GUIDA ALL'AMMINISTRAZI

Cisco Small Business

RV110W Firewall VPN Wireless-N

78-20161-01

Sommari

Chapter 1: Introduzione 8

Panoramica del prodotto 8
- Interfacce LAN Ethernet 9
- Punto di accesso wireless 9
- Accesso al client VPN 9
- Protezione 9
- Quality of Service 9
- Sistema di distribuzione wireless 10
- Reti virtuali 10
- Configurazione e amministrazione 10

Descrizione dell'unità Cisco RV110W 11
- Pannello frontale 11
- Pannello posteriore 12

Installazione dell'unità Cisco RV110W 13
- Posizionamento dell'unità 13

Collegamento dell'apparecchio 13

Utilizzo della procedura di installazione guidata 16
- Uso della pagina Introduzione 17
- Esplorazione delle pagine 19
- Salvataggio delle modifiche 20
- Visualizzazione dei file della Guida 20
- Passaggi successivi di configurazione 21

Verifica dell'installazione fisica 21

Collegamento alla rete wireless 22

Chapter 2: Configurazione della rete 23

Configurazione delle impostazioni WAN 23
- Impostazione della configurazione automatica (DHCP) 24
- Configurazione dell'indirizzo IP statico 24
- Configurazione PPPoE 25
- Configurazione PPTP 26

Configurazione L2TP 27
Configurazione delle impostazioni opzionali 29
Configurazione delle impostazioni LAN 29
Configurazione delle impostazioni LAN di base 30
Configurazione delle VLAN 34
Configurazione di DHCP statico 35
Visualizzazione dei client DHCP in leasing 36
Configurazione di un host DMZ 36
Configurazione RSTP 37
Clonazione dell'indirizzo MAC 38
Configurazione del routing 39
Configurazione della modalità operativa 39
Configurazione del routing dinamico 40
Configurazione del routing statico 41
Configurazione del routing Inter-VLAN 42
Gestione porte 43
Configurazione di DNS dinamico 44
Configurazione della modalità IP 45
Configurazione di IPv6 46
Configurazione della WAN per una rete IPv6 46
Configurazione delle impostazioni LAN IPv6 48
Configurazione del routing statico IPv6 51
Configurazione del routing (RIPng) 53
Configurazione del tunneling IPv6-to-IPv4 54
Visualizzazione dello stato del tunnel IPv6 54
Configurazione dell'annuncio router 54
Configurazione dei prefissi annuncio 56

Chapter 3: Configurazione della rete wireless 58

Sicurezza per reti wireless 58
Suggerimenti per la protezione delle reti wireless 59

Linee guida generali per la sicurezza di rete 60
RV110W Reti wireless 61
Configurazione delle impostazioni wireless 61
Configurazione delle impostazioni wireless di base 62
Configurazione delle impostazioni wireless avanzate 70
Configurazione di WDS 74
Configurazione di WPS 75

Chapter 4: Configurazione del firewall 79
RV110W - Funzionalità firewall 79
Configurazione delle impostazioni firewall di base 81
Configurazione della gestione remota 83
Configurazione di Universal Plug and Play 84
Gestione delle pianificazioni del firewall 84
Configurazione della gestione servizi 85
Configurazione delle regole di accesso 86
Configurazione del criterio predefinito in uscita 86
Aggiunta di regole di accesso 86
Creazione di un criterio di accesso a Internet 90
Configurazione del reindirizzamento delle porte 92
Configurazione reindirizzamento porta singola 92
Configurazione reindirizzamento intervallo porte 93
Configurazione attivazione intervallo di porte 94

Chapter 5: Configurazione VPN 96
Tipi di tunnel VPN 96
Client VPN 97
Configurazione PPTP 97
Creazione e gestione degli utenti PPTP 98
Creazione e gestione degli utenti QuickVPN 99
Importazioni delle impostazioni client VPN 100

Configurazione della gestione dei certificati 101
Configurazione del passthrough VPN 103

Chapter 6: Configurazione della Qualità del servizio (QoS) 104

Configurazione della gestione della larghezza di banda 105
Configurazione della larghezza di banda 105
Configurazione della priorità della larghezza di banda 106
Configurazione delle impostazioni di QoS basato su porta 107
Configurazione delle impostazioni CoS 108
Configurazione delle impostazioni DSCP 108

Chapter 7: Amministrazione dell'unità RV110W 110

Impostazione della complessità della password 111
Configurazione degli account utente 112
Impostazione dell'intervallo di timeout della sessione 113
Configurazione di SNMP (Simple Network Management Protocol) 114
Configurazione delle informazioni di sistema SNMP 114
Modifica degli utenti SNMPv3 115
Configurazione del trap SNMP 116
Utilizzo degli strumenti di diagnostica 117
Strumenti di rete 117
Configurazione del mirroring delle porte 118
Configurazione della registrazione 119
Configurazione delle impostazioni di registrazione 119
Configurazione dell'invio dei registri tramite e-mail 121
Configurazione di Bonjour 122
Configurazione delle impostazioni di data e ora 123
Backup e ripristino del sistema 124
Backup delle impostazioni di configurazione 125
Ripristino delle impostazioni di configurazione 126

Copia delle impostazioni di configurazione 126
Generazione di una chiave di crittografia 127
Aggiornamento del firmware 127
Riavvio dell'unità RV110W 128
Ripristino delle impostazioni di fabbrica 129
Esecuzione della procedura di installazione guidata 130

Chapter 8: Visualizzazione dello stato dell'unità RV110W 132

Visualizzazione del Dashboard 133
Visualizzazione del riepilogo di sistema 135
Visualizzazione delle statistiche wireless 138
Visualizzazione dello stato VPN 139
Visualizzazione dei registri 140
Visualizzazione dei dispositivi connessi 141
Visualizzazione delle statistiche delle porte 142

Appendix A: Utilizzo di Cisco QuickVPN 143

Panoramica 143
Operazioni preliminari 143
Installazione del software QuickVPN di Cisco 144
Installazione del software da CD 144
Download e installazione del software da Internet 146
Utilizzo del software Cisco QuickVPN 146

Appendix B: Risorse aggiuntive 149

1

Introduzione

In questo capitolo vengono fornite le informazioni per acquisire familiarità con le funzionalità del prodotto e per installarlo; viene inoltre presentata una guida introduttiva all'utilizzo di
Device Manager basato su browser.

- **Panoramica del prodotto, pagina 8**
- **Descrizione dell'unità Cisco RV110W, pagina 11**
- **Installazione dell'unità Cisco RV110W, pagina 13**
- **Collegamento dell'apparecchio, pagina 13**
- **Utilizzo della procedura di installazione guidata, pagina 16**
- **Verifica dell'installazione fisica, pagina 21**
- **Collegamento alla rete wireless, pagina 22**

Panoramica del prodotto

Grazie per aver scelto il Firewall VPN Wireless-N RV110W Cisco Small Business.

L'unità RV110W è una soluzione di rete avanzata per la condivisione di Internet appositamente studiata per soddisfare le esigenze delle piccole aziende. Questo dispositivo consente a più computer di un ufficio di condividere la stessa connessione Internet tramite connessioni cablate o wireless.

L'unità RV110W fornisce un punto di accesso Wireless-N in combinazione con il supporto per client VPN (Virtual Private Network), per rendere più sicuro l'accesso remoto alla rete.

L'interfaccia WAN 10/100 Fast Ethernet del router si collega direttamente al modem DSL a banda larga o al modem via cavo.

Interfacce LAN Ethernet

L'unità RV110W mette a disposizione quattro interfacce full-duplex 10/100 Fast Ethernet per poter collegare fino a quattro dispositivi. Uno switch Cisco Small Business può essere collegato a una delle porte disponibili per espandere la rete in base alle necessità.

Punto di accesso wireless

I punti di accesso wireless dell'unità RV110W supportano lo standard 802.11n con tecnologia MIMO che moltiplica la velocità effettiva dei dati. Ciò si traduce in una tecnologia di throughput e di copertura migliore di quella fornita dalle reti 802.11g.

Accesso al client VPN

L'unità RV110W supporta fino a cinque tunnel VPN da gateway a gateway per facilitare la connettività delle filiali attraverso collegamenti virtuali crittografati. Gli utenti che utilizzano un tunnel VPN sono connessi alla rete aziendale come se fossero situati nello stesso edificio fisico e possono accedere in modo sicuro a file, e-mail e intranet.

Protezione

L'unità RV110W implementa la protezione WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise e WEP, oltre ad altre funzionalità di protezione, fra cui la disattivazione delle trasmissioni SSID, il filtro basato su MAC e l'attivazione o la disattivazione a ore del giorno pianificate per SSID.

Quality of Service

L'unità RV110W supporta Wi-Fi Multimedia (WMM) e Wi-Fi Multimedia Power Save (WMM-PS) per Quality of Service (QoS, qualità del servizio).

L'unità RV110W supporta, inoltre, 802.1p, DSCP (Differentiated Services Code Point) e Type of Service (ToS, tipo di servizio) per QoS cablato, che consentono di migliorare la qualità della rete quando si utilizzano applicazioni VoIP (Voice over IP) sensibili ai ritardi e applicazioni di streaming video ad alto utilizzo di banda.

Sistema di distribuzione wireless

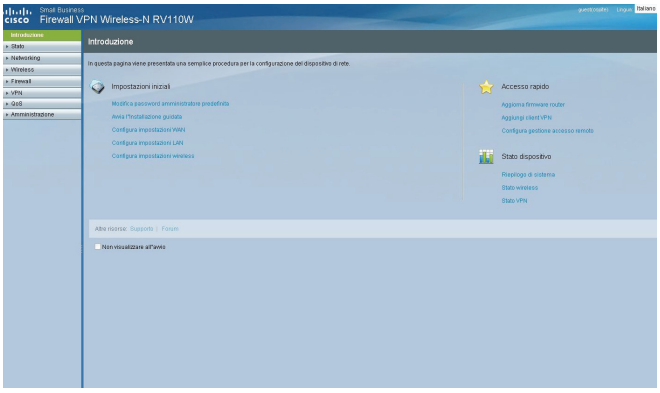
Il punto di accesso wireless dell'unità RV110W supporta il sistema di distribuzione wireless (WDS, Wireless Distribution System), che permette l'espansione senza cavi della copertura wireless.

Reti virtuali

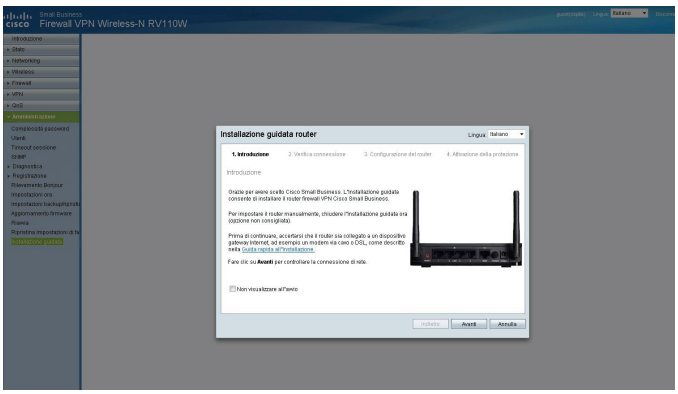
L'unità RV110W supporta anche più SSID (Service Set Identifier) per l'utilizzo di reti virtuali (fino a quattro reti virtuali separate), con supporto VLAN basato su 802.1Q per la separazione del traffico.

Configurazione e amministrazione

Con il server Web incorporato dell'unità RV110W è possibile configurare le impostazioni dell'unità RV110W utilizzando il Device Manager basato su browser. L'unità RV110W supporta i browser Web Internet Explorer, Firefox e Safari.



L'unità RV110W fornisce, inoltre, una procedura di installazione guidata che consente di configurare, con facilità e rapidità, le impostazioni di base dell'unità RV110W.



Descrizione dell'unità Cisco RV110W

Pannello frontale

	**Power (Alimentazione)**	Il led Power acceso e di colore verde indica che l'unità è accesa. La luce verde lampeggia durante l'accensione.
	**WPS**	Il pulsante relativo all'impostazione Wi-Fi protetta (WPS) viene utilizzato per configurare l'accesso wireless dei dispositivi di una rete abilitati per WPS. Per ulteriori informazioni, vedere la sezione **Configurazione di WPS, pagina 75**.
	**WAN (WAN)**	Il led WAN (Internet) è acceso e di colore verde quando l'unità RV110W è connessa a Internet tramite modem via cavo o DSL. Se il led è spento, significa che l'unità RV110W non è connessa a Internet. Il led verde lampeggia quando l'unità sta trasmettendo o ricevendo dati.
	**Wireless (Wireless)**	Il led Wireless è acceso e di colore verde quando il modulo wireless è attivato. Se il led è spento, significa che il modulo wireless è disattivato. Il led verde lampeggia quando il firewall sta trasmettendo o ricevendo dati sul modulo wireless.
	**Porte LAN**	I led numerati corrispondono alle porte LAN dell'unità RV110W. Quando la luce verde dei led è fissa, significa che l'unità RV110W è collegata a un dispositivo tramite la porta corrispondente (1, 2, 3 o 4). La luce verde del led di una porta lampeggia quando il firewall sta attivamente inviando o ricevendo dati attraverso tale porta.

Pannello posteriore

Tasto **RESET** (RESET). Questo tasto svolge due funzioni:

- Se l'unità RV110W non riesce a stabilire una connessione a Internet, tenere premuto il tasto **RESET** per almeno 3 secondi, ma non più di 10 secondi, con una graffetta o la punta di una matita. Questa operazione è analoga alla pressione del pulsante Reset di un PC per riavviarlo.
- Se il problema riscontrato sull'unità RV110W è molto grave e tutte le possibili azioni correttive hanno dato esito negativo, tenere premuto il tasto **RESET** per più di 10 secondi. L'unità viene riavviata e vengono ripristinate le impostazioni di fabbrica. Le modifiche apportate in precedenza alle impostazioni dell'unità RV110W andranno perse.

Porte LAN (1-4). Queste porte forniscono una connessione LAN per dispositivi di rete quali PC, server di stampa o switch.

Porta WAN (Internet). La porta WAN è collegata al dispositivo di connessione a Internet, ad esempio un modem via cavo o DSL.

Tasto **POWER** (ALIMENTAZIONE). Premere questo tasto per accendere e spegnere l'unità RV110W.

Porta **12 V CC**. Alla porta 12 V CC viene collegato l'alimentatore 12 V CA.

Installazione dell'unità Cisco RV110W

Posizionamento dell'unità

- **Temperatura ambiente.** Per evitare il surriscaldamento del firewall, non utilizzarlo in un'area in cui la temperatura ambiente sia maggiore di 40 °C (104 °F).
- **Circolazione dell'aria.** Assicurarsi che vi sia un'adeguata circolazione dell'aria intorno al dispositivo.
- **Carico meccanico.** Assicurarsi che il firewall sia in piano e stabile per evitare qualsiasi situazione pericolosa.

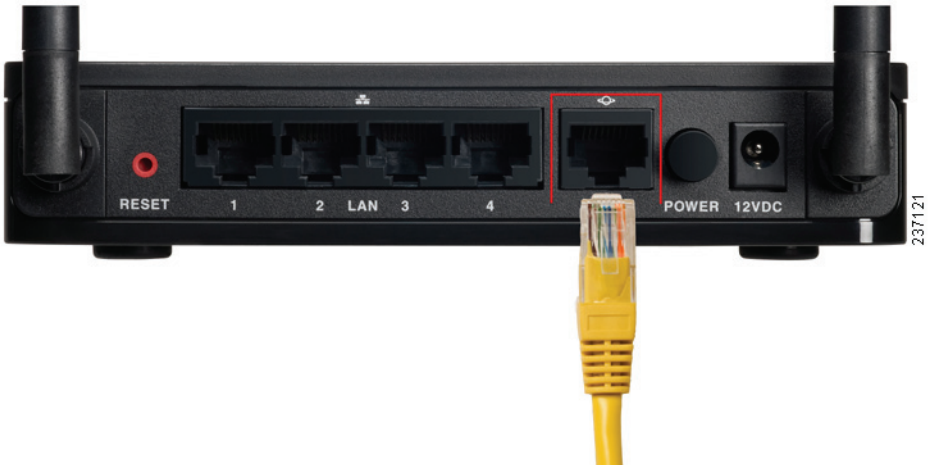
Posizionare l'unità RV110W orizzontalmente su una superficie piana, in modo che poggi sui piedini di gomma.

Collegamento dell'apparecchio

NOTA Per eseguire la configurazione iniziale, è necessario collegare un PC con un cavo Ethernet. Una volta terminata la configurazione iniziale, sarà possibile utilizzare una connessione wireless per lo svolgimento delle normali attività amministrative.

PASSAGGIO1 Spegnere tutte le apparecchiature, compresi il modem via cavo o DSL, il PC da utilizzare per collegarsi all'unità RV110W e l'unità RV110W.

PASSAGGIO 2 Il PC dovrebbe essere già collegato al modem via cavo o DSL corrente con un cavo Ethernet. Scollegare un'estremità del cavo dal PC e collegarla alla porta "WAN" dell'unità.



PASSAGGIO 3 Collegare un'estremità di un altro cavo Ethernet a una delle porte LAN (Ethernet) sul retro dell'unità (in questo esempio viene utilizzata la porta LAN1). Collegare l'altra estremità a una porta Ethernet del PC che verrà utilizzato per eseguire la procedura di installazione guidata e Device Manager, entrambi basati sul Web.

PASSAGGIO 4 Accendere il modem via cavo o DSL e attendere che la connessione sia attiva.

PASSAGGIO 5 Collegare l'alimentatore alla porta di alimentazione dell'unità RV110W (12 V CC).

ATTENZIONE Utilizzare esclusivamente l'alimentatore fornito con l'unità. L'utilizzo di un altro alimentatore potrebbe danneggiare l'unità.

PASSAGGIO 6 Collegare l'altra estremità dell'alimentatore a una presa di corrente. A seconda del paese potrebbe rendersi necessario l'utilizzo di una spina specifica (fornita).

PASSAGGIO 7 Premere il tasto **POWER** sull'unità RV110W per accendere il firewall. Se l'alimentatore è collegato correttamente e l'unità è accesa il led di alimentazione sul pannello anteriore diventa verde.

Utilizzo della procedura di installazione guidata

La procedura di installazione guidata e Device Manager sono supportati da Microsoft Internet Explorer 6.0 o versioni successive, Mozilla Firefox 3.0 o versioni successive e Apple Safari 3.0 o versioni successive.

Per utilizzare la procedura di installazione guidata, attenersi alla seguente procedura:

PASSAGGIO1 Accendere il computer collegato alla porta LAN1 nel passaggio 2 della sezione **Collegamento dell'apparecchio**.

Il computer diventa un client DHCP dell'unità RV110W e riceve un indirizzo IP nell'intervallo 192.168.1.xxx.

PASSAGGIO 2 Aprire il browser Web e immettere **192.168.1.1** nella barra degli indirizzi. Questo è l'indirizzo IP predefinito dell'unità RV110W.

Viene visualizzato un messaggio relativo al certificato di protezione del sito. L'unità RV110W utilizza un certificato di protezione con firma automatica e questo messaggio viene visualizzato perché il computer non riconosce il firewall.

PASSAGGIO 3 Fare clic su **Continua su questo sito** (o sull'opzione equivalente visualizzata nel browser Web) per accedere al sito Web.

L'indirizzo IP predefinito del firewall è 192.168.1.1. Se alla rete è collegato un altro dispositivo che agisce da server DHCP, tale dispositivo può assegnare all'unità RV110W un indirizzo diverso. In questi casi, utilizzare quell'indirizzo IP per collegare l'unità RV110W.

PASSAGGIO 4 Quando viene visualizzata la pagina di accesso, inserire il nome utente e la password.

Il nome utente predefinito è **cisco**. La password predefinita è **cisco**. Le password fanno distinzione tra maiuscole e minuscole. Per proteggere il router, modificare il nome utente e la password predefiniti il prima possibile. Vedere la sezione **Configurazione degli account utente, pagina 112**.

PASSAGGIO 5 Fare clic su **Accedi**.

Viene avviata la procedura di installazione guidata.

PASSAGGIO 6 Attenersi alle istruzioni visualizzate sullo schermo per configurare l'unità RV110W.

La procedura di installazione guidata tenta di rilevare e configurare automaticamente la connessione. Se l'operazione non dovesse dare risultati, la procedura di installazione guidata può richiedere informazioni relative alla connessione Internet. Se non si conoscono le informazioni richieste, contattare il provider di servizi Internet.

Al termine della configurazione dell'unità RV110W, viene visualizzata la pagina **Introduzione**. Per ulteriori informazioni, vedere la sezione **Uso della pagina Introduzione, pagina 17**.

Uso della pagina Introduzione

Nella pagina **Introduzione** vengono visualizzate alcune comuni attività di configurazione dell'unità RV110W. Utilizzare i collegamenti di questa pagina per passare alla pagina di configurazione pertinente.

Questa pagina viene visualizzata per impostazione predefinita all'avvio di Device Manager. Per evitare che venga visualizzata, selezionare la casella di controllo **Non visualizzare all'avvio**.

Impostazioni iniziali

Modifica password amministratore predefinita	Fare clic su questo collegamento per aprire la pagina **Utenti** in cui è possibile modificare la password dell'amministratore. Vedere la sezione **Configurazione degli account utente, pagina 112**.
Avvia l'Installazione guidata	Fare clic su questo collegamento per avviare la procedura di installazione guidata.
Configura impostazioni WAN	Fare clic su questo collegamento per aprire la pagina **Configurazione Internet**. Vedere la sezione **Configurazione delle impostazioni WAN, pagina 23**.
Configura impostazioni LAN	Fare clic su questo collegamento per aprire la pagina **Configurazione LAN**. Vedere la sezione **Configurazione delle impostazioni LAN, pagina 29**.
Configura impostazioni wireless	Fare clic su questo collegamento per aprire la pagina **Impostazioni di base**. Vedere la sezione **Configurazione delle impostazioni wireless di base, pagina 62**.

Accesso rapido

Aggiorna firmware router	Fare clic su questo collegamento per aprire la pagina **Aggiornamento firmware**. Vedere la sezione **Aggiornamento del firmware, pagina 127**.
Aggiungi client VPN	Fare clic su questo collegamento per aprire la pagina **Client VPN**. Vedere la sezione **Client VPN, pagina 97**.
Configura gestione accesso remoto	Fare clic su questo collegamento per aprire la pagina **Impostazioni di base**. Vedere la sezione **Configurazione delle impostazioni firewall di base, pagina 81**.

Stato dispositivo

Riepilogo di sistema	Fare clic su questo collegamento per aprire la pagina **Riepilogo di sistema**. Vedere la sezione **Visualizzazione del riepilogo di sistema, pagina 135**.
Stato wireless	Fare clic su questo collegamento per aprire la pagina **Statistiche wireless**. Vedere la sezione **Visualizzazione delle statistiche wireless, pagina 138**.
Stato VPN	Fare clic su questo collegamento per aprire la pagina **Stato VPN**. Vedere la sezione **Visualizzazione dello stato VPN, pagina 139**.

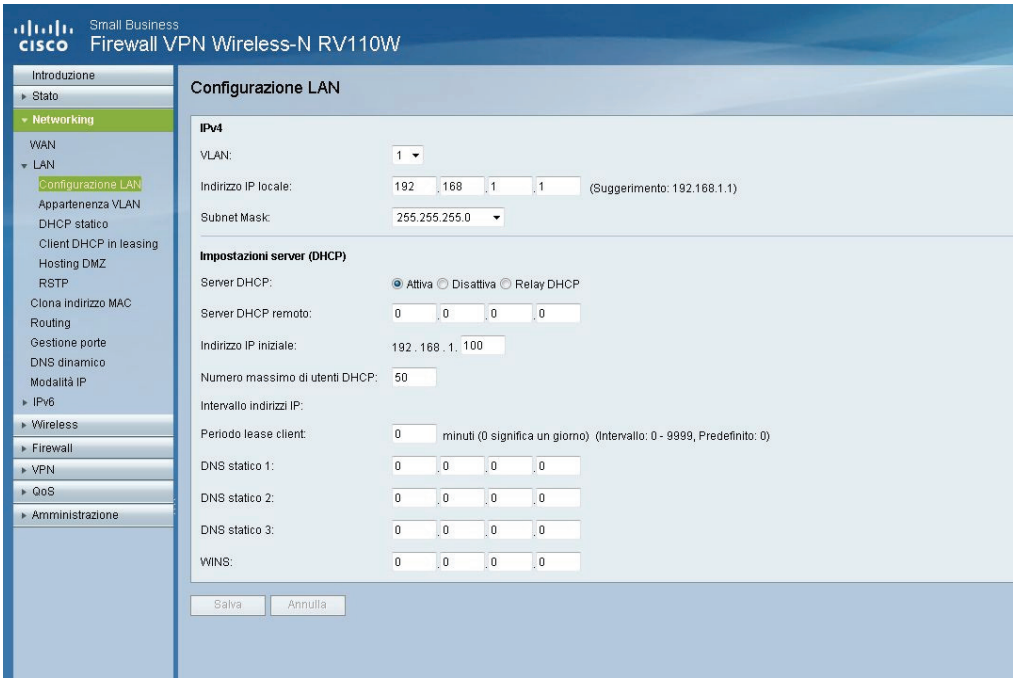
Altre risorse

Supporto	Fare clic su questo collegamento per aprire la pagina di supporto Cisco.
Forum	Fare clic su questo collegamento per visitare i forum di supporto Cisco.

Esplorazione delle pagine

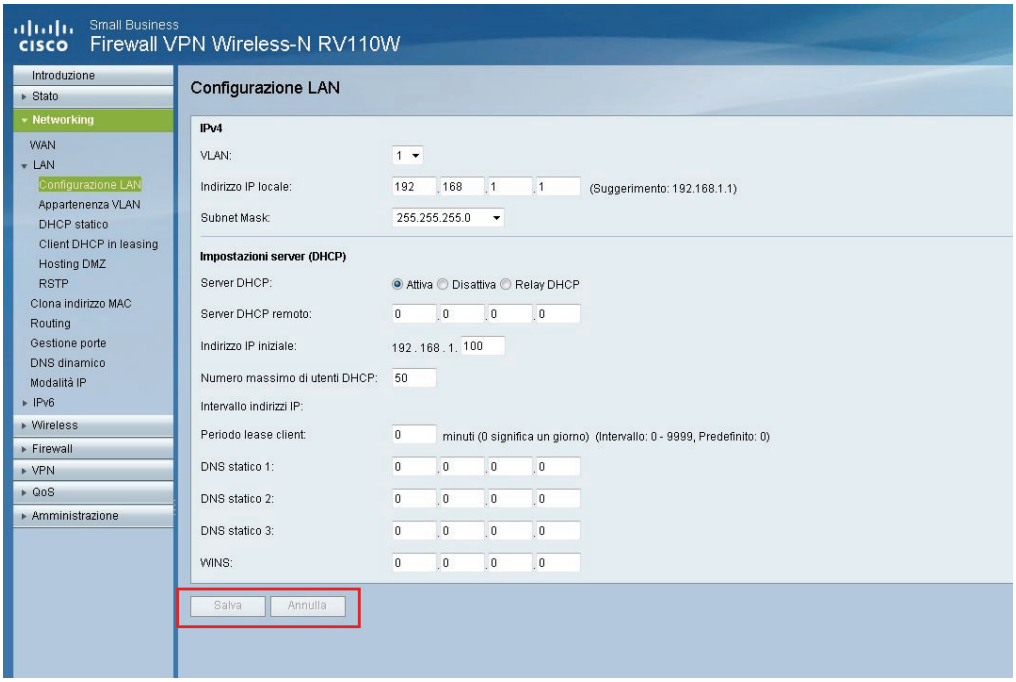
Per aprire le pagine di configurazione, utilizzare la struttura di spostamento nel pannello di sinistra.

Fare clic su una voce di menu nel pannello di sinistra per espanderla. Sotto di essa, fare clic su un nome di menu per eseguire un'azione o visualizzare un menu secondario.



Salvataggio delle modifiche

Dopo avere apportato le modifiche in una pagina di configurazione, fare clic su **Salva** per salvare le modifiche oppure fare clic su **Annulla** per annullare le modifiche.



Visualizzazione dei file della Guida

Per visualizzare ulteriori informazioni relative alla pagina di configurazione, fare clic sul collegamento **Guida** vicino all'angolo superiore destro della pagina.

Passaggi successivi di configurazione

Anche se la procedura di installazione guidata configura automaticamente l'unità RV110W, si raccomanda di modificare alcune delle impostazioni predefinite per fornire una maggiore protezione e prestazioni migliori.

Inoltre, potrebbe essere necessario configurare manualmente alcune impostazioni. Di seguito viene riportata una sequenza di passaggi consigliati:

- Modifica del nome dell'amministratore e della password: vedere la sezione **Configurazione degli account utente, pagina 112**.
- Modifica del valore di timeout di inattività: Device Manager si disconnette per impostazione predefinita dopo 10 minuti di inattività. Questo può essere frustrante se si sta tentando di configurare il dispositivo. Vedere la sezione **Impostazione dell'intervallo di timeout della sessione, pagina 113**.
- (Opzionale) Se la rete dispone già di un server DHCP e non si desidera che l'unità Cisco RV110W agisca da server DHCP, vedere la sezione **Configurazione delle impostazioni LAN, pagina 29**.
- Configurazione della rete wireless, in particolare la protezione wireless: vedere il **Capitolo 3, "Configurazione della rete wireless".**
- Configurazione della VPN (Virtual Private Network) tramite QuickVPN. Il software QuickVPN si trova sul CD della documentazione e software fornito in dotazione al firewall. Vedere **Appendice A, "Utilizzo di Cisco QuickVPN".**

Verifica dell'installazione fisica

Per verificare la corretta installazione dell'hardware, completare le attività seguenti:

- Controllare lo stato dei LED, come descritto nella sezione **Descrizione dell'unità Cisco RV110W, pagina 11**.
- Collegare un computer a una porta LAN disponibile e accertarsi che sia possibile collegarsi a un sito Web su Internet, ad esempio www.cisco.com.
- Configurare un dispositivo per il collegamento alla rete wireless e verificare la funzionalità della rete wireless. Vedere la sezione **Collegamento alla rete wireless, pagina 22**.

Collegamento alla rete wireless

Per collegare un dispositivo, ad esempio un computer, alla rete wireless, occorre configurare la connessione wireless sul dispositivo con le informazioni di protezione wireless configurate per l'unità RV110W durante la procedura guidata.

I seguenti passaggi sono forniti a titolo esemplificativo: potrebbe essere necessario configurare il dispositivo in modo diverso. Per istruzioni specifiche per il proprio dispositivo, consultare la relativa documentazione.

PASSAGGIO 1 Aprire la finestra con le impostazioni della connessione wireless o il programma del dispositivo.

Sul computer potrebbe essere installato un programma software speciale per gestire le connessioni wireless; in alternativa, le connessioni wireless possono essere visualizzate nel Pannello di controllo all'interno della finestra **Connessioni di rete** o **Rete e Internet** (la posizione varia a seconda del sistema operativo).

PASSAGGIO 2 Immettere il nome della propria rete (SSID) specificato durante la procedura guidata.

PASSAGGIO 3 Scegliere il tipo di crittografia e immettere la chiave di protezione definita nella procedura guidata.

Se non è stata attivata la protezione (sconsigliato), lasciare vuoti i campi relativi alla crittografia wireless configurati con il tipo di protezione e la frase chiave.

PASSAGGIO 4 Verificare la connessione wireless e salvare le impostazioni.

2

Configurazione della rete

In questo capitolo viene descritto come configurare le impostazioni di rete dell'unità RV110W.

- **Configurazione delle impostazioni WAN, pagina 23**
- **Configurazione delle impostazioni LAN, pagina 29**
- **Clonazione dell'indirizzo MAC, pagina 38**
- **Configurazione del routing, pagina 39**
- **Gestione porte, pagina 43**
- **Configurazione di DNS dinamico, pagina 44**
- **Configurazione della modalità IP, pagina 45**

Configurazione delle impostazioni WAN

La configurazione delle proprietà WAN per una rete IPv4 varia a seconda del tipo di connessione Internet di cui si dispone.

- **Impostazione della configurazione automatica (DHCP), pagina 24**
- **Configurazione dell'indirizzo IP statico, pagina 24**
- **Configurazione PPPoE, pagina 25**
- **Configurazione PPTP, pagina 26**
- **Configurazione L2TP, pagina 27**

Impostazione della configurazione automatica (DHCP)

Se il provider di servizi Internet (ISP) utilizza il protocollo DHCP (Dynamic Host Control Protocol) per assegnare un indirizzo IP, si riceve un indirizzo IP dinamico sempre nuovo generato a ogni accesso.

Per configurare le impostazioni WAN DHCP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **WAN**.

PASSAGGIO 2 Dal menu a discesa **Tipo di connessione Internet**, selezionare **Configurazione automatica - DHCP**.

PASSAGGIO 3 (Opzionale) Per configurare le impostazioni opzionali, vedere la sezione **Configurazione delle impostazioni opzionali, pagina 29**.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione dell'indirizzo IP statico

Se l'ISP ha assegnato un indirizzo IP permanente, eseguire i passi seguenti per configurare le impostazioni WAN:

PASSAGGIO 1 Selezionare **Networking** > **WAN**.

PASSAGGIO 2 Dal menu a discesa **Tipo di connessione Internet**, selezionare **IP statico**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IP Internet	Immettere l'indirizzo IP della porta WAN.
Subnet mask	Immettere la subnet mask della porta WAN.
Gateway predefinito	Immettere l'indirizzo IP del gateway predefinito.
DNS statico 1	Immettere l'indirizzo IP del server DNS primario.
DNS statico 2	Immettere l'indirizzo IP del server DNS secondario.

PASSAGGIO 4 (Opzionale) Per configurare le impostazioni opzionali, vedere la sezione **Configurazione delle impostazioni opzionali, pagina 29**.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione PPPoE

Per configurare le impostazioni PPPoE, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **WAN**.

PASSAGGIO 2 Dal menu a discesa **Tipo di connessione Internet**, selezionare **PPPoE**.

PASSAGGIO 3 Immettere le seguenti informazioni; se necessario, contattare l'ISP per ottenere le informazioni di accesso PPPoE:

Nome utente	Immettere il nome utente assegnato dall'ISP.
Password	Immettere la password assegnata dall'ISP.
Connessione su richiesta	Selezionare questa opzione se l'ISP calcola i costi sulla base della durata dei collegamenti. Se si seleziona questa opzione, la connessione Internet è attiva solo in presenza di traffico. Se la connessione rimane inattiva, vale a dire in assenza di flusso di traffico, la connessione viene chiusa. Se si fa clic su **Connessione su richiesta**, immettere il numero di minuti dopo i quali la connessione viene chiusa nel campo **Tempo massimo di inattività**.
Mantieni connessione attiva	Se si seleziona questa opzione, la connessione Internet rimane sempre attiva. Immettere il numero di secondi trascorsi i quali l'unità RV110W tenta di riconnettersi dopo una disconnessione.
Tipo di autenticazione	Scegliere il tipo di autenticazione: **Negoziazione automatica**: il server invia una richiesta di configurazione specificando l'algoritmo di protezione impostato. Quindi, l'unità RV110W restituisce le credenziali di autenticazione con il tipo di protezione inviato in precedenza dal server. **PAP**: l'unità RV110W utilizza il protocollo PAP (Password Authentication Protocol), per connettersi all'ISP. **CHAP**: l'unità RV110W utilizza il protocollo CHAP (Challenge Handshake Authentication Protocol) per la connessione all'ISP. **MS-CHAP o MS-CHAPv2**: l'unità RV110W utilizza il protocollo MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) per la connessione all'ISP.

PASSAGGIO 4 (Opzionale) Per configurare le impostazioni opzionali, vedere la sezione **Configurazione delle impostazioni opzionali, pagina 29**.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione PPTP

Per configurare le impostazioni PPTP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **WAN**.

PASSAGGIO 2 Dal menu a discesa **Tipo di connessione Internet**, selezionare **PPTP**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IP Internet	Immettere l'indirizzo IP della porta WAN.
Subnet mask	Immettere la subnet mask della porta WAN.
Gateway predefinito	Immettere l'indirizzo IP del gateway predefinito.
Server PPTP	Immettere l'indirizzo IP del server PPTP.
Nome utente	Immettere il nome utente assegnato dall'ISP.
Password	Immettere la password assegnata dall'ISP.
Connessione su richiesta	Selezionare questa opzione se l'ISP calcola i costi sulla base della durata dei collegamenti. Se si seleziona questa opzione, la connessione Internet è attiva solo in presenza di traffico. Se la connessione rimane inattiva, vale a dire in assenza di flusso di traffico, la connessione viene chiusa. Se si fa clic su **Connessione su richiesta**, immettere il numero di minuti dopo i quali la connessione viene chiusa nel campo **Tempo massimo di inattività**.
Mantieni connessione attiva	Se si seleziona questa opzione, la connessione Internet rimane sempre attiva. Immettere il numero di secondi trascorsi i quali l'unità RV110W tenta di riconnettersi dopo una disconnessione.

Tipo di autenticazione	Scegliere il tipo di autenticazione: **Negoziazione automatica**: il server invia una richiesta di configurazione specificando l'algoritmo di protezione impostato. Quindi, l'unità RV110W restituisce le credenziali di autenticazione con il tipo di protezione inviato in precedenza dal server. **PAP**: l'unità RV110W utilizza il protocollo PAP (Password Authentication Protocol), per connettersi all'ISP. **CHAP**: l'unità RV110W utilizza il protocollo CHAP (Challenge Handshake Authentication Protocol) per la connessione all'ISP. **MS-CHAP o MS-CHAPv2**: l'unità RV110W utilizza il protocollo MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) per la connessione all'ISP.

PASSAGGIO 4 (Opzionale) Per configurare le impostazioni opzionali, vedere la sezione **Configurazione delle impostazioni opzionali, pagina 29**.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione L2TP

Per configurare le impostazioni L2TP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **WAN**.

PASSAGGIO 2 Dal menu a discesa **Tipo di connessione Internet**, selezionare **L2TP**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IP Internet	Immettere l'indirizzo IP della porta WAN.
Subnet mask	Immettere la subnet mask della porta WAN.
Gateway predefinito	Immettere l'indirizzo IP del gateway predefinito.
Server L2TP	Immettere l'indirizzo IP del server L2TP.
Nome utente	Immettere il nome utente assegnato dall'ISP.

Password	Immettere la password assegnata dall'ISP.
Connessione su richiesta	Selezionare questa opzione se l'ISP calcola i costi sulla base della durata dei collegamenti. Se si seleziona questa opzione, la connessione Internet è attiva solo in presenza di traffico. Se la connessione rimane inattiva, vale a dire in assenza di flusso di traffico, la connessione viene chiusa. Se si fa clic su **Connessione su richiesta**, immettere il numero di minuti dopo i quali la connessione viene chiusa nel campo **Tempo massimo di inattività**.
Mantieni connessione attiva	Se si seleziona questa opzione, la connessione Internet rimane sempre attiva. Immettere il numero di secondi trascorsi i quali l'unità RV110W tenta di riconnettersi dopo una disconnessione.
Tipo di autenticazione	Scegliere il tipo di autenticazione: **Negoziazione automatica**: il server invia una richiesta di configurazione specificando l'algoritmo di protezione impostato. Quindi, l'unità RV110W restituisce le credenziali di autenticazione con il tipo di protezione inviato in precedenza dal server. **PAP**: l'unità RV110W utilizza il protocollo PAP (Password Authentication Protocol), per connettersi all'ISP. **CHAP**: l'unità RV110W utilizza il protocollo CHAP (Challenge Handshake Authentication Protocol) per la connessione all'ISP. **MS-CHAP o MS-CHAPv2**: l'unità RV110W utilizza il protocollo MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) per la connessione all'ISP.

PASSAGGIO 4 (Opzionale) Per configurare le impostazioni opzionali, vedere la sezione **Configurazione delle impostazioni opzionali, pagina 29**.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione delle impostazioni opzionali

Per configurare le impostazioni opzionali, attenersi alla seguente procedura:

PASSAGGIO 1 Nella sezione Impostazioni facoltative, configurare le seguenti opzioni:

Nome host	Immettere il nome host dell'unità RV110W.
Nome di dominio	Immettere il nome di dominio della rete.
MTU	Il valore MTU (Maximum Transmit Unit) indica la dimensione del pacchetto più grande che può essere inviato sulla rete. Il valore MTU predefinito per reti Ethernet è solitamente 1500 byte. Per le connessioni PPPoE questo valore è di 1492 byte. A meno che l'ISP non faccia richiesta di modifica, Cisco consiglia di selezionare l'opzione **Auto**. Le dimensioni predefinite MTU sono di 1500 byte. Se l'ISP richiede un'impostazione MTU personalizzata, selezionare **Manuale** e immettere le dimensioni MTU.
Dimensioni	Immettere le dimensioni MTU.

PASSAGGIO 2 Fare clic su **Salva**.

Configurazione delle impostazioni LAN

Le impostazioni DHCP e TCP/IP predefinite funzionano per la maggior parte delle applicazioni. Se si desidera impostare un altro PC della rete come server DHCP o se si desidera configurare manualmente le impostazioni di rete di tutti i PC, disattivare il DHCP.

Inoltre, invece di utilizzare un server DNS, che esegue la mappatura dei nomi di dominio Internet, come www.cisco.com, a numeri IP, è possibile utilizzare un server WINS (Windows Internet Naming Service).

Un server WINS è l'equivalente di un server DNS, ma utilizza il protocollo NetBIOS per risolvere i nomi degli host. L'unità RV110W include l'indirizzo IP del server WINS nella configurazione DHCP inviata ai client DHCP.

NOTA Quando l'unità RV110W è connessa ad un modem o a un dispositivo con una rete configurata sulla stessa sottorete (192.168.1.x), l'unità RV110W cambia automaticamente la sottorete LAN in una sottorete casuale basata su 10.x.x.x in modo da evitare conflitti con la sottorete sul lato WAN dell'unità RV110W.

È possibile assegnare un indirizzo IP a ciascuna sottorete logica aggiuntiva sull'unità RV110W.

- **Configurazione delle VLAN, pagina 34**
- **Configurazione di DHCP statico, pagina 35**
- **Visualizzazione dei client DHCP in leasing, pagina 36**
- **Configurazione di un host DMZ, pagina 36**
- **Configurazione RSTP, pagina 37**

Configurazione delle impostazioni LAN di base

È possibile configurare l'indirizzo IP e le impostazioni DHCP dell'unità RV110W.

- **Modifica dell'indirizzo IP predefinito dell'unità RV110W, pagina 31**
- **Configurazione di DHCP, pagina 32**

Modifica dell'indirizzo IP predefinito dell'unità RV110W

Per configurare indirizzo IP LAN predefinito dell'unità RV110W, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **Configurazione LAN**.

PASSAGGIO 2 Nella sezione **IPv4**, immettere le seguenti informazioni:

VLAN	Selezionare il numero VLAN nel menu a discesa.
Indirizzo IP locale	Immettere l'indirizzo IP LAN dell'unità RV110W. Accertarsi che l'indirizzo non sia utilizzato da un altro dispositivo.
Subnet mask	Selezionare la subnet mask per il nuovo indirizzo IP dal menu a discesa. La sottorete predefinita è 255.255.255.0.

PASSAGGIO 3 Fare clic su **Salva**.

Dopo avere modificato l'indirizzo IP LAN dell'unità RV110W , il PC non è più connesso all'unità RV110W.

PASSAGGIO 4 Per riconnettere il PC all'unità RV110W, eseguire una delle seguenti operazioni:

- Se sull'unità RV110W è configurato DHCP, rilasciare e rinnovare l'indirizzo IP del PC.
- Assegnare un indirizzo manuale al PC. L'indirizzo deve essere nella stessa sottorete dell'unità RV110W. Ad esempio, se si modifica l'indirizzo IP dell'unità RV110W in 10.0.0.1, assegnare al PC un indirizzo IP nell'intervallo compreso tra 10.0.0.2 e 10.0.0.255.

PASSAGGIO 5 Aprire una finestra del browser e immettere il nuovo indirizzo IP per collegarsi nuovamente all'unità RV110W.

Configurazione di DHCP

Per impostazione predefinita, l'unità RV110W funziona da server DHCP per gli host della WLAN (Wireless LAN) o LAN, assegna indirizzi IP e fornisce indirizzi server DNS.

Con DHCP attivato, l'indirizzo IP dell'unità RV110W serve da indirizzo gateway per la LAN. L'unità RV110W assegna indirizzi IP ai PC della LAN da un pool di indirizzi. L'unità RV110W testa ogni indirizzo prima che venga assegnato per evitare la presenza di indirizzi duplicati sulla LAN.

Per impostazione predefinita l'unità RV110W assegna un indirizzo IP a ciascun host della LAN dal pool di indirizzi IP predefinito (da 192.168.1.100 a 192.168.1.149). Se è necessario impostare un indirizzo IP statico per un host, utilizzare un indirizzo IP dal pool di indirizzi da 192.168.1.2 a 192.168.1.99. Questo previene conflitti con il pool di indirizzi IP predefinito.

Per configurare le impostazioni DHCP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **Configurazione LAN**.

PASSAGGIO 2 (Opzionale) Selezionare la VLAN che si desidera modificare dall'elenco a discesa.

PASSAGGIO 3 Nel campo **Server DHCP**, selezionare una delle seguenti opzioni:

Attiva	Fare clic su questo pulsante di opzione per consentire all'unità RV110W di agire come server DHCP sulla rete.
Disattiva	Fare clic su questo pulsante di opzione per disattivare DHCP sull'unità RV110W. Se si desidera che un altro dispositivo della rete agisca da server DHCP oppure per configurare manualmente le impostazioni di rete di tutti i PC, disattivare DHCP.
Relay DHCP	Fare clic su questo pulsante di opzione per selezionare Relay DHCP e configurare l'unità RV110W come unità di relay degli indirizzi IP da un server DHCP diverso.

PASSAGGIO 4 Se è stata selezionata l'opzione **Attiva**, immettere le informazioni seguenti:

Indirizzo IP iniziale	Immettere il primo indirizzo presente nel pool di indirizzi IP. A ogni nuovo client DHCP che si associa alla LAN viene assegnato un indirizzo IP (l'indirizzo IP finale nel pool viene determinato dal valore immesso nel campo **Numero massimo di utenti DHCP**).
Numero massimo di utenti DHCP	Immettere il numero massimo di client DHCP.
Intervallo indirizzi IP	(Solo lettura) Visualizza l'intervallo di indirizzi IP disponibili per i client DHCP.
Durata lease	Immettere la durata (in minuti) del lease degli indirizzi IP ai client.
DNS statico 1	Immettere l'indirizzo IP del server DNS primario.
DNS statico 2	Immettere l'indirizzo IP del server DNS secondario.
DNS statico 3	Immettere l'indirizzo IP del server DNS terziario.
WINS	Immettere l'indirizzo IP del server WINS primario.

PASSAGGIO 5 Se è stata selezionata l'opzione **Relay DHCP**, immettere l'indirizzo del gateway di relay nel campo **Server DHCP remoto**. Il gateway di relay trasmette messaggi DHCP tra sottoreti multiple.

PASSAGGIO 6 Fare clic su **Salva**.

Configurazione delle VLAN

Una VLAN (Virtual LAN) è un gruppo di punti terminali di una rete, associati per funzione o altre caratteristiche condivise. A differenza delle LAN, che hanno solitamente un fondamento geografico, le VLAN possono raggruppare punti terminali senza tenere in considerazione la posizione fisica delle apparecchiature degli utenti.

Per creare una VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **Appartenenza VLAN**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Immettere le informazioni seguenti:

ID VLAN	Immettere l'ID VLAN per assegnare i punti terminali dell'appartenenza VLAN. Immettere un numero compreso tra 3 e 4094. L'ID VLAN 1 è riservato alla VLAN predefinita, che viene utilizzata per i frame senza tag ricevuti sull'interfaccia. L'ID VLAN 2 è riservato e non può essere utilizzato.
Descrizione	Immettere una descrizione per identificare la VLAN.
Porta 1 **Porta 2** **Porta 3** **Porta 4**	È possibile associare le VLAN sull'unità Cisco RV110W alle porte LAN del dispositivo. Per impostazione predefinita, le 4 porte appartengono alla VLAN1. È possibile modificare queste porte per associarle ad altre VLAN. Scegliere il tipo di frame in uscita per ciascuna porta: **Senza tag**: l'interfaccia è un membro senza tag della VLAN. I frame della VLAN vengono inviati senza tag alla porta VLAN. **Con tag**: la porta è un membro con tag della VLAN. I frame della VLAN vengono inviati con tag alla porta VLAN. **Escluso**: la porta al momento non è un membro della VLAN. Questa è l'impostazione predefinita per tutte le porte quando viene creata la VLAN.

PASSAGGIO 4 Fare clic su **Salva**.

Per modificare le impostazioni di una VLAN, selezionare la VLAN e fare clic su **Modifica**. Per eliminare una VLAN selezionata, fare clic su **Elimina**. Fare clic su **Salva** per applicare le modifiche.

Configurazione di DHCP statico

L'unità RV110W può essere configurata per assegnare un indirizzo IP specifico ad un dispositivo con un indirizzo MAC specifico.

Per configurare DHCP statico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **DHCP statico**.

PASSAGGIO 2 Dal menu a discesa **VLAN**, selezionare un numero di VLAN.

PASSAGGIO 3 Fare clic su **Aggiungi riga**.

PASSAGGIO 4 Immettere le informazioni seguenti:

Descrizione	Immettere una descrizione per il client.
Indirizzo IP	Immettere l'indirizzo IP del dispositivo. L'indirizzo IP assegnato deve essere esterno al pool di indirizzi DHCP configurati. Il pool DHCP viene trattato come pool generico e tutti gli indirizzi IP riservati devono trovarsi all'esterno di questo pool. L'assegnazione statica di DHCP significa che il server DHCP assegna lo stesso IP all'indirizzo MAC definito ogni volta che questo dispositivo viene connesso alla rete. Il server DHCP fornisce l'indirizzo IP riservato quando il dispositivo che utilizza l'indirizzo MAC corrispondente richiede un indirizzo IP.
Indirizzo MAC	Immettere l'indirizzo MAC del dispositivo. Il formato dell'indirizzo MAC è XX:XX:XX:XX:XX:XX in cui X è un numero da 0 a 9 (inclusi) o una lettera dell'alfabeto tra A e F (inclusi).

Per modificare le impostazioni di un client DHCP statico, selezionare il client e fare clic su **Modifica**. Per eliminare un DHCP statico selezionato, fare clic su **Elimina**. Fare clic su **Salva** per applicare le modifiche.

Visualizzazione dei client DHCP in leasing

È possibile visualizzare un elenco di tutti i punti terminali su una rete (identificati da nome host, indirizzo IP o indirizzo MAC) e vedere gli indirizzi IP assegnati loro dal server DHCP. Viene visualizzata anche la VLAN dei punti terminali.

Per visualizzare i client DHCP, selezionare **Networking** > **LAN** > **Client DHCP in leasing**.

Per ogni VLAN definita sull'unità RV110W l'interfaccia utente visualizza un elenco dei client associati alla VLAN.

Configurazione di un host DMZ

L'unità RV110W supporta zone demilitarizzate (DMZ). Una zona demilitarizzata o DMZ è una sottorete aperta al pubblico, ma che si trova dietro al firewall. Una rete DMZ consente di reindirizzare i pacchetti che arrivano all'indirizzo IP della porta WAN ad un indirizzo IP specifico della LAN.

Si consiglia di posizionare gli host che devono essere esposti alla WAN, ad esempio il server Web o di posta, nella rete DMZ. È possibile configurare le regole del firewall per consentire l'accesso a servizi e a porte specifiche nella rete DMZ sia dalla LAN che dalla WAN.

Nel caso di attacchi su uno qualsiasi dei nodi DMZ, la LAN non è necessariamente vulnerabile.

È necessario configurare un indirizzo IP fisso (statico) per il punto terminale designato come host DMZ. È necessario assegnare all'host DMZ un indirizzo IP che si trova nella stessa sottorete dell'indirizzo IP dell'unità RV110W, ma che non può essere identico all'indirizzo IP assegnato all'interfaccia LAN di questo gateway.

Per configurare la rete DMZ, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **Hosting DMZ**.

PASSAGGIO 2 Selezionare la casella di controllo **Attiva** per attivare DMZ sulla rete.

PASSAGGIO 3 Dal menu a discesa VLAN, selezionare l'ID della VLAN sulla quale è attivato DMZ.

PASSAGGIO 4 Nel campo **Indirizzo IP host,** immettere l'indirizzo IP dell'host DMZ.

L'host DMZ è il punto terminale che riceve i pacchetti reindirizzati.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione RSTP

Per configurare il protocollo RTSP (Rapid Spanning Tree Protocol), attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **RSTP**.

PASSAGGIO 2 Configurare le seguenti impostazioni:

Priorità di sistema	Selezionare la priorità di sistema dal menu a discesa. È possibile selezionare una priorità di sistema compresa tra 0 e 61440 con incrementi di 4096. I valori validi sono 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344 e 61440. Più bassa è la priorità di sistema, più probabilità ci sono che l'unità RV110W diventi la radice dell'albero di spanning. L'impostazione predefinita è **32768**.
Hello Time	Immettere un numero compreso tra 1 e 10. L'impostazione predefinita è **2**.
Tempo massimo	Immettere un numero compreso tra 6 e 40. L'impostazione predefinita è **20**.
Ritardo reindirizzamento	Immettere un numero compreso tra 4 e 30. L'impostazione predefinita è **15**.
Forza versione	Selezionare la versione del protocollo predefinito da utilizzare. Selezionare **Normale** (utilizzo di RSTP) o **Compatibile** (compatibile con il vecchio STP). L'impostazione predefinita è **Normale**.

PASSAGGIO 3 Nella **tabella delle impostazioni**, configurare le seguenti impostazioni:

Abilita protocollo	Selezionare questa opzione per attivare RSTP sulla porta associata. RSTP è disattivato per impostazione predefinita.
Edge	Selezionare questa opzione per specificare che la porta associata è una porta edge (stazione terminale). Deselezionare questa opzione per specificare che la porta associata è un collegamento (bridge) a un altro dispositivo STP. L'opzione Edge per la porta è attiva per impostazione predefinita.

Costo percorso	Immettere il costo di percorso per la porta. Il costo di percorso RSTP per le porte designate. Inserire un numero da 1 a 200000000 oppure auto (costo di percorso generato automaticamente). L'impostazione predefinita è **auto**.

PASSAGGIO 4 Fare clic su **Salva**.

Clonazione dell'indirizzo MAC

A volte può essere necessario impostare l'indirizzo MAC per la porta WAN dell'unità RV110W in modo che sia identico all'indirizzo MAC del PC o a un altro indirizzo MAC. Questa procedura è denominata clonazione dell'indirizzo MAC.

Ad esempio, alcuni ISP registrano l'indirizzo MAC della scheda NIC del computer durante l'installazione del servizio. Se si posiziona un router dietro al modem via cavo o DSL, l'indirizzo MAC della porta WAN dell'unità RV110W non viene riconosciuto dall'ISP.

In questo caso, per configurare l'unità RV110W in modo da essere riconosciuta dall'ISP, clonare l'indirizzo MAC della porta WAN in modo che sia identico a quello del computer.

Per configurare un clone di indirizzo MAC, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Clona indirizzo MAC**.

PASSAGGIO 2 Nel campo **Clona indirizzo MAC,** selezionare la casella di controllo **Attiva** per attivare la clonazione dell'indirizzo MAC.

PASSAGGIO 3 Per impostare l'indirizzo MAC della porta WAN dell'unità RV110W, procedere come indicato di seguito:

- Per utilizzare l'indirizzo MAC del PC come indirizzo MAC della porta WAN, fare
  clic su **Clona indirizzo MAC del PC**.
- Per specificare un indirizzo MAC diverso, immettere l'indirizzo desiderato nel campo **Indirizzo MAC**.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione del routing

È possibile configurare le seguenti opzioni di routing:

- **Configurazione della modalità operativa, pagina 39**
- **Configurazione del routing dinamico, pagina 40**
- **Configurazione del routing statico, pagina 41**
- **Configurazione del routing Inter-VLAN, pagina 42**

Configurazione della modalità operativa

Per configurare la modalità operativa dell'unità RV110W, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Routing**.

PASSAGGIO 2 Nel campo **Modalità operativa,** selezionare una delle seguenti opzioni:

Gateway	(Opzione consigliata) Fare clic su questo pulsante di opzione per impostare l'unità RV110W come gateway. Mantenere questa impostazione predefinita se l'unità RV110W ospita la connessione di rete a Internet.
Router	Fare clic su questo pulsante di opzione per impostare l'unità RV110W come router. Selezionare questa opzione se l'unità RV110W si trova su una rete con altri router. Se si attiva la modalità router, la funzionalità NAT (Network Address Translation) viene disattivata sull'unità RV110W.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione del routing dinamico

Il protocollo RIP (Routing Information Protocol) è un protocollo IGP (Interior Gateway Protocol) utilizzato comunemente nelle reti interne. Questo protocollo consente al router di scambiare automaticamente le informazioni di routing con altri router; consente, inoltre, di regolare in modo dinamico le tabelle di routing e adattarsi alle modifiche della rete.

Il routing dinamico (RIP) consente all'unità RV110W di regolarsi automaticamente alle modifiche fisiche nella disposizione della rete e scambiare le tabelle di routing con gli altri router.

Il router determina il percorso dei pacchetti di rete con il minor numero di hop tra l'origine e la destinazione. La funzionalità RIP è disattivata per impostazione predefinita.

NOTA La funzionalità RIP è disattivata per impostazione predefinita sull'unità RV110W.

Per configurare il routing dinamico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Routing**.

PASSAGGIO 2 Configurare le seguenti impostazioni:

RIP	Selezionare la casella di controllo **Attiva** per attivare la funzionalità RIP. Questo consente all'unità RV110W di utilizzare la funzionalità RIP per il routing del traffico.
Versione pacchetto RIP Invia	Sezionare la versione pacchetto RIP Invia (**RIPv1** o **RIPv2**). La versione di RIP utilizzata per inviare gli aggiornamenti di routing agli altri router della rete dipende dalle impostazioni di configurazione degli altri router. La soluzione migliore consiste nel contattare l'amministratore di rete per conoscere la versione di RIP supportata dalla rete. RIPv2 è compatibile all'indietro con RIPv1.
Versione pacchetto RIP Ricevi	Scegliere la versione pacchetto RIP Ricevi.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione del routing statico

È possibile configurare i percorsi statici per indirizzare i pacchetti alla rete di destinazione. Un percorso statico è un percorso predeterminato che un pacchetto deve percorrere per raggiungere un host o una rete specifica.

Alcuni ISP richiedono percorsi statici invece dei protocolli di routing dinamico per creare la tabella di routing. I percorsi statici non richiedono risorse della CPU per lo scambio di informazioni di routing con un router paritetico.

È inoltre possibile utilizzare i percorsi statici per raggiungere i router paritetici che non supportano i protocolli di routing dinamico. I percorsi statici possono essere utilizzati insieme a quelli dinamici.

ATTENZIONE Fare però attenzione a non introdurre loop di routing nella rete.

Per configurare il routing statico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Routing**.

PASSAGGIO 2 Dal menu a discesa **Voci percorso**, selezionare una voce percorso.

Per eliminare una voce percorso, fare clic su **Elimina voce**.

PASSAGGIO 3 Configurare le impostazioni seguenti per la voce percorso selezionata:

Immettere il nome del percorso	Immettere il nome del percorso.
IP LAN destinazione	Immettere l'indirizzo IP della LAN di destinazione.
Subnet mask	Immettere la subnet mask della rete di destinazione.
Gateway	Immettere l'indirizzo IP del gateway utilizzato per questo percorso.
Interfaccia	Selezionare l'interfaccia alla quale sono inviati i pacchetti per questo percorso: **LAN e wireless**: fare clic su questo pulsante di opzione per indirizzare i pacchetti verso la rete LAN e wireless. **Internet (WAN)**: fare clic su questo pulsante di opzione per indirizzare i pacchetti verso la rete Internet (WAN).

PASSAGGIO 4 Per visualizzare le informazioni di routing della rete, fare clic su **Mostra tabella di routing**.

Nell'interfaccia viene visualizzata la tabella di routing.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione del routing Inter-VLAN

Per configurare il routing Inter-VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Routing**.

PASSAGGIO 2 Nel campo **Routing Inter-VLAN**, selezionare la casella di controllo **Attiva** per attivare il routing Inter-VLAN.

PASSAGGIO 3 Fare clic su **Salva**.

Gestione porte

È possibile configurare le impostazioni di velocità e di controllo del flusso delle quattro porte LAN dell'unità RV110W.

Per configurare la velocità e il controllo del flusso delle porte, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Network** > **Gestione porte**.

PASSAGGIO 2 Configurare le informazioni seguenti:

Porta	Il numero della porta.
Collegamento	La velocità della porta. Se alla porta non sono collegati dispositivi, in questo campo viene mostrato **Giù**.
Modalità	Selezionare dal menu a discesa una delle seguenti quattro velocità di porta: ▪ **Negoziazione automatica**: l'unità RV110W e il dispositivo connesso scelgono una velocità comune. ▪ **10Mbps Half**: 10 Mbps in entrambe le direzioni, ma solo una direzione alla volta. ▪ **10Mbps Full**: 10 Mbps in entrambe le direzioni simultaneamente. ▪ **100Mbps Half**: 100 Mbps in entrambe le direzioni, ma solo una direzione alla volta. ▪ **100Mbps Full**: 100 Mbps in entrambe le direzioni simultaneamente.
Controllo flusso	Selezionare questa opzione per attivare il controllo di flusso per la porta. Il controllo di flusso è il processo di gestione della frequenza di trasmissione dati tra due nodi per prevenire che un trasmettitore veloce trasmetta più velocemente di quello che un ricevitore lento possa ricevere. Fornisce un meccanismo che permette al ricevitore di controllare la velocità di trasmissione, in modo che il nodo di ricezione non venga sopraffatto con dati dal nodo di trasmissione.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione di DNS dinamico

DDNS (Dynamic DNS) è un servizio Internet che consente di localizzare i router che dispongono di IP pubblici variabili utilizzando i nomi di dominio Internet. Per utilizzare il servizio DDNS è necessario creare un account con un fornitore di servizi DDNS, ad esempio DynDNS.com, TZO.com o 3322.org.

Il router notifica ai server del servizio DNS dinamico i cambiamenti dell'indirizzo IP WAN, in modo da permettere l'accesso ai servizi pubblici della rete tramite il nome di dominio.

Per configurare il servizio DDNS, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **DNS dinamico**.

PASSAGGIO 2 Dal menu a discesa **Servizio DDNS**, selezionare **Disattiva** per disattivare il servizio o selezionare il servizio DDNS da utilizzare.

PASSAGGIO 3 Se non si dispone di un account DDNS, fare clic sull'URL del servizio per visitare il relativo sito Web e creare un account.

PASSAGGIO 4 Configurare le informazioni seguenti:

Indirizzo e-mail	(TZO.com) Immettere l'indirizzo e-mail utilizzato per creare l'account DDNS.
Nome utente	(DynDNS.com e 3322.org) Immettere il nome utente dell'account DDNS.
Password	Immettere la password per l'account DDNS.
Verifica password	Immettere di nuovo la password per l'account DDNS.
Nome host	Immettere il nome host del server DDNS.
Indirizzo IP Internet	(Solo lettura) L'indirizzo IP Internet dell'unità RV110W.
Stato	(Solo lettura) Viene mostrato lo stato per indicare se l'aggiornamento del servizio DDNS è stato completato correttamente o se l'invio al server DDNS delle informazioni di aggiornamento dell'account non è riuscito.

PASSAGGIO 5 Per testare la configurazione DDNS, fare clic su **Test configurazione**.

PASSAGGIO 6 Fare clic su **Salva**.

Configurazione della modalità IP

Le proprietà di configurazione della WAN possono essere definite sia per reti IPv4 che per reti IPv6. In queste pagine è possibile immettere informazioni relative alla connessione Internet e altri parametri.

Per selezionare una modalità IP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Modalità IP**.

PASSAGGIO 2 Dal menu a discesa **Modalità IP**, selezionare una delle seguenti opzioni:

LAN:IPv4, WAN:IPv4	Selezionare questa opzione per utilizzare IPv4 sulle porte LAN e WAN.
LAN:IPv6, WAN:IPv4	Selezionare questa opzione per utilizzare IPv6 sulle porte LAN e IPv4 sulle porte WAN.
LAN:IPv6, WAN:IPv6	Selezionare questa opzione per utilizzare IPv6 sulle porte LAN e WAN.
LAN:IPv4+IPv6, WAN:IPv4	Selezionare questa opzione per utilizzare IPv4 e IPv6 sulle porte LAN e IPv4 sulle porte WAN.

PASSAGGIO 3 (Opzionale) Se si sta utilizzando il tunneling 6to4, che permette la trasmissione di pacchetti IPv6 su una rete IPv4, procedere come segue:

a. Fare clic su **Mostra voce DNS 6to4 statico**.

b. Nei campi **Dominio** e **IP**, immettere fino a 5 mappature dominio-IP.

La funzione di tunneling 6to4 viene solitamente utilizzata quando un sito o un utente finale desidera connettersi a Internet IPv6 utilizzando la rete IPv4 esistente.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione di IPv6

- **Configurazione del tunneling IPv6-to-IPv4, pagina 54, pagina 46**
- **Configurazione delle impostazioni LAN IPv6, pagina 48**
- **Configurazione del routing statico IPv6, pagina 51**
- **Configurazione del routing (RIPng), pagina 53**
- **Configurazione del tunneling IPv6-to-IPv4, pagina 54**
- **Configurazione dell'annuncio router, pagina 54**

Configurazione della WAN per una rete IPv6

La configurazione delle proprietà WAN per una rete IPv6 varia a seconda del tipo di connessione Internet di cui si dispone.

È possibile configurare l'unità RV110W per agire da client DHCPv6 dell'ISP per questa WAN o utilizzare un indirizzo IPv6 statico fornito dall'ISP.

- **Impostazione della modalità IP, pagina 46**
- **Configurazione di DHCPv6, pagina 47**
- **Configurazione di un indirizzo IP statico, pagina 47**

Impostazione della modalità IP

Per configurare le impostazioni WAN di IPv6 sull'unità RV110W, è necessario impostare prima la modalità IP su LAN:IPv6, WAN:IPv6.

Per ulteriori informazioni, vedere la sezione **Configurazione della modalità IP, pagina 45**.

Configurazione di DHCPv6

Se l'ISP fornisce un indirizzo dinamico, configurare l'unità RV110W come client DHCPv6.

Per configurare l'unità RV110W come client DHCPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Configurazione WAN IPv6**.

PASSAGGIO 2 Nel campo **Tipo di connessione WAN**, fare clic sul pulsante di opzione **Configurazione automatica - DHCPv6**.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione di un indirizzo IP statico

Se l'ISP assegna un indirizzo fisso per l'accesso a Internet, configurare l'unità RV110W per l'utilizzo di un indirizzo IPv6 statico.

Per configurare l'unità RV110W per l'utilizzo di un indirizzo IPv6 statico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Configurazione WAN IPv6**.

PASSAGGIO 2 Nel campo **Tipo di connessione WAN**, fare clic sul pulsante di scelta **IPv6 statico**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IPv6	Immettere l'indirizzo IPv6 della porta WAN.
Lunghezza prefisso IPv6	Immettere la lunghezza di prefisso IPv6 definita dall'ISP. La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo che sono denominati prefisso. Ad esempio, nell'indirizzo IP 2001:0DB8:AC10:FE01::, 2001 è il prefisso. Tutti gli host della rete hanno bit iniziali identici per l'indirizzo IPv6; in questo campo viene impostato il numero di bit iniziali comuni degli indirizzi di rete.

Gateway IPv6 predefinito	Immettere l'indirizzo IPv6 del gateway predefinito. Si tratta dell'indirizzo IP del server sull'ISP al quale il router si connette per accedere a Internet.
DNS statico 1	Immettere l'indirizzo IP del server DNS primario sulla rete IPv6 dell'ISP.
DNS statico 2	Immettere l'indirizzo IP del server DNS secondario sulla rete IPv6 dell'ISP.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione delle impostazioni LAN IPv6

Nella modalità IPv6 il server DHCP LAN è attivato per impostazione predefinita (analogamente alla modalità IPv4). Il server DHCPv6 assegna gli indirizzi IPv6 dai pool di indirizzi configurati che utilizzano la lunghezza di prefisso IPv6 assegnata alla LAN.

- **Impostazione della modalità IP, pagina 48**
- **Configurazione di un indirizzo IP statico, pagina 49**
- **Configurazione delle impostazioni di DHCPv6, pagina 50**
- **Configurazione dei pool di indirizzi IPv6, pagina 51**

Impostazione della modalità IP

Per configurare le impostazioni IPv6 LAN sull'unità RV110W, è necessario impostare prima la modalità IP su una delle seguenti modalità:

- LAN:IPv6, WAN:IPv4
- LAN:IPv6, WAN:IPv6
- LAN:IPv4+IPv6, WAN:IPv4

Per ulteriori informazioni, vedere la sezione **Configurazione della modalità IP, pagina 45**.

Configurazione di un indirizzo IP statico

Per configurare le impostazioni LAN IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Configurazione LAN IPv6**.

PASSAGGIO 2 Immettere le seguenti informazioni per configurare l'indirizzo IPv6 LAN:

Indirizzo IPv6	Immettere l'indirizzo IPv6 dell'unità RV110W. L'indirizzo IPv6 predefinito del gateway è fec0::1. È possibile modificare questo indirizzo IPv6 a 128 bit in base ai requisiti di rete.
Lunghezza prefisso IPv6	Immettere la lunghezza del prefisso IPv6. La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Il prefisso è lungo 64 bit per impostazione predefinita. Tutti gli host della rete hanno bit iniziali identici per l'indirizzo IPv6; in questo campo viene impostato il numero di bit iniziali comuni degli indirizzi di rete.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione delle impostazioni di DHCPv6

Per configurare le impostazioni LAN IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Configurazione LAN IPv6**.

PASSAGGIO 2 Immettere le seguenti informazioni per configurare le impostazioni DHCPv6:

Stato DHCP	Selezionare questa opzione per attivare il server DHCPv6. Se attivato, l'unità RV110W assegna un indirizzo IP nell'intervallo specificato più informazioni specifiche aggiuntive per qualsiasi punto terminale LAN che richiede indirizzi assegnati da DHCP.
Nome di dominio	(Opzionale) Immettere il nome di dominio del server DHCPv6.
Preferenza server	Immettere il livello di preferenza per il server DHCP. I messaggi di annuncio DHCP con il valore di preferenza server più alto rispetto a un host LAN sono preferiti rispetto ad altri messaggi di annuncio server DHCP. L'impostazione predefinita è 255.
DNS statico 1	Immettere l'indirizzo IPv6 del server DNS primario sulla rete IPv6 dell'ISP.
DNS statico 2	Immettere l'indirizzo IPv6 del server DNS secondario sulla rete IPv6 dell'ISP.
Periodo lease client	Immettere il periodo di lease del client. Immettere la durata (in secondi) del lease degli indirizzi IPv6 ai punti terminali della LAN.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione dei pool di indirizzi IPv6

È possibile definire il prefisso di delega IPv6 per una serie di indirizzi IPv6 che devono essere forniti dal server DHCPv6 dell'unità RV110W.

L'utilizzo di un prefisso di delega consente di automatizzare il processo di notifica ad altre apparecchiature di rete della LAN delle informazioni DHCP specifiche per il prefisso assegnato.

Per configurare i pool di indirizzi IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Configurazione LAN IPv6**.

PASSAGGIO 2 Nella **Tabella pool indirizzi IPv6**, fare clic su **Aggiungi riga**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo iniziale	Immettere l'indirizzo IPv6 iniziale del pool.
Indirizzo finale	Immettere l'indirizzo IPv6 finale del pool.
Lunghezza prefisso IPv6	Immettere la lunghezza del prefisso. Questo campo determina il numero di bit iniziali comuni negli indirizzi di rete.

PASSAGGIO 4 Fare clic su **Salva**.

Per modificare le impostazioni di un pool, selezionare il pool e fare clic su **Modifica**. Per eliminare un pool selezionato, fare clic su **Elimina**. Fare clic su **Salva** per applicare le modifiche.

Configurazione del routing statico IPv6

È possibile configurare i percorsi statici per indirizzare i pacchetti alla rete di destinazione. Un percorso statico è un percorso predeterminato che un pacchetto deve percorrere per raggiungere un host o un rete specifica.

Alcuni ISP richiedono percorsi statici invece dei protocolli di routing dinamico per creare la tabella di routing. I percorsi statici non richiedono risorse della CPU per lo scambio di informazioni di routing con un router paritetico.

È inoltre possibile utilizzare i percorsi statici per raggiungere i router paritetici che non supportano i protocolli di routing dinamico. I percorsi statici possono essere utilizzati insieme a quelli dinamici. Fare però attenzione a non introdurre loop di routing nella rete.

Per creare un percorso statico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking**> **IPv6** >**Routing statico IPv6**.

PASSAGGIO 2 Nell'elenco dei percorsi statici, fare clic su **Aggiungi riga**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Nome	Immettere il nome del percorso.
Destinazione	Immettere l'indirizzo IPv6 dell'host o della rete di destinazione per il percorso.
Lunghezza prefisso	Immettere il numero di bit prefisso nell'indirizzo IPv6 che definisce la sottorete di destinazione.
Gateway	Immettere l'indirizzo IPv6 del gateway attraverso il quale è possibile raggiungere l'host o la rete di destinazione.
Interfaccia	Selezionare l'interfaccia per il percorso dal menu a discesa: **LAN**, **WAN** o **6to4**.
Costo	Immettere la priorità del percorso scegliendo un valore compreso tra 2 e 15. Se esistono più percorsi per la stessa destinazione, verrà utilizzato il percorso con il costo più basso.
Attivo	Selezionare questa opzione per attivare il percorso. Quando si aggiunge un percorso non attivo, questo viene elencato nella tabella dei percorsi, ma non viene utilizzato dall'unità RV110W. È possibile attivare il percorso successivamente. Questa funzionalità è utile se la rete di destinazione non era disponibile quando è stato aggiunto il percorso. Quando la rete diventa disponibile, è possibile attivare il percorso.

PASSAGGIO 4 Fare clic su **Salva**.

Per modificare le impostazioni di un percorso, selezionare il percorso e fare clic su **Modifica**. Per eliminare un percorso selezionato, fare clic su **Elimina**. Fare clic su **Salva** per applicare le modifiche.

Configurazione del routing (RIPng)

RIPng (RIP Next Generation) è un protocollo di routing basato sull'algoritmo del vettore di distanza (D-V). Il protocollo RIPng utilizza i pacchetti UDP per scambiare informazioni di routing attraverso la porta 521.

Il protocollo RIPng utilizza il numero di hop per misurare la distanza da una destinazione. Il numero di hop viene definito metrica o costo. Il numero di hop da un router ad una rete connessa direttamente è di 0. Il numero di hop tra due router connessi direttamente è 1. Se il numero di hop è maggiore o uguale a 16, la rete o l'host di destinazione non è raggiungibile.

L'aggiornamento di routing viene inviato ogni 30 secondi per impostazione predefinita. Se il router non riceve aggiornamenti di routing da un'unità adiacente dopo 180 secondi , i percorsi appresi dall'unità adiacente sono considerati non raggiungibili. Se dopo altri 240 secondi non si ricevono aggiornamenti di routing, il router rimuove questi percorsi dalla tabella di routing.

Sull'unità RV110W, il protocollo RIPng è disattivato per impostazione predefinita.

Per configurare il protocollo RIPng, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Routing (RIPng)**.

PASSAGGIO 2 Selezionare **Attiva**.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione del tunneling IPv6-to-IPv4

Il tunneling IPv6-to-IPv4 (tunneling 6-to-4) consente la trasmissione di pacchetti IPv6 su una rete IPv4. Il tunneling 6to4 viene solitamente utilizzato quando un sito o un utente finale desidera connettersi a Internet IPv6 utilizzando la rete IPv4 esistente.

Per configurare il tunneling 6to4, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Tunnel 6to4**.

PASSAGGIO 2 Selezionare **Attiva**.

PASSAGGIO 3 Fare clic su **Salva**.

Visualizzazione dello stato del tunnel IPv6

Per visualizzare lo stato del tunnel IPv6, selezionare **Networking** > **IPv6** > **Stato tunnel IPv6**.

Per visualizzare lo stato del tunnel IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Stato tunnel IPv6**.

PASSAGGIO 2 Fare clic su **Aggiorna** per visualizzare le informazioni più recenti.

In questa pagina vengono visualizzate informazioni relative alla configurazione automatica del tunnel tramite interfaccia WAN dedicata. Nella tabella vengono mostrati il nome del tunnel e l'indirizzo IPv6 creati sul dispositivo.

Configurazione dell'annuncio router

Il Router Advertisement Daemon (RADVD) sull'unità RV110W ascolta le sollecitazioni del router sulla LAN IPv6 e risponde con annunci del router come richiesto. Si tratta di una configurazione automatica IPv6 stateless e l'unità RV110W distribuisce prefissi IPv6 a tutti i nodi presenti sulla rete.

Per configurare RADVD, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Annuncio router**.

PASSAGGIO 2 Immettere le informazioni seguenti:

Stato RADVD	Selezionare **Attiva** per attivare RADVD.
Modalità annuncio	Selezionare una delle seguenti modalità: **Multicast non richiesto**: selezionare questa modalità per inviare annunci del router (RA) a tutte le interfacce che appartengono al gruppo multicast. **Solo Unicast**: selezionare questa modalità per includere solo gli annunci relativi a indirizzi IPv6 noti (gli RA vengono inviati all'interfaccia appartenente esclusivamente a indirizzi noti).
Intervallo annuncio	Se si seleziona **Multicast non richiesto** come modalità di annuncio, immettere l'intervallo di annuncio (4-1800). L'impostazione predefinita è **30**. L'intervallo di annuncio è un valore casuale tra l'intervallo di annuncio router minimo (MinRtrAdvInterval) e l'intervallo di annuncio router massimo (MaxRtrAdvInterval). MinRtrAdvInterval = 0,33 * MaxRtrAdvInterval
Flag RA	Selezionare **Gestito** per utilizzare il protocollo stateful/ gestito per la configurazione automatica degli indirizzi. Selezionare **Altro** per utilizzare il protocollo stateful/ gestito di un'altra configurazione automatica di informazioni non relative a indirizzi.
Preferenza router	Selezionare dal menu a discesa **basso**, **medio** o **alto**. L'impostazione predefinita è **medio**. La preferenza router fornisce una metrica di preferenza per i router predefiniti. I valori basso, medio e alto vengono segnalati nei bit inutilizzati dei messaggi RA. Questa estensione è compatibile all'indietro, sia per i router (impostazione del valore di preferenza router) che per gli host (interpretazione del valore di preferenza router). Questi valori sono ignorati dagli host che non implementano la preferenza router. Si tratta di una funzione è utile se nella LAN sono presenti altri dispositivi abilitati per RADVD.

MTU	Immettere le dimensioni MTU (0 o da 1280 a 1500). L'impostazione predefinita è **1500** byte. Il valore MTU indica la dimensione del pacchetto più grande che può essere inviato sulla rete. Il valore MTU viene utilizzato negli RA per garantire che tutti i nodi della rete utilizzino lo stesso valore MTU quando il valore MTU della LAN non è noto.
Durata router	Immettere il valore di durata del router, ovvero la durata, in secondi, dei messaggi di annuncio sul percorso. L'impostazione predefinita è **3600** secondi.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione dei prefissi annuncio

Per configurare i prefissi annuncio RADVD disponibili, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Prefissi annuncio**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Tipo di prefisso IPv6	Selezionare uno dei seguenti tipi dal menu a discesa: **6to4**: 6to4 è un sistema che consente la trasmissione di pacchetti IPv6 su una rete IPv4. Viene solitamente utilizzato quando un sito o un utente finale desidera connettersi a Internet IPv6 utilizzando la rete IPv4 esistente. **Globale/Locale**: un indirizzo IPv6 univoco localmente che può essere utilizzato su reti IPv6 private oppure un indirizzo Internet IPv6 univoco a livello globale.

ID SLA	Se si seleziona **6to4** come tipo di prefisso IPv6, immettere l'ID SLA (Site-Level Aggregation Identifier). L'ID SLA nel prefisso di indirizzo 6to4 viene impostato sull'ID dell'interfaccia sulla quale sono inviati gli annunci.
Prefisso IPv6	Se si seleziona **Globale/Locale** come tipo di prefisso IPv6, immettere il prefisso IPv6. Il prefisso IPv6 specifica l'indirizzo di rete IPv6.
Lunghezza prefisso IPv6	Se si seleziona **Globale/Locale** come tipo di prefisso IPv6, immettere la lunghezza del prefisso. La variabile di lunghezza del prefisso è un valore decimale che indica il numero di bit di ordine superiore adiacenti dell'indirizzo che costituiscono la porzione di rete dell'indirizzo.
Durata prefisso	Immettere la durata del prefisso, ovvero l'intervallo di tempo durante il quale il router che effettua la richiesta è autorizzato a utilizzare il prefisso.

PASSAGGIO 4 Fare clic su **Salva**.

3

Configurazione della rete wireless

In questo capitolo viene descritto come configurare la rete wireless dell'unità RV110W.

- **Sicurezza per reti wireless, pagina 58**
- **RV110W Reti wireless, pagina 61**
- **Configurazione delle impostazioni wireless, pagina 61**

Sicurezza per reti wireless

Le reti wireless sono convenienti e facili da installare, per questo motivo le piccole aziende e le famiglie dotate di accesso Internet ad alta velocità le stanno rapidamente adottando.

Ma poiché le reti wireless utilizzano le onde radio per l'invio delle informazioni, sono più vulnerabili agli attacchi di intrusi rispetto alle tradizionali reti cablate.

In questa sezione vengono fornite informazioni per aiutare a migliorare la protezione delle reti wireless dagli accessi non autorizzati.

- **Suggerimenti per la protezione delle reti wireless, pagina 59**
- **Linee guida generali per la sicurezza di rete, pagina 60**

Suggerimenti per la protezione delle reti wireless

Anche se non è possibile impedire fisicamente ad altri utenti di connettersi alla propria rete wireless, è possibile adottare le seguenti precauzioni per rendere la rete più sicura:

- Modificare il nome di rete wireless o il SSID predefinito.

  I dispositivi wireless sono dotati di un nome di rete wireless o SSID predefinito. Si tratta del nome della rete wireless e può essere costituito da un massimo di 32 caratteri.

  Per proteggere la rete, modificare il nome di rete predefinito con un nome univoco che permetta di distinguere la rete wireless da altre reti wireless circostanti.

  Quando si sceglie un nome, non utilizzare informazioni personali, come il codice fiscale, poiché queste informazioni potrebbero essere visibili a chiunque cerchi reti wireless.

- Modificare la password predefinita.

  Per modificare le impostazioni di prodotti wireless, come punti di accesso, router e gateway, viene chiesto di immettere una password. Questi dispositivi sono dotati di una password predefinita. La password predefinita è spesso **cisco**.

  Gli hacker conoscono questi valori predefiniti e possono provare ad utilizzarli per accedere al dispositivo wireless in questione e modificare le impostazioni della rete corrispondente. Per bloccare l'accesso non autorizzato, personalizzare la password del dispositivo selezionandone una più complessa.

- Attivare il filtro degli indirizzi MAC.

  I router e gateway Cisco offrono la possibilità di attivare il filtro degli indirizzi MAC. L'indirizzo MAC è una serie univoca di numeri e lettere assegnata a ciascun dispositivo di rete.

  Se il filtro degli indirizzi MAC è attivo, l'accesso alla rete wireless è consentito solo ai dispositivi wireless con indirizzi MAC specifici. Ad esempio, è possibile specificare l'indirizzo MAC di ogni computer della rete in modo che solo quei computer possono accedere alla rete wireless.

- Attivare la crittografia.

  La crittografia protegge i dati trasmessi su una rete wireless. WPA/WPA2 (Wi-Fi Protected Access) e WEP (Wired Equivalency Privacy) offrono diversi livelli di protezione per la comunicazione wireless. Attualmente, i dispositivi con certificazione Wi-Fi devono supportare WPA2, ma non hanno l'obbligo di supportare WEP.

  Una rete crittografata con WPA/WPA2 è più sicura di una rete crittografata con WEP, poiché WPA/WPA2 utilizza la crittografia con chiavi dinamiche.

  Per proteggere le informazioni durante la trasmissione sulle onde radio, attivare il livello massimo di crittografia supportato dalle proprie apparecchiature di rete.

  WEP è uno standard di crittografia meno recente e può essere l'unica opzione disponibile su alcuni dispositivi obsoleti che non supportano lo standard WPA.

- Tenere i router, i punti di accesso o i gateway distanti dalle pareti esterne e dalle finestre.
- Quando non sono in uso (ad esempio di notte o durante le vacanze), spegnere i router, i punti di accesso o i gateway.
- Utilizzare sempre frasi chiave con almeno otto caratteri di lunghezza. Combinare lettere e numeri per evitare l'utilizzo di parole standard che possono essere trovate in un dizionario.

Linee guida generali per la sicurezza di rete

La protezione della rete wireless non serve a nulla se la rete sottostante non è sicura. Cisco consiglia di adottare le seguenti precauzioni:

- Proteggere mediante password tutti computer della rete e i singoli file contenenti informazioni riservate.
- Modificare le password su base regolare.
- Installare software antivirus e software firewall personale.
- Disattivare la condivisione dei file (peer-to-peer) per impedire l'utilizzo della condivisione dei file da parte delle applicazioni senza autorizzazione.

RV110W Reti wireless

L'unità RV110W fornisce quattro reti wireless virtuali, ovvero quattro SSID (Service Set Identifier): ciscosb1, ciscosb2, ciscosb3, e ciscosb4. Si tratta dei nomi predefiniti o SSID per queste reti, tuttavia è possibile modificarli e sostituirli con nomi più significativi. In questa tabella sono riportate le impostazioni predefinite di queste reti:

Nome SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Attivato	Sì	No	No	No
Trasmissione SSID	Attivato	Disattivato	Disattivato	Disattivato
Modalità di protezione	Disattivato[1]	Disattivato	Disattivato	Disattivato
Filtro MAC	Disattivato	Disattivato	Disattivato	Disattivato
VLAN	1	1	1	1
Isolamento wireless con SSID	Disattivato	Disattivato	Disattivato	Disattivato
WMM	Attivato	Attivato	Attivato	Attivato
Pulsante hardware WPS	Attivato	Disattivato	Disattivato	Disattivato

1. Nell'Installazione guidata, selezionare **Protezione massima** o **Protezione elevata** per proteggere l'unità RV110W dall'accesso non autorizzato.

Configurazione delle impostazioni wireless

Il Device Manager consente di configurare i seguenti aspetti delle impostazioni wireless:

- **Configurazione delle impostazioni wireless di base, pagina 62**
- **Configurazione delle impostazioni wireless avanzate, pagina 70**
- **Configurazione di WDS, pagina 74**
- **Configurazione di WPS, pagina 75**

Configurazione delle impostazioni wireless di base

È possibile utilizzare la pagina **Impostazioni di base** (**Wireless** > **Impostazioni di base**) per configurare le impostazioni di base wireless.

Per configurare le impostazioni di base wireless, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Wireless** > **Impostazioni di base**.

PASSAGGIO 2 Nel campo **Radio**, selezionare la casella di controllo **Attiva** per attivare tutte le reti wireless.

Questo campo attiva la radio wireless vera e propria. Per impostazione predefinita è attivata una sola rete wireless, ciscosb1.

PASSAGGIO 3 Nel campo **Modalità rete wireless**, selezionare una delle opzioni seguenti dal menu
a discesa:

Combinazione B/G/N	Selezionare questa opzione se la rete è composta da dispositivi Wireless-N, Wireless-B e Wireless-G. Questa è l'impostazione predefinita (consigliata).
Solo B	Selezionare questa opzione se la rete è composta solo da dispositivi Wireless-B.
Solo G	Selezionare questa opzione se la rete è composta solo da dispositivi Wireless-G.
Solo N	Selezionare questa opzione se la rete è composta solo da dispositivi Wireless-N.
Combinazione B/G	Selezionare questa opzione se la rete è composta da dispositivi Wireless-B e Wireless-G.

PASSAGGIO 4 Nel campo **Selezione banda wireless**, selezionare la larghezza di banda della rete (**20MHz** o **20/40MHz**).

PASSAGGIO 5 Nel campo **Canale wireless**, selezionare il canale wireless dal menu a discesa.

PASSAGGIO 6 Nel campo **VLAN gestione punto di accesso**, selezionare VLAN 1 se si utilizzano le impostazioni predefinite.

Se si creano VLAN aggiuntive, selezionare un valore corrispondente alla VLAN configurata sugli altri switch della rete. Questo viene fatto per motivi di sicurezza. Potrebbe essere necessario modificare la VLAN di gestione per limitare l'accesso al Device Manager dell'unità RV110W.

PASSAGGIO 7 (Opzionale) Nel campo **U-APSD (risparmio energia WMM)**, selezionare la casella di controllo **Attiva** per attivare la funzione U-APSD (Unscheduled Automatic Power Save Delivery), anche denominata risparmio energia WMM, che permette alla radio di conservare energia.

U-APSD è un sistema di risparmio energetico ottimizzato per applicazioni in tempo reale, come VoIP, con trasferimento di dati full-duplex su WLAN. Con la classificazione del traffico IP in uscita come dati *Voce*, questi tipi di applicazioni possono aumentare la durata della batteria di circa il 25% riducendo al minimo i ritardi di trasmissione.

PASSAGGIO 8 (Opzionale) Configurare le impostazioni delle quattro reti wireless (vedere la sezione **Configurazione delle impostazioni della rete wireless, pagina 63**).

PASSAGGIO 9 Fare clic su **Salva**.

Configurazione delle impostazioni della rete wireless

Nella **Tabella wireless** nella pagina **Impostazioni di base** (**Wireless** > **Impostazioni di base**) sono elencate le impostazioni delle quattro reti wireless supportate sull'unità RV110W.

Per configurare le impostazioni della rete wireless, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare la casella di controllo delle reti da configurare.

PASSAGGIO 2 Fare clic sul pulsante **Modifica**.

PASSAGGIO 3 Configurare le impostazioni seguenti:

Attiva SSID	Selezionare questa casella di controllo per attivare la rete.
Nome SSID	Immettere il nome della rete.
Trasmissione SSID	Selezionare questa casella di controllo per attivare la trasmissione di SSID.
VLAN	Selezionare la VLAN associata alla rete.

Isolamento wireless con SSID	Selezionare questa casella di controllo per attivare l'isolamento wireless all'interno della rete SSID.
WMM (Wi-Fi Multimedia)	Selezionare questa casella di controllo per attivare WMM.
Pulsante hardware WPS	Selezionare questa casella di controllo per mappare a questa rete il pulsante WPS dell'unità RV110W sul pannello frontale.

PASSAGGIO 4 Fare clic su **Salva**.

Per configurare la modalità di protezione, vedere la sezione **Configurazione della modalità di protezione., pagina 64**. Per configurare il filtro MAC, vedere la sezione **Configurazione del filtro MAC, pagina 68**. Per configurare l'opzione Ora accesso, vedere la sezione **Configurazione dell'opzione Ora accesso, pagina 69**.

Configurazione della modalità di protezione.

È possibile configurare una delle seguenti modalità di protezione per le reti wireless:

- **Configurazione WEP, pagina 64**
- **Configurazione di WPA-Personal, WPA2-Personal e Combinazione WPA2-Personal, pagina 66**
- **Configurazione di WPA-Enterprise, WPA2-Enterprise e Combinazione WPA2-Enterprise, pagina 67**

Configurazione WEP

La modalità di protezione WEP offre una protezione debole, con un metodo di crittografia di base non sicuro come WPA. La protezione WEP potrebbe essere necessaria nel caso in cui i dispositivi di rete non supportino WPA.

NOTA Se non è necessario utilizzare la protezione WEP, si raccomanda l'utilizzo della protezione WPA2.

Per configurare la modalità di protezione WEP, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella di controllo della rete da configurare.

PASSAGGIO 2 Fare clic su **Modifica modalità protezione**.

Verrà visualizzata la pagina **Impostazioni di protezione**.

PASSAGGIO 3 Nel campo **Seleziona SSID**, selezionare l'identificatore SSID per il quale si desidera configurare le impostazioni di protezione.

PASSAGGIO 4 Dal menu **Modalità di protezione**, scegliere **WEP**.

PASSAGGIO 5 Nel campo **Tipo di autenticazione**, selezionare una delle seguenti opzioni:

- **Sistema aperto**: questa è l'opzione predefinita.
- **Chiave condivisa**: selezionare questa opzione se consigliato dall'amministratore di rete. Se non si è sicuri, selezionare l'opzione predefinita.

In entrambi i casi, il client wireless deve fornire la chiave condivisa corretta (password) per accedere alla rete wireless.

PASSAGGIO 6 Nel campo **Crittografia**, selezionare il tipo di crittografia:

- **10/64 bit (10 cifre esadecimali):**fornisce una chiave a 40 bit.
- **26/128 bit(26 cifre esadecimali)**: fornisce una chiave a 104 bit, che offre una migliore crittografia rendendo la chiave più difficile da craccare. Si consiglia la crittografia a 128 bit.

PASSAGGIO 7 (Opzionale) Nel campo **Frase chiave** immettere una frase alfanumerica (per garantire una sicurezza ottimale deve essere più lunga di otto caratteri) e fare clic su **Genera chiave** per generare quattro chiavi WEP univoche nei campi chiave WEP sottostanti.

Se si desidera utilizzare una chiave personale, immetterla direttamente nel campo **Chiave 1** (opzione consigliata). La lunghezza della chiave deve essere di 5 caratteri ASCII (o 10 caratteri esadecimali) per WEP a 64 bit e 13 caratteri ASCII (o 26 caratteri esadecimali) per WEP a 128 bit. I caratteri esadecimali validi sono quelli compresi tra 0 e 9 e tra A e F.

PASSAGGIO 8 Nel campo **Chiave TX**, selezionare la chiave da utilizzare come chiave condivisa che verrà utilizzata dai dispositivi per accedere alla rete wireless.

PASSAGGIO 9 Fare clic su **Salva** per salvare le impostazioni.

PASSAGGIO 10 Fare clic su **Indietro** per tornare alla pagina **Impostazioni di base**.

Configurazione di WPA-Personal, WPA2-Personal e Combinazione WPA2-Personal

Le modalità di protezione WPA Personal, WPA2 Personal e Combinazione WPA2-Personal offrono una protezione potente in sostituzione di WEP.

- **WPA-Personal**: WPA fa parte dello standard di protezione wireless (802.11i) standardizzato dalla Wi-Fi Alliance e progettato come misura intermedia per la sostituzione di WEP durante la preparazione dello standard 802.11i. WPA-Personal supporta il protocollo TKIP (Temporal Key Integrity Protocol) e la crittografia AES (Advanced Encryption Standard).
- **WPA2-Personal**: (Opzione consigliata) WPA2 è l'implementazione dello standard di protezione specificato nello standard finale 802.11i. WPA2 supporta la crittografia AES e questa opzione utilizza la chiave precondivisa PSK per l'autenticazione.
- **Combinazione WPA2-Personal**: consente ad entrambi i client WPA e WPA2 di connettersi simultaneamente tramite l'autenticazione PSK.

L'autenticazione personale corrisponde alla chiave PSK, ovvero una frase chiave alfanumerica condivisa con il peer wireless.

Per configurare la modalità di protezione WPA Personal, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella di controllo della rete da configurare.

PASSAGGIO 2 Fare clic su **Modifica modalità protezione**.

Verrà visualizzata la pagina **Impostazioni di protezione**.

PASSAGGIO 3 Nel campo **Seleziona SSID**, selezionare l'identificatore SSID per il quale si desidera configurare le impostazioni di protezione.

PASSAGGIO 4 Dal menu **Modalità di protezione**, selezionare una delle tre opzioni WPA Personal.

PASSAGGIO 5 (Solo WPA Personal) Nel campo **Crittografia**, selezionare una delle seguenti opzioni:

- **TKIP/AES**: selezionare **TKIP/AES** per garantire la compatibilità con i dispositivi wireless meno recenti che non supportano AES.
- **AES**: questa è l'opzione più sicura.

PASSAGGIO 6 Nel campo **Segreto condiviso**, immettere una frase alfanumerica (8-63 caratteri ASCII o 64 caratteri esadecimali).

PASSAGGIO 7 Nel campo **Rinnovo chiave**, immettere l'intervallo temporale (600-7200 secondi) tra i rinnovi della chiave.

Il valore predefinito è 3600.

PASSAGGIO 8 Fare clic su **Salva** per salvare le impostazioni.

PASSAGGIO 9 Fare clic su **Indietro** per tornare alla pagina **Impostazioni di base**.

Configurazione di WPA-Enterprise, WPA2-Enterprise e Combinazione WPA2-Enterprise

Le modalità di protezione WPA-Enterprise, WPA2-Enterprise e Combinazione WPA2-Enterprise consentono di utilizzare l'autenticazione server RADIUS.

- **WPA-Enterprise**: consente l'utilizzo di WPA con l'autenticazione server RADIUS.
- **WPA2-Enterprise**: consente l'utilizzo di WPA2 con l'autenticazione server RADIUS.
- **Combinazione WPA2-Enteprise**: consente ad entrambi i client WPA e WPA2 di connettersi simultaneamente tramite l'autenticazione RADIUS.

Per configurare la modalità di protezione WPA Enteprise, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella di controllo della rete da configurare.

PASSAGGIO 2 Fare clic su **Modifica modalità protezione**.

PASSAGGIO 3 Nel campo **Seleziona SSID**, selezionare l'identificatore SSID per il quale si desidera configurare le impostazioni di protezione.

PASSAGGIO 4 Dal menu **Modalità di protezione**, selezionare una delle tre opzioni WPA Enteprise.

PASSAGGIO 5 (Solo WPA Enterprise) Nel campo **Crittografia**, selezionare una delle seguenti opzioni:

- **TKIP/AES**: selezionare **TKIP/AES** per garantire la compatibilità con i dispositivi wireless meno recenti che non supportano AES.
- **AES**: questa è l'opzione più sicura.

PASSAGGIO 6 Nel campo **Server RADIUS**, immettere l'indirizzo IP del server RADIUS.

PASSAGGIO 7 Nel campo **Porta RADIUS**, immettere la porta utilizzata per accedere al server RADIUS.

PASSAGGIO 8 Nel campo **Chiave condivisa**, immettere una frase alfanumerica (8-63 caratteri ASCII o 64 caratteri esadecimali).

PASSAGGIO 9 Nel campo **Rinnovo chiave**, immettere l'intervallo temporale (600-7200 secondi) tra i rinnovi della chiave. Il valore predefinito è 3600.

PASSAGGIO 10 Fare clic su **Salva** per salvare le impostazioni.

PASSAGGIO 11 Fare clic su **Indietro** per tornare alla pagina **Impostazioni di base**.

Configurazione del filtro MAC

È possibile utilizzare il filtro MAC per consentire o negare l'accesso alla rete wireless sulla base dell'indirizzo MAC (hardware) del dispositivo richiedente.

Ad esempio, è possibile immettere gli indirizzi MAC di una serie di computer e consentire solo a quei computer di accedere alla rete.

È possibile configurare il filtro MAC per ciascuna rete o SSID.

Per configurare il filtro MAC, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella di controllo della rete da configurare.

PASSAGGIO 2 Fare clic su **Modifica filtro MAC**.

Viene visualizzata la pagina del **Filtro MAC wireless**.

PASSAGGIO 3 Nel campo **Modifica filtro MAC**, selezionare la casella di controllo **Attiva** per attivare il filtro MAC per questo SSID.

PASSAGGIO 4 Nel campo **Controllo connessione**, selezionare il tipo di accesso alla rete wireless:

- **Impedire l'accesso alla rete wireless ai PC elencati di seguito**: selezionare questa opzione per impedire che i dispositivi con gli indirizzi MAC elencati nella **Tabella indirizzi MAC** accedano alla rete wireless. Questa è l'opzione predefinita.
- **Consenti**: selezionare questa opzione per consentire ai dispositivi con gli indirizzi MAC elencati nella **Tabella indirizzi MAC** di accedere alla rete wireless.

PASSAGGIO 5 Per mostrare i computer e gli altri dispositivi della rete wireless, fare clic **Mostra elenco client**.

PASSAGGIO 6 Nel campo **Salva nell'elenco filtri indirizzo MAC** selezionare la casella di controllo per inserire il dispositivo nell'elenco di dispositivi da aggiungere alla **Tabella indirizzi MAC**.

PASSAGGIO 7 Fare clic su **Aggiungi a MAC** per aggiungere i dispositivi selezionati della **Tabella elenco client** alla **Tabella indirizzi MAC**.

PASSAGGIO 8 Fare clic su **Salva** per salvare le impostazioni.

PASSAGGIO 9 Fare clic su **Indietro** per tornare alla pagina **Impostazioni di base**.

Configurazione dell'opzione Ora accesso

Per proteggere ulteriormente la rete, è possibile limitare l'accesso specificando gli orari di accesso.

Per configurare l'opzione Ora accesso, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella di controllo della rete da configurare.

PASSAGGIO 2 Fare clic su **Ora accesso**.

Viene visualizzata la pagina **Ora accesso**.

PASSAGGIO 3 Nel campo **Tempo attività**, selezionare la casella di controllo **Attiva** per attivare l'opzione Ora accesso.

PASSAGGIO 4 Nei campi **Ora di inizio** e **Ora di fine**, specificare gli orari del giorno durante i quali è possibile accedere alla rete.

Configurazione delle impostazioni wireless avanzate

ATTENZIONE Le impostazioni wireless avanzate devono essere regolate solo da un amministratore esperto; se le impostazioni non sono corrette, si potrebbe notare una riduzione delle prestazioni wireless.

Per configurare le impostazioni wireless avanzate, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Wireless** > **Impostazioni avanzate**.

Viene visualizzata la pagina Impostazioni avanzate.

PASSAGGIO 2 Configurare i campi da modificare, quindi fare clic su **Salva**:

Burst frame	Attivare questa opzione per incrementare le prestazioni delle reti wireless, a seconda del produttore dei prodotti wireless. Se non si è sicuri di come utilizzare questa opzione, mantenere l'impostazione predefinita (attivato).
Nessuna conferma WMM	Fare clic per attivare questa funzionalità. L'attivazione dell'opzione Nessuna conferma WMM consente di ottenere un throughput più efficiente, ma frequenze di errore maggiori in un ambiente di frequenza radio (RF) rumoroso. Questa opzione è disattivata per impostazione predefinita.

Velocità di base	L'impostazione della velocità di base non è la velocità di trasmissione, ma una serie di velocità di trasmissione sulla piattaforma Services Ready. L'unità RV110W dichiara la propria velocità di base agli altri dispositivi wireless della rete affinché conoscano le velocità di trasmissione utilizzate. La piattaforma Services Ready dichiara inoltre che verrà selezionata automaticamente la velocità di trasmissione più adatta. L'impostazione predefinita è Predefinito, quando l'unità RV110W può trasmettere a tutte le velocità standard wireless (1-2 Mbps, 5.5 Mbps, 11 Mbps, 18 Mbps, 24 Mbps e così via). Oltre alle velocità di trasmissione B e G, l'unità RV110W supporta le velocità N. Le altre opzioni disponibili sono 1-2 Mbps, da utilizzare con dispositivi con tecnologia wireless meno recente, e Tutte, quando l'unità RV110W può trasmettere a tutte le velocità wireless. La velocità di trasmissione di base non corrisponde alla velocità di trasmissione dei dati effettiva. Per specificare la velocità di trasmissione dei dati dell'unità RV110W, configurare l'impostazione Velocità di trasmissione.
Velocità di trasmissione	Impostare la velocità di trasmissione dei dati in base alla velocità della rete wireless. È possibile scegliere tra varie velocità di trasmissione oppure selezionare l'opzione Auto affinché l'unità RV110W utilizzi automaticamente la massima velocità di trasmissione possibile e attivare la funzione di fallback automatico. Il fallback automatico negozia la migliore velocità di connessione possibile tra l'unità RV110W e un client wireless. L'impostazione predefinita è Auto.

Velocità di trasmissione N	La velocità di trasmissione dei dati deve essere impostata in base alla velocità della rete wireless N. È possibile scegliere tra varie velocità di trasmissione oppure selezionare l'opzione Auto affinché l'unità RV110W utilizzi automaticamente la massima velocità di trasmissione possibile e attivare la funzione di fallback automatico. Il fallback automatico negozia la migliore velocità di connessione possibile tra l'unità RV110W e un client wireless. L'impostazione predefinita è Auto.
Modalità di protezione CTS	L'unità RV110W utilizza automaticamente la modalità di protezione CTS (Clear-To-Send) nel caso si verifichino problemi gravi relativamente ai prodotti Wireless-G e Wireless-N che impediscono la comunicazione con l'unità RV110W in ambienti in cui è presente traffico 802.11b pesante. Questa funzione migliora la capacità dell'unità RV110W di ricezione delle trasmissioni Wireless-G e Wireless-N, ma ne compromette significativamente le prestazioni. L'impostazione predefinita è Auto.
Intervallo beacon	Questo valore indica l'intervallo di frequenza del beacon. Un beacon è un pacchetto trasmesso dall'unità RV110W per sincronizzare la rete wireless. Immettere un valore compreso tra 40 e 3.500 millisecondi. Il valore predefinito è 100.

Intervallo DTIM	Questo valore, compreso tra 1 e 255, indica l'intervallo di invio dei messaggi DTIM (Delivery Traffic Indication Message). Il campo DTIM viene utilizzato per eseguire il conto alla rovescia per indicare ai client la disponibilità della successiva finestra di ascolto di messaggi broadcast e multicast. Quando nel buffer dell'unità RV110W sono presenti messaggi di trasmissione o multicast per i client associati, invia un messaggio DTIM con un valore di intervallo DTIM. In questo modo i client ricevono il beacon e si preparano a ricevere i messaggi broadcast e multicast. Il valore predefinito è 1.
Soglia di frammentazione	Questo valore indica la dimensione massima di un pacchetto prima che i dati vengano suddivisi in più pacchetti. Se si verifica un elevato numero di errori relativi ai pacchetti, è consigliabile incrementare leggermente il valore della soglia di frammentazione. Un valore della soglia di frammentazione troppo basso potrebbe infatti compromettere le prestazioni della rete. Si consiglia di non apportare riduzioni al valore predefinito che non siano di lieve entità. Nella maggior parte dei casi è opportuno non modificare il valore predefinito di 2346.
Soglia RTS	Se si riscontra un flusso di dati inconsistente, immettere solo riduzioni di lieve entità. Si consiglia il valore predefinito di 2347. Se la dimensione di un pacchetto di rete è inferiore alla soglia RTS impostata, il meccanismo RTS/CTS non viene attivato. La piattaforma Services Ready invia frame RTS (Request-To-Send) a una data stazione ricevente e negozia l'invio di un frame di dati. Dopo avere ricevuto un pacchetto RTS, la stazione wireless risponde con un frame CTS (Clear-To-Send) per autorizzare l'avvio della trasmissione.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione di WDS

Un WDS (Wireless Distribution System) è un sistema che consente l'interconnessione wireless dei punti di accesso di una rete. Consente l'espansione di una rete wireless tramite punti di accesso multipli senza la necessità di fornire una backbone cablata per collegarli.

Per stabilire un collegamento WDS, l'unità RV110W e altri peer WDS remoti devono essere configurati sulla stessa modalità di rete wireless, canale wireless, selezione di banda wireless e tipo di crittografia (nessuno e WEP).

Per configurare un WDS, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Wireless** > **WDS**.

PASSAGGIO 2 Selezionare la casella di controllo **Consenti ripetizione del segnale wireless da un ripetitore** per attivare il WDS.

PASSAGGIO 3 Per immettere manualmente l'indirizzo MAC di un ripetitore, fare clic sul pulsante di opzione **Manuale**.

PASSAGGIO 4 (Opzionale) Fare clic sul pulsante **Mostra analisi sito**.

Viene visualizzata la **Tabella reti disponibili** con l'elenco dei punti di accesso della rete wireless disponibili.

a. (Opzionale) Fare clic sul pulsante **Aggiorna** per aggiornare le voci della tabella.

b. Nella **Tabella reti disponibili**, selezionare fino a tre punti di accesso da utilizzare come ripetitori.

c. Per aggiungere gli indirizzi MAC dei punti di accesso selezionati ai campi MAC sotto la tabella, fare clic su **Connetti**.

PASSAGGIO 5 Se è stata selezionata l'opzione **Manuale**, immettere gli indirizzi MAC dei punti di accesso (fino a tre) da utilizzare come ripetitori nei campi **MAC 1**, **MAC 2**, **MAC 3**.

PASSAGGIO 6 Fare clic su **Salva**.

Configurazione di WPS

È possibile configurare il WPS sull'unità RV110W per consentire ai dispositivi WPS di connettersi più facilmente alla rete wireless.

Per configurare WPS sui dispositivi client, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Wireless** > **WPS**. Viene visualizzata la pagina Impostazioni Wi-Fi protetta

PASSAGGIO 2 Dal menu a discesa **SSID**, selezionare la rete wireless per la quale attivare il WPS.

PASSAGGIO 3 Nel campo **WPS**, selezionare la casella di controllo Attiva per attivare il WPS. Per disattivare il WPS, deselezionare la casella di controllo.

PASSAGGIO 4 Configurare il WPS sui dispositivi client in uno dei seguenti tre modi:

- **WPS - Metodo 1, pagina 75**
- **WPS - Metodo 2, pagina 76**
- **WPS - Metodo 3, pagina 76**

Al termine della configurazione del WPS, nella parte inferiore della pagina **WPS** appaiono le seguenti informazioni: Stato impostazione Wi-Fi protetta, Nome rete (SSID), Protezione, Crittografia e Frase chiave.

WPS - Metodo 1

Utilizzare questo metodo se il dispositivo client è dotato di pulsante WPS.

PASSAGGIO 1 Fare clic o premere il tasto WPS sul dispositivo client.

PASSAGGIO 2 Nella pagina **WPS**, fare clic sul pulsante **WPS**.

Al termine della configurazione WPS, viene visualizzata una finestra di dialogo.

PASSAGGIO 3 Fare clic su **OK**.

Fare riferimento al dispositivo client o alla relativa documentazione per ulteriori istruzioni.

WPS - Metodo 2

Utilizzare questo metodo se il dispositivo client è dotato di numero PIN WPS

PASSAGGIO 1 Nella pagina **WPS**, immettere il numero PIN nel campo appropriato.

PASSAGGIO 2 Fare clic su **Registra**.

PASSAGGIO 3 Al termine della configurazione, fare clic su **OK**.

Fare riferimento al dispositivo client o alla relativa documentazione per ulteriori istruzioni.

WPS - Metodo 3

Se il dispositivo client richiede un numero PIN dal router, utilizzare il numero elencato alla voce 3 della pagina **WPS**.

4

Configurazione del firewall

In questo capitolo viene spiegato come configurare le funzionalità firewall dell'unità RV110W.

- **RV110W - Funzionalità firewall, pagina 79**
- **Configurazione delle impostazioni firewall di base, pagina 81**
- **Gestione delle pianificazioni del firewall, pagina 84**
- **Configurazione della gestione servizi, pagina 85**
- **Configurazione delle regole di accesso, pagina 86**
- **Creazione di un criterio di accesso a Internet, pagina 90**
- **Configurazione del reindirizzamento delle porte, pagina 92**

RV110W - Funzionalità firewall

La rete può essere protetta creando e applicando regole che l'unità RV110W utilizza per bloccare e consentire in maniera selettiva il traffico Internet in ingresso e in uscita. Successivamente si specificano i dispositivi a cui vengono applicate le regole e come applicarle. Per questa operazione è necessario definire quanto segue:

- I servizi o tipi di traffico, ad esempio navigazione Internet, VoIP, altri servizi standard e servizi personalizzati definiti, che il router deve consentire o bloccare.
- La direzione del traffico specificando l'origine e la destinazione del traffico stesso; a tal fine si specifica la "zona di origine" (LAN/WAN/DMZ) e la "zona di destinazione" (LAN/WAN/DMZ).
- Le pianificazioni in base alle quali il router deve applicare le regole.
- Le parole chiave, nel nome di dominio o nell'URL di una pagina Web, che il router deve bloccare o consentire.

- Le regole per consentire o bloccare il traffico Internet in ingresso e uscita per servizi specifici in base ad una determinata pianificazione.
- Gli indirizzi MAC dei dispositivi il cui accesso in ingresso alla rete deve essere bloccato dal router.
- I trigger di porta che segnalano al router di consentire o bloccare l'accesso a servizi specifici come definiti dal numero di porta.
- I rapporti e gli avvisi che il router deve inviare.

Ad esempio, è possibile stabilire dei criteri di accesso limitato basati sull'ora del giorno, sugli indirizzi Web e su parole chiave Web. È possibile bloccare l'accesso a Internet da parte di applicazioni e servizi della LAN, come chat room o giochi. È possibile bloccare l'accesso solo ad alcuni gruppi di PC della rete da parte della WAN o della rete DMZ pubblica.

Le regole per il traffico in ingresso (da WAN a LAN/DMZ) limitano l'accesso al traffico in ingresso della rete, consentendo in modo selettivo solo ad alcuni utenti esterni specifici di accedere a risorse locali specifiche. Per impostazione predefinita ogni accesso alla LAN sicura dal lato WAN non sicuro viene bloccato, ad eccezione delle risposte alle richieste provenienti dalla LAN o da DMZ. Per consentire ai dispositivi esterni l'accesso ai servizi della LAN sicura, è necessario creare una regola del firewall per ciascun servizio.

Se si desidera consentire il traffico in ingresso, l'indirizzo IP della porta WAN del router deve essere reso pubblico. Questa operazione è denominata "esposizione dell'host". Il metodo di esposizione dell'host dipende dalla configurazione delle porte WAN; per l'unità RV110W è possibile utilizzare l'indirizzo IP se alla porta WAN è assegnato un indirizzo statico oppure è possibile utilizzare un nome DDNS (DNS dinamico) se l'indirizzo WAN è dinamico.

Le regole per il traffico in uscita (da LAN/DMZ a WAN) limitano il traffico in uscita dalla rete, consentendo in modo selettivo solo ad alcuni utenti locali specifici di accedere a risorse esterne specifiche. La regola predefinita per il traffico in uscita consente l'accesso dalle zone sicure (LAN) alla rete DMZ pubblica o alla WAN non sicura. Per impedire agli host sulla LAN sicura di accedere ai servizi esterni (WAN non sicura) è necessario creare una regola firewall per ciascun servizio.

Configurazione delle impostazioni firewall di base

Per configurare le impostazioni firewall di base, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Impostazioni di base**.

PASSAGGIO 2 Configurare le seguenti impostazioni firewall:

Firewall	Selezionare la casella di controllo **Attiva** per attivare le impostazioni firewall.
Protezione DoS	Selezionare la casella di controllo **Attiva** per attivare la protezione Denial of Service.
Blocco richiesta WAN	Blocca le richieste ping inviate dalla WAN all'unità RV110W.
Accesso Web	Selezionare il tipo di accesso Web che può essere utilizzato per collegarsi al firewall: HTTP o HTTPS (secure HTTP).
Gestione remota	Vedere la sezione **Configurazione della gestione remota, pagina 83**.
Multicast Passthrough (IGMP Proxy)	Selezionare la casella di controllo **Attiva** per attivare il passthrough multicast.
UPnP	Vedere la sezione **Configurazione di Universal Plug and Play, pagina 84**.
Blocca Java	Selezionare questa opzione per bloccare l'esecuzione degli applet Java. Gli applet Java sono piccoli programmi integrati nelle pagine Web che attivano la funzionalità dinamica della pagina. Un applet pericoloso può essere utilizzato per compromettere o infettare i computer. L'attivazione di questa impostazione blocca il download degli applet Java. Fare clic su **Auto** per bloccare automaticamente Java oppure fare clic su **Manuale** e immettere una porta specifica sulla quale bloccare Java.

Blocca cookie	Selezionare questa opzione per bloccare i cookie. I cookie vengono utilizzati per memorizzare informazioni relative alla sessione da parte di siti Web che solitamente richiedono l'accesso. Tuttavia, diversi siti Web utilizzano i cookie per tenere traccia delle informazioni e delle abitudini di navigazione di un utente. L'attivazione di questa opzione impedisce ai siti Web di creare cookie. **ATTENZIONE** Molti siti Web richiedono l'accettazione di cookie per consentire un accesso regolare al sito. Il blocco dei cookie può provocare un funzionamento non corretto dei siti Web. Fare clic su **Auto** per bloccare automaticamente i cookie oppure fare clic su **Manuale** e immettere una porta specifica sulla quale bloccare i cookie.
Blocca ActiveX	Selezionare questa opzione per bloccare i contenuti ActiveX. In modo analogo agli applet Java, i controlli ActiveX vengono installati su un computer Windows quando si esegue Internet Explorer. Un controllo ActiveX pericoloso può essere utilizzato per compromettere o infettare i computer. L'attivazione di questa impostazione blocca il download degli applet ActiveX. Fare clic su **Auto** per bloccare automaticamente ActiveX oppure fare clic su **Manuale** e immettere una porta specifica sulla quale bloccare ActiveX.
Blocca proxy	Selezionare questa opzione per bloccare i server proxy. Un server proxy (o semplicemente proxy) consente ai computer di connettersi ad altri computer tramite il proxy aggirando in questo modo alcune regole del firewall. Ad esempio, se le connessioni ad indirizzi IP specifici sono bloccate da una regola del firewall, le richieste possono essere indirizzate tramite un proxy che non è bloccato dalla regola, rendendo in questo modo la limitazione inefficace. L'attivazione di questa funzionalità blocca i server proxy. Fare clic su **Auto** per bloccare automaticamente i server proxy oppure fare clic su **Manuale** e immettere una porta specifica sulla quale bloccare i server proxy.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione della gestione remota

È possibile attivare la gestione remota per consentire l'accesso all'unità RV110W da una rete WAN remota.

Per configurare la gestione remota, definire le impostazioni seguenti nella pagina **Impostazioni di base**:

Gestione remota	Selezionare la casella di controllo **Attiva** per attivare la gestione remota.
Accesso remoto	Selezionare il tipo di accesso Web che può essere utilizzato per collegarsi al firewall: HTTP o HTTPS (secure HTTP).
Aggiornamento remoto	Per attivare gli aggiornamenti remoti dell'unità RV110W, selezionare la casella di controllo **Attiva**.
Indirizzo IP remoto consentito	Fare clic sul pulsante di scelta **Qualsiasi indirizzo IP** per consentire la gestione remota da qualsiasi indirizzo IP oppure immettere un indirizzo IP specifico nel campo dell'indirizzo.
Porta di gestione remota	Immettere la porta sulla quale è consentito l'accesso remoto.

ATTENZIONE Quando la gestione remota è attivata, il router è accessibile da chiunque conosca il suo indirizzo IP. Poiché un utente WAN malintenzionato può riconfigurare l'unità RV110W e utilizzarla in modo non corretto, si consiglia vivamente di modificare la password dell'amministratore e qualsiasi eventuale password ospite prima di continuare.

Configurazione di Universal Plug and Play

Universal Plug and Play (UPnP) consente il rilevamento automatico dei dispositivi che possono comunicare con l'unità RV110W.

Per configurare UPnP, definire le impostazioni seguenti nella pagina **Impostazioni di base**:

UPnP	Selezionare la casella di controllo **Attiva** per attivare UPnP.
Consenti agli utenti di configurare	Selezionare questa casella di controllo per consentire l'impostazione di regole di mappatura porta UPnP agli utenti che dispongono di computer con supporto UPnP o altri dispositivi con abilitazione UPnP. Se questa opzione è disattivata, l'unità RV110W non consente all'applicazione di aggiungere la regola di reindirizzamento.
Consenti agli utenti di disabilitare l'accesso Internet	Selezionare questa casella di controllo per consentire agli utenti di disattivare l'accesso a Internet.

Gestione delle pianificazioni del firewall

È possibile creare pianificazioni per applicare le regole del firewall in giorni oppure in orari specifici.

Per creare una pianificazione, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Gestione pianificazione**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Nel campo **Nome**, immettere un nome univoco per la pianificazione.

Questo nome viene visualizzato nell'elenco **Seleziona programma** nella pagina Configurazione regola firewall (vedere la sezione **Configurazione delle regole di accesso, pagina 86**).

PASSAGGIO 4 Nella sezione **Giorni pianificati**, selezionare se si desidera applicare la pianificazione a tutti i giorni o solo a giorni specifici. Se si seleziona **Giorni specifici**, selezionare la casella di controllo vicino ai giorni che si desidera includere nella pianificazione.

PASSAGGIO 5 In **Ora del giorno pianificata**, selezionare l'ora del giorno in cui applicare la pianificazione. È possibile scegliere **Tutti gli orari** oppure **Orari specifici**. Se si seleziona **Orari specifici**, immettere gli orari di inizio e fine.

PASSAGGIO 6 Fare clic su **Salva**.

Configurazione della gestione servizi

Quando si crea una regola per il firewall è possibile specificare un servizio che viene controllato dalla regola. È possibile selezionare i tipi di servizio più comuni, oltre a poter creare servizi personalizzati.

La pagina della **Gestione servizio** consente di creare servizi personalizzati per i quali definire regole del firewall. Il nuovo servizio definito appare nell'elenco dei **servizi personalizzati disponibili**.

Per creare un servizio personalizzato, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Gestione servizio**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Nel campo **Nome servizio**, immettere in nome del servizio per l'identificazione e la gestione.

PASSAGGIO 4 Nel campo **Protocollo**, selezionare dal menu a discesa il protocollo Layer 4 utilizzato dal servizio:

- **TCP**
- **UDP**
- **TCP e UDP**
- **ICMP**

PASSAGGIO 5 Nel campo **Porta iniziale**, immettere la prima porta TCP o UDP dell'intervallo utilizzato dal servizio.

PASSAGGIO 6 Nel campo **Porta finale**, immettere l'ultima porta TCP o UDP dell'intervallo utilizzato dal servizio.

PASSAGGIO 7 Fare clic su **Salva**.

Per modificare una voce, selezionarla e fare clic su **Modifica**. Effettuare le modifiche quindi fare clic su **Salva**.

Configurazione delle regole di accesso

- **Configurazione del criterio predefinito in uscita, pagina 86**
- **Aggiunta di regole di accesso, pagina 86**

Configurazione del criterio predefinito in uscita

La pagina **Regole di accesso** consente la configurazione dei criteri predefiniti di uscita per il traffico indirizzato dalla rete sicura (LAN) alla rete non sicura (WAN dedicata/opzionale).

Il criterio predefinito per il traffico in ingresso proveniente dalla zona non sicura alla zona sicura è Blocca sempre e non può essere modificato.

Per configurare il criterio predefinito in uscita, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Regole di accesso**.

PASSAGGIO 2 Selezionare **Consenti** o **Nega**.

Nota: per configurare un firewall IPv6 accertarsi che sull'unità RV110W sia abilitato il supporto per IPv6. Vedere la sezione **Configurazione di IPv6, pagina 46**.

PASSAGGIO 3 Fare clic su **Salva**.

Aggiunta di regole di accesso

Tutte le regole di accesso configurate per l'unità RV110W sono visualizzate nella **Tabella regole di accesso**. Questo elenco mostra anche se la regola è abilitata (attiva) e fornisce un riepilogo della zona "da/a" nonché i servizi e gli utenti coinvolti dalla regola.

Per creare una regola di accesso, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Regole di accesso**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Nel campo **Tipo di connessione**, selezionare l'origine del traffico:

- **Uscita (LAN > WAN)**: selezionare questa opzione per creare una regola per il traffico in uscita.
- **Ingresso (LAN > WAN)**: selezionare questa opzione per creare una regola per il traffico in entrata.
- **Ingresso (WAN > DMZ)**: selezionare questa opzione per creare una regola per il traffico in entrata.

PASSAGGIO 4 Dall'elenco a discesa **Azione** scegliere l'azione:

- **Blocca sempre**: blocca sempre il tipo di traffico selezionato.
- **Consenti sempre**: consente sempre il tipo di traffico selezionato.
- **Blocca in base a pianificazione, in caso contrario consenti**: blocca il tipo di traffico selezionato in base a una pianificazione.
- **Consenti in base a pianificazione, in caso contrario consenti**: consente il tipo di traffico selezionato in base a una pianificazione.

PASSAGGIO 5 Dal menu a discesa **Servizi**, selezionare il servizio da consentire o bloccare per questa regola. Selezionare **Tutto il traffico** per consentire l'applicazione della regola a tutte le applicazioni e servizi oppure selezionare un'applicazione singola da bloccare:

- DNS (Domain Name System, DNS), UDP o TCP
- FTP (File Transfer Protocol)
- HTTP (Hyptertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- TFTP (Trivial File Transfer Protocol)
- IMAP (Internet Message Access Protocol)
- NNTP (Network News Transport Protocol)
- POP3 (Post Office Protocol)
- SNMP (Simple Network Management Protocol)
- SMTP (Simple Mail Transfer Protocol)
- Telnet
- STRMWORKS

- TACACS (Terminal Access Controller Access-Control System)
- Telnet (comando)
- Telnet Secondary
- Telnet SSL
- Voce (SIP)

PASSAGGIO 6 (Opzionale) Fare clic su **Configura servizi** per accedere alla pagina **Gestione servizio** per configurare i servizi prima di applicare le regole di accesso.

Per ulteriori informazioni, vedere la sezione **Configurazione della gestione servizi, pagina 85**.

PASSAGGIO 7 Nel campo **IP di origine**, selezionare gli utenti ai quali verranno applicate le regole del firewall:

- **Qualsiasi**: la regola viene applicata al traffico proveniente da qualsiasi host della rete locale.
- **Indirizzo singolo**: la regola viene applicata al traffico proveniente da un indirizzo IP specifico della rete locale. Immettere l'indirizzo nel campo **Inizio**.
- **Intervallo di indirizzi**: la regola viene applicata al traffico proveniente da un indirizzo IP che si trova in un intervallo di indirizzi IP. Immettere l'indirizzo IP iniziale nel campo **Inizio** e l'indirizzo IP finale nel campo **Fine**.

PASSAGGIO 8 Nel campo **Registro**, specificare se i pacchetti per questa regola devono essere registrati.

Per registrare i dettagli di tutti i pacchetti che soddisfano questa regola, selezionare **Sempre** dal menu a discesa. Ad esempio, se una regola in uscita per una pianificazione è stata contrassegnata come **Blocca sempre**, per ogni pacchetto che tenta di effettuare una connessione in uscita per quel servizio, nel registro viene registrato un messaggio riportante l'indirizzo dell'origine e quello di destinazione, oltre ad altre informazioni, per il pacchetto.

L'attivazione della registrazione può generare un volume significativo di messaggi di registro ed è consigliabile utilizzarla solo a fini di debug.

Selezionare **Mai** per disattivare la registrazione.

Nota: quando il traffico scorre dalla LAN o DMZ verso la WAN, il sistema richiede la riscrittura dell'indirizzo IP di origine o di destinazione dei pacchetti IP in ingresso quando passano dal firewall.

PASSAGGIO 9 Nel campo Priorità **QoS** assegnare una priorità ai pacchetti IP per il servizio.

Le priorità sono definite dal livello QoS: (**1 (più bassa)**, **2**, **3**, **4 (più alta)**).

PASSAGGIO 10 Configurazione di DNAT (Destination Network Address Translation):

Quando il traffico proviene dalla WAN verso la LAN o DMZ, NAT esegue la mappatura di un indirizzo IP pubblico (l'indirizzo WAN dedicato) a un indirizzo IP della rete privata.

Per configurare DNAT, attenersi alla seguente procedura:

a. Nel campo **Invia a server locale (DNAT IP)**, specificare un indirizzo IP di un dispositivo della LAN che ospita il server.

b. (Opzionale) Selezionare la casella di controllo **Attiva reindirizzamento porta** per attivare il reindirizzamento alla porta specificata nel campo **Traduci numero di porta (IT DNAT)**. Questo consente al traffico proveniente da Internet di raggiungere la porta LAN corretta tramite una regola di reindirizzamento porta.

c. Nel campo **Traduci numero di porta (IP DNAT)**, immettere il numero di porta da utilizzare per il reindirizzamento porta.

   Ad esempio, se su una macchina di rete locale viene eseguito un server Telnet sulla porta 2000, attivare il reindirizzamento e immettere 2000 nel campo **Traduci numero di porta**. Se il server è in ascolto sulla porta predefinita 23, è possibile lasciare la casella deselezionata.

PASSAGGIO 11 Nel campo **Stato regola**, selezionare la casella di controllo per attivare la nuova regola di accesso.

PASSAGGIO 12 Fare clic su **Salva**.

Creazione di un criterio di accesso a Internet

L'unità RV110W supporta diverse opzioni di filtro del contenuto.

È possibile bloccare applicazioni Web o componenti specifici, ad esempio ActiveX o Java, e impostare domini affidabili dai quali consentire sempre il contenuto.

Si può anche bloccare l'accesso ai siti Internet, specificando le parole chiave da bloccare. Se le parole chiave si trovano nel nome del sito, ad esempio nell'URL del sito Web oppure nel nome del newsgroup, il sito viene bloccato.

Inoltre è possibile creare delle regole di criteri di accesso a Internet per filtrare la protezione del dominio Internet.

Per creare un criterio di accesso a Internet, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Criterio di accesso Internet**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Nel campo **Stato**, selezionare la casella di controllo **Attiva**.

PASSAGGIO 4 Immettere il nome del criterio per l'identificazione e la gestione.

PASSAGGIO 5 Dal menu a discesa Azione, scegliere il tipo di limitazione di accesso necessario:

- **Blocca sempre**: blocca sempre il tipo di traffico selezionato.
- **Consenti sempre**: consente sempre il tipo di traffico selezionato.
- **Blocca in base a pianificazione, in caso contrario consenti**: blocca il tipo di traffico selezionato in base a una pianificazione.
- **Consenti in base a pianificazione, in caso contrario consenti**: consente il tipo di traffico selezionato in base a una pianificazione.

Se si seleziona **Blocca in base a pianificazione** oppure **Consenti in base a pianificazione**, fare clic su **Configura pianificazioni** per creare una pianificazione. Vedere la sezione **Gestione delle pianificazioni del firewall, pagina 84**.

PASSAGGIO 6 Selezionare una pianificazione dal menu a discesa.

PASSAGGIO 7 (Opzionale) Applicare il criterio di accesso a PC specifici:

Con il filtro degli indirizzi è possibile consentire o bloccare il traffico proveniente da dispositivi specifici.

a. Nella tabella **Applica il criterio di accesso ai seguenti PC** fare clic su **Aggiungi riga**.

b. Dal menu a discesa **Tipo**, selezionare il tipo di identificazione del PC, ovvero in base all'indirizzo MAC o l'indirizzo IP o fornendo un intervallo di indirizzi IP.

c. Nel campo **Valore** immettere le informazioni seguenti, a seconda dell'opzione selezionata nel passaggio precedente:

- L'indirizzo MAC (xx:xx:xx:xx:xx:xx) del PC al quale si applica il criterio.
- L'indirizzo IP del PC al quale si applica il criterio.
- L'indirizzo iniziale e quello finale dell'intervallo di indirizzi da bloccare, ad esempio, 192.168.1.2-192.168.1.30.

PASSAGGIO 8 Per bloccare o consentire siti Web specifici, attenersi alla seguente procedura:

PASSAGGIO 9 È possibile aggiungere un elenco di domini affidabili. Questi domini vengono bypassati durante il filtro per parola chiave basato sulla priorità di regole. L'ultima regola ha una priorità superiore alla prima regola. Per il filtro basato su parola chiave è possibile aggiungere anche un elenco di domini.

a. Nella tabella **Blocco siti Web**, fare clic su **Aggiungi riga**.

b. Dal menu a discesa **Tipo**, selezionare come bloccare un sito Web (specificando l'URL o una parola chiave che appare nell'URL).

c. Nel campo **Valore**, immettere l'URL o la parola chiave utilizzata per bloccare il sito Web.

Ad esempio, per bloccare l'URL esempio.com, selezionare **Indirizzo URL** dal menu a discesa e immettere **esempio.com** nel campo **Valore**. Per bloccare un URL che contiene la parola chiave “esempio”, selezionare **Parola chiave** dal menu a discesa e immettere **esempio** nel campo **Valore**.

PASSAGGIO 10 Fare clic su **Salva**.

Configurazione del reindirizzamento delle porte

Il reindirizzamento delle porte viene utilizzato per instradare il traffico proveniente da Internet da una porta sulla WAN a un'altra porta sulla LAN. Sono disponibili servizi comuni oppure è possibile definire un servizio personalizzato con relative porte da reindirizzare.

Le pagine **Regole reindirizzamento porta singola** e **Regole reindirizzamento intervallo porte** elencano tutte le regole di reindirizzamento porte disponibili per il dispositivo e permettono di configurare tali regole.

NOTA Il reindirizzamento delle porte non è adeguato per i server della LAN poiché il dispositivo LAN dispone di una dipendenza che stabilisce una connessione in uscita prima dell'apertura delle porte in ingresso.

Per il corretto funzionamento di alcune applicazioni è necessario che i dati vengano ricevuti su una porta specifica o un intervallo di porte quando si collegano dispositivi esterni. Il router deve inviare tutti i dati in ingresso per l'applicazione alla porta o all'intervallo di porte richiesto.

Il gateway dispone di un elenco di applicazioni e giochi comuni con porte in ingresso e in uscita corrispondenti da aprire. È anche possibile specificare una regola di reindirizzamento porte definendo il tipo di traffico (TCP o UDP) e l'intervallo di porte in ingresso e in uscita da aprire se abilitate.

Configurazione reindirizzamento porta singola

Per aggiungere una regola di reindirizzamento porta singola, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Reindirizzamento porta singola**.

Viene visualizzato un elenco predefinito di applicazioni.

PASSAGGIO 2 Nel campo **Applicazione**, immettere il nome dell'applicazione per la quale configurare il reindirizzamento porte.

PASSAGGIO 3 Nel campo **Porta esterna**, immettere il numero di porta che attiva la regola quando viene effettuata un richiesta di connessione dal traffico in uscita.

PASSAGGIO 4 Nel campo **Porta interna**, immettere il numero di porta utilizzata dal sistema remoto per rispondere alla richiesta ricevuta.

PASSAGGIO 5 Dal menu a discesa **Protocollo**, selezionare un protocollo (**TCP**, **UDP** o **TCP** e **UDP**).

PASSAGGIO 6 Nel campo **Indirizzo IP**, immettere l'indirizzo IP.

PASSAGGIO 7 Nel campo **Attiva**, selezionare la casella di controllo **Attiva** per attivare la regola.

PASSAGGIO 8 Fare clic su **Salva**.

Configurazione reindirizzamento intervallo porte

Per aggiungere una regola di reindirizzamento di un intervallo di porte, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Reindirizzamento intervallo porte**.

PASSAGGIO 2 Nel campo **Applicazione**, immettere il nome dell'applicazione per la quale configurare il reindirizzamento porte.

PASSAGGIO 3 Nel campo **Porta esterna**, specificare il numero di porta che attiverà la regola quando viene effettuata un richiesta di connessione dal traffico in uscita.

PASSAGGIO 4 Nel campo **Inizio**, specificare il numero di porta iniziale dell'intervallo di porte da reindirizzare.

PASSAGGIO 5 Nel campo **Fine**, specificare il numero di porta finale dell'intervallo di porte da reindirizzare.

PASSAGGIO 6 Dal menu a discesa **Protocollo**, selezionare un protocollo (**TCP**, **UDP** o **TCP** e **UDP**).

PASSAGGIO 7 Nel campo **Indirizzo IP**, immettere l'indirizzo IP.

PASSAGGIO 8 Nel campo **Attiva**, selezionare la casella di controllo **Attiva** per attivare la regola.

PASSAGGIO 9 Fare clic su **Salva**.

Configurazione attivazione intervallo di porte

L'attivazione delle porte consente ai dispositivi della LAN o DMZ di richiedere il reindirizzamento di una o più porte verso tali dispositivi. L'attivazione delle porte attende la richiesta di uscita dalla LAN/DMZ su una delle porte in uscita definite, quindi apre la porta in ingresso per il tipo di traffico specificato.

L'attivazione delle porte è una forma di reindirizzamento porte dinamico durante la trasmissione di dati attraverso porte aperte in uscita o in entrata. L'attivazione delle porte apre una porta in ingresso per un tipo specifico di traffico su una porta in uscita definita. L'attivazione delle porte è più flessibile del reindirizzamento porte statico (disponibile quando si definiscono le regole del firewall) poiché una regola non deve fare riferimento a un intervallo IP LAN o intervallo IP specifico. Le porte, inoltre, non vengono lasciate aperte se non sono in uso, fornendo di conseguenza un livello di sicurezza che il reindirizzamento porte non consente.

NOTA L'attivazione delle porte non è adeguato per i server della LAN poiché il dispositivo LAN dispone di una dipendenza che stabilisce una connessione in uscita prima dell'apertura delle porte in ingresso.

Per il corretto funzionamento di alcune applicazioni è necessario che i dati vengano ricevuti su una porta specifica o un intervallo di porte quando si collegano dispositivi esterni. Il router deve inviare tutti i dati in ingresso per l'applicazione alla porta o all'intervallo di porte richiesto. Il gateway dispone di un elenco di applicazioni e giochi comuni con porte in ingresso e in uscita corrispondenti da aprire. È anche possibile specificare una regola di attivazione delle porte definendo il tipo di traffico (TCP o UDP) e l'intervallo di porte in ingresso e in uscita da aprire se abilitate.

Per aggiungere una regola di attivazione delle porte, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Attivazione intervallo di porte**.

PASSAGGIO 2 Nel campo **Applicazione**, immettere il nome dell'applicazione per la quale configurare il reindirizzamento porte.

PASSAGGIO 3 Nei campi **Intervallo attivati**, specificare il numero di porta o intervallo di porte che attiverà questa regola quando viene effettuata un richiesta di connessione dal traffico in uscita. Se la connessione in uscita utilizza solo una porta, immettere lo stesso numero di porta in entrambi campi.

PASSAGGIO 4 Nei campi **Intervallo reindirizzati**, immettere il numero di porta o l'intervallo di porte utilizzato dal sistema remoto per rispondere alla richiesta ricevuta. Se la connessione in ingresso utilizza solo una porta, immettere lo stesso numero di porta in entrambi campi.

PASSAGGIO 5 Nel campo **Attiva**, selezionare la casella di controllo **Attiva** per attivare la regola.

PASSAGGIO 6 Fare clic su **Salva**.

5

Configurazione VPN

In questo capitolo viene spiegato come configurare la VPN e la protezione dell'unità RV110W.

- **Tipi di tunnel VPN, pagina 96**
- **Client VPN, pagina 97**
- **Configurazione della gestione dei certificati, pagina 101**
- **Configurazione del passthrough VPN, pagina 103**

Tipi di tunnel VPN

La VPN (Virtual Private Network) fornisce un canale di comunicazione sicuro (tunnel) tra un computer remoto e il router RV110W.

Con l'unità RV110W è possibile creare tunnel client remoti (tunnel VPN da gateway a gateway). Un client remoto avvia un tunnel VPN. L'indirizzo IP del client remoto non è noto in anticipo. Il gateway agisce da responder.

Client VPN

- Configurazione PPTP, pagina 97
- Creazione e gestione degli utenti PPTP, pagina 98
- Creazione e gestione degli utenti QuickVPN, pagina 99
- Importazioni delle impostazioni client VPN, pagina 100

Configurazione PPTP

PPTP (Point to Point Tunneling Protocol) è un protocollo di rete che consente il trasferimento sicuro di dati da un client remoto a una rete aziendale creando una connessione VPN sicura attraverso reti pubbliche, quali Internet.

NOTA Quando si attiva la VPN sul router RV110W, la sottorete LAN dell'unità RV110W viene modificata automaticamente per evitare conflitti di indirizzo IP tra la rete remota e la rete locale.

Per configurare il servizio VPN PPTP:

PASSAGGIO 1 Selezionare **VPN** > **Client VPN**.

PASSAGGIO 2 Procedere come indicato di seguito:

Server PPTP	Selezionare questa opzione per attivare il server PPTP.
Indirizzo IP per server PPTP	Immettere l'indirizzo IP del server PPTP.
Indirizzo IP per client PPTP	Immettere l'intervallo di indirizzi IP dei client PPTP.
Crittografia MPPE	Selezionare la casella di controllo **Attiva** per attivare la crittografia MPPE.

PASSAGGIO 3 Fare clic su **Salva**.

Creazione e gestione degli utenti PPTP

Per creare utenti PPTP, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella impostazioni client VPN**, fare clic su **Aggiungi riga**.

PASSAGGIO 2 Immettere le informazioni seguenti:

Attiva	Selezionare questa opzione per attivare l'utente.
Nome utente	Immettere il nome utente PPTP (da 4 a 32 caratteri).
Password	Immettere la password (da 4 a 32 caratteri).
Protocollo	Selezionare **PPTP** dal menu a discesa.

PASSAGGIO 3 Fare clic su **Salva**.

Per modificare le impostazioni di un utente PPTP, selezionare la relativa casella di controllo e fare clic su **Modifica**. Una volta terminate le modifiche, fare clic su **Salva**.

Per eliminare un utente PPTP, selezionare la relativa casella di controllo e fare clic su **Elimina**.

Creazione e gestione degli utenti QuickVPN

Per creare utenti QuickVPN, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella impostazioni client VPN**, fare clic su **Aggiungi riga**.

PASSAGGIO 2 Immettere le informazioni seguenti:

Attiva	Selezionare questa opzione per attivare l'utente.
Nome utente	Immettere il nome utente QuickVPN (da 4 a 32 caratteri).
Password	Immettere la password (da 4 a 32 caratteri).
Consenti all'utente di modificare la password	Selezionare questa opzione per consentire all'utente di modificare la password.
Protocollo	Selezionare **QuickVPN** dal menu discesa.

PASSAGGIO 3 Fare clic su **Salva**.

Per modificare le impostazioni di un utente QuickVPN, selezionare la relativa casella di controllo e fare clic su **Modifica**. Una volta terminate le modifiche, fare clic su **Salva**.

Per eliminare un utente QuickVPN, selezionare la relativa casella di controllo e fare clic su **Elimina**. Quindi, fare clic su **Salva**.

Per ulteriori informazioni su QuickVPN, vedere **Appendice A, "Utilizzo di Cisco QuickVPN".**

Importazioni delle impostazioni client VPN

È possibile importare il file di impostazione dei client VPN contenenti il nome utente e le password dei client in un file di testo di tipo CSV (Comma Separated Value).

È possibile utilizzare Excel per creare un file CSV contenente le impostazioni client VPN. Il file deve contenere una riga per l'intestazione e una o più righe per i client VPN.

Ad esempio, di seguito vengono indicate le impostazioni di due utenti (uno PPTP e uno QuickVPN) da importare:

PROTOCOLLO	NOME UTENTE	PASSWORD
PPTP	pptp-user-1	12345678
QuickVPN	qv-user-1	12345678

ATTENZIONE Quando si importano le impostazioni dei client VPN, le impostazioni esistenti vengono eliminate.

Per importare le impostazioni dei client VPN, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Sfoglia** per selezionare il file.

PASSAGGIO 2 Fare clic su **Importa** per caricare il file.

PASSAGGIO 3 Nella finestra di messaggio in cui viene chiesto se eliminare le impostazioni utente VPN esistenti e importare le impostazioni del file CSV, fare clic su **Sì**.

Configurazione della gestione dei certificati

L'unità Cisco RV110W utilizza certificati digitali per l'autenticazione VPN IPsec e la convalida SSL (per HTTPS). È possibile generare e firmare certificati personalizzati utilizzando le funzionalità dell'unità RV110W.

Generazione di un nuovo certificato

È possibile generare un nuovo certificato che sostituisca quello esistente per l'unità RV110W.

Per generare un certificato, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **VPN** > **Gestione certificati**.

PASSAGGIO 2 Fare clic sul pulsante di opzione **Genera un nuovo certificato**.

PASSAGGIO 3 Fare clic su **Genera certificato**.

Importazione di certificati

Per importare certificati salvati in precedenza in un file, fare clic sul pulsante **Esporta per ammin.**

Per importare un certificato, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **VPN** > **Gestione certificati**.

PASSAGGIO 2 Fare clic sul pulsante di opzione **Importa certificato da file**.

PASSAGGIO 3 Fare clic su **Sfoglia** per selezionare il file del certificato.

PASSAGGIO 4 Fare clic su **Sfoglia** per individuare il file del certificato.

PASSAGGIO 5 Fare clic su **Installa certificato**.

Esportazione di certificati per l'amministratore

Il certificato per l'amministratore contiene la chiave privata e deve essere conservato in un luogo sicuro come copia di riserva. Se vengono ripristinate le impostazioni di fabbrica dell'unità RV110W, è possibile importare e ripristinare il certificato sul router.

Per esportare un certificato per l'amministratore, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **VPN** > **Gestione certificati**.

PASSAGGIO 2 Fare clic su **Esporta per ammin.**

Su un PC, Device Manager salva il file admin.pem in C:\Documents and Settings*userid*\Documenti\Downloads.

Esportazione del certificato per il client

Il certificato per il client consente agli utenti QuickVPN di connettersi in modo sicuro all'unità RV110W. Gli utenti QuickVPN devono salvare il certificato nella directory di installazione del client QuickVPN.

Per esportare un certificato per il client, attenersi alla procedura seguente:

PASSAGGIO 1 Selezionare **VPN** > **Gestione certificati**.

PASSAGGIO 2 Fare clic su **Esporta per client**.

Su un PC, Device Manager salva il file client.pem in C:\Documents and Settings*userid*\Documenti\Downloads.

Configurazione del passthrough VPN

Il passthrough VPN consente il passaggio del traffico VPN generato dai client VPN attraverso l'unità RV110W.

Per configurare il passthrough VPN, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **VPN** > **Passthrough VPN**.

PASSAGGIO 2 Selezionare il tipo di traffico che può essere trasferito attraverso il firewall:

IPsec	Selezionare **Attiva** per consentire il passaggio dei tunnel di sicurezza IP attraverso l'unità RV110W.
PPTP	Selezionare **Attiva** per consentire il passaggio dei tunnel PPTP attraverso l'unità RV110W.
L2TP	Selezionare **Attiva** per consentire il passaggio dei tunnel L2TP (Layer 2 Tunneling Protocol) attraverso l'unità RV110W.

PASSAGGIO 3 Fare clic su **Salva**.

6

Configurazione della Qualità del servizio (QoS)

L'unità Cisco RV110W consente la configurazione delle seguenti funzionalità di Qualità del servizio (QoS):

- **Configurazione della gestione della larghezza di banda, pagina 105**
- **Configurazione delle impostazioni di QoS basato su porta, pagina 107**
- **Configurazione delle impostazioni CoS, pagina 108**
- **Configurazione delle impostazioni DSCP, pagina 108**

Configurazione della gestione della larghezza di banda

È possibile utilizzare la funzionalità di gestione della larghezza di banda dell'unità RV110W per gestire la larghezza di banda del traffico dalla rete sicura (LAN) alla rete non sicura (WAN).

- **Configurazione della larghezza di banda, pagina 105**
- **Configurazione della priorità della larghezza di banda, pagina 106**

Configurazione della larghezza di banda

È possibile limitare la larghezza di banda per ridurre la velocità con cui l'unità RV110W trasmette i dati. Inoltre, è possibile utilizzare un profilo della larghezza di banda per limitare il traffico in uscita e impedire agli utenti della LAN di consumare tutta la larghezza di banda del collegamento Internet.

Per impostare la larghezza di banda upstream e downstream, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **QoS** > **Gestione larghezza di banda**.

PASSAGGIO 2 Nel campo **Gestione larghezza di banda**, selezionare la casella di controllo **Attiva**.

La larghezza di banda massima fornita dall'ISP viene visualizzata nella sezione **Larghezza di banda**.

PASSAGGIO 3 Nella **Tabella larghezza di banda**, immettere le seguenti informazioni per l'interfaccia WAN:

Upstream	La larghezza di banda (kb/s) utilizzata per inviare i dati su Internet.
Downstream	La larghezza di banda (kb/s) utilizzata per ricevere i dati da Internet.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione della priorità della larghezza di banda

Nella **Tabella priorità larghezza di banda**, è possibile assegnare priorità ai servizi per gestire l'utilizzo della larghezza di banda.

Per configurare la priorità della larghezza di banda, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **QoS** > **Gestione larghezza di banda**.

PASSAGGIO 2 Nel campo **Gestione larghezza di banda**, selezionare la casella di controllo **Attiva**.

La larghezza di banda massima fornita dall'ISP viene visualizzata nella sezione **Larghezza di banda**.

PASSAGGIO 3 Nella **Tabella priorità larghezza di banda**, fare clic su **Aggiungi riga**.

PASSAGGIO 4 Immettere le informazioni seguenti:

Attiva	Selezionare questa opzione per attivare la gestione della larghezza di banda per il servizio.
Servizio	Selezionare il servizio a cui assegnare la priorità.
Direzione	Selezionare la direzione del traffico al quale si desidera assegnare la priorità (**downstream** o **upstream**).
Priorità	Selezionare la priorità del servizio (**bassa**, **normale**, **media** o **alta**).

PASSAGGIO 5 Fare clic su **Salva**.

Per modificare le impostazioni di una voce della tabella, selezionare la relativa casella di controllo e fare clic su **Modifica**. Una volta terminate le modifiche, fare clic su **Salva**.

Per eliminare una voce dalla tabella, selezionare la relativa casella di controllo e fare clic su **Elimina**. Quindi, fare clic su **Salva**.

Per aggiungere una nuova definizione del servizio, fare clic sul pulsante **Gestione servizio**. È possibile definire un nuovo servizio da utilizzare per tutte le definizioni del firewall e QoS. Vedere la sezione **Configurazione della gestione servizi, pagina 85**.

Configurazione delle impostazioni di QoS basato su porta

È possibile configurare le impostazioni QoS per ogni porta LAN dell'unità RV110W.

L'unità RV110W supporta 4 code di priorità che permettono di assegnare priorità di traffico per la porta fisica dello switch.

Per configurare le impostazioni di QoS per le porte LAN dell'unità RV110W, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **QoS** > **Impostazioni QoS basato su porta**.

PASSAGGIO 2 Per ciascuna porta della **Tabella impostazioni QoS basato su porta**, immettere le informazioni seguenti:

Modalità Trust	Selezionare una delle seguenti opzioni dal menu a discesa: **Porta**: questa impostazione attiva il QoS basato su porta. È possibile impostare la priorità del traffico per una determinata porta. La priorità della coda di traffico è compresa fra 1 (valore più basso) e 4 (valore più alto). **DSCP**: Differentiated Services Code Point. Se si attiva questa funzionalità, la priorità del traffico di rete della LAN viene assegnata in base alla mappatura della coda DSCP nella pagina **Impostazioni DSCP**. **CoS** : classe di servizio.
Coda reindirizzamento traffico predefinita per dispositivi non attendibili	Selezionare un livello di priorità per il traffico in uscita (da 1 a 4).

PASSAGGIO 3 Fare clic su **Salva**.

Per ripristinare le impostazioni predefinite di QoS basato su porta, fare clic su **Ripristina predefiniti**. Quindi, fare clic su **Salva**.

Configurazione delle impostazioni CoS

È possibile mappare le impostazioni di priorità CoS alla coda di reindirizzamento del traffico dell'unità RV110W.

NOTA È possibile utilizzare il collegamento alla pagina Impostazioni QoS basato su porta per mappare le impostazioni di priorità CoS alla coda QoS.

Per mappare le impostazioni di priorità QoS alla coda di reindirizzamento del traffico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **QoS** > **Impostazioni CoS**.

PASSAGGIO 2 Per ciascun livello di priorità CoS nella **tabella delle impostazioni CoS**, selezionare un valore di priorità dal menu a discesa **Coda reindirizzamento traffico**.

Questi valori contrassegnano i tipi di traffico con priorità di traffico maggiore o minore a seconda del tipo di traffico.

PASSAGGIO 3 Fare clic su **Salva**.

Per ripristinare le impostazioni predefinite di QoS basato su porta, fare clic su **Ripristina predefiniti**. Quindi, fare clic su **Salva**.

Configurazione delle impostazioni DSCP

Utilizzare la pagina delle **Impostazioni DSCP** per configurare la mappatura della coda DSCP a QoS.

Per configurare la mappatura della coda DSCP a QoS, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **QoS** > **Impostazioni DSCP**.

PASSAGGIO 2 Scegliere se elencare solo i valori RFC o tutti i valori DSCP nella **tabella delle impostazioni DSCP** facendo clic sul pulsante di opzione appropriato.

PASSAGGIO 3 Per ciascun valore DSCP nella **tabella delle impostazioni DSCP**, selezionare un livello di priorità dal menu a discesa **Coda**.

Viene così eseguita la mappatura del valore DSCP al valore della coda QoS selezionata.

PASSAGGIO 4 Fare clic su **Salva**.

Per ripristinare le impostazioni DSCP predefinite, fare clic su **Ripristina predefiniti**. Quindi, fare clic su **Salva**.

7

Amministrazione dell'unità RV110W

In questo capitolo vengono descritte le funzionalità relative all'amministrazione dell'unità RV110W, inclusi la creazione di utenti, la gestione della rete, la diagnostica di sistema, i registri, la data e l'ora e altre impostazioni.

- **Impostazione della complessità della password, pagina 111**
- **Configurazione degli account utente, pagina 112**
- **Impostazione dell'intervallo di timeout della sessione, pagina 113**
- **Configurazione di SNMP (Simple Network Management Protocol), pagina 114**
- **Utilizzo degli strumenti di diagnostica, pagina 117**
- **Configurazione della registrazione, pagina 119**
- **Configurazione di Bonjour, pagina 122**
- **Configurazione delle impostazioni di data e ora, pagina 123**
- **Backup e ripristino del sistema, pagina 124**
- **Aggiornamento del firmware, pagina 127**
- **Riavvio dell'unità RV110W, pagina 128**
- **Ripristino delle impostazioni di fabbrica, pagina 129**

Impostazione della complessità della password

Sull'unità RV110W è possibile impostare un requisito minimo di complessità richiesto per le modifiche della password.

Per configurare le impostazioni di complessità password, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Complessità password**.

PASSAGGIO 2 Nel campo Impostazioni complessità password, selezionare la casella di controllo **Attiva**.

PASSAGGIO 3 Configurare le impostazioni di complessità password.

Lunghezza minima password	Immettere la lunghezza minima della password (0-64 caratteri).
Numero minimo classi di caratteri	Immettere un numero che rappresenti una delle seguenti classi di carattere: 1. Lettere maiuscole 2. Lettere minuscole 3. Numeri 4. Caratteri speciali disponibili su una tastiera standard. Per impostazione predefinita, le password devono contenere caratteri di almeno tre di queste classi.
La nuova password deve essere diversa da quella attuale	Selezionare la casella di controllo **Attiva** per impedire che la nuova password sia uguale a quella corrente.
Validità password	Selezionare la casella di controllo **Attiva** per impostare la scadenza delle password dopo un determinato periodo.
Validità temporale password	Immettere il numero di giorni massimo della durata della password (1-365). Il valore predefinito è 180 giorni.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione degli account utente

L'unità RV110W supporta due account utente per l'amministrazione e la visualizzazione delle impostazioni: un utente amministratore (nome utente e password predefiniti: "cisco") e un utente "ospite" (nome utente predefinito: "guest").

L'account ospite ha l'accesso in sola lettura. È possibile impostare e modificare il nome utente e la password per entrambi gli account.

Per configurare gli account utente, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Utenti**.

PASSAGGIO 2 Nella sezione **Selezione utente**, selezionare l'account utente da modificare.

Fare clic su **Modifica impostazioni ammin.** per modificare le impostazioni dell'account amministratore.

Fare clic su **Modifica impostazioni ospite** per modificare le impostazioni dell'account ospite.

PASSAGGIO 3 Per configurare l'account utente amministratore, immettere le seguenti informazioni nella sezione **Impostazioni amministratore**:

Nuovo nome utente	Immettere un nuovo nome utente.
Vecchia password	Immettere la password corrente.
Nuova password	Immettere la nuova password. Si consiglia di utilizzare una combinazione di lettere maiuscole e minuscole), numeri e simboli e di non includere nella password parole in dizionari in qualsiasi lingua. La password può essere composta da un massimo di 30 caratteri.
Digita di nuovo la nuova password	Immettere nuovamente la nuova password.

PASSAGGIO 4 Per configurare l'account utente ospite, immettere le seguenti informazioni nella sezione **Impostazioni ospite**:

Nuovo nome utente	Immettere un nuovo nome utente.
Vecchia password	Immettere la password corrente.
Nuova password	Immettere la nuova password.
Digita di nuovo la nuova password	Immettere nuovamente la nuova password.

PASSAGGIO 5 Per importare i nomi utente e le password da un file CSV, attenersi alla seguente procedura:

a. Nel campo **Importa nome utente e password**, fare clic su **Sfoglia**.

b. Selezionare il file e fare clic su Apri.

c. Fare clic su **Importa**.

PASSAGGIO 6 Immettere la vecchia password.

PASSAGGIO 7 Fare clic su **Salva**.

Impostazione dell'intervallo di timeout della sessione

L'intervallo di timeout è il numero massimo di minuti di inattività dopo il quale la sessione del Device Manager viene terminata. L'intervallo di timeout può essere configurato per gli account Amministratore e Ospite.

Per configurare il timeout della sessione, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministratore** > **Timeout sessione**.

PASSAGGIO 2 Nel campo **Timeout inattività amministratore**, immettere il numero, in minuti, dopo il quale la sessione verrà terminata per inattività.

PASSAGGIO 3 Nel campo **Timeout inattività ospite**, immettere il numero, in minuti, dopo il quale la sessione verrà terminata per inattività.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione di SNMP (Simple Network Management Protocol)

SNMP (Simple Network Management Protocol) consente di monitorare e gestire il router da un manager SNMP. SNMP fornisce un mezzo remoto per monitorare e controllare i dispositivi di rete e per gestire configurazioni, raccolta di statistiche, prestazioni e sicurezza.

- **Configurazione delle informazioni di sistema SNMP, pagina 114**
- **Modifica degli utenti SNMPv3, pagina 115**
- **Configurazione del trap SNMP, pagina 116**

Configurazione delle informazioni di sistema SNMP

È possibile abilitare SNMP nella sezione **Informazioni di sistema SNMP** della pagina **SNMP**.

NOTA Prima di usare SNMP, installare il software SNMP sul computer. L'unità RV110W supporta solo SNMPv3 per la gestione SNMP. L'unità RV110W supporta SNNPv1/2/3 per i messaggi trap SNMP.

Per attivare SNMP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **SNMP**.

PASSAGGIO 2 Per attivare SNMP, selezionare la casella di controllo **Attiva**.

PASSAGGIO 3 Immettere le informazioni seguenti:

SysContact	Immettere il nome del contatto per il firewall (per esempio **admin** o **Mario Rossi**.)
SysLocation	Immettere la posizione fisica del firewall (per esempio **Rack #2, 4° piano**.)
SysName	Immettere un nome per identificare facilmente il firewall.

PASSAGGIO 4 Fare clic su **Salva**.

Modifica degli utenti SNMPv3

È possibile configurare i parametri SNMPv3 per i due account utente predefiniti dell'unità RV110W (Admin e Ospite).

Per configurare le impostazioni SNMPv3, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **SNMP**.

PASSAGGIO 2 Nella sezione **Configurazione utente SNMPv3**, configurare le seguenti impostazioni:

Nome utente	Selezionare l'account da configurare (**admin** o **ospite**).
Privilegio d'accesso	Visualizza i privilegi di accesso dell'account utente selezionato.
Livello di protezione	Selezionare il livello di protezione SNMPv3: **Nessuna autenticazione e nessun privilegio**: non richiede autenticazione e privacy. **Autenticazione e nessun privilegio**: invia solo l'algoritmo di autenticazione e la password. **Autenticazione e privilegio**: invia l'algoritmo di autenticazione/privacy e la password.
Server algoritmo autenticazione	Selezionare il tipo di algoritmo di autenticazione (**MD5** o **SHA**).
Password di autenticazione	Immettere la password di autenticazione.
Algoritmo di privacy	Selezionare il tipo di algoritmo di privacy (**DES** o **AES**).
Password privacy	Immettere la password di privacy.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione del trap SNMP

I campi della sezione **Configurazione trap** SNMP consentono di configurare un agente SNMP al quale il firewall invia i messaggi di trap (notifiche).

Per configurare il trap, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **SNMP**.

PASSAGGIO 2 Nella sezione **Configurazione trap**, configurare le seguenti impostazioni:

Indirizzo IP	Immettere l'indirizzo IP del manager SNMP o dell'agente trap.
Porta	Immettere la porta trap SNMP dell'indirizzo IP al quale verranno inviati i messaggi trap.
Comunità	Immettere la stringa della comunità alla quale appartiene l'agente. La maggior parte degli agenti è configurata per l'ascolto dei trap nella comunità Pubblica.
Versione SNMP	Selezionare la versione SNMP: **v1**, **v2c** o **v3**.

PASSAGGIO 3 Fare clic su **Salva**.

Utilizzo degli strumenti di diagnostica

L'unità RV110W mette a disposizione diversi strumenti di diagnostica per la risoluzione dei problemi di rete.

- **Strumenti di rete, pagina 117**
- **Configurazione del mirroring delle porte, pagina 118**

Strumenti di rete

- **Utilizzo di PING, pagina 117**
- **Uso di Traceroute, pagina 117**
- **Eseguire una ricerca DNS, pagina 118**

Utilizzo di PING

È possibile utilizzare l'utilità Ping per testare la connettività tra il router e un altro dispositivo della rete. Lo strumento Ping può anche essere utilizzato per testare la connessione a Internet eseguendo il ping di un nome di dominio valido, ad esempio www.cisco.com.

Per utilizzare il PING, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Diagnostica** > **Strumenti di rete**.

PASSAGGIO 2 Nel campo **Indirizzo IP/Nome dominio**, immettere l'indirizzo IP o un nome di dominio valido, ad esempio www.cisco.com, sul quale effettuare il ping.

PASSAGGIO 3 Fare clic su **Ping**.

Vengono visualizzati i risultati del ping, che indicano se il dispositivo è raggiungibile.

PASSAGGIO 4 Alla fine, fare clic su **Chiudi**.

Uso di Traceroute

L'utilità Traceroute visualizza tutti i router presenti tra l'indirizzo IP di destinazione e il router.

L'interfaccia utente visualizza fino a 30 hop (router intermedi) tra il router e la destinazione.

Per utilizzare Traceroute, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Diagnostica** > **Strumenti di rete**.

PASSAGGIO 2 Nel campo **Indirizzo IP/Nome dominio**, immettere l'indirizzo IP da tracciare.

PASSAGGIO 3 Fare clic su **Traceroute**.

Vengono visualizzati i risultati di Traceroute.

PASSAGGIO 4 Alla fine, fare clic su **Chiudi**.

Eseguire una ricerca DNS

È possibile utilizzare lo strumento di ricerca per trovare l'indirizzo IP di un host, ad esempio un server Web, FTP o di posta, su Internet.

Per recuperare l'indirizzo IP di un server Web, FTP, di posta o qualsiasi altro server su Internet, digitare il nome Internet nella casella di testo e fare clic su **Ricerca**. Se la voce host o di dominio esiste, verrà restituita una risposta con l'indirizzo IP. Il messaggio "Host sconosciuto" significa che il nome Internet specificato non esiste.

Per utilizzare lo strumento di ricerca, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Diagnostica** > **Strumenti di rete**.

PASSAGGIO 2 Nel campo **Nome Internet**, immettere il nome Internet dell'host.

PASSAGGIO 3 Fare clic su **Ricerca**.

Vengono visualizzati i risultati di nslookup.

PASSAGGIO 4 Alla fine, fare clic su **Chiudi**.

Configurazione del mirroring delle porte

La funzione di mirroring delle porte monitora il traffico di rete mediante l'invio di copie dei pacchetti in ingresso e in uscita a una porta di monitoraggio.

È possibile utilizzare il mirroring delle porte come strumento diagnostico o di debug, soprattutto quando si cerca di difendersi da un attacco o si esamina il traffico utente da LAN a WAN per vedere se gli utenti accedono a informazioni o siti Web ai quali non dovrebbero accedere.

Per configurare il mirroring delle porte, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Diagnostica** > **Mirroring delle porte**.

PASSAGGIO 2 Nel campo **Origine mirroring**, selezionare le porte su cui eseguire il mirroring.

PASSAGGIO 3 Dal menu a discesa **Porta di mirroring**, selezionare una porta di mirroring.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione della registrazione

Sull'unità RV110W è possibile configurare le opzioni di registrazione.

- **Configurazione delle impostazioni di registrazione, pagina 119**
- **Configurazione dell'invio dei registri tramite e-mail, pagina 121**

Configurazione delle impostazioni di registrazione

Per configurare la registrazione, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Registrazione** > **Impostazioni registro**.

PASSAGGIO 2 Nel campo **Modalità registro**, selezionare la casella di controllo **Attiva**.

PASSAGGIO 3 Fare clic su **Aggiungi riga**.

PASSAGGIO 4 Configurare le seguenti impostazioni:

Servizio registro	Selezionare il servizio di registro nel menu a discesa: **Tutto**: seleziona tutti i servizi di registrazione. **Kernel**: i registri del kernel fanno parte del codice del kernel, ad esempio firewall). **Sistema**: i registri degli eventi di sistema che fanno parte delle applicazioni dello spazio utente, ad esempio NTP, Sessione e DHCP. **Wireless**: i registri wireless visualizzano le informazioni relative alla connessione wireless e negoziazione.

Server dei registri	Immettere l'indirizzo IP del server che raccoglie i registri.
Priorità registro	Selezionare gli eventi da registrare nel menu a discesa. I livelli di gravità degli eventi sono elencati dalla gravità maggiore alla minore, come indicato di seguito: **Tutto**: registra tutti gli eventi. **Emergenza**: il sistema non è utilizzabile. **Allarme**: è necessaria un'azione. **Critico**: il sistema è in una condizione critica. **Errore**: il sistema è in una condizione di errore. **Avviso**: è stato generato un avviso di sistema. **Notifica**: il sistema funziona correttamente, ma è stata generata una notifica di sistema. **Informazioni**: informazioni sul dispositivo. **Debug**: fornisce informazioni dettagliate su un evento.
Visualizza nel registro eventi	Per visualizzare i messaggi di registro nel registro eventi, selezionare questa casella di controllo. Tutti i messaggi di registro vengono visualizzati nella pagina **Visualizza registri** (**Stato** > **Visualizza registri**) del Device Manager.
Invia a e-mail	Per inviare i registri ad un indirizzo e-mail configurato (vedere la sezione **Configurazione dell'invio dei registri tramite e-mail, pagina 121**), selezionare questa casella di controllo.
Attiva	Per attivare le informazioni di registrazione, selezionare questa casella di controllo.

PASSAGGIO 5 Fare clic su **Salva**.

Per modificare una voce nella **tabella impostazioni registro**, selezionare la voce e fare clic su **Modifica**. Effettuare le modifiche quindi fare clic su **Salva**.

Configurazione dell'invio dei registri tramite e-mail

È possibile configurare l'unità RV110W in modo da inviare i registri tramite e-mail.

Per configurare l'invio dei registri tramite e-mail, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Registrazione** > **Impostazioni e-mail**.

PASSAGGIO 2 Per attivare l'invio degli eventi di registro tramite e-mail, selezionare la casella di controllo **Attiva**.

PASSAGGIO 3 Nella sezione **Registro configurazione e-mail**, configurare le seguenti impostazioni:

Indirizzo server e-mail	Immettere l'indirizzo del server SMTP.
Porta server e-mail	Immettere la porta del server SMTP.
Indirizzo e-mail risposta	Immettere l'indirizzo di risposta che l'unità RV110W utilizza per inviare qualsiasi notifica di rimbalzo di e-mail.
Invia a indirizzo e-mail (1)	Immettere l'indirizzo e-mail a cui inviare i registri.
Invia a indirizzo e-mail (2) (opzionale)	Immettere l'indirizzo e-mail a cui inviare i registri.
Invia a indirizzo e-mail (3) (opzionale)	Immettere l'indirizzo e-mail a cui inviare i registri.
Crittografia e-mail (SSL)	Per attivare la crittografia e-mail, selezionare la casella di controllo **Attiva**.
Autenticazione con server SMTP	Se il server SMTP richiede l'autenticazione per accettare i collegamenti, selezionare il tipo di autenticazione dal menu a discesa: **Nessuno**, **ACCESSO**, **NORMALE**, e **CRAM-MD5**.
Nome utente autenticazione e-mail	Immettere il nome utente di autenticazione e-mail, ad esempio *nomeutente@dominio*.com).
Password autenticazione e-mail	Immettere la password di autenticazione e-mail.
Test autenticazione e-mail	Fare clic su **Test** per testare l'autenticazione e-mail.

PASSAGGIO 4 Nella sezione **Invia registri tramite e-mail in base a pianificazione**, configurare le seguenti impostazioni:

Unità	Selezionare l'unità di tempo dei registri (**Mai**, **Ogni ora**, **Ogni giorno**, o **Settimanale**). Se si seleziona **Mai**, i registri non vengono inviati.
Giorno	Se si sceglie un programma settimanale per l'invio dei registri, selezionare il giorno della settimana in cui inviare i registri.
Ora	Se si sceglie un programma quotidiano o settimanale per l'invio dei registri, selezionare l'ora del giorno in cui inviare i registri.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione di Bonjour

Bonjour è un protocollo di pubblicità di servizio e di rilevamento. Sull'unità RV110W, Bonjour pubblicizza solo i servizi di default configurati sul dispositivo quando Bonjour è abilitato.

Per abilitare Bonjour, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Bonjour**.

PASSAGGIO 2 Selezionare la casella di controllo **Attiva** per attivare Bonjour.

PASSAGGIO 3 Per attivare Bonjour per una VLAN elencata nella **Tabella controlli interfaccia Bonjour**, selezionare la casella di controllo **Attiva Bonjour** corrispondente.

È possibile attivare Bonjour su VLAN specifiche. L'attivazione di Bonjour su una VLAN consente ai dispositivi presenti sulla VLAN di rilevare i servizi Bonjour disponibili sul router, come http/https).

Ad esempio, se una VLAN è configurata con un ID di 2, i dispositivi e gli host presenti sulla VLAN 2 non possono rilevare i servizi Bonjour in esecuzione sul router a meno che Bonjour non sia abilitato per VLAN 2.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione delle impostazioni di data e ora

È possibile configurare il fuso orario, scegliere se regolare o meno l'ora legale e definire il server NTP (Network Time Protocol) da utilizzare per sincronizzare la data e l'ora. Il router ottiene le informazioni relative alla data e all'ora dal server NTP.

Per configurare le impostazioni di NTP e dell'ora, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Impostazioni ora**.

PASSAGGIO 2 Configurare le informazioni seguenti:

Fuso orario	Selezionare il proprio fuso orario in relazione a Greenwich Mean Time (GMT).
Regola per l'ora legale	Se applicabile alla propria area geografica, selezionare la casella di controllo **Regola per l'ora legale**. Questa casella di controllo viene attivata facendo clic su **Auto** nel campo **Imposta data e ora** sottostante.
Da	Selezionare dal menu a discesa il mese e il giorno di inizio dell'ora legale.
A	Selezionare dal menu a discesa il mese e il giorno di termine dell'ora legale.
Differenza ora legale	Selezionare dal menu a discesa lo scostamento dall'ora UTC (Coordinated Universal Time).
Imposta data e ora	Selezionare come impostare la data e l'ora.
Server NTP	Per utilizzare i server NTP predefiniti, fare clic sul pulsante di selezione **Usa predefinito**. Per utilizzare un server NTP specifico, fare clic su **Server NTP definito dall'utente** e immettere il nome di dominio completo o l'indirizzo IP dei server NTP nei due campi disponibili.
Immettere data e ora	Immettere la data e l'ora.

PASSAGGIO 3 Fare clic su **Salva**.

Backup e ripristino del sistema

È possibile effettuare un backup delle impostazioni di configurazione personalizzate per un ripristino successivo oppure effettuare il ripristino da un backup precedente dalla pagina **Amministrazione** > **Impostazioni backup/ripristino**.

Se il firewall funziona come da configurazione, è possibile eseguire un backup per un ripristino successivo. Durante il backup le impostazioni vengono salvate come file su un PC. È possibile ripristinare le impostazioni del firewall da questo file.

- **Backup delle impostazioni di configurazione, pagina 125**
- **Ripristino delle impostazioni di configurazione, pagina 126**
- **Copia delle impostazioni di configurazione, pagina 126**
- **Generazione di una chiave di crittografia, pagina 127**

ATTENZIONE Durante l'operazione di ripristino non tentare di andare online, spegnere il firewall, spegnere il PC oppure utilizzare il firewall prima che sia stata completata l'operazione. L'operazione dovrebbe durare circa un minuto. Quando la spia di test si spegne, attendere ancora qualche secondo prima di utilizzare il firewall.

Backup delle impostazioni di configurazione

Per eseguire il backup o ripristinare il sistema, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Impostazioni backup/ripristino**.

PASSAGGIO 2 Selezionare la configurazione di cui effettuare il backup o da cancellare:

Configurazione iniziale	Selezionare questa opzione per scaricare la configurazione iniziale. La configurazione iniziale è la configurazione più attuale in esecuzione utilizzata dall'unità RV110W. Se la configurazione iniziale dei router è stata persa, utilizzare questa pagina per copiare la configurazione di backup nella configurazione iniziale e mantenere intatte tutte le informazioni della configurazione precedente. Per facilitare la distribuzione è possibile scaricare la configurazione iniziale su altre unità RV110W.
Configurazione di mirroring	Selezionare questa opzione per indicare all'unità RV110W di eseguire il backup della configurazione iniziale dopo 24 ore di funzionamento senza modifiche della configurazione iniziale.
Configurazione di backup	Selezionare questa opzione per effettuare il backup delle impostazioni di configurazione correnti.

PASSAGGIO 3 Per scaricare un file di backup basato sull'opzione di configurazione selezionata, fare clic su **Download**.

Il file (startup.cfg, mirror.cfg o backup.cfg) viene scaricato per impostazione predefinita nella cartella predefinita Download.

Ad esempio C:\Documents and Settings\admin\My Documents\Downloads\.

PASSAGGIO 4 Per cancellare la configurazione selezionata, fare clic su **Cancella**.

Ripristino delle impostazioni di configurazione

È possibile ripristinare un file di configurazione salvato i precedenza:

PASSAGGIO 1 Selezionare **Amministrazione** > **Impostazioni backup/ripristino**.

PASSAGGIO 2 Nel campo Caricamento configurazione, selezionare la configurazione da caricare (**Configurazione iniziale** o **Configurazione di backup**).

PASSAGGIO 3 Fare clic su **Sfoglia** per selezionare il file.

PASSAGGIO 4 Selezionare il file e fare clic su **Apri**.

PASSAGGIO 5 Fare clic su **Avvia caricamento**.

L'unità RV110W carica il file di configurazione e utilizza le impostazioni contenute nel file per aggiornare la configurazione iniziale. Quindi l'unità RV110W viene riavviata e utilizza la nuova configurazione.

Copia delle impostazioni di configurazione

La configurazione iniziale viene copiata nella configurazione di backup per garantire la disponibilità di una copia di backup nel caso l'utente dimenticasse il nome utente e la password, impedendo l'accesso all'interfaccia. In questo caso, l'unico modo per poter accedere all'interfaccia consiste nella reimpostazione delle impostazioni di fabbrica dell'unità RV110W.

La configurazione di backup rimane in memoria e permette di copiare le informazioni di backup nella configurazione iniziale ripristinando tutte le impostazioni.

Per copiare una configurazione, ad esempio una configurazione iniziale nella configurazione di backup, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Impostazioni backup/ripristino**.

PASSAGGIO 2 Nel campo **Copia**, selezionare le configurazioni di origine e di destinazione dal menu a discesa.

PASSAGGIO 3 Fare clic su **Avvia copia**.

Generazione di una chiave di crittografia

L'interfaccia consente di generare una chiave di crittografia per la protezione dei file di backup.

Per generare una chiave di crittografia, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Impostazioni backup/ripristino**.

PASSAGGIO 2 Fare clic su **Mostra impostazioni avanzate**.

PASSAGGIO 3 Nel campo delle impostazioni avanzate, immettere il seed utilizzato per generare la chiave.

PASSAGGIO 4 Fare clic su **Salva**.

Aggiornamento del firmware

L'aggiornamento a una nuova versione del firmware viene eseguito dalla pagina **Amministrazione** > **Aggiornamento firmware**.

ATTENZIONE Durante l'aggiornamento del firmware, non tentare di andare online, spegnere l'unità, spegnere il PC oppure interrompere il processo in qualsiasi modo prima che sia stata completata l'operazione. Il processo richiede circa un minuto, incluso il riavvio. L'interruzione del processo di aggiornamento in punti specifici di scrittura della memoria flash può danneggiarla e rendere il router inutilizzabile.

Per effettuare l'aggiornamento a una nuova versione del firmware, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Aggiornamento firmware**.

PASSAGGIO 2 (Opzionale) Fare clic su **Download** per scaricare l'ultima versione del firmware.

PASSAGGIO 3 Fare clic su **Sfoglia** per individuare e selezionare il firmware scaricato.

PASSAGGIO 4 (Opzionale) Per ripristinare le impostazioni di fabbrica dell'unità RV110W dopo avere aggiornato il firmware, selezionare la casella di controllo.

ATTENZIONE Il ripristino delle impostazioni di fabbrica dell'unità RV110W elimina tutte le impostazioni personalizzate.

PASSAGGIO 5 Fare clic su **Avvia aggiornamento firmware**.

Dopo la convalida, la nuova immagine firmware viene scritta nella memoria flash e il router viene riavviato automaticamente con il nuovo firmware.

PASSAGGIO 6 Selezionare **Stato** > **Riepilogo di sistema** per accertarsi che sul router sia stata installata la nuova versione firmware.

Riavvio dell'unità RV110W

Per riavviare il router, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Riavvia**.

PASSAGGIO 2 Fare clic su **Riavvia**.

Ripristino delle impostazioni di fabbrica

ATTENZIONE Durante l'operazione di ripristino non tentare di andare online, spegnere il router, spegnere il PC oppure utilizzare il router prima che sia stata completata l'operazione. L'operazione dovrebbe durare circa un minuto. Quando la spia di test si spegne, attendere ancora qualche secondo prima di utilizzare il router.

Per ripristinare le impostazioni di fabbrica del router, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Ripristina impostazioni di fabbrica**.

PASSAGGIO 2 Fare clic su **Predefinito**.

Esecuzione della procedura di installazione guidata

Per eseguire la procedura di installazione guidata, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Installazione guidata**.

PASSAGGIO 2 Attenersi alle istruzioni online.

8

Visualizzazione dello stato dell'unità RV110W

In questo capitolo viene spiegato come visualizzare le statistiche in tempo reale e altre informazioni relative all'unità RV110W.

- **Visualizzazione del Dashboard, pagina 133**
- **Visualizzazione del riepilogo di sistema, pagina 135**
- **Visualizzazione delle statistiche wireless, pagina 138**
- **Visualizzazione dello stato VPN, pagina 139**
- **Visualizzazione dei registri, pagina 140**
- **Visualizzazione dei dispositivi connessi, pagina 141**
- **Visualizzazione delle statistiche delle porte, pagina 142**

Visualizzazione del Dashboard

La pagina **Dashboard** fornisce una visione d'insieme di tutte le informazioni importanti relative al router.

Per visualizzare il Dashboard, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Stato** > **Dashboard**.

PASSAGGIO 2 Per visualizzare una vista interattiva del pannello posteriore del router, fare clic su **Mostra vista pannello**.

La vista del pannello posteriore mostra le porte in uso (colorate di verde) ed è possibile fare clic su una porta per ottenere ulteriori informazioni relative alla connessione.

- Per visualizzare le informazioni relative alla connessione, fare clic sulla porta.
- Per aggiornare le informazioni relative alla porta, fare clic su **Aggiorna**.
- Per chiudere il pannello con le informazioni relative alla porta, fare clic su **Chiudi**.

Nella pagina **Dashboard** vengono visualizzate le informazioni seguenti:

Informazioni dispositivo

Nome sistema	Il nome del dispositivo.
Versione firmware	La versione corrente del software installato sul dispositivo.
Numero di serie	Il numero di serie del dispositivo.

Utilizzo risorse

CPU	Utilizzo della CPU.
Memoria	Utilizzo della memoria.
Ora corrente	L'ora corrente.
Tempo di attività sistema	Il tempo di attività del sistema.

Riepilogo Syslog

Indica se la registrazione è attivata per le seguenti categorie di evento:

- **Emergenza**
- **Allarme**
- **Critico**
- **Errore**
- **Avviso**

Per visualizzare i registri, fare clic su **Dettagli**. Per ulteriori informazioni, vedere la sezione **Visualizzazione dei registri, pagina 140**.

Per gestire i registri, fare clic su **Gestione registrazione**. Per ulteriori informazioni, vedere la sezione **Configurazione della registrazione, pagina 119**.

Interfaccia LAN (rete locale)

Indirizzo MAC	L'indirizzo MAC del router.
Indirizzo IPv4	L'indirizzo IP locale del router.
Server DHCP	Lo stato del server DHCP del router (attivato o disattivato).

Per visualizzare le impostazioni LAN, fare clic su **Dettagli**. Per ulteriori informazioni, vedere la sezione **Configurazione delle impostazioni LAN, pagina 29**.

Informazioni WAN (Internet)

Indirizzo IPv4	L'indirizzo IP della porta WAN del router.
Stato	Lo stato della connessione Internet (attiva o disattiva).

Per visualizzare le impostazioni WAN, fare clic su **Dettagli**. Per ulteriori informazioni, vedere la sezione **Configurazione delle impostazioni WAN, pagina 23**.

Reti wireless

Elenca lo stato dei quattro SSID della rete wireless.

Per visualizzare le impostazioni wireless del router, fare clic su **Dettagli**. Per ulteriori informazioni, vedere la sezione **Visualizzazione delle statistiche wireless, pagina 138**.

VPN

Utenti QuickVPN	Il numero di utenti QuickVPN.
Utenti PPTP	Il numero di utenti PPTP (Point-to-Point Tunneling Protocol).

Visualizzazione del riepilogo di sistema

La pagina **Riepilogo di sistema** mostra un riepilogo delle impostazioni del router.

Per visualizzare un riepilogo delle impostazioni di sistema, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Stato** > **Riepilogo di sistema**.

PASSAGGIO 2 Fare clic su **Aggiorna** per visualizzare le informazioni più recenti.

Nella pagina **Riepilogo di sistema** vengono visualizzate le informazioni seguenti:

Informazioni di sistema

Versione firmware	La versione corrente del software installato sul dispositivo.
Checksum Firmware MD5	L'algoritmo message-digest utilizzato per verificare l'integrità dei file.
PID VID	ID del prodotto e della versione del dispositivo.

Tempo di attività sistema	Il tempo di attività del sistema.
Ora corrente	L'ora corrente.
Modello CPU	Il chipset della CPU in uso.
Numero di serie	Il numero di serie del dispositivo.

Configurazione IPv4

IP LAN	L'indirizzo LAN del dispositivo.
IP WAN	L'indirizzo WAN del dispositivo.
Modalità	Se è attivato NAT, viene indicato **Gateway**, altrimenti appare **Router**.
DNS 1	Indirizzo IP del server DNS primario della porta WAN.
DNS 2	Indirizzo IP del server DNS secondario della porta WAN.
DDNS	Indica se il DNS dinamico è attivato o disattivato.

Configurazione IPv6

IP LAN	L'indirizzo LAN del dispositivo.
IP WAN	L'indirizzo WAN del dispositivo.
DNS 1	L'indirizzo IP del server DNS primario.
DNS 2	L'indirizzo IP del server DNS secondario.

Riepilogo wireless

SSID 1	Il nome pubblico della prima rete wireless.
Protezione	L'impostazione di protezione per SSID 1.
SSID 2	Il nome pubblico della seconda rete wireless.
Protezione	L'impostazione di protezione per SSID 2.
SSID 3	Il nome pubblico della terza rete wireless.
Protezione	L'impostazione di protezione per SSID 3.
SSID 4	Il nome pubblico della quarta rete wireless.
Protezione	L'impostazione di protezione per SSID 4.

Stato impostazione firewall

DoS (Denial of Service)	Indica se la prevenzione DoS è attiva o disattiva.
Blocco richiesta WAN	Indica se il blocco richiesta WAN è attivo o disattivo.
Gestione remota	Indica se la gestione remota è attiva o disattiva.

Stato impostazione VPN

Collegamenti QuickVPN disponibili	Il numero di collegamenti QuickVPN disponibili.
Collegamenti PPTP VPN disponibili	Il numero di collegamenti PPTP VPN disponibili.
Utenti QuickVPN connessi	Il numero di utenti QuickVPN connessi.
Utenti PPTP VPN connessi	Il numero di utenti PPTP VPN connessi.

Visualizzazione delle statistiche wireless

La pagina **Statistiche wireless** mostra un totale complessivo delle statistiche wireless pertinenti per la radio del dispositivo.

Per visualizzare le statistiche wireless, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Stato** > **Statistiche wireless**.

PASSAGGIO 2 Dal menu a discesa **Frequenza aggiornamento**, selezionare una frequenza di aggiornamento.

PASSAGGIO 3 Per ripristinare i contatori delle statistiche wireless, fare clic su **Azzera conteggio**.

Nella pagina **Statistiche wireless** vengono visualizzate queste informazioni:

Nome SSID	Il nome della rete wireless.
Pacchetto	Il numero di pacchetti wireless ricevuti/inviati segnalati alla radio tramite tutti gli SSID configurati e attivi.
Byte	Il numero di byte di informazioni ricevuti/inviati segnalati alla radio tramite tutti gli AP configurati.
Errore	Il numero di errori pacchetto ricevuti/inviati segnalati alla radio tramite tutti gli AP configurati.
Eliminati	Il numero di pacchetti ricevuti/inviati persi dalla radio, per tutti gli AP configurati.
Multicast	Il numero di pacchetti multicast inviati tramite questa radio.
Collisioni	Il numero di collisioni pacchetto segnalati all'AP.

NOTA I contatori vengono azzerati al riavvio del dispositivo.

Visualizzazione dello stato VPN

Nella pagina **VPN** viene visualizzato lo stato delle connessioni VPN.

Per visualizzare lo stato delle connessioni utente VPN, selezionare **Stato** > **Stato VPN**.

Nella pagina **VPN** vengono visualizzate queste informazioni:

Nome utente	Il nome utente VPN associato al tunnel PPTP o QuickVPN.
IP remoto	Visualizza l'indirizzo IP del client QuickVPN remoto. Se il client si trova dietro un router NAT, si tratta dell'IP NAT/Pubblico.
Stato	Visualizza lo stato corrente del client QuickVPN. OFFLINE significa che il tunnel QuickVPN non è stato avviato/connesso dall'utente VPN. ONLINE significa che il tunnel QuickVPN avviato/connesso dall'utente VPN è attivo.
Ora di inizio	L'ora in cui l'utente VPN ha attivato una connessione.
Ora di fine	L'ora in cui l'utente VPN ha terminato la connessione.
Durata (secondi)	La durata della connessione da parte dell'utente VPN.
Protocollo	Il protocollo utilizzato dall'utente: QuickVPN o PPTP.

È possibile modificare lo stato di una connessione per connettere o disconnettere il client VPN configurato.

Per terminare una connessione VPN attiva, fare clic su **Disconnetti**.

Visualizzazione dei registri

La pagina **Visualizza registri** consente di visualizzare i registri dell'unità RV110W.

Per visualizzare i registri, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Stato** > **Visualizza registri**.

PASSAGGIO 2 Fare clic su **Aggiorna registri** per visualizzare le voci di registro più recenti.

PASSAGGIO 3 Per specificare i tipi di registri da visualizzare, selezionare un'opzione dal menu a discesa **Filtro**.

È possibile scegliere una delle opzioni seguenti:

Tutto	Visualizza tutti i registri
Kernel	Visualizza i registri del kernel che sono parte del codice del kernel, per esempio firewall.
Sistema	Visualizza i registri degli eventi di sistema, ovvero quei registri che fanno parte delle applicazioni dello spazio utente, per esempio, NTP, Sessione e DHCP.
Wireless	Visualizza i registri wireless, ovvero quei registri pertinenti alla connessione e alla negoziazione wireless.

Per eliminare tutte le voci della finestra dei registri, fare clic su **Cancella registri**.

Per salvare tutti i messaggi dei registri dal firewall sul disco rigido locale, fare clic su **Salva registri**.

Per specificare il numero di voci da visualizzare per ogni registro, selezionare un numero dal menu a discesa.

Utilizzare i pulsanti di esplorazione delle pagine per spostarsi tra le pagine del registro.

Visualizzazione dei dispositivi connessi

La pagina **Dispositivi connessi** visualizza le informazioni relative ai dispositivi connessi all'unità RV110W.

Per visualizzare i dispositivi connessi, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Stato** > **Dispositivi connessi**.

PASSAGGIO 2 Per specificare i tipi di interfacce da visualizzare, selezionare un'opzione dal menu a discesa **Filtro**.

È possibile scegliere una delle opzioni seguenti:

Tutto	Visualizza un elenco di tutti dispositivi connessi al router.
Wireless	Visualizza un elenco di tutti dispositivi connessi tramite l'interfaccia wireless.
Cablata	Visualizza un elenco di tutti dispositivi connessi tramite le porte Ethernet sul router.
WDS	Visualizza un elenco di tutti dispositivi WDS (Wireless Distribution System) connessi al router.

Visualizzazione delle statistiche delle porte

Nella pagina **Statistiche porte** vengono visualizzate le statistiche delle porte.

Per visualizzare le statistiche delle porte, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Stato** > **Statistiche porte**.

PASSAGGIO 2 Dal menu a discesa **Frequenza aggiornamento**, selezionare una frequenza di aggiornamento.

In questo modo vengono rilette le statistiche del router e la pagina viene aggiornata.

PASSAGGIO 3 Per ripristinare i contatori delle statistiche delle porte, fare clic su **Azzera conteggio**.

Nella tabella vengono visualizzate le statistiche relative al trasferimento dei dati delle porte dedicate WAN, LAN e WLAN, inclusa la relativa durata di attivazione.

Nella pagina **Statistiche porte** vengono visualizzate le informazioni seguenti:

Interfaccia	Nome dell'interfaccia di rete.
Pacchetto	Il numero di pacchetti ricevuti/inviati.
Byte	Il numero di byte di informazioni ricevuti/inviati al secondo.
Errore	Il numero di errori di pacchetto ricevuti/inviati.
Persi	Il numero di pacchetti ricevuti/inviati che sono stati persi.
Multicast	Il numero di pacchetti multicast inviati tramite questa radio.
Collisioni	Il numero di collisioni di segnale che si sono verificate su questa porta. Una collisione si verifica quando la porta tenta di inviare dati contemporaneamente ad una porta su un altro router o computer connesso alla stessa porta.

A

Utilizzo di Cisco QuickVPN

Panoramica

In questa appendice si spiega come installare e utilizzare il software Cisco QuickVPN, che può essere scaricato dal sito Cisco.com. QuickVPN può essere utilizzato su computer che eseguono il sistema operativo Windows 7, Windows XP, Windows Vista o Windows 2000 (per i computer con altri sistemi operativi, è necessario utilizzare un programma software VPN di terze parti).

In questa appendice sono presenti le seguenti sezioni:

- **Operazioni preliminari, pagina 143**
- **Installazione del software QuickVPN di Cisco, pagina 144**
- **Utilizzo del software Cisco QuickVPN, pagina 146**

Operazioni preliminari

Il programma QuickVPN può essere utilizzato solo con un router configurato correttamente per la connessione QuickVPN. È necessario eseguire le seguenti operazioni:

PASSAGGIO 1 Attivare la gestione remota. Vedere la sezione **Configurazione delle impostazioni firewall di base, pagina 81**.

PASSAGGIO 2 Creare gli account utente QuickVPN. Vedere la sezione **Configurazione PPTP, pagina 26**. Dopo avere creato un account utente, è possibile utilizzare le credenziali con il client QuickVPN.

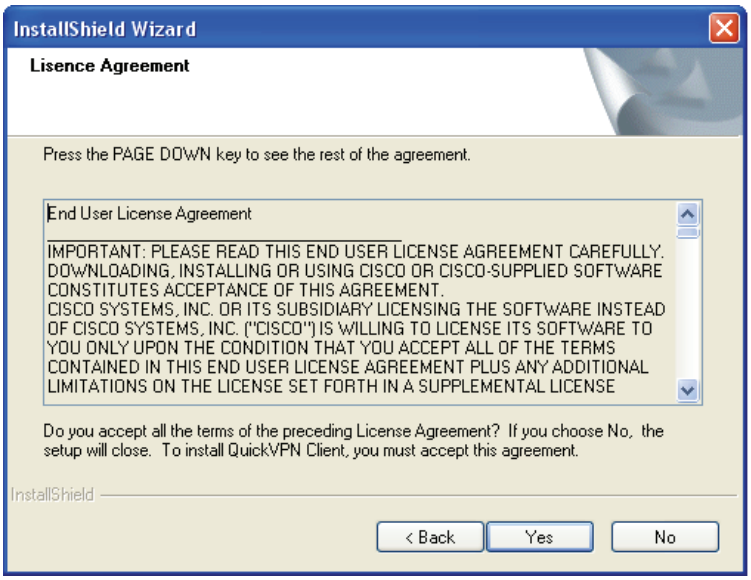
Installazione del software QuickVPN di Cisco

Installazione del software da CD

PASSAGGIO 1 Inserire il CD di Cisco RV110W nell'unità CD-ROM. Dopo l'avvio dell'installazione guidata, fare clic sul collegamento **Install QuickVPN** (Installa QuickVPN).

PASSAGGIO 2 Viene visualizzata la finestra License Agreement (Contratto di licenza). Fare clic su **Yes** (Sì) per accettare il contratto.

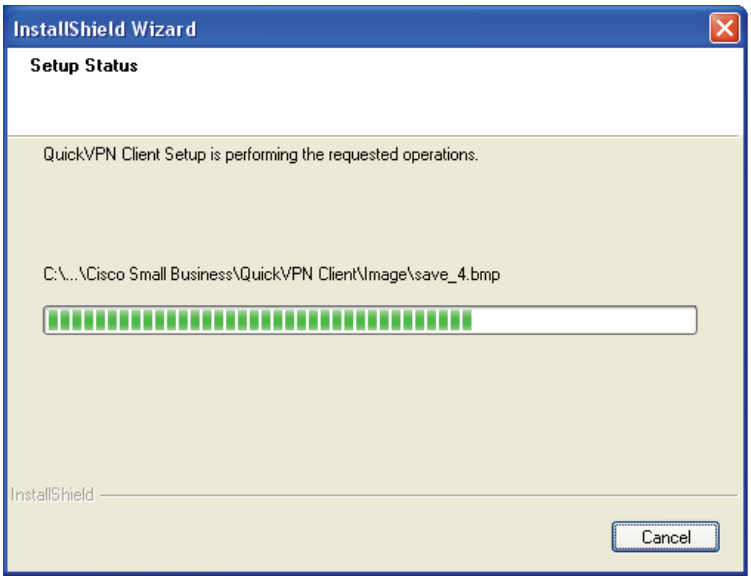
Contratto di licenza



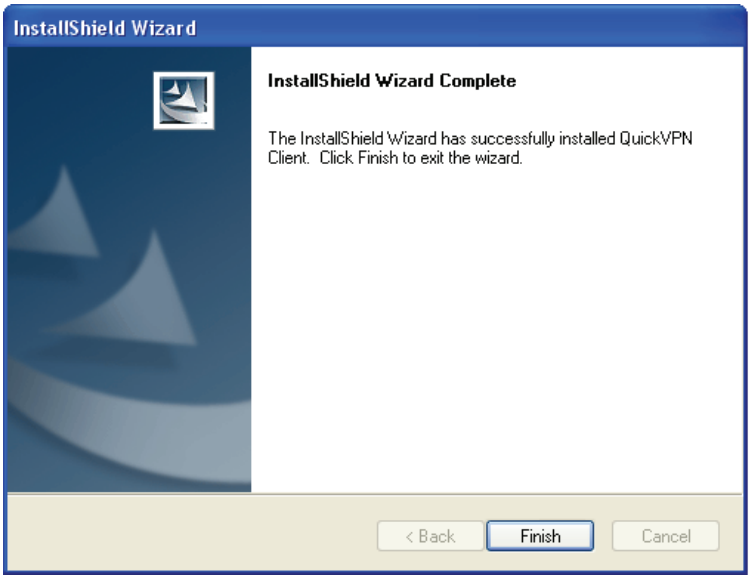
PASSAGGIO 3 Scegliere il percorso di destinazione dei file (per esempio C:\Cisco Small Business\QuickVPN Client). Fare clic su **Browse** (Sfoglia) e selezionare una nuova posizione se non si desidera utilizzare il percorso predefinito proposto. Fare clic su **Next** (Avanti).

PASSAGGIO 4 I file vengono copiati nel percorso selezionato.

Copia dei file



Installazione dei file completata



PASSAGGIO 5 Fare clic su **Finish** (Fine) per completare l'installazione. Passare alla sezione **"Utilizzo del software Cisco QuickVPN", a pagina 146**.

Download e installazione del software da Internet

PASSAGGIO 1 Nell'**Appendice B, "Risorse aggiuntive",** selezionare il collegamento Download di software.

PASSAGGIO 2 Immettere RV110W nella casella di ricerca e individuare il software **QuickVPN**.

PASSAGGIO 3 Salvare il file ZIP sul PC ed estrarre il file .exe.

PASSAGGIO 4 Fare doppio clic sul file .exe e attenersi alle istruzioni visualizzate. Passare alla sezione successiva, **"Utilizzo del software Cisco QuickVPN", a pagina 146**.

Utilizzo del software Cisco QuickVPN

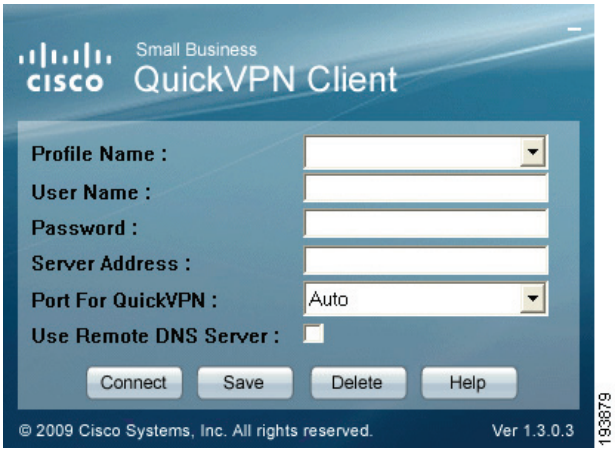
PASSAGGIO 1 Fare doppio sull'icona del software Cisco QuickVPN sul desktop o nell'area di notifica del sistema.

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

PASSAGGIO 2 Viene visualizzata la finestra QuickVPN Login (Accesso QuickVPN). Nel campo **Profile Name** (Nome profilo), immettere un nome per il profilo. Nei campi **User Name** (Nome utente) e **Password** (Password), inserire il nome utente e la password creati nella sezione **Creazione e gestione degli utenti QuickVPN, pagina 99**. Nel campo **Server Address** (Indirizzo server), immettere l'indirizzo IP o il nome di dominio del router Cisco RV110W. Nel campo **Port For QuickVPN** (Porta per QuickVPN) immettere il numero di porta che verrà utilizzata dal client QuickVPN per comunicare con il router VPN remoto oppure mantenere l'impostazione predefinita **Auto** (Automatico).

Finestra di accesso QuickVPN



Per salvare questo profilo, fare clic su **Save** (Salva); se dovete creare un tunnel per più siti, potete creare diversi profili, ma può essere attivo un solo tunnel alla volta. Per eliminare questo profilo, fare clic su **Delete** (Elimina). Per informazioni, fare clic su **Help** (Guida).

PASSAGGIO 3 Per avviare la connessione QuickVPN, fare clic su **Connect** (Connetti). L'indicatore di avanzamento della connessione visualizza: *Connecting*, *Provisioning*, *Activating Policy*, and *Verifying Network* (Collegamento, Provisioning, Criteri di attivazione e Verifica della rete).

PASSAGGIO 4 Dopo aver stabilito la connessione, l'icona di QuickVPN nell'area di notifica del sistema diventa verde e appare la finestra di stato QuickVPN. In questa finestra vengono visualizzati l'indirizzo IP del lato remoto del tunnel VPN, l'ora e la data di creazione del tunnel e il periodo di attività complessivo del tunnel VPN.

QuickVPN Tray Icon—Connection

Per interrompere il tunnel VPN, fare clic sul pulsante **Disconnect** (Disconnetti). Per modificare la password, fare clic su **Change Password** (Modifica password). Per informazioni, fare clic su **Help** (Guida).

PASSAGGIO 5 Se si dispone dei diritti appropriati per modificare la password, quando si seleziona **Change Password** (Cambia password) viene visualizzata la schermata **Connect Virtual Private Connection** (Connetti connessione privata virtuale). Immettere la password corrente nel campo **Old Password** (Vecchia password) e la nuova password nel campo **New Password** (New Password). Immettere di nuovo la nuova password nel campo **Confirm New Password** (Conferma nuova password). Fare clic su **OK** (OK) per salvare la nuova password. Fare clic su **Cancel** (Annulla) per annullare le modifiche. Per informazioni, fare clic su **Help** (Guida).

NOTA È possibile modificare la password solo se la casella **Allow User to Change Password** (Consenti all'utente di modificare la password) è stata selezionata. Vedere la sezione **Creazione e gestione degli utenti QuickVPN, pagina 99**.

B

Risorse aggiuntive

Cisco fornisce un'ampia gamma di risorse per aiutare ad ottenere il massimo dei benefici offerti dall'unità Cisco RV110W.

Risorse del prodotto

Supporto tecnico	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Assistenza tecnica e documentazione online (richiede l'immissione di dati di accesso)	www.cisco.com/support
Contatti del supporto telefonico	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_ center_contacts.html
Download di software (richiede l'immissione di dati di accesso)	Andare su tools.cisco.com/support/downloads e inserire il numero del modello nella casella di ricerca per il software.
Documentazione prodotti	
Cisco RV110W	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Cisco Small Business	
Cisco Partner Central per Small Business (richiede l'immissione di dati di accesso da parte dei partner)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace