

A Smarter Way for Your Broadband Life

Huawei HG8245H, an intelligent routing-type ONT

Smart
service

Smart
interconnection



Smart O&M



○ Device Parameters

Dimensions (HxWxD)	(176 x 138.5 x 28)mm (without an external antenna)
Weight	about 500g
Operating temperature	0°C to +40°C
Operating humidity	5%RH to 95%RH (non-condensing)
Power adapter input	100–240V AC, 50–60Hz
System power supply	11–14V DC, 2 A
Static power consumption	5W
Maximum power consumption	15.5W
Ports	2POTS+4GE+Wi-Fi+USB
Indicators	POWER/PON/LOS/LAN/TEL/USB /WLAN/WPS

○ Interface Parameters

GPON Port	<ul style="list-style-type: none"> • Class B+ • Receiver sensitivity: -27dBm • Wavelengths: US 1310nm, DS 1490nm • WBF • Flexible mapping between GEM Port and TCONT • GPON: consistent with the SN or password authentication defined in G.984.3 • Bi-directional FEC • SR-DBA and NSR-DBA
Ethernet Port	<ul style="list-style-type: none"> • Ethernet port-based VLAN tags and tag removal • 1:1 VLAN, N:1 VLAN, or VLAN transparent transmission • QinQ VLAN • Limit on the number of learned MAC addresses • MAC address learning
POTS Port	<ul style="list-style-type: none"> • Maximum REN: 4 • G.711A/μ, G.729a/b, and G.722 encoding/decoding • T.30/T.38/G.711 fax mode • DTMF • Emergency calls (with the SIP protocol)
USB Port	<ul style="list-style-type: none"> • USB2.0 • FTP-based network storage
WLAN	<ul style="list-style-type: none"> • IEEE 802.11 b/g/n • 2 x 2 MIMO • Antenna gain: 2 dBi • WMM • Multiple SSIDs • WPS

○ Product Function

Smart interconnection

- Smart Wi-Fi coverage (V300R015C10)
- SIP/H.248 auto-negotiation
- Any port any service
- Parental control (V300R015C00)
- L2/L3(IPv4) forwarding: 1G uplink, 2G downlink

Smart service

- Smart Wi-Fi sharing: Portal/802.1x authentication (V300R015C10)
SoftGRE-based sharing (V300R015C10)
- Association of one account with two POTS ports

Smart O&M

- IPTV video quality diagnosis (V300R015C10)
- Variable-length OMCI messages
- Active/Passive rogue ONT detection and isolation
- Call emulation, and circuit test and loop-line test
- PPPoE/DHCP simulation testing
- WLAN emulation

Layer 3 Features

- PPPoE/Static IP/DHCP
- NAT/NAPT
- Port forwarding
- ALG, UPnP
- DDNS/DNS server/DNS client
- IPv6/IPv4 dual stack, and DS-Lite
- Static/Default routes
- Multiple services on one WAN port

Multicast

- IGMP v2/v3 proxy (V300R015C00) /snooping
- MLD v1/v2 snooping
- Multicast services through Wi-Fi

QoS

- Ethernet port rate limitation
- 802.1p priority
- SP/WRR/SP+WRR
- Broadcast packet rate limitation

Security

- SPI firewall
- Filtering based on MAC/IP/URL addresses

Common O&M

- OMCI/Web UI/TR069
- Dual-system software backup and rollback

Power Saving

- Dynamic power saving
- Indicator power saving
- Scheduled Wi-Fi shutdown (V300R015C00)



Sommario

1. Precauzioni di sicurezza	5
2. Accesso alla pagina web locale di configurazione	7
3. Configurazione del server DHCP	8
4. Configurazione dell'IP statico DHCP	11
5. Rete wireless (WLAN)	12
A. Configurazioni base	12
B. Configurazioni avanzate.....	14
6. Sicurezza.....	16
A. Firewall.....	16
B. Filtro indirizzi IP	16
C. Filtro MAC Address.....	18
D. Filtro MAC rete WLAN	20
E. Filtro indirizzi URL	21
F. DoS	22
G. Controllo accessi	23
H. Controllo accessi rete WLAN	25
I. DMZ.....	25
J. Port mapping / forwarding	27
K. Port trigger.....	29
L. Applicazioni USB.....	31
M. ALG.....	33
N. UPNP	33
O. ARP	34
P. Portale.....	35

Q. Dynamic DNS (DDNS)	35
7. Riavvio	37
8. File di configurazione	37
9. Cambio password di accesso	38

1. Precauzioni di sicurezza

Per garantire il normale funzionamento del dispositivo, leggere le precauzioni di sicurezza prima di utilizzarlo e rispettarle durante l'esecuzione delle operazioni.

Requisiti di base

- Fare in modo che il dispositivo resti asciutto durante la conservazione, il trasporto e l'esecuzione.
- Impedire che il dispositivo urti contro altri oggetti durante la conservazione, il trasporto e l'esecuzione.
- Installare il dispositivo in stretta conformità con i requisiti del fornitore.
- Non disinstallare il dispositivo senza autorizzazione. Contattare il centro di assistenza specificato in caso di guasto del dispositivo.
- Nessuna azienda o personale dovrebbe modificare la struttura, il design di sicurezza o il design delle prestazioni del dispositivo senza autorizzazione.
- Rispettare le leggi e i regolamenti locali e rispettare i diritti legali di terzi durante l'utilizzo del dispositivo.

Requisiti ambientali

- Installare il dispositivo in un luogo ben ventilato non direttamente esposto alla luce solare.
- Tenere il dispositivo pulito.
- Tenere il dispositivo lontano da fonti d'acqua o luoghi umidi.
- Non posizionare oggetti sul dispositivo. In tal modo lo si protegge da danni, quali surriscaldamento o distorsione, che possono essere causati dai suddetti oggetti.
- Lasciare uno spazio di almeno 10 cm intorno al dispositivo per la dissipazione del calore.
- Tenere il dispositivo lontano da fonti di calore o fonti di incendio, come stufe elettriche e candele.
- Tenere il dispositivo lontano da apparecchi elettrici con forti campi magnetici o forti campi elettrici, quali forni a microonde, frigoriferi e telefoni cellulari.

Istruzioni per l'uso

- Utilizzare gli accessori forniti con il dispositivo o quelli raccomandati dal fornitore, come ad esempio l'alimentatore e la batteria.
- La tensione di alimentazione del dispositivo deve soddisfare i requisiti relativi alla tensione di ingresso del dispositivo.
- Tenere le spine di alimentazione pulite e asciutte per evitare scosse elettriche o altri pericoli.
- Asciugare le mani prima di rimuovere o inserire i cavi.
- Arrestare il dispositivo e spegnere l'alimentazione prima di rimuovere o inserire i cavi.

- Spegnere l'alimentazione e rimuovere tutti i cavi, compreso il cavo di alimentazione, le fibre ottiche e i cavi di rete dal dispositivo durante i temporali con fulmini.
- Spegnere l'interruttore e staccare la spina se il dispositivo deve essere spento per un periodo di tempo lungo.
- Proteggere l'apparecchio da infiltrazioni di acqua o altri liquidi. Se si verifica un incidente di questo tipo, spegnere immediatamente l'alimentazione e rimuovere tutti i cavi, compreso il cavo di alimentazione, le fibre ottiche e i cavi di rete dal dispositivo. Contattare il centro di assistenza specificato in caso di un guasto del dispositivo.
- Non calpestare, tirare, trascinare o piegare eccessivamente i cavi perché possono danneggiarsi. Cavi danneggiati possono causare un guasto del dispositivo.
- Non utilizzare i cavi danneggiati o deteriorati.
- Non guardare direttamente nella porta ottica sul dispositivo senza protezione per gli occhi. Il laser emesso dalla porta ottica può danneggiare gli occhi.
- In caso di eventuali anomalie, come fumo, rumore anomalo o odori provenienti dal dispositivo, spegnere immediatamente il dispositivo, spegnere l'alimentazione e rimuovere tutti i cavi, compreso il cavo di alimentazione, le fibre ottiche e i cavi di rete dal dispositivo. Contattare il centro di assistenza specificato in caso di un guasto del dispositivo.
- Impedire la caduta di oggetti esterni, quali oggetti metallici, nel dispositivo attraverso la maglia di dissipazione del calore.
- Proteggere l'involucro esterno del dispositivo da graffi, perché la vernice che si stacca nelle aree graffiate può causare anomalie del dispositivo. Se la vernice cade nel dispositivo può causare cortocircuiti. Inoltre, la vernice staccata può causare una reazione allergica al corpo umano.
- Assicurarsi che il dispositivo sia tenuto fuori dalla portata dei bambini. Attenzione ai rischi in cui incorrono i bambini che giocano con il dispositivo o che potrebbero ingoiare piccole parti del dispositivo.

Istruzioni per la pulizia

- Prima di pulire l'apparecchio, arrestare l'esecuzione del dispositivo, spegnere l'alimentazione e rimuovere tutti i cavi, compreso il cavo di alimentazione, le fibre ottiche e i cavi di rete dal dispositivo. Quando si inseriscono e si rimuovono le fibre ottiche, tenere puliti i connettori in fibra ottica.
- Non utilizzare fluidi o spray detergenti per pulire l'involucro esterno del dispositivo. Utilizzare invece un panno morbido.

Istruzioni per la protezione dell'ambiente

- Smaltire il dispositivo ritirato e le batterie presso il luogo di riciclo specificato.
 - Rispettare le leggi e i regolamenti locali per gestire i materiali di imballaggio, le batterie esauste e i dispositivi ritirati.

2. Accesso alla pagina web locale di configurazione

Questo argomento illustra il piano dati e la procedura di accesso all'interfaccia di configurazione Web.

Contesto

Prima di impostare l'ambiente di configurazione, assicurarsi che le informazioni sui dati elencate nella [Tabella 1](#) siano disponibili.

Tabella 1 - Informazioni preliminari	
Elemento	Descrizione
Nome utente e password di accesso (se non modificate in precedenza dall'utente)	Impostazioni predefinite: <ul style="list-style-type: none">Nome utente: rootPassword: admin
<p>NOTA:</p> <ul style="list-style-type: none">L'account dell'utente comune può essere utilizzato per configurare servizi come il Wi-Fi e la condivisione domestica.Dopo l'accesso alla pagina Web, se non si effettuano operazioni per cinque minuti, si verrà bloccati e si ritornerà di nuovo alla interfaccia di accesso e si dovrà ripetere il login.Immettendo tre volte il nome utente e la password errati, il sistema verrà bloccato e sbloccato automaticamente dopo un minuto. È possibile modificare la password (vedi oltre) <p>ATTENZIONE: se si modifica la password iniziale, si consiglia di segnarla su un foglietto e custodirla.</p> <p>In caso venga dimenticata, infatti, si sarà costretti a ripristinare la configurazione di fabbrica del modem, perdendo conseguentemente tutte le personalizzazioni effettuate.</p>	
Indirizzo IP LAN e subnet mask del modem	Impostazioni predefinite: <ul style="list-style-type: none">Indirizzo IP: 192.168.100.1Subnet mask: 255.255.255.0
Indirizzo IP e subnet mask del PC	Se sul proprio dispositivo PC o smartphone è attivo il DHCP, l'indirizzo IP locale (della LAN) verrà assegnato dal modem. Se invece sul proprio dispositivo è configurato l'IP manuale, verificare che sia del tipo 192.168.100.x, con subnet mask 255.255.255.0 e Default Gateway 192.168.100.1

Procedura

1. Utilizzare un cavo di rete per collegare la porta LAN del modem a un PC.
2. Assicurarsi che il browser (IE, Firefox, Chrome, ...) del PC non utilizzi il server proxy. La sezione seguente considera IE 6.0 di esempio per descrivere come verificare se IE utilizza il server proxy.
 - a. Avviare l'IE e scegliere **ToolsInternet Options** dal menu principale della finestra di IE. Quindi, verrà visualizzata l'interfaccia **Internet Options**.
 - b. Nell'interfaccia **Internet Options**, fare clic sulla scheda **Connections**, quindi su **LAN settings**.
 - c. Nell'area **Proxy server**, assicurarsi che la casella di controllo **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)**, non sia selezionata (ossia, senza il segno "✓"). Se la casella di controllo è selezionata, deselegionarla, quindi fare clic su **OK**.
3. Impostare l'indirizzo IP e la subnet mask del PC. Per ulteriori dettagli, vedere la [Tabella 1](#).
4. Accedere all'interfaccia di configurazione Web.
 - a. Immettere **http://192.168.100.1** nella barra degli indirizzi di IE (192.168.100.1 è l'indirizzo IP predefinito del modem), quindi premere **Enter** per visualizzare l'interfaccia di accesso, come illustrato nella [Figura 1](#).

Figura 1 Modalità di accesso

The image shows a login form with a red gradient background. It contains two input fields: one labeled 'Account:' and another labeled 'Password:'. To the right of the 'Password:' field is a button labeled 'Login'.

- b. Nella finestra di accesso, immettere il nome utente e la password. Per ulteriori dettagli sulle impostazioni predefinite del nome utente e della password, vedere la [Tabella 1](#). Dopo aver superato l'autenticazione della password, viene visualizzata l'interfaccia di configurazione Web.

3. Configurazione del server DHCP

1. Nella struttura di navigazione a sinistra, scegliere **LAN > DHCP Server Configuration**. Nel riquadro a destra, è possibile configurare il pool di indirizzi IP LAN (DHCP) che il modem assegna a tutti i dispositivi che si connettono. Dopo la configurazione, il PC collegato alla porta LAN può ottenere automaticamente un indirizzo IP dal pool di indirizzi, come illustrato nella [Figura 1](#).

Figura 1 Configurazione del server DHCP

LAN > DHCP Server Configuration

On this page, you can configure DHCP server parameters for the LAN-side device to obtain IP addresses.

Primary Address Pool

Enable Primary DHCP Server:

Enable DHCP Relay:

Enable Option125:

LAN Host IP Address: 192.168.100.1

Subnet Mask: 255.255.255.0

Start IP Address: 192.168.100.2 * (It must be in the same subnet as the IP address of the LAN host.)

End IP Address: 192.168.100.254 *

Lease Time: 3 days

Primary DNS Server:

Secondary DNS Server:

Secondary Address Pool

Enable Secondary DHCP Server:

IP Address: 192.168.2.1 *

Subnet Mask: 255.255.255.0 *

Start IP Address: 192.168.2.2 *

End IP Address: 192.168.2.254 *

Lease Time: 3 days

Option 60: MSFT 5.0 *

Option 43:

NTP Server:

Primary DNS Server:

Secondary DNS Server:

Apply Cancel

2. Fare clic su **Apply**.

La [Tabella 1](#) descrive i parametri relativi al server DHCP.

Tabella 1 - Parametri relativi al server DHCP	
Parametro	Descrizione
Attivare il server DHCP primario	Indica se attivare il server DHCP primario. Se la casella di controllo è selezionata, sarà possibile impostare il server DHCP primario.
Attivare il relay DHCP L2	Indica se attivare il relay DHCP L2. Il relay DHCP è un processo in cui è implementato l'inoltro tra le sottoreti dei pacchetti di broadcast DHCP tra il client DHCP e il server DHCP. In questo modo, i client DHCP in sottoreti fisiche diverse possono ottenere gli indirizzi IP assegnati in modo dinamico dallo stesso server DHCP. <ul style="list-style-type: none"> Se la Mode della porta WAN è Route, l'indirizzo IP del modem è ottenuto da server DHCP di livello superiore in diverse sottoreti e gli indirizzi IP lato utente sono ottenuti dal

Tabella 1 - Parametri relativi al server DHCP

Parametro	Descrizione
	pool di indirizzi DHCP del modem. <ul style="list-style-type: none">• Se la Mode della porta WAN è Bridge, il modem fungerà da bridge. In questo modo, il modem non disporrà di un indirizzo IP. Gli indirizzi IP lato utente sono ottenuti da server DHCP di livello superiore in diverse sottoreti.
Indirizzo IP iniziale	Indica l'indirizzo IP iniziale nel pool di indirizzi IP sul server DHCP primario. Deve trovarsi nella stessa sottorete dell'indirizzo IP impostato in " Configurazione host LAN ". In caso contrario, il server DHCP non riuscirà a funzionare normalmente.
Indirizzo IP finale	Indica l'indirizzo IP finale nel pool di indirizzi IP sul server DHCP attivo. Deve trovarsi nella stessa sottorete dell'indirizzo IP impostato in " Configurazione host LAN ". In caso contrario, il server DHCP non riuscirà a funzionare.
Tempo di leasing	Indica il tempo di leasing del pool di indirizzi IP sul server DHCP attivo. Opzioni: minuto, ora, giorno e settimana.
NOTA: il Pool di indirizzi secondario non può essere applicato insieme alla configurazione dell'instradamento dei criteri.	
Attivare il server DHCP secondario	Indica se attivare il server DHCP secondario. Se la casella di controllo è selezionata, sarà possibile impostare il server DHCP secondario.
Indirizzo IP	Indica l'indirizzo IP del server DHCP secondario.
Subnet Mask	Indica la maschera di sottorete del server DHCP secondario.
Indirizzo IP iniziale	Indica l'indirizzo IP iniziale nel pool di indirizzi IP sul server DHCP secondario.
Indirizzo IP finale	Indica l'indirizzo IP finale nel pool di indirizzi IP sul server DHCP secondario.
Tempo di leasing	Indica il tempo di leasing del pool di indirizzi IP sul server DHCP secondario. Opzioni: minuto, ora, giorno e settimana.
Option60	Indica il campo di opzione 60 del server DHCP

Tabella 1 - Parametri relativi al server DHCP

Parametro	Descrizione
	secondario. Un client DHCP lato utente può ottenere un indirizzo IP dal pool di indirizzi IP sul server DHCP secondario solo quando il campo di opzione 60 portato dal client DHCP lato utente è lo stesso di questa impostazione.
Option43	Indica il campo di opzione 43 del server DHCP secondario, identificando un server TFTP.
Server NTP	Immette l'indirizzo IP del server NTP.
Server DNS primario	Immette l'indirizzo IP del server DNS primario.
Server DNS secondario	Immette l'indirizzo IP del server DNS secondario.

4. Configurazione dell'IP statico DHCP

1. Fare clic sulla scheda **LAN** e scegliere **DHCP Static IP Configuration** dalla struttura di navigazione a sinistra. Nel riquadro destro, fare clic su **New**. Nella finestra di dialogo visualizzata, impostare **MAC address** e **IP address**, come illustrato nella [Figura 1](#).

Figura 1 Configurazione IP statico DHCP

LAN > DHCP Static IP Configuration

On this page, you can configure the reserved IP address that is assigned through DHCP for the specified MAC address.

	MAC Address	IP Address
MAC Address:	00:00:00:00:00:03 *	
IP Address:		10.10.10.10 *

Apply Cancel

2. Fare clic su **Apply**.

5. Rete wireless (WLAN)

A. Configurazioni base

1. Nella struttura di navigazione a sinistra, scegliere **WLAN > WLAN Basic Configuration**. Nel riquadro a destra, selezionare la casella di controllo **Enable WLAN**. Nella finestra di dialogo visualizzata, impostare i parametri Wi-Fi di base, inclusi SSID, modalità di autenticazione e modalità di crittografia, come illustrato nella [Figura 1](#).

Figura 1 Configurazione WLAN di base

WLAN > WLAN Basic Configuration

On this page, you can set basic WLAN parameters(When the WLAN function is disabled, this page is blank).
⚠ Caution:
Wireless network services may be interrupted temporarily after you modify wireless network parameters.

Enable WLAN

New Delete

SSID Index	SSID Name	SSID Status	Number of Associated Devices	Broadcast SSID	Security Configuration
<input type="checkbox"/> 1	WirelessNet	Enabled	32	Enabled	Configured

SSID Configuration Details

SSID Name: ChinaNet-huawei * (1-32 characters)

Enable SSID:

Number of Associated Devices: 32 * (1-32)

Broadcast SSID:

Enable WMM:

Authentication Mode: WPA PreSharedKey

Encryption Mode: TKIP&AES

WPA PreSharedKey: Hide * (8-63 ASCII characters or 64 hexadecimal characters)

WPA Group Key Regeneration Interval: 3600 * (600-86400s)

Enable WPS:

WPS Mode: PBC

PBC: Start WPS

Apply Cancel

2. Fare clic su **Apply**.

La [Tabella 1](#) descrive le configurazioni di rete wireless di base.

Tabella 1 Configurazioni di base della rete wireless

Parametro	Descrizione
Attiva WLAN	Indica se attivare la rete wireless. I seguenti parametri possono essere impostati solo quando la rete wireless è attivata.

Tabella 1 Configurazioni di base della rete wireless

Parametro	Descrizione
Nome SSID	Indica il nome della rete wireless. È utilizzato per differenziare diverse reti wireless. Si compone di un massimo di 32 caratteri, senza carattere di tabulazione. Un SSID1 predefinito, denominato WirelessNet viene creato dopo la creazione di un modem. Il sistema può configurare fino a quattro SSID alla volta e non può assegnare indirizzi IP ai terminali Wi-Fi per SSID.
Attiva SSID	Specifica se attivare la connessione.
Numero dispositivo associato	Specifica il numero di STA. Va da 1 a 32.
SSID di trasmissione	Indica se attivare o nascondere la trasmissione. <ul style="list-style-type: none">• Se si seleziona la casella d'opzione, significa che la funzione di trasmissione SSID è attivata. Il modem trasmette periodicamente l'SSID, cioè il nome della rete wireless. In questo modo, qualsiasi STA può cercare la rete wireless.• Se la casella d'opzione non è selezionata, indica che la funzione di trasmissione SSID è disattivata. L'SSID è nascosto e la STA non può cercare la rete wireless. L'SSID può essere ottenuto solo attraverso una richiesta.
Attivazione WMM	Specifica se attivare il Wi-Fi multimediale.
Modalità di autenticazione	Indica la modalità di autenticazione in modo che la STA possa richiedere l'accesso alla rete wireless. La modalità può essere Open, Shared, WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA/WPA2 Pre-Shared Key, WPA Enterprise, WPA2 Enterprise o PA/WPA2 Enterprise. È impostata su Open per impostazione predefinita, vale a dire, la STA può accedere alla rete senza autenticazione.
Modalità di crittografia	Indica la modalità di crittografia in modo che la STA possa richiedere l'accesso alla rete wireless. La modalità di crittografia e i parametri di crittografia variano con la modalità di autenticazione. <ul style="list-style-type: none">• Se la modalità di autenticazione è impostata su Open, la modalità di crittografia può essere impostata su None o WEP.• Se la modalità di autenticazione è impostata su Shared, la crittografia è WEP.• Se la modalità di autenticazione è impostata su WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA/WPA2 Pre-Shared Key, WPA Enterprise, WPA2 Enterprise o WPA/WPA2 Enterprise, la modalità di crittografia può essere impostata su AES, TKIP o TKIP&AES.

NOTA:

- la modalità di protezione e la crittografia configurate su un dispositivo Wi-Fi devono essere uguali a quelle di un modem. Se la modalità di crittografia TKIP&AES o AES non è configurata sul terminale Wi-Fi, il terminale Wi-Fi potrebbe avere un driver obsoleto. In tal caso, aggiornare la versione del driver del proprio dispositivo

- Modificano la configurazione anche solo di uno degli SSID, tutte le reti wireless del modem si riavviano, causandone l'indisponibilità temporanea per alcuni minuti, per tutti gli SSID presenti.
- La funzione WPS può essere utilizzata su SSID1 per una sola banda. Inoltre, non attivare WPS per SSID multipli nella stessa banda. In caso contrario, potrebbe verificarsi un'anomalia di collegamento Wi-Fi.

B. Configurazioni avanzate

1. Fare clic sulla scheda **WLAN** e scegliere **WLAN Advance Configuration** dalla struttura di navigazione a sinistra. Nel riquadro di destra, impostare i parametri, come illustrato nella [Figura 1](#).

NOTA:

questa pagina è vuota se **Enable WLAN** non è selezionata in **WLAN Basic Configuration**.

Figura 1 Configurazione avanzata della WLAN

WLAN > WLAN Advanced Configuration

On this page, you can set advanced WLAN parameters(When the WLAN function is disabled, this page is blank).

⚠ Caution:
Wireless network services may be interrupted temporarily after you modify wireless network parameters.

Advanced Configuration

TX Power:	100%	
Regulatory Domain:	China	
Channel:	Automatic	
Channel Width:	20 MHz	
Mode:	802.11b/g/n	
DTIM Period:	1	(1-255, default: 1)
Beacon Period:	100	(20-1000 ms, default: 100)
RTS Threshold:	2346	(1-2346 bytes, default: 2346)
Fragmentation Threshold:	2346	(256-2346 bytes, default: 2346)

Apply Cancel

2. Fare clic su **Apply**.

La [Tabella 1](#) descrive i parametri avanzati della rete wireless.

Tabella 1 - Parametri avanzati della rete wireless

Parametro	Descrizione
Potenza di trasmissione	Indica la potenza ottica di trasmissione dei segnali wireless. Può essere impostata su 20% , 40% , 60% , 80% o 100% . Maggiore è il

Tabella 1 - Parametri avanzati della rete wireless

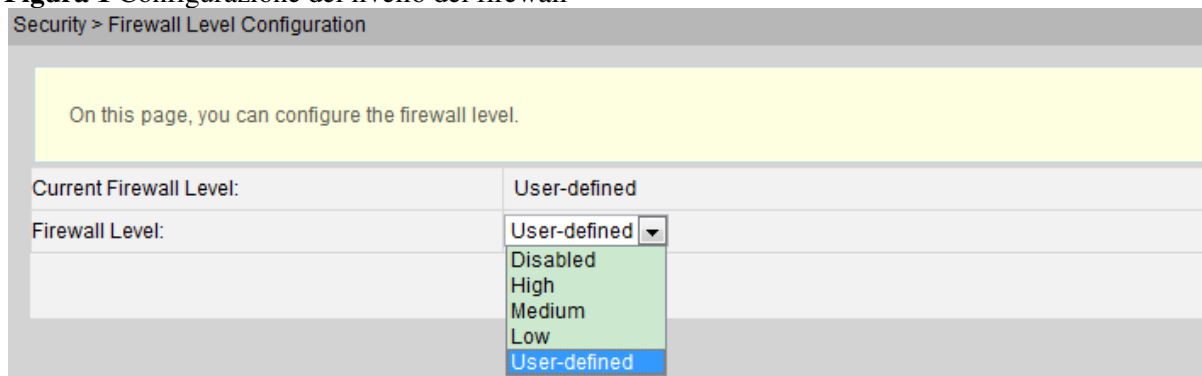
Parametro	Descrizione
	valore, migliore sarà la copertura dei segnali wireless.
Dominio regolatorio	Indica il codice del paese della rete wireless.
Canale	Indica il canale della rete wireless. Il canale varia con il valore del Regulatory Domain .
Ampiezza del canale	Indica l'ampiezza del canale wireless. Può essere impostata su auto 20/40 , 20 MHz o 40 MHz .
Modalità	Indica la modalità di rete wireless supportata. Può essere impostata su 802.11b , 802.11g , 802.11b/g o 802.11b/g/n .
Periodo DTIM	Indica il periodo di consegna della DTIM (Delivery Traffic Indication Map). Il valore varia da 1 a 125 e il valore predefinito è 1.
Periodo segnale luminoso	Indica il periodo di consegna del segnale luminoso. Il segnale luminoso è utilizzato per contattare i dispositivi punto di accesso o i dispositivi di controllo della rete. Il valore varia da 20 ms a 1000 ms e il valore predefinito è 100 ms.
Soglia RTS	Indica la richiesta alla soglia di invio (RTS). È usata per evitare conflitti nella trasmissione dei dati nella LAN wireless. Più piccola è la soglia RTS, maggiore sarà la frequenza di trasmissione dei pacchetti RTS e più velocemente il sistema eseguirà il ripristino da un'interruzione o un conflitto. Tuttavia, vengono utilizzate più larghezze di banda, aspetto che influenza il throughput degli altri pacchetti di dati della rete. Il valore varia da 1 byte a 2346 byte e il valore predefinito è 2346 byte.
Soglia di frammentazione	Indica la soglia di frammentazione. Quando le dimensioni di un pacchetto superano questa soglia, il pacchetto viene frammentato. Se la trasmissione di frammenti viene interrotta, solo le parti non trasmesse correttamente dovranno essere ritrasmesse. Il valore varia da 256 byte a 2346 byte e il valore predefinito è 2346 byte.

6. Sicurezza

A. Firewall

1. Fare clic sulla scheda **Security** e scegliere **Firewall Level Configuration** dalla struttura di navigazione a sinistra. Nel riquadro di destra, impostare il livello di firewall, come illustrato nella [Figura 1](#).

Figura 1 Configurazione del livello del firewall



Current Firewall Level:	User-defined
Firewall Level:	User-defined ▼
	Disabled
	High
	Medium
	Low
	User-defined

2. Fare clic su **Apply**.

Argomento principale: [Sicurezza](#)

B. Filtro indirizzi IP

1. Nella struttura di navigazione a sinistra, scegliere **Security > IP Filter Configuration**. Nel riquadro a destra, attivare la funzione di filtro degli indirizzi IP. Dopo aver selezionato la modalità di filtro, fare clic su **New**. Quindi, nella finestra di dialogo visualizzata, configurare la regola per il filtro degli indirizzi IP dall'interfaccia WAN alla porta LAN, come illustrato nella [Figura 1](#).

Figura 1 Configurazione del filtro IP

Security > IP Filter Configuration

On this page, you can configure WAN-to-LAN filter to prohibit some IP addresses in the WAN from accessing the LAN.

Enable IP Filter:

Filter Mode: Hybrid

New Delete

Priority	Protocol	Direction	LAN-Side IP Address	LAN-Side Port	WAN-Side IP Address	WAN-Side Port	Action
	TCP/UDP	Upstream	192.168.100.2	All		All	Accept

Apply Cancel

2. Fare clic su **Apply**.

La funzione di filtro degli indirizzi IP è un meccanismo di sicurezza configurato sul gateway residenziale. Attiva o disattiva tutte o parte delle porte in un segmento dell'indirizzo IP Intranet per comunicare con tutte o parte delle porte in un segmento dell'indirizzo IP Extranet. La configurazione del filtro degli indirizzi IP è utilizzato per limitare la comunicazione tra un dispositivo Intranet e un dispositivo Extranet.

La [Tabella 1](#) descrive i parametri relativi al filtro degli indirizzi IP.

Tabella 1 Parametri relativi al filtro degli indirizzi IP

Parametro	Descrizione
Attiva filtro IP	Indica se attivare la funzione di filtro degli indirizzi IP.
Modalità filtro	Indica la regola di filtro degli indirizzi IP o della lista nera o della lista bianca. <ul style="list-style-type: none">• Lista nera: indica che i dati che soddisfano la regola nell'elenco delle regole di filtro non sono consentiti.• Lista bianca: indica che i dati che soddisfano la regola nell'elenco delle regole di filtro sono consentiti.• Ibrida: indica che i pacchetti vengono filtrati in base alla direzione upstream o downstream. Alcuni pacchetti IP in direzione upstream o downstream (non) sono autorizzati. È possibile selezionare solo una delle modalità precedenti.

Tabella 1 Parametri relativi al filtro degli indirizzi IP

Parametro	Descrizione
Nome regola	Indica il nome di una regola. Questo parametro è obbligatorio ed è composto solo da caratteri e numeri. Il nome di una regola deve essere univoco.
Protocollo	Indica il tipo di protocollo, che può essere TCP/UDP, TCP, UDP, ICMP o ALL.
Direzione	Indica la direzione a cui si applica la regola del filtro. <ul style="list-style-type: none">• Bidirezionale: questo valore è disponibile solo quando Filter Mode è Blacklist o Whitelist. Il valore non può essere modificato.• Upstream: quando questo valore è selezionato nella modalità ibrida, la regola di filtro viene applicata alla direzione upstream. Nella modalità filtro ibrida, è possibile selezionare solo Upstream o Downstream.• Downstream: quando questo valore viene selezionato nella modalità ibrida, la regola di filtro viene applicata alla direzione downstream.
Priorità	Indica la priorità della regola di filtro IP. Questo parametro è configurabile solo quando Filter Mode è impostata su Hybrid . I valori vanno da 0 a 255. Un valore più basso indica una priorità maggiore. Il valore predefinito è 255.
Indirizzo IP lato LAN	Indica l'indirizzo IP sul lato LAN.
Porta lato LAN	Indica l'ID della porta sul lato LAN. Questo parametro può essere configurato quando Protocol è impostato su TCP/UDP, TCP o UDP .
Indirizzo IP lato WAN	Indica l'indirizzo IP sul lato WAN.
Porta lato WAN	Indica l'ID della porta lato WAN. Questo parametro può essere configurato quando Protocol è impostato su TCP/UDP, TCP o UDP .
Azione	Indica l'azione del filtro IP. <ul style="list-style-type: none">• Accetta: accetta i pacchetti che soddisfano la regola di filtro IP.• Rilascio: rilascia i pacchetti che soddisfano la regola di filtro IP.

C. Filtro MAC Address

1. Nella struttura di navigazione a sinistra, scegliere **Security > MAC Filter Configuration**. Nel riquadro a destra, dopo aver attivato il filtro MAC e selezionato la modalità di filtro, fare clic su **New**. Nella finestra di dialogo visualizzata, configurare la regola di filtro MAC in modo che il PC possa accedere a Internet, come illustrato nella [Figura 1](#).

Figura 1 Configurazione del filtro MAC

Security > MAC Filter Configuration

On this page, you can configure the MAC filtering to prohibit certain PCs from accessing the Internet.

Enable MAC filter:

Filter Mode: Blacklist

New Delete

Source MAC Address	
Source MAC Address:	00:15:17:2C:EF:97 * (AA:BB:CC:DD:EE:FF)

Apply Cancel

2. Fare clic su **Apply**.

Gli elenchi di indirizzi MAC di PC nella rete vengono salvati sul modem. La configurazione delle regole di filtro MAC consente ai PC conformi alle regole di accedere al servizio Internet o impedisce ai PC non conformi alle regole di accedere al servizio Internet. Un PC può avere più di un indirizzo IP, ma un indirizzo MAC univoco. Pertanto, la configurazione delle regole di filtro MAC controlla efficacemente i diritti di accesso al servizio Internet di PC in una LAN.

La [Tabella 1](#) descrive i parametri relativi al filtro MAC.

Tabella 1 Parametri relativi al filtro degli indirizzi MAC

Parametro	Descrizione
Attiva filtro MAC	Indica se attivare la funzione di filtro degli indirizzi MAC.
Modalità filtro	<p>Indica la regola di filtro degli indirizzi MAC o della lista nera o della lista bianca.</p> <ul style="list-style-type: none">• Lista nera: indica che i dati che soddisfano la regola nell'elenco delle regole di filtro non sono consentiti.• Lista bianca: indica che i dati che soddisfano la regola nell'elenco delle regole di filtro sono consentiti. <p>La modalità filtro è la modalità di configurazione globale. Pertanto, la modalità di lista nera e lista bianca non possono essere utilizzate contemporaneamente.</p>
Indirizzo MAC di origine	Indica l'indirizzo MAC di origine nella regola di filtro degli indirizzi MAC.

D. Filtro MAC rete WLAN

1. Fare clic sulla scheda **Security** e scegliere **WLAN MAC Filter Configuration** dalla struttura di navigazione a sinistra. Nel riquadro a destra, selezionare **Enable WAN MAC filter**, impostare la modalità di filtro, fare clic su **New**. Nella finestra di dialogo visualizzata, configurare la regola di filtro degli indirizzi MAC basata su SSID, come illustrato nella [Figura 1](#).

Figura 1 Configurazione del filtro MAC WLAN

Security > WLAN MAC Filter Configuration

On this page, you can configure MAC filter to prohibit some PCs from accessing the Internet.

Enable WLAN MAC Filter:

Filter Mode: Blacklist

New Delete

SSID Index	Source MAC Address
---	---
SSID Index: SSID1	Source MAC Address: 00:00:00:00:00:03 *(AA:BB:CC:DD:EE:FF)

Apply Cancel

2. Fare clic su **Apply**.

La [Tabella 1](#) descrive i parametri di configurazione per il filtro MAC della rete wireless.

Tabella 1 Parametri di filtro MAC della rete wireless	
Parametro	Descrizione
Attiva filtro MAC WLAN	Attiva o disattiva la funzione di filtro MAC WLAN.
Modalità filtro	Indica la modalità del filtro MAC. Può essere impostata su Blacklist o Whitelist . <ul style="list-style-type: none">• Lista nera: vieta il passaggio dei pacchetti che soddisfano le regole nella lista nera.• Lista bianca: consente il passaggio dei pacchetti che soddisfano le regole nella lista bianca. La modalità lista nera o lista bianca è la modalità di configurazione globale. Le due modalità non possono essere usate contemporaneamente.
Indice SSID	Indica l'indice SSID della WLAN per cui è stato configurato il filtro degli indirizzi MAC.
Indirizzo MAC di origine	Indica l'indirizzo MAC di origine nelle regole di filtro MAC.

E. Filtro indirizzi URL

1. Fare clic sulla scheda **Security** e scegliere **URL Filter Configuration** dalla struttura di navigazione a sinistra. Nel riquadro a destra, dopo aver attivato il filtro URL e selezionato la modalità di filtro, fare clic su **New**. Nella finestra di dialogo visualizzata, configurare la regola di filtro URL in modo che il PC possa accedere a Internet, come illustrato nella [Figura 1](#).

Figura 1 Configurazione del filtro URL

Security > URL Filter Configuration

On this page, you can configure URL filter parameters. If the check box next to Enable Smart URL Filter is selected and multiple domains correspond to the same IP address, access to the IP address is restricted. For example, three domain names huawei1, huawei2, and huawei3 correspond to the same IP address 10.1.1.1, and huawei1 is blacklisted. If the smart URL filter function is enabled, access to huawei1 and 10.1.1.1 is restricted. If the smart URL filter function is disabled, only access to huawei1 is restricted.

Enable URL Filter:

Enable Smart URL Filter:

Filter Mode: Blacklist

New Delete

URL Address

URL Address: www.xxx.com *

Apply Cancel

NOTA:

ad esempio, se è necessario filtrare l'indirizzo a.huawei.com e b.huawei.com, impostare l'indirizzo URL su huawei.com. Un indirizzo URL non supporta un carattere jolly e pertanto non è possibile impostarlo su *.huawei.com.

2. Fare clic su **Apply**.

Tabella 1 Parametri relativi al filtro degli indirizzi URL

Parametro	Descrizione
Attiva filtro URL	Indica se attivare la funzione di filtro URL.
Attiva filtro URL intelligente	Indica se attivare la funzione di filtro URL intelligente. Ad esempio, domain1 e domain2 corrispondono allo stesso indirizzo IP 10.10.10.10 e domain1 è inserito nella lista nera. <ul style="list-style-type: none">• Quando la funzione di filtro URL intelligente è attivata, l'accesso a domain1 e 10.10.10.10 è limitato.

Tabella 1 Parametri relativi al filtro degli indirizzi URL

Parametro	Descrizione
	<ul style="list-style-type: none">Quando la funzione di filtro URL intelligente è disattivata, solo l'accesso a domain1 è limitato.
Modalità filtro	<p>Indica la regola di filtro URL o della lista nera o della lista bianca.</p> <ul style="list-style-type: none">Lista nera: indica che i dati che soddisfano la regola nell'elenco delle regole di filtro non sono consentiti.Lista bianca: indica che i dati che soddisfano la regola nell'elenco delle regole di filtro sono consentiti. <p>La modalità filtro è la modalità di configurazione globale. Pertanto, la modalità di lista nera e lista bianca non possono essere utilizzate contemporaneamente.</p>
Indirizzo URL	Indica il nome di dominio o l'indirizzo IP nella regola di filtro URL.

F. DoS

- Nella struttura di navigazione a sinistra, scegliere **Security > DoS Configuration**. Nel riquadro di destra, determinare se attivare la configurazione preventiva degli attacchi DoS, come illustrato nella [Figura 1](#).

Figura 1 Configurazione DoS

The screenshot shows the 'Security > DoS Configuration' page. At the top, there is a yellow banner with the text: 'On this page, you can configure DoS parameters.' Below this, there is a table with seven rows, each representing a different DoS attack type and its prevention status. At the bottom of the page, there are two buttons: 'Apply' and 'Cancel'.

Attack Type	Prevention Status
Prevent SYN Flood Attack:	<input checked="" type="checkbox"/>
Prevent ICMP Echo Attack:	<input checked="" type="checkbox"/>
Prevent ICMP Redirection Attack:	<input checked="" type="checkbox"/>
Prevent LAND Attack:	<input type="checkbox"/>
Prevent Smurf Attack:	<input type="checkbox"/>
Prevent WinNuke Attack:	<input type="checkbox"/>
Prevent Ping Sweep Attack:	<input checked="" type="checkbox"/>

Apply Cancel

2. Fare clic su **Apply**.

DoS (Denial of service) è un attacco basato sulla rete che nega agli utenti di accedere a Internet. L'attacco DoS avvia un ampio numero di connessioni di rete, comportando il crash del server o del programma in esecuzione sul server o esaurendo le risorse del server o negando agli utenti l'accesso al servizio Internet. Di conseguenza, il servizio di rete smette di funzionare.

La [Tabella 1](#) descrive i parametri relativi al filtro DoS.

Tabella 1 Parametri relativi al server DoS	
Parametro	Descrizione
Prevenzione di un attacco SYN Flooding	Indica se attivare la prevenzione di un attacco SYN flooding. Nell'attacco, diversi host di origine inviano pacchetti SYN ad un host di destinazione. Dopo aver ricevuto i pacchetti SYN ACK dall'host di destinazione, gli host di origine non rispondono. In questo caso, la connessione host di destinazione stabilisce molte code per gli host di origine e gestisce queste code costantemente perché non viene ricevuta nessuna risposta ACK. Di conseguenza, vengono utilizzate molte risorse e l'host di destinazione non riesce a fornire servizi normali per le connessioni normali.
Prevenzione di un attacco ICMP Echo	Indica se attivare la prevenzione di un attacco ICMP echo. Nell'attacco, diversi pacchetti CMP echo vengono inviati ad un host di destinazione in breve tempo. Di conseguenza, la rete è congestionata o le risorse dell'host vengono esaurite.
Prevenzione di un attacco ICMP Redirect	Indica se attivare la prevenzione di un attacco ICMP redirect. Nell'attacco, diversi pacchetti ICMP redirect vengono inviati ad un host di destinazione in breve tempo. Di conseguenza, la rete è congestionata o le risorse dell'host vengono esaurite.

G. Controllo accessi

1. Nella struttura di navigazione a sinistra, scegliere **Security > ONT Access Control Configuration**. Nel riquadro di destra, configurare la regola del controllo degli accessi al modem, come illustrato nella [Figura 1](#).



PERICOLO:

completare la pianificazione della sicurezza della rete prima di attivare il controllo degli accessi in remoto per garantire che l'accesso al modem avvengano in condizioni di rete sicura. Al termine delle operazioni di accesso al modem, disattivare il controllo degli accessi in remoto in modo tempestivo. Se non si completa la pianificazione della sicurezza della rete o non si disattiva il controllo degli accessi in remoto in modo tempestivo, la rete può diventare difettosa o essere attaccata e Huawei non sarà responsabile di eventuali conseguenze correlate.

Figura 1 Configurazione del controllo degli accessi al modem

Security > ONT Access Control Configuration

On this page, you can grant or deny ONT access.

LAN Service	
Enable the LAN-Side PC to Access the ONT Through FTP:	<input type="checkbox"/>
Enable the LAN-Side PC to Access the ONT Through HTTP:	<input checked="" type="checkbox"/>
Enable the LAN-Side PC to Access the ONT Through Telnet:	<input checked="" type="checkbox"/>
Enable the LAN-Side PC to Access the ONT Through SSH:	<input type="checkbox"/>

WLAN Service	
Enable devices on the WLAN side to access web pages:	<input checked="" type="checkbox"/>
Enable PCs on the WIFI side to access ONTs through Telnet:	<input checked="" type="checkbox"/>

WAN Service	
Enable the WAN-Side PC to Access the ONT Through FTP:	<input type="checkbox"/>
Enable the WAN-Side PC to Access the ONT Through HTTP:	<input type="checkbox"/>
Enable the WAN-Side PC to Access the ONT Through Telnet:	<input type="checkbox"/>
Enable the WAN-Side PC to Access the ONT Through SSH:	<input type="checkbox"/>

WAN-Side Source Address Whitelist	
Enable the WAN-Side Source Address Whitelist:	<input type="checkbox"/>

Source IP Address Whitelist	
----	----
Source IP Address:	<input type="text"/> *(A.B.C.D/E)

2. Fare clic su **Apply**.

H. Controllo accessi rete WLAN

1. Nella struttura di navigazione a sinistra, scegliere **Security > WAN Access Control Configuration**. Nel riquadro destro, fare clic su **New**. Nella finestra di dialogo visualizzata, impostare il controllo degli accessi WAN, come illustrato nella [Figura 1](#).



PERICOLO:

completare la pianificazione della sicurezza della rete prima di attivare il controllo degli accessi in remoto per garantire che l'accesso al modem avvengano in condizioni di rete sicura. Al termine delle operazioni di accesso al modem, disattivare il controllo degli accessi in remoto in modo tempestivo. Se non si completa la pianificazione della sicurezza della rete o non si disattiva il controllo degli accessi in remoto in modo tempestivo, la rete può diventare difettosa o essere attaccata e Huawei non sarà responsabile di eventuali conseguenze correlate.

Figura 1 Configurazione del controllo degli accessi WAN

Security > WAN Access Control Configuration

On this page, you can configure network access control based on a single WAN port. Access to a WAN port is allowed from the configured source addresses. If no source address is configured, access to the WAN port from any addresses is allowed. An IPv6 WAN port supports access only in HTTP mode and does not support access in telnet, FTP, or SSH mode.

	WAN Name	Protocol	Source Address	Enable
Enable:	<input checked="" type="checkbox"/>			
WAN Name:	2_INTERNET_R_VID_1001			
Protocol:	<input type="checkbox"/> TELNET <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> FTP <input type="checkbox"/> SSH			
Source Address:	10.172.168.0/24 (IPv4 or IPv6 address/mask) <input type="button" value="Delete"/>			
	10.172.168.20/32 (IPv4 or IPv6 address/mask) <input type="button" value="Delete"/>			
	<input type="button" value="Add"/>			
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

2. Fare clic su **Apply**.

I. DMZ

1. Nella struttura di navigazione a sinistra, scegliere **Forward Rules > DMZ Configuration**. Nel riquadro destro, fare clic su **New**. Nella finestra di dialogo visualizzata, impostare i parametri correlati alla DMZ, come illustrato nella [Figura 1](#).

Figura 1 Configurazione della DMZ

Forward Rules > DMZ Configuration

On this page, you can configure DMZ parameters. The DMZ device restricts unreliable external connections from linking up to the device. It is a buffer between a secure system and an insecure system. If the WAN port is not listed in the port mapping table, the application requests from the WAN connection are forwarded to the DMZ device.

New Delete

WAN Name	Enable DMZ	Host Address
Enable DMZ:	<input checked="" type="checkbox"/>	
WAN Name:	1_INTERNET_R_VID_1001	
Host Address:	192.168.100.100	* Select...

Apply Cancel

2. Fare clic su **Apply**.

La zona demilitarizzata, DMZ, è una tecnologia che consente al modem di inoltrare tutti i pacchetti ricevuti attraverso un server interno specificato. La tecnologia consente a un computer nella LAN di essere esposto completamente a tutti gli utenti su Internet o attiva la comunicazione reciproca, senza limitazioni, tra un host con un indirizzo IP specificato e altri utenti o altri server su Internet. In questo modo, molte applicazioni possono eseguire sull'host con l'indirizzo IP specificato. L'host con l'indirizzo IP specificato riceve tutti i collegamenti e i file che possono essere identificati.

AVVISO:

se il dispositivo lato LAN non fornisce il servizio del sito Web o altri servizi di rete, non impostare il dispositivo su un host DMZ poiché tutte le porte di un host DMZ sono aperte a Internet.

La [Tabella 1](#) descrive i parametri relativi al filtro DMZ.

Parametro	Descrizione
Abilita DMZ	Indica se attivare la DMZ.
Nome WAN	Indica il nome dell'interfaccia WAN. Se l'interfaccia WAN non è nella tabella di mapping delle porte, le richieste dell'app dalla connessione WAN vengono inoltrate direttamente all'host nella DMZ.
Indirizzo host	Indica l'indirizzo IP dell'host DMZ.

J. Port mapping / forwarding

Il mapping delle porte indica che il server Intranet può essere aperto alla extranet (ad esempio, la intranet fornisce alla extranet un server WWW o un server FTP). Il mapping delle porte serve ad eseguire il mapping dell'indirizzo IP e dell'ID della porta dell'host intranet all'indirizzo IP e all'ID della porta corrispondente della extranet in modo che gli utenti dalle extranet possano accedere al server intranet. Con il mapping delle porte, gli utenti non possono vedere l'indirizzo IP intranet ma vedono quello della extranet.

Percorso di navigazione

1. Nella struttura di navigazione a sinistra, scegliere **Forward Rules > Port Mapping Configuration**. Nel riquadro destro, fare clic su **New**. Nella finestra di dialogo visualizzata, impostare i parametri correlati al mapping delle porte, come illustrato nella [Figura 1](#).

Figura 1 Configurazione del mapping delle porte

Forward Rules > Port Mapping Configuration

On this page, you can configure port mapping parameters to set up virtual servers on the LAN network and allow these servers to be accessed from the Ethernet.
Note: The well-known ports for voice services cannot be in the range of the mapping ports.

New Delete

WAN Name	Mapping Name	Protocol	External Port	Internal Port	Internal Host	Enable
Type:	<input type="radio"/> User-defined	<input checked="" type="radio"/> Application	Domain Name Server (D)			
Enable Port Mapping:	<input checked="" type="checkbox"/>					
WAN Name:	1_INTERNET_R_VI	Protocol:	UDP			
Start External Port:	53 *	End External Port:	53 *			
Start Internal Port:	53 *	End Internal Port:	53			
Start External Source Port:		End External Source Port:				
Mapping Name:		External Source IP Address:				
Internal Host:	192.168.100.100 *	Select...				

Apply Cancel

2. Fare clic su **Apply**.

Esempio di configurazione

Abilitare i pacchetti inviati dal lato WAN al modem il cui numero della porta WAN di destinazione è 2000 in modo che possano essere inoltrati al PC lato LAN il cui indirizzo IP è 192.168.100.20 e il numero di porta viene modificato in 3000.

Forward Rules > Port Mapping Configuration

On this page, you can configure port mapping parameters to set up virtual servers on the LAN network and allow these servers to be accessed from the Ethernet.
 Note: The well-known ports for voice services cannot be in the range of the mapping ports.

New Delete

WAN Name	Mapping Name	Protocol	External Port	Internal Port	Internal Host	Enable
Type: <input checked="" type="radio"/> User-defined <input type="radio"/> Application Select... ▼						
Enable Port Mapping: <input checked="" type="checkbox"/>						
WAN Name:		1_INTERNET_R_VI ▼	Protocol:		TCP ▼	
Start External Port:		3000 *	End External Port:		3000 *	
Start Internal Port:		2000 *	End Internal Port:		2000	
Start External Source Port:			End External Source Port:			
Mapping Name:			External Source IP Address:			
Internal Host:		192.168.100.20 *	Select... ▼			

Apply Cancel

Descrizione del parametro

La [Tabella 1](#) descrive i parametri relativi al mapping delle porte.

Tabella 1 Parametri relativi al mapping delle porte	
Parametro	Descrizione
Attiva mapping delle porte	Indica se attivare il mapping delle porte.
Nome mapping	Indica il nome della regola di mapping delle porte.
Nome WAN	Indica il nome dell'interfaccia WAN dove il mapping delle porte è attivato.
Host interno	Indica l'indirizzo IP dell'host la cui porta è stata sottoposta a mapping.
Protocollo	Indica il tipo di protocollo del pacchetto di mapping delle porte che può essere TCP, UDP, o TCP/UDP.
Porta esterna iniziale	Indica la porta iniziale della destinazione del pacchetto dati esterno.
Porta esterna finale:	Indica la porta finale della destinazione del pacchetto dati esterno.
Porta interna iniziale	Indica la porta iniziale della destinazione interna del pacchetto di mapping delle porte.
Porta esterna finale	Indica la porta finale della destinazione interna del pacchetto di

Tabella 1 Parametri relativi al mapping delle porte

Parametro	Descrizione
	mapping delle porte.
Porta di origine esterna iniziale	Indica la porta iniziale di origine del pacchetto dati esterno.
Porta di origine esterna finale	Indica la porta finale di origine del pacchetto dati esterno.
Indirizzo IP di origine esterno	Indica l'indirizzo IP di origine del pacchetto dati esterno.

K. Port trigger

1. Nella struttura di navigazione a sinistra, scegliere **Forward Rules > Port Trigger Configuration**. Nel riquadro destro, fare clic su **New**. Nella finestra di dialogo visualizzata, impostare i parametri correlati all'attivazione delle porte, come illustrato nella [Figura 1](#).

Figura 1 Configurazione dell'attivazione delle porte

Forward Rules > Port Trigger Configuration

On this page, you can configure the range of the ports that are used by LAN-side applications to access the Internet. You can also enable the port automatically.
Note: The well-known ports for voice services cannot be in the range of open ports.

New Delete

	WAN Name	Enable Port Trigger	Trigger Port	Open Port	Trigger Protocol	Open Protocol
----	----	----	----	----	----	----
Enable Port Trigger:		<input checked="" type="checkbox"/>				
WAN Name:	1_INTERNET_R_VID_1001					
Trigger Protocol:	UDP					
Open Protocol:	UDP					
Start Trigger Port:	200					*
End Trigger Port:	201					*
Start Open Port:	145					*
End Open Port:	146					*

Apply Cancel

2. Fare clic su **Apply**.

L'attivazione delle porte indica che una porta extranet specifica viene automaticamente attivata quando una porta intranet corrispondente invia un

pacchetto e il pacchetto viene mappato alla porta intranet sull'host. Un pacchetto di mapping specifico viene inviato dal modem attraverso l'intranet in modo che i pacchetti specifici dell'extranet possano essere mappati all'host corrispondente. Una porta specificata sul firewall gateway è aperta ad alcune applicazioni per l'accesso remoto. L'attivazione delle porte può attivare dinamicamente la porta aperta del firewall.

La [Tabella 1](#) descrive i parametri relativi all'attivazione delle porte.

Tabella 1 Parametri relativi all'attivazione delle porte	
Parametro	Descrizione
Abilita attivazione delle porte	Indica se abilitare l'attivazione delle porte.
Nome WAN	Indica il nome dell'interfaccia WAN dove l'attivazione delle porte è abilitata.
Protocollo di attivazione	Indica il tipo di protocollo del pacchetto di attivazione delle porte che può essere TCP, UDP o TCP/UDP.
Protocollo aperto	Indica il tipo di protocollo del pacchetto dati aperto.
Porta di attivazione iniziale	Indica la porta iniziale della destinazione del pacchetto di attivazione delle porte.
Porta di attivazione finale	Indica la porta finale della destinazione del pacchetto di attivazione delle porte.
Porta aperta iniziale	Indica la porta iniziale della destinazione del pacchetto aperto.
Porta aperta finale	Indica la porta finale della destinazione del pacchetto aperto.

L. Applicazioni USB

1. Nella struttura di navigazione a sinistra, scegliere **Network Applications > USB Application**. Nel riquadro di destra, impostare i parametri correlati al download da FTP per condividere il file FTP sul modem, come illustrato nella [Figura 1](#).

Figura 1 Applicazione USB

Network Application > USB Application

FTP Client Configuration

On this page, you can configure the FTP client to download files from a network to a USB device.

⚠ Caution:
Do not insert or remove the USB storage device when the USB connection indicator is flashing. Otherwise, files on the USB storage device may be damaged.

FTP URL:	<input type="text" value="ftp://"/>
Port ID:	<input type="text" value="21"/>
User Name:	<input type="text"/>
Password:	<input type="password"/>
USB Device:	<input type="text" value="No USB Device"/>
Path:	<input type="text"/>

User Name	Password	Port ID	FTP URL	Path	Status
--	--	--	--	--	--

FTP Server Configuration

On this page, you can configure the FTP server to share data on the USB device with devices on the LAN.

⚠ Caution:
Do not insert or remove the USB storage device when the USB connection indicator is flashing. Otherwise, files on the USB storage device may be damaged.

Enable FTP Server:	<input type="checkbox"/>
User Name:	<input type="text" value="root"/>
Password:	<input type="password"/>
USB Device:	<input type="text" value="No USB Device"/>
Root Path:	<input type="text"/>

2. Fare clic su **Download** per scaricare i file dal server FTP al dispositivo di archiviazione USB.

La [Tabella 1](#) descrive i parametri relativi all'USB.

Tabella 1 Parametri relativi all'USB	
Parametro	Descrizione
Configurazione del client FTP	
URL FTP	Indica il percorso del file scaricato attraverso l'FTP.

Tabella 1 Parametri relativi all'USB

Parametro	Descrizione
ID porta	Indica il numero di porta FTP. È impostato su 21 per impostazione predefinita. In generale, l'impostazione non è richiesta.
Nome utente	Indica il nome utente per la connessione al server FTP. Se il server FTP supporta l'accesso anonimo, non è richiesta l'impostazione.
Password	Indica la password per la connessione al server FTP. Se il server FTP supporta l'accesso anonimo, non è richiesta l'impostazione.
Dispositivo USB	Indica l'unità del dispositivo USB esterno per il salvataggio del file scaricato tramite FTP. Quando il dispositivo di memoria USB è collegato alla porta USB, è disponibile l'elenco a discesa.
Percorso	Indica il percorso per il salvataggio del file FTP scaricato sul dispositivo USB esterno. Se il percorso non viene inserito, viene utilizzato il percorso specificato nell'URL di download per impostazione predefinita.
Configurazione del server FTP	
Attiva server FTP	Attiva il server FTP quando il modem funge da server FTP.
Nome utente	Indica il nome utente del server FTP. Questo nome utente è necessario quando il client FTP accede al server FTP.
Password	Indica la password del server FTP. Questa password è necessaria quando il client FTP accede al server FTP.
Dispositivo USB	Indica l'unità del dispositivo USB esterno per il salvataggio del file scaricato tramite FTP.
Percorso root	Indica il percorso per il salvataggio dei file condivisi quando il modem funge da server.

NOTA:

l'FTP non è stato progettato per fungere da protocollo di sicurezza. I dati sensibili trasmessi dagli utenti tramite FTP sono soggetti a furto e attacchi. Quando si scaricano file tramite FTP, approntare un piano di sicurezza in anticipo.

M. ALG

1. Nella struttura di navigazione a sinistra, scegliere **Network Applications > ALG Configuration**. Nel riquadro di destra, determinare se attivare l'FTP o il TFTP, come illustrato nella [Figura 1](#).

Figura 1 Configurazione ALG

Network Application > ALG Configuration	
On this page, you can enable the ALGs of various services.	
Enable FTP ALG:	<input checked="" type="checkbox"/>
Enable TFTP ALG:	<input checked="" type="checkbox"/>
Enable H.323 ALG:	<input checked="" type="checkbox"/>
Enable SIP ALG:	<input checked="" type="checkbox"/>
Enable RTSP ALG:	<input checked="" type="checkbox"/>
Enable RTCP ALG:	<input type="checkbox"/> Port: <input type="text" value="0"/>
Enable PPTP ALG:	<input checked="" type="checkbox"/>
Enable L2TP ALG:	<input checked="" type="checkbox"/>
Enable IPsec ALG:	<input checked="" type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Fare clic su **Apply**.

Quando la funzione NAT è attivata, la funzione di gateway a livello dell'applicazione (ALG) deve essere attivata per garantire che alcuni software applicativi e l'hardware possano essere utilizzati normalmente.

N. UPnP

1. Nella struttura di navigazione a sinistra, scegliere **Network Applications > UPnP Configuration**. Nel riquadro di destra, determinare se attivare l'UPnP, come illustrato nella [Figura 1](#).

Figura 1 Configurazione UPnP

Network Application > UPnP Configuration	
On this page, you can enable or disable the universal plug-and-play (UPnP) function, which supports automatic discovery of multiple types of network devices. If this function is enabled for a device, the device can access networks, obtain an IP address, transmit data, discover other devices, and acquire the data of other devices.	
Enable UPnP:	<input checked="" type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Fare clic su **Apply**.

UPnP (Universal Plug and Play) è il nome di un gruppo di protocolli. L'UPnP supporta il networking a configurazione zero e il rilevamento automatico di diversi dispositivi di rete. Se l'UPnP è attivato, il dispositivo UPnP può essere collegato dinamicamente alla rete per ottenere l'indirizzo IP, ottenere le prestazioni di trasferimento, rilevare altri dispositivi e apprendere le prestazioni degli altri dispositivi. Il dispositivo UPnP può essere automaticamente disconnesso dalla rete, senza influenzare il dispositivo o altri dispositivi.

Quando l'UPnP è attivato, il PC lato LAN trova automaticamente il modem, che è considerato come una periferica del PC ed è plug-and-play. Dopo l'esecuzione di software applicativo sul PC, vengono generate automaticamente voci di mapping delle porte sul modem attraverso il protocollo UPnP, migliorando così la velocità di esecuzione.

O. ARP

1. Nella struttura di navigazione a sinistra, scegliere **Network Applications > ARP Configuration**. Nel riquadro destro, fare clic su **New**. Nella finestra di dialogo visualizzata, impostare la regola di risoluzione tra un indirizzo MAC e un indirizzo IP, come illustrato nella [Figura 1](#).

Figura 1 Configurazione ARP

	IP Address	MAC Address
IP Address:	192.168.100.100 *	
MAC Address:		00:15:17:2C:EF:97 *

2. Fare clic su **Apply**.

ARP statico significa aggiungere manualmente una voce ARP su un modem. Un ARP statico non diventa mai obsoleto e può essere eliminato solo manualmente. Se il mapping tra l'indirizzo IP e l'indirizzo MAC del dispositivo peer è disponibile, la configurazione di una voce di ARP statico apporta molti vantaggi. Ad esempio, l'apprendimento della voce di ARP dinamico viene omesso durante la comunicazione del dispositivo e la voce di ARP statico impedisce a un dispositivo di apprendere una voce ARP non corretta in caso di attacchi dannosi.

P. Portale

1. Fare clic sulla scheda **Network Application** e scegliere **Portal Configuration** dalla struttura di navigazione. Nel riquadro di destra, attivare/disattivare la funzione del portale e impostare gli indirizzi URL di reindirizzamento per i diversi tipi di dispositivi, come illustrato nella [Figura 1](#).

Figura 1 Configurazione del portale

The screenshot shows the 'Portal Configuration' page. At the top, there is a yellow informational box: 'On this page, you can configure portal. The browser displays a special web page based on your device type when you access the Internet for the first time.' Below this, there are two main configuration sections. The first section has a checkbox for 'Enable Portal' which is checked, and a text input for 'Default Redirection URL' containing 'www.xxx.com'. There are 'Apply' and 'Cancel' buttons. The second section is a table with columns 'Device Type' and 'Redirection URL Address'. It has 'New' and 'Delete' buttons. Below the table, there is a form for adding a new entry: 'Device Type' is a dropdown menu set to 'Computer', and 'Redirection URL Address' is a text input containing 'www.xxx.com' with a red asterisk indicating a required field. There are 'Apply' and 'Cancel' buttons at the bottom.

2. Fare clic su **Apply**.

Se il tipo di dispositivo in uso non è configurato con un indirizzo URL o il tipo di dispositivo non può essere identificato, il sistema reindirizza all'indirizzo URL predefinito al momento del primo accesso a Internet.

Q. Dynamic DNS (DDNS)

1. Fare clic sulla scheda **Network Application** e scegliere **DDNS Configuration** dalla struttura di navigazione. Nel riquadro a destra, configurare i parametri DDNS, inclusi **Service Provider**, **Host Name**, **Service Port**, **Domain Name**, **Username** e **Password**, come illustrato nella [Figura 1](#).

Figura 1 Configurazione DDNS

Network Application > DDNS Configuration

On this page, you can set DDNS parameters, including the service provider, host name, service port, domain name to be updated, user name, and password.

New Delete

WAN Name	Status	Service Provider	Domain Name
Enable DDNS:	<input type="checkbox"/>		
WAN Name:			
Service Provider:		dyndns	
Host Name:		members.dyndns.org	*(1-255 characters)
Service Port:		80	*(1-65535)
Domain Name:		www.abc123.com	*(1-255 characters)
User Name:		user	*(1-255 characters)
Password:		*(1-255 characters)

Apply Cancel

2. Fare clic su **Apply**.

DDNS (Dynamic Domain Name Service) associa un nome di dominio statico all'indirizzo IP dinamico del suo host.

Si supponga che il server A fornisca un servizio HTTP o FTP e sia collegato ai router che utilizzano Internet. Se il server A ottiene un indirizzo IP tramite DHCP o il server A è connesso a Internet tramite PPPoE, PPTP o L2TP, l'indirizzo IP sarà un indirizzo IP dinamico. Cioè, il suo indirizzo IP cambia ogni volta che il server A inizializza il collegamento a Internet.

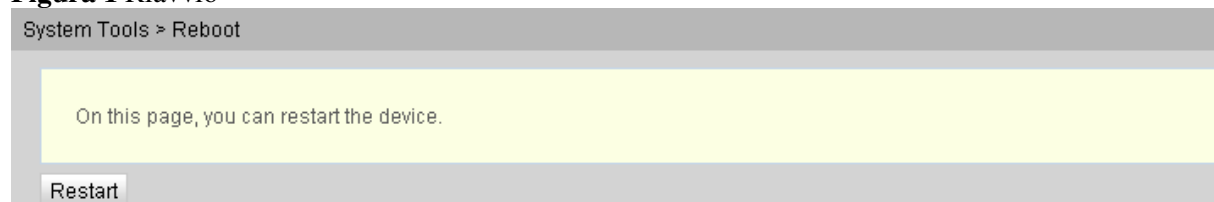
Il mapping tra il nome di dominio e l'indirizzo IP fornito dal server DNS (Domain Name Service) è statico e il mapping non si aggiorna quando l'indirizzo IP cambia. Di conseguenza, quando l'indirizzo IP del server A cambia, gli utenti su Internet non possono accedere al server A con i nomi di dominio.

Con DDNS, che associa un nome di dominio statico all'indirizzo IP dinamico dell'host, gli utenti su Internet possono accedere solo al server con i nomi di dominio.

7. Riavvio

Nella struttura di navigazione a sinistra, scegliere **System Tools > Reboot**. Nel riquadro di destra, fare clic su **Reboot** per riavviare il dispositivo, come illustrato nella [Figura 1](#).

Figura 1 Riavvio



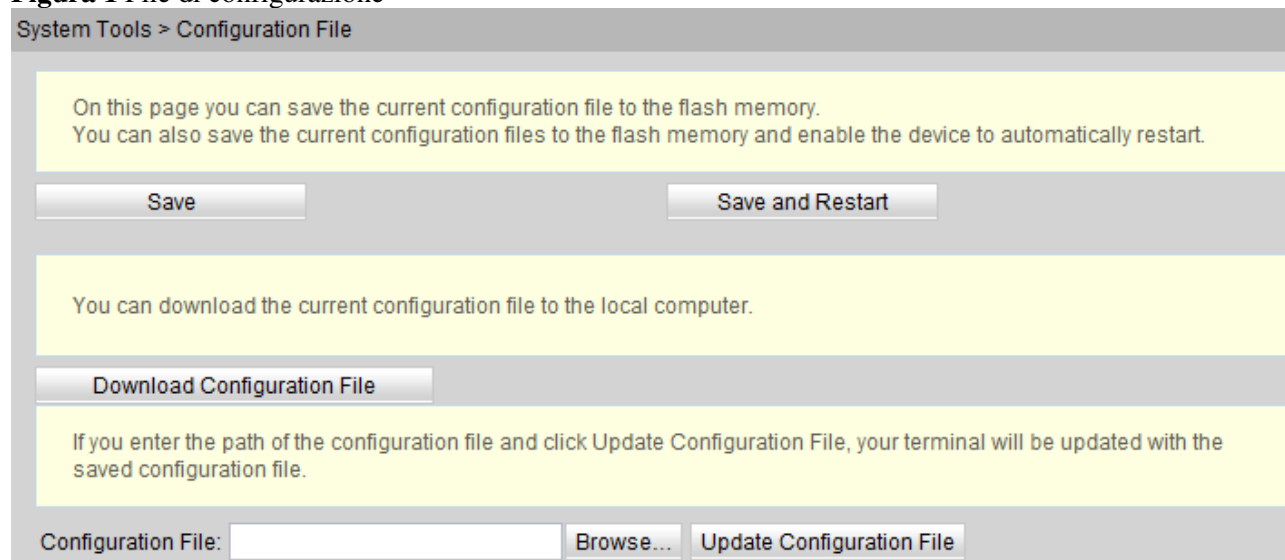
AVVISO:

salvare i dati di configurazione prima di riavviare il dispositivo. Per ulteriori dettagli, vedere [File di configurazione](#).

8. File di configurazione

Nella struttura di navigazione a sinistra, scegliere **System Tools > Configuration File**. Nel riquadro di destra, fare clic sul pulsante richiesto, come illustrato nella [Figura 1](#).

Figura 1 File di configurazione



- Fare clic su **Save** per salvare il file di configurazione nella memoria flash. Questa operazione previene la perdita di dati dovuta al riavvio del dispositivo.
- Fare clic su **Save and Restart** per salvare il file di configurazione e riavviare il modem.
- Fare clic su **Download Configuration File**. Nella finestra di dialogo visualizzata, fare clic su **Save**, specificare il percorso di salvataggio del file di configurazione, quindi eseguire il backup del file sul disco locale.

- Fare clic su **Browse** dopo la casella di testo **Configuration File**. Nella finestra di dialogo visualizzata, selezionare il file di configurazione da caricare. Fare clic su **Update Configuration File** per caricare il file di configurazione salvato nel disco locale. Dopo che il file di configurazione è caricato correttamente, il dispositivo si riavvia automaticamente, quindi viene applicata la nuova configurazione.

AVVISO:

prima di caricare il file di configurazione, scegliere il file di configurazione con il tipo corretto e verificare che il nome del file di configurazione selezionato non coincida con quelli di un qualsiasi file salvato nel dispositivo. In caso contrario, il file di configurazione non potrà essere caricato.

9. Cambio password di accesso

1. Fare clic sulla scheda **System Tools** e scegliere **Modify Login Password** dalla struttura di navigazione. Nel riquadro di destra, modificare la password dell'utente **root**, come illustrato nella [Figura 1](#).

Figura 1 Modalità della password di accesso

System Tools > Modify Login Password

On this page, you can change the password of a common user to ensure security and make it easy to remember.

User Name:	root	1.The password must contain at least 6 characters. 2.The password must contain at least two of the following combinations: Digit, uppercase letter, lowercase letter Special characters (~!@#\$%^&*()-_+=\ []{};:~<, .>/? and space). 3.The password cannot be any user name or user name in reverse order.
New Password:	<input type="text"/>	
Confirm Password:	<input type="text"/>	

Apply Cancel

NOTA:

- Dopo l'accesso dell'utente all'interfaccia Web del modem mediante il nome utente comune e la password predefiniti, l'interfaccia **Modify Login Password** viene visualizzata automaticamente e richiede all'utente di cambiare la password iniziale. Dopo che l'utente ha cambiato correttamente la password, l'interfaccia **Modify Login Password** non viene più visualizzata nei successivi accessi.
 - Cambiare il nome utente e la password iniziali dopo l'accesso alla pagina Web.
2. Fare clic su **Apply**.