

TP-LINK®

Guida Utente

TD-W8960N

Modem Router ADSL2+ Wireless N 300Mbps



COPYRIGHT & TRADEMARKS

Le specifiche sono soggette a modifiche senza obbligo di preavviso. **TP-LINK**[®] è un marchio registrato di TP-LINK TECHNOLOGIES CO., LTD. Tutti gli altri marchi e nomi di prodotto sono marchi registrati dai legittimi proprietari.

Nessuna parte delle presenti specifiche può essere riprodotta, neppure parzialmente, in alcuna forma o mezzo oppure utilizzata per traduzioni, modifiche o adattamenti senza specifica autorizzazione scritta da parte di TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2015 TP-LINK TECHNOLOGIES CO., LTD. Tutti i diritti riservati.

<http://www.tp-link.com>

FCC STATEMENT



Questo apparecchio è stato testato ed è risultato conforme ai limiti per i dispositivi digitali di Classe B, in conformità alle norme FCC parte 15. Questi limiti hanno lo scopo di assicurare una protezione adeguata dalle interferenze dannose in una installazione residenziale. Questo apparecchio genera, utilizza e può irradiare energia a radiofrequenza e, se non viene installato ed utilizzato in conformità alle istruzioni del produttore, può causare interferenze dannose nella ricezione delle comunicazioni radio. Non vi è comunque alcuna garanzia che tali interferenze non si verifichino in un'installazione specifica. Qualora il dispositivo dovesse essere causa di interferenze dannose nella ricezione radiotelevisiva, che può essere verificata accendendo e spegnendo l'apparecchio, si consiglia all'utente di provare a correggere l'interferenza adottando una o più delle seguenti misure:

- riorientare o riposizionare l'antenna ricevente;
- aumentare la distanza tra apparecchio e ricevitore;
- collegare l'apparecchio ad una presa di un circuito diverso da quello a cui è collegato il ricevitore;
- consultare il rivenditore od un tecnico esperto radio / TV per altri suggerimenti.

Questo dispositivo è conforme alla norme FCC parte 15. Il funzionamento è soggetto alle due seguenti condizioni:

1. questo dispositivo non deve causare interferenze dannose;
2. questo dispositivo deve accettare qualsiasi interferenza ricevuta, incluse interferenze che potrebbero comprometterne il funzionamento.

Qualsiasi cambiamento o modifica apportati all'apparecchio non espressamente approvati dalla parte competente in materia di conformità può invalidare il diritto dell'utente ad utilizzare l'apparecchio.

Nota: Il produttore non è responsabile per eventuali interferenze radio o tv causate da modifiche non autorizzate di questo dispositivo. Tali modifiche invalidano il diritto dell'utente ad utilizzare l'apparecchio.

Dichiarazione Precauzioni per l'esposizione a RF della FCC:

Questo apparecchio è conforme ai limiti stabiliti dalle norme FCC RF relative all'esposizione a radiazioni in ambienti non soggetti a controllo. Questo dispositivo e la sua antenna non devono essere posizionati o funzionare in combinazione con qualsiasi altra antenna o trasmettitore.

“In conformità alle norme FCC RF relative all'esposizione a radiazioni, questo accordo è applicabile solo a dispositivi mobili. Le antenne usate per questo trasmettitore devono essere installate ad una distanza dal corpo di almeno 20 cm e non devono essere posizionati o funzionare in combinazione con qualsiasi altra antenna o trasmettitore”.

CE Mark Warning

CE 1588

Questo è un prodotto digitale di classe B. In un ambiente domestico potrebbe causare interferenze radio, nel qual caso l'utente è tenuto a prendere misure adeguate.

Restrizioni nazionali

Questo dispositivo è inteso per utilizzo in tutti i paesi EU (e negli altri paesi che seguono le direttive EU 1999/5/EC) senza alcuna limitazione ad eccezione dei paesi qui sotto elencati:

| Paese | Restrizione | Nota |
|-------------------|--|--|
| Bulgaria | Nessuna | E' richiesta un'autorizzazione generica per uso in esterni e come pubblico servizio |
| Francia | Uso limitato in ambienti esterni a 10 mW (10dBm) entro una banda di frequenza di 2454-2483.5 MHz | Uso radio-localizzazione militare. Negli ultimi anni è in corso l'assegnazione della banda a 2.4 GHz per permettere più flessibilità. Piena attuazione pianificata per il 2012 |
| Italia | Nessuna | Se utilizzata al di fuori dei propri locali, è richiesta un'autorizzazione generica. |
| Lussemburgo | Nessuna | Richiesta di autorizzazione generica per la rete e la fornitura del servizio (non per lo spettro) |
| Norvegia | In attuazione | Questa sottosezione non si applica per l'area geografica nel raggio di 20Km dal centro di Ny-Alesund |
| Federazione Russa | Nessuna | Solo per applicazioni in ambienti interni |

Nota: In Francia si prega di non utilizzare il prodotto in ambienti esterni.

Questo dispositivo è progettato per operare con antenne di guadagno massimo 3dBi. L'utilizzo di antenne con guadagno maggiore non è consentito. L'impedenza nominale richiesta per le antenne è 50Ω.

Per ridurre il rischio di interferenza la potenza irradiata (E.I.R.P.) non deve superare i limiti consentiti.

DICHIARAZIONE DI CONFORMITA'

Per i seguenti dispositivi:

Descrizione Prodotto: **Modem Router ADSL2+ Wireless N 300Mbps**

Modello N.: **TD-W8960N**

Marchio: **TP-LINK**

Dichiariamo sotto la nostra responsabilità che i prodotti precedenti soddisfano tutti i regolamenti tecnici applicabili ai prodotti stessi nell'ambito delle Direttive del Concilio:

Directives 1999/5/EC, Directives 2004/108/EC, Directives 2006/95/EC, Directives 1999/519/EC, Directives 2011/65/EU

Il prodotto precedente è conforme ai seguenti standard o documenti relativi ad altre normative

EN 300328 V1.8.1

ETSI EN 301 489-1 V1.9.2:2011& EN301489-17 V2.2.1

EN 55022:2010

EN 55024:2010

EN 61000-3-2:2006+A1:2009+A2:2009

EN 61000-3-3:2008

EN60950-1:2006+A11: 2009+A1:2010+A12:2011

EN62311:2008

Il prodotto riporta il Marchio CE:

CE 1588

Persona responsabile della conformità di questa dichiarazione:



Yang Hongliang

Product Manager of International Business

Data di rilascio: 2015

INDICE DEI CONTENUTI

| | |
|--|-----------|
| Contenuto della confezione | 1 |
| Capitolo 1.Introduzione | 2 |
| 1.1 Panoramica del prodotto | 2 |
| 1.2 Caratteristiche principali | 3 |
| 1.3 Pannello | 4 |
| 1.3.1 Pannello anteriore | 4 |
| 1.3.2 Pannello posteriore | 5 |
| Capitolo 2.Installazione hardware | 6 |
| 2.1 Requisiti di sistema | 6 |
| 2.2 Ambiente d'installazione | 6 |
| 2.3 Collegamento del modem/router | 6 |
| Capitolo 3.Guida rapida all'installazione | 8 |
| 3.1 Configurazione computer | 8 |
| 3.2 Guida rapida all'installazione | 9 |
| Capitolo 4.Configurazione software | 13 |
| 4.1 Accesso..... | 13 |
| 4.2 Informazioni dispositivo | 13 |
| 4.3 Quick Setup..... | 14 |
| 4.4 Configurazione avanzata | 14 |
| 4.4.1 Interfaccia layer 2..... | 14 |
| 4.4.2 WAN..... | 16 |
| 4.4.3 MAC Clone..... | 23 |
| 4.4.4 LAN | 24 |
| 4.4.5 NAT | 27 |
| 4.4.6 Sicurezza | 31 |
| 4.4.7 Parental Control | 33 |
| 4.4.8 QoS | 35 |
| 4.4.9 Bandwidth Control..... | 38 |
| 4.4.10 Routing..... | 40 |
| 4.4.11 DNS..... | 42 |
| 4.4.12 DSL | 44 |

| | |
|--|-----------|
| 4.4.13 UPnP | 45 |
| 4.4.14 Interface Grouping | 45 |
| 4.4.15 Tunnel IP | 46 |
| 4.4.16 IPSec..... | 48 |
| 4.4.17 Multicast | 50 |
| 4.5 Wireless | 51 |
| 4.5.1 Wireless | 51 |
| 4.5.2 Sicurezza | 52 |
| 4.5.3 Timer..... | 61 |
| 4.5.4 Filtro MAC | 62 |
| 4.5.5 Bridge wireless..... | 63 |
| 4.5.6 Avanzate | 64 |
| 4.5.7 Informazioni dispositivo..... | 65 |
| 4.6 Rete guest..... | 65 |
| 4.6.1 Configurazione di base | 65 |
| 4.6.2 Dispositivi collegati..... | 66 |
| 4.7 Diagnostica | 67 |
| 4.8 Gestione..... | 67 |
| 4.8.1 Configurazione | 68 |
| 4.8.2 Log di sistema..... | 69 |
| 4.8.3 SNMP..... | 70 |
| 4.8.4 TR-069 | 71 |
| 4.8.5 Ora Internet..... | 72 |
| 4.8.6 Controllo accessi..... | 73 |
| 4.8.7 Aggiornamento..... | 74 |
| 4.8.8 Riavvio | 75 |
| 4.9 Logout..... | 75 |
| Appendice A: Specifiche..... | 76 |
| Appendice B: Risoluzione dei problemi | 77 |
| Appendice C: Supporto Tecnico | 85 |

Contenuto della confezione

La confezione contiene:

- 1 x TD-W8960N
- 1 x Alimentatore
- 1 x Guida Rapida d'Installazione
- 1 x Cavo Ethernet RJ45
- 2 x Cavo ADSL/Fonia RJ11
- 1 x Splitter ADSL
- 1 x CD-ROM contenente:
 - Questa Guida Utente
 - Software

 **Nota:**

Dovessero una o più parti risultare danneggiate o mancanti, contattare immediatamente il Rivenditore.

Capitolo 1. Introduzione

1.1 Panoramica del prodotto

Il Modem Router ADSL2+ Wireless N300 TD-W8960N è una soluzione all-in-one che integra modem, router ed access point, garantendo eccezionali prestazioni. La tecnologia wireless MIMO 2x2 offre massime ampiezza di copertura, stabilità e velocità di trasferimento dati wireless.

Il modem ADSL2+ è coadiuvato da una CPU High Speed MIPS, con router full-rate ADSL2+ conforme alle specifiche ITU ed ANSI.

È supportato il framing ADSL2+ a doppia latenza (fast ed interleaved); è supportato il Physical Layer I.432 ATM.

La connettività wireless raggiunge i 300Mbps tramite lo standard 802.11n. Questa velocità rende agevolmente fruibili più applicazioni allo stesso tempo. Le performance dello standard 802.11n consentono il raggiungimento di velocità pari al 650% rispetto alla standard 802.11g pur mantenendo la retrocompatibilità con gli standard IEEE 802.11g e IEEE 802.11b.

Le funzionalità di sicurezza, quali SSID broadcast control, crittografia WEP 64/128, sicurezza WPA2-PSK/WPA-PSK, rete guest e protezione Firewall avanzata assicurano la protezione dei dati gestiti.

Gli accessi sono ampiamente regolamentabili consentendo ad amministratori di rete e genitori di definire policy personalizzate. Sono supportati host DMZ e Port Triggering, per consentire il monitoraggio della rete in tempo reale.

Nota:

Il “Modem Router ADSL2+ Wireless N300 TD-W8960N” è normalmente indicato in questa Guida come “dispositivo”, “modem”, “router”, “modem/router” o “TD-W8960N” senza ulteriori dettagli.

1.2 Caratteristiche principali

- 4 porte LAN 10/100Mbps Auto-Negotiation RJ45 (Auto MDI/MDIX), 1 porta RJ11
- Splitter esterno
- Modulazione e demodulazione DMT
- Modalità bridge e router
- Downstream fino a 24Mbps, upstream fino a 3.5Mbps (con Annex M abilitato)
- Massima lunghezza di linea: 6.5Km
- Configurazione remota e gestione via SNMP o CWMP
- Supporto PPPoE con gestione della policy di connessione
- Supporto modalità asimmetrica downstream/upstream
- Supporto PVC Multipli
- Protezione ESD
- Server DHCP
- Firewall, Filtro IP/MAC, Application ed URL
- Supporto Virtual Server, Host DMZ ed IP Address Mapping
- Supporto Dynamic DNS, UPnP e Static Routing
- System log e statistiche di traffico
- Protezione WPA-PSK/WPA2-PSK, WPA/WPA2 e WEP
- Rete guest
- Wireless LAN ACL (Access Control List)
- Ethernet WAN (EWAN)
- Bandwidth Control
- IPv6

1.3 Pannello

1.3.1 Pannello anteriore

Gli indicatori LED situati sul pannello frontale, indicano lo stato operativo del dispositivo.



Figura 1-1

Descrizione indicatori LED:

| Nome | Stato | Indicazioni |
|--------------|--------------|--|
| ⏻ (Power) | Acceso | Il modem router è acceso. |
| | Spento | Il modem router è spento: verificare che l'alimentatore sia correttamente collegato. |
| ⚡ (ADSL) | Lampeggiante | La linea ADSL è sincronizzata e pronta all'uso. |
| | Acceso | L'apertura della connessione ADSL è in corso. |
| | Spento | Sincronizzazione ADSL fallita: fare riferimento alla Nota 1 per la risoluzione del problema. |
| 🌐 (Internet) | Spento | La connessione Internet è pronta. |
| | Acceso | Trasmissione dati via Internet in corso. |
| | Spento | Non c'è connessione ad Internet od il modem router sta operando in modalità Bridge. Fare riferimento alla Nota 2 nota 2 per la risoluzione del problema. |
| 📶 (WLAN) | Acceso | Funzionalità wireless abilitata. |
| | Lampeggiante | Trasmissione dati wireless in corso. |
| | Spento | Funzionalità wireless disabilitata. |
| 🔒 (WPS) | Lamp. lento | Un dispositivo wireless ha completato la connessione in modalità WPS. |
| | Acceso | Pronto alla connessione WPS: attivare WPS sul dispositivo da connettere mentre il LED WPS lampeggia (entro 2 minuti). |
| | Lamp. veloce | La funzionalità WPS non è attiva o la connessione non è andata a buon fine nel tempo limite. |
| 🔌 (LAN 1-4) | Lampeggiante | Dispositivo connesso alla porta LAN. |
| | Acceso | Trasmissione in corso sulla porta LAN. |
| | Spento | Nessun dispositivo connesso alla porta LAN. |

Nota:

1. Se il LED ADSL è spento, controllare il collegamento. Fare riferimento a [2.3 Collegamento del modem/router](#). Se il collegamento è corretto, contattare l'ISP (Internet Service Provider).
2. Se il LED Internet è spento, controllare il LED ADSL; se anche il LED ADSL è spento, fare riferimento alla [Nota 1](#). Se il LED ADSL è acceso, verificare i parametri di connessione con l'ISP (Internet Service Provider).

1.3.2 Pannello posteriore

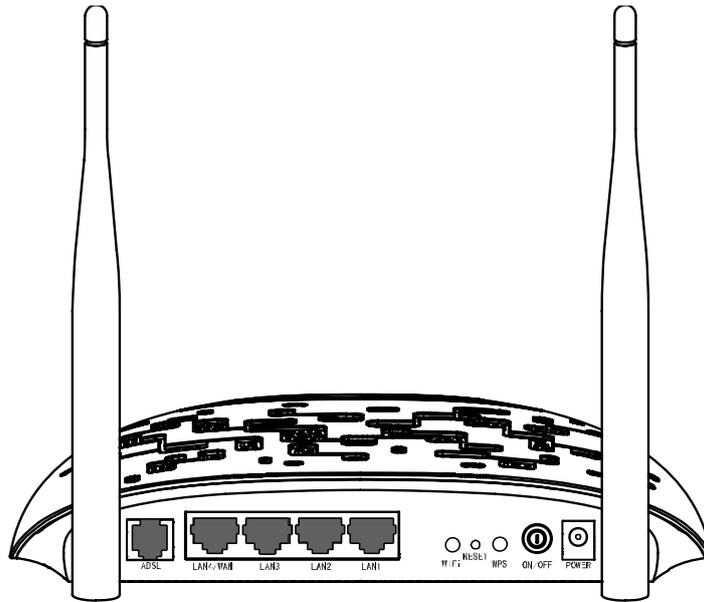


Figura 1-2

- **POWER (Alimentazione):** Collegare all'ingresso Power il connettore dell'alimentatore.
- **ON/OFF:** Interruttore di alimentazione.
- **WPS:** Questo pulsante attiva l'omonima funzionalità. Fare riferimento a [4.5.2.1 WPS](#) per maggiori informazioni.
- **RESET:** Ci sono due modi per ripristinare le impostazioni predefinite di fabbrica:
 1. A router acceso, mantenere premuto tramite un oggetto sottile il tasto Reset per almeno 10 secondi. Il router si riavvierà con le impostazioni predefinite di fabbrica.
 2. Ripristinare le impostazioni predefinite dalla pagina di configurazione web del router tramite "Manutenzione - Riavvio Sistema".
- **Wi-Fi:** Questo pulsante attiva o disattiva la funzionalità wireless.
- **1, 2, 3, 4 (LAN):** Tramite ognuna di queste porte, è possibile collegare il router ad un PC o ad altri dispositivi con interfaccia Ethernet.
- **ADSL:** Tramite questa porta è possibile collegare il router alla linea telefonica od alla presa Modem dello splitter esterno. Per ulteriori dettagli, fare riferimento al punto [2.3 Collegamento del modem/router](#).
- **Antenna:** Consente le connessioni wireless e la trasmissione dei dati.

Capitolo 2. Installazione hardware

2.1 Requisiti di sistema

- Accesso Internet a banda larga (DSL/Cable/Ethernet).
- Computer.

2.2 Ambiente d'installazione

- Il prodotto deve essere al riparo da umidità o da fonti di calore.
- Tenere lontano il dispositivo da forti radiazioni elettromagnetiche e da dispositivi sensibili alle radiazioni elettromagnetiche.
- L'eventuale installazione a muro deve essere eseguito secondo le seguenti indicazioni:

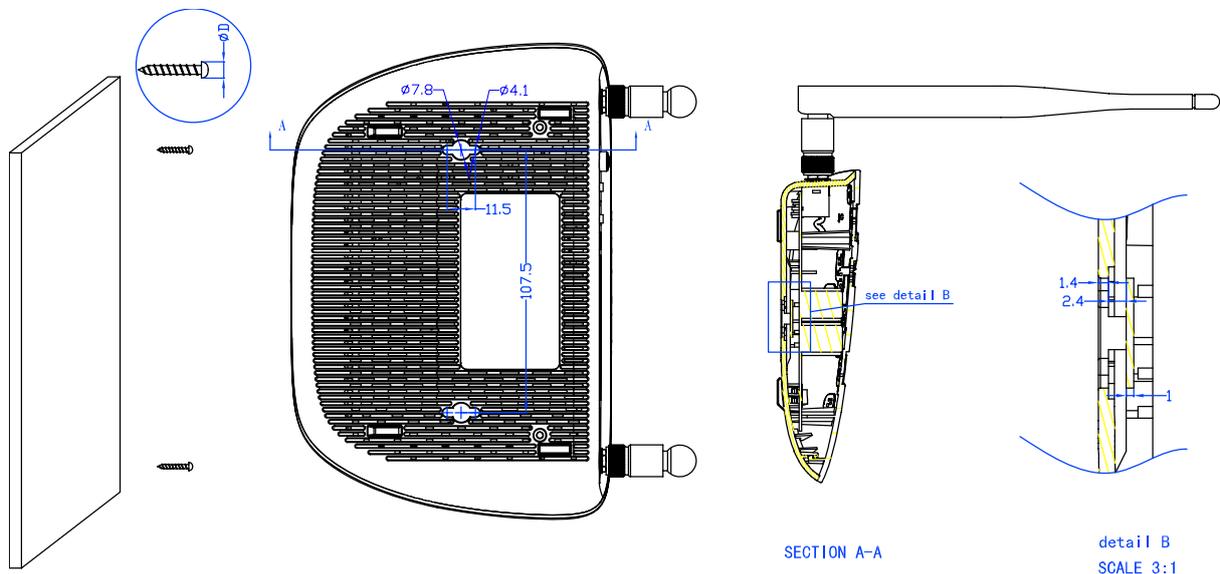


Figura 2-1 Installazione a muro

Nota:

Il diametro della vite è di $4.1\text{mm} < D < 7.8\text{mm}$, e la distanza delle due viti è di 107.5mm. La vite che sporge dal muro richiede una base di circa 4mm, e la lunghezza della vite stessa deve essere di almeno 20mm per reggere il peso del prodotto.

2.3 Collegamento del modem/router

1. Collegare la linea ADSL.

Metodo 1 (telefono non presente): collegare il cavo telefonico/ADSL alla porta LINE sul pannello posteriore del TD-W8968 ed alla presa a muro.

Metodo 2 (telefono presente): utilizzare uno splitter. Gli splitter esterni separano dati e voce, permettendo di accedere ad Internet ed effettuare chiamate telefoniche contemporaneamente. Lo splitter esterno dispone di tre porte:

- LINE. Collegare alla presa telefonica a muro.

- PHONE. Collegare all'apparecchio telefonico mediante cavo telefonico/ADSL.
- MODEM. Collegare alla porta LINE di TD-W8960N mediante cavo telefonico/ADSL.

2. Collegare il cavo di rete Ethernet.

Collegare il cavo di rete alla porta Ethernet del computer (o ad una porta di un hub/switch se presente) e ad una porta LAN del TD-W8960N.

3. Accendere il computer.

4. Collegare l'alimentatore.

5. Connettere l'alimentatore alla presa Power sul retro del router ed inserire la spina in una presa elettrica.

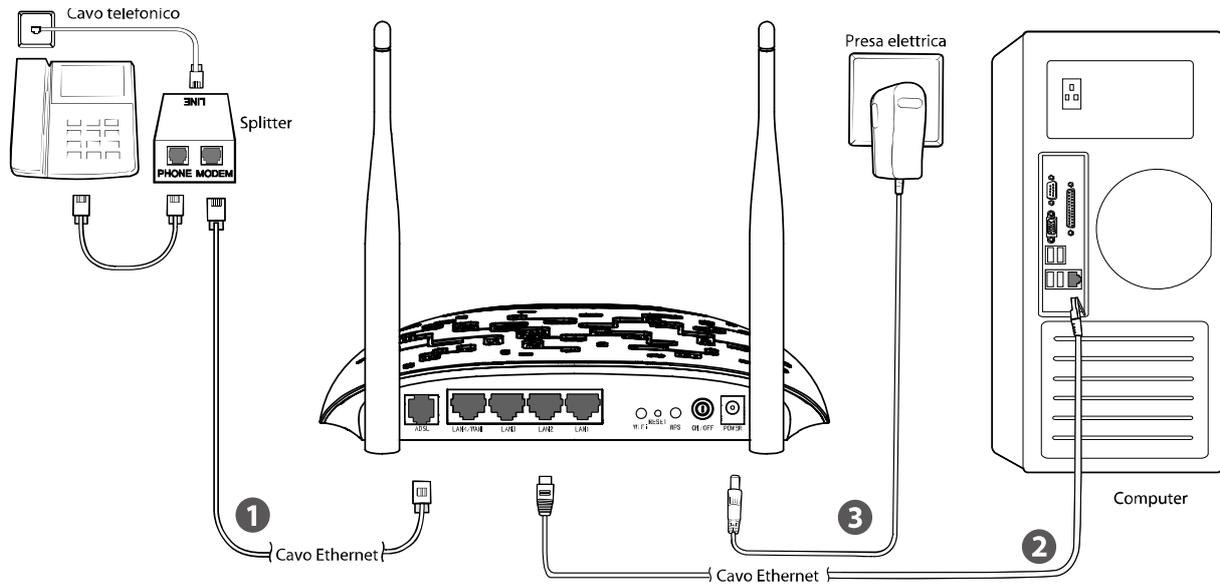


Figura 2-2

Capitolo 3. Guida rapida all'installazione

3.1 Configurazione computer

TD-W8960N è programmato per assegnare automaticamente un indirizzo IP al PC. Tipicamente, il pc assumerà indirizzo 192.168.1.100, mentre il router risponderà all'indirizzo 192.168.1.1.

Nota:

È possibile configurare il PC in modo da personalizzarne indirizzo IP, Subnet Mask, Gateway e DNS. È in questo caso opportuno disabilitare la funzionalità DHCP del router od inserire un'Address Reservation.

È ora possibile verificare la rete eseguendo il comando Ping nel prompt dei comandi: fare clic su sul menu **Start** del desktop, selezionare **Esegui** (o digitare Win+R), digitare **cmd** e premere **Invio**. Digitare **ping 192.168.1.1** sulla prossima schermata e premere **Invio**. Se il risultato visualizzato è simile alla schermata sottostante, la connessione tra il PC ed il router è correttamente stabilita.

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 3-1

Se il risultato visualizzato è invece simile alla seguente schermata, il collegamento al PC non è correttamente operativo.

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 3-2

È possibile eseguire una verifica tramite la seguente procedura.

1) Il PC ed il router sono collegati correttamente?

Gli indicatori LED della porta LAN alla quale si collega il PC e l'indicatore LED sulla scheda di rete Ethernet del PC devono essere accesi o lampeggianti.

2) La configurazione TCP/IP del PC è corretta?

L'indirizzo IP preconfigurato del router è 192.168.1.1: se l'indirizzo del router e la subnet mask non sono stati modificati, l'indirizzo IP del PC deve essere compreso tra 192.168.1.100 e 192.168.1.200.

3.2 Guida rapida all'installazione

TD-W8960N è facilmente configurabile tramite web console, accessibile via browser (come Mozilla Firefox, Google Chrome, Microsoft Internet Explorer o Safari).

1. Aprire un browser web e navigare <http://tplinkmodem.net/> .



Figura 3-3

Alla richiesta di autenticazione, come in Figura 3-4, digitare in lettere minuscole come Nome Utente **“admin”** e come Password **“admin”**; quindi fare clic su **Login**.



Figura 3-4

2. Appare la web console come in Figura 3-5, fare clic su **Quick Setup**.

| Informazioni dispositivo | | |
|-------------------------------|------------------------------------|---|
| Versioni | | |
| Versione firmware: | 1.1.1 Build 140317 Rel.31821 | |
| Versione hardware: | TD-W8960N V5 0x00000001 | |
| Tempo di attività: | 0Day(s) 00:17:12 | |
| LAN | | |
| IPv4 | Indirizzo IP LAN: | 192.168.1.1 |
| | Indirizzo MAC LAN: | 02:10:18:01:00:01 |
| IPv6 | Lunghezza indirizzo/prefisso IPv6: | NULL |
| | Configurazione automatica: | RADVD&DHCPv6 |
| ADSL | | |
| Stato linea: | Non attiva | |
| Velocità - Upstream (Kbps): | 0 | |
| Velocità - Downstream (Kbps): | 0 | |
| Internet | | |
| IPv4 | Stato: | Non attiva |
| | Tipo WAN: | ATM WAN |
| | Interfaccia layer 2: | atm0(8/35) |
| | Tipo Connessione: | PPPoA |
| | Indirizzo IP WAN: | 0.0.0.0 |
| | Shortcut: | Fare clic qui per visualizzare le interfacce WAN e le informazioni per la risoluzione dei problemi. |

Figura 3-5

3. Selezionare poi il tipo di connessione WAN corretto, quindi fare clic su **Avanti**.

| Quick Setup - WAN | | |
|--|--|---|
| Selezionare il tipo di interfaccia WAN. | | |
| Tipo WAN: | <input checked="" type="radio"/> ADSL | Per la connessione ad una linea ADSL |
| | <input type="radio"/> Ethernet | Per la connessione ad una rete Ethernet |
| | <input type="checkbox"/> Abilita IPv6 per questa interfaccia | |
| <input type="button" value="Salta WAN"/> <input type="button" value="Avanti"/> | | |

Figura 3-6

4. Selezionando **ADSL** occorre specificare regione e provider ISP, quindi verificare l'esattezza dei parametri e modificarli se differenti da quanto specificato dal provider. Fare clic su **Avanti** per continuare (la presente guida mostra, a titolo esemplificativo, la configurazione in modalità PPPoA).

Quick Setup - WAN

Regione:

ISP:

VPI/VC1: / (

Incapsulamento: (opzionale)

Tipo accesso WAN:

Nome utente PPP:

Password PPP:

MTU (byte): (opzionale)

Figura 3-7

 **Nota:** Se il provider in uso non è elencato, selezionare **Altro** ed immettere manualmente i parametri.

Selezionando Ethernet occorre specificare la modalità di connessione prescritta dal provider per la porta WAN, quindi fare clic su **Avanti**.

Quick Setup - WAN

Porta Ethernet WAN:

Tipo accesso WAN:

Nome utente PPP:

Password PPP:

Nome connessione PPPoE: (opzionale)

MTU (byte): (opzionale)

Figura 3-8

5. La funzionalità wireless è abilitata di default, è possibile modificare nome della rete (SSID) e password, quindi fare click su **Avanti** per continuare.

Quick Setup - Wireless

Abilita Wireless:

È possibile configurare il nome della rete e la sicurezza wireless.

Nome rete wireless: (SSID)

Si raccomanda caldamente l'utilizzo della protezione WPA2-PSK.

Sicurezza: ▼

Password: (WPA Pre-Shared Key)
(da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimali)

Figura 3-9

6. Verificare tutti i parametri e fare clic su **Confermare** per applicare la configurazione.

Quick Setup - Sommario

Configurazioni WAN

| | |
|-----------------------|---------------|
| Tipo WAN: | ADSL WAN |
| Informazioni layer 2: | 8/35 VCMUX |
| Tipo link WAN: | PPPoA |
| Nome utente PPP: | username |
| Password PPP: | password |
| MTU PPP: | 1480 |

Nota 1: Alcune connessioni WAN od interfacce layer 2 devono essere sostituite.
Nota 2: Alcuni virtual server devono essere eliminati.

Configurazioni Wi-Fi

| | |
|----------------------------|---------------|
| Nome rete wireless (SSID): | 123 |
| Autenticazione: | WPA2-Personal |
| Password: | 12345678 |

Figura 3-10

Capitolo 4. Configurazione software

4.1 Accesso

| |
|--------------------------|
| Informazioni dispositivo |
| Quick Setup |
| Configurazione avanzata |
| Wireless |
| Rete guest |
| Diagnostica |
| Gestione |
| Logout |

Dopo l'accesso è visualizzato il menu della web console. Sulla destra, le istruzioni relative alla voce selezionata.

4.2 Informazioni dispositivo

Selezionare “**Informazioni dispositivo**” per visualizzare le informazioni relative allo stato del sistema.

| Informazioni dispositivo | | |
|-------------------------------|------------------------------------|---|
| Versioni | | |
| Versione firmware: | 1.1.1 Build 140317 Rel.31821 | |
| Versione hardware: | TD-W8960N V5 0x00000001 | |
| Tempo di attività: | 0Day(s) 00:17:12 | |
| LAN | | |
| IPv4 | Indirizzo IP LAN: | 192.168.1.1 |
| | Indirizzo MAC LAN: | 02:10:18:01:00:01 |
| IPv6 | Lunghezza indirizzo/prefisso IPV6: | NULL |
| | Configurazione automatica: | RADVD&DHCPv6 |
| ADSL | | |
| Stato linea: | Non attiva | |
| Velocità - Upstream (Kbps): | 0 | |
| Velocità - Downstream (Kbps): | 0 | |
| Internet | | |
| IPv4 | Stato: | Non attiva |
| | Tipo WAN: | ATM WAN |
| | Interfaccia layer 2: | atm0(8/35) |
| | Tipo Connessione: | PPPoA |
| | Indirizzo IP WAN: | 0.0.0.0 |
| | Shortcut: | Fare clic qui per visualizzare le interfacce WAN e le informazioni per la risoluzione dei problemi. |

Figura 4-1

4.3 Quick Setup

Fare riferimento a [3.2 Guida rapida all'installazione](#).

4.4 Configurazione avanzata



4.4.1 Interfaccia layer 2

Selezionare “**Configurazione avanzata**” → “**Interfaccia layer2**” per specificare il tipo d’interfaccia.

- **Interfaccia ATM:** TD-W8960N opera come modem/router ADSL tramite la porta RJ11, occorre specificare i parametri di connessione forniti dal provider ISP. (Figura 4-2)
- **Interfaccia ETH:** TD-W8960N opera come router Ethernet tramite porta WAN RJ45.

4.4.1.1 Interfaccia ATM

Selezionare “**Configurazione avanzata**” → “**Interfaccia Layer2**” → “**Interfaccia ATM**”.

| Configurazione interfaccia ATM DSL | | | | | | | | | | | | | | |
|---|-----|-----|-----------|----------------|-----------|-----|-----|----------------|-------------------------|-----------|-----------|-----------|-----------------|--------------------------|
| Fare clic su Aggiungi od Elimina per configurare le interfacce ATM. | | | | | | | | | | | | | | |
| Interfaccia | VPI | VCI | Tipo link | Incapsulamento | Categoria | PCR | SCR | Max Burst Size | Modalità di connessione | IP QoS | Sched Alg | Peso cosa | Presenza gruppo | Elimina |
| atm0 | 8 | 35 | PPPoA | VC/MUX | UBR | | | | DefaultMode | Abilitato | WRR | 1 | 8 | <input type="checkbox"/> |
| <input type="button" value="Aggiungi"/> <input type="button" value="Elimina tutto"/> <input type="button" value="Elimina"/> | | | | | | | | | | | | | | |

Figura 4-2

- **Elimina:** Selezionare le interfacce da rimuovere e fare clic per eliminarle.

Nota:

Se l'interfaccia è utilizzata da una connessione WAN in [4.4.2 WAN](#) è necessario rimuovere la connessione prima dell'interfaccia.

- **Aggiungi:** Fare clic per aggiungere un'interfaccia.

Figura 4-3

- **VPI/VCI:** Specificare i valori prescritti dal provider ISP.
- **Selezionare la tipologia link DSL(EoA per PPPoE, IpoE o Bridge):** Selezionare la modalità prescritta fra **EoA** (PPPoE, IPoE, e bridge), **PPPoA** ed **IPoA**.
- **Incapsulamento:** Selezionare la modalità prescritta dal provider ISP.
- **Categoria servizio:** Selezionare il tipo di servizio offerto dal provider ISP.

Nota:

1. Contattare il provider ISP in mancanza dei parametri di configurazione.
2. L'abilitazione di QoS sul PVC aumenta le performance ma utilizza molte risorse di sistema, sarà pertanto ridotto il numero di PVC configurabili. QoS non può essere configurato per connessioni CBR e Real-time VBR. Selezionando QoS apparirà la voce di menu descritta in [4.4.8 QoS](#).

4.4.1.2 Interfaccia ETH

Selezionare “**Configurazione avanzata**” → “**Interfaccia layer 2**” → “**Interfaccia ETH**”.

Figura 4-4

Nota:

È necessario abilitare la porta ETH in “**Configurazione avanzata**” → “**LAN**”.

➤ **Aggiungi:** Fare clic per aggiungere un’interfaccia.

Figura 4-5

➤ **Selezionare una Porta ETH:** Selezionare la porta da utilizzare come WAN.

Fare clic su **Salva/Applica** per applicare le impostazioni e visualizzare la schermata in Figura 4-6.

| Interfaccia | Modalità di connessione | Elimina |
|-----------------|-------------------------|--------------------------|
| eth3/(LAN4/WAN) | DefaultMode | <input type="checkbox"/> |

Figura 4-6

➤ **Elimina:** Selezionare le interfacce da eliminare e fare clic per rimuoverle.

Nota:

Solo una ETH può essere configurata come WAN layer 2.

4.4.2 WAN

Selezionare “**Configurazione avanzata**” → “**Connessione WAN**” per visualizzare le informazioni relative alle interfacce WAN come in Figura 4-7. Dopo aver configurato un’interfaccia di layer 2 sono disponibili 5 modalità: PPPoE, PPPoA, IPoE, IPoA e Bridge. Selezionare la modalità prescritta dal provider ISP.

| Interfaccia | Descrizione | Tipo | Vlan8021p | VlanMuxId | Icmp | NAT | Firewall | IPv6 | Mld | Elimina | Modifica |
|-------------|--------------|-------|-----------|-----------|-----------|-----------|-----------|--------------|--------------|--------------------------|----------|
| ppp0a0 | ppp0a_0_8_35 | PPPoA | N/A | N/A | Abilitato | Abilitato | Abilitato | Disabilitato | Disabilitato | <input type="checkbox"/> | Modifica |

Figura 4-7

4.4.2.1 ATM-EoA-PPPoE

Se il provider ISP prescrive **PPPoE** come metodo di connessione:

1. Aggiungere una nuova interfaccia ATM e selezionare **EoA** in [4.4.1.1 Interfaccia ATM](#).
2. Fare clic su **Aggiungi** come in Figura 4-7 per mostrare la schermata in Figura 4-8. Fare clic su **Avanti**.

Configurazione interfaccia connessione WAN

Selezionare un'interfaccia layer 2

Nota: Per interfacce ATM la stringa del descrittore (portId_vpi_vci)

Interfaccia layer 2: atm0/(0_8_40) ▼

Indietro Avanti

Figura 4-8

3. Selezionare PPPoE in Figura 4-9, inserire una breve descrizione e fare clic su **Avanti**.

Configurazione connessione WAN

Tipo servizio WAN:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Inserire una descrizione per la connessione: pppoe_0_8_40

Per le connessioni taggate, specificare una Priorità 802.1P valida ed un ID VLAN 802.1Q.
Per le connessioni non taggate inserire -1 come Priorità 802.1P ed ID VLAN 802.1Q.

Specificare Priorità 802.1P [0-7]: -1

Specificare ID VLAN 802.1Q [0-4094]: -1

Selezione protocollo: Solo IPV4 ▼

Indietro Avanti

Figura 4-9

4. Specificare i parametri richiesti e fare clic su **Avanti**.

Credenziali PPP

Specificare le credenziali PPP se fornite dal provider ISP.

| | |
|---------------------------|---|
| Nome utente PPP: | <input type="text" value="12345678"/> |
| Password PPP: | <input type="password" value="••••••"/> |
| Nome connessione PPPoE: | <input type="text"/> |
| Metodo di Autenticazione: | <input type="text" value="AUTO"/> |
| MTU (bytes): | <input type="text" value="1480"/> (predefinito 1480, modificare solamente se necessario.) |

- Abilita NAT fullcone
- Dial on demand (con timer di timeout inattivo)
- Estensione IP PPP
- Utilizza indirizzo IPv4 statico
- Abilita modalità PPP debug
- Esegui il bridge sui frame PPPoE tra WAN e porte locali

Proxy Multicast

- Abilita proxy IGMP multicast

Figura 4-10

- **Nome utente / Password PPP:** Specificare le credenziali fornite dal provider ISP per l'accesso.
- **Nome connessione PPPoE:** Specificare opzionalmente un nome per la connessione.
- **Authentication Method:** Si consiglia di non modificare il valore predefinito.

Nota:

Contattare il provider ISP in mancanza delle credenziali.

- **MTU (bytes):** dimensione massima del pacchetto. Selezionare questa opzione per impostare un valore personalizzato se richiesto dal provider ISP.
 - **Abilita NAT fullcone:** Tipo di NAT alternativo al tradizionale.
 - **Dial on demand(with idle timeout timer):** La connessione è stabilita quando un dispositivo fa traffico non locale e viene mantenuta fino a quando non si raggiunge un periodo d'inattività corrispondente al timeout.
 - **Estensione IP PPP:** Selezionare se il provider ISP lo richiede per trasferire l'IP pubblico ad un dispositivo.
 - **Utilizza indirizzo IPv4 statico:** Selezionare se il provider ISP prescrive dei valori d'indirizzamento statici.
 - **Abilita modalità PPP debug:** Selezionare per registrare ogni evento PPP nel log di sistema.
 - **Esegui il bridge sui frame PPPoE tra WAN e porte locali:** Selezionare per consentire ai dispositivi in LAN di effettuare connessioni PPP dirette.
 - **Abilita proxy IGMP multicast:** IGMP (Internet Group Management Protocol) è utilizzato per le connessioni multicast e può essere utilizzato anche dal provider ISP per la configurazione remota, abilitare se necessario.
5. Selezionare l'interfaccia WAN predefinita per il gateway predefinito come in Figura 4-11 e fare clic su **Avanti**.

Routing -- Gateway predefinito

È possibile configurare più interfacce WAN, verrà utilizzata l'interfaccia disponibile con maggiore priorità. La priorità può essere gestita rimuovendo e ricreando le interfacce.

Selezione interfacce gateway predefinito

Interfacce WAN disponibili

ppp0.1

>

<

Indietro Avanti

Figura 4-11

6. Configurare I server DNS e fare clic su **Avanti**.

Configurazione server DNS

Selezionare un'interfaccia per il server DNS o configurare manualmente l'indirizzo IP del server. In modalità ATM l'indirizzo IP deve essere configurato solo se è presente un solo PVC in modalità IPoE od IPoA. Possono coesistere più interfacce server DNS, sarà utilizzata l'interfaccia disponibile con maggiore priorità. La priorità può essere variata rimuovendo e ricreando le interfacce.

Selezionare le interfacce per il server DNS tra le interfacce WAN disponibili:

Selezione interfacce server DNS

Interfacce disponibili

ppp0.1

>

<

Utilizza il seguente server DNS:

Server DNS primario:

Server DNS secondario:

Indietro Avanti

Figura 4-12

- **Selezione le interfacce per il server DNS tra le interfacce WAN disponibili:** Specificare l'interfaccia WAN predefinita per i server DNS.
- **Utilizza il seguente server DNS:** È possibile specificare manualmente l'IP dei server DNS.

Nota:

Se è configurato un solo PVC in modalità IPoA è necessario specificare gli indirizzi.

7. Verificare la correttezza delle informazioni e fare clic su **Salva/Applica** per applicarle.

Configurazione WAN - Sommario

Assicurarsi che i parametri coincidano con quelli forniti dal provider ISP.

| | |
|-------------------|--------------|
| Tipo connessione: | PPPoE |
| NAT: | Abilitato |
| NAT fullcone: | Disabilitato |
| Firewall: | Abilitato |
| IGMP multicast: | Abilitato |
| QoS: | Abilitato |

Fare clic su "Salva/Applica" per attivare l'interfaccia o su "Indietro" per modificarla.

Indietro Salva/Applica

Figura 4-13

8. La nuova interfaccia è ora elencata.

Configurazione connessione WAN (Wide Area Network)

Fare clic su **Aggiungi**, **Modifica** od **Elimina** per configurare le interfacce WAN.

| Interfaccia | Descrizione | Tipo | Vlan8021p | VlanMuxId | Igmp | NAT | Firewall | IPv6 | Mld | Elimina | Modifica |
|-------------|--------------|-------|-----------|-----------|-----------|-----------|-----------|--------------|--------------|--------------------------|---|
| ppp0.1 | pppoe_0_8_40 | PPPoE | N/A | N/A | Abilitato | Abilitato | Abilitato | Disabilitato | Disabilitato | <input type="checkbox"/> | <input type="button" value="Modifica"/> |

Figura 4-14

- **Elimina tutto:** Fare clic per eliminare tutte le interfacce.
- **Elimina:** Selezionare le interfacce da rimuovere e fare clic per eliminarle.

4.4.2.2 ATM-EoA-IPoE

Se il provider ISP prescrive **IPoE** come metodo di connessione.

1. Aggiungere una nuova interfaccia ATM e selezionare **EoA** in [4.4.1.1 Interfaccia ATM](#).
2. Fare clic su **Aggiungi** come in Figura 4-7 per mostrare la schermata in Figura 4-8. Fare clic su **Avanti**.
3. Selezionare IPoE in Figura 4-9, inserire una breve descrizione e fare clic su **Avanti**.
4. Specificare i parametri richiesti e fare clic su **Avanti**.

Configurazione IP WAN

Specificare i parametri d'indirizzamento WAN forniti dal provider ISP.
 Attenzione: Selezionando "Ottieni indirizzo IP automaticamente" sarà abilitato DHCP per i PVC in modalità IPoE.
 Se "Utilizza il seguente indirizzo IP statico" è selezionato è necessario specificare manualmente i parametri.

Ottieni indirizzo IP automaticamente

Opzione 60 Vendor ID:

Opzione 61 IAID: (8 cifre esadecimali)

Opzione 61 DUID: (esadecimale)

Opzione 125: Disabilita Abilita

Utilizza il seguente indirizzo IP statico:

Indirizzo IP WAN:

Subnet mask WAN:

Gateway:

MTU (bytes): (opzionale)

Figura 4-15

- **Ottieni indirizzo IP automaticamente:** Selezionare se il provider utilizza un server DHCP per la configurazione dell'indirizzamento.

Nota:

Se il router opera come client DHCP deve identificarsi in option 61 (client-identifier) in tutti i messaggi DHCP e DUID/IAID è parte dell'opzione 61.

- **Opzione 60 Vendor ID:** Opzione che identifica la classe Vendor.
- **Opzione 61 IAID:** IAID (Identity Association ID) assegna un Identity Association ID ad interfacce individuali. Se il dispositivo funziona con un singolo DHCP occorre utilizzare il

valore 1 per IAID in tutte le interazioni DHCP. Se sono in uso DHCP multipli è possibile utilizzare valori superiori per ogni oggetto della connessione.

- **Opzione 61 DUID:** Seleziona l'interfaccia con l'indirizzo link-layer da usare come DUID (DHCP Unique Identifier).
 - **Opzione 125:** L'opzione 125 permette la configurazione del server DHCP con una policy per la gestione delle classi senza che il server debba analizzare il formato utilizzato nell'opzione client-identifier.
- **Utilizza il seguente indirizzo IP statico:** Specificare i parametri d'indirizzamento se forniti dal provider ISP.
5. È possibile abilitare **NAT**, **Firewall** ed **IGMP Multicast**, fare quindi click su **Avanti**.

Figura 4-16

- **Abilita NAT:** Selezionare per utilizzare la mappatura degli indirizzi LAN su un unico indirizzo WAN.
- **Abilita firewall:** Il firewall SPI blocca le connessioni in ingresso incrementando la sicurezza.
- **Abilita IGMP multicast:** Si consiglia di abilitare l'opzione.

Nota:

Selezionando **Abilita NAT** apparirà il menu **NAT** utilizzabile come descritto in [4.4.5 NAT](#).

6. Selezionare l'interfaccia WAN predefinita per il gateway predefinito e fare clic su **Avanti**.

Figura 4-17

7. Configurare i server DNS e fare clic su **Avanti**.

Configurazione server DNS

Selezionare un'interfaccia per il server DNS o configurare manualmente l'indirizzo IP del server. In modalità ATM l'indirizzo IP deve essere configurato solo se è presente un solo PVC in modalità IPoE od IPoA.
 Possono coesistere più **interfacce server DNS**, sarà utilizzata l'interfaccia disponibile con maggiore priorità. La priorità può essere variata rimuovendo e ricreando le interfacce.

Selezionare le interfacce per il server DNS tra le interfacce WAN disponibili:

Selezione interfacce server DNS

atm0.2
ppp0.1

Interfacce disponibili

Utilizza il seguente server DNS:

Server DNS primario:

Server DNS secondario:

Figura 4-18

Nota:

Se è configurato un solo PVC in modalità IPoA è necessario specificare gli indirizzi.

8. Verificare la correttezza delle informazioni e fare clic su **Salva/Applica** per applicarle.

Configurazione WAN - Sommario

Assicurarsi che i parametri coincidano con quelli forniti dal provider ISP.

| | |
|--------------------------|--------------|
| Tipo connessione: | IPoE |
| NAT: | Abilitato |
| NAT fullcone: | Disabilitato |
| Firewall: | Disabilitato |
| IGMP multicast: | Abilitato |
| QoS: | Abilitato |

Fare clic su "Salva/Applica" per attivare l'interfaccia o su "Indietro" per modificarla.

Figura 4-19

4.4.2.3 ATM-EoA-Bridging

Per creare connessioni **Bridge** occorre creare un'interfaccia ATM.

1. Aggiungere una nuova interfaccia ATM e selezionare **EoA** in [4.4.1.1 Interfaccia ATM](#).
2. Fare clic su **Aggiungi** come in Figura 4-7 per mostrare la schermata in Figura 4-8. Fare clic su **Avanti**.
3. Selezionare Bridge in Figura 4-9, inserire una breve descrizione e fare clic su **Avanti**.
4. Specificare i parametri richiesti e fare clic su **Avanti**.

4.4.2.4 ATM-PPPoA

Se il provider prescrive una connettività **PPPoA** occorre utilizzare un'interfaccia ATM.

1. Aggiungere una nuova interfaccia ATM e selezionare **EoA** in [4.4.1.1 Interfaccia ATM](#).

2. Fare clic su **Aggiungi** come in Figura 4-7 e procedere come da [4.4.2.1 ATM-EoA-PPPoE](#).

4.4.2.5 ATM-IPoA

Se il provider prescrive una connettività **IPoA** occorre utilizzare un'interfaccia ATM.

1. Aggiungere una nuova interfaccia ATM e selezionare **EoA** in [4.4.1.1 Interfaccia ATM](#).
2. Fare clic su **Aggiungi** come in Figura 4-7 e procedere come da [4.4.2.2 ATM-EoA-IPoE](#).

Nota:

Non possono coesistere connessioni ETH ed ATM.

4.4.2.6 ETH-PPPoE

Se il provider ISP prescrive **PPPoE** come metodo di connessione:

1. Aggiungere una nuova interfaccia ETH come in [4.4.1.2 Interfaccia ETH](#).
2. Fare clic su **Aggiungi** come in Figura 4-7 e configurare come descritto in [4.4.2.1 ATM-EoA-PPPoE](#).

4.4.2.7 ETH-IPoE

Se il provider ISP prescrive **IPoE** come metodo di connessione.

1. Aggiungere una nuova interfaccia ETH in [4.4.1.2 Interfaccia ETH](#).
2. Fare clic su **Aggiungi** come in Figura 4-7 e configurare come descritto in [4.4.2.2 ATM-EoA-IPoE](#).

4.4.2.8 ETH-Bridge

Per creare connessioni bridge occorre utilizzare un'interfaccia ETH.

1. Aggiungere una nuova interfaccia ETH in [4.4.1.2 Interfaccia ETH](#).
2. Fare clic su **Aggiungi** come in Figura 4-7 e configurare come descritto in [4.4.2.3 ATM-EoA-Bridging](#).

4.4.3 MAC Clone

Selezionare “**Configurazione avanzata**” → “**MAC Clone**” per gestire gli indirizzi MAC da clonare.

La schermata elenca le interfacce configurate in [4.4.1 Interfaccia layer 2](#) col relativo indirizzo MAC predefinito. Se non è ancora stata configurata la connessione WAN per un'interfaccia in [4.4.2 WAN](#), il campo MAC mostrerà “Need a corresponding WAN Service (Occorre una connessione WAN corrispondente)”.

L'ultimo indirizzo mostrato corrisponde all'indirizzo del dispositivo in uso.

MAC address clone

Configurare l'indirizzo MAC per il servizio WAN selezionato.

| | | |
|---------------------------------|-------------------|------------------------|
| Clona indirizzo MAC per ppp0.1: | Non configurato | Ripristino Predefinita |
| MAC dispositivo in uso: | 94:de:80:b4:d0:51 | Clona su ppp0.1 |

Nota: MAC address clone è disponibile solo sulle interfacce WAN e gli indirizzi MAC specificati devono essere differenti.

Figura 4-20

Modificare l'indirizzo MAC specificato se necessario, selezionare l'interfaccia e fare clic su **Clona** per copiarlo.

Fare clic su **Ripristino Predefinita** per ripristinare l'indirizzo originale.

 **Nota:**

Tutti gli indirizzi MAC devono essere univoci.

4.4.4 LAN

Selezionare “**Configurazione avanzata**” → “**LAN**” per visualizzare la schermata in Figura 4-21.

Configurazione LAN

Configurare l'indirizzo IP LAN e la relativa subnet mask. GroupName

Indirizzo IP:
 Subnet Mask:

Abilita IGMP snooping

- Modalità standard
- Modalità blocking

Disabilita server DHCP

Abilita server DHCP

Indirizzo IP iniziale:
 Indirizzo IP finale:
 Leased Time (ore): (1~48)

Lista riserve statiche (possono essere configurate fino a 32 riserve statiche):

| Indirizzo MAC | Indirizzo IP | Stato | Abilita/Disabilita | Modifica | Elimina |
|--|--------------|-------|--------------------|----------|---------|
| <input type="button" value="Aggiungi"/> <input type="button" value="Abilita Tutto"/> <input type="button" value="Seleziona Tutto"/> <input type="button" value="Elimina"/> | | | | | |

Abilita relay DHCP

Indirizzo IP server DHCP:

Nota: Occorre disabilitare il NAT sulle connessioni WAN per utilizzare il relay DHCP.

Configurare il secondo indirizzo IP e la subnet mask per l'interfaccia LAN

Figura 4-21

- **Indirizzo IP / Subnet Mask:** Configurare indirizzo IP e Subnet Mask dell'interfaccia LAN.
- **Abilita IGMP Snooping:** Abilitando questa opzione è necessario selezionare la modalità standard o bloccante.
- **Disabilita server DHCP:** È possibile configurare un indirizzo LAN secondario attraverso il quale raggiungere la web console.

- **Abilita server DHCP:** Dynamic Host Configuration Protocol è il sistema di assegnamento automatico dell'indirizzo IP per i dispositivi collegati ed è abilitato di default.
 - **Indirizzo IP iniziale:** Inserire il primo indirizzo del range assegnabile automaticamente. Con indirizzo IP predefinito del router **192.168.1.100** e subnet mask predefinita **255.255.255.0** è assegnabile l'intervallo **192.168.1.100 – 192.168.1.200**.
 - **Indirizzo IP finale:** Inserire l'ultimo indirizzo del range assegnabile automaticamente. Con indirizzo IP predefinito del router **192.168.1.100** e subnet mask predefinita **255.255.255.0** è assegnabile l'intervallo **192.168.1.100 – 192.168.1.200**.
 - **Leased Time(ore):** È la durata degli indirizzi assegnati, normalmente **24** ore. Al termine dell'intervallo di tempo l'IP assegnato viene liberato ed è eventualmente necessario un nuovo assegnamento automatico.
- **Lease statiche:** Fare clic su **Aggiungi** in Figura 4-21, per forzare un abbinamento MAC / IP sul server DHCP.

Lease DHCP statica

Specificare indirizzo MAC ed indirizzo IP, quindi fare clic su "Salva/Applica".

Indirizzo MAC:
 Indirizzo IP:

Figura 4-22

- **Indirizzo MAC:** Specificare l'indirizzo MAC del dispositivo.
- **Indirizzo IP:** Specificare l'IP da assegnare.

4.4.4.1 LAN IPv6

Selezionare **“Configurazione avanzata”** → **“LAN”** → **“Configurazione LAN IPV6”** per visualizzare la schermata in Figura 4-23.

Configurazione automatica LAN IPv6

Nota: Stateful DHCPv6 è supportato con lunghezza prefisso inferiore a 64. L'ID interfaccia non supporta la ZERO COMPRESSION "...". Specificare l'indirizzo completo. Esempio: Inserire "0:0:0:2" anzichè "::2".

Configurazione statica LAN IPv6
 Indirizzo interfaccia (lunghezza prefisso richiesta):

Applicazioni LAN IPv6

Abilita server DHCPv6

Stateless
 Stateful

ID interfaccia iniziale:
 ID interfaccia finale:
 Leased Time (ore):

Abilita RADVD

Abilita notifica prefisso ULA Prefix Advertisement

Casuale
 Configurazione statica

Prefisso:
 Preferred Life Time (ora):
 Valid Life Time (ora):

Figura 4-23

- **Indirizzo interfaccia (lunghezza prefisso richiesta):** Indirizzo e prefisso dell'interfaccia.
- **Applicazioni LAN IPv6:** Scegliere il metodo di assegnamento degli indirizzi.

For Server DHCPv6:

- 1) **Stateless** non necessita di configurazione.
- 2) **Stateful** richiede i seguenti parametri.
 - **ID interfaccia iniziale:** Inserire il primo indirizzo del range assegnabile automaticamente.
 - **ID interfaccia finale:** Inserire l'ultimo indirizzo del range assegnabile automaticamente.
 - **Leased Time(ore):** È la durata degli indirizzi assegnati, normalmente **24** ore. Al termine dell'intervallo di tempo l'IP assegnato viene liberato ed è eventualmente necessario un nuovo assegnamento automatico.

Applicazioni LAN IPv6

Abilita server DHCPv6

Stateless
 Stateful

ID interfaccia iniziale:
 ID interfaccia finale:
 Leased Time (ore):

For RADVD:

- 1) **Casuale** non necessita di configurazione.
- 2) **Configurazione statica** richiede i seguenti parametri.

- **Prefisso:** Specificare un prefisso.

Fare clic su **Salva/Applica** per applicare la configurazione.

4.4.5 NAT

NAT (Network Address Translation) permette di condividere un indirizzo WAN tra molteplici indirizzi LAN.

Nota:

Con connessioni **PPPoA** o **PPPoE** o selezionando **Abilita NAT** con connessioni **IPoA** ed **IPoE (4.4.2 WAN)** è possibile visualizzare la schermata in Figura 4-24.

Selezionare **“Configurazione avanzata”** → **“NAT”**, quindi **Virtual Server**, **Port Triggering**, **Host DMZ** od **ALG** per visualizzare le relative impostazioni.

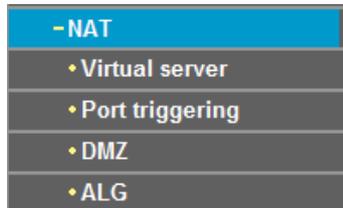


Figura 4-24

4.4.5.1 Virtual Server

Selezionare **“Configurazione avanzata”** → **“NAT”** → **“Virtual server”** per visualizzare la schermata in Figura 4-25.

I server virtuali consentono di inoltrare una connessione proveniente da Internet su una specifica porta applicativa verso un dispositivo connesso alla rete LAN specificandone l'indirizzo IP. I dispositivi verso i quali sono configurati dei server virtuali devono avere indirizzo IP statico od indirizzo IP con riserva DHCP.

Figura 4-25

- **Tabella virtual server:** La tabella elenca i server configurati.
 - **Nome server:** Nome identificativo del server.
 - **Porta esterna iniziale:** Prima porta esterna inoltrata.
 - **Porta esterna finale:** Ultima porta esterna inoltrata.
 - **Protocollo:** Protocolli inoltrati.
 - **Porta interna iniziale:** Prima porta interna alla quale inoltrare.
 - **Porta interna finale:** Ultima porta interna alla quale inoltrare.
 - **Indirizzo IP:** Indirizzo del dispositivo a cui inoltrare le connessioni.
 - **Interfaccia WAN:** Interfaccia WAN ascoltata.
- **Aggiungi:** Fare clic per aggiungere un server.
- **Elimina:** Selezionare i server da rimuovere e fare clic per eliminarli.

Per aggiungere un virtual server:

1. Fare clic su **Aggiungi** come in Figura 4-25 per visualizzare la schermata in Figura 4-26.

NAT -- Virtual server

Specificare un'applicazione standard o personalizzata, l'indirizzo IP di destinazione e fare clic su "Salva/Applica" per inoltrare il traffico relativo all'applicazione all'indirizzo IP specificato.
 NOTA: La porta finale interna viene calcolata automaticamente.
 Possono essere configurati ancora 32 virtual server.

Interfaccia:

Nome applicazione:

Select a Service:

Applicazione personalizzata:

Indirizzo IP:

| Porta esterna iniziale | Porta esterna finale | Protocollo | Porta interna iniziale | Porta interna finale |
|------------------------|----------------------|------------|------------------------|----------------------|
| | | TCP | | |

Figura 4-26

2. Selezionare l'interfaccia da configurare.
3. Selezionare il servizio da supportare o creare un nuovo servizio.
4. Specificare l'IP di destinazione.
5. Specificare le porte ed i protocolli.
6. Fare clic su **Salva/Applica** per abilitare il server.

4.4.5.2 Port triggering

Selezionare “**Configurazione avanzata**” → “**NAT**” → “**Port Triggering**” per visualizzare la schermata in Figura 4-27.

Alcune applicazioni come giochi on-line, video conferencing, telefonia Internet richiedono connessioni su porte multiple. Port Triggering è utilizzato per permettere a queste applicazioni di lavorare attraverso router NAT.

NAT -- Configurazione port triggering

Alcune applicazioni richiedono l'inoltro di alcune porte. Questa funzione consente di inoltrare le porte designate quando l'applicazione è attiva. Selezionare un'applicazione o definirne una nuova e fare clic su "Salva/Applica" per aggiungerne. È possibile configurare un massimo di 32 porte.

| Nome applicazione | Trigger | | | | Aperta | | | Interfaccia WAN | Stato | Abilita/Disabilita | Modifica | Elimina |
|-------------------|------------|-------------|--------|------------|-------------|--------|--|-----------------|-------|--------------------|----------|---------|
| | Protocollo | Range porte | | Protocollo | Range porte | | | | | | | |
| | | Iniziale | Finale | | Iniziale | Finale | | | | | | |
| | | | | | | | | | | | | |

Figura 4-27

- **Port triggering:** Tabella dei trigger programmati.
 - **Nome applicazione:** Nome della regola.
 - **Trigger:** Protocolli e range porte trigger.
 - **Aperta:** Protocolli e range porte aperte.
 - **Interfaccia WAN:** Interfaccia di trigger.
- **Aggiungi:** Fare clic per aggiungere una regola.
- **Elimina:** Selezionare le regole da rimuovere e fare clic per eliminarle.

Per aggiungere una regola:

1. Fare clic su **Aggiungi** come in Figura 4-27 per visualizzare la schermata in Figura 4-28.

NAT -- Port triggering

Alcune applicazioni richiedono l'inoltro di alcune porte. Questa funzione consente di inoltrare le porte designate quando l'applicazione è attiva. Selezionare un'applicazione o definirne una nuova e fare clic su "Salva/Applica" per aggiungerne.

Possono essere configurate ancora 32 entrate.

Interfaccia:

Nome applicazione:

Selezionare un'applicazione:

Applicazione personalizzata:

| Porta trigger iniziale | Porta trigger finale | Protocollo trigger | Porta aperta iniziale | Porta aperta finale | Protocollo aperto |
|------------------------|----------------------|--------------------|-----------------------|---------------------|-------------------|
| | | TCP ▾ | | | TCP ▾ |
| | | TCP ▾ | | | TCP ▾ |
| | | TCP ▾ | | | TCP ▾ |
| | | TCP ▾ | | | TCP ▾ |
| | | TCP ▾ | | | TCP ▾ |
| | | TCP ▾ | | | TCP ▾ |
| | | TCP ▾ | | | TCP ▾ |
| | | TCP ▾ | | | TCP ▾ |
| | | TCP ▾ | | | TCP ▾ |

Figura 4-28

2. Selezionare l'applicazione dalla lista o selezionare **Applicazione personalizzata** e specificarne il nome.
3. Specificare porte e protocolli.
4. Fare clic su **Salva/Applica** per salvare la regola.

4.4.5.3 Host DMZ

Selezionare "Configurazione avanzata" → "NAT" → "Host DMZ" per visualizzare la schermata in Figura 4-29.

Tutte le connessioni da WAN saranno inoltrate all'host indicato.

NAT -- Host DMZ

Il modem/router inoltrerà tutte le connessioni provenienti dalla WAN al dispositivo configurato come host DMZ.

Specificare l'IP del dispositivo e fare clic su 'Salva/Applica' per salvare le impostazioni.

Cancellare l'indirizzo e fare clic su 'Salva/Applica' per disattivare DMZ.

Indirizzo IP host DMZ:

Figura 4-29

Per impostare un host DMZ:

Specificare l'IP e fare clic su **Salva/Applica**.

 **Nota:**

L'host DMZ deve avere IP statico.

4.4.5.4 ALG

Selezionare **“Configurazione avanzata”** → **“NAT”** → **“ALG”** per visualizzare la schermata in Figura 4-29.

Figura 4-30

Fare clic su **Salva/Applica** per salvare le impostazioni.

4.4.6 Sicurezza

Selezionare **“Configurazione avanzata”** → **“Sicurezza”** per visualizzare le schermate relative a **Filtro IP** e **Filtro MAC** (solo modalità bridge) tramite la voce corrispondente del menu.

| Nome filtro | Versione IP | Protocollo | SrcIP/ LunghPref | SrcPort | DstIP/ LunghPref | DstPort | Elimina |
|--|-------------|------------|------------------|---------|------------------|---------|---------|
| <input type="button" value="Aggiungi"/> <input type="button" value="Elimina"/> | | | | | | | |

Figura 4-31

4.4.6.1 Filtro IP

Filtro IP – In uscita:

Selezionare **“Configurazione avanzata”** → **“Sicurezza”** → **“Filtro IP”**.

È possibile bloccare il traffico verso alcuni indirizzi IP.

| Nome filtro | Versione IP | Protocollo | SrcIP/ LunghPref | SrcPort | DstIP/ LunghPref | DstPort | Elimina |
|--|-------------|------------|------------------|---------|------------------|---------|---------|
| <input type="button" value="Aggiungi"/> <input type="button" value="Elimina"/> | | | | | | | |

Figura 4-32

Per aggiungere una regola:

1. Fare clic su **Aggiungi** in Figura 4-32 per visualizzare la schermata in Figura 4-33.

Aggiungi filtro IP -- In uscita

La schermata consente la creazione di un filtro IP per regolamentare il traffico in uscita. Il filtro è applicato se tutte le condizioni sono soddisfatte. Fare clic su 'Salva/Applica' per attivare il filtro.

Nome filtro:

Versione IP: IPv4

Protocol:

Indirizzo IP sorgente (lunghezza prefisso):

Porta sorgente (porta o porta:porta):

Indirizzo IP destinazione (lunghezza prefisso):

Porta destinazione (porta o porta:porta):

Figura 4-33

2. Specificare un nome per il filtro.
3. Specificare il protocollo.
4. Specificare un **Indirizzo IP sorgente** ed un range **Porta sorgente** (porta o porta:porta).
5. Enter a **Indirizzo IP destinazione** ed un range **Porta destinazione** (porta o porta:porta).
6. Fare clic su **Salva/Applica** per salvare le impostazioni.

Nota:

Le condizioni non specificate non limitano l'applicazione della regola; è necessario specificare almeno una condizione.

4.4.6.2 Filtro MAC

Selezionare **“Configurazione avanzata”** → **“Sicurezza”** → **“Filtro MAC”** per visualizzare la schermata in Figura 4-34.

Nota:

Il filtro MAC è utilizzabile solo con PVS ATM in modalità bridge.

Configurazione MAC filtering

MAC filtering è attivo solo su PVC ATM PVC in modalità bridge. **FORWARDED** indica che verranno inoltrati tutti i frame ad eccezione di quelli descritti dalle regole. **BLOCKED** indica che verranno bloccati tutti i frame ad eccezioni di quelli descritti dalle regole.

Policy MAC filtering per tutte le interfacce:
ATTENZIONE: Il cambio di policy cancella tutte le regole.

| Interfaccia | Policy | Cambio |
|-------------|-----------|--------------------------|
| atm0.2 | FORWARDED | <input type="checkbox"/> |

Scegli Aggiungi o Elimina per configurare le MAC filtering rule. Possono essere configurati al massimo 36 filtri MAC

| Interfaccia | Protocollo | MAC di destinazione | MAC Sorgente | Elimina |
|-------------|------------|---------------------|--------------|---------|
| | | | | |

Figura 4-34

- **Cambio policy:** Sono disponibili **INOLTRA** e **BLOCCA**. **FORWARDED (INOLTRA)** inoltra tutti i frame ad eccezione di quelli specificati, **BLOCCA** blocca tutti i frame ad eccezione di

quelli specificati. Selezionare **Cambia** e fare clic su **Cambia policy** per cambiare il comportamento sulle interfacce selezionate.

- **Aggiungi:** Fare clic su **Aggiungi** e specificare un indirizzo MAC.
- **Elimina:** Selezionare le regole da rimuovere e fare clic su **Elimina** per cancellarle.

Per aggiungere una regola procedere come segue.

1. Fare clic su **Aggiungi** in Figura 4-34.

Figura 4-35

2. Selezionare il **Protocollo**.
3. Specificare **Indirizzo MAC destinazione** ed **Indirizzo MAC sorgente**.
4. Selezionare la **Direzione**.
5. Selezionare le **Interfacce WAN**.
6. Fare clic su **Salva/Applica** per salvare le impostazioni.

4.4.7 Parental Control

Selezionare **“Configurazione avanzata”** → **“Parental Control”**. La funzionalità consente la limitazione dei contenuti a soggetti sensibili (es. minori).

Figura 4-36

4.4.7.1 Orario

È possibile limitare l'orario consentito per la navigazione a specifici dispositivi.

Restrizione temporale accesso

È possibile configurare un massimo di 16 entries can be configured.

| Nome utente | MAC | Giorni | | | | | | | Ora | | Stato | Abilita/Disabilita | Modifica | Elimina |
|-------------|-------------------|--------|-----|-----|-----|-----|-----|-----|--------|-------|-----------|---|---|--------------------------|
| | | Lun | Mar | Mer | Gio | Ven | Sab | Dom | Inizio | Fine | | | | |
| child-1 | 94:de:80:b4:d0:51 | x | x | x | x | x | | | 18:00 | 21:00 | Abilitato | <input type="button" value="Disabilita"/> | <input type="button" value="Modifica"/> | <input type="checkbox"/> |

Figura 4-37

Per aggiungere una regola:

1. Fare clic su **Aggiungi** come in Figura 4-37 per visualizzare la schermata in Figura 4-38.

Restrizione temporale accesso

La sezione permette di aggiungere restrizioni a dispositivi in LAN. "Indirizzo MAC in uso" mostra l'indirizzo MAC del dispositivo dal quale si sta accedendo la console. Per applicare una restrizione ad un altro dispositivo selezionare "Altro indirizzo MAC" e specificarlo. Per verificare il MAC di un computer windows digitare ipconfig /all in una finestra prompt comandi.

Nome utente:

Indirizzo MAC in uso:

Altro Indirizzo MAC (xx:xx:xx:xx:xx:xx):

| Giorni: | Lun | Mar | Mer | Gio | Ven | Sab | Dom |
|--------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Selezionare: | <input type="checkbox"/> |

Inizio periodo blocco (hh:mm):

Fine periodo blocco (hh:mm):

Figura 4-38

2. Specificare il **Nome utente** del dispositivo da limitare.
3. Specificare l'indirizzo MAC del dispositivo o selezionare **Indirizzo MAC dispositivo in uso** per impostare il MAC del dispositivo dal quale si visualizza la console.
4. Specificare i giorni effettivi.
5. Specificare un **Orario di inizio** ed un **Orario di fine** per il periodo effettivo.
6. Fare clic su **Salva/Applica** per salvare le impostazioni.

Nota:

Configurare innanzitutto l'orologio di sistema in "**Strumenti** → **Orologio**".

4.4.7.2 Filtro URL

Il filtro consente di regolamentare gli URL raggiungibili da alcuni dispositivi.

Figura 4-39

Sono disponibili 3 modalità.

- **Disabilita:** Il filtro non è operativo.
- **Abilita:** URL elencati consentiti.
- **Nega:** URL elencati non consentiti.

Per aggiungere un filtro:

1. Selezionare la modalità (l'esempio illustra la modalità Nega).
2. Fare clic su **Aggiungi** in Figura 4-39, quindi specificare indirizzi LAN, porta ed URL.

Figura 4-40

3. Fare clic su **Salva/Applica** per salvare le impostazioni.

4.4.8 QoS

Selezionare “**Configurazione avanzata**” → “**QoS**” per regolamentare la priorità di traffico per le varie applicazioni.

Figura 4-41

Selezionare **Abilita QoS** per abilitare la funzionalità.

Selezionare un **Mark DSCP predefinito** per specificare la priorità da applicare ai pacchetti non categorizzati.

Fare clic su **Salva/Applica** per salvare la configurazione.

 **Nota:**

Il Mark DSCP predefinito è utilizzato per classificare il traffico non definito da alcuna regola.

4.4.8.1 Coda

Selezionare **“Configurazione avanzata”** → **“QoS”** → **“Coda”**.

Configurazione coda QoS

In modalità ATM possono essere configurate fino a 8 code.
 In modalità PTM possono essere configurate fino a 8 code.
 Possono essere configurate fino a 4 code per interfaccia Ethernet.
 Possono essere configurate fino a 4 code per interfaccia WAN.
 Fare clic su **Aggiungi** per creare una coda.

Per rimuovere delle code selezionare la checkbox di rimozione e fare clic su **Elimina**.
 Il pulsante **Abilita** eseguirà una scansione di tutte le regole. Saranno abilitate le regole selezionate e non saranno abilitate le regole non selezionate.
 La casella di controllo mostra inoltre lo stato di abilitazione dopo l'aggiornamento della pagina.
 Disabilitando WMM la classificazione non potrà essere applicata all'interfaccia wireless.

| Nome | Chiave | Interfaccia | QID | Prec/Alg/Wght | Latenza DSL | Priorità PTM | Bitrate min (bps) | Bitrate max (bps) | Burst Size(byte) | Abilita | Elimina |
|--------------------|--------|-------------|-----|---------------|-------------|--------------|-------------------|-------------------|------------------|-------------------------------------|--------------------------|
| WMM Voice Priority | 1 | wl0 | 1 | 1/SP | | | | | | <input type="checkbox"/> | <input type="checkbox"/> |
| WMM Voice Priority | 2 | wl0 | 2 | 2/SP | | | | | | <input type="checkbox"/> | <input type="checkbox"/> |
| WMM Video Priority | 3 | wl0 | 3 | 3/SP | | | | | | <input type="checkbox"/> | <input type="checkbox"/> |
| WMM Video Priority | 4 | wl0 | 4 | 4/SP | | | | | | <input type="checkbox"/> | <input type="checkbox"/> |
| WMM Best Effort | 5 | wl0 | 5 | 5/SP | | | | | | <input type="checkbox"/> | <input type="checkbox"/> |
| WMM Background | 6 | wl0 | 6 | 6/SP | | | | | | <input type="checkbox"/> | <input type="checkbox"/> |
| WMM Background | 7 | wl0 | 7 | 7/SP | | | | | | <input type="checkbox"/> | <input type="checkbox"/> |
| WMM Best Effort | 8 | wl0 | 8 | 8/SP | | | | | | <input type="checkbox"/> | <input type="checkbox"/> |
| Default Queue | 37 | atm0 | 1 | 8/WRR/1 | Path0 | | | | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| TCP ACK Queue | 38 | atm0 | 2 | 7/WRR/1 | Path0 | | | | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Figura 4-42

Fare clic su **Aggiungi** in Figura 4-42 per visualizzare la schermata in Figura 4-43.

Configurazione coda QoS

Questa schermata permette la configurazione di una coda QoS e l'assegnamento di un'interfaccia layer 2.

Nome:

Abilita:

Interfaccia:

Precedenza coda: (minimo valore, massima priorità)
 - La lista precedenze mostra l'algoritmo di schedulazione per ogni livello di precedenza.
 - Code con equal precedenza saranno schedulate secondo l'algoritmo.
 - Code con diversa precedenza saranno schedulate mediante SP.

Algoritmo schedulazione

Round robin pesato
 Fair queuing pesato

Peso coda: [1-63]

Latenza DSL:

Figura 4-43

- **Nome:** Nome della regola.
- **Abilità:** Controllo di abilitazione della regola.
- **Interfaccia:** Interfaccia sulla quale la regola è attiva.
- **Peso coda:** Priorità QoS della coda.
- **Latenza DSL:** È disponibile solo Path0.

Fare clic su **Salva/Applica** per applicare le impostazioni.

Nota:

1. Valori minori indicano priorità maggiori.
2. La coda è utilizzata per la classificazione del traffico in ingresso.

4.4.8.2 Classificazione

La sezione permette la classificazione del traffico in upstream, l’assegnazione di code e priorità, ed opzionalmente la sovrascrittura dell’header IP DSCP.

Configurazione classificazione QoS -- Possono essere configurate fino a 32 regole.

Per aggiungere una regola fare clic su **Aggiungi**.
 Per rimuovere delle code selezionare la checkbox di rimozione e fare clic su **Elimina**.
 Il pulsante **Abilita** eseguirà una scansione di tutte le regole. Saranno abilitate le regole selezionate e non saranno abilitate le regole non selezionate.
 La casella di controllo mostra inoltre lo stato di abilitazione dopo l’aggiornamento della pagina.
 Disabilitando WMM la classificazione non potrà essere applicata all’interfaccia wireless.

| Nome classe | Ordinamento | CRITERIO CLASSIFICAZIONE | | | | | | | | | | | | | RISULTATO |
|---|-------------|--------------------------|------------|--------------|--------------|------------------|------------------|------------|---------|---------|------------|--------------|-------------|------|-----------|
| | | Class Intf | Tipo Ether | SrcMAC/ Mask | DstMAC/ Mask | SrcIP/ LunghPref | DstIP/ LunghPref | Protocollo | SrcPort | DstPort | DSCP Check | 802.1P Check | Chiave coda | Mark | |
| <input type="button" value="Aggiungi"/> <input type="button" value="Abilita"/> <input type="button" value="Elimina"/> | | | | | | | | | | | | | | | |

Figura 4-44

Fare clic su **Aggiungi** in Figura 4-44.

Aggiunta regola di traffico

Questa schermata consente la creazione di una regola per classificare il traffico in ingresso in code con priorità e marcarlo opzionalmente tramite DSCP o priorità Ethernet. Fare clic su 'Salva/Applica' per attivare la regola.

Nome classe:

Indice regola:

Stato regola:

Critero di classificazione (un eventuale criterio nullo sarà ignorato)

Interfaccia della classe:

Tipo Ether:

Indirizzo MAC sorgente:

Maschera MAC sorgente:

Indirizzo MAC destinazione:

Maschera MAC destinazione:

Risultato classificazione (un eventuale valore nullo sarà ignorato).

Coda classe (richiesto):

Mark DSCP (Differentiated Service Code Point):

Mark priorità 802.1p:

I pacchetti in egress di classe non-vlan indirizzati ad un'interfaccia non-vlan saranno taggati con VID 0 e p-bit della classe.
 I pacchetti in egress di classe vlan indirizzati ad un'interfaccia non-vlan non saranno taggati e verrà aggiornato il p-bit col p-bit della classe.
 I pacchetti in egress di classe non-vlan indirizzati ad un'interfaccia vlan saranno taggati con VID dell'interfaccia e sarà aggiornato il p-bit.
 I pacchetti in egress di classe vlan indirizzati ad un'interfaccia vlan saranno taggati con VID aggiuntivo del pacchetto e sarà aggiornato il p-bit.

Figura 4-45

Specificare le condizioni e la classificazione, quindi fare clic su **Salva/Applica**.

4.4.9 Bandwidth Control

Selezionare **“Configurazione avanzata”** → **“Bandwidth Control”** per impostare il controllo di banda.

Bandwidth control

Questa schermata permette l'abilitazione della funzionalità di bandwidth control. Fare clic su "Salva/Applica" per applicare la configurazione.

Nota:
 Le regole bandwidth control non sono abilitate se la funzionalità non è abilitata.
 Assicurarsi che la banda totale sia configurata correttamente.

Abilita bandwidth control

Tipo linea: ADSL Altro

Banda totale in upstream: Kbps

Banda totale in downstream: Kbps

Figura 4-46

- **Abilita bandwidth control:** Controllo di abilitazione della funzionalità.
- **Tipo linea:** Tipo di linea in uso.
- **Banda totale in upstream (kbps):** Banda disponibile in upstream.

- **Banda totale in downstream (kbps):** Banda disponibile in downstream.

Fare clic su **Salva/Applica** per applicare le impostazioni.

4.4.9.1 Regole

Selezionare “**Configurazione avanzata**” → “**Bandwidth Control**” → “**Lista regole**” per visualizzare la schermata in Figura 4-47.

Lista regole bandwidth control

La schermata mostra le regole di bandwidth control. È possibile configurare un massimo di 16 regole.
Se la banda *massima* non è configurata o è maggiore della banda totale sarà applicata la banda totale.
Assicurarsi che la banda *minima* sia inferiore alla banda totale.

| Descrizione | priorità | Upstream Bandwidth (Kbps) | | Downstream Bandwidth (Kbps) | | Stato | Modifica | |
|-------------|----------|---------------------------|-----|-----------------------------|-----|-------|----------|--|
| | | Min | Max | Min | Max | | | |
| | | | | | | | | |

Figura 4-47

Per aggiungere una regola fare clic su **Aggiungi** in Figura 4-48.

Configurazione regola bandwidth control

La schermata permette la creazione di una regola bandwidth control e l'assegnazione di una priorità.
Fare clic su "Salva/Applica" per salvare la regola.

Stato: Abilita Disabilita

Range IP: -

Range porte: -

Protocollo:

priorità:

| | | | |
|-------------|----------------------|------------------------|------|
| | Rate minimo | Rate massimo | |
| Upstream: | <input type="text"/> | - <input type="text"/> | Kbps |
| Downstream: | <input type="text"/> | - <input type="text"/> | Kbps |

Figura 4-48

- **Stato:** Stato di abilitazione della regola.
- **Range IP:** Range IP regolato.
- **Range porte:** Range porte regolate.
- **Protocollo:** Protocolli regolati.
- **Priorità:** Priorità applicata.
- **Upstream:** Specificare i limiti di banda in upstream.
- **Downstream:** Specificare i limiti di banda in downstream.

Fare clic su **Salva/Applica** per applicare le impostazioni.

Fare eventualmente clic su **Modifica** o **Elimina** per gestire le regole selezionate.

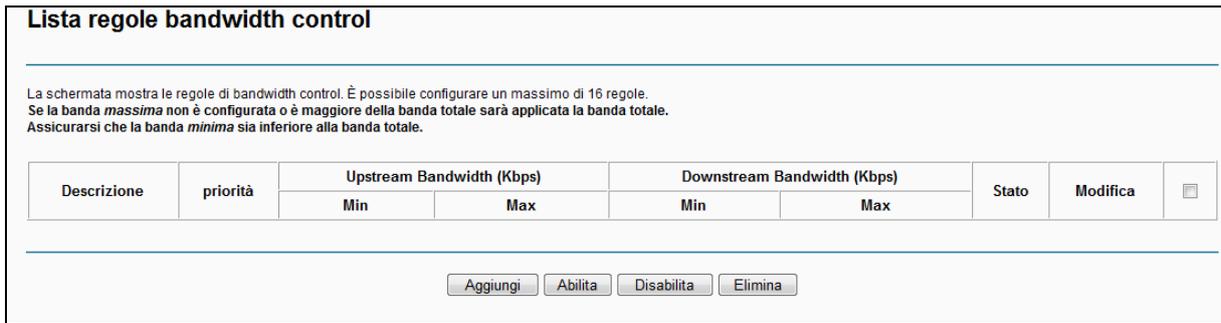


Figura 4-49

4.4.10 Routing

Selezionare “Configurazione avanzata” → “Routing”.

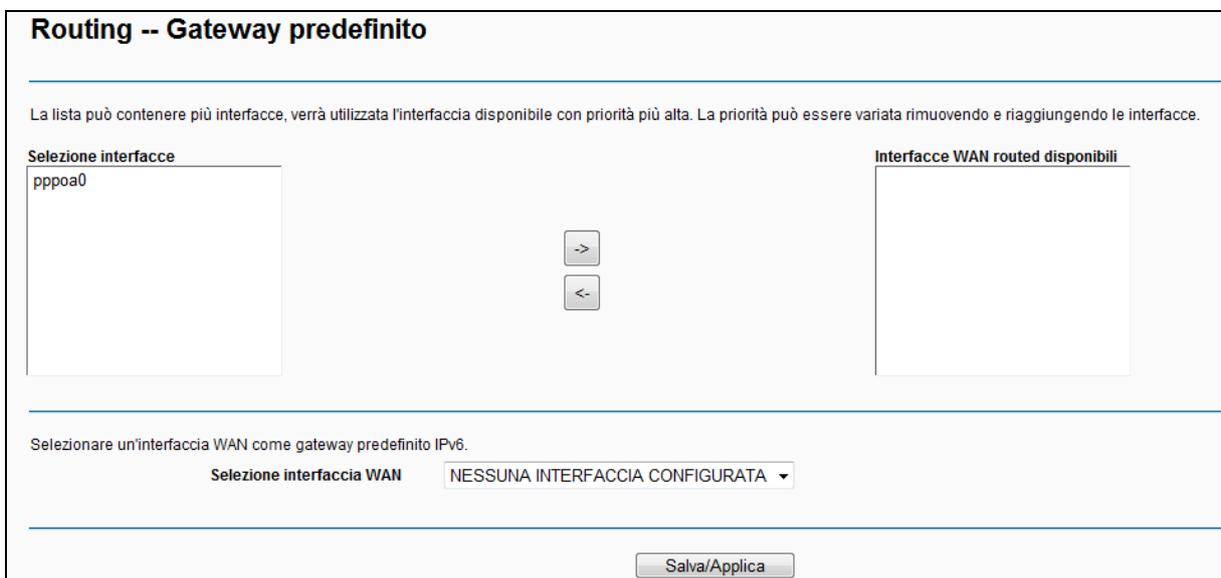


Figura 4-50

4.4.10.1 Gateway predefinito

Selezionare “Configurazione avanzata” → “Routing” → “Gateway predefinito”.

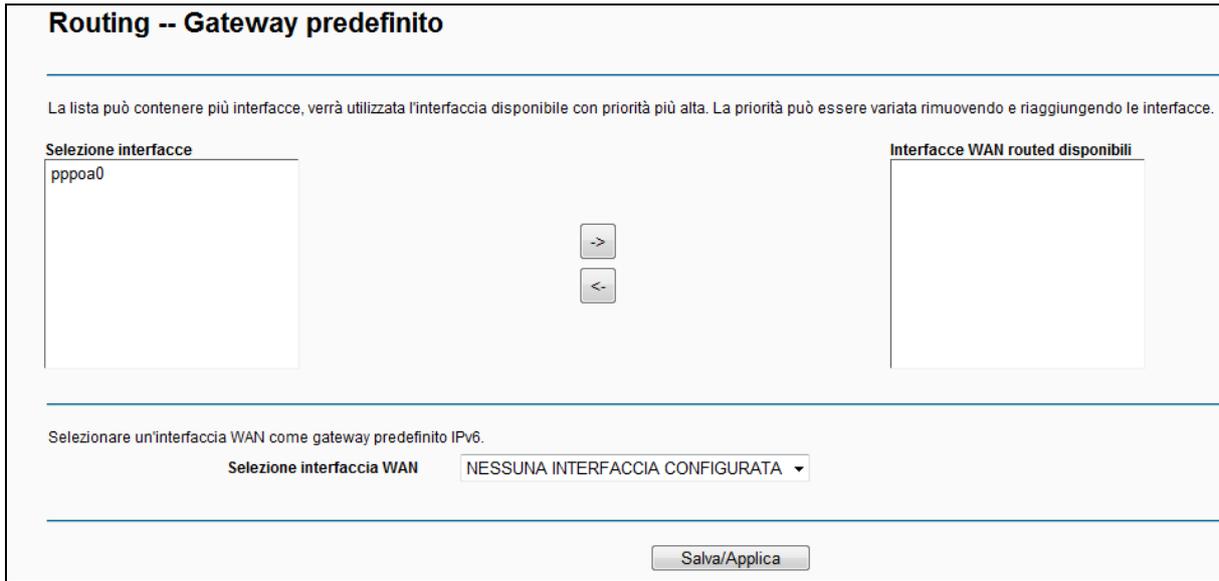


Figura 4-51

4.4.10.2 Static route

Selezionare **“Configurazione avanzata”** → **“Routing”** → **“Static route”**.



Figura 4-52

Per aggiungere una static route procedere come segue.

1. Fare clic su **Aggiungi** in Figura 4-52.

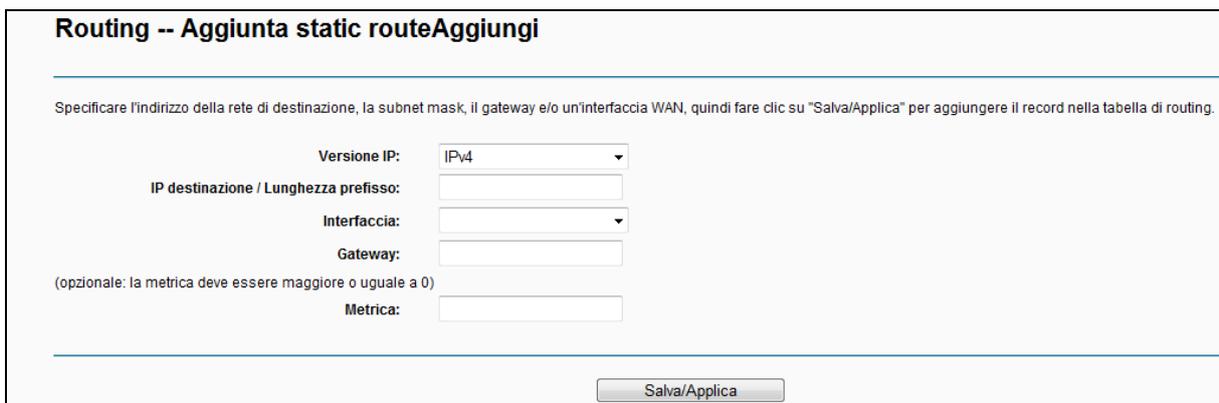


Figura 4-53

2. Specificare i seguenti parametri
 - **Versione IP:** Specificare la versione.
 - **IP destinazione / Lunghezza prefisso:** Indirizzo target ed eventuale prefisso.

- **Interfaccia:** Specificare l'interfaccia per il gateway.
 - **Gateway:** In modalità di connessione IPoE od IPoA specificare l'IP del gateway da utilizzare.
3. Fare clic su **Salva/Applica** per salvare le impostazioni.

Per rimuovere una static route procedere come segue.

- 1) Selezionare le route da rimuovere in Figura 4-52.
- 2) Fare clic su **Elimina**.

4.4.10.3 RIP

Selezionare “**Configurazione avanzata**” → “**Routing**” → “**RIP**” per visualizzare la schermata in Figura 4-54.

| Routing -- Configurazione RIP | | | |
|--|----------|------------|------------|
| <p>NOTA: RIP NON è disponibile su interfacce WAN con NAT abilitato (es. PPPoE).</p> <p>Selezionare la versione e la checkbox 'Abilitato' per abilitare RIP. Deselezionare la checkbox per disabilitarlo. Fare clic su 'Salva/Applica' per applicare le impostazioni.</p> | | | |
| Interfaccia | Versione | Operazione | Operazione |
| Nessuna WAN per il protocollo RIP | | | |

Figura 4-54

Nota:

RIP non è operativo con NAT abilitato (es. connessioni PPP).

4.4.11 DNS

Con connessioni **PPPoE**, **PPPoA** od **IPoA** è disponibile la gestione DNS.

| Configurazione server DNS | |
|--|---|
| <p>Selezionare un'interfaccia per il server DNS o specificarne manualmente l'IP. In modalità ATM occorre specificare manualmente un server DNS solamente se è configurato un singolo PVC con IPoA od IPoE statico. Possono coesistere interfacce server DNS multiple, verrà utilizzata solamente l'interfaccia con maggiore priorità. La priorità può essere modificata rimuovendo e riaggiungendo le interfacce.</p> | |
| <p><input checked="" type="radio"/> Selezionare l'interfaccia WAN per i server DNS dall'elenco delle interfacce WAN disponibili:</p> | |
| <p>Selezionare interfacce server DNS</p> <div style="border: 1px solid gray; padding: 5px; min-height: 50px;">pppoa0</div> | <p>Interfacce WAN disponibili</p> <div style="border: 1px solid gray; padding: 5px; min-height: 50px;"></div> |
| <p>-></p> <p><-</p> | |
| <p><input type="radio"/> Utilizza il seguente server DNS:</p> <p>Server DNS primario: <input type="text"/></p> <p>Server DNS secondario: <input type="text"/></p> | |
| <p>Selezionare un'interfaccia per il server DNS IPv6 o specificarne manualmente l'IPv6. La selezione di un'interfaccia WAN per DNS IPv6 causerà l'attivazione del client DHCPv6 sull'interfaccia.</p> | |
| <p><input type="radio"/> Otteni DNS IPv6 dall'interfaccia:</p> <p>Interfaccia WAN selezionata: <input type="text" value="NESSUNA INTERFACCIA CONFIGURATA"/></p> | |
| <p><input checked="" type="radio"/> Utilizza il seguente server DNS IPv6:</p> <p>Server DNS IPv6 primario: <input type="text"/></p> <p>Server DNS IPv6 secondario: <input type="text"/></p> | |
| <p><input type="button" value="Salva/Applica"/></p> | |

Figura 4-55

4.4.11.1 Server DNS

Selezionare “**Configurazione avanzata**” → “**DNS**” → “**Server DNS**” per visualizzare la schermata in Figura 4-56.

Figura 4-56

Per PVC PPPoA e PPPoE è possibile **selezionare l'interfaccia WAN per i server DNS dall'elenco delle interfacce WAN disponibili** per apprendere automaticamente l'indirizzo dei server.

Per PVC IPoA ed IPoE static selezionare **Utilizza i seguenti server DNS** e specificare manualmente i server DNS.

Lo stesso approccio è valido per i DNS IPv6.

Fare clic su **Salva/Applica** per salvare la configurazione.

4.4.11.2 Dynamic DNS

Selezionare “**Configurazione avanzata**” → “**DNS**” → “**Dynamic DNS**”.

Selezionare il provider DDNS e specificare i parametri forniti.

| Hostname | Nome utente | Servizio | Interfaccia | Elimina |
|----------|-------------|----------|-------------|---------|
| | | | | |

Figura 4-57

Per aggiungere un DDNS procedure come segue.

1. Fare clic su **Aggiungi** in Figura 4-57.

Figura 4-58

2. Selezionare il provider.
3. Specificare **Interfaccia**.
4. Specificare **Nome utente** e **Password**.

Fare clic su **Salva/Applica** per salvare le impostazioni.

4.4.12 DSL

Selezionare “**Configurazione avanzata**” → “**DSL**”.

Figura 4-59

Modificare i parametri solamente se necessario.

4.4.13 UPnP

Selezionare “**Configurazione avanzata**” → “**UPnP**”.

UPnP (Universal Plug and Play) è un protocollo distribuito multifunzionale per la collaborazione automatica fra dispositivi in rete LAN.

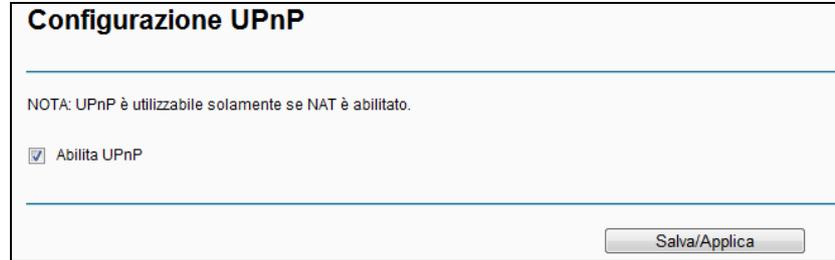
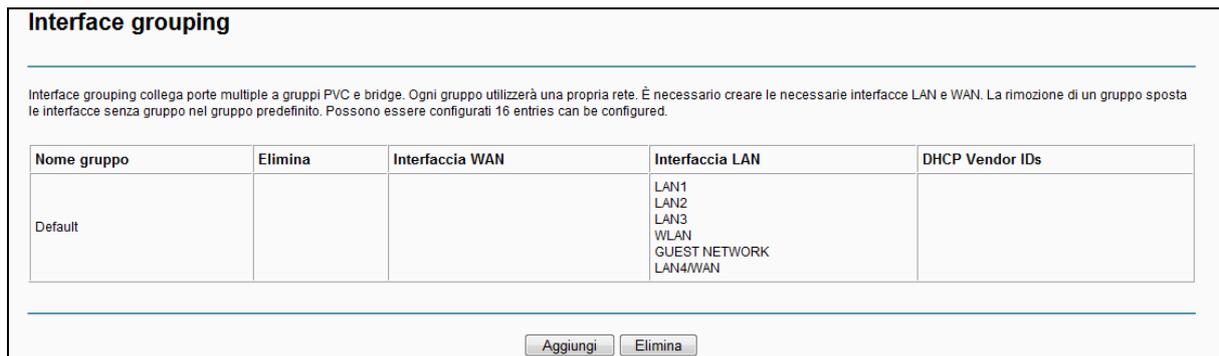


Figura 4-60

Abilitare UPnP se desiderato e fare clic su **Salva/Applica**.

4.4.14 Interface Grouping

Selezionare “**Configurazione avanzata**” → “**Interface Grouping**” per gestire i collegamenti logici fra interfaccia, PVC e bridging group.



| Nome gruppo | Elimina | Interfaccia WAN | Interfaccia LAN | DHCP Vendor IDs |
|-------------|---------|-----------------|---|-----------------|
| Default | | | LAN1 LAN2 LAN3 WLAN GUEST NETWORK LAN4/WAN | |

Figura 4-61

Fare clic su **Aggiungi** per creare la mappatura desiderata o su **Elimina** per eliminare una mappatura esistente.

Per creare un gruppo d’interfacce procedure come segue.

1. Fare clic su **Aggiungi**.

Configurazione interface grouping

Per creare un nuovo gruppo:

1. Specificare un nome unico per il gruppo e selezionare 2. (dynamic) o 3. (static);
2. Se si decidera aggiungere client LAN ad un'interfaccia WAN in un nuovo gruppo aggiungere la stringa DHCP vendor ID. Configurando una stringa DHCP vendor ID ogni richiesta da client DHCP con specifico vendor ID (DHCP opzione 60) sarà rigettata e sarà negato un indirizzo IP dal server DHCP locale.
3. Selezionare le interfacce da aggiungere al gruppo per creare la mappatura porte desiderata.
Questi client non dovrebbero ottenere IP pubblici
4. Fare clic su Salva/Applica per applicare le impostazioni.
ATTENZIONE Se un vendor ID è configurato per uno specifico client, si prega di **RIAVVIARE** il client per far sì che esso ottenga l'IP appropriato.

Nome gruppo:

Interfacce WAN utilizzate nel gruppo:

Interfacce LAN raggruppate

Interfacce LAN disponibili

LAN1
LAN2
LAN3
LAN4/WAN
WLAN
GUEST NETWORK

Aggiungi automaticamente i client con i seguenti vendor ID DHCP:

Salva/Applica

Figura 4-62

2. Specificare un nome.
3. Selezionare un'interfaccia.

 **Nota:**

Per collegare automaticamente dei client LAN ad un'interfaccia WAN utilizzare la stringa vendor ID. Con l'opzione DHCP 60 il server DHCP locale non fornirà indirizzi in favore del server DHCP sull'interfaccia WAN.

4. Selezionare le interfacce da raggruppare tramite i pulsanti freccia.
5. Fare clic su **Salva/Applica** per salvare le impostazioni.

 **Nota:**

Potrebbe essere necessario riavviare i dispositivi client affinché ottengano l'IP corretto.

4.4.15 Tunnel IP

I tunnel possono essere impiegati come soluzioni di transizione IPv4 / IPv6 per connettere reti IPv6 tramite IPv4 o mantenere la retrocompatibilità per servizi IPv4 su reti IPv6.

Selezionare **“Configurazione avanzata”** → **“Tunnel IP”**.

4.4.15.1 IPv6inIPv4

Selezionare “**Configurazione avanzata**” → “**Tunnel IP**” → “**IPv6inIPv4**” per configurare un tunnel IPv6 in IPv4 in Figura 4-63.

| Nome tunnel | Interfaccia WAN | Interfaccia LAN | Dinamico | Lunghezza maschera IPv4 | Prefisso 6rd | Indirizzo Border Relay | Elimina |
|---|-----------------|-----------------|----------|-------------------------|--------------|------------------------|---------|
| <input type="button" value="Aggiungi"/> <input type="button" value="Elimina tutto"/> <input type="button" value="Elimina"/> | | | | | | | |

Figura 4-63

Fare clic su **Aggiungi** in Figura 4-63 per configurare un tunnel 6in4 come in Figura 4-64.

È supportato solamente 6rd.

Nome tunnel:

Meccanismo: 6RD

Interfaccia WAN:

Interfaccia LAN: LAN/br0

Manuale Automatica

Lunghezza maschera IPv4:

Lunghezza massima prefisso 6rd:

Indirizzo IPv4 border relay:

Figura 4-64

- **Meccanismo:** 6RD è utilizzabile con LAN IPv6 e WAN IPv4.
- **Interfaccia WAN:** Selezionare un'interfaccia.
- **Interfaccia LAN:** Selezionare un'interfaccia LAN connessa.
- **Lunghezza maschera IPv4:** Specificare la lunghezza in uso.
- **Lunghezza massima prefisso 6RD:** Specificare il prefisso in uso.
- **Indirizzo IPv4 border relay:** Specificare l'IPv4 del router border relay.

Fare clic su **Salva/Applica** per applicare la configurazione.

Nota:

In questa modalità non sono consentite connessioni WAN IPv6.

4.4.15.2 IPv4inIPv6

Selezionare “**Configurazione avanzata**” → “**Tunnel IP**” → “**IPv4inIPv6**” per configurare un tunnel IPv4 in IPv6 come in Figura 4-65.

| Tunnel IP -- Configurazione tunnel 4in6 | | | | | |
|---|-----------------|-----------------|----------|------|---------|
| Nome tunnel | Interfaccia WAN | Interfaccia LAN | dinamico | AFTR | Elimina |
| <input type="button" value="Aggiungi"/> <input type="button" value="Elimina tutto"/> <input type="button" value="Elimina"/> | | | | | |

Figura 4-65

Fare clic su **Aggiungi** in Figura 4-65.

| Tunnel IP -- Configurazione tunnel 4in6 | |
|--|---|
| È supportato solamente DS-Lite. | |
| Nome tunnel: | <input type="text"/> |
| Meccanismo: | DS-Lite <input type="button" value="v"/> |
| Interfaccia WAN: | <input type="button" value="v"/> |
| Interfaccia LAN: | LAN/br0 <input type="button" value="v"/> |
| | <input checked="" type="radio"/> Manuale <input type="radio"/> Automatica |
| AFTR: | <input type="text"/> |
| <input type="button" value="Salva/Applica"/> | |

Figura 4-66

- **Meccanismo:** DS-Lite è utilizzabile con LAN IPv4 e WAN IPv6.
- **Interfaccia WAN:** Selezionare un'interfaccia.
- **Interfaccia LAN:** Selezionare un'interfaccia LAN connessa.
- **AFTR:** Specificare l'IPv6 del nodo remoto.

Fare clic su **Salva/Applica** per salvare le impostazioni.

 **Nota:**

In questa modalità non sono permesse connessioni WAN IPv4.

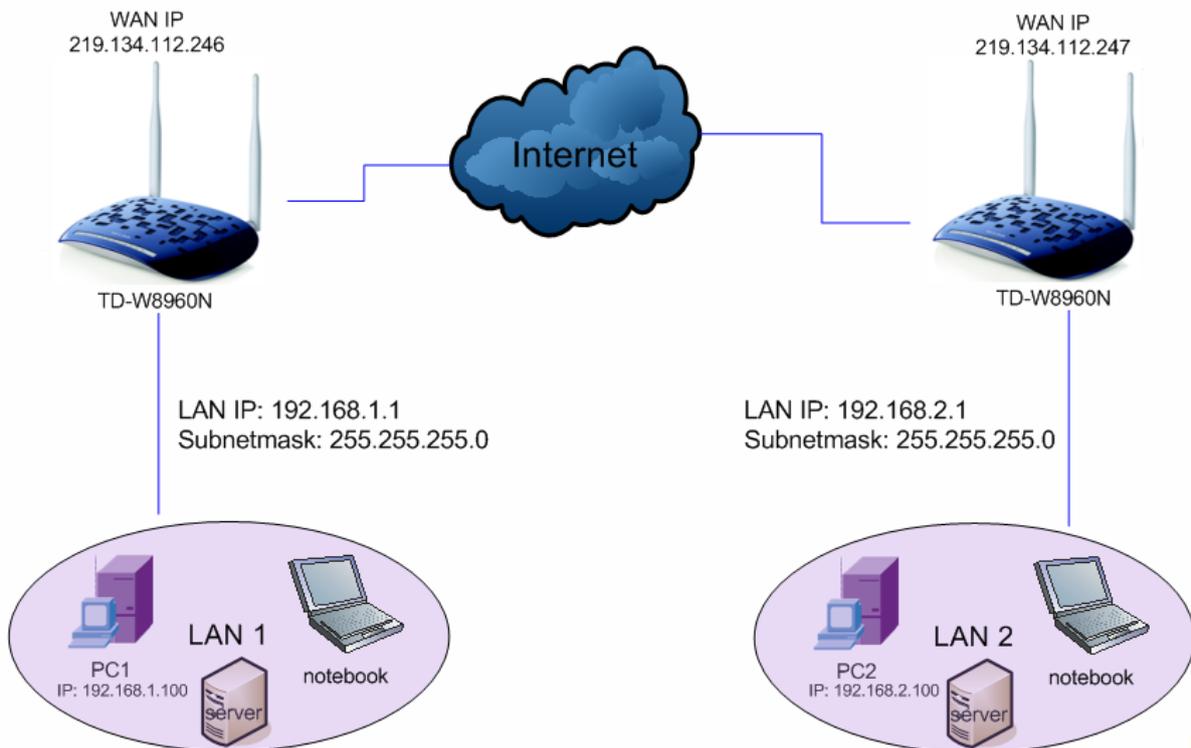
4.4.16 IPSec

Selezionare **“Configurazione avanzata”** → **“IPSec”** per gestire i tunnel IPsec come in Figura 4-67.

| Connessioni tunnel IPsec | | | | | | | |
|--|----------------|------------------|------------------|-------|--------------------|----------|---------|
| La schermata permette la gestione dei tunnel IPsec. | | | | | | | |
| <input checked="" type="checkbox"/> DPD - Dead Peer Detection (Attenzione: potrebbe destabilizzare la trasmissione) | | | | | | | |
| Nome connessione | Gateway remoto | Indirizzo locale | Indirizzo remoto | Stato | Abilita/Disabilita | Modifica | Elimina |
| <input type="button" value="Aggiungi Nuova Connessione"/> <input type="button" value="Abilita Tutto"/> <input type="button" value="Seleziona Tutto"/> <input type="button" value="Elimina"/> | | | | | | | |

Figura 4-67

L'esempio mostra una tipica topologia VPN.



Nota:

È possibile configurare fino a 10 tunnel IPsec fra differenti tipi di router/gateway.

Fare clic su **Aggiungi tunnel IPsec** in Figura 4-67.

| Configurazione IPsec | |
|--|---|
| Nome connessione IPsec: | <input type="text" value="new connection"/> |
| Gateway remoto IPsec (URL/IPv4): | <input type="text" value="0.0.0.0"/> |
| Accesso al tunnel da IP locali: | <input type="text" value="Subnet"/> |
| Indirizzo IP VPN: | <input type="text" value="0.0.0.0"/> |
| Subnet mask: | <input type="text" value="255.255.255.0"/> |
| Accesso tunnel da IP remoti: | <input type="text" value="Subnet"/> |
| Indirizzo IP VPN: | <input type="text" value="0.0.0.0"/> |
| Subnet mask: | <input type="text" value="255.255.255.0"/> |
| Metodo scambio chiavi: | <input type="text" value="Auto(IKE)"/> |
| Metodo autenticazione: | <input type="text" value="Pre-Shared Key"/> |
| Pre-Shared Key: | <input type="text" value="key"/> |
| Perfect Forward Secrecy: | <input type="text" value="Disabilita"/> |
| Configurazione IKE avanzata: | <input type="button" value="Mostra Impostazioni Avanzate"/> |
| <input type="button" value="Salva/Applica"/> | |

Figura 4-68

- **Nome connessione IPsec:** Specificare un nome.
- **Gateway remoto IPsec(URL/IPv4):** Specificare il gateway VPN sul nodo remoto.
- **Accesso al tunnel da IP Locali:** Selezionare per permettere l'accesso ai dispositivi nella LAN locale.

- **Indirizzo IP VPN:** Specificare su ogni nodo l'IP della LAN locale.
- **Subnet mask:** Specificare su ogni nodo la subnet mask in uso sulla LAN locale.
- **Accesso tunnel da IP remoti:** Su ogni nodo, selezionare Subnet per consentire l'accesso da remoto a tutta la LAN locale o specificare l'IP dei dispositivi in LAN locale cui si può accedere.
- **Indirizzo IP VPN:** Specificare su ogni nodo l'IP della LAN remota.
- **Subnet mask:** Specificare su ogni nodo la subnet mask in uso sulla LAN remota.
- **Metodo scambio chiavi:** Selezionare Auto (IKE) o Manual (Manuale).
- **Metodo autenticazione:** Si raccomanda Pre-Shared Key.
- **Pre-Shared Key:** Specificare una chiave.
- **Perfect Forward Secrecy:** PFS è un protocollo di sicurezza aggiuntiva.

 **Nota:**

I nodi che operano da gateway/endpoint VPN devono condividere le stesse chiavi e le stesse impostazioni FPS.

Si consiglia di non modificare i parametri di configurazione avanzata.

Fare clic su **Mostra Impostazioni Avanzate** per visualizzare la configurazione avanzata.

Configurazione IKE avanzata: nascondi Avanzate

Fase 1

Modo: Main ▼

Tipo My Identifier: IP WAN locale ▼

My Identifier:

Tipo Remote Identifier: IP WAN remoto ▼

Remote Identifier:

Algoritmo crittografia: 3DES ▼

Algoritmo integrità: MD5 ▼

Gruppo Diffie-Hellman per scambio chiavi: 1024bit ▼

Key Life Time: Secondi

Fase 2

Algoritmo crittografia: 3DES ▼

Algoritmo integrità: MD5 ▼

Key Life Time: Secondi

Salva/Applica

- **Main Mode:** Selezionare per utilizzare la negoziazione standard IKE fase 1.
- **Aggressive Mode:** Selezionare per accelerare la negoziazione IKE fase 1 a scapito del livello di sicurezza.

 **Nota:**

In modalità aggressiva alcuni parametri non sono negoziati offrendo maggiori velocità di connessione e compatibilità.

- **Key Life Time:** Si consiglia di non modificare il valore predefinito.

4.4.17 Multicast

Selezionare “**Configurazione avanzata**” → “**Multicast**” per configurare il protocollo IGMP.

Configurazione IGMP

Abilitare IGMP per modificare i parametri sottostanti.

| | |
|--|-------------------------------------|
| Versione predefinita: | <input type="text" value="3"/> |
| Intervallo query: | <input type="text" value="125"/> |
| Intervallo responso query: | <input type="text" value="10"/> |
| Intervallo ultimo membro query: | <input type="text" value="10"/> |
| Valore robustness: | <input type="text" value="2"/> |
| Limite gruppi multicast: | <input type="text" value="25"/> |
| Limite sorgenti dati multicast (per IGMPv3 : (1 - 24): | <input type="text" value="10"/> |
| Limite membri gruppo multicast: | <input type="text" value="25"/> |
| Abilita fast leave: | <input checked="" type="checkbox"/> |
| Abilita multicast LAN to LAN (Intra LAN): | <input type="checkbox"/> |

Figura 4-69

Fare clic su **Salva/Applica** per salvare le impostazioni.

4.5 Wireless



4.5.1 Wireless

Selezionare **“Wireless”** → **“Impostazioni di base”** per visualizzare la schermata in Figura 4-70.

Wireless -- Configurazione di base

La schermata permette la gestione dei parametri wireless di base.
Fare clic su "Salva/Applica" per salvare le impostazioni.

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Abilita Wireless |
| <input type="checkbox"/> | Nascondi SSID |
| <input type="checkbox"/> | Isolamento client |
| Nome rete wireless: | <input type="text" value="123"/> (SSID) |
| BSSID: | <input type="text" value="02:10:18:01:00:01"/> |
| Regione: | <input type="text" value="ITALY"/> |

Figura 4-70

➤ **Abilita wireless:** Controllo di abilitazione dell'interfaccia.

- **Nascondi SSID:** Abilitare per rendere la rete non visibile.
- **Isolamento client:** Abilitare per impedire la comunicazione tra dispositivi wireless.
- **Nome rete wireless:** Nome identificativo della rete wireless.
- **BSSID:** Indirizzo MAC dell'interfaccia.
- **Regione:** Specificare la regione per non contravvenire alla locale normativa.

Fare clic su **Salva/Applica** per salvare le impostazioni.

4.5.2 Sicurezza

Selezionare **"Wireless"** → **"Sicurezza"** per visualizzare la schermata in Figura 4-71.

Wireless -- Sicurezza

Questa pagina permette la configurazione dei parametri di sicurezza wireless.
È possibile, in alternativa, configurare tramite WPS (Wi-Fi Protected Setup).

WPS

Abilitato WPS:

Aggiungi Client

Tasto WPS PIN

[Aiuto](#)

PIN dispositivo: [Aiuto](#)

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.
È possibile specificare autenticazione, crittografia e password.
Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.
Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP.

Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

Password: (WPA Pre-Shared Key)
[Visualizza password](#)
(da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimali)

WPA Group Rekey Interval: (opzionale)

Crittografia WPA:

Crittografia WEP:

Figura 4-71

4.5.2.1 WPS

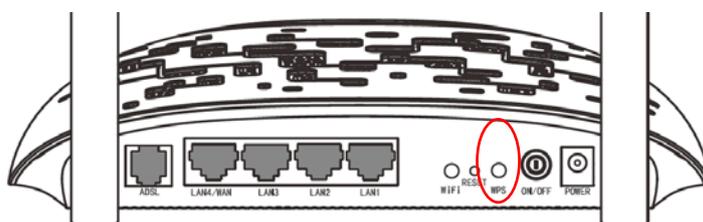
WPS consente la rapida connessione sicura di nuovi dispositivi.

Esistono 3 metodi per connettere un dispositivo.

I. Pulsante WPS/QSS (PBC)

Utilizzare questo metodo se il dispositivo ha un pulsante WPS/QSS.

Passo 1: Premere il pulsante WPS sul retro del modem router come in figura.



Passo 2: Premere il pulsante WPS sul dispositivo.



Passo 3: Il LED WPS sul modem router lampeggia mentre WPS è in attesa.

Passo 4: Se il LED WPS si accende la connessione è avvenuta con successo.

Fare riferimento alla guida utente del dispositivo da collegare per ulteriori informazioni.

II. Inserimento del codice PIN del dispositivo nel modem/router

Utilizzare questo metodo se il dispositivo ha un PIN WPS.

Passo 1: Selezionare **PIN** in Figura 4-72, inserire il PIN del dispositivo e fare clic su **Connetti**.

Wireless -- Sicurezza

Questa pagina permette la configurazione dei parametri di sicurezza wireless.
È possibile, in alternativa, configurare tramite WPS (Wi-Fi Protected Setup).

WPS

Abitato WPS:

Aggiungi Client

Tasto WPS
 PIN

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.
È possibile specificare autenticazione, crittografia e password.
Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.
Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP.

Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

Password: (WPA Pre-Shared Key)
[Visualizza password](#)
(da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimali)

WPA Group Rekey Interval: (opzionale)

Crittografia WPA:

Crittografia WEP:

Figura 4-72

Passo 2: Attendere il completamento della connessione.

III. Inserimento del PIN del modem/router nel dispositivo

Utilizzare questo metodo se il dispositivo richiede il PIN del modem/router.

Passo 1: Inserire il PIN del modem router nel dispositivo. Il PIN predefinito è riportato sulla targia di prodotto.

Passo 2: Il LED WPS lampeggia per 2 minuti durante la connessione.

Passo 3: Se il LED WPS si accende la connessione è avvenuta.

Fare riferimento alla guida utente del dispositivo da collegare per ulteriori informazioni.

4.5.2.2 Configurazione manuale AP

La sottosezione permette la configurazione manuale della sicurezza wireless.

Questa pagina permette la configurazione dei parametri di sicurezza wireless.
È possibile, in alternativa, configurare tramite WPS (Wi-Fi Protected Setup).

WPS

Abilitato WPS:

Aggiungi Client

Tasto WPS PIN

[Aiuto](#)

PIN dispositivo: [Aiuto](#)

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.
È possibile specificare autenticazione, crittografia e password.
Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.
Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP*.
Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

Password: (WPA Pre-Shared Key)
[Visualizza password](#)
(da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimali)

WPA Group Rekey Interval: (opzionale)

Crittografia WPA:

Crittografia WEP:

Figura 4-73

➤ **Autenticazione:** Si consiglia Mixed WPA2/WPA-PSK.

1. WEP

WEP (Wired Equivalent Privacy) è un obsoleto standard di sicurezza senza autenticazione, se ne sconsiglia pertanto l'adozione.

Nota:

WEP non è compatibile con IEEE 802.11n .

2. WPA

WPA-Enterprise (Wi-Fi Protected Access - Enterprise) è uno standard di sicurezza che comprende crittografia ed autenticazione basata su server Radius.

Nota:

WPA potrebbe non essere compatibile con IEEE 802.11n .

Wireless -- Sicurezza

Questa pagina permette la configurazione dei parametri di sicurezza wireless.
È possibile, in alternativa, configurare tramite WPS (Wi-Fi Protected Setup).

WPS

Abilitato WPS:

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.
È possibile specificare autenticazione, crittografia e password.
Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.
Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP*.

Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

WPA Group Rekey Interval: (opzionale)

Indirizzo IP server radius:

Porta radius: (1-65535)

Password radius: (opzionale)
(da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimali)

Crittografia WPA:

Crittografia WEP:

Figura 4-74

- **WPA Group ReKey Interval:** Durata delle chiavi, si consiglia di non modificare il valore predefinito.
 - **Indirizzo IP server radius:** Indirizzo del server radius.
 - **Porta radius:** Porta del server radius, si consiglia di non modificare il valore predefinito.
 - **Password radius:** Password per l'accesso al server radius.
 - **Crittografia WPA:** Si consiglia la crittografia AES (TKIP non è compatibile con 802.11n).
- Fare clic su **Salva/Applica** per applicare le impostazioni.

WPS

Abilitato WPS:

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.
 È possibile specificare autenticazione, crittografia e password.
 Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.
 Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP.

Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

WPA Group Rekey Interval: (opzionale)

Indirizzo IP server radius:

Porta radius: (1-65535)

Password radius: (opzionale)
 (da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimali)

Crittografia WPA:

Crittografia WEP:

Figura 4-75

3. WPA-Personal (WPA-PSK)

WPA-PSK (Wi-Fi Protected Access – Pre Shared Key) è uno standard di sicurezza che comprende crittografia ed autenticazione basata su password precondivisa.

 **Nota:**

WPA potrebbe non essere compatibile con IEEE 802.11n .

Wireless -- Sicurezza

Questa pagina permette la configurazione dei parametri di sicurezza wireless.
È possibile, in alternativa, configurare tramite WPS (Wi-Fi Protected Setup).

WPS

Abilitato WPS:

Aggiungi Client

Tasto WPS
 PIN

[Aiuto](#)

PIN dispositivo:

[Aiuto](#)

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.
È possibile specificare autenticazione, crittografia e password.
Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.
Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP".

Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

Password: (WPA Pre-Shared Key)
[Visualizza password](#)
 (da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimale)

WPA Group Rekey Interval: (opzionale)

Crittografia WPA:

Crittografia WEP:

Figura 4-76

- **Password:** Specificare una password da 8 a 63 caratteri ASCII o da 8 a 64 cifre esadecimale.
- **Visualizza password:** Fare clic per visualizzare la password.

Fare clic su **Salva/Applica** per salvare le impostazioni.

WPS

Abilitato WPS:

Aggiungi Client

Tasto WPS PIN

[Aiuto](#)

PIN dispositivo: [Aiuto](#)

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.
 È possibile specificare autenticazione, crittografia e password.
Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.
 Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP".

Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

Password: (WPA Pre-Shared Key)
[Visualizza password](#)
 (da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimale)

WPA Group Rekey Interval: (opzionale)

Crittografia WPA:

Crittografia WEP:

Figura 4-77

4. WPA2-Enterprise (WPA2)

WPA2-Enterprise (Wi-Fi Protected Access 2 - Enterprise) è uno standard di sicurezza che comprende crittografia ed autenticazione basata su server radius con preautenticazione.

 **Nota:**

Consigliato per l'utilizzo con server radius.

Wireless -- Sicurezza

Questa pagina permette la configurazione dei parametri di sicurezza wireless.
 È possibile, in alternativa, configurare tramite WPS (Wi-Fi Protected Setup).

WPS

Abilitato WPS:

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.
 È possibile specificare autenticazione, crittografia e password.
Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.
 Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP".

Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

Preautenticazione WPA2:

Intervallo re-auth: (opzionale)

WPA Group Rekey Interval: (opzionale)

Indirizzo IP server radius:

Porta radius: (1-65535)

Password radius: (opzionale)
 (da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimale)

Crittografia WPA:

Crittografia WEP:

Figura 4-78

- **Preautenticazione WPA2:** Selezionare per abilitare l'autenticazione in fase di scansione.
- **Intervallo re-auth:** Si consiglia di non modificare il valore predefinito.

5. WPA2-Personal (WPA2-PSK)

WPA2-PSK (Wi-Fi Protected Access 2 – Pre Shared Key) è uno standard di sicurezza che comprende crittografia ed autenticazione basata su password precondivisa con preautenticazione (consigliato).

 **Nota:**

Consigliato per l'utilizzo senza server.

Wireless -- Sicurezza

Questa pagina permette la configurazione dei parametri di sicurezza wireless.
È possibile, in alternativa, configurare tramite WPS (Wi-Fi Protected Setup).

WPS

Abilitato WPS:

Aggiungi Client

Tasto WPS
 PIN

[Aiuto](#)

PIN dispositivo:

[Aiuto](#)

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.
È possibile specificare autenticazione, crittografia e password.
Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.
Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP*.

Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

Password: (WPA Pre-Shared Key)
[Visualizza password](#)
 (da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimale)

WPA Group Rekey Interval: (opzionale)

Crittografia WPA:

Crittografia WEP:

Figura 4-79

6. Mixed WPA2/WPA Enterprise (WPA2/WPA)

Sarà utilizzato preferenzialmente WPA2; sarà utilizzato WPA se il dispositivo in connessione non supporta WPA2.

Wireless -- Sicurezza

Questa pagina permette la configurazione dei parametri di sicurezza wireless.
È possibile, in alternativa, configurare tramite WPS (Wi-Fi Protected Setup).

WPS

Abilitato WPS:

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.

È possibile specificare autenticazione, crittografia e password.

Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.

Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP.

Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

Preautenticazione WPA2:

Intervallo re-auth: (opzionale)

WPA Group Rekey Interval: (opzionale)

Indirizzo IP server radius:

Porta radius: (1-65535)

Password radius: (opzionale)

(da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimali)

Crittografia WPA:

Crittografia WEP:

Figura 4-80

7. Mixed WPA2/WPA-Personal (WPA2/WPA)

Sarà utilizzato preferenzialmente WPA2-PSK; sarà utilizzato WPA-PSK se il dispositivo in connessione non supporta WPA2-PSK.

Wireless -- Sicurezza

Questa pagina permette la configurazione dei parametri di sicurezza wireless.
È possibile, in alternativa, configurare tramite WPS (Wi-Fi Protected Setup).

WPS

Abilitato WPS:

Aggiungi Client

Tasto WPS PIN

[Aiuto](#)

PIN dispositivo: [Aiuto](#)

Configurazione manuale

Si raccomanda caldamente la sicurezza WPA2-PSK.
È possibile specificare autenticazione, crittografia e password.
Nota: si raccomanda di non utilizzare la crittografia WEP in modalità 11n.
Attenzione: la modalità 11n non è supportata con crittografia WEP abilitata o con crittografia TKIP".

Fare clic su "Salva/Applica" per salvare le impostazioni.

Autenticazione:

Password: (WPA Pre-Shared Key)
[Visualizza password](#)
(da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimali)

WPA Group Rekey Interval: (opzionale)

Crittografia WPA:

Crittografia WEP:

Figura 4-81

4.5.3 Timer

Selezionare menu **"Wireless"** → **"Timer"** per configurare la temporizzazione dell'interfaccia wireless.

Wireless -- Timer

La schermata permette la configurazione del timer per la funzionalità wireless.
Fare clic su **Aggiungi** per specificare il periodo di sospensione della funzionalità.
Fare clic [qui](#) per configurare l'orologio di sistema.

Timer wireless: Abilita Disabilita

Timer: Orario iniziale: Orario finale:

| Orario | 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 |
|--------|------|------|------|------|------|------|------|------|------|------|-------|-------|-------|-------|-------|
| Dom | | | | | | | | | | | | | | | |
| Lun | | | | | | | | | | | | | | | |
| Mar | | | | | | | | | | | | | | | |
| Mer | | | | | | | | | | | | | | | |
| Gio | | | | | | | | | | | | | | | |
| Ven | | | | | | | | | | | | | | | |
| Sab | | | | | | | | | | | | | | | |

Figura 4-82

Nota:

1. Configurare il periodo di spegnimento.
2. È necessario configurare innanzitutto [4.9.5 Ora Internet](#).

- **Timer:** Selezionare i giorni.
- **Orario iniziale, Orario finale:** Specificare gli orari di inizio e fine blocco.
- **Aggiungi:** Fare clic per aggiungere la schedulazione definita.

Fare clic su **Pulisci Schedulazione** per azzerare la tabella.

Fare clic su **Salva/Applica** per salvare le informazioni.

4.5.4 Filtro MAC

Selezionare “**Wireless**” → “**Filtro MAC**” per visualizzare la schermata in Figura 4-83.

Wireless -- Filtro MAC

Possono essere configurate fino a 64 indirizzi MAC.

Modalità MAC restrict: Disabilitata Permetti Nega Nota: Selezionando 'permetti' senza specificare un indirizzo MAC WPS sarà disabilitato.

| Indirizzo MAC | Elimina |
|---------------|---------|
| | |

Figura 4-83

Selezionare una delle seguenti modalità.

- **Disabilitata:** Filtro inattivo.

- **Permetti:** Consente la connessione solo ai dispositivi con indirizzo MAC in lista.
- **Nega:** Blocca la connessione ai dispositivi con indirizzo MAC in lista.
- **Aggiungi:** Fare clic per aggiungere un indirizzo MAC in formato xx:xx:xx:xx:xx:xx come in Figura 4-83.
- **Elimina:** Fare clic per eliminare gli indirizzi selezionati.

Figura 4-84

Fare clic su **Salva/Applica** per salvare le impostazioni.

4.5.5 Bridge wireless

Selezionare **“Wireless”** → **“Bridge wireless”** per visualizzare la schermata in Figura 4-85.

Figura 4-85

- **Modalità:** Selezionare la modalità operativa.
 - **Access Point:** Modalità standard per la connessione di client wireless.
 - **Wireless Bridge:** Conosciuto come WDS (Wireless Distribution System) esegue un bridge verso altro access point per connettere le 2 LAN.
- **Restrizione bridge:**
 - **Disabilitata:** Accesso non regolato.
 - **Abilitata:** Accesso consentito solo agli indirizzi MAC specificati.

Modalità:

Restrizione bridge:

Indirizzi MAC bridge remoti:

Figura 4-86

- **Abilitata (Scan):** Restrizione con scansione automatica.
- **Aggiorna:** Fare clic per aggiornare la lista degli access point rilevati.

Modalità:

Restrizione bridge:

Indirizzi MAC bridge remoti:

| | SSID | BSSID | Canale |
|-------------------------------------|-----------------------|-------------------|--------|
| <input type="checkbox"/> | TP-LINK_2.4GHz_B2426D | C0:4A:00:B2:42:6D | 11 |
| <input type="checkbox"/> | TL-PA2010 | 00:03:7F:BE:F0:F4 | 7 |
| <input type="checkbox"/> | WLAN-PS | 62:31:26:06:7E:B5 | 6 |
| <input type="checkbox"/> | Keenetic-8818 | EA:28:5D:94:4E:70 | 3 |
| <input checked="" type="checkbox"/> | TP-LINK_2C907E | 0C:82:68:2C:90:7E | 11 |
| <input checked="" type="checkbox"/> | TP-LINK_662FDE | 10:FE:ED:66:2F:DE | 11 |
| <input checked="" type="checkbox"/> | TP-LINK_EC6763 | 00:0A:EC:EC:67:63 | 11 |
| <input type="checkbox"/> | MikroTik-0A5F2F | D4:CA:6D:0A:5F:2F | 1 |
| <input checked="" type="checkbox"/> | TP-LINK_GuestDE | 1A:FE:ED:66:2F:DE | 11 |

Figura 4-87

4.5.6 Avanzate

Selezionare “Wireless” → “Avanzate” per editare le impostazioni avanzate.

Wireless -- Avanzate

Modificare le impostazioni solamente se necessario.
 Fare clic su "Salva/Applica" per applicare le impostazioni.

Canale:

Modo:

Ampiezza canale:

Selezione sideband:

Soglia di frammentazione:

Soglia RTS:

Intervallo DTIM:

Intervallo beacon:

Potenza segnale:

WMM(Wi-Fi Multimedia):

Figura 4-88

- **Canale:** Selezione del canale in uso. Si raccomanda di modificare il valore predefinito solamente in caso di problemi.

- **Modo:** Modalità 802.11 in uso. Si raccomanda di modificare il valore predefinito solamente in caso di problemi.
- **Ampiezza canale:** Si raccomanda di modificare il valore predefinito solamente in caso di problemi.
- **Selezione sideband:** Si raccomanda di modificare il valore predefinito solamente in caso di problemi.
- **Soglia di frammentazione:** Dimensione massima dei pacchetti. Si raccomanda il valore predefinito.
- **Soglia RTS:** Soglia Request to Send. Si consiglia il valore predefinito.
- **Intervallo DTIM:** Si raccomanda il valore predefinito. Sono utilizzabili valori nel range 1-255.
- **Intervallo beacon:** Si raccomanda il valore predefinito. Sono utilizzabili valori nel range 25-1000ms.
- **Potenza segnale:** Si raccomanda Alta.
- **WMM(Wi-Fi Multimedia):** WMM abilita la priorità per i pacchetti ad altra priorità. Disabilitare solo in caso di problemi.

4.5.7 Informazioni dispositivo

Selezionare “Wireless” → “Informazioni dispositivo” per visualizzare i dispositivi collegati.

| Wireless -- Dispositivi autenticati | | | |
|---|-----------|-------------|------|
| Questa pagina mostra lo stato dei dispositivi wireless. | | | |
| MAC | Associato | Autorizzato | SSID |
| <input type="button" value="Aggiorna"/> | | | |

Figura 4-89

- **MAC:** Indirizzo MAC del dispositivo.
- **Associato:** Stato dell’associazione all’access point.
- **Autorizzato:** Stato dell’autenticazione alla rete.
- **SSID:** SSID a cui il dispositivo è connesso.

Fare clic su **Aggiorna** per aggiornare la pagina.

4.6 Rete guest

| |
|--------------------------|
| Rete guest |
| • Configurazione di base |
| • Dispositivi collegati |

4.6.1 Configurazione di base

Selezionare “Rete guest” → “Configurazione di base” per configurare una rete isolata dedicata a dispositivi ospite come Figura 4-90.

Wireless -- Rete guest

La schermata permette la configurazione di una rete guest.

Rete guest: Abilita Disabilita

Guest SSID:

Autenticazione:

Crittografia:

Password: (da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimali.)
[Visualizza password](#)

Group Key Update Period: (minimo 30 secondi, 0 significa nessun aggiornamento)

Permetti ospiti alla rete locale:

Isolamento rete guest:

Bandwidth control rete guest:

| | Min Rate(Kbps) | Max Rate(Kbps) |
|-------------|----------------------------------|-----------------------------------|
| Upstream: | <input type="text" value="500"/> | <input type="text" value="1000"/> |
| Downstream: | <input type="text" value="500"/> | <input type="text" value="1000"/> |

Figura 4-90

- **Guest SSID:** Nome della rete guest.
- **Autenticazione:** Si consiglia WPA2-Personal (WPA2-PSK).
- **Crittografia:** Si consiglia AES.
- **Password:** Specificare una password da 8 a 63 caratteri ASCII o da 8 a 64 caratteri esadecimali.
- **Group Key Update Period:** Si consiglia di non modificare il valore predefinito.
- **Accesso ospiti alla rete locale:** Permette l'accesso degli ospiti a dispositivi nella rete locale, senza accesso alla console di gestione.
- **Isolamento rete guest:** L'isolamento impedisce ad ogni dispositivo di comunicare con gli altri dispositivi senza fili.
- **Bandwidth control rete guest:** La funzionalità permette di limitare la banda offerta ai dispositivi ospite.

Fare clic su **Salva/Applica** per applicare le impostazioni.

4.6.2 Dispositivi collegati

Selezionare **"Rete guest"** → **"Dispositivi collegati"**.

Wireless -- Dispositivi autenticati

Questa pagina mostra lo stato dei dispositivi wireless.

| MAC | Associato | Autorizzato | SSID |
|-----|-----------|-------------|------|
| | | | |

Figura 4-91

- **MAC:** Indirizzo MAC del dispositivo.

- **Associato:** Stato dell'associazione all'access point.
- **Autorizzato:** Stato dell'autenticazione alla rete.
- **SSID:** SSID a cui il dispositivo è connesso.

Fare clic su **Aggiorna** per aggiornare la pagina.

4.7 Diagnostica

Selezionare “**Diagnostica**” per visualizzare gli strumenti atti all'analisi dei problemi.

pppoa_0_8_35 Diagnostica

I test disponibili sono elencati di seguito. Se un test fallisce fare clic su "Riesegui Test" in fondo alla pagina per verificare nuovamente. Se il test fallisce costantemente fare clic su "Aiuto" ed eseguire la procedura di risoluzione dei problemi.

Verifica connessione alla rete locale

| | | |
|---------------------------------|---------|-----------------------|
| Verifica connessione LAN1 : | PASSATO | Aiuto |
| Verifica connessione LAN2 : | FALLITO | Aiuto |
| Verifica connessione LAN3 : | FALLITO | Aiuto |
| Verifica connessione LAN4/WAN : | FALLITO | Aiuto |
| Verifica connessione wireless: | PASSATO | Aiuto |

Verifica connessione al provider ISP

| | | |
|--------------------------------------|--------------|-----------------------|
| Verifica sincronizzazione ADSL: | FALLITO | Aiuto |
| Verifica ping segmento ATM OAM F5: | DISABILITATO | Aiuto |
| Verifica ping end-to-end ATM OAM F5: | DISABILITATO | Aiuto |

Verifica connessione al provider ISP

| | | |
|--|--------------|-----------------------|
| Verifica sessione server PPP: | DISABILITATO | Aiuto |
| Verifica autenticazione al provider ISP: | DISABILITATO | Aiuto |
| Verifica indirizzo IP assegnato: | DISABILITATO | Aiuto |
| Verifica ping gateway predefinito: | FALLITO | Aiuto |
| Verifica ping DNS primario: | FALLITO | Aiuto |

Figura 4-92

4.8 Gestione

| Gestione |
|--------------------------|
| + Impostazioni |
| • Log di sistema |
| • Agente SNMP |
| • Client TR-069 |
| • Ora Internet |
| + Controllo accessi |
| • Aggiornamento firmware |
| • Riavvio |

4.8.1 Configurazione

La sezione permette backup e ripristino della configurazione.

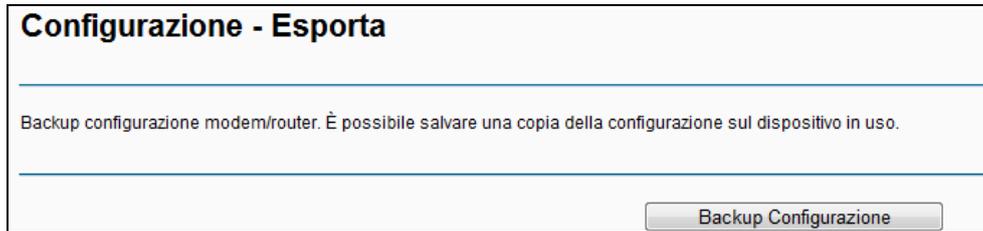


Figura 4-93

4.8.1.1 Esportazione

Selezionare “**Gestione**” → “**Configurazione**” → “**Esporta**”, per visualizzare la schermata in Figura 4-94.

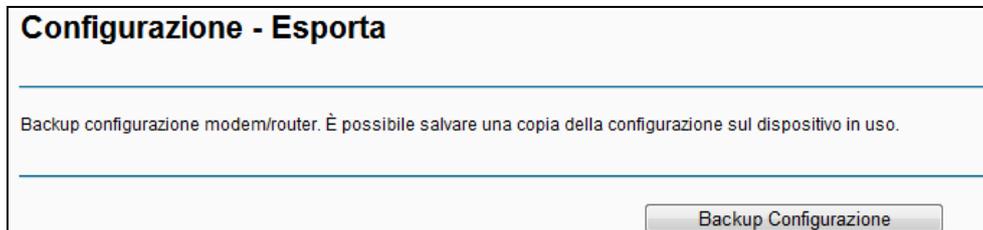


Figura 4-94

Per esportare su file la configurazione procedere come segue.

1. Fare clic su **Backup Configurazione** in Figura 4-94).

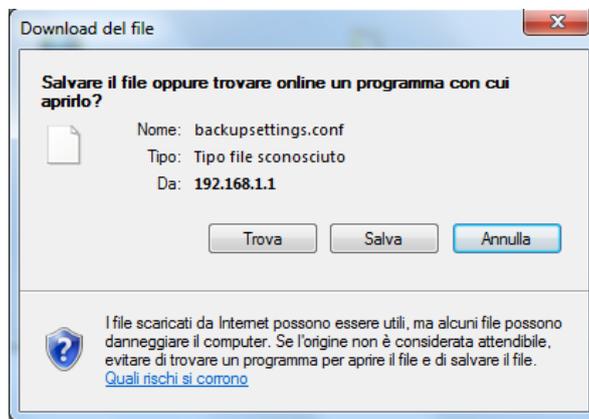


Figura 4-95

2. Fare clic su **Salva** e salvare il file nella cartella designata.

4.8.1.2 Importazione

Selezionare “**Gestione**” → “**Configurazioni**” → “**Importa**” per visualizzare la schermata in Figura 4-96.

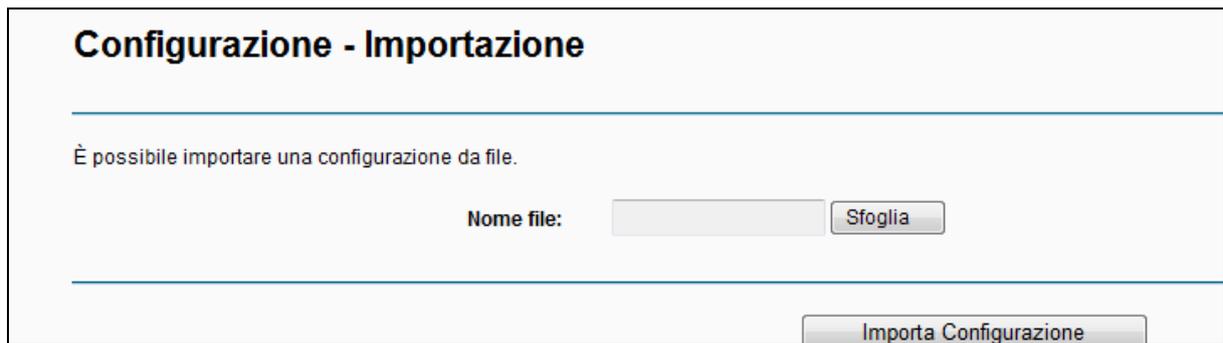


Figura 4-96

Per importare la configurazione da file procedere come segue.

1. Fare clic su **Sfoggia** e selezionare il file da importare.
2. Fare clic su **Importazione**.

Nota:

Attendere il riavvio del modem/router.

4.8.1.3 Ripristino configurazione predefinita

Selezionare “**Gestione**” → “**Impostazioni**” → “**Ripristino impostazioni predefinite**” per visualizzare la schermata in Figura 4-97.

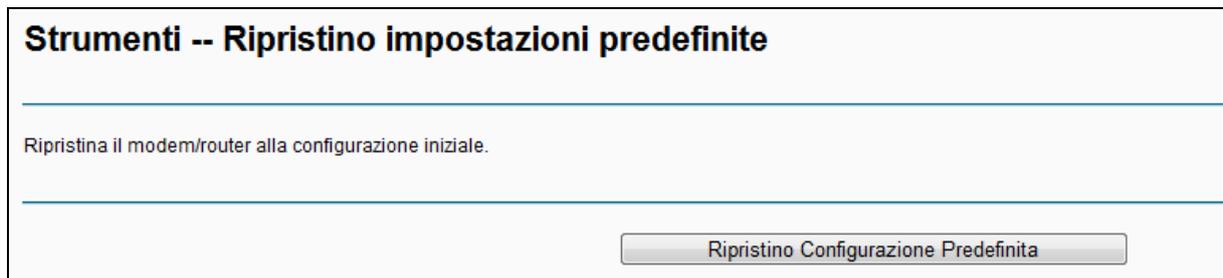


Figura 4-97

- **Ripristino Configurazione Predefinita:** Fare clic per ripristinare le impostazioni predefinite.

Nota:

Attendere il riavvio del modem/router.

Account e password: saranno ripristinate le credenziali predefinite admin / admin.

Indirizzo IP: sarà ripristinato l'IP predefinito 192.168.1.1.

4.8.2 Log di sistema

Selezionare “**Gestione**” → “**Log di sistema**” per visualizzare la schermata in Figura 4-98.

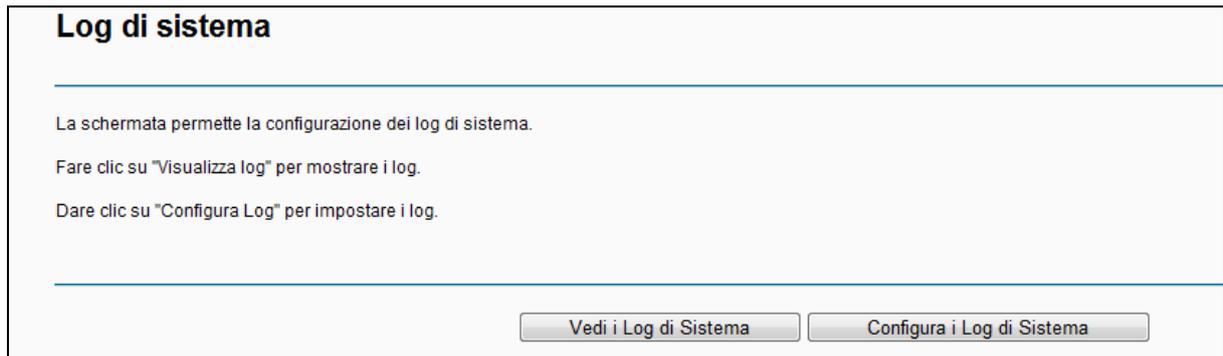


Figura 4-98

Per visualizzare il log fare clic su **Vedi i Log di Sistema** in Figura 4-99.

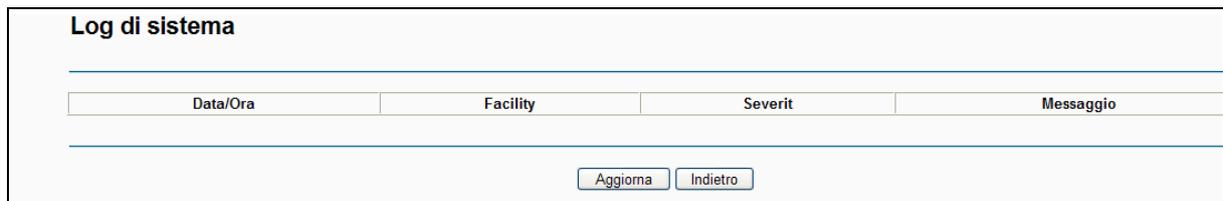


Figura 4-99

- **Aggiorna:** Fare clic per aggiornare la schermata.
- **Indietro:** Fare clic per tornare alla pagina precedente.

Per configurare il log di sistema fare clic su **Configura log** in Figura 4-100.



Figura 4-100

- **Abilita / Disabilita:** Stato di abilitazione del server log.
- **Livello log:** Saranno registrati solo gli eventi di livello pari o superiore al livello ivi specificato.
- **Livello display:** Saranno visualizzati solo gli eventi di livello pari o superiore al livello ivi specificato.
- **Modo:** Specificare se salvare gli eventi sulla memoria locale, su server remoto o su entrambi.

4.8.3 SNMP

Selezionare **“Gestione”** → **“SNMP”** per configurare l’agente SNMP.

SNMP (Simple Network Management Protocol) è il più comune protocollo per il monitoraggio e la telegestione di dispositivi di rete.

Il router integra un agente SNMP in grado di inviare eventi a trap manager SNMP, nonché di rispondere alle richieste degli stessi trap manager.

SNMP - Configurazione

SNMP (Simple Network Management Protocol) consente la lettura remota degli eventi.

Specificare i valori desiderati e fare clic su "Salva/Applica" per configurare SNMP.

SNMP Agent: Disabilita Abilita

Read Community: public

Set Community: private

Nome sistema: TP-LINK

Posizione sistema: unknown

Contatto sistema: unknown

IP trap manager: 0.0.0.0

Salva/Applica

Figura 4-101

- **SNMP Agente:** Controllo di abilitazione dell'agente.

Nota:

SNMP autentica i dispositivi tramite SNMP Community.

- **Read Community:** Community con accesso in sola lettura, il valore predefinito è "public".
- **Set Community:** Community con accesso in lettura e scrittura, il valore predefinito è "public".
- **Nome sistema:** Nome del dispositivo in uso visualizzato sul trap manager.
- **Posizione sistema:** Posizione fisica del dispositivo.
- **Contatto sistema:** Specifiche di contatto per l'amministratore del dispositivo.
- **IP trap manager:** Indirizzo IP del trap manager.

Fare clic su **Salva/Applica** per applicare le impostazioni.

4.8.4 TR-069

Selezionare "**Gestione**" → "**Client TR-069**" per visualizzare la schermata in Figura 4-102.

TR-069 (WAN Management Protocol) permette la telegestione automatizzata di numerosi dispositivi attraverso un server ACS.

Client TR-069 - Configurazione

TR-069 (WAN Management Protocol) permette ad un server Auto-Configuration (ACS) di eseguire operazioni di configurazione automatizzata e diagnostica sul modem/router. Specificare i parametri forniti e fare clic su "Salva/Applica".

Inform Disabilita Abilita

Intervallo inform:

URL ACS URL:

Nome utente ACS:

Password ACS:

Interfaccia WAN:

Mostra messaggi SOAP sulla console seriale Disabilita Abilita

Autenticazione richiesta connessione

Nome utente richiesta connessione:

Password richiesta connessione:

URL richiesta connessione:

Figura 4-102

- **Inform:** Controllo di abilitazione della funzionalità.
- **Intervallo inform:** Frequenza di inform al server ACS.
- **URL ACS URL:** URL del server ACS.
- **Nome utente ACS:** Nome utente per l'accesso al server ACS.
- **Password ACS:** Password per l'accesso al server ACS.
- **Interfaccia WAN:** Interfaccia WAN per la comunicazione con il server ACS.
- **Nome utente richiesta connessione:** Nome utente per l'accesso TR-069 al dispositivo.
- **Password richiesta connessione:** Password per l'accesso TR-069 al dispositivo.

Fare clic su **Salva/Applica** per applicare le impostazioni.

4.8.5 Ora Internet

Selezionare "**Gestione**" → "**Ora Internet**" per gestire l'orologio di sistema.

Orologio

Questa schermata permette la configurazione dell'orologio di sistema.

Data/Ora: Thu Jan 1 00:07:32 1970
 Data/Ora dispositivo in uso: Fri Mar 21 10:38:52 2014

Configura data/ora

Data (Y/M/D):
 Ora (H:M:S):

Sincronizza automaticamente con time server

NTP server 1:
 NTP server 2:
 NTP server 3:
 NTP server 4:
 NTP server 5:
 Fuso orario:

Figura 4-103

4.8.6 Controllo accessi

- Controllo accessi
- Password
- Accesso remoto

4.8.6.1 Password

Selezionare **“Gestione”** → **“Controllo accessi”** → **“Password”** per configurare le credenziali di accesso all’interfaccia di gestione.

Controllo accesso -- Password

Il modem/router può essere gestito attraverso 3 account: admin, support e user.

L'account "admin" ha permessi totali.

L'account "support" può essere utilizzato da un servizio di supporto tecnico per la diagnostica.

L'account "user" può solamente visualizzare la configurazione e le statistiche, nonchè aggiornare il firmware del router.

Specificare una password fino a 16 caratteri e fare clic su "Salva/Applica".

Username:

Vecchia password:

Nuova password:

Conferma nuova password:

Figura 4-104

Per cambiare una password procedere come segue.

1. Selezionare l’utente da modificare.

2. Specificare la vecchia password.
3. Specificare la nuova password e confermarla.

Fare clic su **Salva/Applica** per applicare la modifica.

Nota:

1. L'utente "admin" ha accesso illimitato, l'utente "support" ha le autorizzazioni necessarie per consentire le operazioni di risoluzione dei problemi ad un servizio di supporto tecnico, mentre l'utente "user" può solamente visualizzare le informazioni.
2. Sono supportate password fino a 16 caratteri.

4.8.6.2 Accesso remoto

Selezionare **"Gestione"** → **"Controllo accessi"** → **"Accesso remoto"** per configurare l'accesso remoto alla console.

Figura 4-105

- **Web:** Selezionare per abilitare l'accesso all'interfaccia web.
- **Telnet:** Selezionare per abilitare l'accesso Telnet.
- **ICMP (ping):** Selezionare per abilitare la risposta al ping da interfaccia WAN.

Fare clic su **Salva/Applica** per salvare le impostazioni.

4.8.7 Aggiornamento

Selezionare **"Gestione"** → **"Aggiornamento firmware"** per visualizzare la schermata in Figura 4-106.

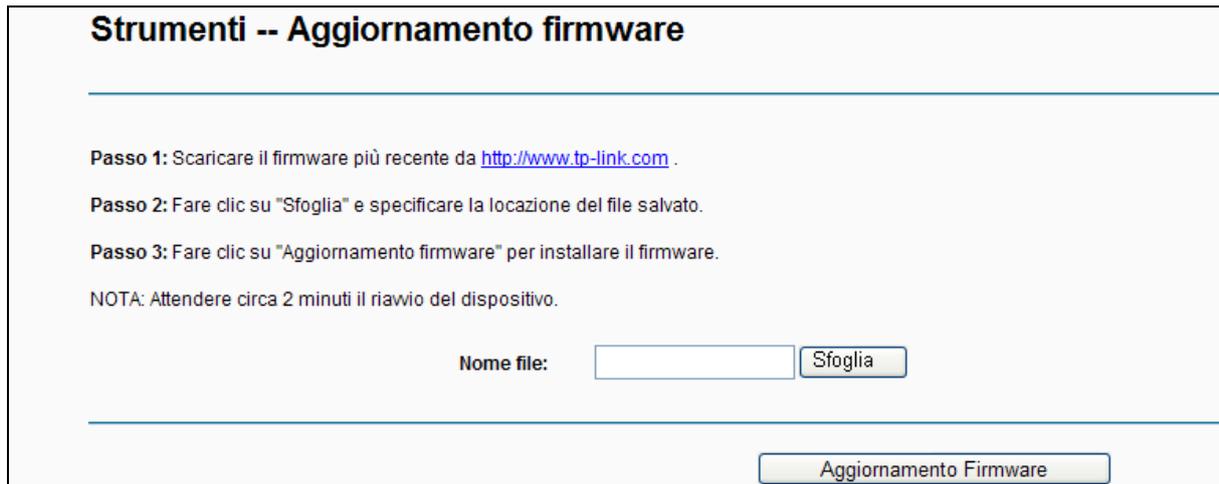


Figura 4-106

- **Sfoglia:** Fare clic per selezionare il firmware da caricare.
- **Aggiornamento Firmware:** Fare clic per eseguire l'aggiornamento.

Per aggiornare il modem/router procedere come segue.

1. Scaricare il firmware più recente da <http://www.tp-link.com> .
2. Estrarre il file contenente il firmware dell'archivio .zip scaricato.
3. Fare clic su **Sfoglia** per selezionare il file estratto contenente il firmware.
4. Fare clic su **Aggiornamento Firmware**.

Nota:

1. Si consiglia di esportare una copia della configurazione prima dell'aggiornamento.
2. Non eseguire alcuna operazione sul modem/router durante l'aggiornamento.
3. Attendere il riavvio automatico a conclusione del processo.

4.8.8 Riavvio

Selezionare "**Gestione**" → "**Riavvio**" per visualizzare la schermata in Figura 4-130 e procedere al riavvio.

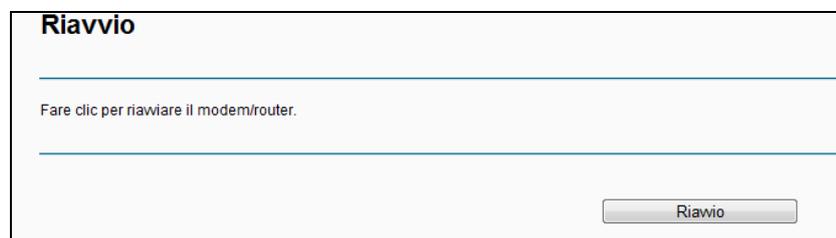


Figura 4-107

4.9 Logout

Selezionare "**Logout**" per scollegarsi dall'interfaccia web.

Appendice A: Specifiche

| Generale | |
|------------------------|---|
| Standard | ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5, IEEE 802.3, IEEE 802.3u, IEEE 802.11b , IEEE 802.11g , 802.11n |
| Protocolli | TCP/IP, IPoA, PPPoA, PPPoE, SNTP, HTTP, DHCP, ICMP, NAT |
| Porte | LAN/WAN: 4 x RJ45 10/100Mbps |
| | DSL: 1 x RJ11 |
| Cablaggio | 10BASE-T: UTP categoria 3, 4, 5 (fino a 100m) EIA/TIA-568 100Ω STP (fino a 100m) |
| | 100BASE-TX: UTP categoria 5, 5e (fino a 100m) EIA/TIA-568 100Ω STP (fino a 100m) |
| LED | Power, ADSL, Internet, WLAN, WPS, 1,2,3,4(LAN), |
| Sicurezza ed emissioni | FCC, CE |

| Wireless | |
|----------------------|--|
| Frequenze | 2.4~2.4835GHz |
| Data Rate | 11n: fino a 300Mbps 11g: 54/48/36/24/18/12/9/6Mbps 11b: 11/5.5/2/1Mbps |
| Espansione frequenza | DSSS (Direct Sequence Spread Spectrum) |
| Modulazione | DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM |
| Sicurezza | WEP/WPA/WPA2/WPA2-PSK/WPA-PSK |
| Sensibilità @PER | 270M: -62dBm@10% PER 130M: -64dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER |

| Ambiente | |
|-------------|---|
| Temperatura | Operativa: 0°C~40°C |
| | Stoccaggio: -40°C~70°C |
| Umidità | Operativa: 10% ~ 90% RH, Non-condensing |
| | Stoccaggio: 5% ~ 90% RH, Non-condensing |

Appendice B: Risoluzione dei problemi

T1. Come posso ripristinare il modem/router alle impostazioni predefinite?

Inserire per 10 secondi un oggetto appuntito nel foro **RESET** su pannello posteriore del prodotto.

 **Nota:**

Tutti i parametri configurati andranno persi e sarà necessario configurare nuovamente il modem router.

T2. Cosa posso fare se dimentico la password di gestione?

- 1) Occorre ripristinare il modem router alle impostazioni predefinite. Per ulteriori informazioni fare riferimento a **T1**.
- 2) Nome utente e password predefiniti sono: **admin, admin**.
- 3) Provare a riconfigurare il modem router seguendo le istruzioni in [3.2 Guida rapida all'installazione](#).

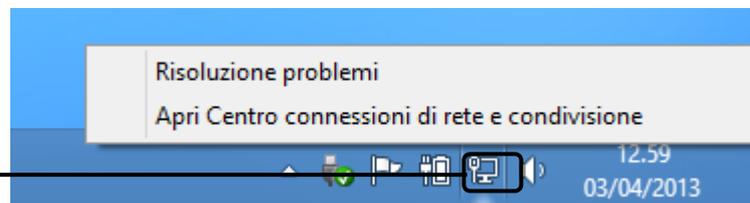
T3. Cosa posso fare se non riesco ad accedere alla consolle di gestione web?

- 1) Secondo il sistema operativo in uso, configurare l'indirizzo IP del computer come segue.

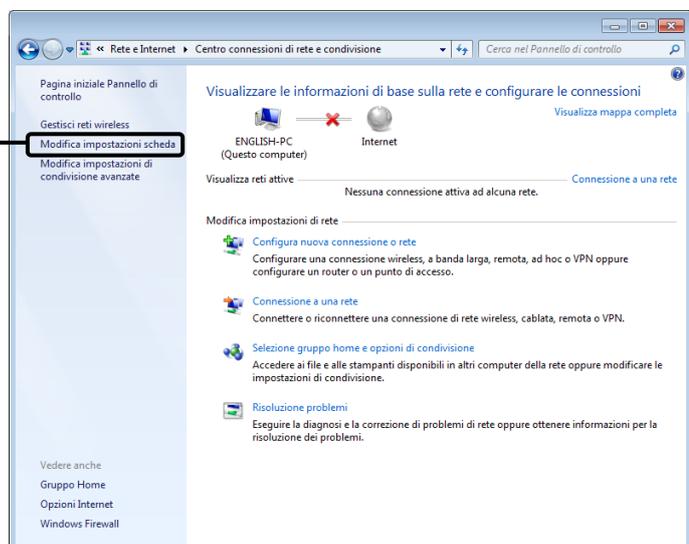
Per Windows® 7 / 8

Clic col tasto destro sull'icona della rete vicino all'orologio di sistema, nell'angolo basso destro dello schermo.

Selezionare quindi **Apri Centro connessioni di rete e condivisione**.

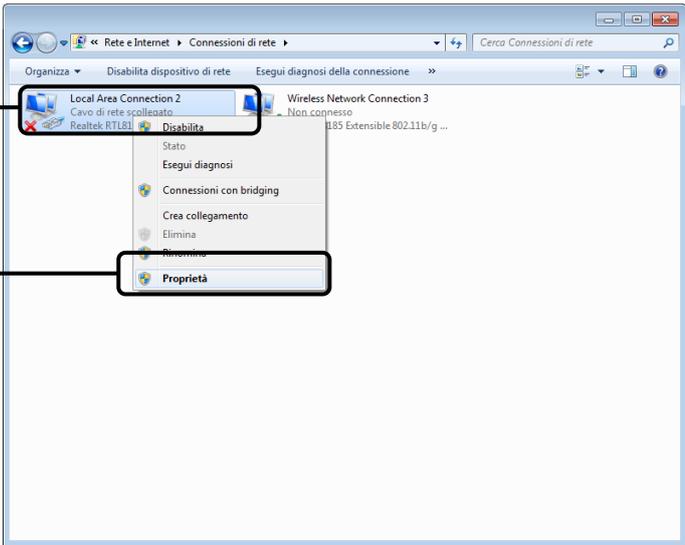


Fare clic su **Modifica impostazioni scheda**

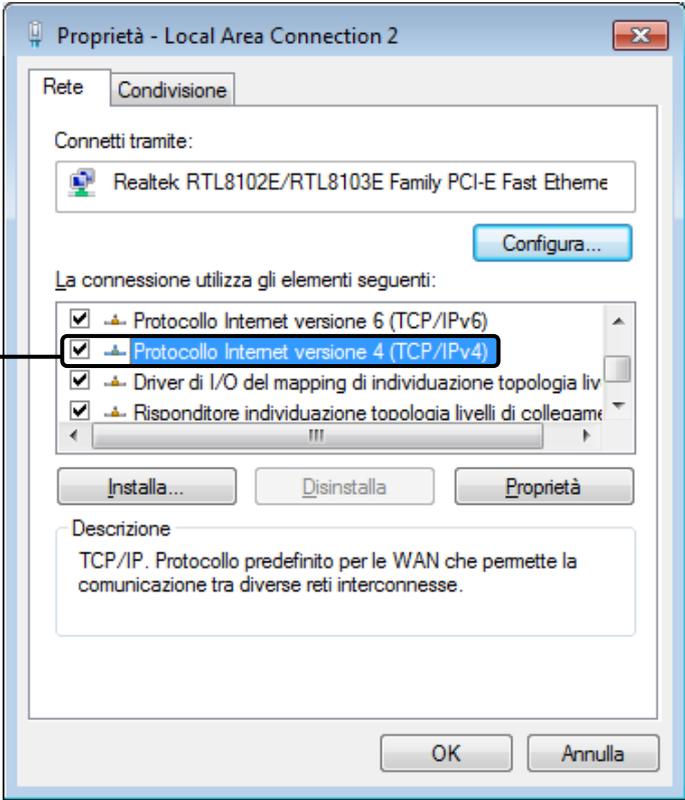


Fare clic col tasto destro su **Connessione alla rete locale LAN**

Clic su **Proprietà**



Doppio clic su **Protocollo Internet versione 4 (TCP/IPv4)**



Selezionare automaticamente un indirizzo IP **Ottieni un indirizzo IP**

Selezionare automaticamente un indirizzo server DNS **Ottieni indirizzo server DNS automaticamente**

Clic su OK

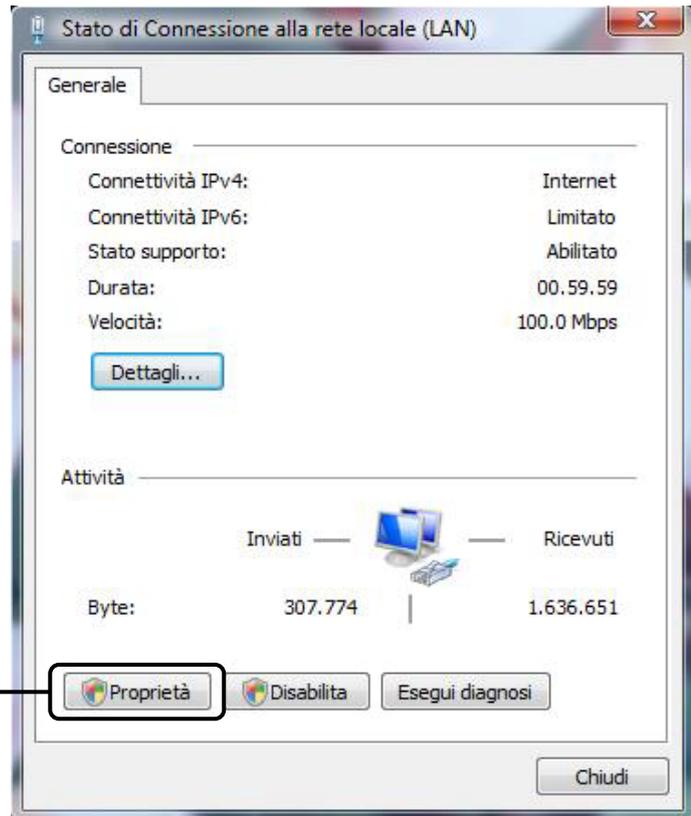
Per Windows® Vista™

Facendo clic su **Start > Impostazioni > Pannello di controllo**, viene visualizzata questa pagina.

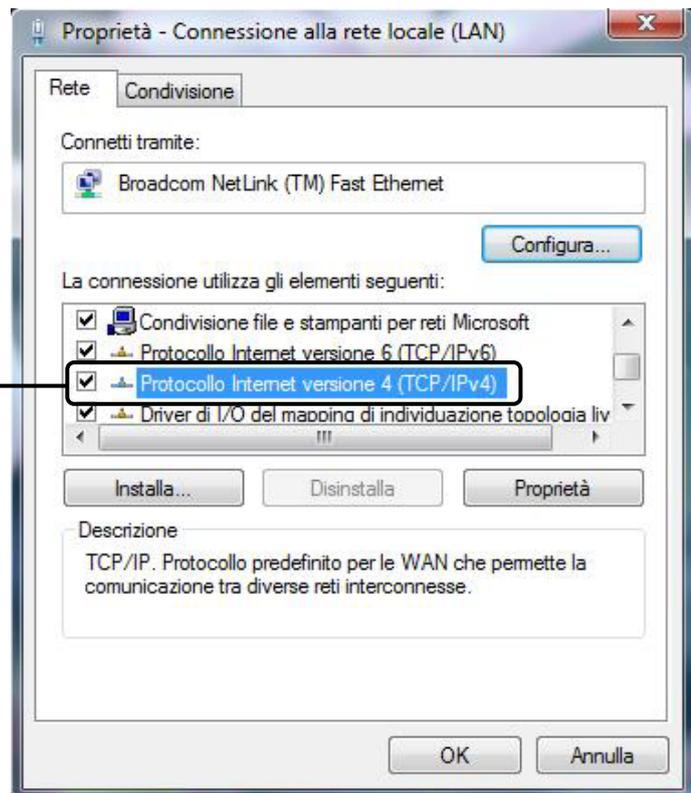
Clic su Visualizza stato della rete e attività

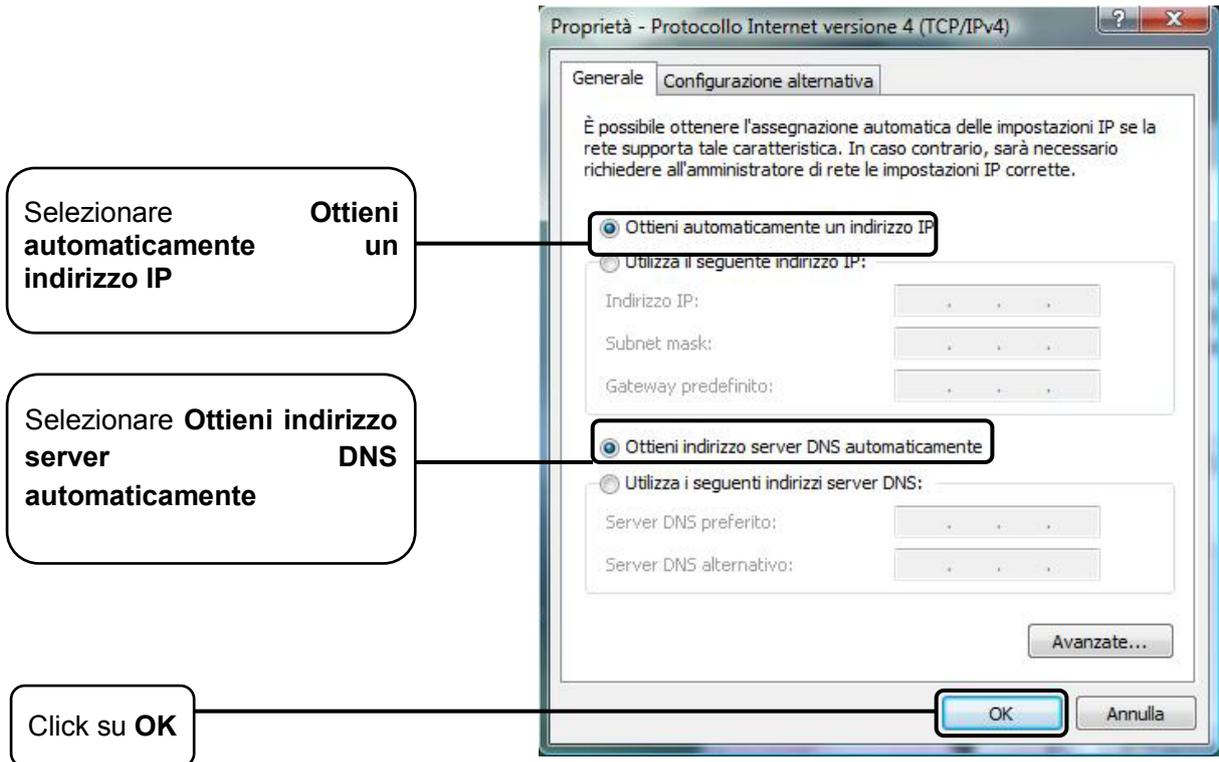
Clic su Visualizza stato

Clic su **Proprietà**



Doppio clic su **Protocollo Internet versione 4 (TCP/IPv4)**





Per Windows® XP

Clic su **Start > Pannello di controllo**, viene visualizzata questa pagina.



Clic su **Connessioni di rete**

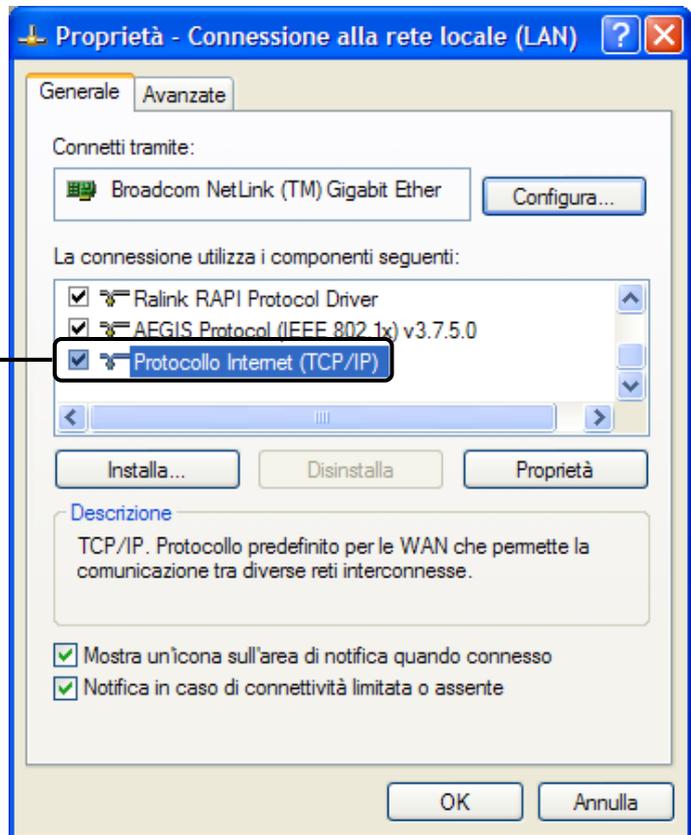


Clic col tasto destro su **Connessione alla rete locale (LAN)**



Clic su **Proprietà**

Doppio clic su **Protocollo Internet (TCP/IP)**



Proprietà - Protocollo Internet (TCP/IP)

Generale **Configurazione alternativa**

È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.

Ottieni automaticamente un indirizzo IP

Utilizza il seguente indirizzo IP:

Indirizzo IP:

Subnet mask:

Gateway predefinito:

Ottieni indirizzo server DNS automaticamente

Utilizza i seguenti indirizzi server DNS:

Server DNS preferito:

Server DNS alternativo:

Avanzate...

OK Annulla

Selezionare automaticamente un indirizzo IP

Selezionare indirizzo server DNS automaticamente

Clic su OK

Proprietà - Connessione alla rete locale (LAN)

Generale **Avanzate**

Connetti tramite:

Broadcom NetLink (TM) Gigabit Ether

La connessione utilizza i componenti seguenti:

- Ralink RAPI Protocol Driver
- AEGIS Protocol (IEEE 802.1x) v3.7.5.0
- Protocollo Internet (TCP/IP)**

Installa... Disinstalla Proprietà

Descrizione

TCP/IP. Protocollo predefinito per le WAN che permette la comunicazione tra diverse reti interconnesse.

- Mostra un'icona sull'area di notifica quando connesso
- Notifica in caso di connettività limitata o assente

OK Annulla

Clic su OK

Per Mac™ OS X

- Fare clic su **Apple** nell'angolo superiore sinistro.
- Selezionare "**Preferenze di sistema -> Network**".
- Selezionare
 - i. **Airport** dal menu di sinistra se si desidera utilizzare la connessione wireless.
 - ii. **Ethernet** dal menu di sinistra se si desidera utilizzare la connessione cablata.
- Selezionare **Avanzate**.
- Nella scheda **TCP/IP**, sezione **Configura IPv4** selezionare **Utilizza DHCP**.

Fare clic su **OK** per applicare la configurazione.

Riprovare ad accedere all'interfaccia web di gestione. Se il problema persiste, ripristinare le impostazioni predefinite e riconfigurare il router come descritto in [3.2 Guida rapida all'installazione](#). Contattare il Supporto Tecnico in caso di difficoltà.

T4. Cosa posso fare se non riesco ad accedere ad Internet?

- 1) Verificare che tutti i cavi siano perfettamente connessi.
- 2) Verificare l'accesso alla console Web. Nel caso in cui non fosse possibile accedere fare riferimento a **T3**.
- 3) Verificare con il provider ISP la correttezza dei parametri VPI/VCI, modalità di connessione, modalità d'incapsulamento, nome utente, password. In caso di errori, riconfigurare il modem router.
- 4) Se il problema persiste ripristinare le impostazioni predefinite e riconfigurare il modem router facendo riferimento a [4.1 Accesso](#).
- 5) Contattare il Supporto Tecnico in caso di ulteriore difficoltà.

Appendice C: Supporto Tecnico

- Per maggior aiuto nella Risoluzione dei Problemi collegarsi ad:
<http://www.tp-link.it/support/>
- Per il download degli ultimi firmware, driver, utility e guide utente:
<http://www.tp-link.it/support/download/>
- È inoltre possibile contattare il Supporto Tecnico ai seguenti recapiti:

Italiano

E-mail Supporto Tecnico:

<http://www.tp-link.it/support/contact>

Hotline Supporto Tecnico:

+39 0230519020 (Lu-Ve 9:00-13:00 14:00-18:00)

Internazionale

E-mail: support@tp-link.com

Tel: +86 755 26504400 (24/24 7/7)

TP-LINK TECHNOLOGIES CO., LTD.

Building 24 (floors 1, 3, 4, 5), and 28 (floors 1-4) Central Science and
Technology Park, Shennan Rd, Nanshan, Shenzhen, China