

# TP-LINK®

## User Guide

### TD-W8960N

### 300Mbps Wireless N ADSL2+ Modem Router



## 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 © 2013 TP-LINK TECHNOLOGIES CO., LTD. Tutti i diritti riservati.

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

## 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-Ålesund
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: **300Mbps Wireless N ADSL2+ Modem Router**

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

**ETSI EN 300 328 V1.7.1: 2006**

**ETSI EN 301 489-1 V1.9.2:2011& ETSI EN 301 489-17 V2.1.1:2009**

**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: 2013

# INDICE DEI CONTENUTI

<b>Contenuto della confezione</b> .....	<b>1</b>
<b>Capitolo 1.Introduzione</b> .....	<b>2</b>
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
<b>Capitolo 2.Installazione hardware</b> .....	<b>7</b>
2.1 Requisiti di sistema .....	7
2.2 Ambiente d'installazione .....	7
2.3 Collegamento del modem/router.....	7
<b>Capitolo 3.Guida rapida all'installazione</b> .....	<b>9</b>
3.1 Configurazione computer .....	9
3.2 Guida rapida all'installazione .....	10
<b>Capitolo 4.Configurazione software</b> .....	<b>14</b>
4.1 Accesso.....	14
4.2 Stato.....	14
4.3 Quick Setup.....	14
4.4 Configurazione avanzata .....	15
4.4.1 Interfaccia layer 2.....	15
4.4.2 WAN.....	17
4.4.3 MAC Clone.....	24
4.4.4 LAN .....	25
4.4.5 NAT .....	28
4.4.6 Sicurezza .....	31
4.4.7 Parental Control .....	34
4.4.8 QoS .....	36
4.4.9 Bandwidth Control.....	38
4.4.10 Routing.....	40
4.4.11 DNS.....	43
4.4.12 DSL .....	44

4.4.13 UPnP .....	45
4.4.14 Interface Grouping .....	45
4.4.15 Tunnel IP .....	47
4.4.16 IPSec.....	49
4.4.17 Multicast .....	51
4.5 Wireless .....	52
4.5.1 Wireless .....	52
4.5.2 Sicurezza .....	53
4.5.3 Timer .....	60
4.5.4 Filtro MAC .....	61
4.5.5 Bridge wireless.....	62
4.5.6 Avanzate .....	63
4.5.7 Dispositivi collegati.....	64
4.6 Rete guest.....	64
4.6.1 Rete guest.....	64
4.6.2 Dispositivi collegati.....	65
4.7 USB.....	66
4.7.1 Storage USB .....	66
4.7.2 Account utente .....	67
4.7.3 Condivisione storage .....	67
4.7.4 Server FTP.....	69
4.7.5 Media Server.....	70
4.7.6 Print Server .....	71
4.8 Diagnostica .....	72
4.9 Gestione.....	72
4.9.1 Configurazione .....	73
4.9.2 Log di sistema.....	74
4.9.3 SNMP.....	76
4.9.4 TR-069 .....	76
4.9.5 Ora Internet.....	77
4.9.6 Amministrazione.....	78
4.9.7 Aggiornamento.....	79
4.9.8 Riavvio .....	80
4.10Logout .....	80
<b>Appendice A: Specifiche.....</b>	<b>81</b>

<b>Appendice B: Risoluzione dei problemi .....</b>	<b>82</b>
<b>Appendice C:Supporto Tecnico .....</b>	<b>90</b>

# 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)
- USB Storage Sharing, Print Server, FTP Server, Media Server
- 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 <a href="#">Nota 1</a> 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 <a href="#">Nota 2</a> 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.
🔌 (USB)	Acceso	Un dispositivo è connesso alla porta USB.
	Lampeggiante	Trasmissione dati in corso.
	Spento	Nessun dispositivo connesso alla porta USB.

 (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

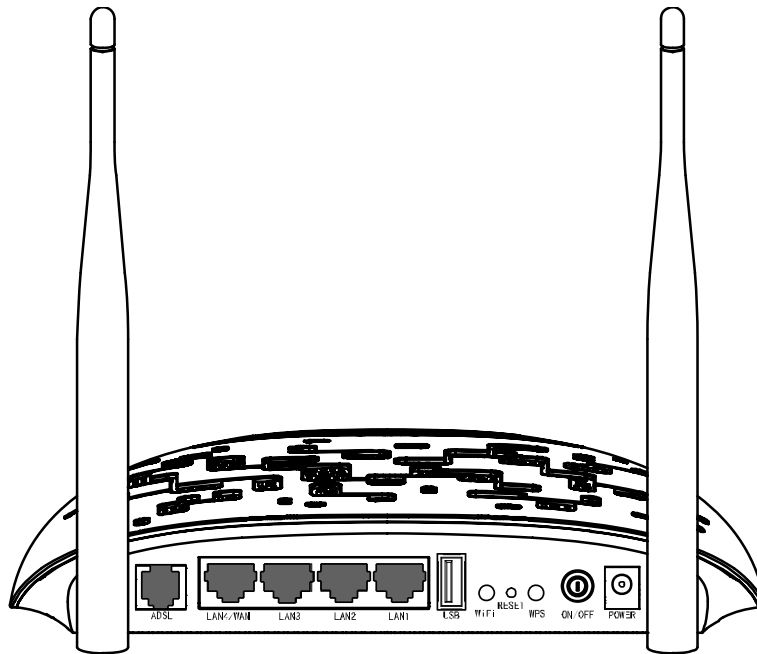


Figura 1-2

- **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 5 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.
    - **USB:** La porta USB connette dispositivi storage o stampanti.

- **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, far 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 riparato 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 specifiche:

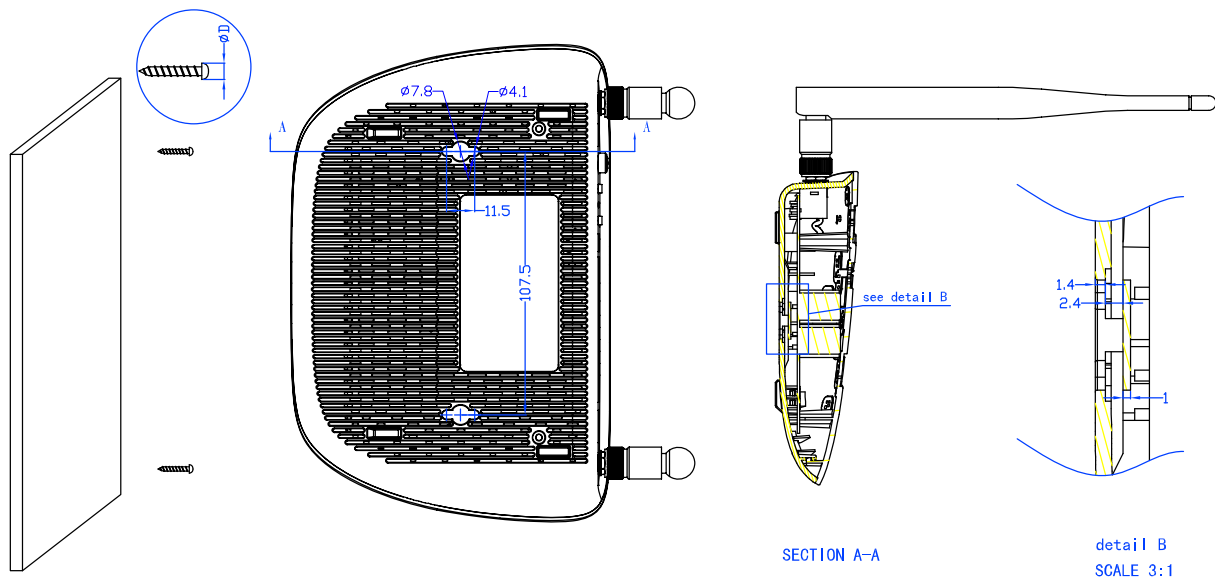


Figura 2-1 Installazione a muro

## 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.

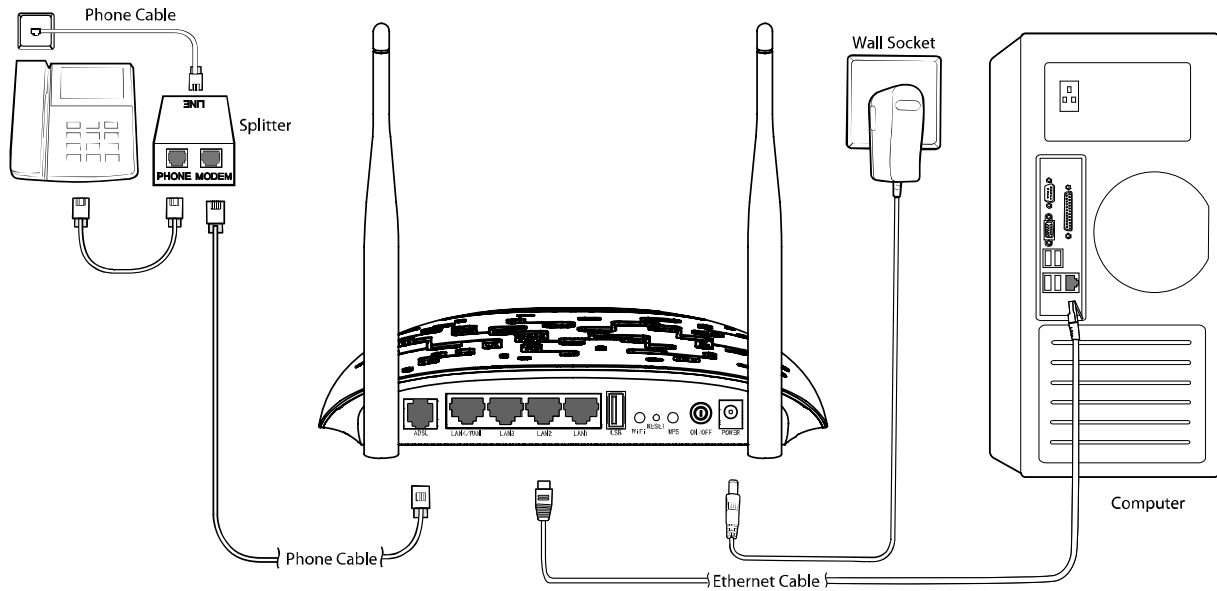


Figura 2-2

## 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 **Run (Esegui)** (o digitare Win+R), digitare **cmd** e premere **Enter (Invio)**. Digitare **ping 192.168.1.1** sulla prossima schermata e premere **Enter (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
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
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 192.168.1.2 e 192.168.1.254.

## 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 3-9, fare clic su **Quick Setup**.

**Device Info**

---

**Version Info**

<b>Firmware Version:</b>	1.0.1 Build 130604 Rel.36480
<b>Hardware Version:</b>	TD-W8960N V5 0x00000001
<b>System Running time:</b>	0Day(s) 01:20:45

---

**LAN Info**

IPv4	<b>LAN IP Address:</b>	192.168.1.1
	<b>LAN MAC Address:</b>	02:10:18:01:00:01
IPv6	<b>IPv6 Address:Prefix Length:</b>	NULL
	<b>Auto Configuration:</b>	RADVD&DHCP6

---

**ADSL Info**

<b>Line State:</b>	Down
<b>Line Rate - Upstream (Kbps):</b>	0
<b>Line Rate - Downstream (Kbps):</b>	0

---

**Internet Info**

<b>Notice:</b>	There is no Route Interface.
<b>Shortcut:</b>	Click <a href="#">here</a> to do Quick Setup. Click <a href="#">here</a> to view all WAN interface's status and troubleshooting information.

Figura 3-5

3. Selezionare poi il tipo di connessione WAN prescritto, quindi fare clic su **Next (Avanti)**.

**Quick Setup - WAN Configurations**

---

Please choose the Wan type for Internet access.

**Choose WAN Type:**

- ADSL WAN For ADSL(Telephone line/RJ11) Service
- Ethernet WAN For Ethernet(RJ45) Service

---

Enable IPv6 for this service

---

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 **Next (Avanti)** per continuare (la presente guida mostra, a titolo esemplificativo, la configurazione in modalità PPPoE).

**Quick Setup - WAN Configurations**

Country: Other

ISP: Other

VPI/VCI: 8 / 35 ([0-255] / [32-65535])

Encapsulation Mode: LLC/SNAP-BRIDGING (optional)

WAN Link Type: PPPoE(PPP over Ethernet)

PPP Username: 1

PPP Password: ●

PPPoE Service Name: 1 (optional)

MTU (bytes): 1480 (optional)

Back Skip Wan Next

Figura 3-7

 **Nota:** Se il provider in uso non è elencato fare selezionare **Other (Altro)** e specificare manualmente i parametri.

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

**Quick Setup - WAN Configurations**

Ethernet WAN Port: LAN4/WAN

WAN Link Type: PPPoE(PPP over Ethernet)

PPP Username:

PPP Password:

PPPoE Service Name: (optional)

MTU (bytes): 1480 (optional)

Back Skip Wan Next

Figura 3-8

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

**Quick Setup - Wireless Configurations**

**Enable Wireless:**

You can configure SSID and your WLAN Authentication type.

**Wireless Network Name:**  (Also called SSID)

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

**Network Authentication:**  ▼

**Wireless Network Key:**  (Also called WPA Pre-Shared Key)  
 (You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.)

Figura 3-9

- Verificare tutti i parametri e fare clic su **Confirm (Conferma)** per applicare la configurazione.

**Quick Setup - Summary**

**WAN Configurations**

<b>WAN Type:</b>	ADSL WAN
<b>Layer2 Information:</b>	8035 LLC/SNAP-BRIDGING
<b>WAN Link Type:</b>	PPPoE
<b>PPP Username:</b>	1
<b>PPP Password:</b>	1
<b>PPP MTU:</b>	1480

**Note1:** Some WAN Connection(s) or Layer2 interface(s) may be replaced by new one!  
**Note2:** The Virtual Server Rules of some WAN Connection(s) may be deleted!

**Wi-Fi Configurations**

<b>Wireless Network Name:</b>	TP-LINK_010001
<b>Network Authentication:</b>	WPA2-Personal
<b>Wireless NetWork Key:</b>	1234567890

Figura 3-10

# Capitolo 4. Configurazione software

## 4.1 Accesso



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

## 4.2 Stato

Selezionare “**Status (Stato)**” per visualizzare le informazioni relative allo stato del sistema.

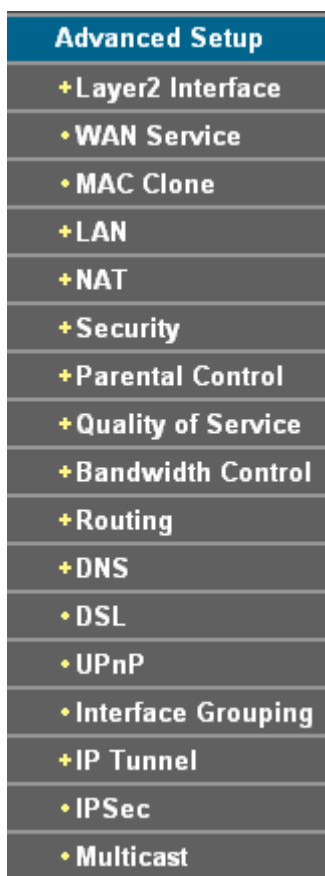
Device Info	Device Info	
• Summary	<b>Version Info</b>	
• WAN	<b>Firmware Version:</b>	1.0.1 Build 130704 Rel.61797
+ Statistics	<b>Hardware Version:</b>	TD-W8960N V5 0x00000001
• Route	<b>System Running time:</b>	0Day(s) 00:35:09
• ARP	<b>LAN Info</b>	
• DHCP	<b>LAN IP Address:</b>	192.168.1.1
Quick Setup	<b>LAN MAC Address:</b>	02:10:18:01:00:01
Advanced Setup	<b>IPv6 Address Prefix Length:</b>	NULL
Wireless	<b>Auto Configuration:</b>	RADVD&DHCPv6
Guest Network	<b>ADSL Info</b>	
Quick Setup	<b>Line State:</b>	Down
Advanced Setup	<b>Line Rate - Upstream (Kbps):</b>	0
Wireless	<b>Line Rate - Downstream (Kbps):</b>	0
Guest Network	<b>Internet Info</b>	
Wireless	<b>Notice:</b>	There is no Route Interface.
Guest Network	<b>Shortcut:</b>	Click <a href="#">here</a> to do Quick Setup. Click <a href="#">here</a> to view all WAN interface's status and troubleshooting information.
USB Settings		
Diagnostics		
Management		
Logout		

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 layer 2**” per specificare il tipo d’interfaccia.

- **ATM Interface (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)
- **ETH Interface (Interfaccia ETH):** TD-W8960N opera come router Ethernet tramite porta WAN RJ45.

#### 4.4.1.1 Interfaccia ATM

Selezionare “**Advanced Setup (Configurazione avanzata) (Configurazione avanzata)**” → “**Interfaccia layer**” → **ATM Interface (Interfaccia ATM)**”.

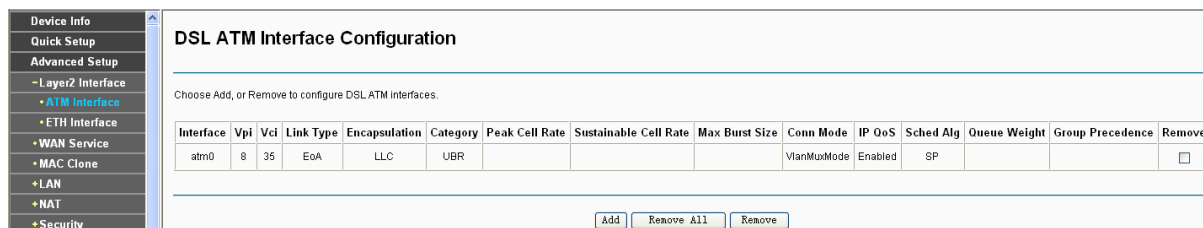


Figura 4-2

- **Remove (Elimina):** Selezionare le entrate 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.

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

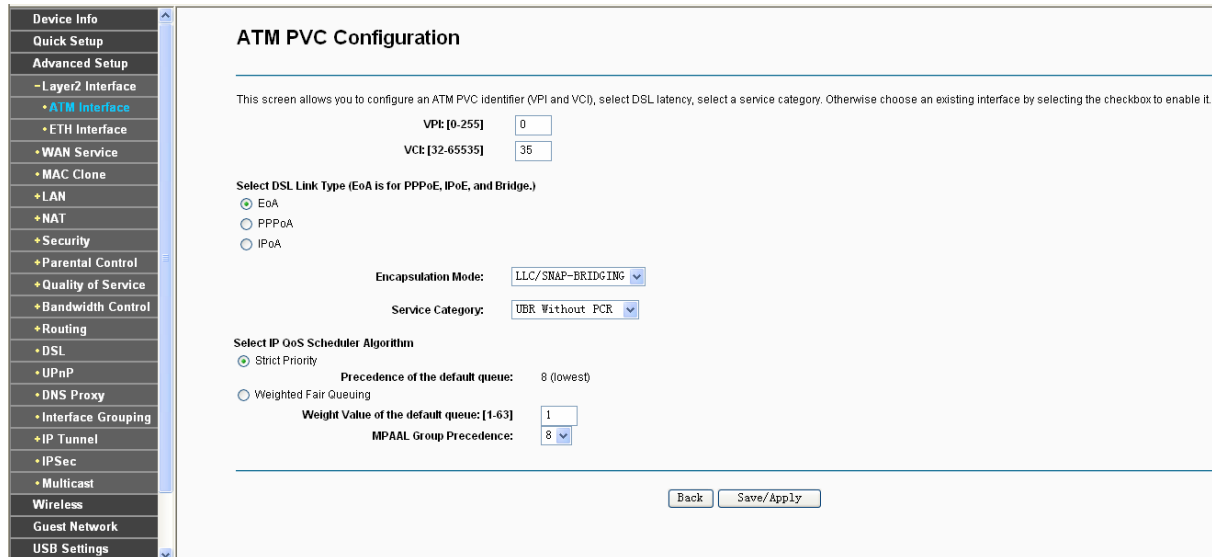


Figura 4-3

- **VPI/VCI:** Specificare i valori prescritti dal provider ISP.
- **DSL Link Type (Modalità di connessione):** Selezionare la modalità prescritta fra **EoA** (PPPoE, IPoE, e bridge), **PPPoA** ed **IPoA**.
- **Encapsulation Mode (Modalità d'incapsulamento):** Selezionare la modalità prescritta dal provider ISP.
- **Service Category (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 “**Advanced Setup (Configurazione avanzata) (Configurazione avanzata)**” → “**Layer2 Interface (Interfaccia layer 2)**” → “**ETH Interface (Interfaccia ETH)**”.

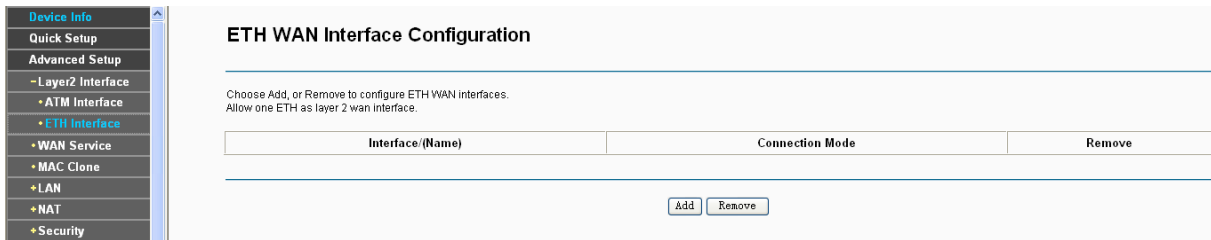


Figura 4-4

**Nota:**

È necessario abilitare la porta ETH in “Advanced Setup (Configurazione avanzata) (Configurazione avanzata)” → “LAN Ports (LAN)”.

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

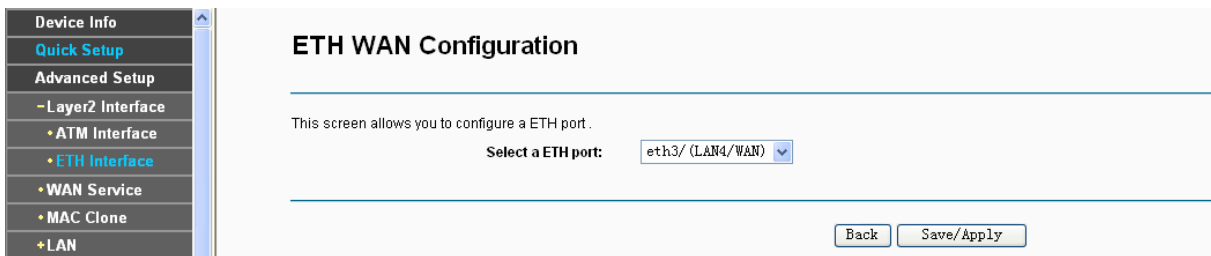


Figura 4-5

➤ **ETH port (Porta ETH):** Selezionare la porta da utilizzare come WAN.

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

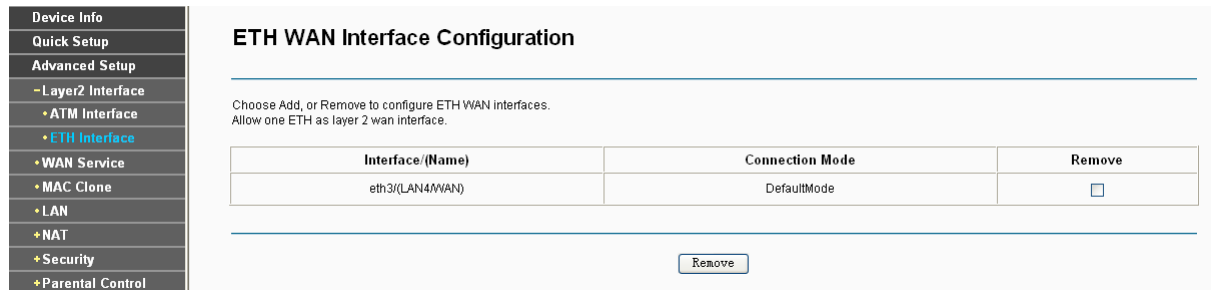


Figura 4-6

➤ **Remove (Elimina):** Selezionare le entrate da eliminare e fare clic per rimuoverle.

**Nota:**

Solo una ETH può essere configurata come WAN layer 2.

### 4.4.2 WAN

Selezionare “Advanced Settings (Configurazione avanzata)” → “WAN Service (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.



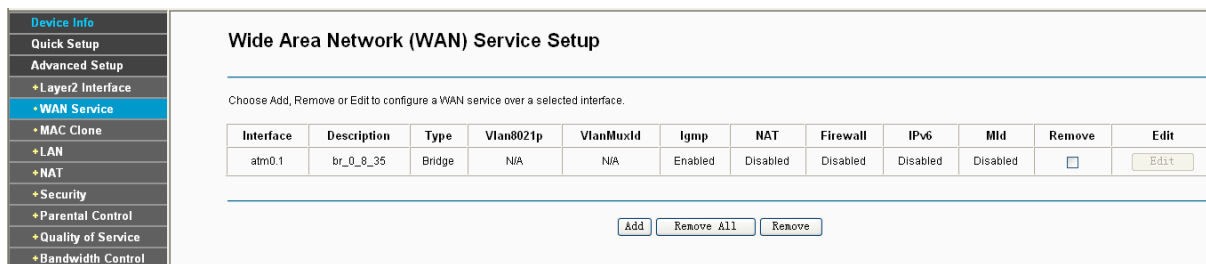


Figura 4-7

#### 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 **Add (Aggiungi) (Aggiungi)** come in Figura 4-7 per mostrare la schermata in Figura 4-8. Fare clic su **Next (Avanti)**.

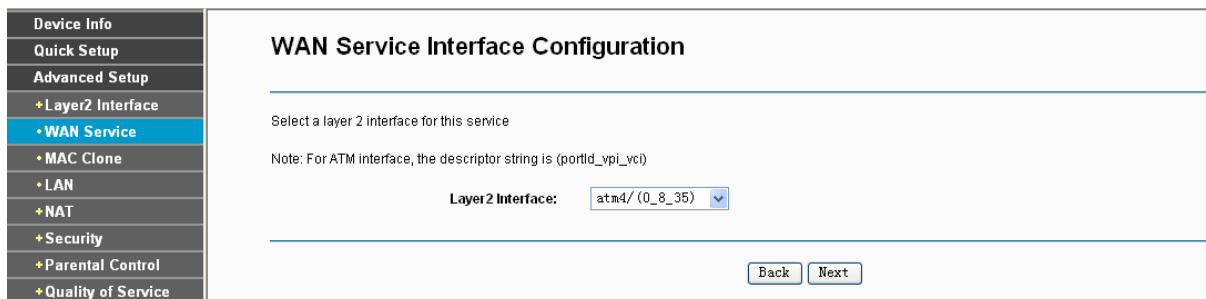


Figura 4-8

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

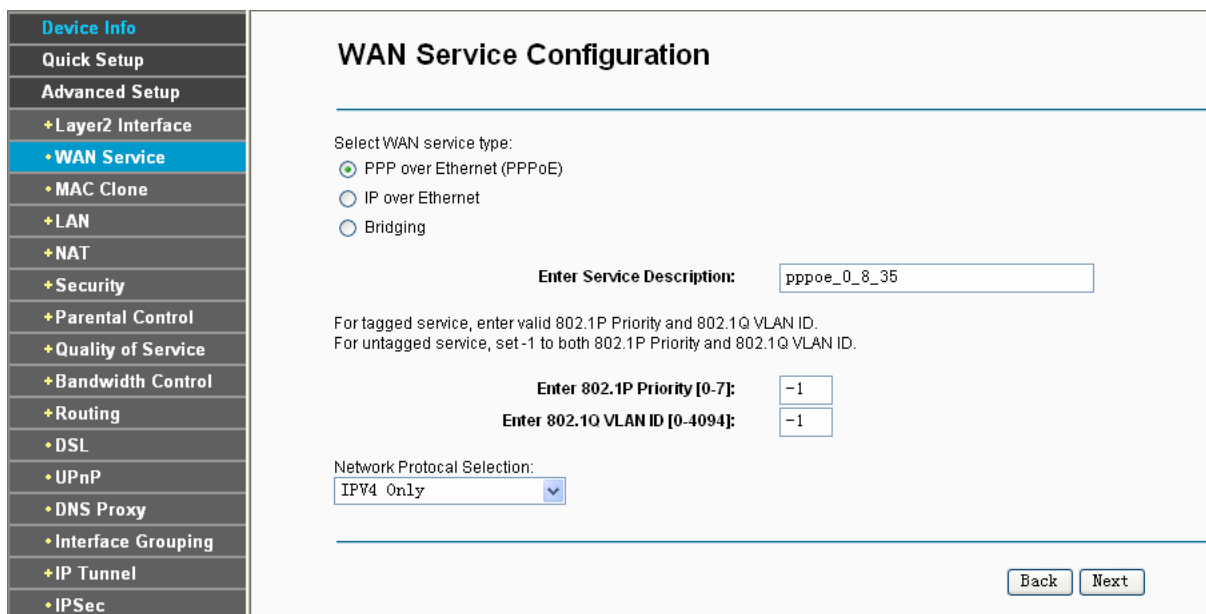


Figura 4-9

#### 4. Specificare i parametri richiesti e fare clic su **Next (Avanti)**.

The screenshot shows the 'PPP Username and Password' configuration page. On the left is a sidebar menu with 'WAN Service' selected. The main area contains the following fields and options:

- PPP Username:** 1234567890
- PPP Password:** [Masked]
- PPPoE Service Name:** [Empty]
- Authentication Method:** AUTO (dropdown menu)
- MTU (bytes):** 1480 (The default is 1480, do not change unless necessary.)
- Advanced Options (checkboxes):**
  - Enable Fullcone NAT
  - Dial on demand (with idle timeout timer)
  - PPP IP extension
  - Use Static IPv4 Address
  - Enable PPP Debug Mode
  - Bridge PPPoE Frames Between WAN and Local Ports
- Multicast Proxy:**
  - Enable IGMP Multicast Proxy

Navigation buttons: Back, Next

Figura 4-10

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

#### **Nota:**

Contattare il provider ISP in mancanza delle credenziali.

- **MTU (byte):** dimensione massima del pacchetto. Selezionare questa opzione per impostare un valore personalizzato se richiesto dal provider ISP.
- **Enable Fullcone NAT (Abilita NAT fullcone):** Tipo di NAT alternativo al tradizionale.
- **Dial on demand (with idle timeout timer) (Connessione on demand (con timeout inattività):** 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.
- **PPP IP extension (Estensione IP PPP):** Selezionare se il provider ISP lo richiede per trasferire l'IP pubblico ad un dispositivo.
- **Use Static IPv4 Address (Utilizza indirizzo IPv4 statico):** Selezionare se il provider ISP prescrive dei valori d'indirizzamento statici.
- **Enable PPP Debug Mode (Abilita debug PPP):** Selezionare per registrare ogni evento PPP nel log di sistema.
- **Bridge PPPoE Frames Between WAN and Local Ports (Supporto connessioni bridge):** Selezionare per consentire ai dispositivi in LAN di effettuare connessioni PPP dirette.
- **Enable IGMP Multicast Proxy:** 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 **Next (Avanti)**.

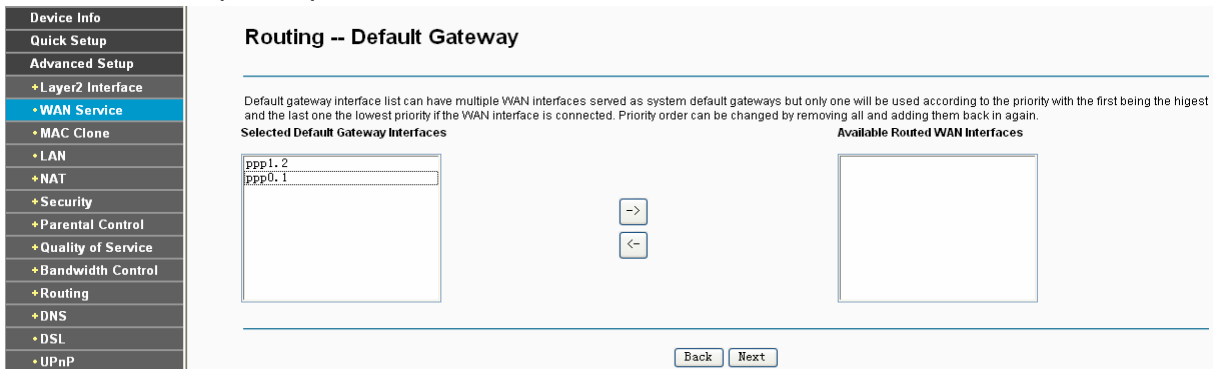


Figura 4-11

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

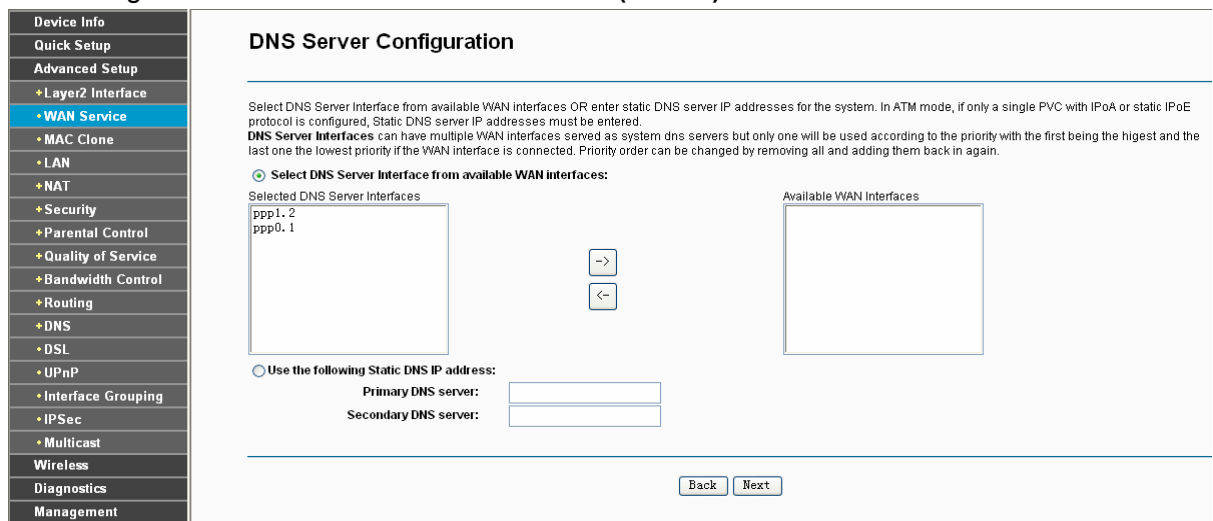


Figura 4-12

- **Select DNS Server Interface from available WAN Interfaces (Selezione interfaccia WAN server DNS):** Specificare l'interfaccia WAN predefinita per I server DNS.
- **Use the following Static DNS IP Address (Utilizza il seguente indirizzo IP DNS statico):** 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 **Save/Apply (Salva/Applica)** per applicarle.

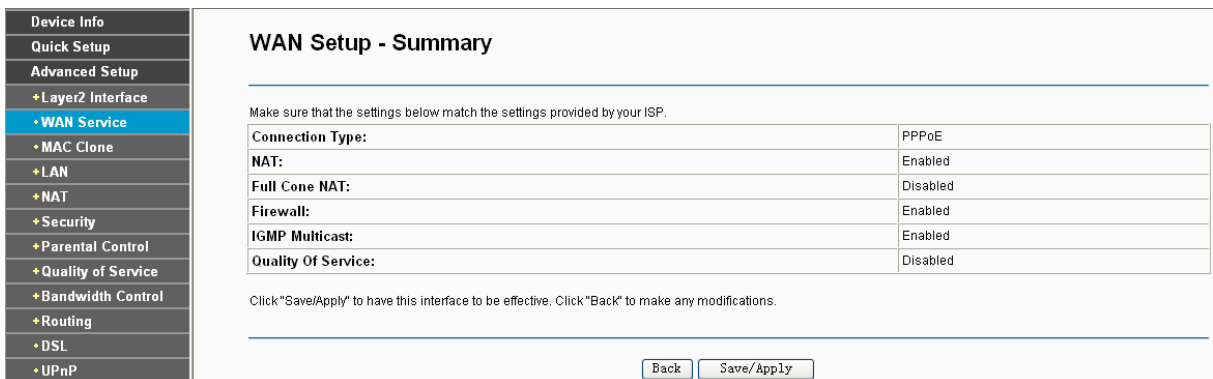


Figura 4-13

8. La nuova interfaccia è ora elencata.

Interface	Description	Type	Vlan8021p	VlanMuxId	Icmp	NAT	Firewall	IPv6	Mld	Remove	Edit
atm0.1	br_0_8_35	Bridge	N/A	N/A	Enabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
ppp0.2	pppoe_0_8_35	PPPoE	N/A	N/A	Enabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	Edit

Figura 4-14

- **Remove All (Elimina tutto):** Fare clic per eliminare tutte le interfacce.
- **Remove (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 **Add (Aggiungi) (Aggiungi)** come in Figura 4-7 per mostrare la schermata in Figura 4-8. Fare clic su **Next (Avanti)**.
3. Selezionare IPoE in Figura 4-9, inserire una breve descrizione e fare clic su **Next (Avanti)**.
4. Specificare i parametri richiesti e fare clic su **Next (Avanti)**.

Figura 4-15

- **Obtain an IP address automatically (Ottieni automaticamente indirizzo IP):** Selezionare se il provider utilizza un server DHCP per la configurazione dell'indirizzamento.

#### 👉 Nota:

- 1) 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.

➤ **Use the following IP Address (Utilizza il seguente indirizzo IP):** Specificare i parametri d'indirizzamento se forniti dal provider ISP.

5. È possibile abilitare **NAT**, **Firewall** ed **IGMP Multicast**, fare quindi click su **Next (Avanti)**.

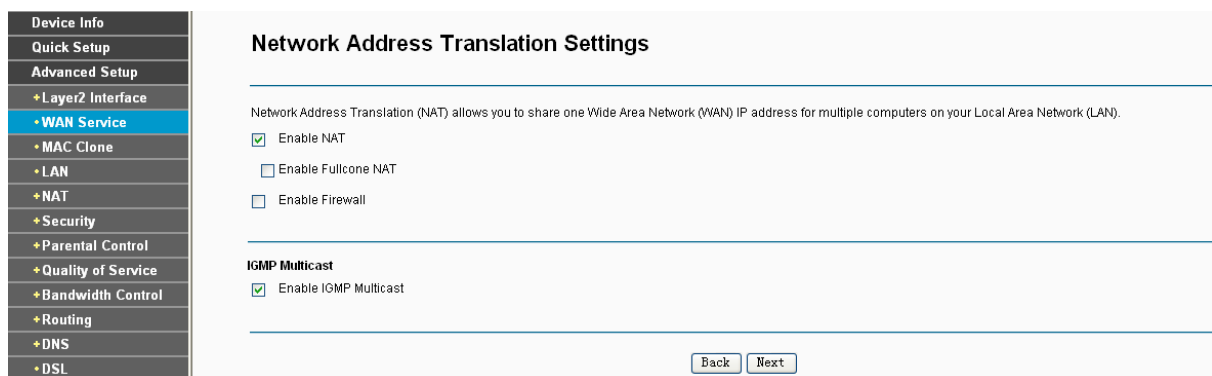


Figura 4-16

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

 **Nota:**

Selezionando **Enable NAT (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 **Next (Avanti)**.

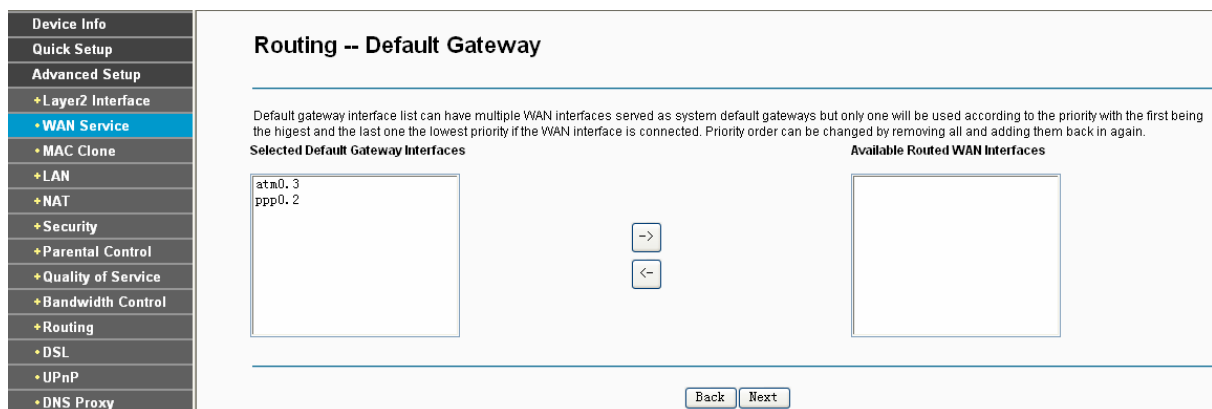


Figura 4-17

## 7. Configurare i server DNS e fare clic su **Next (Avanti)**.

**DNS Server Configuration**

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.  
**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

Available WAN Interfaces

atm0.3  
ppp0.2

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Back Next

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 **Save/Apply (Salva/Applica)** per applicarle.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save/Apply" to have this interface to be effective. Click "Back" to make any modifications.

Back Save/Apply

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 **Add (Aggiungi) (Aggiungi)** come in Figura 4-7 per mostrare la schermata in Figura 4-8. Fare clic su **Next (Avanti)**.
3. Selezionare Bridge in Figura 4-9, inserire una breve descrizione e fare clic su **Next (Avanti)**.
4. Specificare i parametri richiesti e fare clic su **Next (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 **Add (Aggiungi) (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 **Add (Aggiungi) (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 **Add (Aggiungi) (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 **Add (Aggiungi) (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 **Add (Aggiungi) (Aggiungi)** come in Figura 4-7 e configurare come descritto in [4.4.2.3 ATM-EoA-Bridging](#).

### 4.4.3 MAC Clone

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

La schermata lista le interfacce configurate in [4.4.1 Interfaccia layer 2](#) col relativo 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.

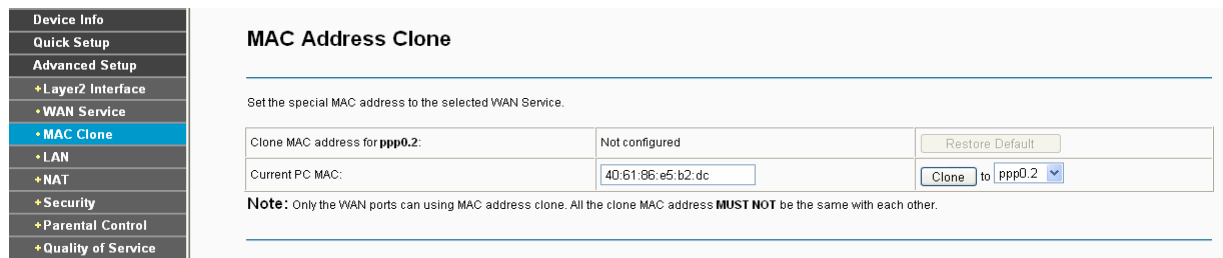


Figura 4-20

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

Fare clic su **Restore Default (Predefinito)** per ripristinare l'indirizzo originale.

 **Nota:**

Tutti gli indirizzi MAC devono essere univoci.

#### 4.4.4 LAN

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

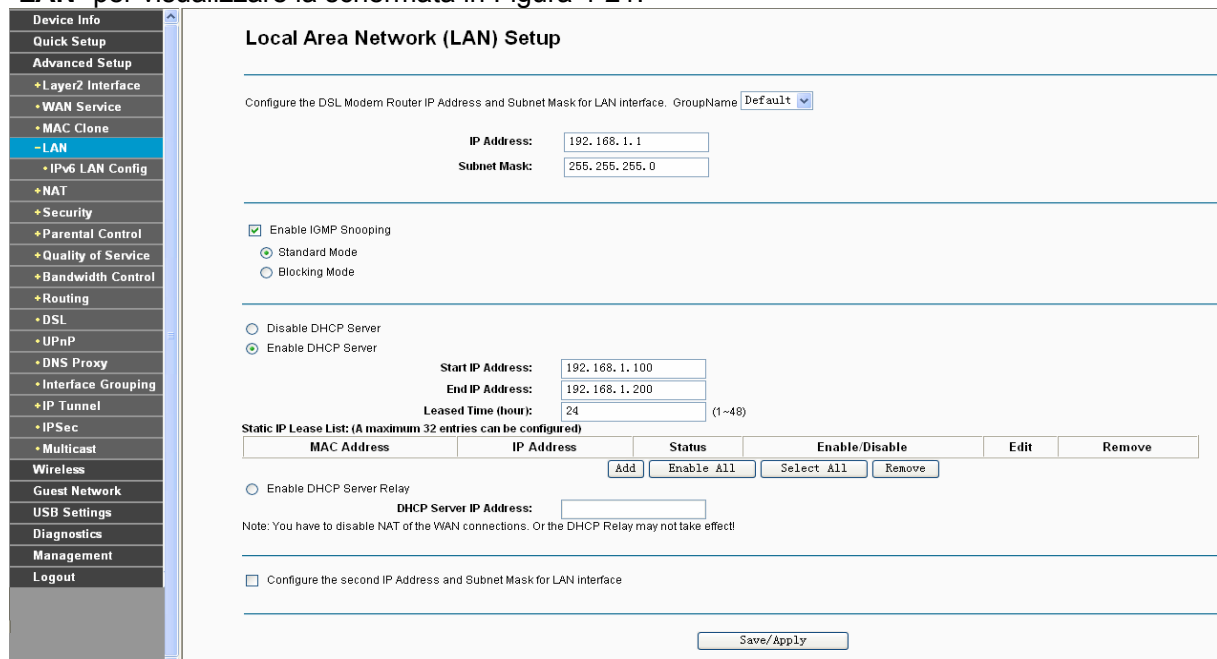


Figura 4-21

- **IP Address (Indirizzo IP) / Subnet Mask:** Configurare indirizzo IP e Subnet Mask per l'interfaccia LAN.
- **Enable IGMP Snooping (Abilita IGMP Snooping):** Abilitando questa opzione è necessario selezionare la modalità standard o bloccante.



- **Enable second IP (Abilita IP secondario):** È possibile configurare un indirizzo LAN secondario attraverso il quale raggiungere la web console.
- **DHCP Server:** Dynamic Host Configuration Protocol è il sistema di assegnamento automatico dell'indirizzo IP per i dispositivi collegati ed è abilitato di default.
  - **Start IP address (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 **192.168.1.2 – 192.168.1.254**.
  - **End IP Address (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 **192.168.1.2 – 192.168.1.254**.
  - **Leased Time:** È la durata degli indirizzi assegnati, normalmente **1440** minuti. Al termine dell'intervallo di tempo l'IP assegnato viene liberato ed è eventualmente necessario un nuovo assegnamento automatico.
- **Static IP Lease List (Lease statiche):** Fare clic su **Add (Aggiungi) Entries (Aggiungi)** in Figura 4-21, per forzare un abbinamento MAC / IP sul server DHCP.



Figura 4-22

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

#### 4.4.4.1 LAN IPv6

Selezionare **“Advanced Setup (Configurazione avanzata) (Configurazione avanzata)”** → **“LAN”** → **“LAN IPv6”** per visualizzare la schermata in Figura 4-23.

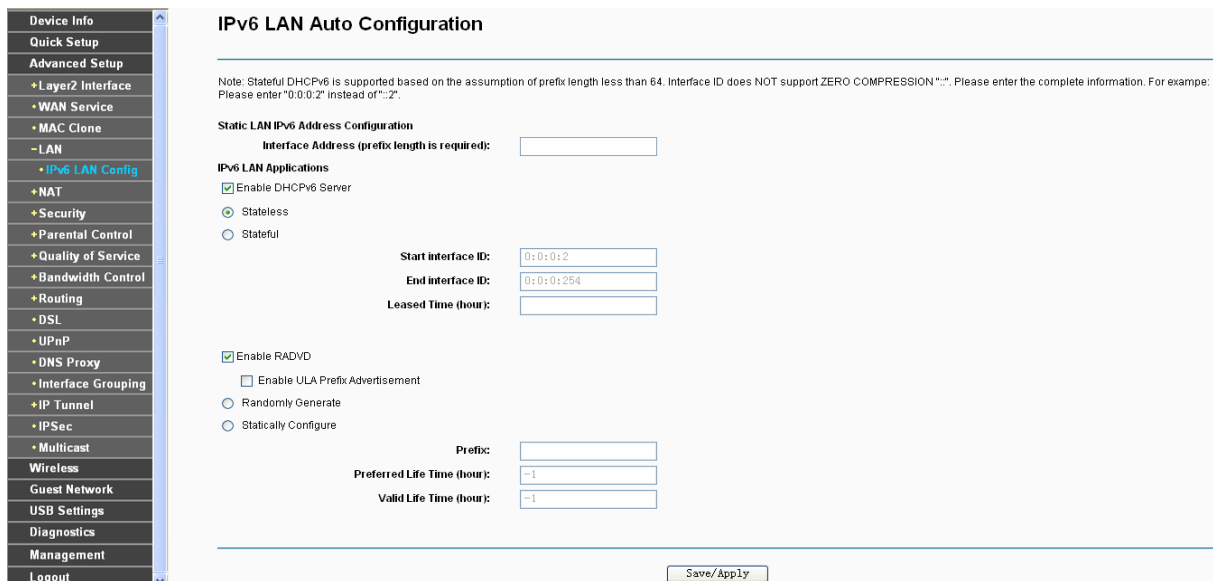


Figura 4-23

- **Interface Address (prefix length is required) (Indirizzo interfaccia (con prefisso)):** Indirizzo e prefisso dell'interfaccia.
- **IPv6 LAN Applications (Servizi IPv6):** Scegliere il metodo di assegnamento degli indirizzi.

**For DHCPv6 Server (Server DHCPv6):**

- 1) **Stateless** non necessita di configurazione.
- 2) **Stateful** richiede i seguenti parametri.
  - **Start Interface ID (ID interfaccia iniziale):** Inserire il primo indirizzo del range assegnabile automaticamente.
  - **End Interface ID (ID interfaccia finale):** Inserire l'ultimo indirizzo del range assegnabile automaticamente.
  - **Leased Time:** È la durata degli indirizzi assegnati, normalmente **86400** secondi. Al termine dell'intervallo di tempo l'IP assegnato viene liberato ed è eventualmente necessario un nuovo assegnamento automatico.

<input checked="" type="checkbox"/> Enable DHCPv6 Server	
<input type="radio"/> Stateless	
<input checked="" type="radio"/> Stateful	
<b>Start interface ID:</b>	<input type="text" value="0:0:0:2"/>
<b>End interface ID:</b>	<input type="text" value="0:0:0:254"/>
<b>Leased Time (hour):</b>	<input type="text" value="24"/>

**For RADVD (RADVD):**

- 1) **Randomly Generate (Casuale)** non necessita di configurazione.
- 2) **Statically Configure (Statico)** richiede i seguenti parametri.

<input checked="" type="checkbox"/> Enable RADVD	
<input checked="" type="checkbox"/> Enable ULA Prefix Advertisement	
<input type="radio"/> Randomly Generate	
<input checked="" type="radio"/> Statically Configure	
<b>Prefix:</b>	<input type="text"/>
<b>Preferred Life Time (hour):</b>	<input type="text" value="-1"/>
<b>Valid Life Time (hour):</b>	<input type="text" value="-1"/>

- **Prefix (Prefisso):** Specificare un prefisso.

Fare clic su **Save/Apply (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 **Enable NAT (Abilita NAT)** con connessioni **IPOA** ed **IPOE (4.4.2 WAN)** è possibile visualizzare la schermata in Figura 4-24.

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

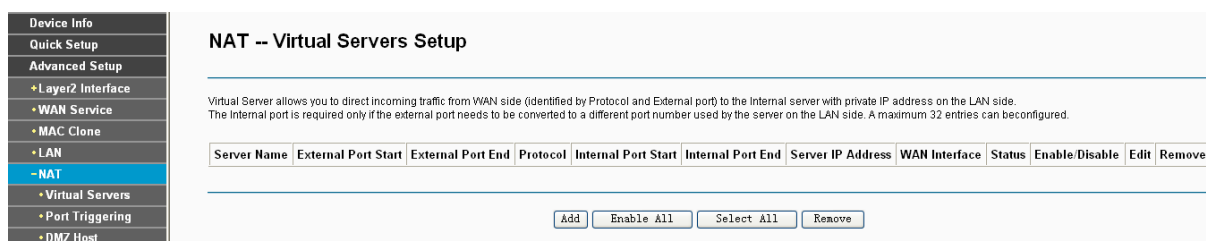


Figura 4-24

### 4.4.5.1 Virtual Server

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

I server virtuali consentono di inoltrare una connessione provenienti 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.

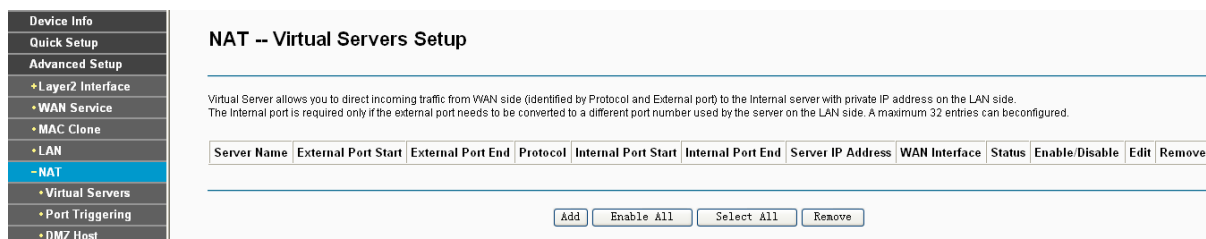


Figura 4-25

➤ **Virtual Server Table (Tabella virtual server):** La tabella elenca i server configurati.

- **Server Name (Nome server):** Nome identificativo del server.
- **External Port Start (Porta esterna iniziale):** Prima porta esterna inoltrata.
- **External Port End (Porta esterna finale):** Ultima porta esterna inoltrata.
- **Protocol (Protocollo):** Protocolli inoltrati.
- **Internal Port Start (Porta interna iniziale):** Prima porta interna alla quale inoltrare.
- **Internal Port End (Porta interna finale):** Ultima porta interna alla quale inoltrare.
- **Server IP Address (Indirizzo IP):** Indirizzo del dispositivo a cui inoltrare le connessioni.

- **WAN Interface (Interfaccia WAN):** Interfaccia WAN ascoltata.
- **Add (Aggiungi) (Aggiungi):** Fare clic per aggiungere un server.
- **Remove (Elimina):** Selezionare i server da rimuovere e fare clic per eliminarli.

#### Per aggiungere un virtual server:

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

**NAT -- Virtual Servers**

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server.  
 NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".  
 Remaining number of entries that can be configured: 32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Figura 4-26

2. Selezionare l'interfaccia da ascoltare.
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 **Save/Apply (Salva/Applica)** per abilitare il server.

#### 4.4.5.2 Port triggering

Selezionare **"Advanced Setup (Configurazione avanzata) (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.

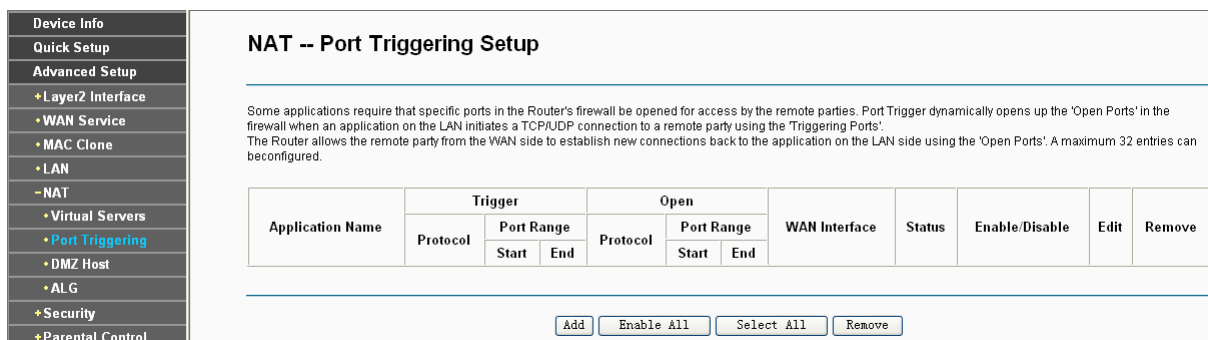


Figura 4-27

- **Port Triggering Table (Port triggering):** Tabella dei trigger programmati.
  - **Application (Name):** Nome della regola.
  - **Trigger:** Protocolli e range porte trigger.
  - **Open:** Protocolli e range porte aperte.
  - **WAN Interface (Interfaccia WAN):** Interfaccia di trigger.
- **Add (Aggiungi) (Aggiungi):** Fare clic per aggiungere una regola.
- **Remove (Elimina):** Selezionare le regole da rimuovere e fare clic per eliminarle.

**Per aggiungere una regola:**

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

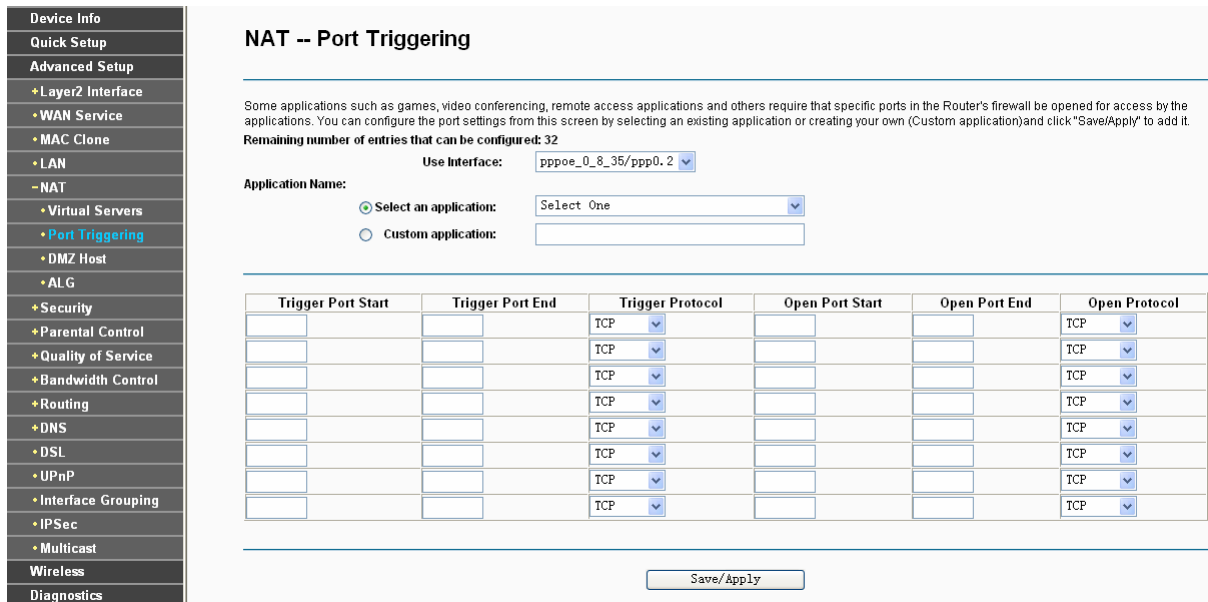


Figura 4-28

2. Selezionare l'applicazione dalla lista o selezionare **Custom application (Personalizzata)** e specificarne il nome.
3. Specificare porte e protocolli.
4. Fare clic su **Save/Apply (Salva/Applica)** per salvare la regola.

#### 4.4.5.3 Host DMZ

Selezionare “**Advanced Setup (Configurazione avanzata)**” → “**NAT**” → “**DMZ Host (Host DMZ)**” per visualizzare la schermata in Figura 4-29.

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

Figura 4-29

#### Per impostare un host DMZ:

Specificare l’IP e fare clic su **Save/Apply (Salva/Applica)**.

#### **Nota:**

L’host DMZ deve avere IP statico.

#### 4.4.5.4 ALG

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

Figura 4-30

Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

#### 4.4.6 Sicurezza

Selezionare “**Advanced Setup (Configurazione avanzata)**” → “**Security**” per visualizzare le schermate relative ad **IP Filtering (Filtro IP)** e **MAC Filtering (Filtro MAC)** (solo modalità bridge) tramite la corrispondente voce di menu.

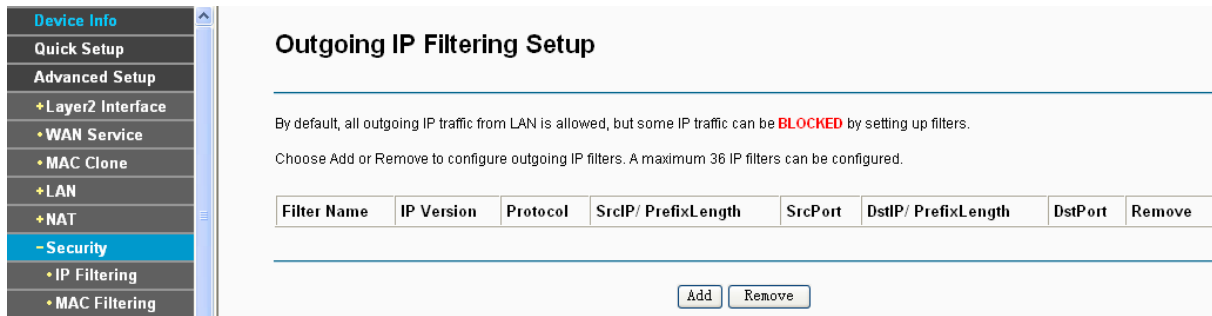


Figura 4-31

#### 4.4.6.1 Filtro MAC

##### Filtro IP – In uscita

Selezionare “Advanced Setup (Configurazione avanzata)” → “Security (Sicurezza)” → “IP Filtering (Filtro IP)”.

È possibile bloccare il traffico verso alcuni IP.

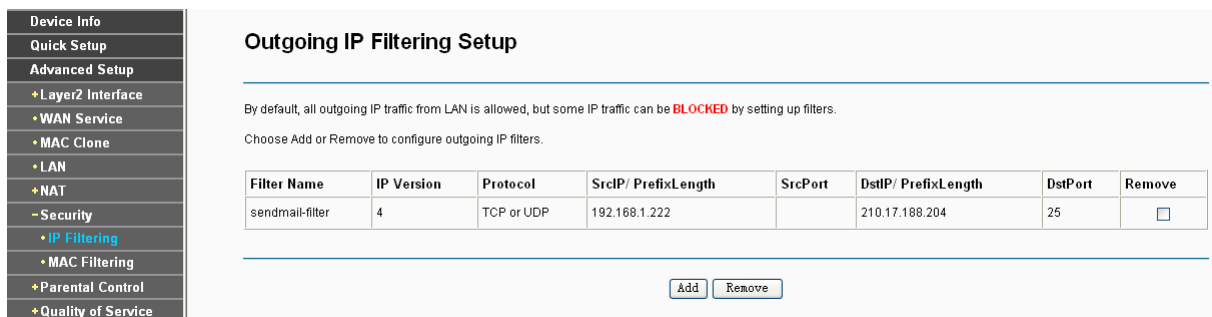


Figura 4-32

##### Per aggiungere una regola:

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

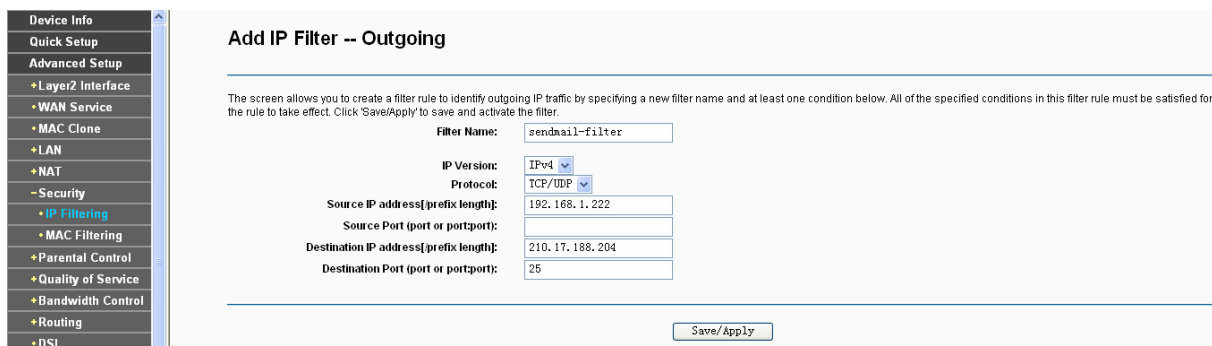


Figura 4-33

2. Specificare un nome per il filtro.
3. Specificare il protocollo.
4. Specificare un **Source IP Address (Indirizzo IP sorgente)** ed un range **Source Port (Porte sorgente)** (porta o porta:porta).
5. Enter a **Destination IP Address (Indirizzo IP destinazione)** ed un range **Destination Port (Porte destinazione)** (porta o porta:porta).

6. Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

 **Nota:**

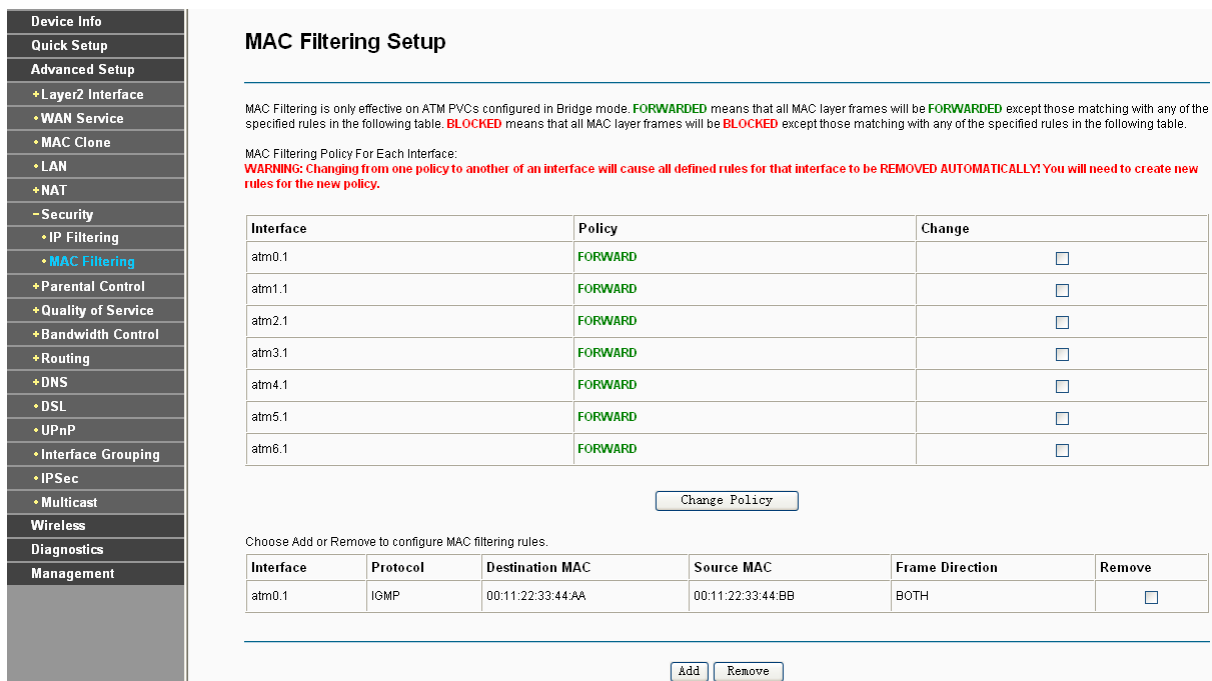
Le condizioni non specificate non limitano l'applicazione della regola; è necessario specificare almeno una condizione.

#### 4.4.6.2 Filtro MAC

Selezionare **“Advanced Setup (Configurazione avanzata)”** → **“Security (Sicurezza)”** → **“MAC Filtering (Filtro MAC)”** per visualizzare la schermata in Figura 4-34.

 **Nota:**

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



**MAC Filtering Setup**

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:  
**WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

Interface	Policy	Change
atm0.1	FORWARD	<input type="checkbox"/>
atm1.1	FORWARD	<input type="checkbox"/>
atm2.1	FORWARD	<input type="checkbox"/>
atm3.1	FORWARD	<input type="checkbox"/>
atm4.1	FORWARD	<input type="checkbox"/>
atm5.1	FORWARD	<input type="checkbox"/>
atm6.1	FORWARD	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
atm0.1	IGMP	00:11:22:33:44:AA	00:11:22:33:44:BB	BOTH	<input type="checkbox"/>

Figura 4-34

- **Change Policy (Cambio policy):** Sono disponibili **FORWARDED (INOLTRA)** e **BLOCKED (BLOCCA)**. **FORWARDED (INOLTRA)** inoltra tutti i frame ad eccezione di quelli specificati, **BLOCKED (BLOCCA)** blocca tutti i frame ad eccezione di quelli specificati. Selezionare **Change (Cambia)** e fare clic su **Change Policy (Cambia policy)** per cambiare il comportamento sulle interfacce selezionate.
- **Add (Aggiungi):** Fare clic su **Add (Aggiungi)** e specificare un indirizzo MAC.
- **Remove (Elimina):** Selezionare le regole da rimuovere e fare clic su **Remove (Elimina)** per cancellarle.

**Per aggiungere una regola procedure come segue.**

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



Device Info
Quick Setup
Advanced Setup
+ Layer2 Interface
+ WAN Service
+ MAC Clone
+ LAN
+ NAT
- Security
+ IP Filtering
+ MAC Filtering
+ Parental Control
+ Quality of Service
+ Bandwidth Control
+ Routing

### Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only):

Figura 4-35

2. Selezionare il **Protocol Type (Protocollo)**.
3. Specificare **Destination MAC Address (Indirizzo MAC destinazione)** ed **Source MAC Address (Indirizzo MAC sorgente)**.
4. Selezionare la **Frame Direction (Direzione)**.
5. Selezionare le **WAN interfaces (Interfacce WAN)**.
6. Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

#### 4.4.7 Parental Control

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

Device Info
Quick Setup
Advanced Setup
+ Layer2 Interface
+ WAN Service
+ MAC Clone
+ LAN
+ NAT
+ Security
- Parental Control
+ Time Restriction

### Access Time Restriction

A maximum 16 entries can be configured.

Username	MAC	Days							Time		Status	Enable/Disable	Edit	Remove	
		Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop					
<input type="button" value="Add"/> <input type="button" value="Enable All"/> <input type="button" value="Select All"/> <input type="button" value="Remove"/>															

Figura 4-36

##### 4.4.7.1 Orario

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

Device Info
Quick Setup
Advanced Setup
+ Layer2 Interface
+ WAN Service
+ MAC Clone
+ LAN
+ NAT
+ Security
- Parental Control
+ Time Restriction
+ URL Filter

### Access Time Restriction

A maximum 16 entries can be configured.

Username	MAC	Days							Time		Status	Enable/Disable	Edit	Remove	
		Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop					
child-1	00:11:22:33:44:CC	x	x	x	x	x			18:00	21:00	Enabled	<input type="button" value="Disable"/>	<input type="button" value="Edit"/>	<input type="checkbox"/>	
<input type="button" value="Add"/> <input type="button" value="Enable All"/> <input type="button" value="Select All"/> <input type="button" value="Remove"/>															

Figura 4-37

**Per aggiungere una regola:**

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

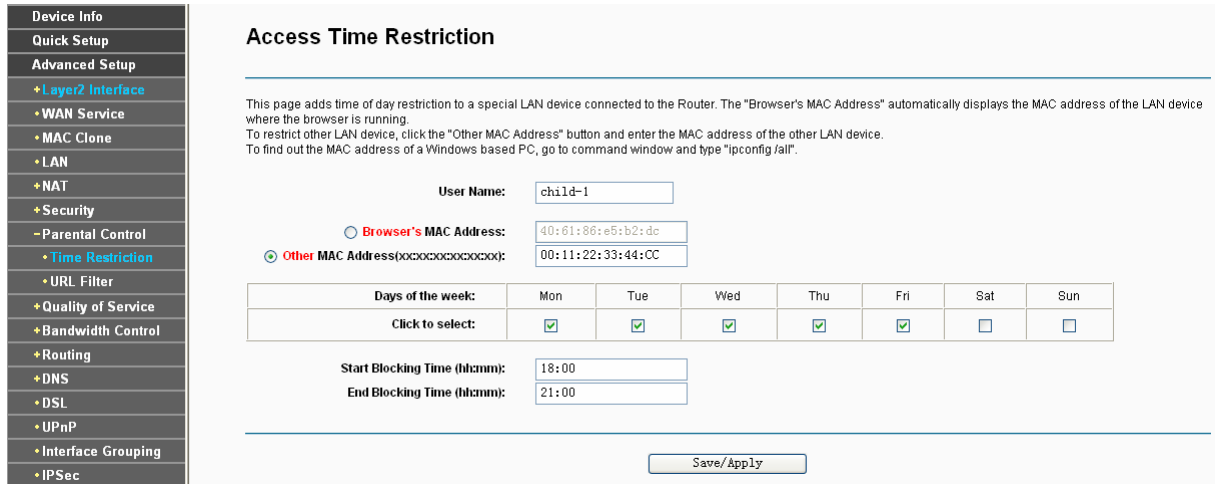


Figura 4-38

2. Specificare il **User Name (Nome)** del dispositivo da limitare.
3. Specificare l'indirizzo MAC del dispositivo o selezionare **Browser's MAC Address (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 **Start Blocking Time (Orario di inizio)** ed un **End Blocking Time (Orario di fine)** per il periodo effettivo.
6. Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

**Nota:**

Configurare innanzitutto l'orologio di sistema in **“Management (Strumenti) → Internet Time (Orologio)”**.

**4.4.7.2 Filtro URL**

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

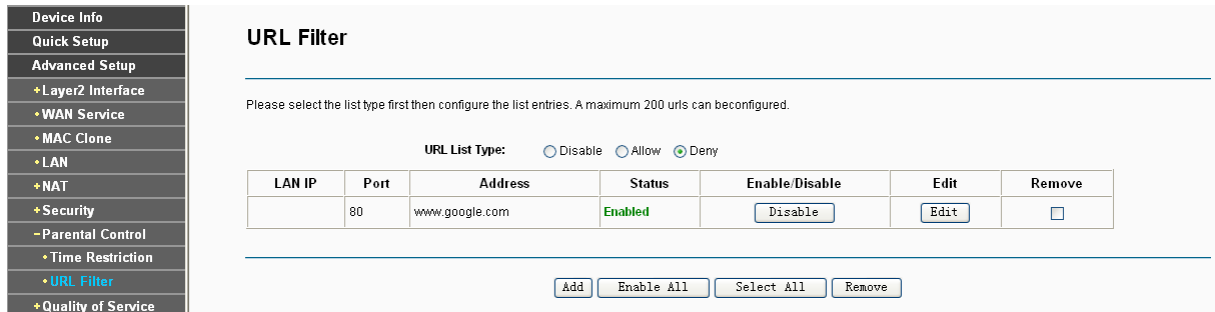


Figura 4-39

Sono disponibili 3 modalità.

- **Disable (Disabilita):** Il filtro non è operativo.

- **Allow (Consenti):** URL non elencati non consentiti.
- **Deny (Nega):** URL elencati non consentiti.

#### Per aggiungere un filtro:

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

Figura 4-40

3. Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

## 4.4.8 QoS

Selezionare “**Advanced Setup (Configurazione avanzata)**” → “**Quality of Service (QoS)**” per regolamentare la priorità di traffico per le varie applicazioni.

Figura 4-41

Selezionare **Enable QoS (Abilita QoS)** per abilitare la funzionalità.

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

Fare clic su **Save/Apply (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 “**Advanced Setup (Configurazione avanzata)**” → “**Quality of Service (QoS)**” → “**Queue Config (Coda)**”.

- Device Info
- Quick Setup
- Advanced Setup
- + Layer2 Interface
- + WAN Service
- + MAC Clone
- + LAN
- + NAT
- + Security
- + Parental Control
- Quality of Service
- + Queue Config
- + QoS Classification
- + Bandwidth Control
- + Routing
- + DNS
- + DSL
- + UPnP
- + Interface Grouping
- + IPSec
- + Multicast
- Wireless
- Diagnostics
- Management

### QoS Queue Setup

In ATM mode, maximum 8 queues can be configured.  
 For each Ethernet interface, maximum 4 queues can be configured.  
 To add a queue, click the **Add** button.  
 To remove queues, check their remove-checkboxes, then click the **Remove** button.  
 The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.  
 The enable-checkbox also shows status of the queue after page reload.  
 Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	
Default Queue	34	atm0	SP	8		Path0		<input type="checkbox"/>	
Default Queue	35	atm1	SP	8		Path0		<input type="checkbox"/>	
Default Queue	36	atm2	SP	8		Path0		<input type="checkbox"/>	
Default Queue	37	atm3	SP	8		Path0		<input type="checkbox"/>	
Default Queue	39	atm5	SP	8		Path0		<input type="checkbox"/>	
Default Queue	40	atm6	SP	8		Path0		<input type="checkbox"/>	
Default Queue	41	atm4	SP	8		Path0		<input type="checkbox"/>	

Add Enable Remove

Figura 4-42

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

- Device Info
- Quick Setup
- Advanced Setup
- + Layer2 Interface
- + WAN Service
- + MAC Clone
- + LAN
- + NAT
- + Security
- + Parental Control
- Quality of Service
- + Queue Config
- + QoS Classification
- + Bandwidth Control
- + Routing
- + DNS
- + DSL
- + UPnP

### QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.  
**Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others**  
 Click 'Save/Apply' to save and activate the queue.

**Name:**

**Enable:**

**Interface:**

**Precedence:**

**DSL Latency:**

Figura 4-43

- **Name (Nome):** Nome della regola.
- **Enable (Abilita):** Controllo di abilitazione della regola.
- **Interface (Interfaccia):** Interfaccia sulla quale la regola è attiva.
- **Precedence (Priorità):** Priorità QoS della coda.
- **DSL Latency (Latenza DSL):** È disponibile solo Path0.

Fare clic su **Save/Apply (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'assegnamento di code e priorità ed opzionalmente la sovrascrittura dell'header IP DSCP.

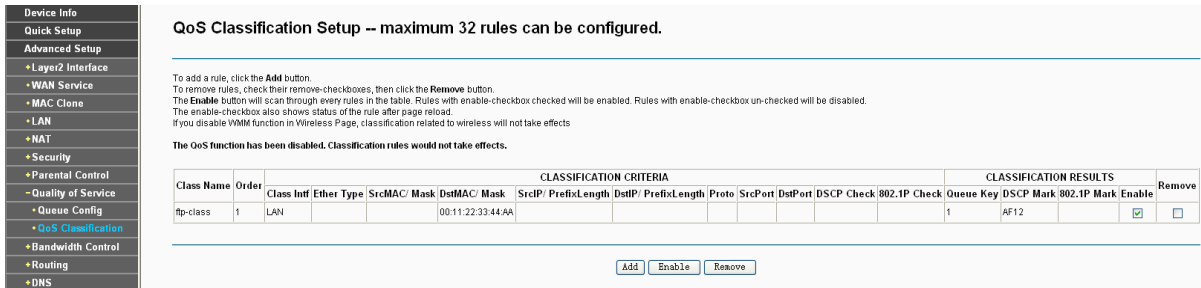


Figura 4-44

Fare clic su **Add (Aggiungi)** in Figura 4-44.

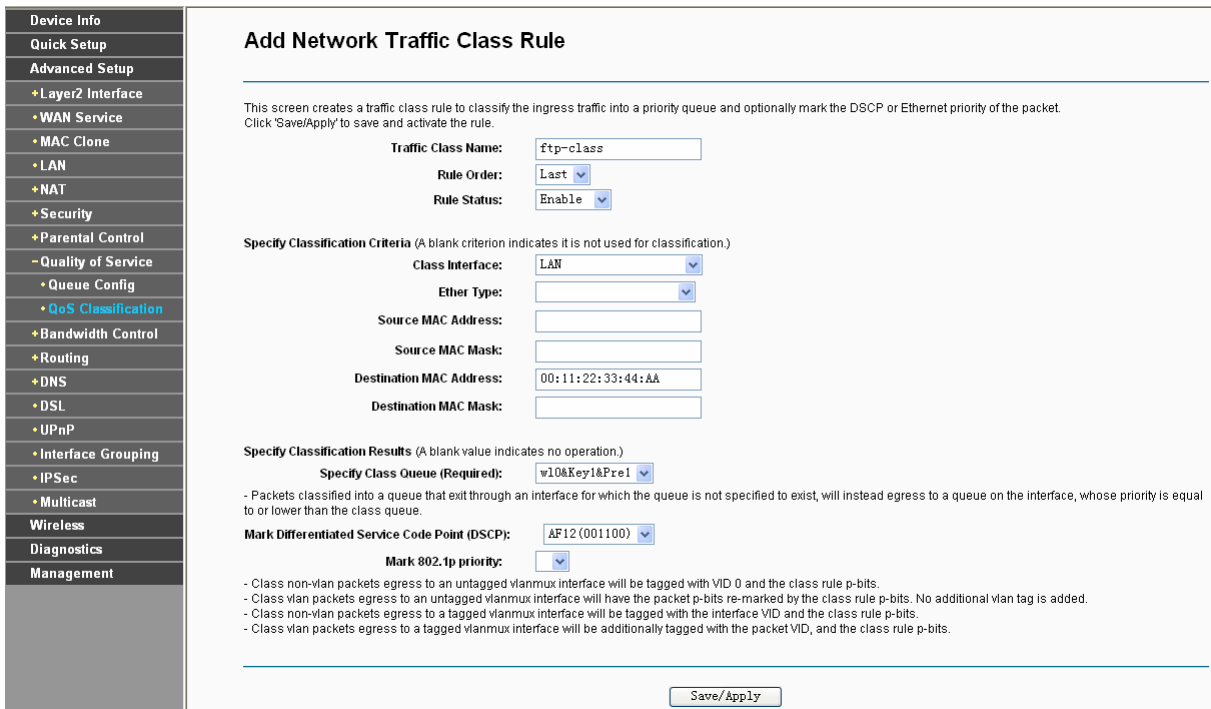


Figura 4-45

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

### 4.4.9 Bandwidth Control

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

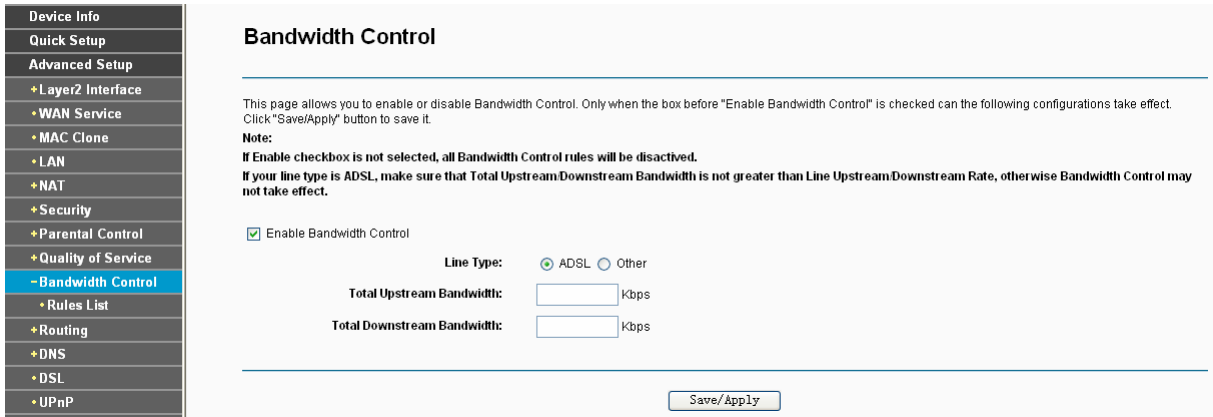


Figura 4-46

- **Enable Bandwidth Control (Abilita bandwidth control):** Controllo di abilitazione della funzionalità.
- **Line Type (Tipo linea):** Tipo di linea in uso.
- **Total Upstream Bandwidth (Kbps) (Banda totale in upstream (kbps)):** Banda disponibile in upstream.
- **Total Downstream Bandwidth (Kbps) (Banda totale in downstream (kbps)):** Banda disponibile in downstream.

Fare clic su **Save/Apply (Salva/Applica)** per applicare le impostazioni.

#### 4.4.9.1 Regole

Selezionare **“Advanced Setup (Configurazione avanzata)”** → **“Bandwidth Control”** → **“Rules List (Regole)”** per visualizzare la schermata in Figura 4-47.

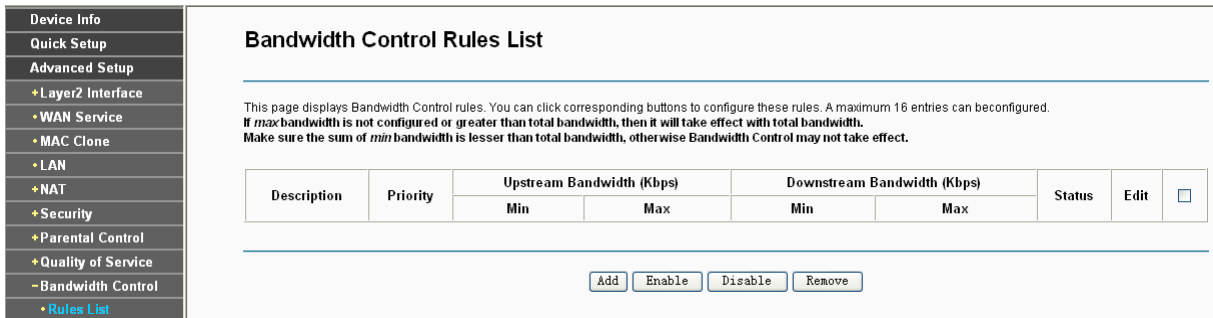


Figura 4-47

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

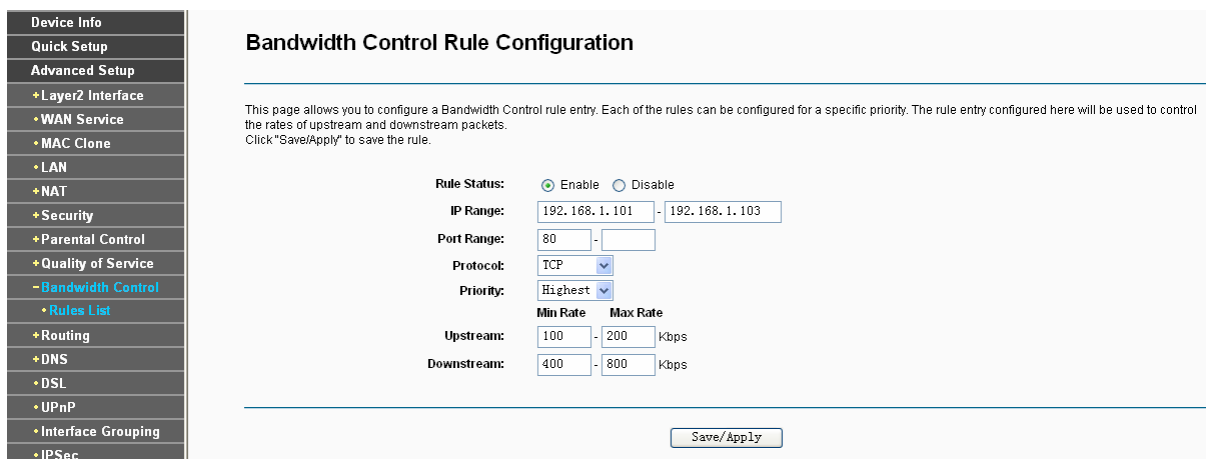


Figura 4-48

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

Fare clic su **Save/Apply (Salva/Applica)** per applicare le impostazioni.

Fare eventualmente clic su **Edit (Modifica)** o **Remove (Elimina)** per gestire le regole selezionate.

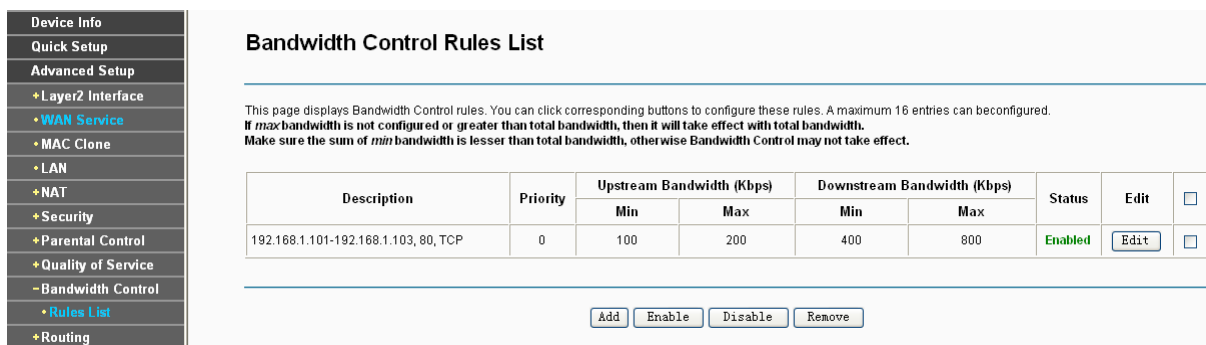


Figura 4-49

#### 4.4.10 Routing

Selezionare **“Advanced Setup (Configurazione avanzata)”** → **“Routing”**.

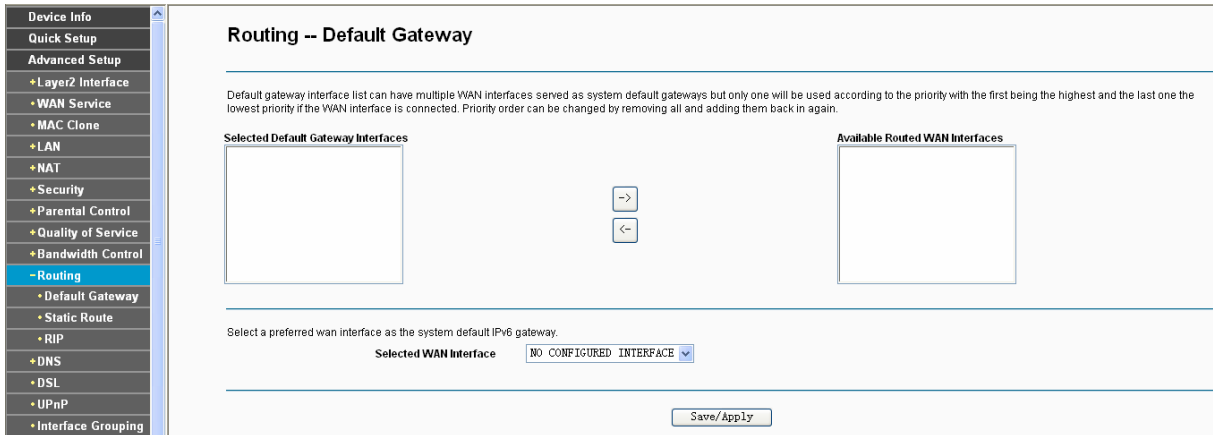


Figura 4-50

#### 4.4.10.1 Gateway predefinito

Selezionare “Advanced Setup (Configurazione avanzata)” → “Routing” → “Default Gateway (Gateway predefinito)”.

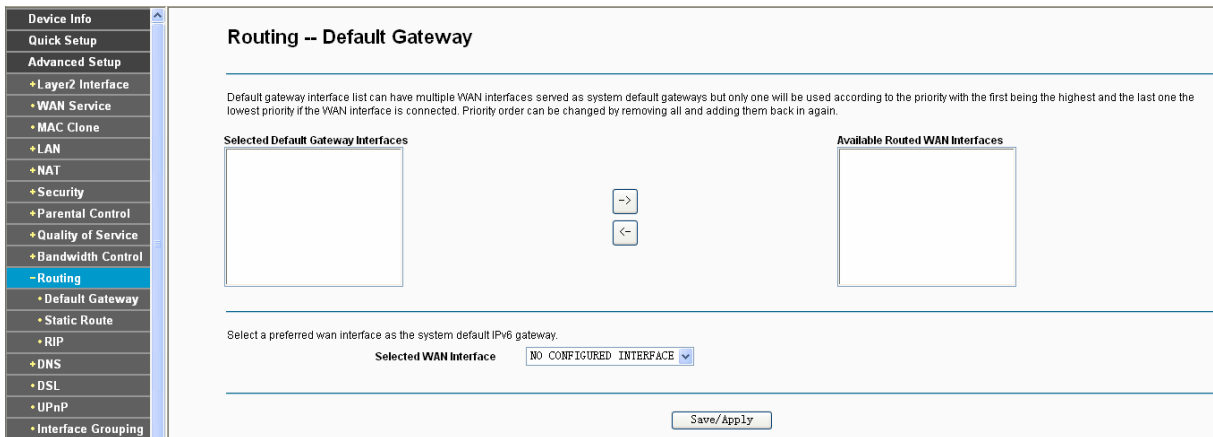


Figura 4-51

#### 4.4.10.2 Static route

Selezionare “Advanced Setup (Configurazione avanzata)” → “Routing” → “Static Route”.

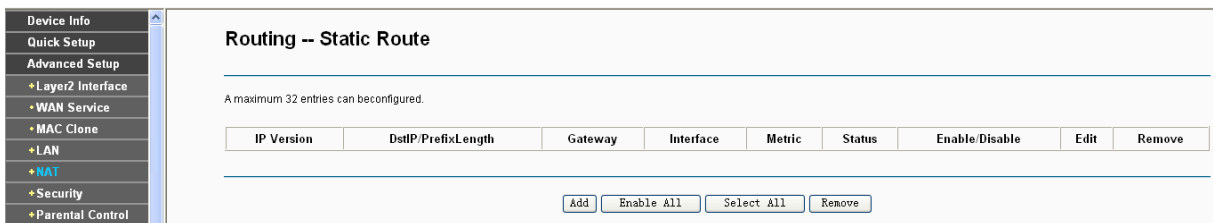


Figura 4-52

Per aggiungere una static route procedere come segue.

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



Figura 4-53

2. Specificare i seguenti parametri
  - **IP Version (Versione IP):** Specificare la versione.
  - **Destination IP Address/prefix length (Indirizzo IP destinazione / Lunghezza prefisso):** Indirizzo target ed eventuale prefisso.
  - **Interface (Interfaccia):** Specificare l'interfaccia per il gateway.
  - **Gateway IP Address (Indirizzo IP gateway):** In modalità di connessione IPoE od IPoA specificare l'IP del gateway da utilizzare.
3. Fare clic su **Save/Apply (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 **Remove (Elimina)**.

#### 4.4.10.3 RIP

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

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.

**DNS Server Configuration**

Select DNS Server Interface from available WAN Interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.  
**DNS Server Interfaces** can have multiple WAN Interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN Interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.  
 Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Figura 4-55

### 4.4.11.1 Server DNS

Selezionare “Advanced Setup (Configurazione avanzata)” → “DNS” → “DNS Server (Server DNS)” per visualizzare la schermata in Figura 4-56.

**DNS Server Configuration**

Select DNS Server Interface from available WAN Interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.  
**DNS Server Interfaces** can have multiple WAN Interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN Interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.  
 Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Figura 4-56

Per PVC PPPoA e PPPoE è possibile selezionare **Select DNS Server Interface from available WAN interfaces (Seleziona interfaccia DNS dalle interface WAN disponibili)** per apprendere automaticamente l'indirizzo dei server.

Per PVC IPoA ed IPoE static selezionare **Use the following Static DNS IP address (Utilizza I seguenti server DNS)** e specificare manualmente i server DNS.

Lo stesso approccio è valido per i DNS IPv6.

Fare clic su **Save/ Apply** per salvare la configurazione.

#### 4.4.11.2 Dynamic DNS

Selezionare “**Advanced Setup (Configurazione avanzata)**” → “**DNS**” → “**Dynamic DNS**”.

Selezionare il provider DDNS e specificare I parametri forniti.

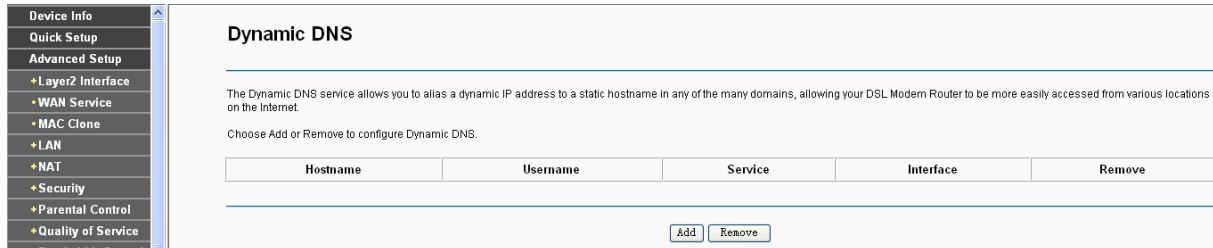


Figura 4-57

Per aggiungere un DDNS procedure come segue.

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

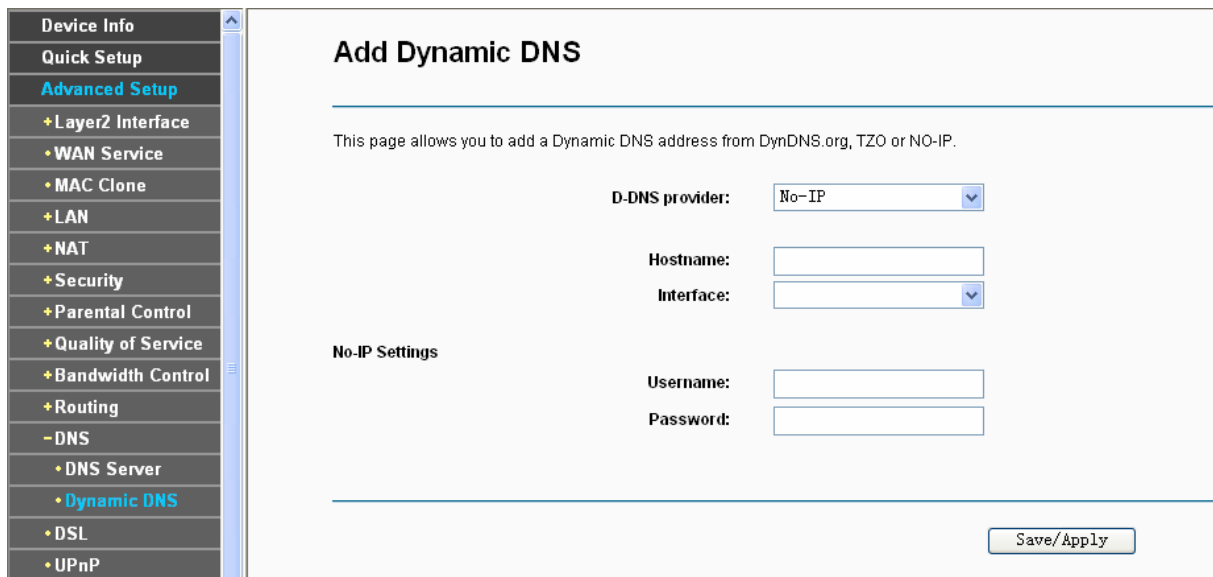


Figura 4-58

2. Selezionare il provider.
3. Specificare **Hostname** ed **Interface (Interfaccia)**.
4. Specificare **User Name (Nome utente)** e **Password**.

Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

#### 4.4.12 DSL

Selezionare “**Advanced Setup (Configurazione avanzata)**” → “**DSL**”.

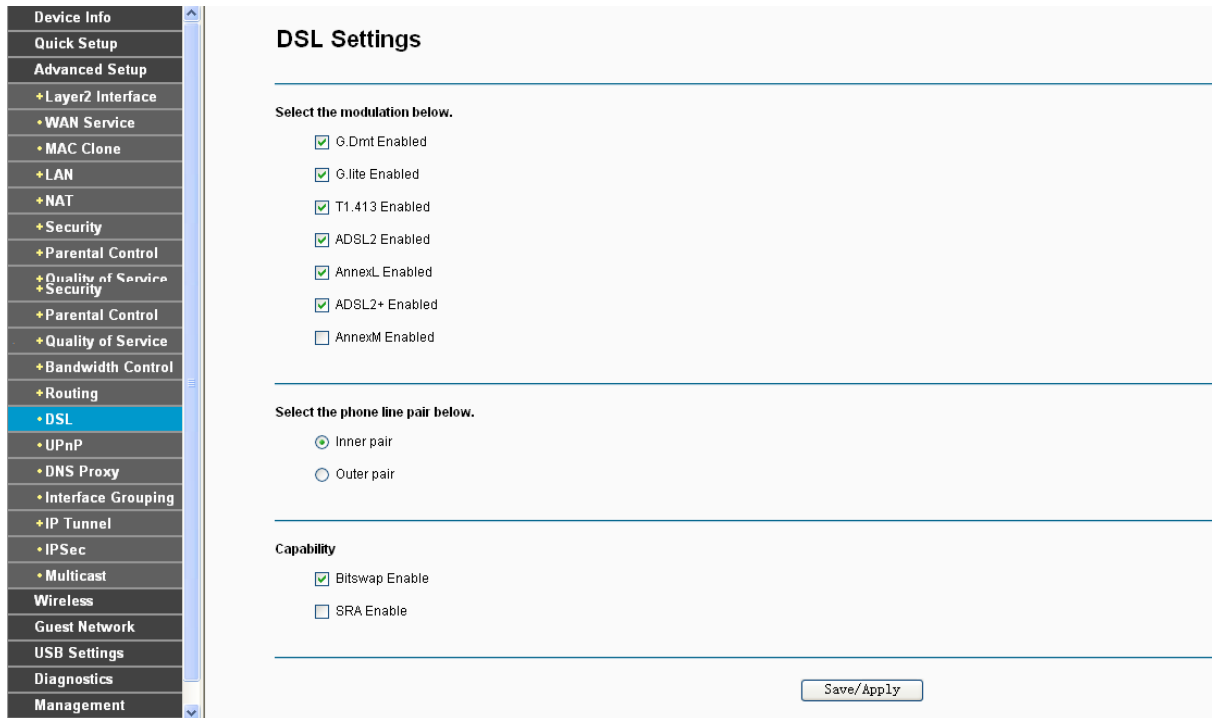


Figura 4-59

Modificare i parametri solamente se necessario.

#### 4.4.13 UPnP

Selezionare “**Advanced Setup (Configurazione avanzata)**” → “**UPnP**”.

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

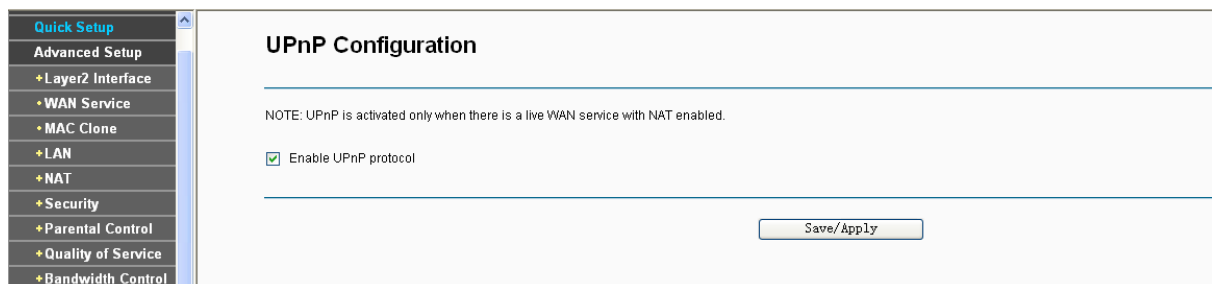


Figura 4-60

Abilitare UPnP se desiderato e fare clic su **Save/Apply (Salva/Applica)**.

#### 4.4.14 Interface Grouping

Selezionare “**Advanced Setup (Configurazione avanzata)**” → “**Interface Grouping**” per gestire i collegamenti logici fra interfacce, PVC e bridging group.

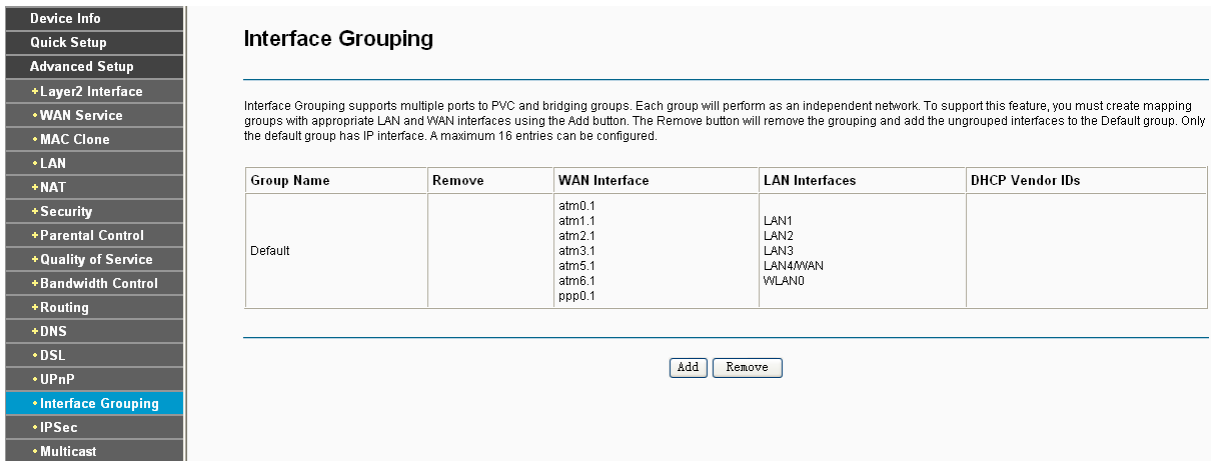


Figura 4-61

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

**Per creare un gruppo d'interfacce procedure come segue.**

1. Fare clic su **Add (Aggiungi)**.

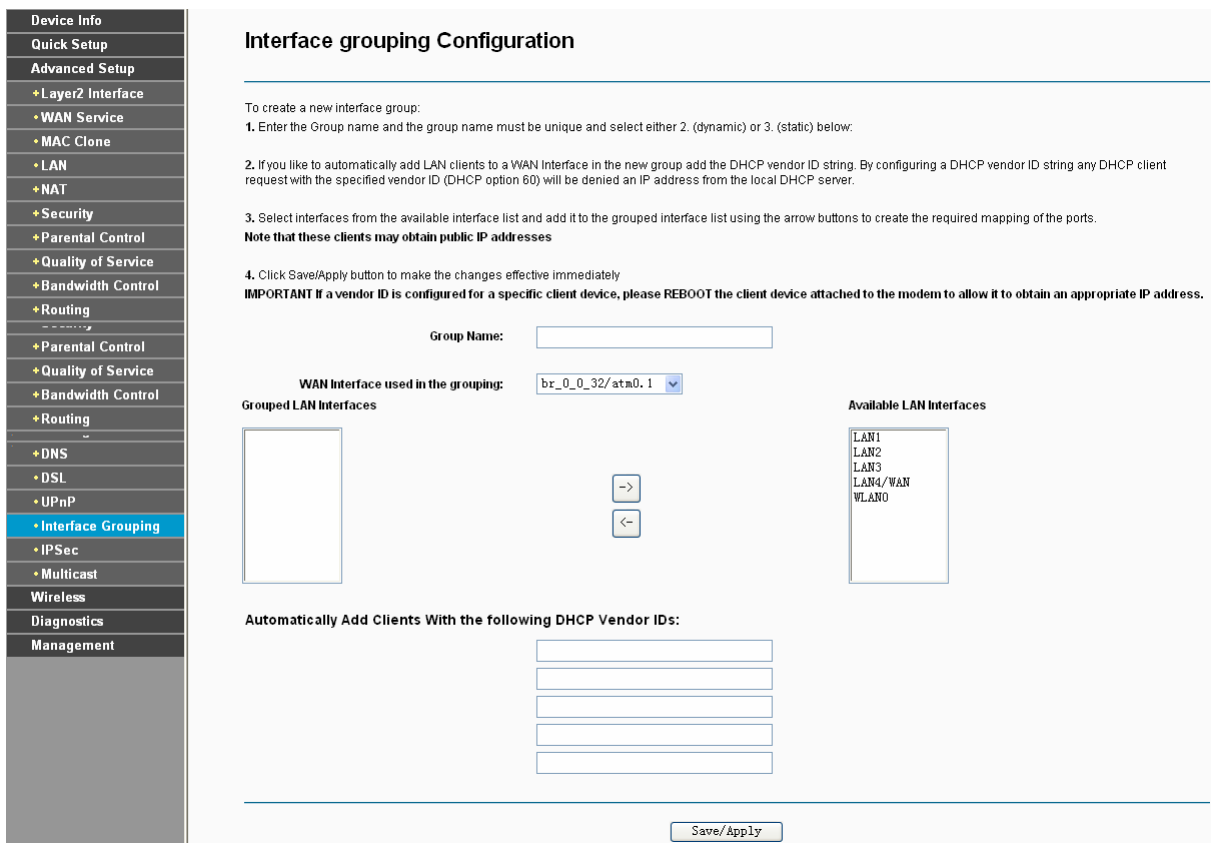


Figura 4-62

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 **Save/Apply (Salva/Applica)** per salvare le impostazioni.

 **Nota:**

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

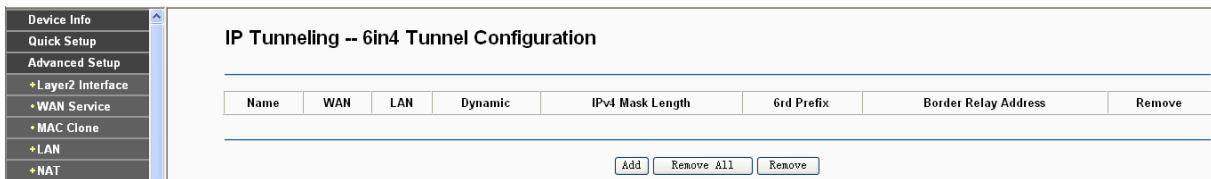
## 4.4.15 Tunnel IP

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 “**Advanced Setup (Configurazione avanzata)**” → “**IP Tunnel (Tunnel IP)**”.

### 4.4.15.1 IPv6inIPv4

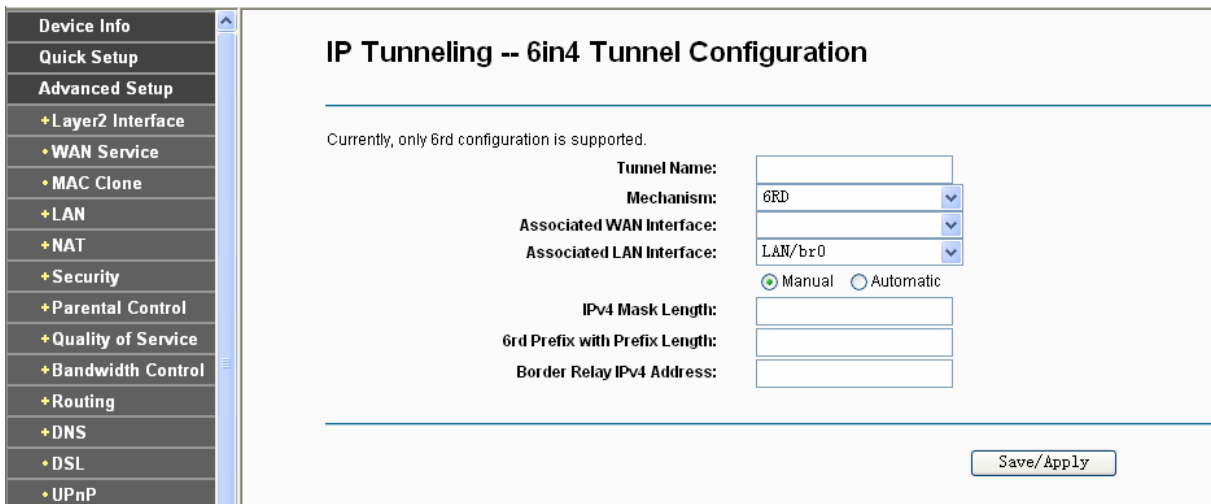
Selezionare “**Advanced Setup (Configurazione avanzata)**” → “**IP Tunnel (Tunnel IP)**” → “**IPv6inIPv4**” per configurare un tunnel IPv6 in IPv4 in Figura 4-63.



The screenshot shows the 'IP Tunneling -- 6in4 Tunnel Configuration' page. On the left is a navigation menu with 'Advanced Setup' selected. The main area contains a table with the following columns: Name, WAN, LAN, Dynamic, IPv4 Mask Length, 6rd Prefix, Border Relay Address, and Remove. Below the table are three buttons: 'Add', 'Remove All', and 'Remove'.

Figura 4-63

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



The screenshot shows the 'IP Tunneling -- 6in4 Tunnel Configuration' page with the configuration form. The left navigation menu is visible. The main area contains the following fields and options:

- Text: "Currently, only 6rd configuration is supported."
- Tunnel Name:
- Mechanism: 6RD (dropdown menu)
- Associated WAN Interface: (dropdown menu)
- Associated LAN Interface: LAN/br0 (dropdown menu)
- Radio buttons:  Manual,  Automatic
- IPv4 Mask Length:
- 6rd Prefix with Prefix Length:
- Border Relay IPv4 Address:
- Save/Apply button at the bottom right.

Figura 4-64

- **Mechanism (Meccanismo):** 6RD è utilizzabile con LAN IPv6 e WAN IPv4.
- **Associated WAN Interface (Interfaccia WAN associata):** Selezionare un'interfaccia.
- **Associated LAN Interface (Interfaccia LAN associate):** Selezionare un'interfaccia LAN connessa.

- **IPv4 Mask Length (Lunghezza maschera IPv4):** Specificare la lunghezza in uso.
- **6rd Prefix with Prefix Length (Lunghezza prefisso 6RD):** Specificare il prefisso in uso.
- **Border Relay IPv4 Address (Indirizzo border relay IPv4):** Specificare l'IPv4 del router border relay.

Fare clic su **Save/Apply (Salva/Applica)** per applicare la configurazione.

 **Nota:**

In questa modalità non sono consentite connessioni WAN IPv6.

#### 4.4.15.2 IPv4inIPv6

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

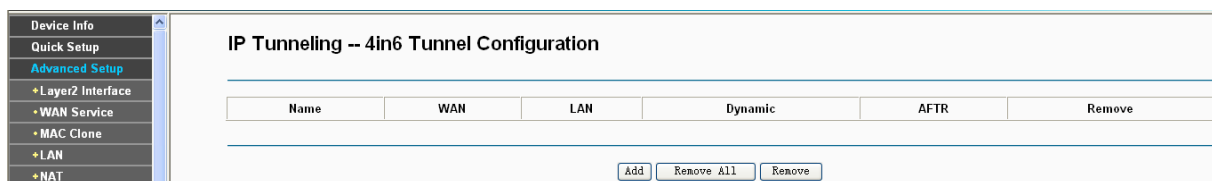


Figura 4-65

Fare clic su **Add (Aggiungi)** in Figura 4-65.

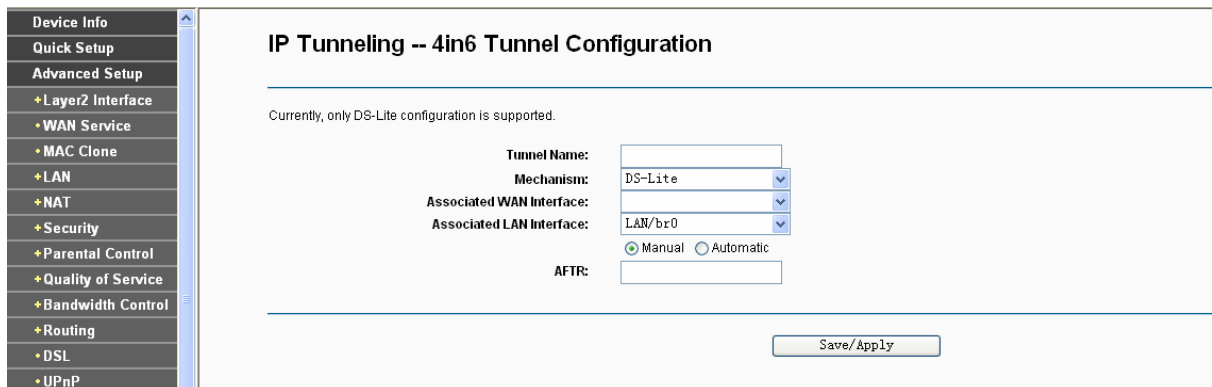


Figura 4-66

- **Mechanism (Meccanismo):** DS-Lite è utilizzabile con LAN IPv4 e WAN IPv6.
- **Associated WAN Interface (Interfaccia WAN associata):** Selezionare un'interfaccia.
- **Associated LAN Interface (Interfaccia LAN associate):** Selezionare un'interfaccia LAN connessa.
- **AFTR:** Specificare l'IPv6 del nodo remoto.

Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

 **Nota:**

In questa modalità non sono permesse connessioni WAN IPv4.

#### 4.4.16 IPSec

Selezionare “**Advanced Setup (Configurazione avanzata)**” → “**IPSec**” per gestire i tunnel IPSec come in Figura 4-67.

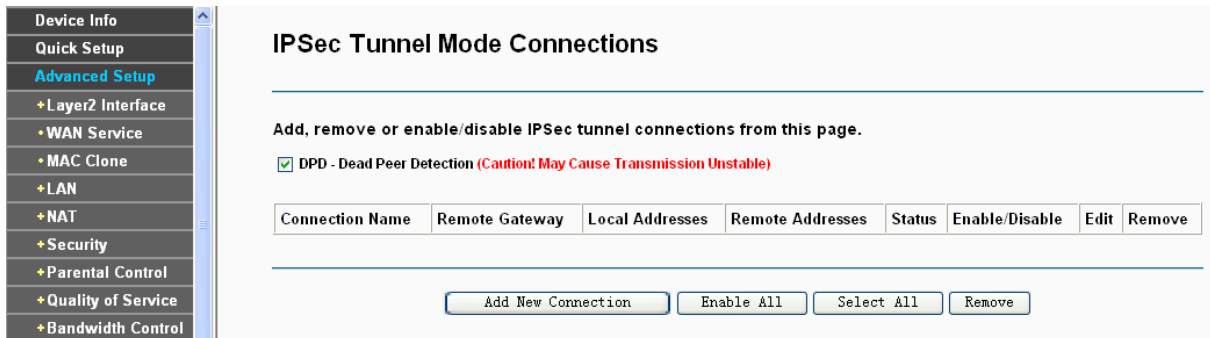
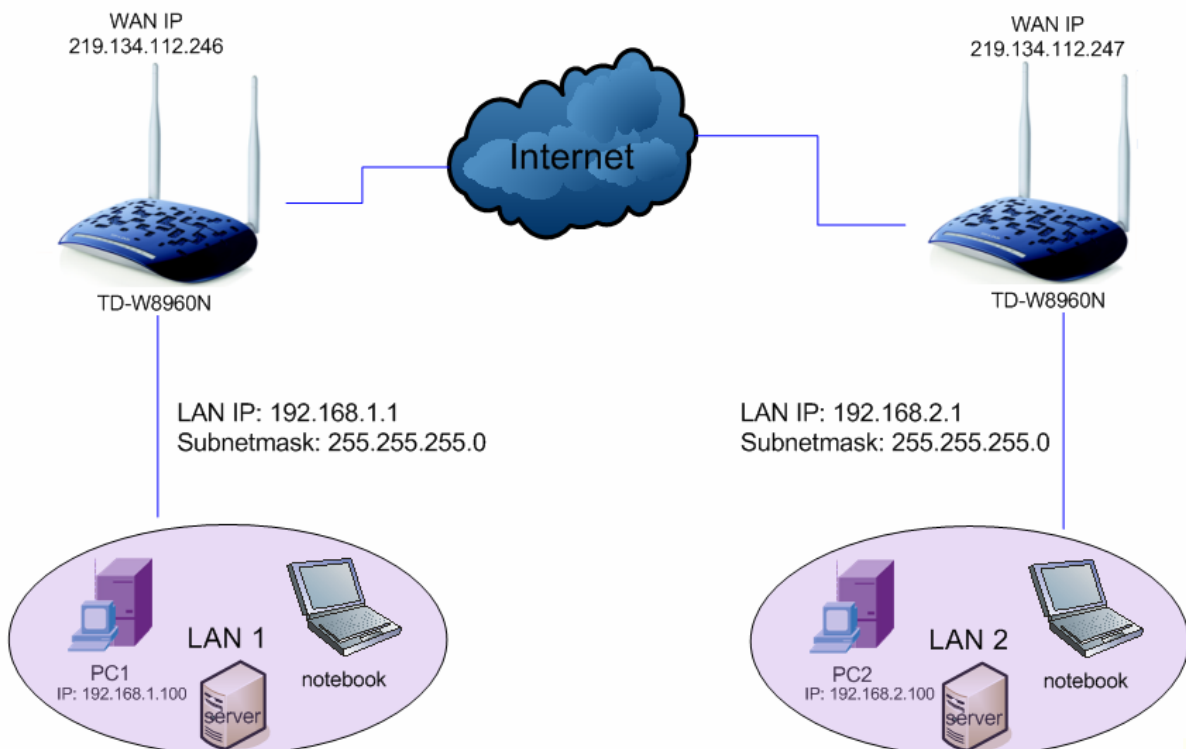


Figura 4-67

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 **Add New Connection (Aggiungi tunnel IPSec)** in Figura 4-67.



**IPsec Settings**

IPsec Connection Name:

Remote IPsec Gateway Address(URL IPv4):

Tunnel access from local IP addresses:

IP Address for VPN:

IP Subnetmask:

Tunnel access from remote IP addresses:

IP Address for VPN:

IP Subnetmask:

Key Exchange Method:

Authentication Method:

Pre-Shared Key:

Perfect Forward Secrecy:

Advanced IKE Settings:

Figura 4-68

- **IPsec Connection Name (Nome tunnel IPsec):** Specificare un nome.
- **Remote IPsec Gateway Address (IP o domain name gateway remoto):** Specificare il gateway VPN sul nodo remoto.
- **Tunnel access from local IP addresses (Accesso tunnel da LAN):** Selezionare per permettere l'accesso ai dispositivi nella LAN locale.
- **IP Address for VPN (Indirizzo IP VPN locale):** Specificare su ogni nodo l'IP della LAN locale.
- **IP Subnetmask (Subnet mask IP locale):** Specificare su ogni nodo la subnet mask in uso sulla LAN locale.
- **Tunnel access from remote IP addresses (Accesso tunnel da dispositivi remote):** 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 che possono essere acceduti.
- **IP Address for VPN (Indirizzo IP VPN remota):** Specificare su ogni nodo l'IP della LAN remota.
- **IP Subnetmask (Subnet mask IP remota):** Specificare su ogni nodo la subnet mask in uso sulla LAN remota.
- **Key Exchange Method (Metodo scambio chiavi):** Selezionare Auto (IKE) o Manual (Manuale).
- **Authentication Method (Metodo autenticazione):** Si raccomanda Pre-Shared Key.
- **Pre-Shared Key (Chiave precondivisa):** 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 **Show Advanced Settings (Avanzate)** per visualizzare la configurazione avanzata.

**Advanced IKE Settings:** Hide Advanced Settings

**Phase 1**

Mode: Main

My Identifier Type: Local Wan IP

My Identifier:

Remote Identifier Type: Remote Wan IP

Remote Identifier:

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time: 3600 Seconds

**Phase 2**

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time: 3600 Seconds

Save/Apply

- **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 **“Advanced Setup (Configurazione avanzata)”** → **“Multicast”** per configurare il protocollo IGMP.

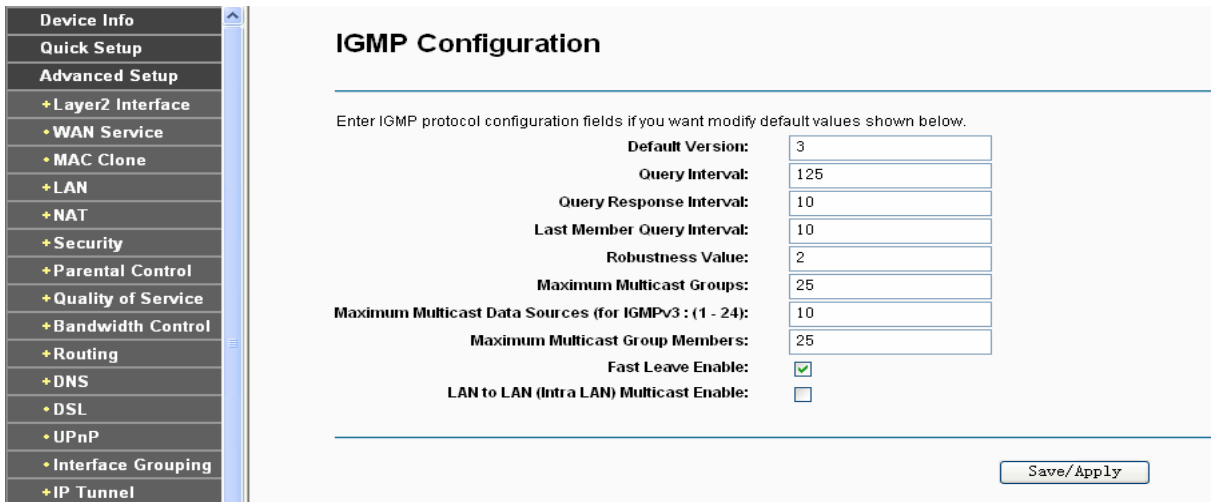
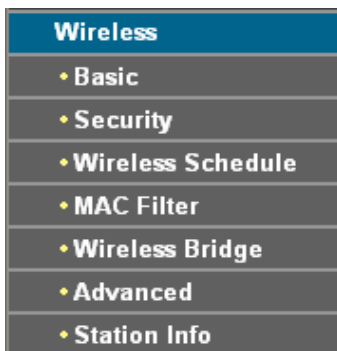


Figura 4-69

Fare clic su **Apply/Save** per salvare le impostazioni.

## 4.5 Wireless



### 4.5.1 Wireless

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

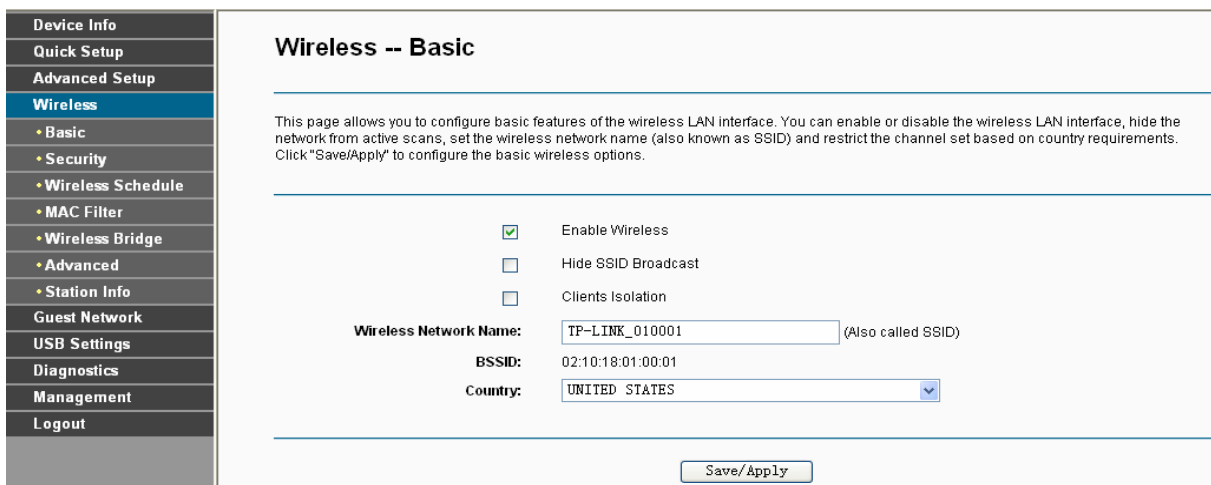


Figura 4-70

- **Enable Wireless (Abilita wireless):** Controllo di abilitazione dell'interfaccia.
- **Hide SSID Broadcast (Nascondi SSID):** Abilitare per rendere la rete non visibile.
- **Clients Isolation (Isolamento client):** Abilitare per impedire la comunicazione tra dispositivi wireless.
- **Wireless Network Name (Nome rete wireless):** Nome identificativo della rete wireless.
- **BSSID:** Indirizzo MAC dell'interfaccia.
- **Country (Regione):** Specificare la regione per non contravvenire la locale normativa.

Fare clic su **Apply/Save** per salvare le impostazioni.

## 4.5.2 Sicurezza

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

The screenshot shows the 'Wireless -- Security' configuration page. On the left is a navigation menu with 'Security' selected. The main content area is divided into two sections: 'WPS' and 'Manual Setup AP'. In the 'WPS' section, 'Enable WPS' is set to 'Enabled' and 'Device PIN' is '49518863'. There are buttons for 'Add Enrollee', 'Gen. new PIN', and 'Help'. The 'Manual Setup AP' section includes 'Network Authentication' (WPA2-Personal), 'Wireless Network Key' (masked with dots), 'WPA Group Rekey Interval' (0), 'WPA Encryption' (AES), and 'WEP Encryption' (Disabled). A 'Save/Apply' button is located at the bottom right.

Figura 4-71

### 4.5.2.1 WPS

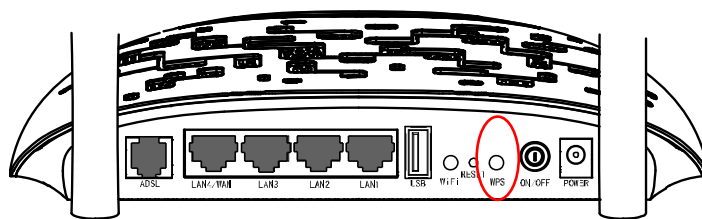
Nota anche come **QSS**, questa funzionalità consente la rapida connessione sicura di nuovi dispositivi.

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 4-76, inserire il PIN del dispositivo e fare clic su **Add Enrollee (Connetti)**.

**Wireless -- Security**

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually or through Wi-Fi Protected Setup(WPS).

**WPS**

Enable WPS:

Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured)

Push-Button
  **PIN**

**Manual Setup AP**

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption type. Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode. Click "Save/Apply" when done.

Network Authentication:

Wireless Network Key:  (Also called WPA Pre-Shared Key)
   
[Click here to display](#)
  
(You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.)

WPA Group Rekey Interval:  (optional)
   
 WPA Encryption: 
  
 WEP Encryption:

Figura 4-76

**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.

**Wireless -- Security**

This page allows you to configure security features of the wireless LAN interface.  
You may setup configuration manually or through Wi-Fi Protected Setup(WPS)

**WPS**

Enable WPS:

Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured)

Push-Button  PIN

Device PIN:   [Help](#)

**Manual Setup AP**

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.  
You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.  
**Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption type.**  
Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP".  
Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode.  
Click "Save/Apply" when done.

Network Authentication:

Wireless Network Key:  (Also called WPA Pre-Shared Key)  
[Click here to display](#)  
(You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.)

WPA Group Rekey Interval:  (optional)

WPA Encryption:

WEP Encryption:

Figura 4-80

➤ **Network Authentication (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-Enterprise (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 .

Device Info
Quick Setup
Advanced Setup
Wireless
• Basic
• <b>Security</b>
• MAC Filter
• Wireless Bridge
• Advanced
• Station Info
Diagnostics
Management

## Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.  
You may setup configuration manually or through Wi-Fi Protected Setup(WPS)

---

**WPS**

Enable WPS:

---

**Manual Setup AP**

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

**Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption type.**

Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP".  
Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode.  
Click "Apply/Save" when done.

Network Authentication:

WPA Group Rekey Interval:  (optional)

RADIUS Server IP Address:

RADIUS Port:  (1-65535)

RADIUS Key:  (optional)  
(You can enter ASCII characters between 0 and 63 characters or 0 to 64 Hexadecimal characters.)

WPA Encryption:

WEP Encryption:

Figura 4-84

- **WPA Group ReKey Interval:** Durata delle chiavi, si consiglia di non modificare il valore predefinito.
- **RADIUS Server IP Address (Indirizzo IP server radius):** Indirizzo del server radius.
- **RADIUS Port (Porta radius):** Porta ascoltata dal server, si consiglia di non modificare il valore predefinito.
- **RADIUS key (Password radius):** Password per l'accesso al server radius.
- **WPA Encryption (Crittografia WPA):** Si consiglia la crittografia AES (TKIP non è compatibile con 802.11n).

Fare clic su **Save/Apply (Salva/Applica)** per applicare le impostazioni.

The screenshot shows the 'Wireless -- Security' configuration page. On the left is a navigation menu with 'Security' selected. The main content area has a title 'Wireless -- Security' and a description: 'This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually or through Wi-Fi Protected Setup(WPS)'. Under the 'WPS' section, 'Enable WPS' is set to 'Disabled'. Below this is the 'Manual Setup AP' section, which includes instructions and a warning about WEP encryption. The configuration fields are: Network Authentication (WPA-Enterprise (good)), WPA Group Rekey Interval (30), RADIUS Server IP Address (192.168.1.20), RADIUS Port (1812), RADIUS Key (masked), WPA Encryption (AES), and WEP Encryption (Disabled). An 'Apply/Save' button is at the bottom.

Figura 4-85

### 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 condivisa.

**Nota:**

WPA potrebbe non essere compatibile con IEEE 802.11n .

The screenshot shows the 'Wireless Security' configuration page with 'Enable WPS' set to 'Enabled'. Under the 'WPS' section, 'Add Client' is selected, and the 'Device PIN' is 49518863. The 'Manual Setup AP' section is also visible, with 'Network Authentication' set to 'WPA-Personal (better/recommended)'. The 'Wireless Network Key' field is empty, with a note '(Also called WPA Pre-Shared Key)'. Other fields include WPA Group Rekey Interval (30), WPA Encryption (AES), and WEP Encryption (Disabled). An 'Apply/Save' button is at the bottom.

Figura 4-86



➤ **Wireless Network Key (Password):** Specificare una password da 8 a 63 caratteri ASCII o da 8 a 64 cifre esadecimali.

➤ **Click here to display (Mostra password):** Fare clic per visualizzare la password.

Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

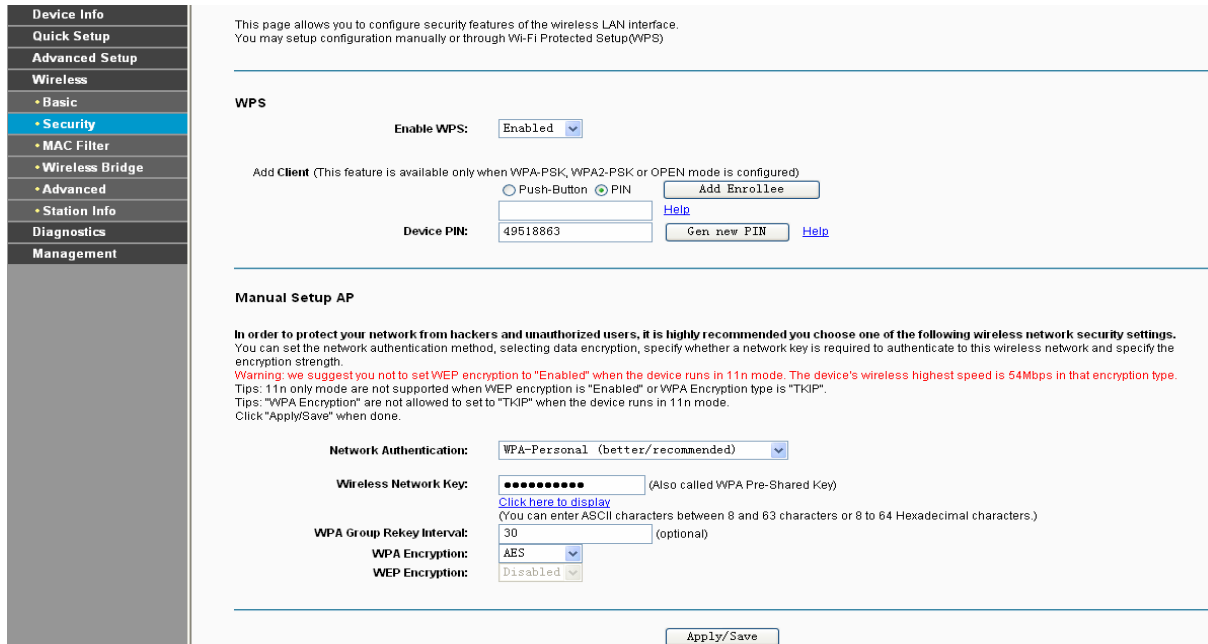


Figura 4-87

#### 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.

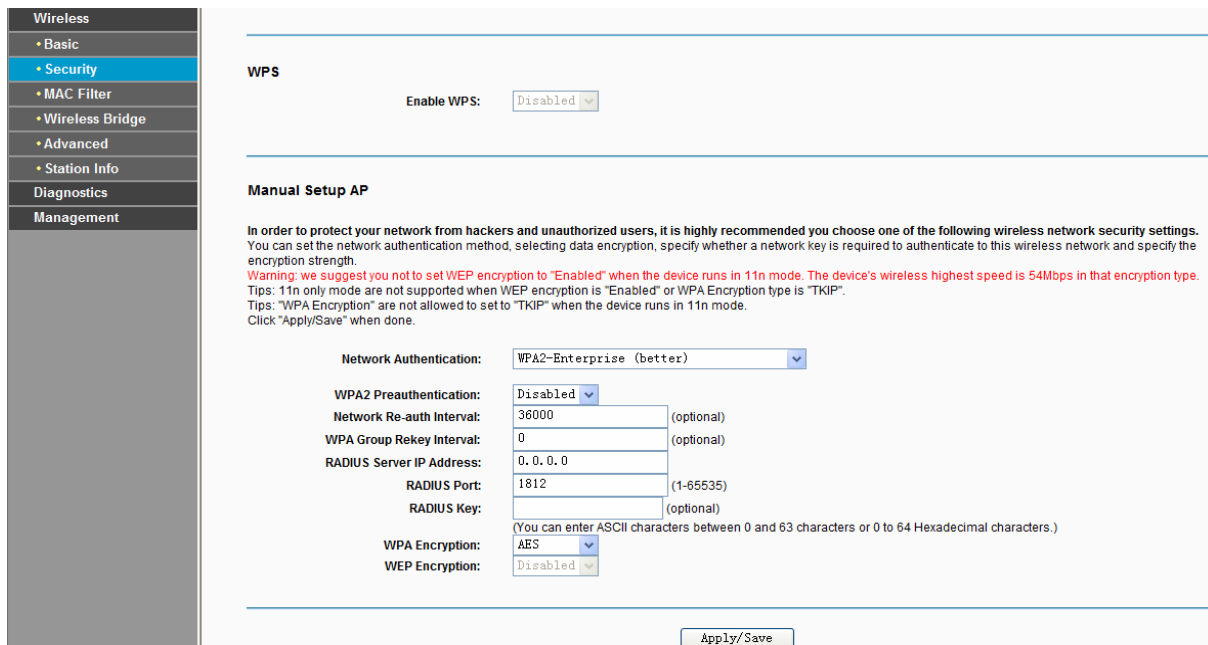


Figura 4-89

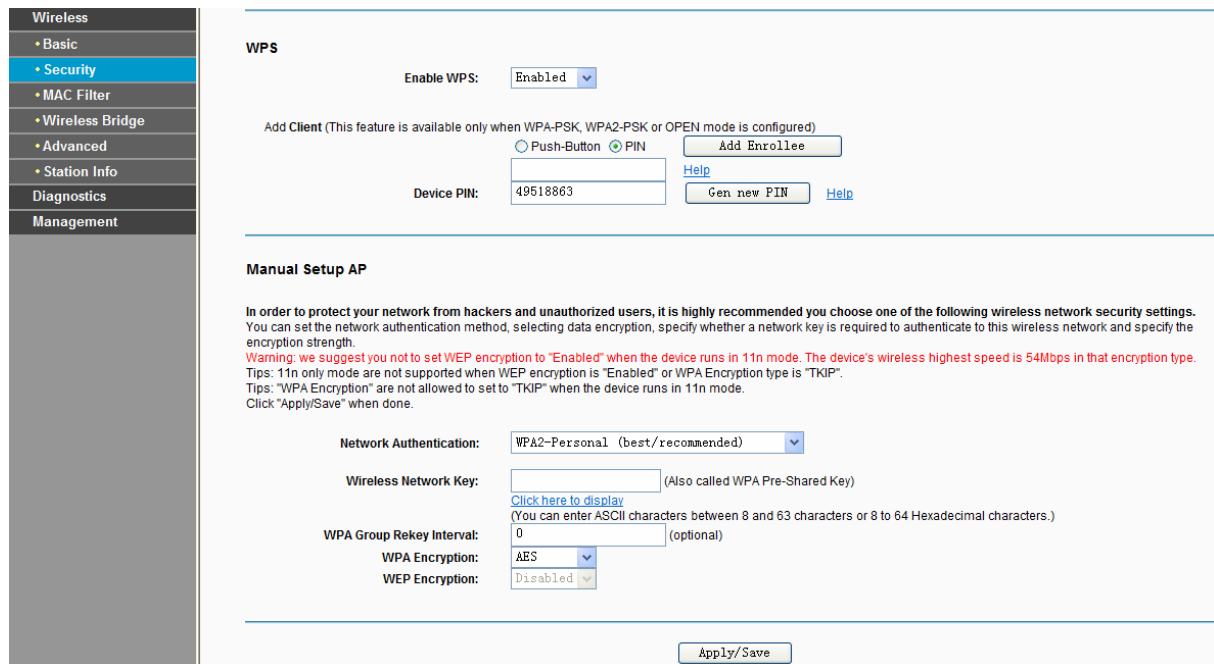
- **WPA2 Preauthentication (Preautenticazione WPA2):** Selezionare per abilitare l'autenticazione in fase di scansione.
- **Network Re-auth Interval (Intervallo riautenticazione):** Si consiglia di non modificare il valore predefinito.

## 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**

- Basic
- **Security**
- MAC Filter
- Wireless Bridge
- Advanced
- Station Info
- Diagnostics
- Management

**WPS**

Enable WPS:

Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured)

Push-Button  PIN

Device PIN:   [Help](#)

---

**Manual Setup AP**

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

**Warning:** we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption type.

Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP".

Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode.

Click "Apply/Save" when done.

Network Authentication:

Wireless Network Key:  (Also called WPA Pre-Shared Key)

[Click here to display](#)  
(You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.)

WPA Group Rekey Interval:  (optional)

WPA Encryption:

WEP Encryption:

Figura 4-90

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

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

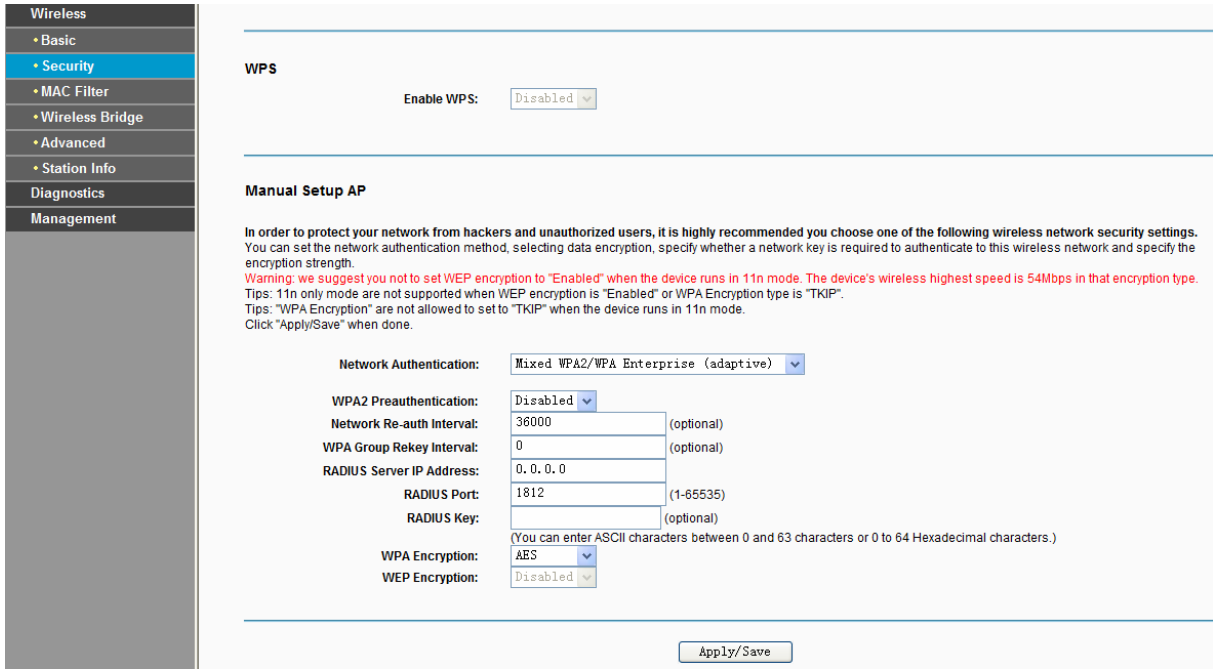


Figura 4-91

### 7. Mixed WPA2/WPA-Personal

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

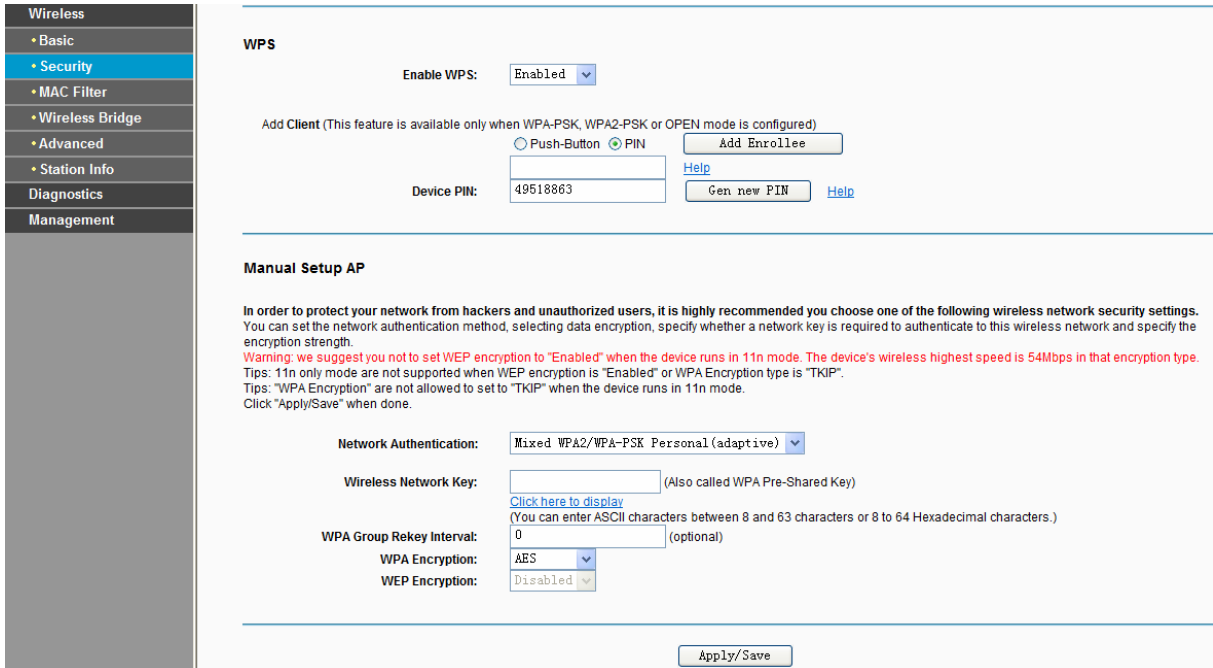


Figura 4-92

### 4.5.3 Timer

Selezionare menu **“Wireless”** → **“Wireless Schedule (Timer)”** per configurare la temporizzazione dell’interfaccia wireless.

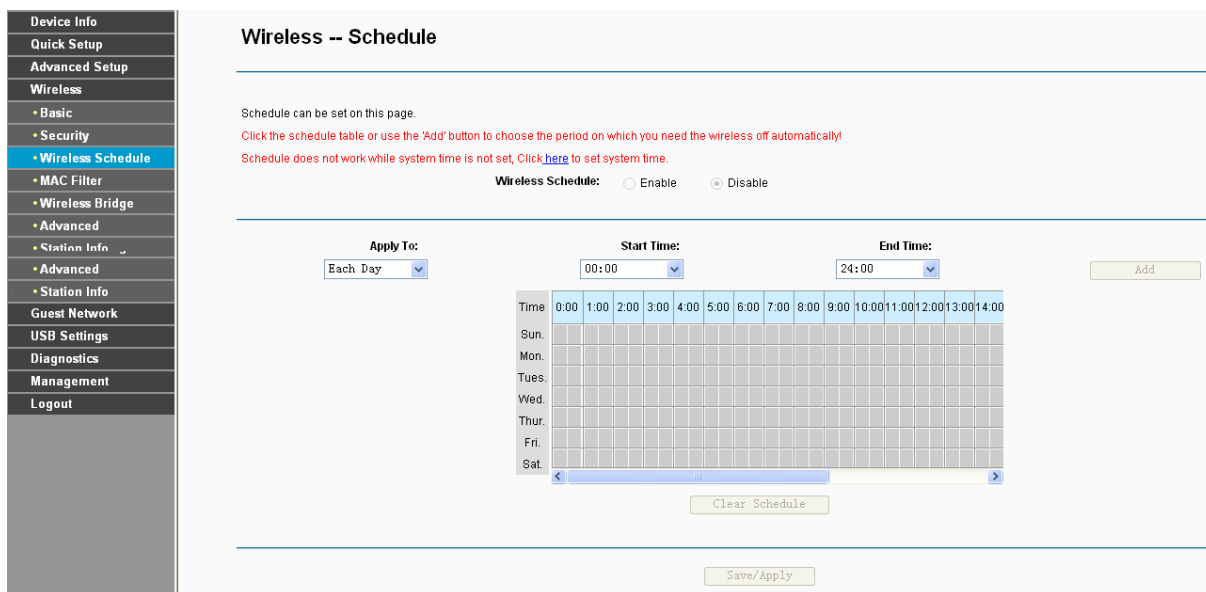


Figura 4-93

**Nota:**

1. Configurare il periodo di spegnimento.
  2. È necessario configurare innanzitutto [4.9.5 Ora Internet](#) .
- **Apply To (Applica il):** Selezionare i giorni.
  - **Start Time, End Time (Inizio, Fine):** Specificare gli orari di inizio e fine blocco.
  - **Add (Aggiungi):** Fare clic per aggiungere la schedulazione definita.

Fare clic su **Clear Schedule (Azzera)** per azzerare la tabella.

Fare clic su **Save** per salvare le informazioni.

### 4.5.4 Filtro MAC

Selezionare “**Wireless**” → “**MAC Filter (Filtro MAC)**” per visualizzare la schermata in Figura 4-94.

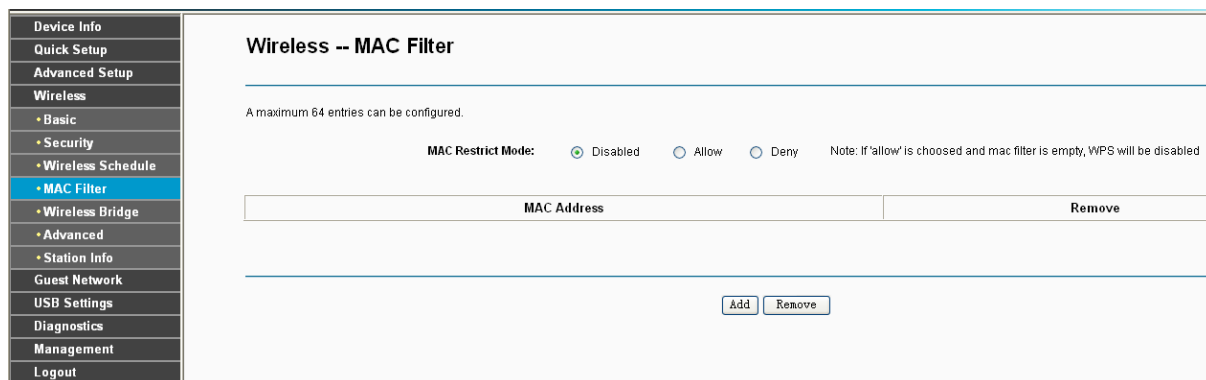


Figura 4-94

Selezionare una delle seguenti modalità.

- **Disabled (Disabilitato):** Filtro inattivo.
- **Allow (Permetti):** Consente la connessione solo ai dispositivi con indirizzo MAC in lista.
- **Deny (Nega):** Blocca la connessione ai dispositivi con indirizzo MAC in lista.

- **Add (Aggiungi):** Fare clic per aggiungere un indirizzo MAC in formato xx:xx:xx:xx:xx:xx come in Figura 4-95.
- **Remove (Elimina):** Fare clic per eliminare gli indirizzi selezionati.

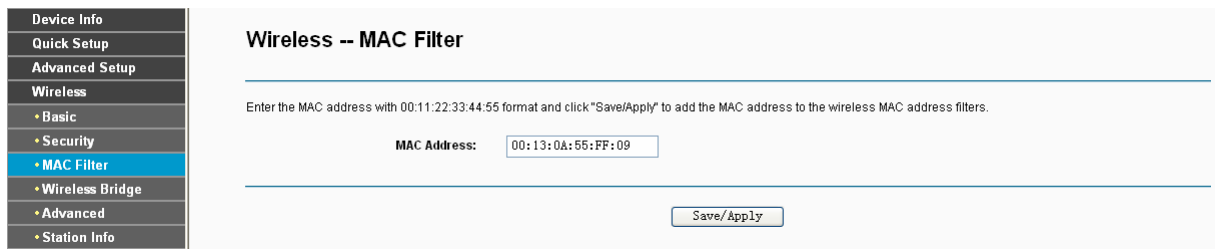


Figura 4-95

Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

### 4.5.5 Bridge wireless

Selezionare **“Wireless”** → **”Wireless Bridge (Bridge wireless)”** per visualizzare la schermata in Figura 4-96.

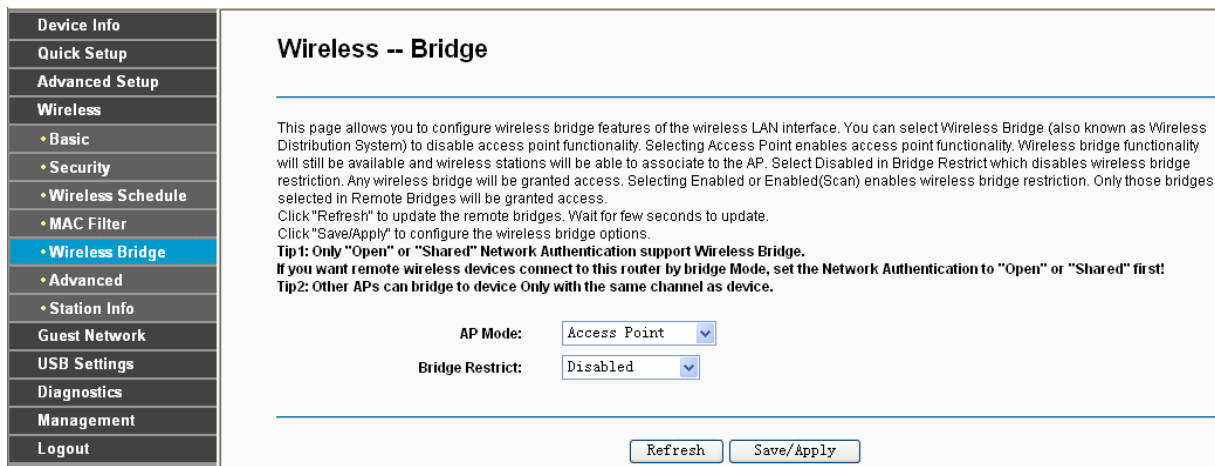


Figura 4-96

- **AP Mode (Modalità AP):** 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 reti.
- **Bridge Restrict (Restrizione bridge):**
  - **Disabled (Disabilitata):** Accesso non regolato.
  - **Enabled (Abilitata):** Accesso consentito solo agli indirizzi MAC specificati.

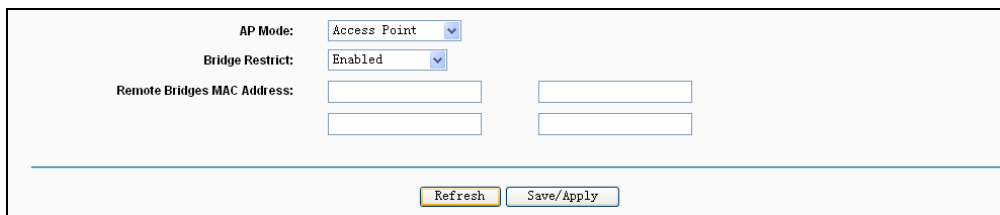


Figura 4-97

- **Enabled (Scan) (Abilitata (Scan)):** Restrizione con scansione automatica.

- **Refresh (Aggiorna):** Fare clic per aggiornare la lista degli access point percepiti.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

	SSID	BSSID
<input type="checkbox"/>	TP-LINK_341108	00:11:22:34:11:08
<input type="checkbox"/>	TP-LINK_334434	00:11:22:33:44:34
<input type="checkbox"/>	TP-LINK_4BFA6A	90:F6:52:4B:FA:6A
<input type="checkbox"/>	TP-LINK_130969	00:0A:EB:13:09:69
<input type="checkbox"/>	TP-LINK_BF5101	40:16:9F:BF:51:01
<input type="checkbox"/>	TP-LINK_BF6005	D8:5D:4C:BF:60:05

Figura 4-98

## 4.5.6 Avanzate

Selezionare **"Wireless" → "Advanced (Avanzate)"** per editare le impostazioni avanzate.

**Wireless -- Advanced**

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point.  
 Tips: If you set Mode to "11n only", you couldn't set Wireless encryption type to "WEP" or "TKIP".  
 Click "Apply/Save" to configure the advanced wireless options.

Channel:

Mode:

Bandwidth:

Control Sideband:

Fragmentation Threshold:

RTS Threshold:

DTIM Interval:

Beacon Interval:

Transmit Power:

WMM/Wi-Fi Multimedia:

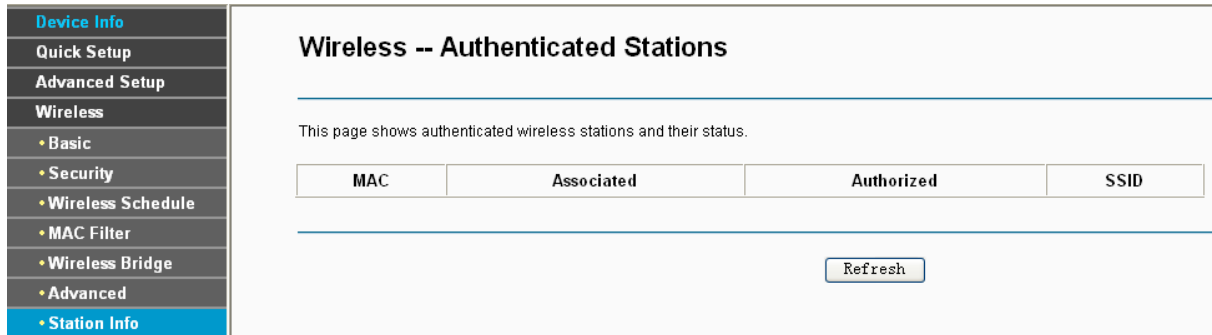
Figura 4-99

- **Channel (Canale):** Selezione del canale in uso. Si raccomanda di modificare il valore predefinito solamente in caso di problemi.
- **Mode (Modalità):** Modalità 802.11 in uso. Si raccomanda di modificare il valore predefinito solamente in caso di problemi.
- **Bandwidth (Ampiezza canale):** Si raccomanda di modificare il valore predefinito solamente in caso di problemi.
- **Control Sideband (Sideband):** Si raccomanda di modificare il valore predefinito solamente in caso di problemi.
- **Fragmentation Threshold (Soglia di frammentazione):** Dimensione massima dei pacchetti. Si raccomanda il valore predefinito.
- **RTS Threshold (Soglia RTS):** Soglia Request to Send. Si consiglia il valore predefinito.
- **DTIM Interval (Intervallo DTIM):** Si raccomanda il valore predefinito. Sono utilizzabili valori nel range 1-255.

- **Beacon interval (Intervallo Beacon):** Si raccomanda il valore predefinito. Sono utilizzabili valori nel range 25-1000ms.
- **Transmit power (Potenza trasmittiva):** 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 Dispositivi collegati

Selezionare “Wireless” → “Station Info (Stato)” per visualizzare i dispositivi collegati.



The screenshot shows the 'Station Info' page under the 'Wireless' section. The page title is 'Wireless -- Authenticated Stations'. Below the title, there is a text line: 'This page shows authenticated wireless stations and their status.' A table with four columns is present: 'MAC', 'Associated', 'Authorized', and 'SSID'. The table is currently empty. Below the table, there is a 'Refresh' button.

Figura 4-100

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

Fare clic su **Refresh (Aggiorna)** per aggiornare la pagina.

## 4.6 Rete guest



The screenshot shows a sidebar menu with the following items: 'Guest Network' (highlighted), 'Basic', and 'Station list'.

### 4.6.1 Rete guest

Selezionare “Guest Network (Rete guest)” → “Basic (Rete guest)” per configurare una rete isolata dedicata a dispositivi ospite come Figura 4-101.

Figura 4-101

- **Guest SSID (SSID guest):** Nome della rete guest.
- **Authentication Type (Autenticazione):** Si consiglia WPA2-Personal (WPA2-PSK).
- **Encryption (Crittografia):** Si consiglia AES.
- **Wireless Password (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.
- **Allow Guests to access my Local Network (Accesso ospiti alla rete locale):** Permette l'accesso degli ospiti a dispositivi nella rete locale, senza accesso alla console di gestione.
- **Allow Guests to access my USB Storage Sharing (Accesso alle condivisioni USB):** Permette l'accesso degli ospiti alle condivisioni USB.
- **Guest Network Isolation (Isolamento rete guest):** L'isolamento impedisce ad ogni dispositivo di comunicare con gli altri dispositivi senza fili.
- **Guest Network Bandwidth Control:** La funzionalità permette di limitare la banda offerta ai dispositivi ospite.

Fare clic su **Save/Apply (Salva/Applica)** per applicare le impostazioni.

## 4.6.2 Dispositivi collegati

Selezionare **“Guest Network (Rete guest)”** → **“Station list (Dispositivi collegati)”**.

MAC	Associated	Authorized	SSID

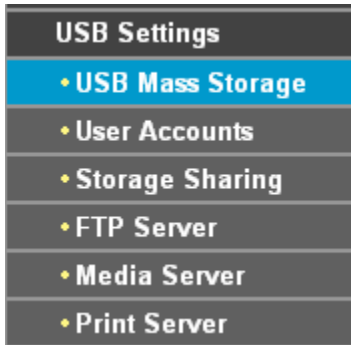
Figura 4-102



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

Fare clic su **Refresh (Aggiorna)** per aggiornare la pagina.

## 4.7 USB



### 4.7.1 Storage USB

Selezionare “**USB Settings (USB)**” → “**USB Mass Storage (Storage USB)**” per configurare la condivisione storage.

**USB Mass Storage**

This page provides the basic information about the connected USB mass storage, to configure Storage Sharing/FTP/Media Server, please click the corresponding menu on the left side.

**USB Mass storage List:**  
Disk1: Samsung U5 Rev. 0100 [Connected](#) [Disconnect](#)

Volume	File System	Capacity	Status	Action
usb1_1	FAT32	1.8 GB	Activated	<a href="#">Deactivate</a>

[Refresh](#)

Note:

1. Click the REFRESH button to detect your USB device. The Modem Router will automatically activate the first two USB storage devices or up to eight volumes.
2. If you want to use other volumes in your storage device(s), please "Deactivate" some unused volumes and "Activate" the other desired volumes.
3. Click "Disconnect" button before unplugging your USB device to avoid data loss or damage to the device.
4. **Supported USB Mass Storage:** hard disk, flash disk or memory card reader;  
**Supported File System Type:** FAT32 and NTFS;  
**Supported Volumes:** Only two USB storage devices with up to eight volumes could be activated simultaneously, up to four USB storage devices with about eighteen volumes could be recognized.

Figura 4-103

- **Volume:** Nome del volume montabile.
- **File System:** File system in uso sul dispositivo.
- **Capacity (Capacità):** Capacità del dispositivo.
- **Status (Stato):** **Online** indica che il volume può essere condiviso, **Offline** no. Abilitando **Deactivate (Disattiva)** verrà visualizzato lo stato, **Disabled (Disabilitato)**.
- **Action (Azione):** Fare clic su **Deactivate (Disattiva)** per interrompere la condivisione del volume o su **Enable (Attiva)** per attivarla.

Fare clic su **Disconnect (Disconnetti)** per rimuovere il dispositivo USB in sicurezza.

## 4.7.2 Account utente

È possibile configurare le 5 utenze disponibili e le autorizzazioni per i servizi USB. Lo storage condiviso può essere acceduto localmente digitando [\\192.168.1.1](http://192.168.1.1) (od altro IP del modem/router se modificato) in Esplora File. L'accesso remoto è invece possibile tramite client FTP.

L'utente admin ha permessi illimitati.

The screenshot shows the 'User Accounts' configuration page. On the left is a navigation menu with 'User Accounts' selected. The main content area has a title 'User Accounts' and a subtitle 'This page allows you to configure user accounts for Storage Sharing/FTP Server.' Below this is a table with 5 rows and 4 columns: Index, Username, Status, and Action. The first row shows 'admin\*' with status 'Enabled' and 'Enable/Disable' buttons. Below the table is a note: '\*: "Super User", It has full-access permission to all active volume(s) and shared folder(s).' At the bottom is a form with fields for 'Choose Index' (a dropdown menu), 'New Username', 'New Password', and 'Confirm Password', followed by a 'Set' button.

Index	Username	Status	Action
1	admin*	Enabled	<input type="radio"/> Enable <input type="radio"/> Disable
2			
3			
4			
5			

Figura 4-104

Per aggiungere un account procedure come segue.

1. Selezionare l'indice.
2. Specificare un nome utente.
3. Specificare una password e confermarla.

Fare clic su **Set** per salvare l'account.

## 4.7.3 Condivisione storage

Selezionare “**USB Settings (USB)**” → “**Storage Sharing (Condivisione storage)**” per gestire le proprietà delle condivisioni.

The screenshot shows the 'Storage Sharing Settings' page. On the left is a navigation menu with 'Storage Sharing' selected. The main content area has a title 'Storage Sharing Settings' and a subtitle 'Storage Sharing allows you to share the files on the USB storage device with other computers locally.' Below this is a 'Server Status' section with 'Enabled' selected and a 'Disable' button. There is also a checked checkbox for 'Anonymous access to all the volumes'. Below this is a 'Note' section with three points: 1. Storage Sharing function is based on NetBIOS/SMB protocol which is supported by most Windows operating system and some other operating systems. 2. anonymous: All active volume(s) will be shared and authentication is not required. 3. You will be able to access the folders with the following methods: For Windows OS: Open "Run" window in the Start menu and enter \\(IP Address) or \\(IP Address)\(Share Name) e.g. \\192.168.1.1 or \\192.168.1.1\photo; For Mac OS: Open "Connect to Server" window in the Go menu and enter smb://(IP Address) or smb://(IP Address)\(Share Name) e.g. smb://192.168.1.1 or smb://192.168.1.1/photo.

Figura 4-105

➤ **Server Status (Stato server):** Stato di attivazione del server SMB.

- **Anonymous access to all the volumes (Accesso anonimo indiscriminato):** Consente l'accesso indiscriminato a tutte le condivisioni a tutti gli utenti.

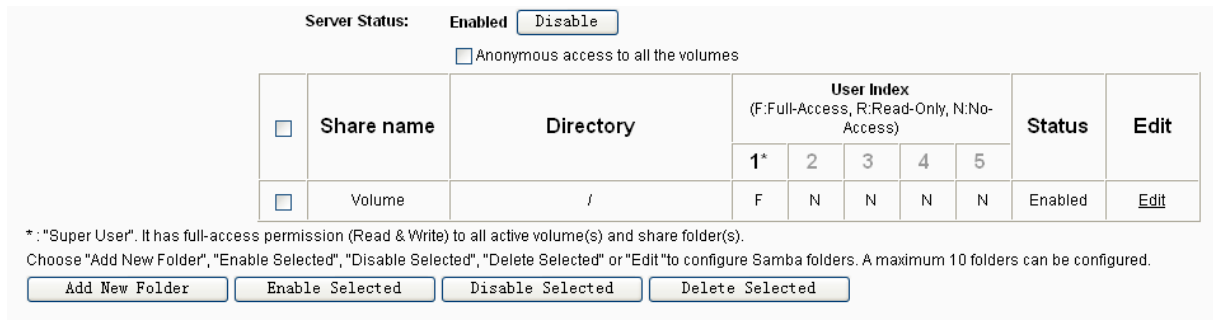


Figura 4-106

- **Share Name (Nome condivisione):** Nome pubblico della condivisione.
- **Directory:** Percorso della directory nel file system.
- **User Index (Indice utente):** Autorizzazioni assegnate a ciascun utente per la condivisione in oggetto.
- **Status (Stato):** Stato di abilitazione della condivisione.
- **Edit (Modifica):** Fare clic per modificare la condivisione.

Per aggiungere una condivisione procedere come segue.

1. Fare clic su **Add New Folder (Aggiungi)** in Figura 4-106.

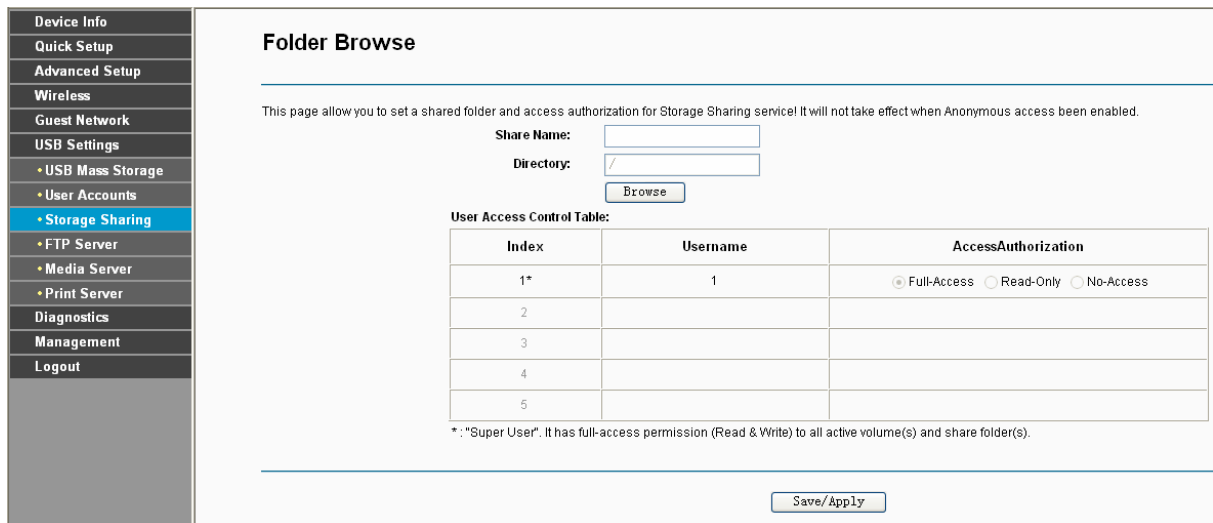


Figura 4-107

2. Fare clic su **Browse (Sfoggia)** e selezionare il volume dalla lista.
3. Specificare il nome della condivisione nel campo **Share Name (Nome condivisione)**.
4. Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

Fare clic su **Enable/Disable Selected (Abilita/disabilita selezione)** per gestire le condivisioni selezionate.

Fare clic su **Delete Selected (Elimina selezione)** per cancellare le condivisioni selezionate.

**Nota:**

È possibile configurare fino a 10 condivisioni.

#### 4.7.4 Server FTP

Selezionare “**USB Settings (USB)**” → “**FTP Server (Server FTP)**” per configurare la condivisione storage remota.

**FTP Server Settings**

FTP (File Transfer Protocol) server allows you to share the files on the USB storage device to the local or public network. You will need to define the shared folders and assign the user's authorization for the different folders.

Server Status:  Enabled  Disable

Internet Access:  Enable  Disable

Internet Address: 0.0.0.0

Service Port:  (The default is 21. Do not change unless necessary.)

Choose "Add New Folder", "Enable Selected", "Disable Selected", "Delete Selected" or "Edit" to configure ftp folders. A maximum 10 folders can be configured.

**Folder Table:**

	Share name	Directory	User Index (F:Full-Access, R:Read-Only, N:No-Access)					Status	Edit
			1*	2	3	4	5		
<input type="checkbox"/>	Volume	/	F	N	N	N	N	Enabled	Edit

\*.: "Super User". It has full-access permission (Read & Write) to all active volume(s) and share folder(s).

Note:  
 1. You could be able to access the folders by entering the following URL on Windows Explorer or other FTP software: ftp://(IP Address) eg. ftp://192.168.1.1  
 2. FTP Server will get restarted and all your current FTP connections will be terminated after you click Apply button.

Figura 4-108

- **Server Status (Stato):** Stato del server FTP.
- **Internet Access (Accesso da Internet):** Abilita l'accesso alle condivisioni da Internet.
- **Internet Address (Indirizzo Internet):** Se l'accesso da Internet è abilitato viene mostrato l'IP WAN al quale raggiungere le condivisioni.
- **Service Port (Porta):** Si consiglia di non modificare la porta predefinita.
- **Share Name (Nome condivisione):** Nome pubblico della condivisione.
- **Directory:** Percorso della condivisione nel file system.
- **User Index (Indice utente):** Indice dell'utente.
- **Status (Stato condivisione):** Stato di attivazione della condivisione.
- **Edit (Modifica):** Fare clic per modificare la condivisione.

**Per aggiungere una condivisione procedere come segue.**

1. Fare clic su **Add New Folder (Aggiungi)** in Figura 4-108.

**Folder Browse**

This page allow you to set a shared folder and access authorization for Ftp services!

Share Name:

Directory:

User Access Control Table:

Index	Username	AccessAuthorization
1*	1	<input checked="" type="radio"/> Full-Access <input type="radio"/> Read-Only <input type="radio"/> No-Access
2		
3		
4		
5		

\*: "SuperUser". It has full-access permission (Read & Write) to all active volume(s) and share folder(s).

Figura 4-109

2. Fare clic su **Browse (Sfoglia)** e selezionare il volume dalla lista.
3. Specificare il nome della condivisione.
4. Fare clic su **Save/Apply (Salva/Applica)** per salvare le impostazioni.

Fare clic su **Enable/Disable Selected (Abilita/disabilita selezione)** per gestire le condivisioni selezionate.

Fare clic su **Delete Selected (Elimina selezione)** per cancellare le condivisioni selezionate.

**Nota:**

È possibile configurare fino a 10 condivisioni.

#### 4.7.5 Media Server

Selezionare **"USB Settings (USB)"** → **"Media Server"** per gestire lo streaming multimediale.

**Media Server Settings**

Server Enable:  Enable  Disable

Server Name:

Content Scan: Manual Scan:

Auto Scan Every  hour(s)

Figura 4-110

- **Server Enable (Abilita server):** Selezionare per abilitare il server.

- **Server Name (Nome condivisione):** Nome del catalogo pubblicato dal server.

Per aggiungere una cartella condivisa procedure come segue.

1. Fare clic su **Add New Folder (Aggiungi)** in Figura 4-111.

**Folder Browse**

This page allow you to set a scan folder for DLNA media service!

Share Name:

Directory:

Select Volume:

Figura 4-111

2. Specificare il nome della cartella condivisa.
3. Fare clic su **Save/Apply (Salva/Applica)**.

**Media Server Settings**

Server Enable:  Enable  Disable

Server Name:

Content Scan: Manual Scan:   Auto Scan Every  hour(s)

Choose "Add New Folder", "Edit" or "Delete" to configure Dina folders. A maximum 4 folders can be configured.  
You have shared the following contents:

ID	Share Name	Folder Name	Edit
1	1	/	<a href="#">Edit</a> <a href="#">Delete</a>

Figura 4-112

4. Fare clic su **Scan Now (Scansione)** per rilevare immediatamente I file multimediali. La funzione **Auto-Scan** scansiona le cartelle con la frequenza specificata.

**Nota:**

È possibile configurare fino a 6 cartelle condivise.

#### 4.7.6 Print Server

Selezionare **"USB Settings (USB)"** → **"Print Server"**.

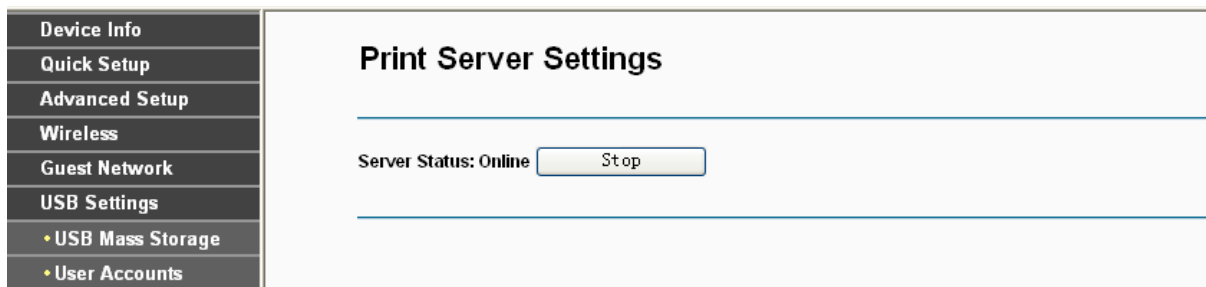


Figura 4-113

Il server può assumere i seguenti stati

- **Online:** Server in linea, fare clic su **Stop** per arrestarlo.
- **Offline:** Server arrestato, fare clic su **Start** per avviarlo.
- **Busy (In uso):** Server operativo.

## 4.8 Diagnostica

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

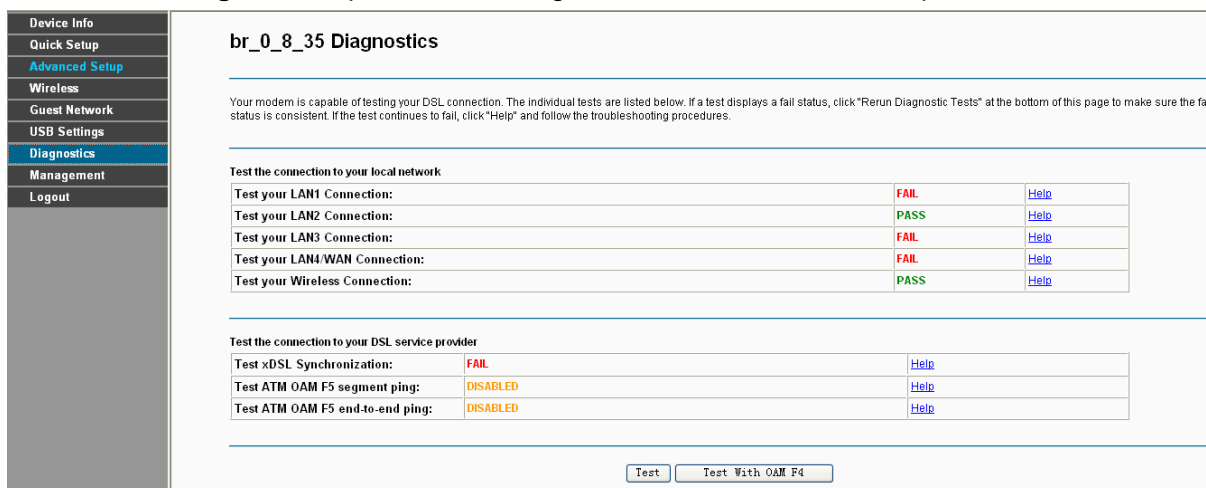
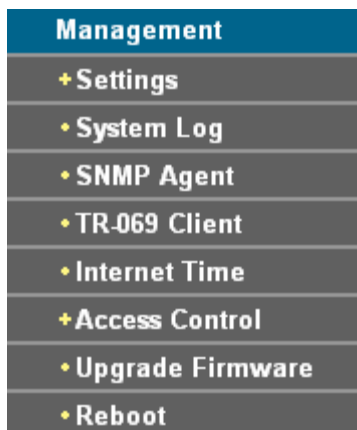


Figura 4-114

## 4.9 Gestione



## 4.9.1 Configurazione

La sezione permette backup e ripristino della configurazione.

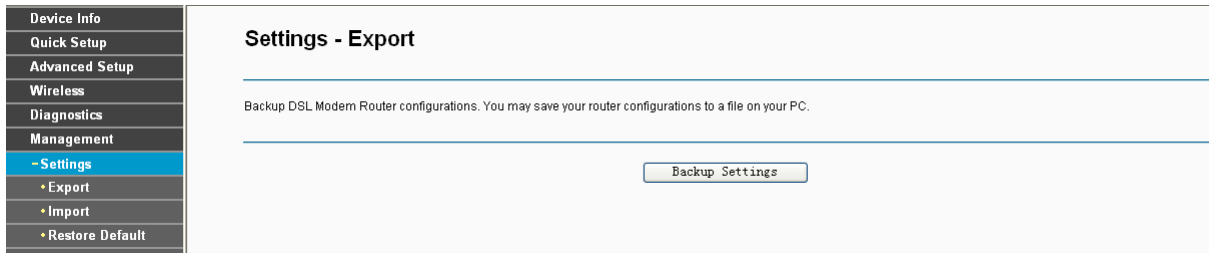


Figura 4-115

### 4.9.1.1 Esportazione

Selezionare **“Management (Gestione)”** → **“Settings (Configurazione)”** → **“Export (Esporta)”**, per visualizzare la schermata in Figura 4-116.

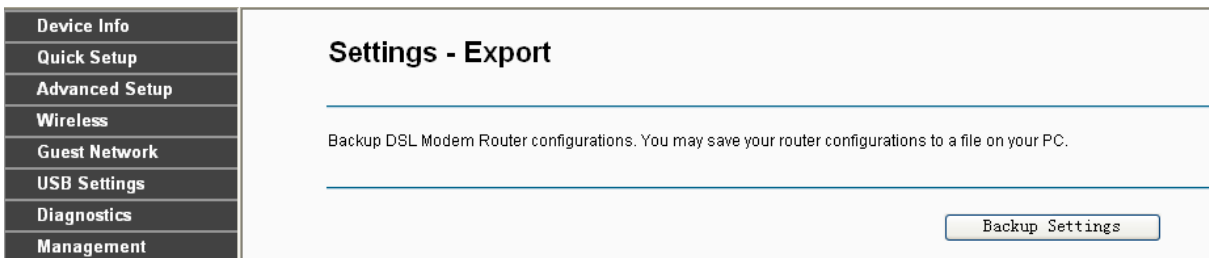


Figura 4-116

Per esportare su file la configurazione procedere come segue.

1. Fare clic su **Export Settings (Esporta)** in Figura 4-116).

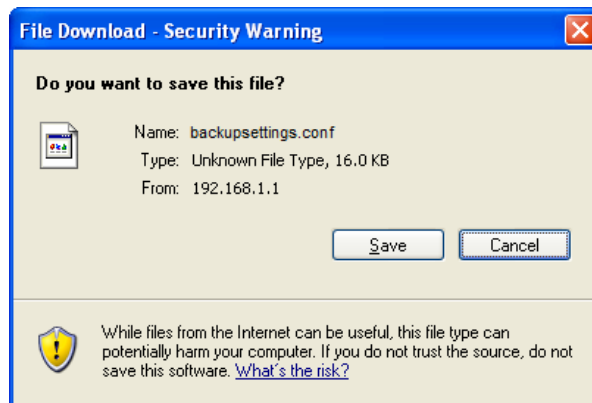


Figura 4-117

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

### 4.9.1.2 Importazione

Selezionare **“Management (Gestione)”** → **“Settings (Configurazione)”** → **“Import (Importazione)”** per visualizzare la schermata in Figura 4-119.



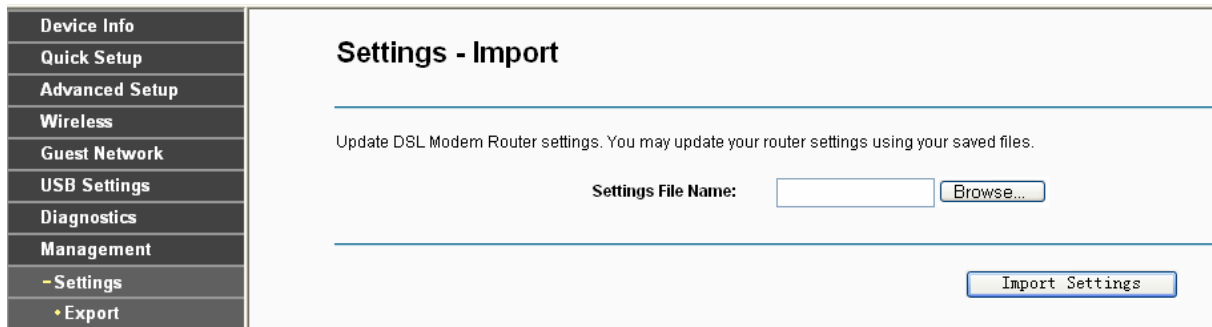


Figura 4-119

Per importare la configurazione da file procedere come segue.

1. Fare clic su **Browse (Sfogliare)** e selezionare il file da importare.
2. Fare clic su **Import Settings (Importa)**.

**Nota:**

Attendere il riavvio del modem/router.

#### 4.9.1.3 Ripristino configurazione predefinita

Selezionare **“Management (Gestione)”** → **“Settings (Configurazione)”** → **“Restore Default (Ripristino)”** per visualizzare la schermata in Figura 4-120.

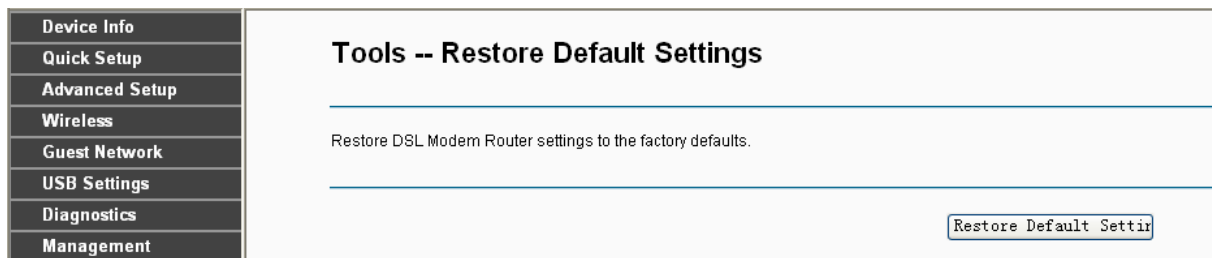


Figura 4-120

- **Restore Default Settings (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.

#### 4.9.2 Log di sistema

Selezionare **“Management (Gestione)”** → **“System Log (Log di Sistema)”** per visualizzare la schermata in Figura 4-121.

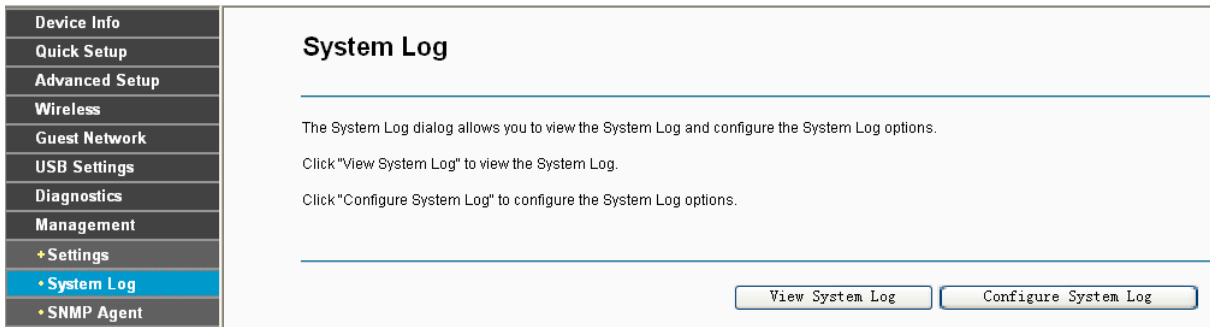


Figura 4-121

Per visualizzare il log fare clic su **View System Log (Visualizza log)** in Figura 4-122.

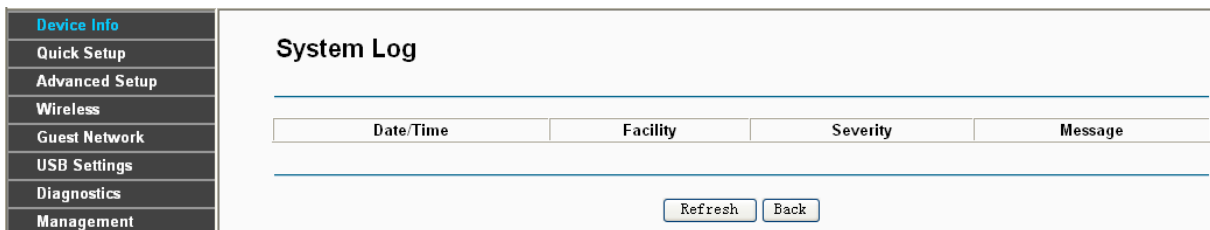


Figura 4-122

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

Per configurare il log di sistema fare clic su **Configure System Log (Configura log)** in **Figura 4-121**.

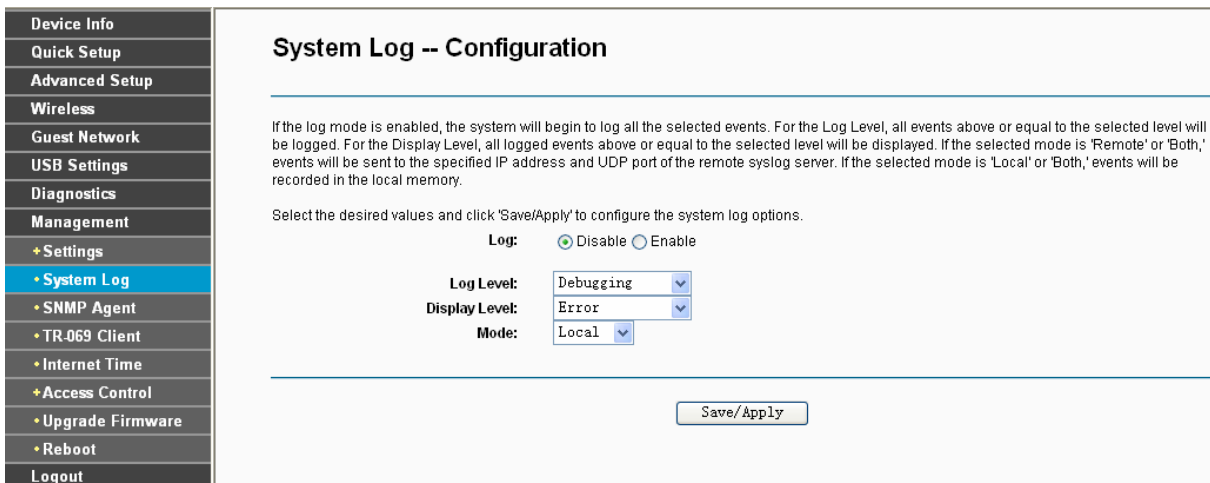


Figura 4-123

- **Disable/Enable (Abilita / Disabilita):** Stato di abilitazione del server log.
- **Log Level (Livello log):** Saranno loggati solamente gli eventi di livello pari o superiore al livello ivi specificato.
- **Display Level (Livello display):** Saranno visualizzati solamente gli eventi di livello pari o superiore al livello ivi specificato.
- **Mode (Modalità):** Specificare se salvare gli eventi sulla memoria locale, su server remoto o su entrambi.

### 4.9.3 SNMP

Selezionare “**Management (Gestione)**” → “**SNMP Agent (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 - Configuration**

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Save/Apply" to configure the SNMP options.

**SNMP Agent:**  Disable  Enable

**Read Community:**

**Set Community:**

**System Name:**

**System Location:**

**System Contact:**

**Trap Manager IP:**

Figura 4-124

- **SNMP Agent (Agente SNMP):** 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”.
- **System Name (Nome sistema):** Nome del dispositivo in uso visualizzato sul trap manager.
- **System Location (Posizione):** Posizione fisica del dispositivo.
- **System Contact (Amministratore):** Specifiche di contatto per l’amministratore del dispositivo.
- **Trap Manager IP (IP trap manager):** Indirizzo IP del trap manager.

Fare clic su **Save/Apply (Salva/Applica)** per applicare le impostazioni.

### 4.9.4 TR-069

Selezionare “**Management (Gestione)**” → “**TR-069**” per visualizzare la schermata in Figura 4-125.

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

Figura 4-125

- **Inform:** Controllo di abilitazione della funzionalità.
  - **Inform Interval (Intervallo inform):** Frequenza di inform al server ACS.
  - **ACS URL (URL ACS):** URL del server ACS.
  - **ACS User Name (Nome utente ACS):** Nome utente per l'accesso al server ACS.
  - **ACS Password (Password ACS):** Password per l'accesso al server ACS.
  - **WAN Interface used by TR-069 Client (WAN TR-069):** Interfaccia WAN per la comunicazione con il server ACS.
  - **Connection Request User Name (Nome utente):** Nome utente per l'accesso TR-069 al dispositivo.
  - **Connection Request Password (Password):** Password per l'accesso TR-069 al dispositivo.
- Fare clic su **Save/Apply (Salva/Applica)** per applicare le impostazioni.

#### 4.9.5 Ora Internet

Selezionare “**Management (Gestione)**” → “**Internet Time (Ora Internet)**” per gestire l'orologio di sistema.

Device Info
Quick Setup
Advanced Setup
Wireless
Guest Network
USB Settings
Diagnostics
Management
+ Settings
+ System Log
+ SNMP Agent
+ TR-069 Client
+ Internet Time
+ Access Control
+ Upgrade Firmware
+ Reboot

## Time settings

This page allows you to the modem's time configuration.

**Date/Time :** Thu Jan 1 17:29:44 1970  
**Date/Time on your PC :** Tue Jul 2 11:02:07 2013

Setup Adsl Modem Router's Date/Time

**Date (Y/M/D) :**   
**Time (H:M:S) :**

Automatically synchronize with Internet time servers

Figura 4-126

## 4.9.6 Amministrazione

- Access Control
+ Passwords
+ Remote Access

### 4.9.6.1 Password

Selezionare **“Management (Gestione)”** → **“Access Control (Amministrazione)”** → **“Password”** per configurare le credenziali di accesso all’interfaccia di gestione.

Device Info
Quick Setup
Advanced Setup
Wireless
Guest Network
USB Settings
Diagnostics
Management
+ Settings
+ System Log
+ SNMP Agent
+ TR-069 Client
+ Internet Time
- Access Control
+ Passwords
+ Remote Access
+ Upgrade Firmware
+ Reboot
Logout

## Access Control -- Passwords

Access to your DSL Modem Router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Modem Router.

The user name "support" is used to allow an ISP technician to access your DSL Modem Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Modem Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Save/Apply" to change or create passwords. Note: Password cannot contain a space.

**Username:**    
**Old Password:**   
**New Password:**   
**Confirm Password:**

Figura 4-127

**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 **Save/Apply (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.

#### 4.9.6.2 Accesso remoto

Selezionare **"Management (Gestione)"** → **"Access Control (Amministrazione)"** → **"Remote Access (Accesso remoto)"** per configurare l'accesso remoto alla console.

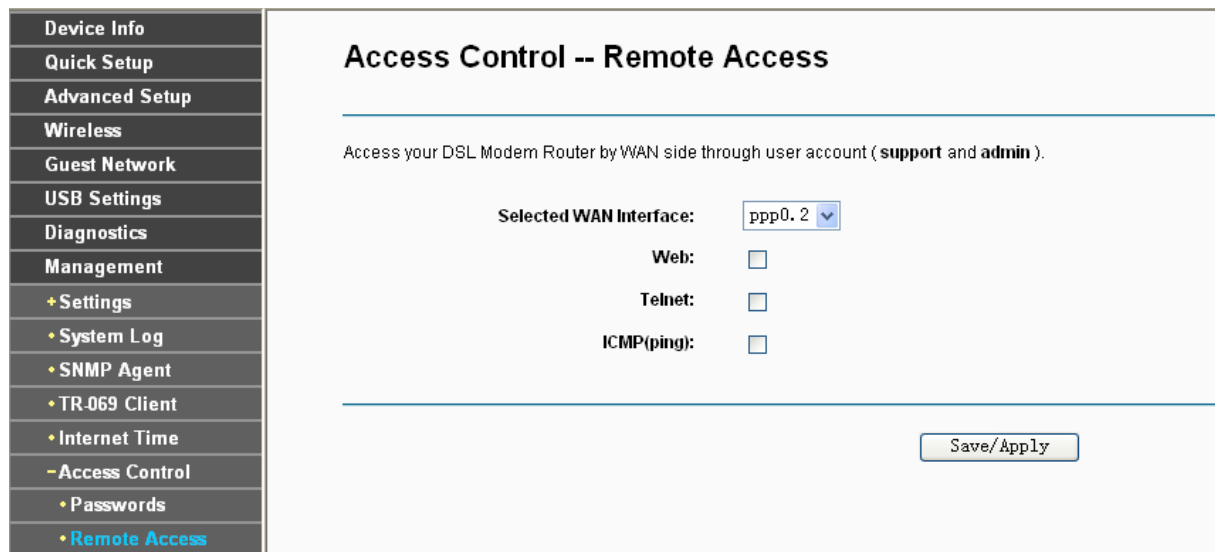


Figura 4-128

- **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 **Save/Apply (Salva/Applica)** per salvare le impostazioni.

#### 4.9.7 Aggiornamento

Selezionare **"Management (Gestione)"** → **"Update Firmware (Aggiornamento)"** per visualizzare la schermata in Figura 4-129.

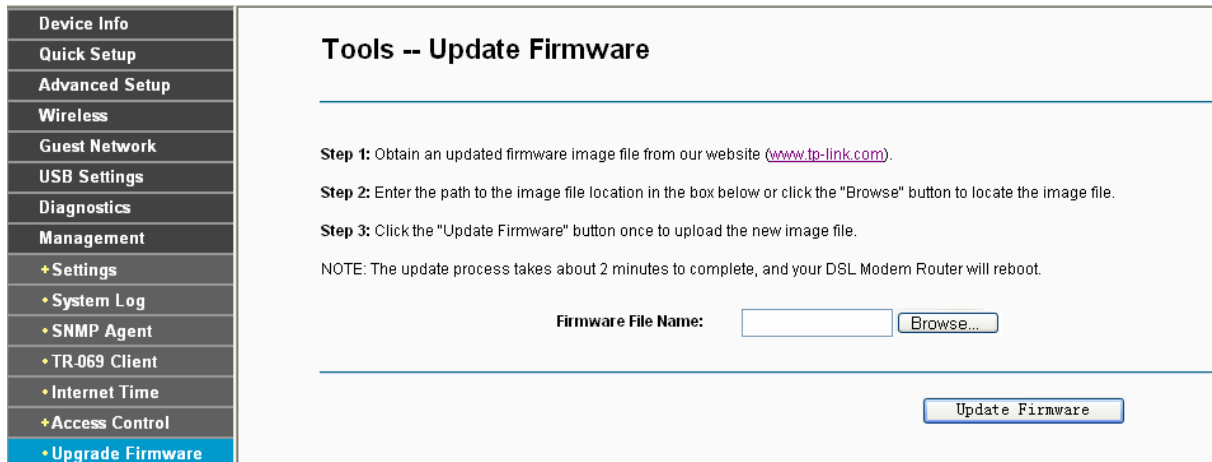


Figura 4-129

- **Browse (Sfoggia):** Fare clic per selezionare il firmware da caricare.
- **Update Firmware (Aggiorna):** 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.it>.
2. Estrarre il file contenente il firmware dell'archivio .zip scaricato.
3. Fare clic su **Browse (Sfoggia)** per selezionare il file estratto contenente il firmware.
4. Fare clic su **Update Firmware (Aggiorna)**.

 **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.

#### 4.9.8 Riavvio

Selezionare “**Management (Gestione)**” → “**Reboot (Riavvio)**” per visualizzare la schermata in Figura 4-130 e procedere al riavvio.

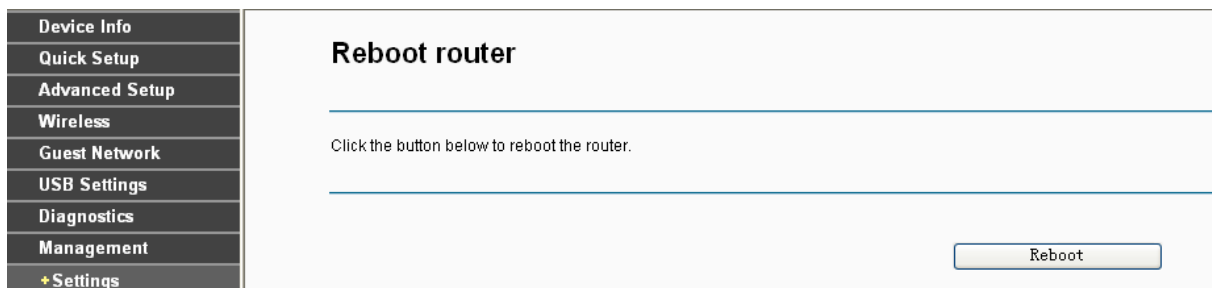


Figura 4-130

#### 4.10 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
	USB: 1 x USB 2.0
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, USB, 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?

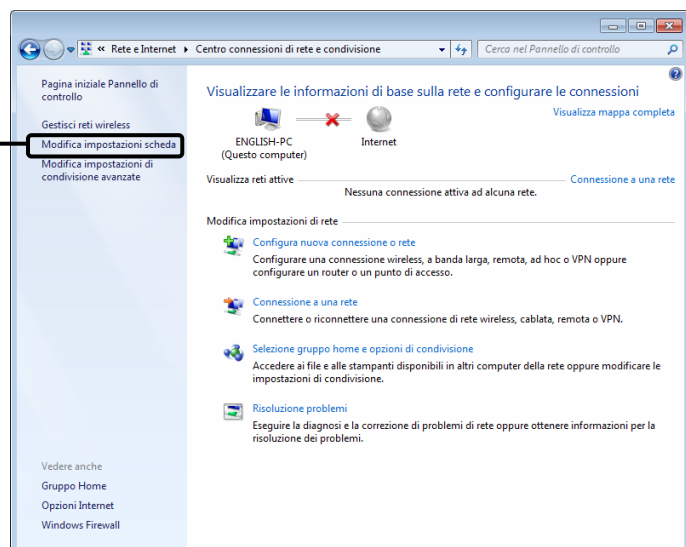
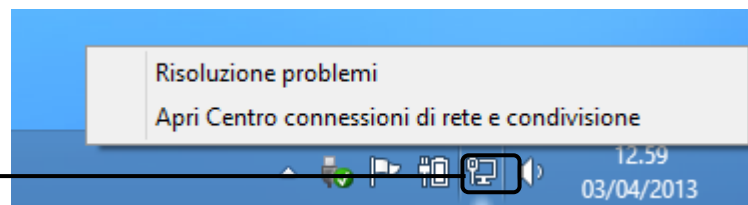
- 1) Secondo il sistema operativo in uso, configurare l'indirizzo IP del computer come segue.

#### Per Windows® 7 / 8

Clic col tasto destro sull'icona della rete in prossimità dell'orologio di sistema, nell'angolo basso destro dello schermo.

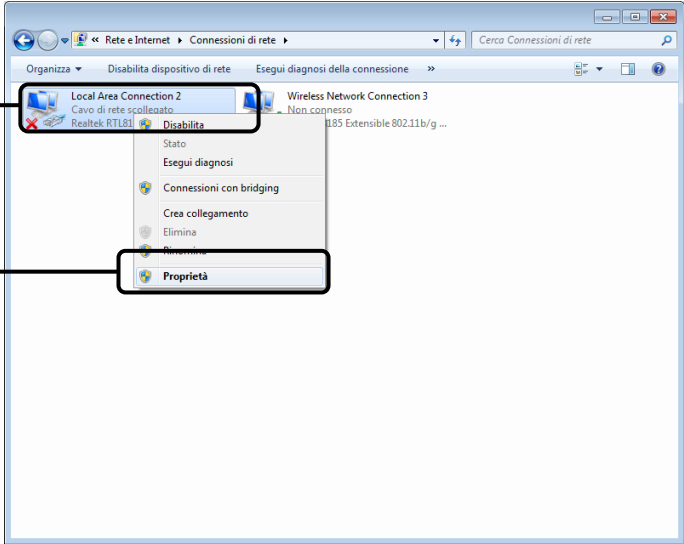
Selezionare quindi **Apri Centro connessioni di rete e condivisione**.

Clic su **Change adapter settings (Modifica impostazioni scheda)**

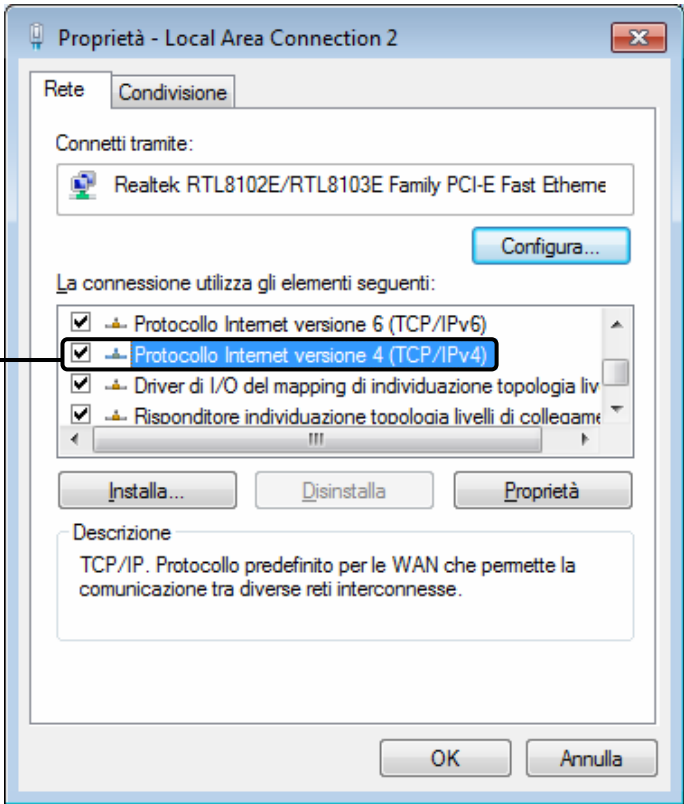


Clic destro su **Local Area Connection (Connessione alla rete locale LAN)**

Clic su **Properties (Proprietà)**



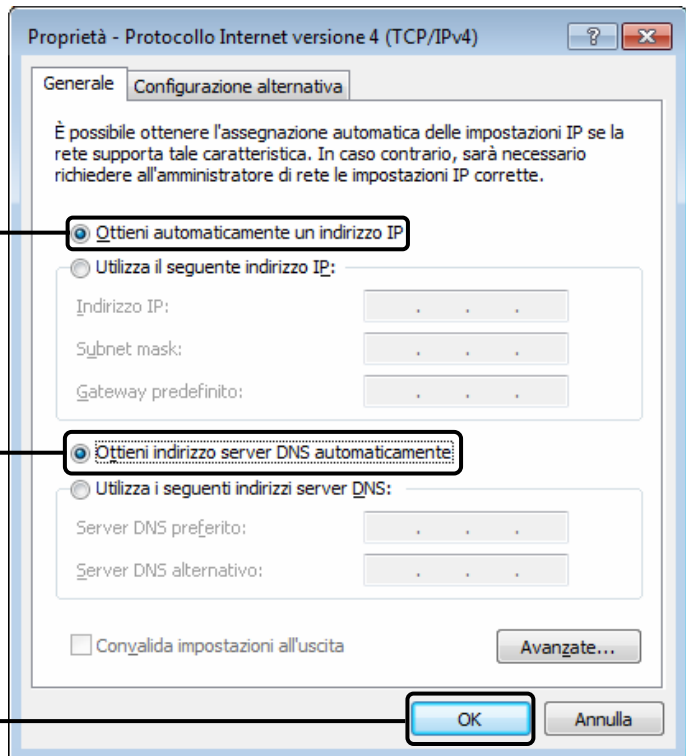
Doppio clic su **Internet Protocol Version 4 (TCP/IPv4) (Protocollo Internet versione 4 (TCP/IPv4))**



Selezionare **Internet Protocol Version 4 (TCP/IPv4)** (Ottieni automaticamente un indirizzo IP)

Selezionare **Obtain an IP address automatically** (Ottieni indirizzo server DNS automaticamente)

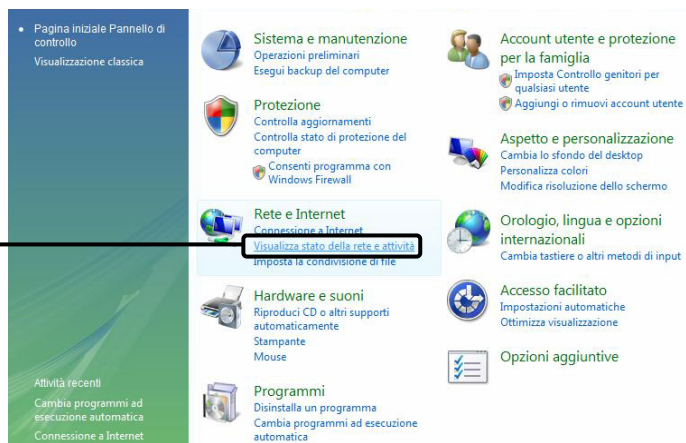
Clic su **OK**



**Per Windows® Vista™**

Clic su **Start > Impostazioni > Control Panel (Pannello di controllo)**, viene visualizzata questa pagina.

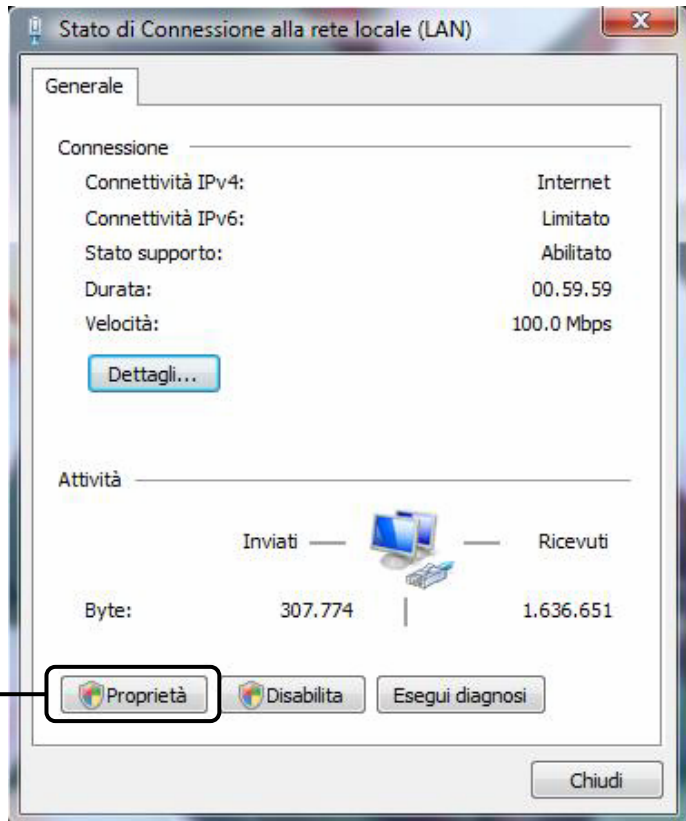
Clic su **View network status and tasks** (Visualizza stato della rete e attività)



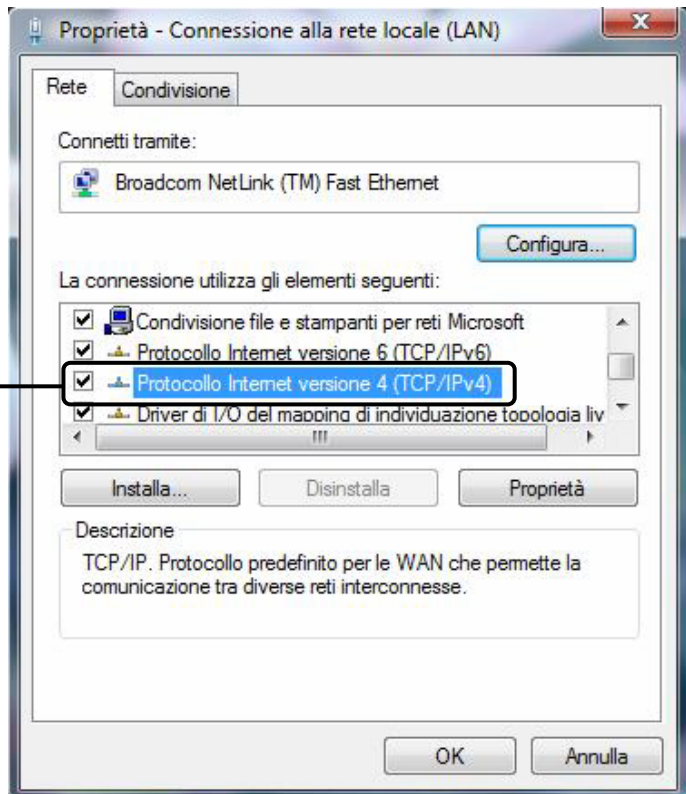
Clic su **Visualizza stato**



Clic su **Properties**  
(Proprietà)



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



Proprietà - Protocollo Internet versione 4 (TCP/IPv4)

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 **Obtain an IP address automatically** (Ottieni automaticamente un indirizzo IP)

Selezionare **Obtain DNS server address automatically** (Ottieni indirizzo server DNS automaticamente)

Click su **OK**

**Per Windows® XP**

Click su **Start > Control Panel (Pannello di controllo)**, viene visualizzata questa pagina.

Pannello di controllo

Passa alla visualizzazione classica

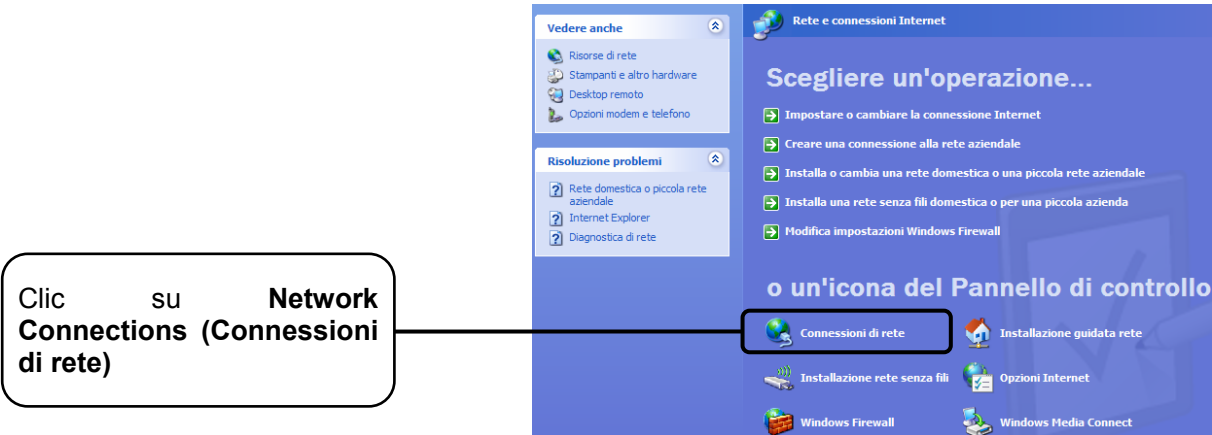
Vedere anche

- Windows Update
- Guida in linea e supporto tecnico
- Altre opzioni del Pannello di controllo

Scegliere una categoria

- Aspetto e temi
- Stampanti e altro hardware
- Rete e connessioni Internet**
- Account utente
- Installazione applicazioni
- Data, ora, lingua e opzioni internazionali
- Suoni, voce e periferiche audio
- Accesso facilitato
- Prestazioni e manutenzione
- Centro sicurezza PC

Clic su **Network and Internet Connections (Rete e connessioni Internet)**

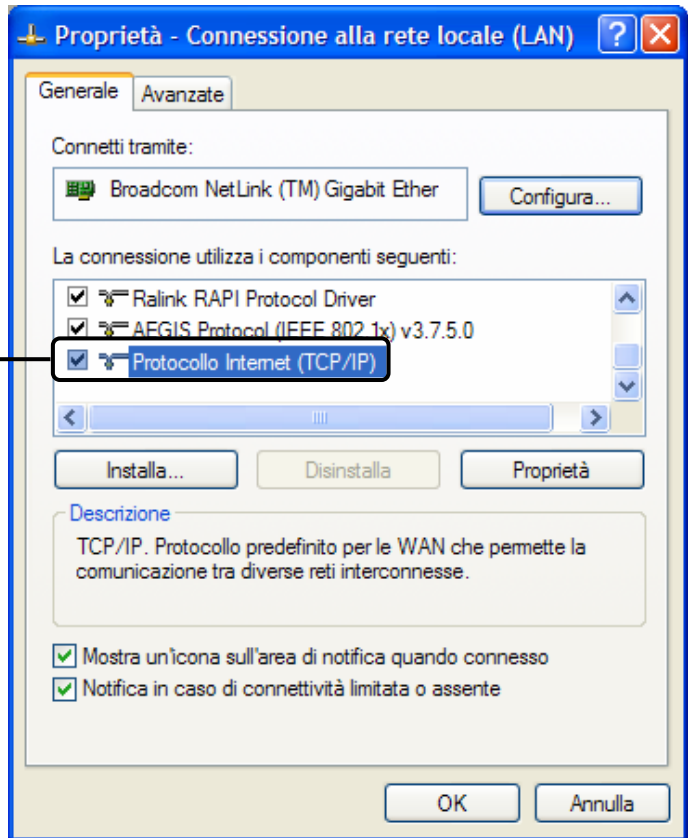


Clic destro su **Local Area Connection (Connessione alla rete locale)**



Clic su **Properties (Proprietà)**

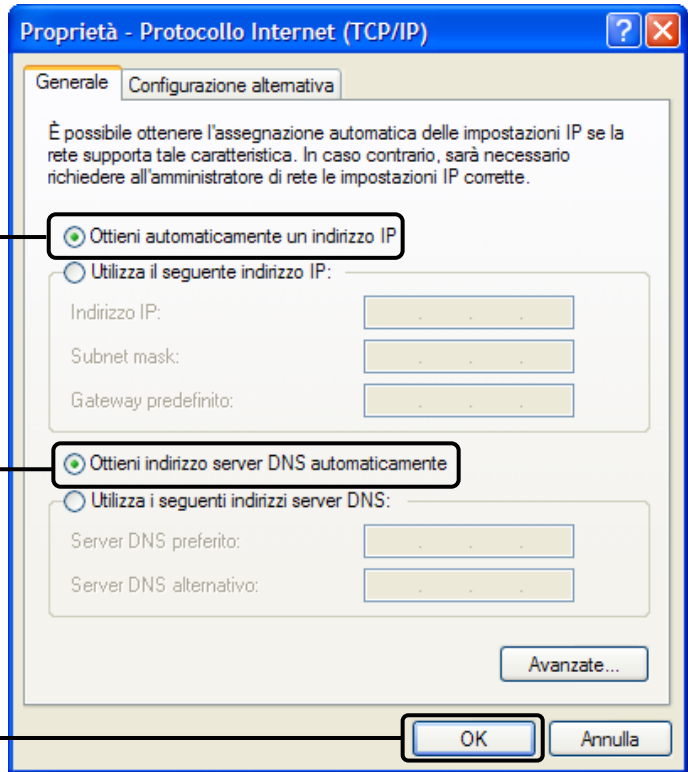
Doppio clic su **Internet Protocol (TCP/IP) Internet (TCP/IP)**



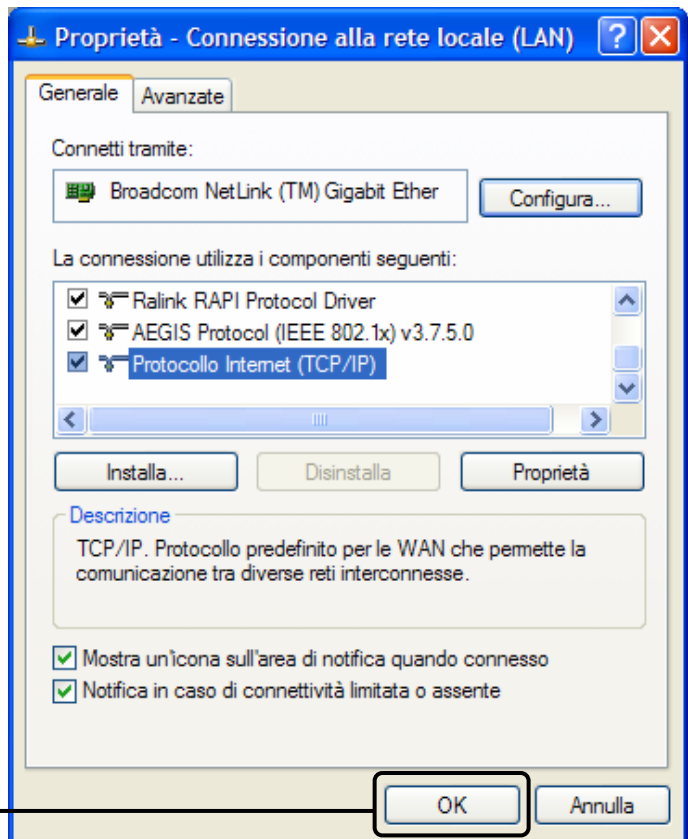
Selezionare **Obtain an IP address automatically (Ottieni automaticamente un indirizzo IP)**

Selezionare **Obtain DNS server address automatically (Ottieni indirizzo server DNS automaticamente)**

Clic su **OK**



Clic su **OK**



### Per Mac™ OS X

- Fare clic su **Apple** nell'angolo alto sinistro.
- Selezionare "**System Preferences (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 **Advanced (Avanzate)**.
- Nella scheda **TCP/IP**, sezione **Configure IPv4 (Configura IPv4)** selezionare **Using DHCP (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 Web console. 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.

### **T5. Come posso configurare le funzionalità USB?**

Fare riferimento alla guida alle applicazioni nella cartella "Application Guide" sul CD-ROM o su <http://www.tp-link.it>.



## 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](mailto: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