domestica](#)
- [Connessioni VPN](#)

12.1. Utilizzo OpenVPN per accedere alla rete domestica

Il server OpenVPN viene utilizzato per creare una connessione OpenVPN che consente ai dispositivi remoti di accedere alla rete domestica.

Per utilizzare la funzione VPN, è necessario abilitare il server OpenVPN sul router e installare ed eseguire il software client VPN sui dispositivi remoti. Per configurare una connessione OpenVPN, seguire la seguente procedura.



Passo1 Impostazione del server OpenVPN sul router

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andate su **Avanzate > VPN > OpenVPN** e spuntate la casella **Abilita Server VPN**.

OpenVPN

Nota: Nessun certificato al momento, **Genera un certificato** prima di abilitare il Server VPN.

Abilita Server VPN

Tipo Servizio: UDP TCP

Porta di Servizio:

VPN Subnet/Netmask:

Accesso Client: Solo Rete Domestica Internet e Rete Domestica

Salva

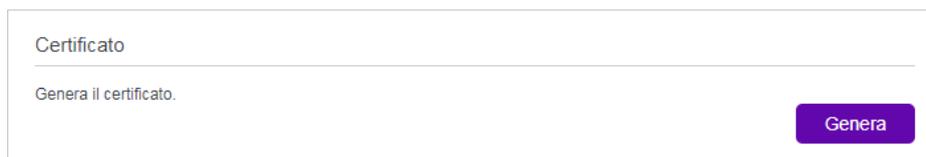
■ Note:

- Prima di attivare il server VPN, si consiglia di configurare il servizio DNS dinamico (consigliato) o di assegnare un indirizzo IP statico alla porta WAN del router e di sincronizzare l'ora del sistema con Internet.
 - La prima volta che si configura il server OpenVPN, potrebbe essere necessario generare un certificato prima di abilitare il server VPN.
3. Selezionare il **Tipo Servizio** (protocollo di comunicazione) per il server OpenVPN: UDP, TCP.
 4. Inserire una **Porta di Servizio** VPN a cui si connette un dispositivo VPN; il numero della porta deve essere compreso tra 1024 e 65535.
 5. Nei campi **VPN Subnet/Netmask**, inserire il range di indirizzi IP che possono essere assegnati al dispositivo dal server OpenVPN.
 6. Selezionare il tipo di **Accesso client**. Selezionare **Solo Rete Domestica** se si desidera che il dispositivo remoto acceda solo alla rete domestica; selezionare **Internet e Rete**

Domestica se si desidera che il dispositivo remoto acceda anche a Internet attraverso il server VPN.

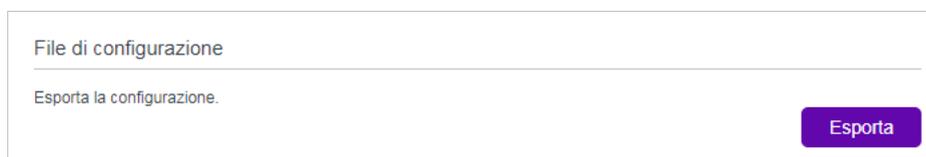
7. Fare clic su **Salva**.

8. Fare clic su **Genera** per ottenere un nuovo certificato.



Nota: Se ne avete già generato uno, saltate questo passaggio, oppure fate clic su **Genera** per aggiornare il certificato.

9. Fare clic su **Esporta** per salvare il file di configurazione OpenVPN che verrà utilizzato dal dispositivo remoto per accedere al router.



Passo 2 Configurazione della connessione OpenVPN sul dispositivo remoto

1. Visitare il sito <http://openvpn.net/index.php/download/community-downloads.html> per scaricare il software OpenVPN e installarlo sul dispositivo in cui si desidera eseguire l'utility client OpenVPN.

Nota: È necessario installare l'utility client **OpenVPN** su ogni dispositivo che si intende applicare alla funzione VPN per accedere al router. I dispositivi mobili devono scaricare un'applicazione di terze parti da Google Play o Apple App Store.

2. Dopo l'installazione, copiare il file esportato dal router nella cartella "config" dell'utility client OpenVPN (ad esempio, **C:\Program Files\OpenVPN\config** su Windows). Il percorso dipende dal luogo in cui è installata l'utility client OpenVPN.

3. Eseguire l'utility client OpenVPN e collegarla al server OpenVPN.

12.2. Utilizzo VPN PPTP per accedere alla rete domestica

Il server VPN PPTP viene utilizzato per creare una connessione VPN PPTP che consente ai dispositivi remoti di accedere alla rete domestica.

Per utilizzare la funzione VPN, è necessario impostare il server VPN PPTP sul router e configurare la connessione PPTP sui dispositivi remoti. Per configurare una connessione PPTP VPN, attenersi alla seguente procedura.

Passo 1 Impostazione del server VPN PPTP sul router

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.

2. Andate su **Avanzate > VPN > VPN PPTP** e spuntate la casella **Abilita Server VPN**.

VPN PPTP

Abilita Server VPN

Indirizzo IP Client: 10 . 7 . 0 . 11 -10.7.0. 20 (fino a 10 client)

Username:

Password:

Salva

Nota:

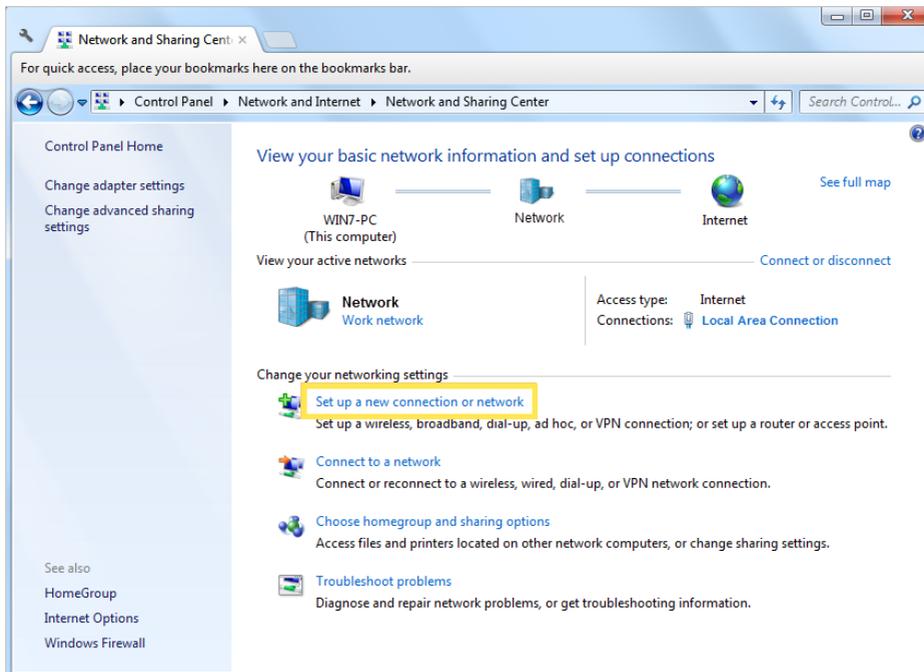
Prima di attivare il **Server VPN**, si consiglia di configurare il Servizio DNS Dinamico (consigliato) o di assegnare un indirizzo IP statico alla porta WAN del router e di sincronizzare l'**ora del sistema** con Internet.

3. Nel campo **Indirizzo IP Client**, inserire il range di indirizzi IP (fino a 10) che possono essere affittati ai dispositivi dal server PPTP VPN.
4. Immettere il **Username** e la **Password** per autenticare i clienti al server PPTP VPN.
5. Fare clic su **Salva**.
6. Sui dispositivi client, creare una connessione VPN PPTP. Le piattaforme ufficiali supportate sono Windows, Mac OSX, Linux, iOS e Android.
7. Avviare il programma PPTP VPN, aggiungere una nuova connessione e inserire il nome di dominio del servizio DDNS registrato o l'indirizzo IP statico assegnato alla porta WAN, per collegare il dispositivo client al server PPTP VPN.

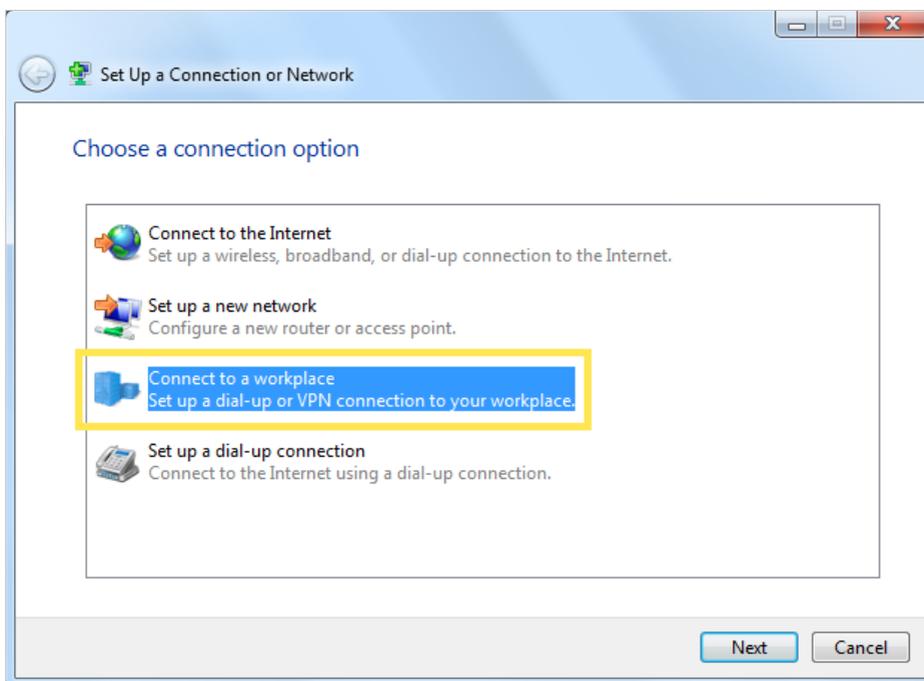
Passo 2 Configurare la connessione VPN PPTP sul dispositivo remoto

Il dispositivo remoto può utilizzare il software PPTP integrato in Windows o un software PPTP di terze parti per connettersi al server PPTP. In questo caso utilizziamo il **software PPTP integrato in Windows** come esempio.

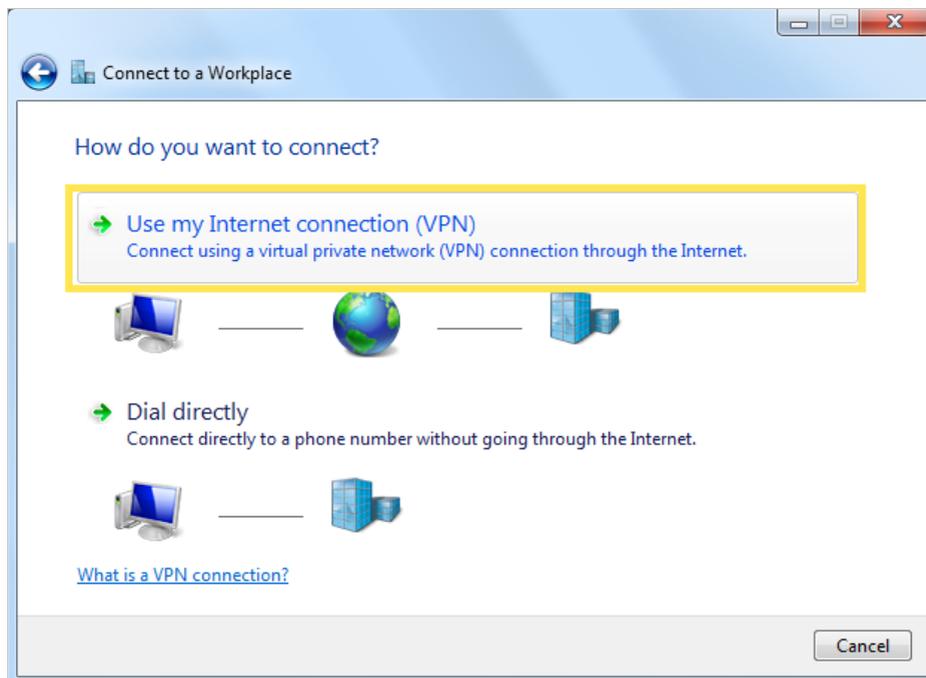
1. Accedere a **Start > Pannello di controllo > Rete e Internet > Centro connessioni di rete e condivisione**.
2. Selezionare **Imposta una nuova connessione o rete**.



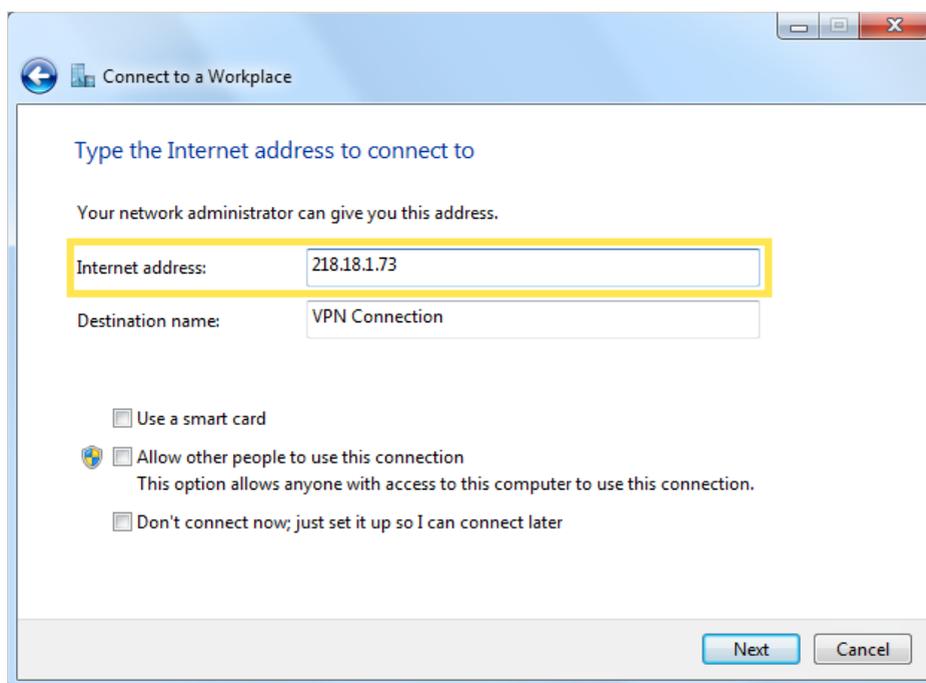
3. Selezionare **Connetti ad un workplace** e fare clic su **Avanti**.



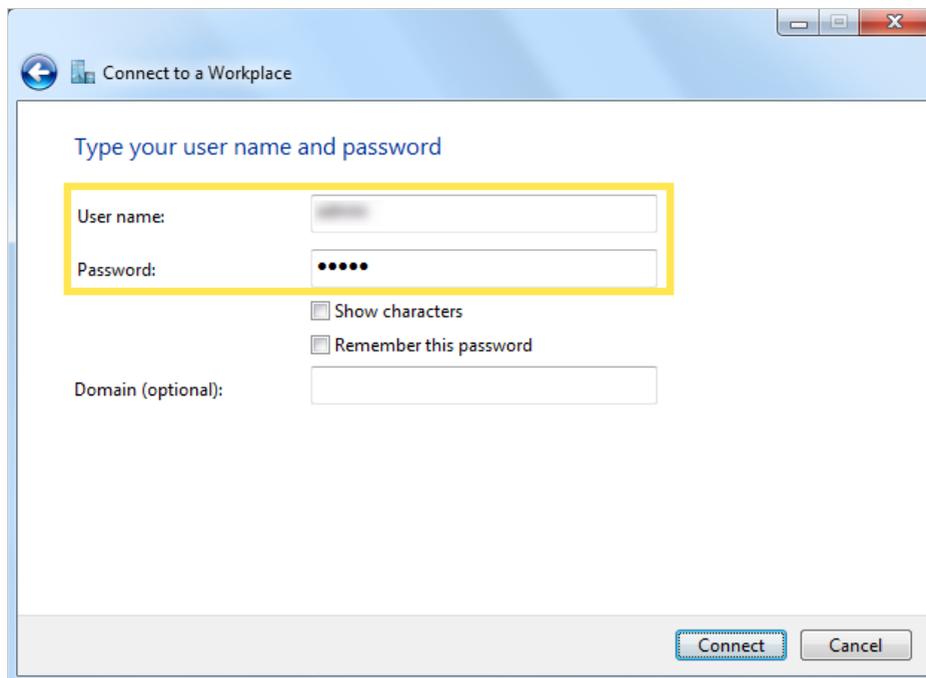
4. Selezionare **Usa la mia connessione Internet (VPN)**.



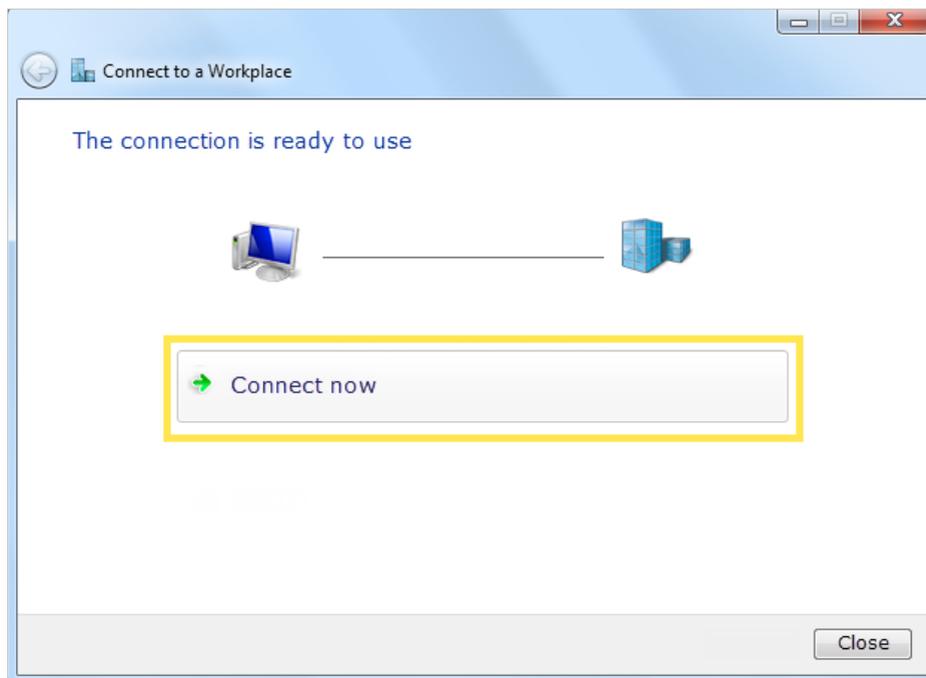
5. Inserite l'indirizzo IP Internet del router (ad esempio: 218.18.1.73) nel campo **Indirizzo Internet**. Fare clic su **Avanti**.



6. Inserite il **nome utente** e la **password** impostati per il server VPN PPTP sul router e fate clic su **Connetti**.



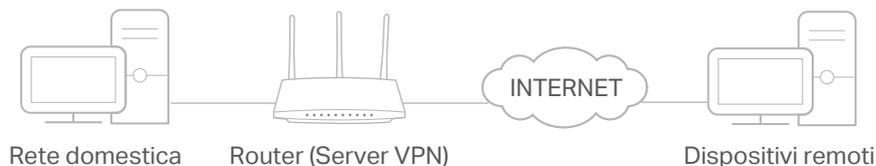
7. Fare clic su **Connetti ora** quando la connessione VPN è pronta per l'uso.



12.3. Utilizzo VPN IPSec per accedere alla rete domestica

Il server VPN IPSec viene utilizzato per creare una connessione VPN IPSec che consente ai dispositivi remoti di accedere alla rete domestica.

Per utilizzare la funzione VPN, è necessario impostare il server VPN IPSec sul router e configurare la connessione IPSec sui dispositivi remoti. Per configurare la connessione VPN IPSec, attenersi alla seguente procedura.



Passo 1 Impostazione del server VPN IPSec sul router

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > VPN > Impostazioni IPSec** e abilitare il **Rilevamento Dead Peer**.

📌 **Note:**

- Potrebbe essere necessario un aggiornamento del firmware per supportare il server VPN IPSec.
- Prima di attivare il **Rilevamento Dead Peer**, si consiglia di configurare il Servizio DNS Dinamico (consigliato) o di assegnare un indirizzo IP statico alla porta WAN del router e di sincronizzare l'**ora del sistema** con Internet.

Impostazioni IPSec

Rilevamento Dead Peer:

+ **Aggiungi**
- **Elimina**

<input type="checkbox"/>	Nome Connessione	Gateway Remoto	Indirizzo Locale	Indirizzo Remoto	Stato	Abilita	Modifica
--	--	--	--	--	--	--	--

3. Fare clic su **Aggiungi**.
4. Configurare i parametri del server VPN IPSec.

Impostazioni IPsec

Rilevamento Dead Peer:

+ Aggiungi - Elimina

<input type="checkbox"/>	Nome Connessione	Gateway Remoto	Indirizzo Locale	Indirizzo Remoto	Stato	Abilita	Modifica
--	--	--	--	--	--	--	--

Nome Connessione IPsec:

Gateway IPsec Remoto (URL):

Accesso Tunnel da indirizzi IP locali:

Indirizzo IP per VPN:

Subnet Mask:

Accesso Tunnel da indirizzi IP remoti:

Indirizzo IP per VPN:

Subnet Mask:

Metodo Key Exchange:

Metodo Autenticazione:

Pre-Shared Key:

Perfect Forward Secrecy:

Avanzate

Cancella
OK

5. Configurare le Impostazioni Avanzate in base alla seguente spiegazione. Si consiglia di mantenere le impostazioni di default. Se si desidera modificare queste impostazioni, assicurarsi che entrambi gli endpoint del server VPN utilizzino gli stessi Algoritmo di Crittografia, Algoritmo di Integrity, Gruppo Diffie-Hellman e Durata Key sia nella phase1 che nella phase2.

Avanzate

==Fase 1==

Modalità: Principale

Tipo Identifier Locale: IP WAN Locale

Identifier Locale:

Tipo Identifier Remoto: IP WAN Remoto

Identifier Remoto:

Algoritmo Crittografia: 3DES

Integrità Algoritmo: MD5

Diffie-Hellman Group for Key Exchange: 1024bit

Durata Key(Secondi): 3600

==Fase 2==

Algoritmo Crittografia: 3DES

Integrità Algoritmo: MD5

Diffie-Hellman Group for Key Exchange: 1024bit

Durata Key(Secondi): 3600

Cancella OK

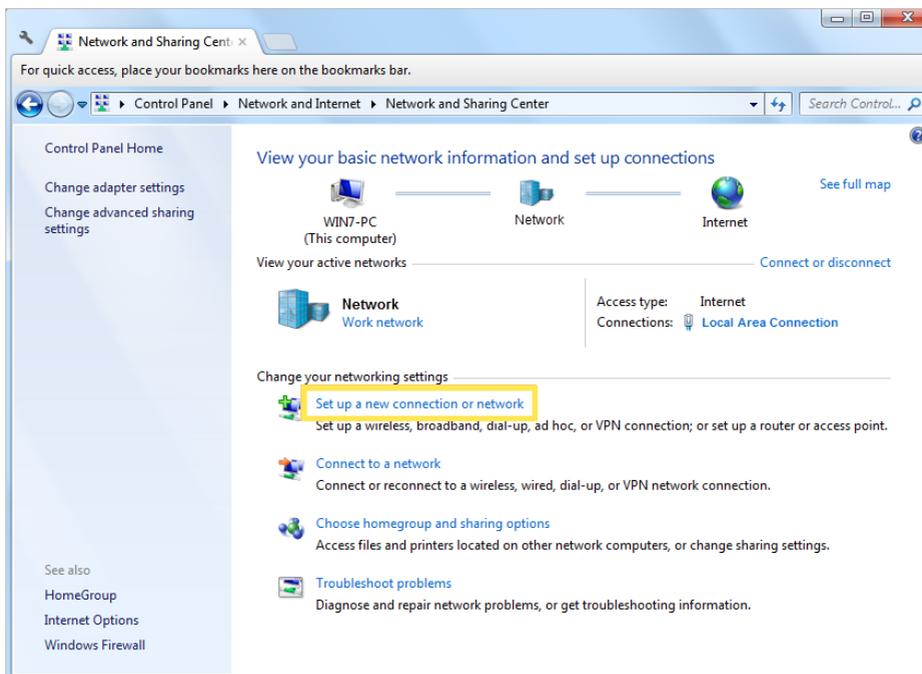
6. Fare clic su **OK**.

Nota: Per una guida completa, consultare la Guida dell'utente nella pagina di supporto del prodotto.

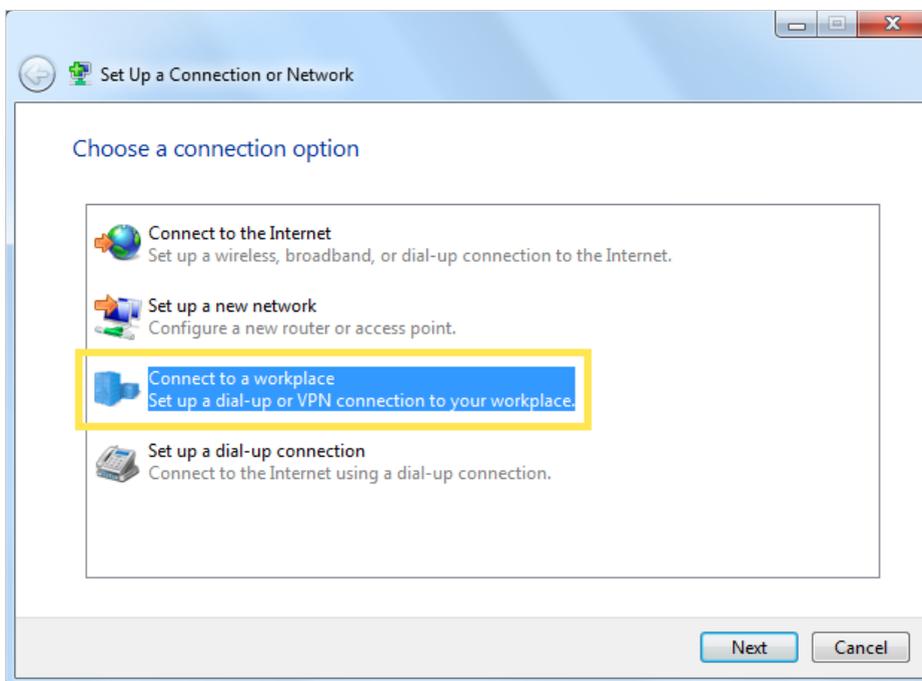
Passo 2 Configurazione della connessione VPN IPsec sul dispositivo remoto

Il dispositivo remoto può utilizzare il software IPsec integrato di Windows o Mac OS o un software IPsec di terze parti per connettersi a Server IPsec. In questo caso utilizziamo il **software IPsec integrato in Windows** come esempio.

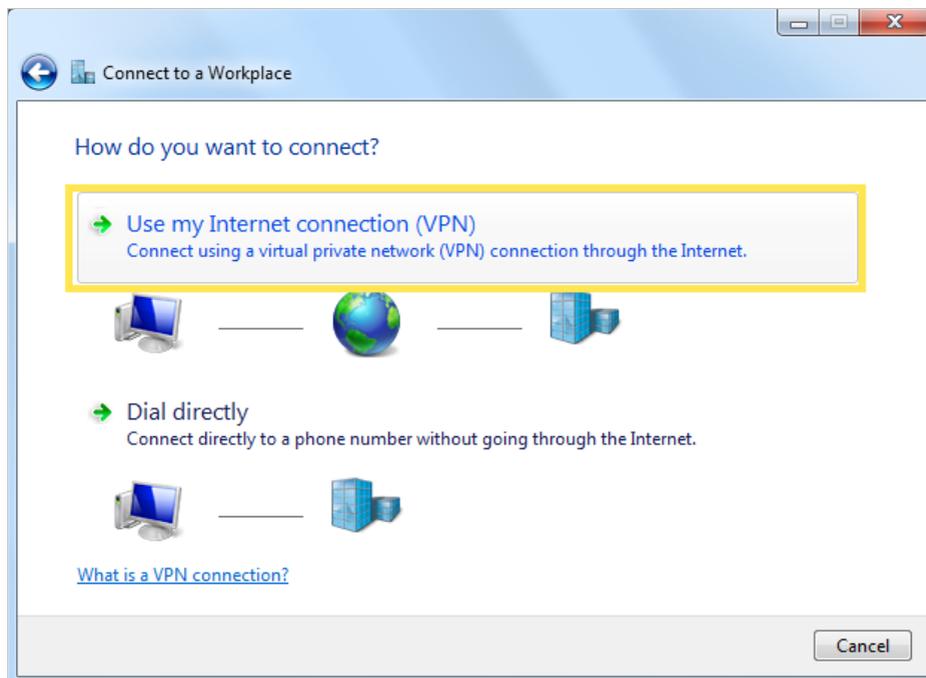
1. Accedere a **Start > Pannello di controllo > Rete e Internet > Centro connessioni di rete e condivisione**.
2. Selezionare **Imposta una nuova connessione o rete**.



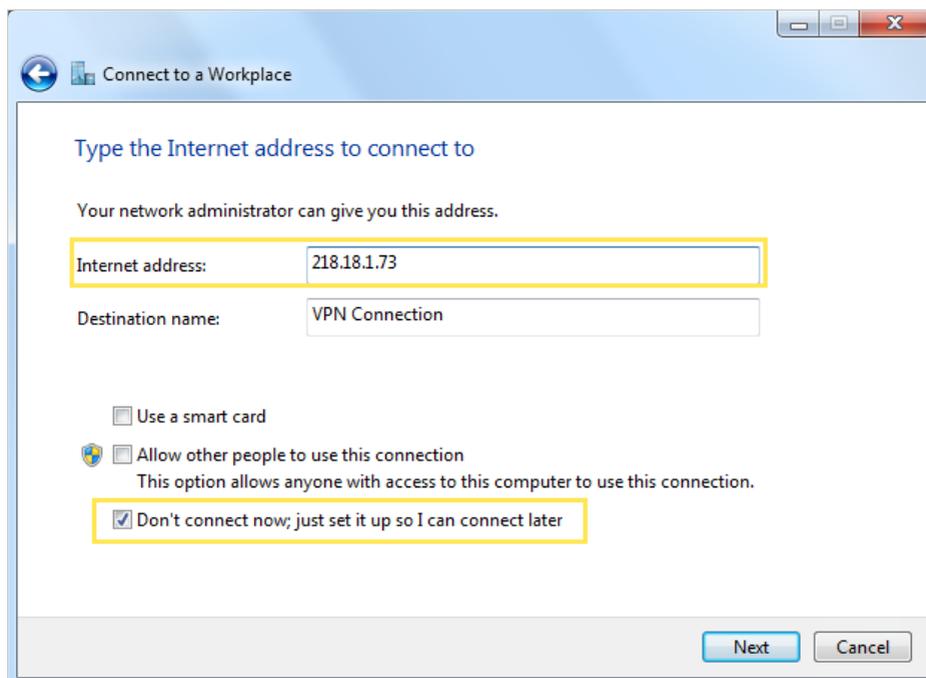
3. Selezionare **Connetti ad un workplace** e fare clic su **Avanti**.



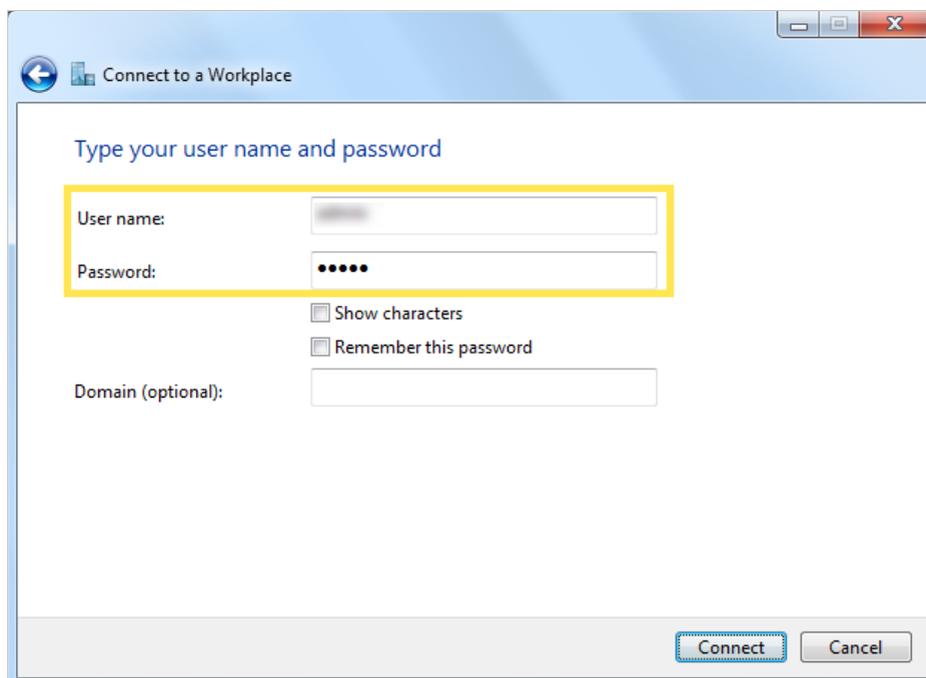
4. Selezionare **Usa la mia connessione Internet (VPN)**.



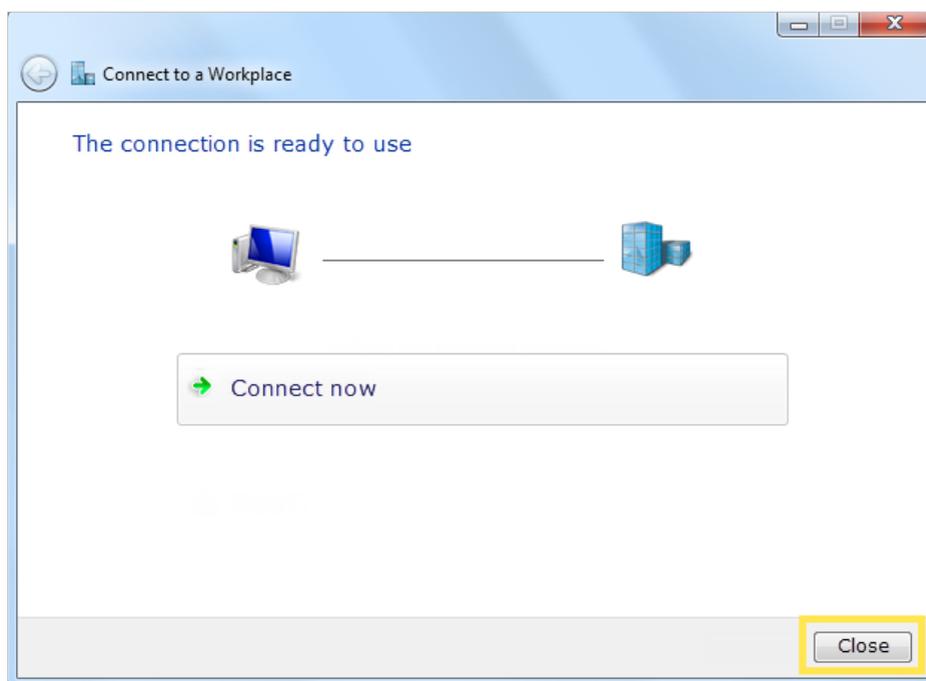
5. Inserite l'indirizzo IP del router (ad esempio: 218.18.1.73) nel campo **Indirizzo Internet** e selezionate la casella di controllo **Non connetterti ora; configuralo in modo che possa connettermi in seguito**. Fare clic su **Avanti**.



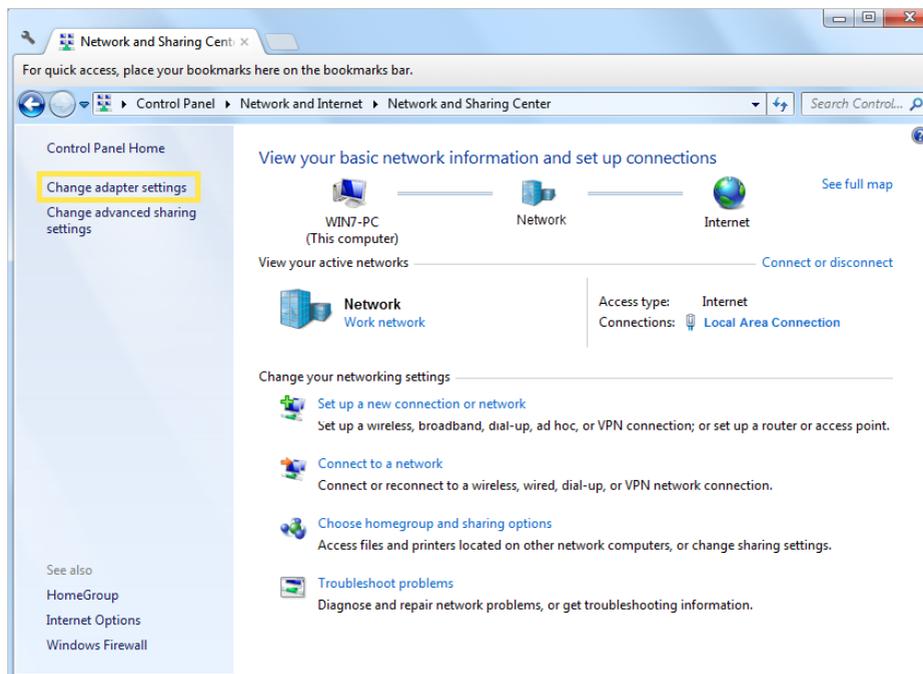
6. Inserite il **nome utente** e la **password** impostati per il server VPN IPsec sul router e fate clic su **Connetti**.



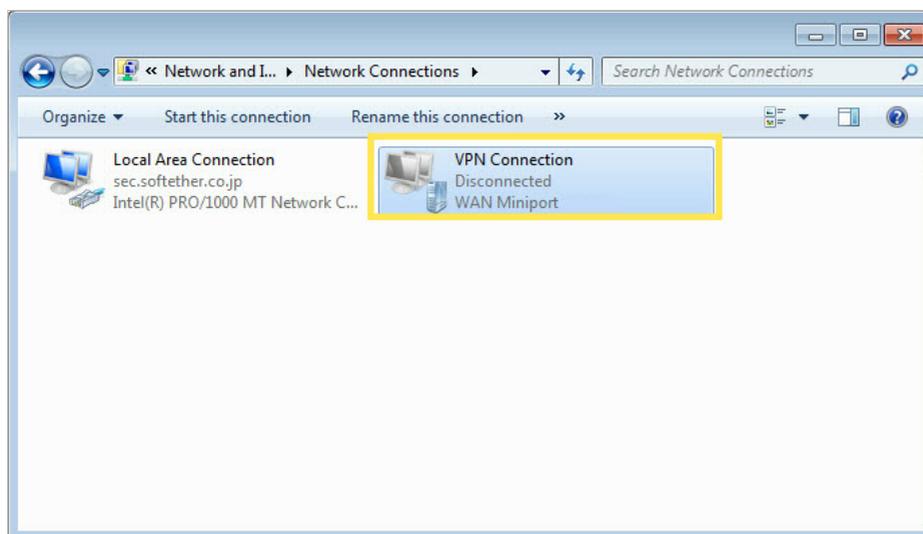
7. Fare clic su **Chiudi** quando la connessione VPN è pronta per l'uso.



8. Accedere a **Centro connessioni di rete e condivisione** e fare clic su **Modifica impostazioni dell'adattatore**.



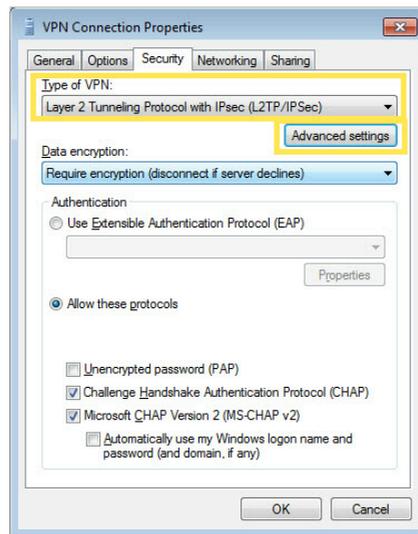
9. Individuare la connessione VPN creata e fare doppio clic su di essa.



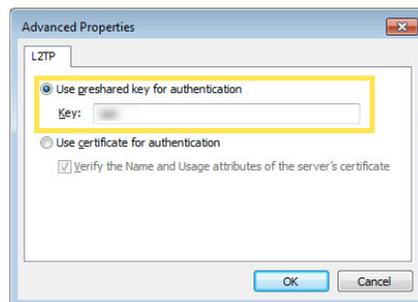
10. Inserite il **nome utente** e la **password** impostati per il server VPN IPsec sul router e fate clic su **Proprietà**.



11. Passare alla scheda **Sicurezza**, selezionare **Layer 2 Tunneling Protocol con IPsec (L2TP/ IPsec)** e fare clic su **Impostazioni Avanzate**.



12. Selezionare **Usa chiave preshared per l'autenticazione** e inserire la chiave preshared IPsec impostata per il server VPN IPsec sul router. Quindi fare clic su **OK**.



Fatto! Fare clic su **Connetti** per avviare la connessione VPN.



12.4. Connessioni VPN

La pagina Connessioni VPN visualizza i client attualmente connessi ai server OpenVPN, PPTP VPN e IPSec VPN ospitati sul router.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > VPN > Connessioni VPN**.

Connessioni VPN							
Connessione OpenVPN							
ID	Indirizzo IP del client			Modifica			
--	--			--			
Connessione PPTP VPN							
ID	Indirizzo IP del client			Modifica			
--	--			--			
Connessione VPN IPSec							
<input type="checkbox"/>	Nome Connessione	Gateway Remoto	Indirizzo Locale	Indirizzo Remoto	Stato	Abilita	Modifica
--	--	--	--	--	--	--	--

Capitolo 13

Gestione del router GPON

Questo capitolo illustra come modificare le impostazioni di sistema e amministrare la rete del router.

Questo capitolo contiene le seguenti sezioni:

- [Impostare l'ora del sistema](#)
- [Controllo del LED](#)
- [Test Connettività Internet](#)
- [Aggiornare il firmware](#)
- [Backup e ripristino delle impostazioni di configurazione](#)
- [Riavvia il router GPON](#)
- [Amministrazione](#)
- [Log di Sistema](#)
- [Monitorare le statistiche del traffico Internet](#)

13. 1. Impostare l'ora del sistema

L'ora del sistema è l'ora visualizzata quando il router è in funzione. L'ora del sistema configurata qui sarà utilizzata per altre funzioni basate sull'ora, come il Parental Control e la Schedulazione Wireless. È possibile impostare manualmente come ottenere l'ora del sistema.

Per impostare l'ora del sistema, procedere come segue.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare alla pagina **Avanzate > Strumenti Sistema > Impostazioni data/ora**.

The screenshot shows the 'Ora di Sistema' configuration page. It includes a dropdown menu for 'Fuso Orario' set to '(GMT+01:00) Amsterdam, Berlino, Roma, Stoccolma, Parigi, Praga, Bratisl...'. The 'Data' field is '8/27/2024' with '(MM/DD/YY)' below it. The 'Ora' field is '4 : 43 : 24'. The 'NTP' checkbox is checked and labeled 'Abilita'. The 'NTP Server I' field is 'time.inrim.it' (opzionale). The 'NTP Server II' field is '0.0.0.0' (opzionale). At the bottom, there are three buttons: 'Ottieni da PC', 'Ottieni GMT', and 'Salva'.

3. Configurare l'ora del sistema utilizzando i seguenti metodi:

Ottieni da PC: Fare clic su questo pulsante se si desidera utilizzare l'ora corrente del PC.

Ottieni GMT: Fare clic su questo pulsante se si desidera ottenere l'ora da Internet. Assicurarsi che il router possa accedere a Internet prima di selezionare questo metodo per ottenere l'ora del sistema.

4. Fare clic su **Salva**.
5. Dopo aver impostato l'ora del sistema, è possibile impostare l'**Salva Ora Legale** in base alle proprie esigenze. Attivare l'**Salva Ora Legale**, impostare l'ora iniziale e finale e fare clic su **Salva** per rendere effettive le impostazioni.

The screenshot shows the 'Salva Ora Legale' configuration page. It features a checkbox 'Abilita Salvataggio Ora Legale'. Below it, the 'Inizio' field is set to '2024' with month 'Gen', day 'Ultimo', and time '00:00'. The 'Fine' field is set to '2024' with month 'Ott', day 'Ultimo', and time '03:00'. A 'Salva' button is at the bottom right.

13.2. Controllo del LED

Il LED del router indica le sue attività e il suo stato. È possibile attivare la funzione Modalità Notte per specificare un periodo di tempo durante il quale il LED è spento.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate** > **Strumenti Sistema** > **Controllo LED**.
3. Abilita la **Modalità Notte**.
4. Specificando l'orario di spegnimento del LED, il LED si spegnerà ogni giorno durante questo periodo.
5. Fare clic su **Salva**.

Controllo LED

LED Enable:

Modalità Notte: Abilita

Periodo Modalità Notte: 22 : 0 a 6 : 0 (HH:MM)

Nota: il periodo di modalità notturna ha effetto in base all'ora di sistema del router. Assicurati di aver già impostato l'ora del router.

Salva

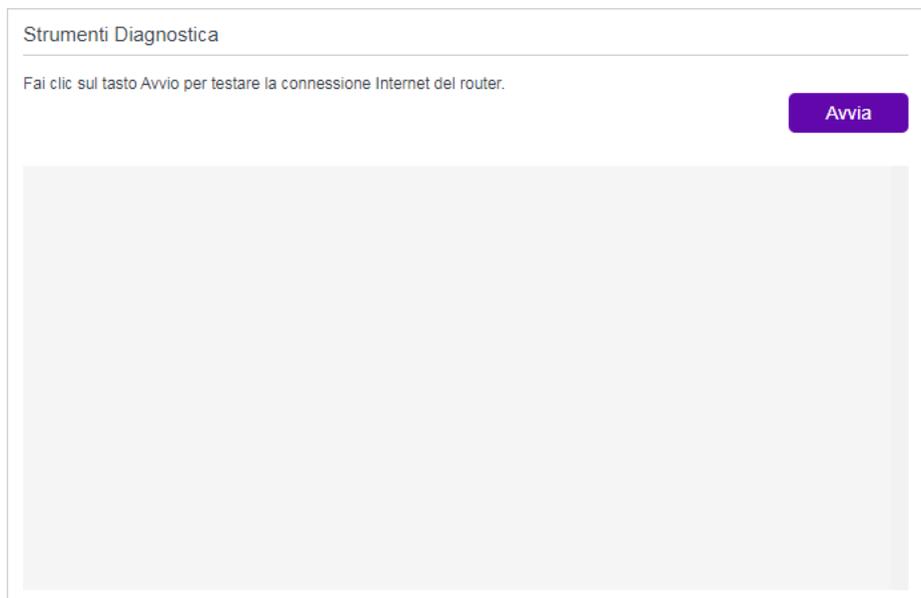
13.3. Test Connettività Internet

La funzione di diagnostica viene utilizzata per verificare la connettività tra il router e l'host o altri dispositivi di rete.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Accedere alla pagina **Avanzate** > **Strumenti Sistema** > **Diagnostica**.

➤ **Per verificare la connessione a Internet del router:**

Individuare la sezione **Diagnostica** e fare clic su **Avvia** per testare la connettività Internet; i risultati del test saranno visualizzati nella casella grigia.



13. 4. Aggiornare il firmware

Wind3 e TP-Link si impegnano a migliorare le caratteristiche dei prodotti, offrendo una migliore esperienza di rete.

Vi informeremo attraverso la pagina di gestione web se è disponibile un firmware di aggiornamento per il vostro router. Il firmware più recente può essere scaricato gratuitamente anche dalla pagina di [supporto](#) del nostro sito web www.tp-link.com/it.

■ Note:

1. Assicurarsi di avere una connessione stabile tra il router e il computer. NON è consigliabile aggiornare il firmware in modalità wireless.
2. Eseguire il backup della configurazione del router prima di aggiornare il firmware.
3. NON spegnere il router durante l'aggiornamento del firmware.

➤ Per aggiornare manualmente il firmware, attenersi alla seguente procedura:

1. Scaricare il file del firmware più recente per il router dal nostro sito web www.tp-link.com.
2. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
3. Andare in **Avanzate > Strumenti Sistema > Aggiornamento Firmware**.
4. Concentrarsi sulla sezione **Informazioni Dispositivo**. Assicurarsi che il file del firmware scaricato corrisponda alla **Versione dell'Hardware**.

Informazioni Dispositivo	
Versione Firmware:	XB432v_1.0_WI_20240827
Versione Hardware:	1.0
Numero di serie:	202404190925

5. Concentrarsi sulla sezione **Aggiornamento Locale**. Fare clic su **Sfoglia** per individuare il file del nuovo firmware scaricato e fare clic su **Aggiorna**.

Aggiornamento Locale	
Nuovo Firmware:	<input type="text"/>
	Sfoglia
	Aggiorna

6. Attendere qualche minuto per l'aggiornamento e il riavvio.

13.5. Backup e ripristino delle impostazioni di configurazione

Le impostazioni di configurazione sono memorizzate nel router come file di configurazione. È possibile eseguire il backup del file di configurazione sul computer per un uso futuro e ripristinare il router alle impostazioni precedenti dal file di backup quando necessario. Inoltre, se necessario, è possibile eliminare le impostazioni correnti e resettare le impostazioni di fabbrica del router.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate** > **Strumenti Sistema** > **Backup & Ripristino**.

➤ **Per eseguire il backup delle impostazioni di configurazione:**

Backup per salvare una copia delle impostazioni correnti sul computer locale. Sul computer verrà salvato un file conf.bin.

Backup
Salva una copia delle impostazioni correnti.
Backup

➤ **Per ripristinare le impostazioni di configurazione:**

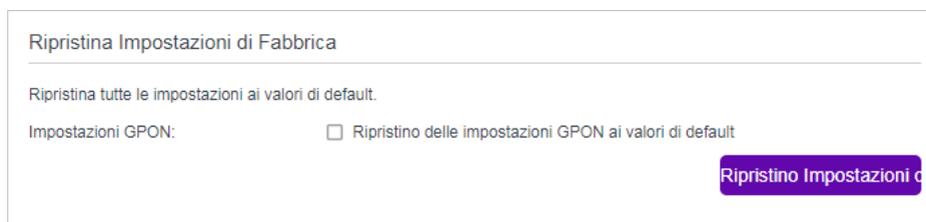
- 1) Fare clic su **Sfoglia** per individuare il file di configurazione di backup precedente e fare clic su **Ripristina**.



2) Attendere qualche secondo per il ripristino e il riavvio.

➤ **Per ripristinare le impostazioni di fabbrica del router:**

1) Individuare la sezione **Ripristino Impostazioni di Fabbrica** e fare clic su **Ripristino Impostazioni** per resettare il router.



2) Attendere qualche minuto per il reset e il riavvio.

📌 **Note:**

1. Durante il processo di reset, non spegnere il router.
2. Si consiglia vivamente di eseguire il backup delle impostazioni di configurazione correnti prima di resettare il router.

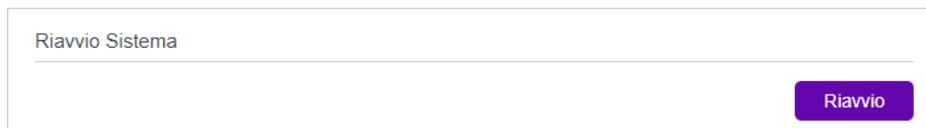
13.6. Riavvia il router GPON

La funzione Riavvio pulisce la cache per migliorare le prestazioni del router. È possibile riavviare il router manualmente o impostare un riavvio regolare.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andate su **Avanzate > Strumenti Sistema > Schedulazione Riavvio** e potrete riavviare il router.

➤ **Per riavviare manualmente il router:**

Fare clic su **Riavvio** e attendere qualche minuto affinché il router si riavvii.



➤ **Per programmare il riavvio del router a un'ora specifica:**

- 1) Abilita la **Schedulazione Riavvio**.
- 2) Specificare l'**Ora Riavvio** del router.

Schedulazione Riavvio

Nota: prima di abilitare Schedulazione Riavvio, assicurati che il tuo router sia connesso a Internet. Quindi vai su [Impostazioni Ora](#) e scegli [Ottieni da Internet](#) per ottenere l'ora di rete corretta.

Ora attuale: 08/27/2024 01:03:12

Schedulazione Riavvio: Abilita

Ripeti: Ogni giorno

Ora Riavvio: 3 : 0

[Salva](#)

3) Fare clic su **Salva** per rendere effettive le impostazioni.

Alcune impostazioni del router possono diventare effettive solo dopo il riavvio, tra cui:

- Modificare l'indirizzo IP della LAN (il sistema si riavvia automaticamente).
- Cambiare la modalità di funzionamento (il sistema si riavvia automaticamente).
- Aggiornare il firmware del router (il sistema si riavvia automaticamente).
- Ripristinare le impostazioni di fabbrica del router (il sistema si riavvia automaticamente).
- Aggiornare la configurazione con il file (il sistema si riavvia automaticamente).

📌 **Nota:** La funzione di riavvio automatico funziona in base all'ora del sistema del router. Assicurarsi di aver già impostato l'ora del router.

13. 7. Amministrazione

13. 7. 1. Modificare la password di accesso

Per accedere alla pagina di gestione web del router è necessaria una password di accesso. Al primo accesso viene richiesto di impostare una password di accesso. È possibile modificarla con la funzione di gestione dell'account.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate** > **Strumenti Sistema** > **Amministrazione** e individuare la sezione **Gestione Account**.

Gestione Account:

Tipologia utente: Admin

Vecchio Username: admin

Vecchia Password: [input field]

Nuovo Username: admin

Nuova Password: [input field] Basso Medio Alto

Conferma Nuova Password: [input field]

Salva

3. Inserire una volta la vecchia password e due volte una nuova password (entrambe sensibili alle maiuscole e alle minuscole).
4. Fare clic su **Salva** per rendere effettive le impostazioni.

13.7.2. Gestione locale

È possibile controllare i dispositivi locali di gestire il router tramite la funzione Gestione Locale. Di default, tutti i dispositivi locali collegati sono autorizzati a gestire il router. È anche possibile specificare un dispositivo per la gestione del router e abilitare la gestione locale tramite un metodo più sicuro, HTTPS.

Seguire la procedura seguente per consentire solo al dispositivo specifico di gestire il router tramite la gestione locale su HTTPS.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Strumenti Sistema > Amministrazione** e individuare la sezione **Gestione locale**.
3. Abilitare la **Gestione locale tramite HTTPS** e mantenere le impostazioni di default di **Porta per HTTP** e **Porta per HTTPS**. Inserire l'**Indirizzo IP/MAC** del dispositivo locale per la gestione del router.

Gestione Locale HTTP || TELNET || SSH

Porta per HTTP: 80

Gestione locale tramite HTTPS: Abilita

Porta per HTTPS: 443

Indirizzo IP/MAC: [input field]

Salva

4. Fare clic su **Salva**.

Ora è possibile gestire il router GPON sia tramite HTTP (<http://192.168.1.1>) che HTTPS (<https://192.168.1.1>).

Nota: Se si desidera che tutti i dispositivi locali possano gestire il router, lasciare vuoto il campo **Indirizzo IP/MAC**.

13.7.3. Gestione remota

Di default, i dispositivi remoti non possono gestire il router da Internet. Se necessario, è possibile abilitare la gestione remota tramite HTTP e/o HTTPS. HTTPS è un modo più sicuro per accedere al router.

Nota: Se Wind3 assegna un indirizzo IP WAN privato (ad esempio 192.168.x.x o 10.x.x.x), non è possibile utilizzare la funzione di gestione remota perché gli indirizzi privati non vengono instradati su Internet.

Seguite la procedura seguente per consentire ai dispositivi remoti di gestire il router tramite HTTPS.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate** > **Strumenti Sistema** > **Amministrazione** e individuare la sezione **Gestione Remota**.

Gestione Remota HTTP | | SSH

Gestione remota tramite HTTPS: Abilita

Porta per HTTPS:

Gestisci questo router tramite l'indirizzo:

Dispositivo Client Autorizzato per la gestione remota:

Solo i seguenti indirizzi IP

Aggiungi un nuovo IP

Aggiungi un nuovo range

Tutti

Salva

3. Abilitare **Gestione remota tramite HTTPS** per consentire la connessione HTTPS. Mantenere la **Porta per HTTPS** come impostazione di default.

4. Impostare il dispositivo client consentito per la gestione remota. Selezionate **Tutti** per consentire a tutti i dispositivi remoti di gestire il router. Se si desidera consentire solo a un dispositivo specifico di gestire il router, selezionare **Solo i seguenti indirizzi IP** e inserire l'indirizzo IP del dispositivo remoto.

5. Fare clic su **Salva**.

Tutti i dispositivi o il dispositivo specifico su Internet possono accedere al router utilizzando l'indirizzo visualizzato nel campo **Gestisci questo router tramite l'indirizzo** per gestire il router.

🔗 S suggerimenti:

1. Se durante la visita alla pagina di gestione web da remoto è stato emesso un avviso relativo al certificato, fare clic su **Fidati** (o su un'opzione simile) per continuare. Per evitare questo avviso, è possibile scaricare e installare il certificato nella pagina di gestione web del router in **Avanzate > Strumenti Sistema > Amministrazione**.

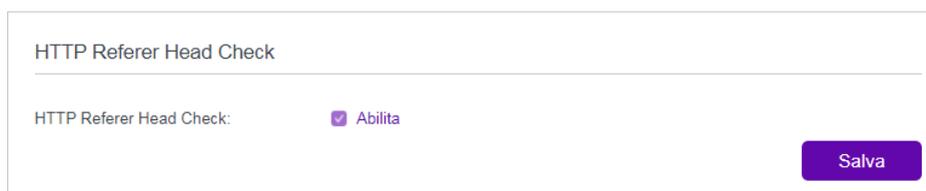


2. L'IP WAN del router è solitamente un IP dinamico. Se si desidera accedere al router tramite un nome di dominio, consultare la sezione **Impostazione account del servizio DNS dinamico**.

13.7.4. HTTP Referer Head Check

La funzione HTTP Referer Head Check può proteggere le reti dagli attacchi CSRF. Questa funzione è abilitata di default. Se necessario, è possibile disabilitare questa funzione.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Strumenti Sistema > Amministrazione** e individuare la sezione **HTTP Referer Head Check**.
3. Deselezionare la casella di controllo **Abilita** e fare clic su **Salva** se si desidera disattivare questa funzione.

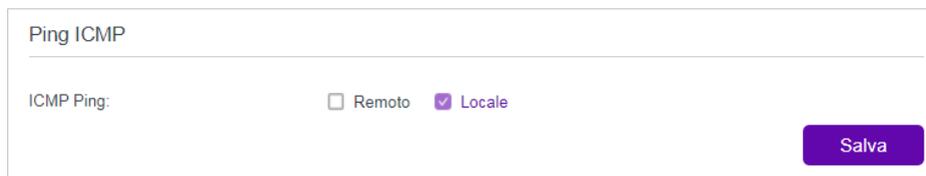


13.7.5. Ping ICMP

Ping ICMP (Internet Control Message Protocol) viene utilizzato per fare una diagnosi della rete inviando pacchetti di richiesta echo ICMP all'host remoto o locale di destinazione e attendendo una risposta ICMP.

È possibile controllare le risposte del router alle richieste Ping ICMP.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Strumenti Sistema > Amministrazione** e individuare la sezione **Ping ICMP**.



3. Specificare le opzioni di risposta ICMP Ping.

- **Remoto:** Selezionare questa opzione se si desidera che i computer di una rete pubblica eseguano il ping dell'indirizzo IP WAN del router.
- **Locale:** è abilitato di default. Se abilitato, i computer di una rete privata possono pingare l'indirizzo IP LAN del router.

4. Fare clic su **Salva** per rendere effettive le impostazioni.

13.7.6. ID Sessione

Quando la funzione ID sessione è abilitata, viene salvata nella memoria flash ogni volta che la connessione PPP viene aggiornata. In questo modo si possono evitare alcuni problemi di rifiuto della connessione PPPoE/L2TP/PPTP per la riconnessione ai server quando il dispositivo viene spento o la rete si disconnette accidentalmente.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate** > **Strumenti Sistema** > **Amministrazione** e individuare la sezione **ID Sessione**.



3. Attivare l'opzione **Aggiorna ID Sessione** e fare clic su **Salva** per rendere effettive le impostazioni.

13.8. Log di Sistema

Log di Sistema può aiutare a sapere cosa è successo al router, facilitando l'individuazione dei malfunzionamenti. Ad esempio, quando il router non funziona correttamente, può essere necessario salvare i Log di Sistema e inviarli all'assistenza tecnica per la risoluzione dei problemi.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare a **Avanzate** > **Strumenti Sistema** > **Log di Sistema**.

Log di Sistema

Tipo:

Livello:

 [Aggiorna](#)  [Elimina Tutto](#)

ID	Ora/Data	Tipo	Livello	Log Contenuto
1	2024-08-27 01:03:08	VOIP	Notice	ip_contrack module is not loaded, or we did not open the CONFIG_NF_CT_LOCAL_LIMIT
2	2024-08-27 01:03:08	VOIP	Notice	ip_contrack module is not loaded, or we did not open the CONFIG_NF_CT_LOCAL_LIMIT
3	2024-08-27 01:02:38	VOIP	Notice	ip_contrack module is not loaded, or we did not open the CONFIG_NF_CT_LOCAL_LIMIT
4	2024-08-27 01:02:38	VOIP	Notice	ip_contrack module is not loaded, or we did not open the CONFIG_NF_CT_LOCAL_LIMIT
5	2024-08-27 00:01:36	MESH	Notice	Add Device :MAC : 20:24:04:19:09:25
6	2024-08-27 00:01:34	WANCON DETECT	Informazioni	Start Wan Connection Detect...
7	2024-08-27 00:01:34	VOIP	Notice	ip_contrack module is not loaded, or we did not open the CONFIG_NF_CT_LOCAL_LIMIT
8	2024-08-27 00:01:34	VOIP	Notice	ip_contrack module is not loaded, or we did not open the CONFIG_NF_CT_LOCAL_LIMIT

 1 2 

[Impostazioni Log](#) [Salva Log](#)

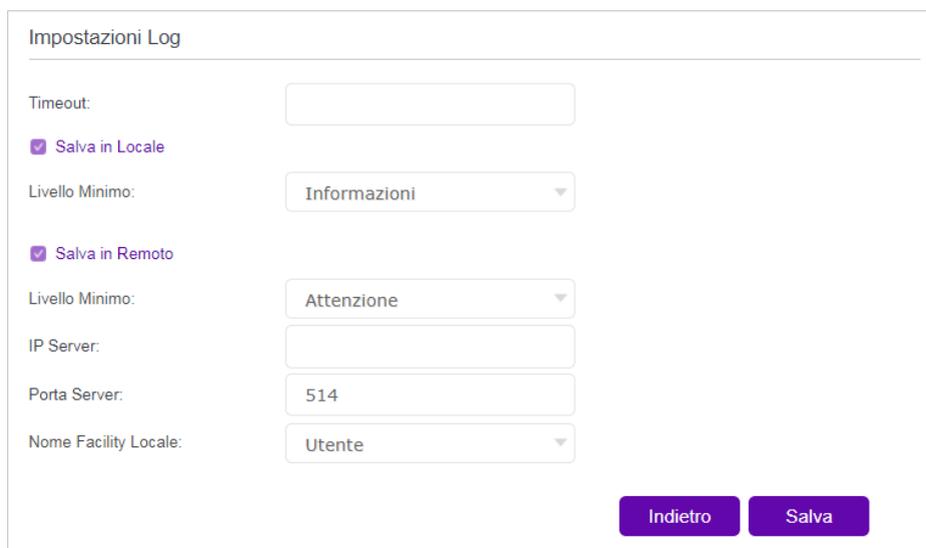
➤ **Per visualizzare i log di sistema:**

È possibile visualizzare log di sistema specifici selezionando il tipo e il livello dei log. Fare clic su [Aggiorna](#) per aggiornare l'elenco dei log.

➤ **Per salvare i log di sistema:**

È possibile salvare i log di sistema sul computer locale o su un server remoto. Fare clic su [Salva Log](#) per salvare i log in un file txt sul computer.

Fare clic su [Impostazioni Log](#) per impostare il percorso di archiviazione dei log.



- **Salva in Locale:** Selezionare questa opzione per memorizzare il Log di Sistema nella memoria locale del router, selezionando il livello minimo di Log di Sistema da salvare dall'elenco a discesa. I log saranno visualizzati nella tabella in ordine decrescente nella pagina Log di Sistema.
- **Salva in Remoto:** Selezionare questa opzione per inviare il Log di Sistema a un server remoto, selezionare il livello minimo di Log di Sistema da salvare dall'elenco a discesa e inserire le informazioni del server remoto. Se il server remoto dispone di un client di visualizzazione dei log o di uno strumento di sniffer, è possibile visualizzare e analizzare il log di sistema da remoto in tempo reale.

13.9. Monitorare le statistiche del traffico Internet

La funzione Statistiche Traffico consente di monitorare il volume delle statistiche sul traffico Internet. È possibile visualizzare il traffico di rete dei pacchetti LAN, WAN e WLAN inviati e ricevuti.

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare in **Avanzate > Strumenti Sistema > Statistiche Traffico**.
3. Attiva **Abilita Statistiche Traffico** per abilitare la funzione di statistiche sul traffico; è possibile visualizzare il numero totale di pacchetti e byte ricevuti e trasmessi dal router nel range **Intervallo Statistiche** selezionato. Questa funzione è disattivata di default.

Statistiche Traffico

Abilita Statistiche Traffico:

Statistiche Traffico e NAT Boost non possono essere attivati contemporaneamente.

Intervallo Statistiche: secondi

[Salva](#)

4. Per informazioni dettagliate sull'utilizzo del traffico di tutti i dispositivi, è possibile consultare [Elenco Statistiche Traffico](#).

Elenco Statistiche Traffico

[Aggiorna](#) [Resetta](#) [Elimina Tutto](#)

Indirizzo IP/ Indirizzo MAC	Pacchetti Totali	Byte Totali	Pacchetti Correnti	Byte Correnti	ICMP Tx Corrente	UDP Tx Corrente	SYN Tx Corrente	Modifica
[blurred]	6	348	0	0	0	0	0	↻ 🗑️

FAQ

Q1. Cosa devo fare se dimentico la password wireless?

La password wireless di default è stampata sull'etichetta del router. Se la password è stata modificata:

1. Collegare il computer al router utilizzando un cavo Ethernet.
2. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
3. Andare su **Avanzate > Wireless > Impostazioni Wireless** per recuperare o reimpostare la password wireless.

Q2. Cosa devo fare se dimentico la mia password di gestione web?

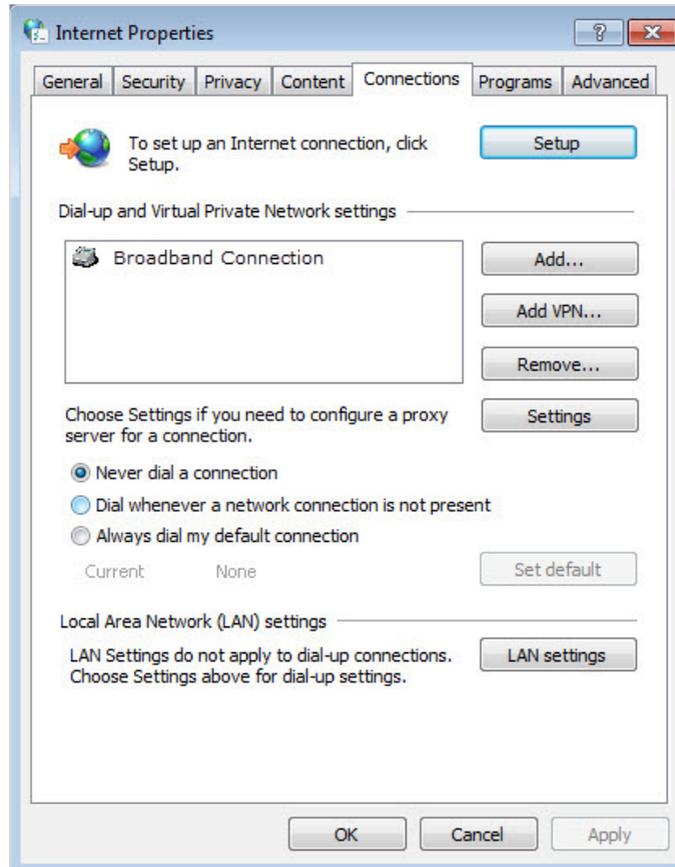
- Se si utilizza un ID TP-Link per accedere o si è attivata la funzione di recupero password del router, fare clic su **Password dimenticata** nella pagina di accesso e seguire le istruzioni per reimpostarla.
- In alternativa, tenere premuto il pulsante **Reset** del router finché il LED Power non lampeggia per ripristinare le impostazioni di fabbrica, quindi visitare <http://192.168.1.1> per inserire il nome utente e la password di accesso.

Nota: Una volta ripristinato il router, è necessario riconfigurarne per navigare in Internet e annotare la nuova password per un uso futuro.

Q3. Cosa devo fare se non riesco ad accedere alla pagina di gestione web del router?

Questo può accadere per una serie di motivi. Provare a effettuare nuovamente l'accesso con i metodi indicati di seguito.

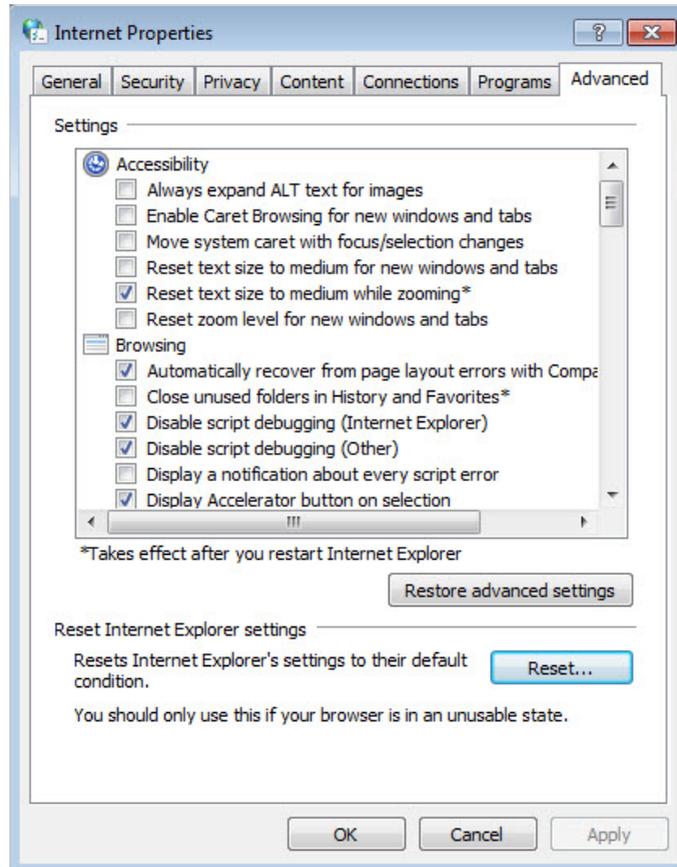
- Assicurarsi che il computer sia collegato correttamente al router e che gli indicatori LED corrispondenti si accendano.
- Assicurarsi che l'indirizzo IP del computer sia configurato come **Ottieni automaticamente un indirizzo IP** e **Ottieni automaticamente l'indirizzo del server DNS**.
- Assicurarsi che <http://192.168.1.1> siano inseriti correttamente.
- Controllare le impostazioni del computer:
 - 1) Andare in **Start > Pannello di controllo > Rete e Internet** e fare clic su **Visualizza stato e attività della rete**.
 - 2) Fare clic su **Opzioni Internet** in basso a sinistra.
 - 3) Fare clic su **Connessioni** e selezionare **Non comporre mai una connessione**.



- 4) Fare clic su **Impostazioni LAN**, deselezionare le tre opzioni seguenti e fare clic su **OK**.



- 5) Andare su **Avanzate** > **Ripristina Impostazioni Avanzate**, fare clic su **OK** per salvare le impostazioni.



- Utilizzare un altro browser web o un altro computer per accedere nuovamente.
- Ripristinare le impostazioni di fabbrica del router e riprovare. Se il login continua a non funzionare, contattare l'assistenza tecnica.

📌 Nota: una volta resettato il router, è necessario riconfigurarli per navigare in Internet.

Q4. Cosa devo fare se non riesco ad accedere a Internet nonostante la configurazione sia terminata?

1. Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
2. Andare su **Avanzate** > **Stato** per controllare lo stato di Internet:

Se l'indirizzo IP è valido, provare i metodi indicati di seguito e riprovare:

- Il computer potrebbe non riconoscere alcun indirizzo di server DNS. Configurare manualmente il server DNS.
 - 1) Andare in **Avanzate** > **Rete** > **Impostazioni LAN** > **Server DHCP**.
 - 2) Inserire 8.8.8.8 come DNS primario e fare clic su **Salva**.

🔗 Suggerimenti: 8.8.8.8 è un server DNS pubblico e sicuro gestito da Google.

DHCP: Abilita

Server DHCP DHCP Relay

Pool Indirizzi IP: 192 . 168 . 1 . 2 - 192 . 168 . 1 . 254

Durata Indirizzo: 1440 minuti (1-2880. Il valore di default è 120).

Default Gateway: 0 . 0 . 0 . 0 (opzionale)

Dominio di Default: (opzionale)

DNS Primario: 8 . 8 . 8 . 8 (opzionale)

DNS Secondario: 0 . 0 . 0 . 0 (opzionale)

Salva

- Riavviare il modem e il router.
 - 1) Spegnere il modem e il router e lasciarli spenti per 1 minuto.
 - 2) Accendere il modem e attendere circa 2 minuti finché non si accende una luce fissa sul cavo o su Internet.
 - 3) Accendere il router.
 - 4) Attendere ancora 1 o 2 minuti e verificare l'accesso a Internet.
- Ripristinare le impostazioni di fabbrica del router e riconfigurarlo.
- Aggiornare il firmware del router.
- Controllare le impostazioni TCP/IP del dispositivo in questione se tutti gli altri dispositivi possono accedere a Internet dal router.

Come mostra l'immagine sottostante, se l'indirizzo IP è 0 0 0 0, provare i metodi indicati di seguito e riprovare:

Status

Internet status overview is displayed on this page.

Internet

Status: WAN port is unplugged

Internet Connection Type: Dynamic IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

- Assicuratevi che il collegamento fisico tra il router e il modem sia corretto.
- Clonare l'indirizzo MAC del computer.

- 1) Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
- 2) Andare in **Avanzate > Rete > WAN GPON** e concentrarsi sulla sezione **MAC Clone**.
- 3) Scegliere l'opzione necessaria (inserire l'indirizzo MAC se **Usa un Indirizzo MAC Personalizzato** è selezionato), quindi fare clic su **OK**.

MAC Clone

NON clonare l'Indirizzo MAC

Clonare l'indirizzo MAC del computer corrente

Usa un Indirizzo MAC Personalizzato

- - - - -

Cancella OK

🔗 **Suggerimenti:**

- Alcuni ISP registrano l'indirizzo MAC del computer quando si accede a Internet per la prima volta tramite il modem via cavo; se si aggiunge un router alla rete per condividere la connessione a Internet, Wind3 non lo accetterà perché l'indirizzo MAC è stato modificato, quindi è necessario clonare l'indirizzo MAC del computer sul router.
- Gli indirizzi MAC di un computer in connessione cablata e in connessione wireless sono diversi.

• **Modificare l'indirizzo IP LAN del router.**

📌 **Nota:** Il router Wind3 utilizza 192.168.1.1 come indirizzo IP di default LAN, Se volete modificarlo, impostando ad esempio 192.168.2.1.

- 1) Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
- 2) Andare in **Avanzate > Rete > Impostazioni LAN**.
- 3) Modificare l'indirizzo IP della LAN come mostra l'immagine seguente. Prendiamo come esempio 192.168.2.1.
- 4) Fare clic su **Salva**.

Server DHCP IPv4 | IPv6

Indirizzo MAC: 20:24:04:19:09:25

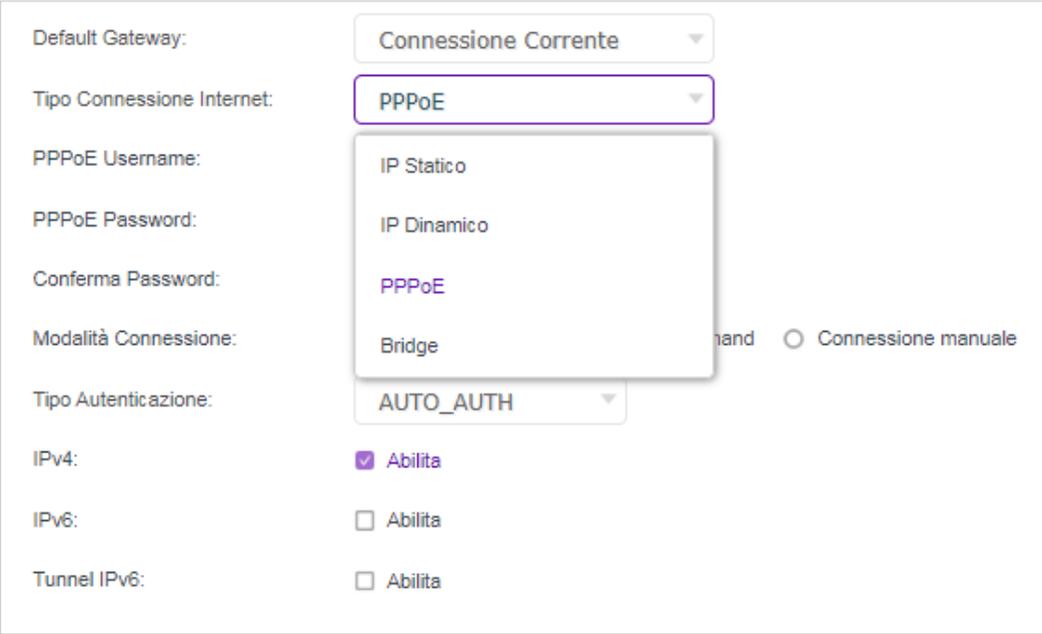
Indirizzo IP: 192 . 168 . 2 . 1

Subnet Mask: 255.255.255.0

• **Riavviare il modem router.**

- 1) Spegnere il modem router e lasciarlo spento per 1 minuto.
- 2) Accendere il modem router.

- 3) Attendere 1 o 2 minuti e verificare l'accesso a Internet.
- Verificare due volte il tipo di connessione a Internet.
 - 1) Confermare il tipo di connessione a Internet, che può essere appreso da Wind3.
 - 2) Visitare <http://192.168.1.1> e accedere con la password impostata per il router GPON.
 - 3) Andare in **Avanzate > Rete > WAN GPON**.
 - 4) Selezionare il **Tipo Connessione Internet** e compilare gli altri parametri.
 - 5) Fare clic su **Salva**.



Default Gateway: Connessione Corrente

Tipo Connessione Internet: PPPoE

PPPoE Username: IP Statico

PPPoE Password: IP Dinamico

Conferma Password: PPPoE

Modalità Connessione: Connessione automatica Connessione manuale

Tipo Autenticazione: AUTO_AUTH

IPv4: Abilita

IPv6: Abilita

Tunnel IPv6: Abilita

- 6) Riavviare il modem router.
- Aggiornare il firmware del router.

Se avete provato tutti i metodi sopra descritti ma non riuscite ancora ad accedere a Internet, contattate il supporto tecnico.

Q5. Cosa devo fare se non riesco a trovare la rete wireless o non riesco a connettermi alla rete wireless?

Se non si riesce a trovare una rete wireless, seguire la procedura seguente:

- Assicurarsi che la funzione wireless del dispositivo sia abilitata se si utilizza un portatile con adattatore wireless incorporato. Si può fare riferimento alla relativa documentazione o contattare il produttore del portatile.
- Assicurarsi che il driver dell'adattatore wireless sia stato installato correttamente e che l'adattatore wireless sia abilitato.
 - **Su Windows 7/8/10/11**

- 1) Se viene visualizzato il messaggio **Nessuna connessione disponibile**, di solito è perché la funzione wireless è disabilitata o bloccata in qualche modo.
- 2) Fare clic su **Risoluzione dei problemi** e Windows potrebbe essere in grado di risolvere il problema da solo.

Se si trova un'altra rete wireless oltre alla propria, seguire la procedura seguente:

- Controllare l'indicatore LED WLAN del router/modem wireless.
- Assicurarsi che il computer/dispositivo sia ancora nel raggio d'azione del router/modem. Avvicinatelo se attualmente è troppo lontano.
- Andare su **Wireless** o **Avanzate > Wireless > Impostazioni Wireless** e controllare le Impostazioni Wireless. Verificare che il nome della rete wireless e l'SSID non siano nascosti.

Se si riesce a trovare la rete wireless ma non si riesce a connettersi, seguire la procedura seguente:

- **Problema di autenticazione/incompatibilità della password:**

- 1) A volte viene chiesto di digitare un numero PIN quando ci si connette alla rete wireless per la prima volta. Questo numero PIN è diverso dalla password wireless/chave di sicurezza della rete; di solito si trova solo sull'etichetta del router.



- 2) Se non si riesce a trovare il PIN o il PIN non è riuscito, si può scegliere di **connettersi utilizzando una chiave di sicurezza**, quindi digitare la **password wireless/chave di sicurezza della rete**.
- 3) Se continua a visualizzare la nota di **Network Security Key Mismatch**, si suggerisce di confermare la password wireless del router wireless.

■ Nota: la password wireless/chave di sicurezza della rete è sensibile alle maiuscole e alle minuscole.

- **Windows non è in grado di connettersi a XXXX / Non è possibile unirsi a questa rete / Ci vuole più tempo del solito per connettersi a questa rete:**

- Controllare la potenza del segnale wireless della rete. Se è debole (1~3 barre), avvicinare il router e riprovare.

- Modificare il canale wireless del router su 1, 6 o 11 per ridurre l'interferenza di altre reti.
- Reinstallare o aggiornare il driver dell'adattatore wireless del computer.

Dichiarazione di conformità CE

TP-Link dichiara che il dispositivo è conforme ai requisiti essenziali e alle altre disposizioni pertinenti delle direttive 2014/53/UE, 2009/125/CE, 2011 /65/UE e (UE) 2015/863.

La dichiarazione di conformità originale dell'UE è disponibile all'indirizzo <https://www.tp-link.com/en/support/ce/>

Attenzione:

La banda 5150-5250 MHz è riservata esclusivamente all'uso interno, al fine di ridurre i rischi di disturbo che possono derivare dai sistemi di satelliti mobili che utilizzano gli stessi canali;

I prodotti utilizzano la tecnica di attenuazione DFS (selezione dinamica delle frequenze) sulle bande 5250- 5350 MHz, 5470-5600MHz e 5650-5725MHz.

Dichiarazione di esposizione alle radiazioni:

Questa apparecchiatura è conforme ai limiti di esposizione alle radiazioni IC stabiliti per un ambiente non controllato. Questa apparecchiatura deve essere installata e utilizzata a una distanza minima di 20 cm tra il radiatore e il corpo.

Dichiarazione di esposizione alle radiazioni:

L'apparecchiatura è conforme ai limiti di esposizione ai raggi IC stabiliti per un ambiente non controllato. L'apparecchio deve essere installato e utilizzato a una distanza minima di 20 cm tra la sorgente di raggi e il corpo.

Informazioni sulla sicurezza

- Tenere il dispositivo lontano da acqua, fuoco, umidità o ambienti caldi.
- Non tentare di smontare, riparare o modificare il dispositivo. Se avete bisogno di assistenza, contattateci.
- Non utilizzare alimentatori diversi da quelli raccomandati.
- Non utilizzare il dispositivo in luoghi in cui i dispositivi wireless non sono ammessi.
- L'alimentatore deve essere installato vicino all'apparecchiatura e deve essere facilmente accessibile.
- Utilizzare solo gli alimentatori forniti dal produttore e contenuti nella confezione originale del prodotto. Per qualsiasi domanda, non esitate a contattarci.
- Questo prodotto utilizza radio e altri componenti che emettono campi elettromagnetici. I campi elettromagnetici e i magneti possono interferire con pacemaker e altri dispositivi medici impiantati. Tenere sempre il prodotto e il suo alimentatore a una distanza di oltre 20 cm da pacemaker o altri dispositivi

medici impiantati. Se si sospetta che il prodotto interferisca con il pacemaker o con altri dispositivi medici impiantati, spegnere il prodotto e consultare il medico per informazioni specifiche sul dispositivo medico.

- Temperatura di esercizio: 0°C~40°C

Durante l'utilizzo del dispositivo, leggere e seguire le informazioni di sicurezza sopra riportate. Non possiamo garantire che non si verifichino incidenti o danni dovuti a un uso improprio del dispositivo. Utilizzare il prodotto con cautela e a proprio rischio e pericolo.

Suggerimenti: L'etichetta del prodotto si trova sul fondo del prodotto.

Spiegazioni dei simboli sull'etichetta del prodotto

Simbolo	Spiegazione
	Tensione CC
	Tensione CA
	Apparecchiature di classe II
	Polarità dei morsetti di uscita
	Efficienza energetica Marcatura
	Solo per uso interno
	Attenzione
	Manuale dell'operatore
	RICICLO Questo prodotto reca il simbolo di selezione selettiva dei rifiuti di apparecchiature elettriche ed elettroniche (RAEE). Ciò significa che questo prodotto deve essere trattato in conformità alla direttiva europea 2012/19/UE per essere riciclato o smantellato al fine di ridurre al minimo l'impatto sull'ambiente. L'utente può scegliere se consegnare il proprio prodotto a un'organizzazione di riciclaggio competente o al rivenditore quando acquista una nuova apparecchiatura elettrica o elettronica.