GUIDA ALL'AMMINISTRAZIONE

Cisco RV215W Firewall VPN Wireless-N

Rivisto a novembre 2013

78-20779-02

Sommario

1

Introduzione

In questo capitolo vengono fornite le informazioni per eseguire l'installazione e una guida introduttiva all'utilizzo di Device Manager basato su browser.

- **Verifica dell'installazione dell'hardware**
- **Utilizzo della procedura di installazione guidata**
- **Utilizzo della pagina Introduzione**
- **Collegamento alla rete wireless**

Verifica dell'installazione dell'hardware

Configurare il dispositivo per connettersi alle reti wireless e cablate utilizzando la Guida di riferimento rapido del firewall VPN Wireless-N Cisco RV215W.

CAUTION Utilizzare l'alimentatore 12 V e 1,67 A fornito con il dispositivo. L'utilizzo di un alimentatore diverso potrebbe limitare le prestazioni o danneggiare il dispositivo.

Per verificare l'installazione dell'hardware e la connessione a Internet, attenersi alla seguente procedura:

PASSAGGIO 1 Controllare lo stato dei LED, Per ulteriori informazioni, consultare la Guida di riferimento rapido del firewall VPN Wireless-N Cisco RV215W fornita con il dispositivo.

PASSAGGIO 2 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.

PASSAGGIO 3 Utilizzando un PC con funzionalità wireless, connettersi a un sito Web su Internet, ad esempio www.cisco.com. Per configurare la frequenza radio, consultare la sezione **Collegamento alla rete wireless**.

Utilizzo della procedura di installazione guidata

La procedura di installazione guidata e Device Manager sono supportati su 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 procedura seguente:

PASSAGGIO 1 Avviare il computer connesso a una porta LAN.

Il computer diventa un client DHCP del router 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 del router dispositivo.

Viene visualizzato un messaggio relativo al certificato di protezione del sito. L'unità dispositivo utilizza un certificato di protezione con firma automatica e questo messaggio viene visualizzato dal momento che il computer non riconosce il dispositivo dispositivo.

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

PASSAGGIO 4 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.

PASSAGGIO 5 Fare clic su **Accedi**. Viene avviata la procedura di installazione guidata.

PASSAGGIO 6 Attenersi alle istruzioni visualizzate sullo schermo per configurare il router dispositivo.

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 potrebbe richiedere informazioni relative alla connessione Internet. Se non si conoscono le informazioni richieste, contattare il provider di servizi Internet.

Una volta che la procedura di installazione guidata ha terminato di configurare il dispositivo, viene richiesto di modificare la password predefinita. Seguire le istruzioni visualizzate. Dopo aver modificato la password predefinita, viene visualizzata la pagina **Introduzione**.

Passaggi successivi di configurazione

Anche se la procedura di installazione guidata configura automaticamente il dispositivo, si consiglia di personalizzare alcune impostazioni per fornire una maggiore protezione e prestazioni migliori:

- Se la rete dispone già di un server DHCP e non si desidera che l'unità dispositivo agisca da server DHCP, disabilitare il server. Vedere la sezione **Configurazione delle impostazioni LAN**.
- Configurazione della VPN (Virtual Private Network) tramite QuickVPN. QuickVPN è presente sul CD fornito in dotazione con il router. Vedere la sezione **Appendice A, Utilizzo del software Cisco QuickVPN.**
- Il router dispositivo supporta fino a 4 reti wireless. È possibile configurare una sola rete wireless (o SSID) utilizzando la procedura guidata di configurazione. Per configurare reti wireless aggiuntive utilizzando il Device Manager basato su Web, consultare la sezione **Configurazione della rete wireless**.

Utilizzo della pagina Introduzione

Nella pagina **Introduzione** vengono visualizzate alcune comuni attività di configurazione del router dispositivo. Utilizzare i collegamenti di questa pagina per passare alla pagina di configurazione pertinente.

Questa pagina viene visualizzata a ogni avvio del Device Manager. Per evitare che venga visualizzata, selezionare **Non visualizzare all'avvio**.

Impostazioni iniziali

Modifica password amministratore predefinita	Visualizza la pagina **Utenti**, in cui è possibile modificare la password dell'amministratore e configurare un account ospite. Vedere la sezione **Configurazione degli account utente**.
Avvia installazione guidata	Avvia la procedura di installazione guidata. Seguire le istruzioni visualizzate.
Configura impostazioni WAN	Apre la pagina **Configurazione Internet** per modificare i parametri, come il nome host del router. Vedere la sezione **Configurazione delle impostazioni WAN**.
Configura impostazioni LAN	Apre la pagina **Configurazione LAN** per modificare i parametri della LAN, come l'indirizzo IP di gestione. Vedere la sezione **Configurazione delle impostazioni LAN**.
Configura impostazioni wireless	Apre la pagina **Impostazioni di base** per gestire la radio. Vedere la sezione **Configurazione della rete wireless**.

Accesso rapido

Aggiorna firmware router	Apre la pagina **Aggiornamento firmware/lingua** per aggiornare il firmware o il pacchetto lingua del router. Vedere la sezione **Aggiornamento del firmware o modifica della lingua**.
Aggiungi client VPN	Apre la pagina **Client VPN** per gestire le reti private virtuali. Vedere la sezione **Client VPN**.
Configura accesso gestione remota	Apre la pagina **Impostazioni di base** per abilitare le funzionalità di base del router. Vedere la sezione **Configurazione delle impostazioni firewall di base**.

Stato dispositivo

Riepilogo di sistema	Visualizza la pagina **Riepilogo del sistema** che indica lo stato del router. Vedere la sezione **Visualizzazione del riepilogo di sistema**.
Stato wireless	Visualizza la pagina **Statistiche wireless** che visualizza lo stato della radio. Vedere la sezione **Visualizzazione delle statistiche wireless**.
Stato VPN	Visualizza la pagina **Stato VPN** che elenca le VPN gestite da questo router. Vedere la sezione **Visualizzazione dello stato VPN**.

Altre risorse

Assistenza	Fare clic per aprire la pagina dell'assistenza Cisco.
Forum	Fare clic per visitare i forum online dell'assistenza Cisco.

Salvataggio delle modifiche

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

Collegamento alla rete wireless

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

I seguenti passaggi sono forniti a titolo esemplificativo: potrebbe essere necessario configurare il dispositivo client in modo diverso. Per istruzioni specifiche del dispositivo client, 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, è possibile visualizzare le connessioni wireless nel Pannello di controllo 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

Visualizzazione dello stato del dispositivo

In questo capitolo viene spiegato come visualizzare le statistiche in tempo reale e altre informazioni relative al router dispositivo.

Visualizzazione del Dashboard

La pagina **Dashboard** offre importanti informazioni sul router.

Per visualizzare il Dashboard, selezionare **Stato** > **Dashboard**.

Per modificare la velocità di aggiornamento delle statistiche e dei valori dei parametri visualizzati, selezionare la frequenza dal menu a discesa **Frequenza di aggiornamento**.

Per visualizzare una vista interattiva del pannello posteriore del router, fare clic su **Mostra vista pannello**.

Il pannello posteriore mostra le porte collegate a un dispositivo (con una luce verde).

- Per visualizzare le informazioni relative alla connessione di una porta, spostare il cursore del mouse sulla porta.
- Per aggiornare le informazioni relative alla porta, fare clic su **Aggiorna**.

- Per chiudere la finestra con le informazioni relative alla porta, fare clic su **Chiudi**.

Nella pagina **Dashboard** vengono visualizzate le informazioni seguenti:

Informazioni dispositivo

- **Nome sistema**: 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**: ora del giorno.
- **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**
- **Errori**
- **Avviso**

Per visualizzare i registri, fare clic su **Dettagli**. Per ulteriori informazioni, vedere la sezione **Visualizzazione dei registri**.

Per gestire i registri, fare clic su **Gestione registrazione**. Per ulteriori informazioni, vedere la sezione **Configurazione delle impostazioni di registrazione**.

Interfaccia LAN (rete locale)

- **Indirizzo MAC**: l'indirizzo MAC del dispositivo.
- **Indirizzo IPv4**: l'indirizzo IP di gestione del dispositivo.
- **Indirizzo IPv6**: l'indirizzo IP di gestione del dispositivo (se IPv6 è attivo).

- **Server DHCP**: lo stato del server DHCP IPv4 del dispositivo (attivato o disattivato).
- **Server DHCPv6**: lo stato del server DHCP IPv6 del dispositivo (attivato o disattivato).

Per visualizzare le impostazioni LAN, fare clic su **Dettagli**. Per ulteriori informazioni, vedere la sezione **Configurazione delle impostazioni LAN**.

Informazioni WAN (Rete mobile)

- **Indirizzo IPv4**: l'indirizzo IPv4 della porta USB.
- **Stato**: lo stato della connessione WAN della rete mobile (attiva o disattiva).

Per visualizzare le impostazioni WAN, fare clic su Dettagli. Per ulteriori informazioni, vedere la sezione **Configurazione delle connessioni alla WAN cablata**.

Informazioni WAN (Internet)

- **Indirizzo IPv4**: l'indirizzo IPv4 della porta WAN del router.
- **Indirizzo IPv6**: l'indirizzo IPv6 della porta WAN del router, se IPv6 è attivo.
- **Stato**: lo stato della connessione WAN (attiva o inattiva).

Per visualizzare le impostazioni WAN, fare clic su **Dettagli**. Per ulteriori informazioni, vedere la sezione **Configurazione delle connessioni alla WAN cablata**.

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**.

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** visualizza un riepilogo dei valori dei dispositivi, come ad esempio la versione e il numero di serie del firmware.

Per visualizzare un riepilogo delle impostazioni di sistema, selezionare **Stato** > **Riepilogo di sistema**.

Per passare alla finestra correlata, fare clic sul parametro sottolineato. Ad esempio, per modificare l'indirizzo IP della LAN, fare clic su **IP LAN**. Verrà visualizzata la schermata Configurazione LAN.

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.
- **Impostazioni locali**: la lingua installata sul router.
- **Versione lingua**: versione del pacchetto della lingua installato. La versione del pacchetto lingua deve essere compatibile con il software attualmente installato. In alcuni casi, è possibile utilizzare un pacchetto lingua precedente con un'immagine del firmware più recente. Il router controlla la versione del pacchetto lingua verificandone la compatibilità con la versione corrente del firmware.
- **Checksum lingua MD5**: il checksum MD5 del pacchetto lingua.
- **Modello CPU**: il chipset della CPU in uso.
- **Numero di serie**: il numero di serie del dispositivo.
- **Tempo di attività sistema**: il tempo di attività del sistema.
- **Ora corrente**: ora del giorno.
- **ID prodotto e versione**: ID del prodotto e ID della versione del dispositivo.

Configurazione IPv4

- **IP LAN**: indirizzo IP LAN del dispositivo.

- **IP WAN**: indirizzo IP WAN del dispositivo. È possibile rilasciare l'indirizzo IP attuale e ottenerne uno nuovo selezionando **Rilascia** o **Rinnova**.
- **Gateway**: l'indirizzo IP del gateway a cui è connesso il router dispositivo (ad esempio, il modem via cavo).
- **Modalità**: visualizza **Gateway** se il NAT è attivo o **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**: indirizzo IP LAN del dispositivo.
- **IP WAN**: indirizzo IP WAN del dispositivo.
- **Gateway**: l'indirizzo IP del gateway a cui è connesso il router dispositivo (ad esempio, il modem via cavo).
- **NTP**: il server NTP (nome host o indirizzo IPv6).
- **Delegazione prefisso**: il prefisso IPv6 restituito dal dispositivo all'ISP assegnato agli indirizzi IP nel 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**: impostazioni di protezione per il SSID 1.
- **SSID 2**: il nome pubblico della seconda rete wireless.
  - **Protezione**: impostazioni di protezione per il SSID 2.
- **SSID 3**: il nome pubblico della terza rete wireless.
  - **Protezione**: impostazioni di protezione per il SSID 3.
- **SSID 4:** il nome pubblico della quarta rete wireless.
  - **Protezione**: impostazioni di protezione per il 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 attivato o disattivato.
- **Gestione remota**: indica se è possibile accedere in remoto a Device Manager.

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** visualizza le statistiche wireless della radio del dispositivo.

Per visualizzare le statistiche dell'interfaccia, selezionare **Stato** > **Statistiche wireless**.

Per modificare la velocità di aggiornamento, selezionare una velocità dal menu a discesa **Velocità di aggiornamento**.

Per mostrare i byte in kilobyte (KB) e i dati numerici in formato arrotondato, selezionare **Mostra dati statistici semplificati** e fare clic su **Salva**. Per impostazione predefinita, i dati byte sono visualizzati in byte mentre gli altri dati numerici in formato esteso.

Per ripristinare i contatori delle statistiche wireless, fare clic su **Azzera conteggio**. I contatori vengono azzerati anche al riavvio del dispositivo.

Nella pagina **Statistiche wireless** vengono visualizzate queste informazioni:

Nome SSID	Il nome della rete wireless.
Pacchetti	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 SSID configurati.
Errori	Il numero di errori pacchetto ricevuti/inviati segnalati alla radio tramite tutti gli SSID configurati.
Eliminati	Il numero di pacchetti ricevuti/inviati persi dalla radio, per tutti i SSID configurati.
Multicast	Il numero di pacchetti multicast inviati tramite questa radio.
Collisioni	Il numero di collisioni pacchetto segnalati al router.

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 QuickVPN PPTP.
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 del tempo intercorso fra la creazione e la conclusione della connessione da parte dell'utente VPN.
Protocollo	Il protocollo utilizzato dall'utente.

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 dello stato della connessione IPsec

Lo stato della connessione IPSec mostra lo stato dei criteri VPN attivi sul dispositivo. (tali criteri sono configurati nella pagina **VPN** > **Impostazione VPN avanzata**). Per visualizzare lo stato delle connessioni IPsec, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Stato** > **Stato connessione IPSec**. Nella tabella vengono visualizzate le seguenti informazioni:

- **Frequenza aggiornamento**: scegliere la frequenza con cui visualizzare i dati per cancellare e mostrare i dati più recenti.
- **Mostra dati statistici semplificati**: per impostazione predefinita, i dati byte sono visualizzati in byte mentre gli altri dati numerici in formato esteso. Per mostrare i byte in kilobyte (KB) e i dati numerici in formato arrotondato, selezionare **Mostra dati statistici semplificati**.
- **Nome criterio**: il nome del criterio in base a cui vengono visualizzati i dati.
- **Locale o Remoto**: mostra gli indirizzi IP locali e remoti.
- **Ora di inizio e Ora di fine**: mostra l'ora di inizio e di fine delle connessioni IPSec.
- **Durata**: mostra l'intervallo di tempo durante il quale la connessione è o era attiva.

- **Pacchetti**: mostra i pacchetti ricevuti (Rx) e trasmessi (Tx) durante la connessione.
- **Byte**: mostra i byte ricevuti (Rx) e trasmessi (Tx) durante la connessione.
- **Stato**: mostra lo stato della connessione (ad esempio, attiva o non connessa).
- **Azione**: mostra le azioni eseguibili durante la connessione (ad esempio, eseguire la disconnessione).
- **Azione int**: mostra se l'utente può passare da una connessione VPN primaria a una secondaria. Se si seleziona la casella di controllo **Attiva rollback** sulla pagina **Parametri VPN avanzati**, il pulsante **Switch** non è disponibile.

PASSAGGIO 2 Se sono state apportate modifiche, fare clic su **Salva**.

Visualizzazione dei registri

La pagina **Visualizza registri** visualizza i registri del router dispositivo.

Per visualizzare i registri, selezionare **Stato** > **Visualizza registri**.

Per visualizzare le voci di registro più recenti, fare clic su **Aggiorna registri**.

Per filtrare i registri o specificare la gravità dei registri da visualizzare, selezionare le caselle accanto al tipo di registro e fare clic su **Vai**. Tutti i tipi di registri sopra un tipo di registro selezionato vengono inclusi automaticamente e non è possibile deselezionarli. Ad esempio, la scelta di log di errore include automaticamente anche i log di emergenza, allarme e critici.

I livelli di gravità degli eventi sono elencati dalla gravità maggiore alla minore, come indicato di seguito:

- **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.
- **Informativo**: informazioni sul dispositivo.
- **Debug**: fornisce informazioni dettagliate su un evento.

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 salvare tutti i messaggi di log su un dispositivo USB esterno, fare clic su **Salva log su USB**.

Per specificare il numero di voci da visualizzare per ogni pagina, 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 attivi connessi al router dispositivo.

La tabella ARP IPv4 visualizza le informazioni dai dispositivi che hanno risposto alla richiesta dispositivo ARP (Address Resolution Protocol). Se un dispositivo non risponde alla richiesta, viene rimosso dall'elenco.

La tabella NDP IPv6 visualizza tutti i dispositivi NDP (Neighbor Discover Protocol, protocollo di rilevamento adiacente) IPv6 connessi al collegamento locale del dispositivo.

Per visualizzare i dispositivi connessi, selezionare **Stato** > **Dispositivi connessi**.

Per specificare i tipi di interfacce da visualizzare, selezionare un valore dal menu a discesa **Filtro**.

Tutti: tutti i dispositivi collegati al router.

Wireless: tutti i dispositivi collegati attraverso un'interfaccia wireless.

Cablati: tutti i dispositivi collegati al router attraverso le porte Ethernet.

WDS: tutti dispositivi WDS (Wireless Distribution System) connessi al router.

Visualizzazione delle statistiche delle porte

Nella pagina **Statistiche porte** vengono visualizzate le statistiche dettagliate dell'attività delle porte.

Per visualizzare le statistiche dell'interfaccia, selezionare **Stato** > **Statistiche dell'interfaccia**.

Per fare in modo che la pagina legga di nuovo le statistiche del router e aggiorni la visualizzazione, selezionare una frequenza di aggiornamento dal menu a discesa **Frequenza di aggiornamento**.

Per mostrare i byte in kilobyte (KB) e i dati numerici in formato arrotondato, selezionare **Mostra dati statistici semplificati** e fare clic su **Salva**. Per impostazione predefinita, i dati byte sono visualizzati in byte mentre gli altri dati numerici in formato esteso.

Per ripristinare i contatori delle statistiche delle porte, fare clic su **Azzera conteggio**.

Nella pagina **Statistiche porte** vengono visualizzate le informazioni seguenti:

Interfaccia	Nome dell'interfaccia di rete.
Pacchetti	Numero di pacchetti ricevuti/inviati.
Byte	Numero di byte di informazioni ricevuti/inviati al secondo.
Errori	Numero di errori di pacchetto ricevuti/inviati.
Eliminati	Numero di pacchetti ricevuti/inviati che sono stati persi.
Multicast	Il numero di pacchetti multicast inviati tramite questa radio.
Collisioni	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.

Visualizzazione dello stato della rete ospite

Le statistiche della rete ospite mostrano le informazioni sulla rete ospite wireless configurata sul router dispositivo.

Per visualizzare lo stato della rete ospite, selezionare **Stato** > **Stato rete ospite**. Vengono visualizzate le seguenti informazioni:

- **Nome host**: il dispositivo connesso alla rete ospite.
- **Indirizzo IP**: l'indirizzo IP assegnato al dispositivo connesso.
- **Indirizzo MAC**: l'indirizzo MAC o hardware del dispositivo connesso.
- **Tempo rimasto**: il tempo di connessione alla rete ospite che rimane al dispositivo (i limiti di tempo sono configurati nella pagina **Wireless** > **Impostazioni di base** > **Impostazioni rete ospite**).
- **Azione**: le azioni eseguibili sul dispositivo connesso (ad esempio, eseguire la disconnessione).

Visualizzazione dello stato della rete mobile

Le statistiche della rete mobile 3G/4G e dei dispositivi mobili (chiavette) configurati sul router dispositivo.

Per visualizzare lo stato della rete mobile, selezionare **Stato** > **Rete mobile**. Vengono visualizzate le seguenti informazioni:

- **Connessione**: il dispositivo connesso alla rete ospite.
- **Indirizzo IP Internet**: l'indirizzo IP assegnato al dispositivo USB.
- **Subnet Mask**: subnet mask del dispositivo USB.
- **Gateway predefinito**: indirizzo IP del gateway predefinito.
- **Tempo di attività della connessione**: il tempo di attività del sistema.
- **Utilizzo della sessione corrente**: volume dei dati ricevuti (Rx) e trasmessi (Tx) sulla connessione mobile.
- **Produttore**: nome del produttore della scheda.
- **Modello scheda**: numero del modello della scheda.
- **Firmware scheda**: versione del firmware della scheda.
- **Stato SIM**: stato della scheda SIM.
- **IMS**: identificativo univoco associato agli utenti telefonici mobili della rete GSM, UMTS o LTE.

- **Gestore**: gestore della rete mobile.
- **Tipo di servizio**: tipo di servizio a cui si accede.
- **Intensità del segnale**: intensità del segnale della rete wireless mobile.

3

Configurazione della rete

In questo capitolo viene descritto come configurare le impostazioni di rete del router dispositivo.

Configurazione delle impostazioni WAN

È possibile stabilire una connessione Internet attraverso la porta WAN o tramite un modem wireless installato nella porta USB. In questa sezione viene descritta la configurazione della WAN, della rete mobile, del failover e del ripristino.

Configurazione delle connessioni alla WAN cablata

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

Configurazione di 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 generato dinamicamente a ogni accesso.

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

PASSAGGIO 1 Scegliere **Networking** > **WAN**.

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

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione dell'indirizzo IP statico

Se l'ISP ha assegnato un indirizzo IP permanente, attenersi alla seguente procedura per configurare le impostazioni WAN:

PASSAGGIO 1 Scegliere **Networking** > **WAN**.

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

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IP Internet	Indirizzo IP della porta WAN del firewall.
Subnet mask	Subnet mask della porta WAN del firewall.

Gateway predefinito	Indirizzo IP del gateway predefinito.
DNS statico 1	Indirizzo IP del server DNS primario.
DNS statico 2	Indirizzo IP del server DNS secondario.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione PPPoE

Per configurare le impostazioni PPPoE (Point-to-Point Protocol over Ethernet), attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **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	Il nome utente assegnato dall'ISP.
Password	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. Nel campo per il periodo di richiamata, immettere il numero di secondi trascorsi i quali il router dispositivo tenta di riconnettersi dopo una disconnessione.

Tipo di autenticazione	**Negoziazione automatica**: il server invia una richiesta di configurazione specificando l'algoritmo di protezione impostato. Il dispositivo restituisce le credenziali di autenticazione con il tipo di protezione inviato dal server. **PAP**: protocollo PAP (Password Authentication Protocol) utilizzato dal protocollo Point-to-Point per connettersi all'ISP. **CHAP**: il protocollo CHAP (Challenge Handshake Authentication Protocol) richiede che il client e il server debbano conoscere il testo non criptato della chiave segreta per l'utilizzo dei servizi dell'ISP. **MS-CHAP o MS-CHAPv2**: la versione Microsoft del protocollo CHAP utilizzata per accedere ai servizi dell'ISP.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione PPTP

Per configurare le impostazioni PPTP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **WAN**.

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

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IP Internet	L'indirizzo IP della porta WAN.
Subnet mask	La subnet mask della porta WAN.
Gateway predefinito	Indirizzo IP del gateway predefinito.
Server PPTP	L'indirizzo IP del server PPTP (Point-To-Point Tunneling Protocol).
Nome utente	Il nome utente assegnato dall'ISP.
Password	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. Nel campo per il periodo di richiamata, immettere il numero di secondi trascorsi i quali il router dispositivo 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. L'unità dispositivo restituisce le credenziali di autenticazione con il tipo di protezione inviato dal server. **PAP**: il router dispositivo utilizza il protocollo PAP (Password Authentication Protocol) per connettersi all'ISP. **CHAP**: il router dispositivo utilizza il protocollo CHAP (Challenge Handshake Authentication Protocol) per connettersi all'ISP. **MS-CHAP o MS-CHAPv2**: il router dispositivo 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**.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione L2TP

Per configurare le impostazioni L2TP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **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. Nel campo per il periodo di richiamata, immettere il numero di secondi trascorsi i quali il router dispositivo tenta di riconnettersi dopo una disconnessione.

Tipo di autenticazione	**Negoziazione automatica**: il server invia una richiesta di configurazione specificando l'algoritmo di protezione impostato. Il dispositivo restituisce le credenziali di autenticazione con il tipo di protezione inviato dal server. **PAP**: il protocollo PAP (Password Authentication Protocol) viene utilizzato per connettersi all'ISP. **CHAP**: il protocollo CHAP (Challenge Handshake Authentication Protocol) viene utilizzato per connettersi all'ISP. **MS-CHAP o MS-CHAPv2**: il protocollo MS- CHAP (Microsoft Challenge Handshake Authentication Protocol) viene utilizzato per connettersi all'ISP.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione delle impostazioni opzionali

Per configurare le impostazioni opzionali, attenersi alla seguente procedura:

PASSAGGIO 1 In **Impostazioni facoltative**, configurare le seguenti opzioni:

Nome host	Il nome host del dispositivo dispositivo.
Nome dominio	Il nome di dominio della rete.

MTU	La MTU (Maximum Transmission Unit) indica la dimensione del pacchetto più grande che è possibile inviare tramite la 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 della MTU sono di 1500 byte. Se l'ISP richiede un'impostazione MTU personalizzata, selezionare **Manuale** e immettere le dimensioni MTU.
Dimensioni	Dimensione MTU.

PASSAGGIO 2 Fare clic su **Salva**.

Configurazione di una rete mobile

Utilizzare la pagina Rete mobile per configurare il router dispositivo in modo da connettersi a un modem USB mobile a banda larga collegato all'interfaccia USB del router.

Per visualizzare la finestra **Rete mobile**, fare clic su **Networking** > **WAN > Rete mobile**.

Impostazioni globali

Per installare un modem USB, attenersi alla seguente procedura:

PASSAGGIO 1 Collegare il modem USB. Se il modem è supportato, verrà automaticamente rilevato e visualizzato nella pagina Rete mobile.

PASSAGGIO 2 Selezionare la modalità di connessione **Automatica** o **Manuale** Il ripristino della connessione Ethernet funziona soltanto se la modalità di connessione è automatica.

- Per consentire al modem di stabilire automaticamente una connessione, selezionare la modalità **Auto**. Selezionando Auto, è necessario impostare un tempo per "Connetti su richiesta" oppure selezionare Mantieni connessione attiva. "Connetti su richiesta" conclude la connessione Internet dopo il periodo di inattività specificato (Tempo massimo di inattività).

  Se la connessione Internet viene interrotta per inattività, il modem stabilirà nuovamente una connessione non appena l'utente proverà ad accedere a Internet. Nel campo **Tempo di inattività massimo**, immettere il numero di minuti che devono trascorrere prima che la connessione Internet venga interrotta. Selezionando **Mantieni connessione attiva**, la connessione resterà attiva.

- Per eseguire manualmente la disconnessione e la connessione del modem, selezionare la modalità **Manuale**.

Il dispositivo visualizza lo stato attuale della connessione del modem, che comprende inizializzazione, connessione, disconnessione o disconnesso.

PASSAGGIO 3 Verificare che il campo **Stato scheda dati** della scheda mobile sia su **Connesso**.

Potrebbero essere visualizzati anche i seguenti messaggi:

- Impostare manualmente l'APN (poiché il dispositivo non è in grado di definire il nome del punto di accesso)
- Ricerca servizio in corso...
- Nessuna scheda SIM
- SIM bloccata
- SIM occupata
- SIM pronta
- Codice PIN necessario

- Errore codice PIN
- Scheda bloccata
- La scheda non è attivata
- Errore di inizializzazione della scheda
- Errori

Configurazione della rete mobile

Se occorre modificare uno dei parametri della rete mobile presenti nell'area **Configurazione della rete mobile**, fare clic sul pulsante di opzione **Manuale** nel campo Configura modalità. Il dispositivo rileva automaticamente i modem supportati ed elenca i corretti parametri di configurazione. Il PIN della SIM può essere modificato sia in modalità manuale che automatica.

"Modello scheda" visualizza il modello del modem collegato alla porta USB. Le schede non supportate vengono identificate come **non riconosciute**.

Per annullare qualsiasi altro parametro, selezionare **Manuale** e compilare i seguenti campi:

Campo	Descrizione
APN (Access Point Name)	La rete Internet a cui è connesso il dispositivo mobile. Inserire il nome dell'access point fornito dal provider della rete mobile. Se non si conosce il nome dell'access point, contattare il provider.
Numero di composizione	Il numero di composizione fornito dal service provider della rete mobile per la connessione Internet.
Nome utente Password	Il nome utente e la password forniti dal provider della rete mobile.
Verifica SIM	Attivazione o disattivazione del controllo della scheda SIM.
PIN della SIM	Il codice PIN associato alla scheda SIM. Il campo viene visualizzato soltanto per le schede SIM GSM.
Nome server	Il nome del server per la connessione a Internet (se fornito dal provider).

Campo	Descrizione
Autenticazione	L'autenticazione utilizzata dal provider. Questo valore può essere modificato scegliendo il tipo di autenticazione dall'elenco a discesa. L'impostazione predefinita è Auto. Se non si conosce il tipo di autenticazione da usare, selezionare Auto.
Tipo di servizio	Il tipo di connessione ai servizi dati mobili più diffuso in base al segnale di servizio della zona. Se nella postazione attuale è disponibile un solo servizio dati mobile, è possibile limitare l'opzione preferita riducendo i tempi di configurazione della connessione. La prima selezione cerca un servizio HSPDA/3G/UMTS e passa automaticamente in GPRS, se disponibile.
Servizio LTE	Impostazione del servizio LTE (Long-term Evolution). Selezionare **Automatico** per un segnale in base al segnale di servizio della zona. Selezionare **solo per 4G** solo per i segnali 4G. Selezionare **solo per 3G** solo per i segnali 3G.

PASSAGGIO 4 Fare clic su **Salva** per salvare le impostazioni.

Impostazione limite larghezza di banda

Il dispositivo esegue il monitoraggio dell'attività dati di collegamento di rete mobile e invia una notifica al raggiungimento di una determinata soglia.

Per abilitare o disabilitare "Tracciamento limite larghezza di banda" e impostare i limiti:

PASSAGGIO 1 Selezionare **Abilitato** o **Disabilitato**.

PASSAGGIO 2 Selezionare **Data di rinnovo mensile** dall'elenco a discesa per indicare il giorno del mese in cui viene reimpostato il limite di larghezza di banda.

PASSAGGIO 3 Nel campo **Limite mensile larghezza di banda**, inserire la quantità massima di dati in megabyte che è possibile trasferire prima che il dispositivo intraprenda azioni, come l'invio di un'e-mail a un amministratore.

Impostazione e-mail

Una volta raggiunto il limite della larghezza di banda, è possibile inviare un'e-mail all'amministratore. Per impostare l'indirizzo e-mail di destinazione, selezionare la casella **Invia e-mail a** e fare clic su **Indirizzo e-mail**. Per ulteriori informazioni, vedere la sezione **Configurazione delle impostazioni e-mail**.

Dopo aver selezionato la casella, un'e-mail verrà inviata:

- Quando l'utilizzo della rete mobile supera una percentuale prestabilita.
- Quando il dispositivo esegue il failover sul percorso di backup e avvia il ripristino.
- A ogni intervallo specificato in cui un collegamento di rete mobile è attivo.

Impostazione di failover e ripristino

Anche se fosse essere disponibile un collegamento di rete mobile o Ethernet, per stabilire un collegamento WAN è possibile utilizzare una sola connessione alla volta. In caso di problemi con una connessione WAN, il dispositivo tenterà di eseguire la connessione con un'altra interfaccia. Questa funzionalità si chiama failover. Al ripristino della connessione WAN primaria, la connessione di backup verrà abbandonata. Questa funzione si chiama Ripristino.

PASSAGGIO 1 Selezionare **Networking > WAN > Failover e ripristino**.

PASSAGGIO 2 Selezionare se la connessione di rete primaria è una connessione WAN Ethernet o una connessione di rete mobile tramite chiave USB 3G.

PASSAGGIO 3 Fare clic sul pulsante di scelta **Abilita failover su secondario** per abilitare il failover sul dispositivo dalla connessione di rete primaria e ripristinare la connessione utilizzando la connessione secondaria.

Ad esempio, la connessione primaria dell'utente è una connessione WAN Ethernet e il collegamento WAN viene interrotto. Il dispositivo tenta di ripristinare la connessione utilizzando un collegamento di rete mobile 3G sull'interfaccia USB. Se non si seleziona la casella **Abilita failover su secondario**,la connessione secondaria viene disattivata.

PASSAGGIO 4 Fare clic sul pulsante di scelta **Ripristina a primario Abilita** per consentire al dispositivo di ripristinare automaticamente la connessione primaria e di abbandonare quella secondaria. La modalità di connessione **WAN > Rete mobile** deve essere impostata su Automatico per ripristinare automaticamente la connessione primaria.

PASSAGGIO 5 Nel campo **Intervallo controllo failover** , inserire il tempo (in secondi), trascorso il quale il dispositivo deve tentare di rilevare la presenza di traffico sulla connessione secondaria.

PASSAGGIO 6 Nel campo **Intervallo controllo ripristino**, inserire il tempo (in secondi), trascorso il quale il dispositivo deve tentare di rilevare la presenza di traffico sulla connessione primaria. Se il collegamento è inattivo, a questo intervallo il dispositivo eseguirà un ping verso la destinazione. Se il pacchetto di ping riceve risposta, il dispositivo considererà attivo il collegamento e tenterà di ripristinare la connessione di rete primaria.

PASSAGGIO 7 Fare clic sul pulsante di scelta **Torna immediatamente a Primario quando disponibile** oppure impostare un tempo nel campo **Torna a Primario in un intervallo di tempo specifico** . Se si seleziona un intervallo di tempo specifico, immettere l'ora di inizio e di fine.

PASSAGGIO 8 Nel campo **Ping di ripristino** , immettere il numero di volte in cui il dispositivo deve eseguire il ping del sito di convalida della connessione dopo il ripristino. Sul sito è possibile indicare fino a 5 ping di ripristino. Per impostazione predefinita, il dispositivo eseguirà il ping del sito di convalida una sola volta.

PASSAGGIO 9 Nel campo **Sito convalida connessione** , scegliere la posizione su cui eseguire il ping durante la convalida di ripristino e failover. È possibile scegliere un indirizzo IP personalizzato, il DNS o il gateway del dispositivo come sito di convalida. Se si seleziona un sito personalizzato, immettere l'indirizzo IPv4 or IPv6. Per impostazione predefinita, il dispositivo esegue il ping sul gateway predefinito per convalidare il failover.

PASSAGGIO 10 Per risolvere i problemi di connessione alla rete mobile 3G, fare clic sul pulsante di scelta **Abilita diagnostica 3G** Impostare l'ora in cui, ogni giorno, il dispositivo deve verificare la connessione 3G.

PASSAGGIO 11 Fare clic su **Salva**.

La tabella "Interfaccia WAN" visualizza lo stato della WAN Ethernet e di collegamento di rete mobile su Internet. Per visualizzare i dettagli della porta, fare clic sul collegamento ipertestuale **Stato** .

Aggiornamento del dispositivo USB/WAN

Utilizzare questa pagina per caricare i file di modulo USB che supportano le chiavi USB. Per ottenere i file di modulo USB, contattare l'assistenza Cisco. L'elenco dei modem USB di caricamento dinamico mostra i file di modulo delle chiavi USB 3G e 4G supportate dal dispositivo.

Per eliminare un file di modulo, selezionarlo dall'elenco dei modem USB di caricamento dinamico e fare clic su **Elimina**.

Per caricare il firmware del dispositivo USB (un modulo) dal PC, attenersi alla seguente procedura:

PASSAGGIO 1 Verificare che la chiave USB non sia connessa al dispositivo.

PASSAGGIO 2 Individuare e selezionare il modulo di file della chiave USB.

PASSAGGIO 3 Fare clic su **Importa**.

PASSAGGIO 4 Connettere la chiave USB al dispositivo.

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 dispositivi, 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. Il dispositivo include l'indirizzo IP del server WINS nella configurazione DHCP che il dispositivo invia ai client DHCP.

Quando il router dispositivo è connesso ad un modem o a un dispositivo con una rete configurata sulla stessa sottorete (192.168.1.x), dispositivo 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 del router dispositivo.

Modifica dell'indirizzo IP di gestione dispositivo

L'indirizzo IP per la gestione del dispositivo locale di dispositivo è statico ed è 192.168.1.1 per impostazione predefinita.

Per modificare l'indirizzo IP di gestione del dispositivo, attenersi alla seguente procedura:

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

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

VLAN	Numero della rete VLAN.
Indirizzo IP locale	Indirizzo IP LAN del router dispositivo. Assicurarsi che questo indirizzo IP non sia utilizzato da un altro dispositivo.
Subnet mask	La subnet mask dell'indirizzo IP locale. La subnet mask predefinita è 255.255.255.0.

PASSAGGIO 3 Fare clic su **Salva**.

Dopo avere modificato l'indirizzo IP del dispositivo, il PC non è più in grado di visualizzare il Device Manager.

Per visualizzare il Device Manager, eseguire una delle seguenti operazioni:

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

Aprire una finestra del browser e immettere il nuovo indirizzo IP per collegarsi nuovamente al router dispositivo.

Configurazione del server DHCP

Per impostazione predefinita, l'unità dispositivo agisce da server DHCP per gli host della WLAN (Wireless LAN) o LAN cablata. Il dispositivo può assegnare indirizzi IP e server DNS.

Una volta abilitato DHCP, il router dispositivo assegna indirizzi IP ai dispositivi di rete della LAN da un pool di indirizzi IPv4. Il router dispositivo esegue il test di ciascun indirizzo prima che questo venga assegnato per evitare la presenza di indirizzi duplicati sulla LAN.

Il pool di indirizzi IP predefinito va da 192.168.1.100 a 192.168.1.149. Per impostare un indirizzo IP statico su un dispositivo di rete, utilizzare un indirizzo IP non compreso nel pool. Ad esempio, supponendo che il pool DHCP sia impostato con i parametri predefiniti, è possibile utilizzare gli indirizzi IP statici compresi fra 192.168.1.2 e 192.168.1.99. Questo previene conflitti con il pool di indirizzi IP DHCP predefinito.

Per configurare le impostazioni DHCP, attenersi alla seguente procedura:

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

PASSAGGIO 2 (Opzionale) Selezionare la VLAN da modificare dall'elenco a discesa.

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

Attiva	Consente al router dispositivo di agire come server DHCP sulla rete.
Disattiva	Disabilita DHCP sul router dispositivo per configurare manualmente gli indirizzi IP di tutti i dispositivi di rete.
Inoltro DHCP	Inoltra gli indirizzi IP assegnati da un altro server DHCP ai dispositivi di rete.

Se il server DHCP di dispositivo è abilitato, inserire queste informazioni:

Indirizzo IP iniziale	Il primo indirizzo presente nel pool di indirizzi IP. Qualsiasi client DHCP che accederà alla LAN riceverà un indirizzo IP estratto da questo intervallo.

Numero massimo di utenti DHCP	Il numero massimo di client DHCP.
Intervallo indirizzi IP	(Solo lettura) L'intervallo di indirizzi IP disponibili per i client DHCP.
Durata lease client	La durata (in ore) del lease degli indirizzi IP ai client.
DNS statico 1	Indirizzo IP del server DNS primario.
DNS statico 2	Indirizzo IP del server DNS secondario.
DNS statico 3	Indirizzo IP del server DNS terziario.
WINS	Indirizzo IP del server WINS primario.

PASSAGGIO 4 Se è stata selezionata l'opzione **Inoltro DHCP**, immettere l'indirizzo del gateway di inoltro nel campo **Server DHCP remoto**. Il gateway di inoltro trasmette messaggi di DHCP ai dispositivi di rete, compresi quelli presenti su altre sottoreti.

PASSAGGIO 5 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.

Il router dispositivo dispone di una VLAN predefinita (VLAN 1) che non può essere eliminata. È possibile creare fino a quattro ulteriori VLAN sull'unità dispositivo.

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	L'ID VLAN numerico 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.
Descrizione	Una descrizione che identifica la VLAN.
Routing inter-VLAN	Consente alla stazione finale di una VLAN di comunicare con una stazione finale di un'altra VLAN.
Porta 1 **Porta 2** **Porta 3** **Porta 4**	È possibile associare le VLAN sul router dispositivo alle porte LAN del dispositivo. Per impostazione predefinita, tutte le porte LAN 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

Il router dispositivo può essere configurato 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	La descrizione del client.
Indirizzo IP	L'indirizzo IP del dispositivo. L'indirizzo IP assegnato deve essere esterno al pool di indirizzi DHCP. 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 assegna l'indirizzo IP riservato quando il dispositivo che utilizza l'indirizzo MAC corrispondente richiede un indirizzo IP.
Indirizzo MAC	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 compresa tra la A e la F (incluse).

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 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 sul router dispositivo, una tabella mostra un elenco dei client associati alla VLAN.

Per assegnare un indirizzo IP statico a uno dei dispositivi connessi:

PASSAGGIO 1 Nella riga dei dispositivi collegati, selezionare la casella **Aggiungi al DHCP statico**.

PASSAGGIO 2 Fare clic su **Salva**.

Il server DHCP sul router dispositivo assegna sempre l'indirizzo IP mostrato quando il dispositivo richiede un indirizzo IP.

Configurazione di un host DMZ

Il router dispositivo 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 l'endpoint designato come host DMZ. È necessario assegnare all'host DMZ un indirizzo IP che si trova nella stessa sottorete dell'indirizzo IP del router dispositivo, 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 **Attiva** per attivare la 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

RSTP (Rapid Spanning Tree Protocol) è un protocollo di rete che previene i loop nella rete e riconfigura dinamicamente i canali fisici che devono inoltrare i frame. 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 il router dispositivo diventi la radice dello spanning tree. L'impostazione predefinita è **327688**.
Hello Time	Il tempo di attesa costituisce il periodo di tempo atteso dalla radice dello spanning tree prima di inviare messaggi di saluto. Immettere un numero compreso tra 1 e 10. Il valore predefinito è **2**.
Tempo massimo	Il tempo massimo rappresenta il periodo di tempo atteso dal router per ricevere un messaggio di saluto. Se si raggiunge il tempo massimo, il router tenta di modificare lo spanning tree. Immettere un numero compreso tra 6 e 40. Il valore predefinito è **20**.

Ritardo reindirizzamento	Il ritardo di reindirizzamento è l'intervallo dopo il quale un'interfaccia passa da condizione di blocco a reindirizzamento. Immettere un numero compreso tra 4 e 30. Il valore predefinito 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:

Attiva 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 del percorso	Immettere il costo di percorso RSTP per le porte designate. Segliere 0 per il valore predefinito (il router dispositivo determina automaticamente il valore del percorso). È anche possibile immettere un numero compreso tra 2 e 200000000.

PASSAGGIO 4 Fare clic su **Salva**.

Gestione delle porte

È possibile configurare le impostazioni di velocità e di controllo del flusso delle quattro porte LAN del router dispositivo.

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

PASSAGGIO 1 Scegliere **Networking** > **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 **Disattivato**.
Modalità	Selezionare dal menu a discesa una delle seguenti quattro velocità di porta: • **Negoziazione automatica**: il router dispositivo 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 quanto possa ricevere un ricevitore lento. 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**.

Clonazione dell'indirizzo MAC

A volte può essere necessario impostare lo stesso indirizzo MAC per la porta WAN del router dispositivo e il PC o un indirizzo MAC identico a un altro indirizzo MAC. Questa procedura viene 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 del router dispositivo non viene riconosciuto dall'ISP.

In questo caso, per configurare il dispositivo affinché venga riconosciuto dall'ISP, copiare 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 **Attiva** per attivare la clonazione dell'indirizzo MAC.

PASSAGGIO 3 Per impostare l'indirizzo MAC della porta WAN del router dispositivo, attenersi alla seguente procedura:

- 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

Configurazione delle opzioni di routing.

Configurazione della modalità operativa

Per configurare la modalità operativa del router dispositivo, 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 per impostare il router dispositivo come gateway. Mantenere questa impostazione predefinita se il router dispositivo ospita la connessione di rete a Internet e svolge le funzioni di routing.
Router	(Solo per utenti avanzati) Fare clic su questo pulsante per impostare l'unità dispositivo come router. Selezionare questa opzione se l'unità dispositivo si trova su una rete con altri router. Se si attiva la modalità router, la funzione NAT (Network Address Translation) viene disattivata sull'unità dispositivo.

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 al router dispositivo 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 funzione RIP è disattivata per impostazione predefinita.

NOTA La funzione RIP è disattivata per impostazione predefinita sul router dispositivo.

Per configurare il routing dinamico, attenersi alla seguente procedura:

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

PASSAGGIO 2 Configurare le seguenti impostazioni:

RIP	Selezionare **Attiva** per attivare RIP. Questo consente al router dispositivo di utilizzare la funzione 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. 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. Il router dispositivo supporta fino a 30 percorsi statici.

Fare 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 per indirizzare i pacchetti verso la rete LAN e wireless. • **Internet (WAN)**: fare clic su questo pulsante per indirizzare i pacchetti verso la rete Internet (WAN).

PASSAGGIO 4 Fare clic su **Salva**.

Visualizzazione della tabella di routing

Nella tabella di routing sono contenute le informazioni sulla topologia della rete presente.

Per visualizzare le informazioni di routing della rete, fare clic su **Networking** > **Tabella di routing** e scegliere una delle seguenti opzioni:

- **Mostra tabella routing IPv4**: la tabella di routing viene visualizzata con i campi configurati nelle pagine **Networking** > **Routing**.
- **Mostra tabella routing IPv6**: la tabella di routing viene visualizzata con i campi configurati nelle pagine **Networking** > **IPv6**.

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, 3322.org o noip.com.

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 Scegliere **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 e noip.com) Indirizzo e-mail utilizzato per creare l'account DDNS.
Nome utente	(DynDNS.com e 3322.org) Nome utente dell'account DDNS.
Password	Password per l'account DDNS.
Verifica password	(TZO.com, DynDNS.com e noip.com) Conferma password per l'account DDNS.
Nome host	(DynDNS.com, 3322.org e noip.com) Nome host del server DDNS.
Nome dominio	(TZO.com) Nome del dominio utilizzato per accedere alla rete.
Intervallo di aggiornamento	Selezionare una delle seguenti opzioni per impostare la frequenza con cui aggiornare l'indirizzo IP e il nome di dominio sul server DDNS: **Mai**: nessun aggiornamento. **Settimanale**: aggiornamento ogni settimana alle 00:MM di lunedì (MM è un numero casuale tra 0 e 59). Per impostazione predefinita, viene selezionata l'opzione Settimanale. **Bimestrale**: aggiornamento il primo e il quindicesimo giorno del mese alle 00:MM di lunedì (MM è un numero casuale tra 0 e 59). **Mensile**: aggiornamento il primo giorno del mese alle 00:MM di lunedì (MM è un numero casuale tra 0 e 59).

Indirizzo IP Internet	(Solo lettura) L'indirizzo IP Internet del router dispositivo.
Stato	(Solo lettura) Indica 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	Usare IPv4 sulle porte LAN e WAN.
LAN:IPv6, WAN:IPv4	Usare IPv6 sulle porte LAN e IPv4 sulle porte WAN.
LAN:IPv6, WAN:IPv6	Usare IPv6 sulle porte LAN e WAN.
LAN:IPv4+IPv6, WAN:IPv4	Usare IPv4 e IPv6 sulle porte LAN e IPv4 sulle porte WAN.
LAN:IPv4+IPV6, WAN:IPv4+IPv6	Usare IPv4 e IPv6 sulle porte LAN e WAN.
LAN:IPv4, WAN:IPv6	Usare IPv4 sulle porte LAN e IPv6 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 cinque 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

IPv6 (Internet Protocol version 6) è la versione del protocollo Internet (IP) designata a sostituire IPv4. La configurazione delle proprietà WAN per una rete IPv6 varia a seconda del tipo di connessione Internet di cui si dispone.

Configurazione della connessione WAN IPv6

È possibile configurare il router dispositivo per agire da client DHCPv6 dell'ISP per questa WAN o utilizzare un indirizzo IPv6 statico fornito dall'ISP.

Per configurare le impostazioni IPv6 WAN sul router dispositivo, è necessario impostare prima la modalità IP su una delle seguenti modalità:

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

Per ottenere istruzioni sulle modalità di configurazione della modalità IP, vedere la sezione **Configurazione della modalità IP**.

Configurazione di DHCPv6

Se l'ISP fornisce un indirizzo dinamico, configurare il dispositivo come client DHCPv6.

Per configurare il router dispositivo come client DHCPv6, attenersi alla seguente procedura:

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

PASSAGGIO 2 Nel campo **Tipo di connessione WAN**, selezionare **Configurazione automatica - DHCPv6**.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione di un indirizzo IPv6 WAN statico

Se l'ISP assegna un indirizzo fisso per l'accesso alla WAN, configurare il router dispositivo per l'utilizzo di un indirizzo IPv6 statico.

Per configurare un indirizzo IPv6 statico, attenersi alla seguente procedura:

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

PASSAGGIO 2 Nel campo **Tipo di connessione WAN**, selezionare **IPv6 statico**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IPv6	Indirizzo IPv6 della porta WAN.
Lunghezza prefisso IPv6	Lunghezza di prefisso IPv6 (di solito definita dall'ISP). La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Tutti gli host della sottorete utilizzano lo stesso prefisso. Ad esempio, nell'indirizzo IPv6 `2001:0DB8:AC10:FE01::`, il prefisso è `2001`.
Gateway IPv6 predefinito	Indirizzo IPv6 del gateway predefinito. Di solito si tratta dell'indirizzo IP del server presso l'ISP.
DNS statico 1	Indirizzo IP del server DNS IPv6 primario.
DNS statico 2	Indirizzo IP del server DNS IPv6 secondario.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione delle impostazioni PPPoE IPv6

È possibile utilizzare IPv4 PPPoE, IPv6 PPPoE o entrambi. Se utilizzano entrambi, le impostazioni IPv6 WAN PPPoE devono corrispondere a quelle IPv4 WAN PPPoE. Se non corrispondono, verrà visualizzato un messaggio che richiede di impostare il protocollo IPv6 in modo che corrisponda a quello IPv4. . Per maggiori informazioni, consultare la sezione **Configurazione PPPoE**.

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

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

PASSAGGIO 2 Nel campo **Tipo di connessione WAN**, scegliere **IPv6 PPPoE**.

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

Nome utente	Nome utente assegnato dall'ISP.
Password	Password assegnata dall'ISP.
Connessione su richiesta	Se l'ISP calcola i costi sulla base della durata dei collegamenti, selezionare il pulsante di opzione. Se si seleziona questa opzione, la connessione Internet sarà attiva solo in presenza di traffico. Se la connessione rimane inattiva, vale a dire in assenza di flusso di traffico, la connessione viene chiusa. Nel campo **Tempo massimo di inattività**, inserire il numero di minuti trascorsi senza che venga rilevato traffico sul collegamento prima che quest'ultimo venga interrotto.
Mantieni connessione attiva	Mantiene attivo il collegamento WAN inviando un messaggio di mantenimento della connessione attiva attraverso la porta. Nel campo per il periodo di richiamata, immettere il numero di secondi trascorsi i quali il router dispositivo tenta di riconnettersi dopo una disconnessione.

Tipo di autenticazione	Tipi di autenticazione: **Negoziazione automatica**: il server invia una richiesta di configurazione specificando l'algoritmo di protezione impostato sul server. L'unità dispositivo risponde con le proprie credenziali di autenticazione, tra cui il tipo di protezione inviato in precedenza dal server. **PAP**: utilizzo del protocollo PAP (Password Authentication Protocol) per connettersi all'ISP. **CHAP**: utilizzo del protocollo CHAP (Challenge Handshake Authentication Protocol) per connettersi all'ISP. **MS-CHAP or MS-CHAPv2**: utilizzo del protocollo MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) per connettersi all'ISP.
Nome servizio	Nome che potrebbe essere richiesto dall'ISP per eseguire l'accesso al server PPPoE.
MTU	La MTU (Maximum Transmission Unit) o la dimensione del pacchetto più grande che è possibile inviare tramite la rete. A meno che l'ISP non faccia richiesta di modifica, Cisco consiglia di selezionare l'opzione **Auto**. Il valore di MTU standard per le reti Ethernet è di 1500 byte. Per le connessioni PPPoE questo valore è di 1492 byte. Se l'ISP richiede un'impostazione MTU personalizzata, selezionare **Manuale.**
Dimensioni	Dimensione MTU. Se l'ISP richiede un'impostazione MTU personalizzata, immettere le dimensioni MTU.
Modalità indirizzi	Modalità indirizzi statici o dinamici. Se si seleziona l'opzione statica, immettere l'indirizzo IPv6 nel campo successivo.
Lunghezza prefisso IPv6	Lunghezza prefisso IPv6.
Gateway IPv6 predefinito	Indirizzo IP del gateway IPv6 predefinito.

DNS statico 1	Indirizzo IP del server DNS primario.
DNS statico 2	Indirizzo IP del server DNS secondario.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione delle connessioni 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.

Per configurare le impostazioni IPv6 LAN sul router dispositivo, 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
- LAN:IPv4+IPv6, WAN:IPv4+IPv6

Per ulteriori informazioni su come impostare la modalità IP, vedere la sezione **Configurazione della modalità IP**.

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 del router dispositivo. L'indirizzo IPv6 predefinito del gateway è fec0::1 (or FEC0:0000:0000:0000:0000:0000:0000:0001). 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** o continuare la configurazione delle impostazioni LAN DHCP IPv6.

PASSAGGIO 4 Immettere le seguenti informazioni per configurare le impostazioni DHCPv6:

Stato DHCP	Selezionare questa opzione per attivare il server DHCPv6. Se attivato, l'unità dispositivo assegna un indirizzo IP nell'intervallo specificato, con l'aggiunta di informazioni specifiche, a qualsiasi punto terminale LAN che richiede indirizzi DHCP.
Nome dominio	(Opzionale) Nome di dominio del server DHCPv6.
Preferenza server	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	Indirizzo IPv6 del server DNS primario sulla rete IPv6 dell'ISP.
DNS statico 2	Indirizzo IPv6 del server DNS secondario sulla rete IPv6 dell'ISP.
Durata lease client	Durata (in secondi) del lease degli indirizzi IPv6 ai punti terminali della LAN.

PASSAGGIO 5 Selezionare **Networking** > **IPv6** > **Configurazione LAN IPv6**.

PASSAGGIO 6 Nella **Tabella pool indirizzi IPv6**, fare clic su **Aggiungi riga**.

PASSAGGIO 7 Immettere le informazioni seguenti:

Indirizzo iniziale	Indirizzo IPv6 iniziale del pool.
Indirizzo finale	Indirizzo IPv6 finale del pool.
Lunghezza prefisso IPv6	Lunghezza del prefisso che definisce il numero di bit iniziali comuni negli indirizzi di rete.

PASSAGGIO 8 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 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. Fare attenzione a non introdurre loop di routing nella rete.

Per creare un percorso statico, attenersi alla seguente procedura:

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

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

PASSAGGIO 3 Immettere le informazioni seguenti:

Nome	Nome percorso.

Destinazione	Indirizzo IPv6 dell'host o della rete di destinazione per il percorso.
Lunghezza prefisso	Numero di bit prefisso nell'indirizzo IPv6 che definisce la sottorete di destinazione.
Gateway	Indirizzo IPv6 del gateway attraverso il quale è possibile raggiungere l'host o la rete di destinazione.
Interfaccia	Interfaccia del percorso: **LAN**, **WAN** o **6to4**.
Metrica	Priorità del percorso. Selezionare un valore 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 dal router dispositivo. Può essere utile inserire un percorso inattivo se quest'ultimo non è disponibile al momento dell'aggiunta. 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 a una rete connessa direttamente è 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 dispositivo adiacente dopo 180 secondi, i percorsi appresi dal dispositivo 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.

Sul router dispositivo, 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

Il tunneling IPv6-to-IPv4 (tunneling 6-to-4) consente la trasmissione di pacchetti IPv6 su una rete IPv4. Il tunneling IPv4-to-IPv6 (tunneling 4-to-6) consente la trasmissione di pacchetti IPv4 su una rete IPv6.

Tunneling 6to4

6Il tunneling 6-to-4 viene solitamente utilizzato quando un sito o un utente finale desidera connettersi a Internet IPv6 utilizzando la rete IPv4 esistente.

Per configurare il tunneling 6-to-4, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **IPv6** > **Tunneling**.

PASSAGGIO 2 Nel campo **Tunneling 6to4**, selezionare **Attiva**.

PASSAGGIO 3 Scegliere il tipo di tunneling (**6to4** o **6RD** [Rapid Deployment]).

PASSAGGIO 4 Per il tunneling 6RD, scegliere **automatico** o **manuale**.

PASSAGGIO 5 Immettere le seguenti informazioni:

- **Prefisso IPv6**
- **Lunghezza prefisso IPv6**
- **Inoltro bordo**

- **Lunghezza maschera IPv4.**

PASSAGGIO 6 Fare clic su **Salva**.

Tunneling 4to6

Per configurare il tunneling 4to6, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **IPv6** > **Tunneling**.

PASSAGGIO 2 Nel campo **Tunneling 4to6**, selezionare **Attiva**.

PASSAGGIO 3 Immettere l'indirizzo IPv6 WAN locale nel router dispositivo.

PASSAGGIO 4 Immettere l'indirizzo IPv6 remoto o l'indirizzo IP dell'endpoint remoto.

PASSAGGIO 5 Fare clic su **Salva**.

Visualizzazione dello stato del 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) sul router dispositivo 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 il router dispositivo distribuisce prefissi IPv6 a tutti i nodi presenti sulla rete.

Per configurare RADVD, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **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**: inviare annunci del router (RA) a tutte le interfacce che appartengono al gruppo multicast. **Solo Unicast**: includere solo gli annunci relativi a indirizzi IPv6 noti (gli RA vengono inviati all'interfaccia appartenente esclusivamente a indirizzi noti).
Intervallo annuncio	Intervallo di annuncio (4-1800) per **Multicast non richiesto**. Il valore predefinito 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 utile se nella LAN sono presenti altri dispositivi abilitati per RADVD.
MTU	Dimensione MTU (0 oppure da 1280 a 1500). L'impostazione predefinita è 1500 byte. Il valore MTU (Maximum Transmit Unit) 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	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 Scegliere **Networking** > **IPv6** > **Prefissi annuncio**.

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

PASSAGGIO 3 Immettere le informazioni seguenti:

Tipo di prefisso IPv6	Scegliere uno dei tipi seguenti: **6to4**: consente la trasmissione di pacchetti IPv6 su una rete IPv4. Viene solitamente utilizzato quando un utente finale desidera connettersi a Internet IPv6 utilizzando la connessione 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	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**.

4

Configurazione della rete wireless

In questo capitolo viene descritto come configurare le impostazioni di rete wireless del router dispositivo.

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.

Suggerimenti per la protezione delle reti wireless

Pur non essendo 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, dato che queste informazioni potrebbero essere visibili a chiunque cerchi reti wireless.

- Modificare la password predefinita.

  Per modificare le impostazioni di prodotti wireless, come access point, 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 applicandone 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 possano 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, gli access point 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, gli access point 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 i computer della rete e i singoli file contenenti informazioni riservate.
- Modificare le password a intervalli regolari.
- 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.

Reti wireless Cisco RV215W

Il router dispositivo 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

Nome SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
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 il router dispositivo dall'accesso non autorizzato.

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 Scegliere **Wireless** > **Impostazioni di base**.

PASSAGGIO 2 Nel campo **Radio**, selezionare **Attiva** per attivare la radio wireless. 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.
Combinazione G/N	Selezionare questa opzione se la rete è composta da dispositivi Wireless-G e Wireless-N.

PASSAGGIO 4 Se si sceglie **Combinazione B/G/N**, **Solo N** o **Combinazione G/N** nel campo **Selezione banda wireless**, selezionare la larghezza di banda della rete (**20 MHz** or **20/40 MHz**). Se è stata selezionata l'opzione Solo N, sulla rete è necessario utilizzare la protezione WPA2. Vedere la sezione **Configurazione della modalità di protezione**.

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

PASSAGGIO 6 Nel campo **VLAN di gestione AP**, 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 del router dispositivo.

PASSAGGIO 7 (Opzionale) Nel campo **U-APSD (risparmio energia WMM)**, selezionare **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**).

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 sul router dispositivo.

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

PASSAGGIO 1 Selezionare la casella delle reti da configurare.

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

PASSAGGIO 3 Configurare le impostazioni seguenti:

Attiva SSID	Selezionare **Attiva** per attivare la rete.
Nome SSID	Immettere il nome della rete.
Trasmissione SSID	Selezionare questa casella per attivare la trasmissione di SSID. Se il broadcast SSID è attivo, il router wireless dichiara la sua disponibilità ai dispositivi dotati di wireless nel raggio del router.
VLAN	Selezionare la VLAN associata alla rete.
Isolamento wireless con SSID	Selezionare questa casella per attivare l'isolamento wireless all'interno della rete SSID.
WMM (Wi-Fi Multimedia)	Selezionare questa casella per attivare WMM.

Pulsante hardware WPS	Selezionare questa casella per mappare a questa rete il pulsante WPS del router dispositivo sul pannello frontale.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione della modalità di protezione

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

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 consiglia l'utilizzo della protezione WPA2. Se si utilizza la modalità solo wireless N, è necessario utilizzare WPA2.

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

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella 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 decodificare. 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.

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 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 **Chiave di protezione**, immettere una frase alfanumerica (8-63 caratteri ASCII o 64 caratteri esadecimali). L'indicatore di complessità della password indica il grado di sicurezza offerto dalla password: inferiore al minimo, debole, buona, molto buona o sicura. Consigliamo l'uso di una chiave di sicurezza che risulti sicura sull'indicatore di complessità.

PASSAGGIO 7 Per mostrare la chiave di sicurezza inserita selezionare la casella **Password in chiaro**.

PASSAGGIO 8 Nel campo **Rinnovo chiave**, immettere l'intervallo temporale (600-7200 secondi) tra i rinnovi della chiave. Il valore predefinito è 3600.

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 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 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.

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 filtraggio MAC, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella 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 **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 su **Mostra elenco client**.

PASSAGGIO 6 Nel campo **Salva nell'elenco filtri indirizzo MAC**, selezionare la casella 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 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 **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.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione della rete ospite wireless

Il router dispositivo supporta una rete ospite wireless separata da altri SSID o reti wireless sul router. Questo router offre un acesso ospite protetto che è isolato dal resto della rete ed è configurabile per limitare il tempo di accesso e la larghezza di banda utilizzata. Vengono applicate le seguenti limitazioni e linee guida di configurazione:

- È possibile configurare una rete ospite per ciascun dispositivo.
- La rete ospite viene configurata come uno dei quattro SSID disponibili sul dispositivo.
- La rete ospite non può essere configurata sulla VLAN di gestione AP (ID 1 della VLAN).

Per configurare la rete ospite, attenersi alla seguente procedura:

Creare una nuova VLAN

PASSAGGIO 1 Nell'interfaccia di gestione selezionare **Networking** > **LAN** > **Appartenenza VLAN**.

PASSAGGIO 2 Nella tabella Impostazioni VLAN, aggiungere una nuova VLAN per la rete ospite. Ad esempio, fare clic su **Aggiungi riga** e immettere le seguenti informazioni:

- **ID VLAN**: immettere un numero per la VLAN (ad esempio **4**).
- **Descrizione**: immettere un nome per la VLAN (ad esempio **guest-net**).

PASSAGGIO 3 Lasciare le porte così come sono **contrassegnate** e fare clic su **Salva**.

Impostare la rete ospite

PASSAGGIO 1 Nell'interfaccia di gestione, selezionare **Wireless** > **Impostazioni di base**.

PASSAGGIO 2 Nella Tabella wireless, selezionare il SSID o la rete designata come rete ospite.

PASSAGGIO 3 Fare clic su **Modifica**. Modificare il nome SSID per rispecchiare la designazione "ospite" (ad esempio "*guest-net*").

PASSAGGIO 4 Selezionare la casella di controllo **Trasmissione SSID** di modo che la rete venga visualizzata come connessione wireless disponibile per i clienti in cerca di una rete.

PASSAGGIO 5 Selezionare la casella di controllo **Rete ospite** per configurare questo SSID come rete ospite.

PASSAGGIO 6 Selezionare la VLAN creata per la rete ospite (oppure, se non è ancora stata creata nessuna rete, selezionare **Aggiungi nuova VLAN**).

PASSAGGIO 7 Fare clic su **Salva**. Il sistema notifica che le porte Ethernet fisiche del router dispositivo sono escluse dalla VLAN assegnata alla rete ospite. Inoltre, le funzioni Isolamento wireless con SSID e WMM vengono attivate automaticamente.

Configurare la password e altre opzioni

PASSAGGIO 1 Nell'interfaccia di gestione, selezionare **Wireless** > **Impostazioni di base**.

PASSAGGIO 2 Nella Tabella wireless, fare clic su **Modifica rete ospite**.

PASSAGGIO 3 Immettere la password che gli utenti dovranno inserire per accedere alla rete ospite.

PASSAGGIO 4 Immettere nuovamente la password per confermarla.

PASSAGGIO 5 Immettere il tempo, in minuti, in cui la connessione ospite sarà disponibile agli utenti.

PASSAGGIO 6 (Opzionale) Per limitare l'utilizzo della larghezza di banda dalla rete ospite, selezionare **Attiva restrizione larghezza di banda ospite**. Prima è necessario attivare la funzione QoS: per configurarla, fare clic sul collegamento alla pagina relativa alla gestione della larghezza di banda. Nel campo **Larghezza di banda disponibile**, immettere il valore percentuale della larghezza di banda da allocare alla rete ospite.

PASSAGGIO 7 Fare clic su **Salva**.

Configurazione delle impostazioni wireless avanzate

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 Scegliere **Wireless** > **Impostazioni avanzate**. Viene visualizzata la pagina Impostazioni avanzate.

PASSAGGIO 2 Configurare le impostazioni seguenti:

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. Il router dispositivo 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 il router dispositivo può trasmettere a tutte le velocità standard wireless (1 Mb/s, 2 Mb/s, 5,5 Mb/s, 11 Mb/s, 18 Mb/s, 24 Mb/s, 36 Mb/s, 48 Mb/s e 54 Mb/s). Oltre alle velocità di trasmissione B e G, il router dispositivo supporta le velocità N. Le altre opzioni disponibili sono 1-2 Mbps, da utilizzare con dispositivi con tecnologia wireless meno recente, e Tutte, quando il router dispositivo 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 del router dispositivo, 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 il router dispositivo 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 il router dispositivo 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 il router dispositivo 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 il router dispositivo e un client wireless. L'impostazione predefinita è Auto.

Modalità di protezione CTS	Il router dispositivo 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 il router dispositivo in ambienti in cui è presente traffico 802.11b pesante. Questa funzione migliora la capacità del router dispositivo 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 dal router dispositivo 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 del router dispositivo 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 apportare solo riduzioni di lieve entità al valore predefinito. 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 (Request to Send) impostata, il meccanismo RTS/CTS (Request to Send) non viene attivato. La piattaforma Services Ready invia frame RTS 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 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 degli access point di una rete. Consente l'espansione di una rete wireless tramite access point multipli senza la necessità di fornire una backbone cablata per collegarli.

Per stabilire un collegamento WDS, il router dispositivo 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 o WEP).

WDS è supportato solo sui SSID 1.

Per configurare un WDS, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Wireless** > **WDS**.

PASSAGGIO 2 Selezionare la casella **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 **Manuale** o scegliere **Auto** in modo che il router identifichi automaticamente gli access point remoti.

Per selezionare i ripetitori dalla tabella Reti attive, fare clic su **Mostra analisi sito** per visualizzare la **Tabella reti disponibili**.

a. Fare clic sulle caselle di selezione per scegliere fino a tre access point da utilizzare come ripetitori.

b. Per aggiungere gli indirizzi MAC degli access point selezionati ai campi MAC, fare clic su **Connetti**.

È possibile immettere gli indirizzi MAC degli access point (fino a tre) da utilizzare come ripetitori nei campi **MAC 1**, **MAC 2** e **MAC 3**.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione di WPS

Configurare WPS in modo da consentire a tutti i dispositivi compatibili di connettersi alla rete wireless in maniera semplice e sicura. Fare riferimento al dispositivo client o alla relativa documentazione per ulteriori istruzioni su come configurare WPS sul dispositivo client.

Per configurare WPS:

PASSAGGIO 1 Scegliere **Wireless** > **WPS**. Viene visualizzata la pagina Wi-Fi Protected Setup.

PASSAGGIO 2 Selezionare la rete wireless per cui abilitare WPS dal menu a discesa **SSID**.

PASSAGGIO 3 Selezionare **Attiva WPS** per attivare il WPS. Per disattivare il WPS, deselezionare la casella.

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

a. Fare clic o premere il pulsante WPS sul dispositivo client, quindi fare clic sull'icona WPS di questa pagina.

b. Inserire il numero PIN WPS del client e fare clic su **Registra**.

c. Immettere un numero PIN per il router; utilizzare il numero PIN del router indicato.

Stato PIN dispositivo: stato del PIN del dispositivo WPA.

PIN dispositivo: identifica il PIN di un dispositivo che sta cercando di connettersi.

Validità PIN: la validità della chiave. Alla scadenza viene negoziata una nuova chiave.

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

5

Configurazione del firewall

In questo capitolo viene spiegato come configurare le funzionalità firewall del dispositivo.

Funzioni del firewall Cisco RV215W

La rete può essere protetta creando e applicando regole che il dispositivo 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 i tipi di traffico (esempi: esplorazione del Web, VoIP, altri servizi standard e servizi personalizzati definiti dall'utente) 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 viene denominata "esposizione dell'host". Il modo di comunicare l'indirizzo dell'utente dipende dalla configurazione delle porte WAN. Per il dispositivo, è possibile utilizzare l'indirizzo IP se alla porta WAN è assegnato un indirizzo statico oppure 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 **Attiva** per attivare le impostazioni firewall.
Protezione DoS	Selezionare **Attiva** per attivare la protezione Denial of Service.
Blocco richiesta WAN	Blocca le richieste ping inviate dalla WAN al dispositivo.
Accesso Web	Selezionare il tipo di accesso Web che può essere utilizzato per collegarsi al firewall: HTTP o HTTPS (HTTP protetto).
Gestione remota **Accesso remoto** **Aggiornamento remoto** **Indirizzo IP remoto consentito** **Porta di gestione remota**	Vedere la sezione **Configurazione della gestione remota**.
Multicast Passthrough IPv4 (proxy IGMP)	Selezionare **Attiva** per attivare il passtrough multicast per l'IPv4.
Multicast Passthrough IPv6 (proxy IGMP)	Selezionare **Attiva** per attivare il passtrough multicast per l'IPv6.
UPnP **Consenti agli utenti di configurare** **Consenti agli utenti di disabilitare l'accesso Internet**	Vedere la sezione **Configurazione di Universal Plug and Play**.

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. 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 viene bloccato dalla regola, rendendo quindi inefficace la limitazione. L'attivazione di questa funzione 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.
ALG FTP	Fare clic su **Automatico** per utilizzare la porta 21 di FTP predefinita. Fare clic su **Manuale** per immettere il numero di porta tramite cui si desidera reindirizzare il traffico FTP sul dispositivo.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione della gestione remota

È possibile attivare la gestione remota per consentire l'accesso al dispositivo da una rete WAN remota.

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

Gestione remota	Selezionare **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 (HTTP protetto).

Aggiornamento remoto	Per attivare gli aggiornamenti remoti del dispositivo, selezionare **Attiva**.
Indirizzo IP remoto consentito	Fare clic su **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. La porta predefinita è 443. Se si accede da remoto al router, è necessario inserire la porta di gestione remota nell'indirizzo IP. Ad esempio: **https://<remote-ip>:<remote-port>** oppure **https://168.10.1.11:443**

CAUTION Quando la gestione remota viene attivata, il router diventa accessibile a chiunque conosca il suo indirizzo IP. Dato che un utente WAN malintenzionato potrebbe riconfigurare il dispositivo 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 il dispositivo.

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

UPnP	Selezionare **Attiva** per attivare UPnP.
Consenti agli utenti di configurare	Selezionare questa casella 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 viene disattivata, il dispositivo non consente all'applicazione di aggiungere la regola di reindirizzamento.
Consenti agli utenti di disabilitare l'accesso Internet	Selezionare questa casella 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.

Aggiunta o modifica di una pianificazione del firewall

Per creare o modificare una pianificazione, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Firewall** > **Gestione pianificazioni**.

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**).

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 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 nella tabella **Elenco dei servizi personalizzati disposnibili**.

Per creare un servizio personalizzato, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Firewall** > **Gestione servizi**.

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

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 Scegliere **Firewall** > **Regole di accesso**.

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

Nota: per configurare un firewall IPv6 accertarsi che sul dispositivo sia abilitato il supporto per IPv6. Vedere la sezione **Configurazione di IPv6**.

PASSAGGIO 3 Fare clic su **Salva**.

Riordinamento delle regole di accesso

L'ordine di visualizzazione delle regole di accesso nella tabella corrispondente indica l'ordine in cui tali regole vengono applicate. È possibile assegnare un nuovo ordine alla tabella se si desidera che alcune regole vengano applicate prima di altre, Ad esempio, è pissibile applicare una regola che consenta certi tipi di traffico prima di bloccarne altri.

Per riordinare le regole di accesso, attenersi alla seguente procedura:

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

PASSAGGIO 2 Fare clic su **Riordina**.

PASSAGGIO 3 Selezionare la casella di controllo nella riga della regola da spostare in alto o in basso, quindi fare clic sulla freccia corrispondente per spostare la regola in alto o in basso, oppure selezionare la posizione desiderata per la regola nell'elenco a discesa e fare clic su **Sposta in**.

PASSAGGIO 4 Fare clic su **Salva**.

Aggiunta di regole di accesso

Tutte le regole di accesso configurate per il dispositivo sono disponibili nella **Tabella regole di accesso**. Questo elenco mostra anche se la regola è abilitata (attiva) e fornisce un riepilogo della zona "da/a", dei servizi e degli utenti coinvolti dalla regola.

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

PASSAGGIO 1 Scegliere **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 per pianificazione**: blocca il tipo di traffico selezionato in base a una pianificazione.
- **Consenti per pianificazione**: 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**.

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

PASSAGGIO 11 Fare clic su **Salva**.

Creazione di un criterio di accesso a Internet

Il dispositivo supporta diverse opzioni per bloccare l'accesso a Internet. È possibile bloccare tutto il traffico Internet, bloccare il traffico Internet di certi PC o punti terminali o bloccare l'accesso a Internet specificando 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.

Aggiunta o modifica di un criterio di accesso a 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 traffico Internet. Questa opzione consente di bloccare il traffico Internet da e verso tutti i punti terminali. Se si desidera bloccare tutto il traffico, pur consentendo ad alcuni punti terminali di ricevere traffico Internet, vedere il passaggio 7.
- **Consenti sempre**: consente sempre il traffico Internet. È possibile perfezionare questa opzione per bloccare punti terminali specifici dal traffico Internet; vedere il passaggio 7. Inoltre, è possibile consentire il traffico Internet tranne che per alcuni siti Web; vedere il passaggio 8.
- **Blocca per pianificazione**: blocca il traffico Internet in base a una pianificazione (ad esempio, per bloccare il traffico Internet durante le ore lavorative della settimana, pur consentendo la navigazione dopo le ore lavorative e nei weekend).
- **Consenti per pianificazione**: consente il traffico Internet 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**.

PASSAGGIO 6 Selezionare una pianificazione dal menu a discesa.

PASSAGGIO 7 (Opzionale) Applicare il criterio di accesso a PC specifici per 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, 192.168.1.2-192.168.10,253.

PASSAGGIO 8 Per bloccare il traffico da siti Web specifici, attenersi alla seguente procedura:

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 9 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 dato che 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 i dispositivi esterni si collegano. 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 Nel menu a discesa Interfaccia, selezionare **Entrambi (Ethernet e 3G)**, **Ethernet** o **3G**.

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 dell'host lato LAN al quale viene inoltrato lo specifico traffico IP. Ad esempio, è possibile inoltrare il traffico HTTP alla porta 80 dell'indirizzo di un server Web lato LAN.

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

PASSAGGIO 9 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 Nel menu a discesa Interfaccia, selezionare **Entrambi (Ethernet e 3G)**, **Ethernet** o **3G**.

PASSAGGIO 7 Dal menu a discesa **Protocollo**, selezionare un protocollo (**TCP**, **UDP** o **TCP** e **UDP**).

PASSAGGIO 8 Nel campo **Indirizzo IP**, immettere l'indirizzo IP dell'host lato LAN al quale viene inoltrato lo specifico traffico IP.

PASSAGGIO 9 Nel campo **Attiva**, selezionare la casella **Attiva** per attivare la regola.

PASSAGGIO 10 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 da parte di un'applicazione 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) dato che una regola non deve fare riferimento a un indirizzo o a un intervallo IP LAN 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 visto che 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 i dispositivi esterni si collegano. 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 **Intervalli 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 **Intervalli 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 menu a discesa Interfaccia, selezionare **Entrambi (Ethernet e 3G)**, **Ethernet** o **3G**.

PASSAGGIO 6 Nel campo **Attiva**, selezionare la casella **Attiva** per attivare la regola.

PASSAGGIO 7 Fare clic su **Salva**.

6

Configurazione VPN

In questo capitolo viene spiegato come configurare la VPN e la protezione del dispositivo.

Tipi di tunnel VPN

Una rete VPN offre un canale di comunicazione sicuro (tunnel) tra due router gateway oppure tra un lavoratore remoto e un router gateway. È possibile creare diversi tipi di tunnel VPN a seconda delle esigenze dell'azienda. Di seguito vengono descritti vari scenari. Leggere le descrizioni seguenti per comprendere le opzioni e i passaggi necessari per impostare la propria VPN.

Accesso remoto tramite PPTP

In questo scenario, un utente remoto con un computer Microsoft si connette a un server PPTP presso la sede dell'utente per accedere alle risorse di rete. Utilizzare questa opzione per semplificare l'impostazione della VPN. Non è necessario configurare i criteri VPN. Gli utenti remoti possono collegarsi utilizzando il client PPTP da un computer Microsoft. Non è necessario installare un client VPN. Tuttavia, per questo protocollo sono state riscontrate delle vulnerabilità della protezione.

Accesso remoto con Cisco QuickVPN

Per una rapida configurazione con impostazioni di protezione VPN di base, distribuire il software Cisco QuickVPN agli utenti, che potranno quindi accedere in sicurezza alle risorse di rete. Utilizzare questa opzione se si desidera semplificare la procedura di impostazione della VPN. Non è necessario configurare i criteri VPN. Gli utenti remoti possono connettersi in sicurezza con il client Cisco QuickVPN e una connessione Internet.

VPN sito a sito

Il dispositivo supporta la funzionalità VPN sito a sito per un tunnel VPN gateway a gateway singolo. Ad esempio, è possibile configurare il dispositivo al sito di una filiale per connettere il router al sito aziendale, così che il sito della filiale possa accedere in tutta sicurezza alla rete aziendale. La funzionalità VPN sito a sito è configurata nella pagina **VPN** > **Impostazione VPN di base**.

Client VPN

Il software del client VPN è necessario per stabilire un tunnel VPN fra il router e l'endpoint remoto. Il dispositivo supporta i client Cisco QuickVPN e PPTP VPN.

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 dispositivo, la sottorete LAN del dispositivo 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 Immettere le seguenti informazioni:

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. La crittografia MPPE (Microsoft Point-to-Point Encryption) viene utilizzata quando gli utenti configurano e utilizzano il client VPN PPTP per connettersi al dispositivo.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione di QuickVPN

PASSAGGIO 1 Aggiungere gli utenti QuickVPN nella pagina **VPN > Client VPN** . Vedere le sezioni **Importazioni delle impostazioni client VPN** e **Creazione e gestione degli utenti QuickVPN**.

PASSAGGIO 2 Indicare agli utenti di scaricare il software gratuito Cisco QuickVPN dal sito Cisco.com e di installarlo sui propri computer. Vedere la sezione **Utilizzo del software Cisco QuickVPN**.

PASSAGGIO 3 Per attivare l'accesso tramite Cisco QuickVPN sul dispositivo, è necessario attivare la gestione remota per l'apertura della porta 443 per SSL. Vedere la sezione **Configurazione delle impostazioni firewall di base**.

Configurazione NetBIOS su VPN

Per attivare Netbios su VPN, attenersi alla seguente procedura:

PASSAGGIO 1 Nel campo **NetBIOS su VPN**, selezionare la casella per consentire il passaggio dei broadcast NetBIOS nel tunnel VPN. Per impostazione predefinita, la funzione NetBIOS è disponibile per i criteri del client.

PASSAGGIO 2 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 un utente **PPTP** dal menu a discesa.

PASSAGGIO 3 Fare clic su **Salva**.

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

Per eliminare un utente PPTP, selezionare la relativa casella 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:

PASSAGGIO 3 Fare clic su **Salva**.

Per modificare le impostazioni di un utente QuickVPN, selezionare la relativa casella e fare clic su **Modifica**. Effettuare le modifiche, quindi fare clic su **Salva**.

Per eliminare un utente QuickVPN, selezionare la relativa casella, fare clic su **Elimina**, quindi su **Salva**.

Per ulteriori informazioni su QuickVPN, vedere **Appendice A, Utilizzo del software 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 un programma come Microsoft 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 da importare:

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

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

Per riportare 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 delle impostazioni VPN IPsec sito a sito di base

Il dispositivo supporta la funzionalità VPN sito a sito per un tunnel VPN gateway a gateway singolo. In questa configurazione, il dispositivo consente di creare una connessione protetta a un altro router con abilitazione VPN. Ad esempio, è possibile configurare il dispositivo al sito di una filiale per connettere il router al sito aziendale, così che il sito della filiale possa accedere in tutta sicurezza alla rete aziendale.

Per configurare le impostazioni VPN di base per una connessione sito a sito, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **VPN** > **Impostazione VPN di base**.

PASSAGGIO 2 Nel campo **Nome connessione**, immettere il nome del tunnel VPN.

PASSAGGIO 3 Nel campo **Chiave pre-condivisa**, immettere la chiave pre-condivisa, o la password, che verrà scambiata tra due router. Il numero di caratteri deve essere compreso tra 8 e 49.

PASSAGGIO 4 Nel campo **Informazioni endpoint**, immettere le seguenti informazioni:

- **Punto finale remoto**: scegliere il metodo di identificazione del punto finale remoto o del router a cui il dispositivo si collegherà. Ad esempio, con un indirizzo IP come 192.168.1.1 oppure con un nome di dominio completo come cisco.com.
- **Indirizzo IP (Internet) WAN remoto**: immettere l'indirizzo IP pubblico o il nome di dominio dell'endpoint remoto.
- **Punto finale di ridondanza**: per consentire al dispositivo di passare a un gateway alternativo quando la connessione VPN principale non funziona, selezionare la casella di controllo **Attiva**. Immettere l'indirizzo IP WAN oppure il FQDN per il punto finale di ridondanza.
- **Indirizzo IP (Internet) WAN locale**: immettere l'indirizzo IP pubblico o il nome di dominio dell'endpoint locale (dispositivo).

PASSAGGIO 5 Nei campi **Accessibilità remota connessione protetta**, immettere le seguenti informazioni:

- **Indirizzo IP (rete locale) LAN remoto**: immettere l'indirizzo (LAN) della rete privata dell'endpoint remoto. Si tratta dell'indirizzo IP della rete interna al sito remoto.

- **Subnet mask LAN remota**: immettere la subnet mask (LAN) della rete privata dell'endpoint remoto.
- **Indirizzo IP (rete locale) LAN locale**: immettere l'indirizzo (LAN) della rete privata appartenente alla rete locale. Si tratta dell'indirizzo IP della rete interna sul router dispositivo.
- **Subnet mask (rete locale) LAN locale**: immettere la subnet mask (LAN) della rete privata appartenente alla rete locale (dispositivo).

Nota: gli indirizzi IP LAN e WAN remoti non possono coesistere nella stessa sottorete. Ad esempio, un indirizzo IP LAN remoto di 192.168.1.100 e un indirizzo IP LAN locale di 192.168.1.115 causerebbero un conflitto quando il traffico viene indirizzato sulla VPN. Il terzo ottetto deve essere differente affinché gli indirizzi IP siano su sottoreti diverse. Ad esempio, un indirizzo IP LAN remoto di 192.168.1.100 e un indirizzo IP LAN locale di 192.168.2.100 sono accettabili.

PASSAGGIO 6 Fare clic su **Salva**.

Visualizzazione dei valori predefiniti

I valori predefiniti utilizzati nelle impostazioni VPN di base sono quelli proposti da VPNC; tali valori presumono l'utilizzo di una chiave pre-condivisa o di una password, conosciuta dal dispositivo e dal router all'altra estremità (ad esempio, un dispositivo Cisco RV220W). Per visualizzare i valori predefiniti, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **VPN** > **Impostazione VPN di base**.

PASSAGGIO 2 Fare clic su **Visualizza impostazioni predefinite** al fine di visualizzare i valori predefinti.

Per ulteriori informazioni su questi valori, vedere la sezione **Configurazione dei parametri VPN avanzati**.

Configurazione dei parametri VPN avanzati

Nella pagina Impostazione VPN avanzata è possibile configurare i parametri avanzati della VPN, come IKE e altri criteri VPN. Questi criteri consentono di controllare il modo in cui il dispositivo stabilisce e riceve le connessioni VPN con altri punti finali.

Gestione dei criteri IKE

Il protocollo IKE (Internet Key Exchange) consente lo scambio dinamico di chiavi fra due host IPsec. È possibile creare criteri IKE per definire i parametri di protezione da utilizzare in questo processo, come l'autenticazione dei peer e gli algoritmi di crittografia. Per il criterio VPN, assicurarsi di utilizzare una crittografia, un'autenticazione e parametri di gruppo chiave compatibili.

PASSAGGIO 1 Scegliere **VPN** > **IPsec** > **Impostazione VPN avanzata**.

PASSAGGIO 2 Nella **Tabella criteri VPN**, la selezione della casella di controllo nella riga della connessione VPN consente di eseguire le seguenti operazioni:

- **Aggiungi riga** o**Modifica**: consente di modificare le proprietà del criterio IKE. Vedere la sezione **Aggiunta o modifica di criteri IKE**.
- **Attiva**: consente di attivare il criterio.
- **Disattiva**: consente di disattivare il criterio.
- **Elimina**: consente di eliminare il criterio.

NOTA Non è possibile eliminare un criterio IKE se utilizzato in un criterio VPN. Prima è necessario disattivare e rimuovere il criterio VPN nella tabella **Criterio VPN**.

- **Aggiungi riga**: consente di aggiungere un criterio IKE. Vedere la sezione **Aggiunta o modifica di criteri IKE**.

NOTA Se è già stata configurata una connessione VPN, non è possibile aggiungerne un'altra senza prima eliminare quella esistente.

PASSAGGIO 3 Fare clic su **Salva**.

Aggiunta o modifica di criteri IKE

PASSAGGIO 1 Quando si aggiungono o modificano criteri IKE, configurare le seguenti impostazioni:

- **Nome criterio**: immettere un nome univoco per il criterio a fini di identificazione e gestione.
- **Modalità di scambio**: scegliere una delle seguenti opzioni:
  - **Principale**: consente di negoziare il tunnel con una protezione di livello superiore, ma a una minore velocità.
  - **Aggressiva**: stabilisce una connessione più veloce, ma con un livello di protezione inferiore.
- **Identificatore locale**: identificatore IKE locale.
- **Identificatore remoto**: identificatore IKE remoto.
- **Identificatore di ridondanza**: l'identificatore univoco per il punto finale di backup alternativo utilizzato per ripristinare la connessione quando la connessione VPN originale non funziona.

PASSAGGIO 2 Nella sezione **Parametri SA IKE**, i parametri SA (Security Association) definiscono la potenza e la modalità per la negoziazione della SA. È possibile configurare le seguenti impostazioni:

- **Algoritmo di crittografia**: scegliere l'algoritmo utilizzato per negoziare la SA:
  - **DES**
  - **3DES**
  - **AES-128**
  - **AES-192**
  - **AES-256**
- **Algoritmo di autenticazione**: specificare l'algoritmo di autenticazione per l'intestazione VPN:
  - **MD5**
  - **SHA-1**

- **SHA2-256**

  Assicurarsi che l'algoritmo di autenticazione sia configurato allo stesso modo su entrambe le estremità del tunnel VPN (ad esempio, il dispositivo e il router a cui si connette).

- **Chiave pre-condivisa**: immettere la chiave nello spazio fornito. La chiave pre-condivisa non supporta il carattere virgolette (").
- **Gruppo Diffie-Hellman (DH)**: specificare l'algoritmo del gruppo DH utilizzato durante lo scambio delle chiavi. Il gruppo DH imposta la potenza dell'algoritmo in termini di bit. Assicurarsi che il gruppo DH sia configurato in maniera identica su entrambi i lati del criterio IKE.
- **Durata SA**: immettere l'intervallo in secondi passato il quale la SA (Security Association) non sarà più valida.
- **DPD (Dead Peer Detection)**: selezionare la casella **Attiva** per attivare questa funzione oppure deselezionarla per disattivarla. La funzione DPD viene utilizzata per rilevare se un peer è attivo o meno. Se il peer viene rilevato come inattivo, il router elimina la SA (Security Association) IPsec e IKE. Se è stata attivata la funzione, immettere anche queste impostazioni:
  - **Ritardo DPD**: immettere l'intervallo in secondi che intercorre tra messaggi DPD R-U-THERE consecutivi. I messaggi DPD R-U-THERE vengono inviati solo quando il traffico IPsec è inattivo.
  - **Timeout DPD**: immettere il tempo massimo di attesa del dispositivo per ottenere una risposta al messaggio DPD prima di considerare il peer inattivo.

PASSAGGIO 3 Selezionare la casella di controllo **Attiva tipo XAUTH** per configurare l'autenticazione estesa per il criterio VPN IPsec. Fornire il nome utente e la password di autenticazione.

PASSAGGIO 4 Fare clic su **Salva**.

Gestione dei criteri VPN

Per gestire i criteri VPN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **VPN** > **IPsec** > **Impostazione VPN avanzata**.

PASSAGGIO 2 Nella **Tabella criteri VPN**, la selezione della casella di controllo nella riga della connessione VPN consente di eseguire le seguenti operazioni:

- **Aggiungi riga** o**Modifica**: consente di modificare le proprietà del criterio VPN. Vedere la sezione **Aggiunta o modifica di criteri VPN**.
- **Attiva**: consente di attivare il criterio.
- **Disattiva**: consente di disattivare il criterio.
- **Elimina**: consente di eliminare il criterio.
- **Aggiungi riga**: consente di aggiungere un criterio VPN. Vedere la sezione **Aggiunta o modifica di criteri VPN**.

NOTA Se è già stata configurata una connessione VPN, non è possibile aggiungerne un'altra senza prima eliminare quella esistente.

PASSAGGIO 3 Fare clic su **Salva**.

Aggiunta o modifica di criteri VPN

Per creare un criterio VPN automatico, per prima cosa è necessario creare un criterio IKE, quindi aggiungere il criterio automatico corrispondente per quel criterio IKE.

Quando si aggiunge o modifica un criterio VPN, è possibile configurare le seguenti impostazioni:

- **Nome criterio**: immettere un nome univoco che identifichi il criterio.
- **Tipo di criterio**: scegliere una delle seguenti opzioni:
  - **Criterio automatico**: alcuni parametri del tunnel VPN vengono generati automaticamente. Tale operazione richiede l'utilizzo del protocollo IKE (Internet Key Exchange) per eseguire le negoziazioni tra i due endpoint della VPN.
  - **Criterio manuale**: tutte le impostazioni (comprese le chiavi) di un tunnel VPN vengono inserite manualmente per ciascun endpoint. In questa operazione non viene coinvolto alcun server o organizzazione di terze parti.
- **Endpoint remoto**: selezionare il tipo di identificatore da fornire al gateway nell'endpoint remoto: **Indirizzo IP** o **FQDN** (nome di dominio completo). Immettere l'identificatore nello spazio fornito.
- **Punto finale di ridondanza:** per consentire al dispositivo di passare a un gateway alternativo quando la connessione VPN principale non funziona,

selezionare la casella di controllo **Attiva**. Immettere l'indirizzo IP WAN oppure il FQDN per il punto finale di ridondanza.

Per tornare automaticamente al VPN primario, una volta ripristinata la connessione, selezionare la casella di controllo **Attiva rollback**.

Nella sezione **Selezione traffico locale** e **Selezione traffico remoto**, immettere le seguenti impostazioni:

- **IP locale/remoto**: selezionare il tipo di identificatore da fornire per l'endpoint:
  - **Singolo**: limita il criterio a un unico host. Nel campo Indirizzo IP iniziale, immettere l'indirizzo IP dell'host che farà parte della VPN. Immettere l'indirizzo IP nel campo **Indirizzo iniziale**.
  - **Sottorete**: consente a un'intera sottorete di connettersi alla rete VPN. Immettere l'indirizzo di rete nel campo Indirizzo IP iniziale, quindi immettere la subnet mask nel campo Subnet mask. Immettere l'indirizzo IP di rete della sottorete nel campo **Indirizzo iniziale**. Immettere la subnet mask, ad esempio 255.255.255.0, nel campo **Subnet mask**. Nel campo viene visualizzato automaticamente un indirizzo di sottorete predefinito in base all'indirizzo IP.

    IMPORTANTE: assicurarsi di non utilizzare sottoreti sovrapposte per i selettori del traffico locale o remoto. L'utilizzo di queste sottoreti richiederebbe l'aggiunta di percorsi statici sul router e sugli host da utilizzare. Evitare, ad esempio, combinazioni di questo tipo:

    Selettore del traffico locale: 192.168.1.0/24

    Selettore del traffico remoto: 192.168.0.0/16

Per un tipo di criterio **manuale**, immettere le impostazioni nella sezione **Parametri criterio manuale**:

- **SPI in arrivo, SPI in uscita**: immettere un valore esadecimale di lunghezza compresa tra 3 e 8 caratteri (ad esempio 0x1234).
- **Algoritmo di crittografia**: selezionare l'algoritmo utilizzato per crittografare i dati:
  - DES
  - 3DES
  - AES-128
  - AES-192

- AES-256

- **Chiave ingresso**: immettere la chiave di crittografia del criterio in arrivo. La lunghezza della chiave dipende dall'algoritmo di crittografia selezionato:
  - DES, 8 caratteri
  - 3DES, 24 caratteri
  - AES-128, 16 caratteri
  - AES-192, 24 caratteri
  - AES-256, 32 caratteri
- **Chiave uscita**: immettere la chiave di crittografia del criterio in uscita. La lunghezza della chiave dipende dall'algoritmo di crittografia selezionato, come indicato sopra.
- **Algoritmo di integrità**: selezionare l'algoritmo utilizzato per verificare l'integrità dei dati.
  - MD5
  - SHA-1
  - SHA2-256
- **Chiave ingresso**: immettere la chiave di integrità (per l'ESP con modalità di integrità) per il criterio in arrivo. La lunghezza della chiave dipende dall'algoritmo scelto:
  - MD5, 16 caratteri
  - SHA-1, 20 caratteri
  - SHA2-256, 32 caratteri
- **Chiave uscita**: immettere la chiave di integrità (per l'ESP con modalità di integrità) per il criterio in uscita. La lunghezza della chiave dipende dall'algoritmo scelto, come indicato sopra.

Per un tipo di criterio **automatico**, immettere le impostazioni nella sezione **Parametri criterio automatico**.

- **Durata SA**: immettere la durata della SA (Security Association) in secondi. Una volta trascorso il numero di secondi specificato, la SA (Security Association) viene rinegoziata. Il valore predefinito è 3.600 secondi. Il valore minimo è 300 secondi.

- **Algoritmo di crittografia**: selezionare l'algoritmo utilizzato per crittografare i dati.
- **Algoritmo di integrità**: selezionare l'algoritmo utilizzato per verificare l'integrità dei dati.
- **Gruppo chiave PFS**: selezionare la casella **Attiva** per attivare la PFS (Perfect Forward Secrecy), in modo da migliorare la protezione. Seppur lento, questo protocollo aiuta a impedire gli ascolti indesiderati garantendo l'esecuzione di uno scambio Diffie-Hellman per ogni negoziazione di fase 2.
- **Seleziona il criterio IKE**: scegliere il criterio IKE che definirà le caratteristiche della fase 1 della negoziazione. Fare clic su **Visualizza** per visualizzare o modificare il criterio IKE esistente che è stato configurato sul dispositivo.

Configurazione della gestione dei certificati

Il dispositivo utilizza certificati digitali per l'autenticazione VPN IPsec e la convalida SSL (per HTTPS). È possibile generare e firmare certificati personalizzati utilizzando le funzioni del dispositivo.

Generazione di un nuovo certificato

È possibile generare un nuovo certificato che sostituisca quello esistente per il dispositivo.

Per generare un certificato, attenersi alla seguente procedura:

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

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

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

PASSAGGIO 4 Fare clic su **Installa certificato automatico attivo**.

Esportazione di certificati per l'amministratore

È possibile esportare il certificato per l'amministratore in una cartella sul computer o in una posizione esterna su un'unità USB. Il certificato per l'amministratore contiene la chiave privata e dovrebbe essere memorizzato in un luogo sicuro come backup. Se vengono ripristinate le impostazioni di fabbrica del dispositivo, 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 Per esportare il certificato sul computer, fare clic su **Esporta per amministratore**. Device Manager salva il file admin.pem in C:\Documents and Settings\userid\My Documents\Downloads.

Per esportare il certificato su un'unità USB esterna, fare clic su **Esporta a USB per l'amministratore**.

Esportazione del certificato per il client

È possibile esportare i certificati per i client sul computer o in una posizione esterna su un'unità USB. Il certificato per il client consente agli utenti QuickVPN di connettersi in modo sicuro a Cisco RV215W. 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 Per esportare il certificato sul computer, fare clic su **Esporta per il client**. Su un PC, Device Manager salva il file client.pem in C:\Documents and Settings\userid\My Documents\Downloads.

Per esportare il certificato su un'unità USB esterna, fare clic su **Esporta a USB per il client**.

Configurazione del passthrough VPN

Il passthrough VPN consente il passaggio del traffico VPN generato dai client VPN attraverso il dispositivo.

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 il dispositivo.
PPTP	Selezionare **Attiva** per consentire il passaggio dei tunnel PPTP attraverso il dispositivo.
L2TP	Selezionare **Attiva** per consentire il passaggio dei tunnel L2TP (Layer 2 Tunneling Protocol) attraverso il dispositivo.

PASSAGGIO 3 Fare clic su **Salva**.

7

Configurazione della Qualità del servizio (QoS)

Cisco RV215W consente la configurazione delle seguenti funzioni QoS (Qualità del servizio):

QoS assegna la priorità ad applicazioni, utenti o flussi di dati, oppure garantisce un determinato livello di prestazioni per un flusso di dati. Tale garanzia è importante in caso di capacità di rete insufficiente. Soprattutto per le applicazioni multimediali in streaming in tempo reale, come voice-over-IP, giochi online e IPTV, dal momento che questo tipo di servizi richiede spesso una velocità di dati fissa ed è molto sensibile in termini di ritardi, oltre che nelle reti limitate in termini di capacità, ad esempio per quanto riguarda le comunicazioni dati cellulari.

Configurazione della gestione della larghezza di banda

È possibile utilizzare la funzione di gestione della larghezza di banda del dispositivo per gestire la larghezza di banda del traffico dalla rete sicura (LAN) alla rete non sicura (WAN).

Configurazione della larghezza di banda

È possibile limitare la larghezza di banda per ridurre la velocità con cui il dispositivo 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 **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 **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 e fare clic su **Modifica**. Una volta terminate le modifiche, fare clic su **Salva**.

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

Configurazione delle impostazioni di QoS basato su porta

È possibile configurare le impostazioni QoS per ogni porta LAN del router Cisco RV215W. Il dispositivo 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 del dispositivo, 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 funzione, 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 Per ciascuna porta della **Tabella impostazioni QoS 3G 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 funzione, 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 4 Fare clic su **Salva**.

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

Configurazione delle impostazioni CoS

Utilizzare il collegamento alla pagina Impostazioni QoS basato su porta per mappare le impostazioni di priorità CoS alla coda QoS.

Per associare le impostazioni di priorità CoS alla coda di reindirizzamento del traffico, attenersi alla seguente procedura:

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

PASSAGGIO 2 Selezionare il pulsante di opzione **Ethernet** o **3G**.

PASSAGGIO 3 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 4 Fare clic su **Salva**.

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

Configurazione delle impostazioni DSCP

Utilizzare la pagina **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 Selezionare il pulsante di opzione **Ethernet** o **3G**.

PASSAGGIO 3 Scegliere se elencare solo i valori RFC o tutti i valori DSCP nella **tabella delle impostazioni DSCP** facendo clic sul pulsante appropriato.

PASSAGGIO 4 Per ciascun valore DSCP nella **tabella delle impostazioni DSCP**, selezionare un livello di priorità dal menu a discesa **Coda**.

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

PASSAGGIO 5 Fare clic su **Salva**.

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

8

Amministrazione del router

In questo capitolo vengono descritte le funzionalità relative all'amministrazione del dispositivo, 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 password

Sul dispositivo 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 **Attiva**.

PASSAGGIO 3 Configurare le impostazioni di complessità password.

Lunghezza minima password	Immettere la lunghezza minima della password (da 0 a 64 caratteri).
Numero minimo classi di caratteri	Immettere un numero che rappresenti una delle seguenti classi di carattere: • Lettere maiuscole • Lettere minuscole • Numeri • 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 **Attiva** per impedire che la nuova password sia uguale a quella corrente.
Scadenza password	Selezionare **Attiva** per impostare la scadenza delle password dopo un determinato periodo.
Durata 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

Il dispositivo supporta due account utente per le impostazioni di amministrazione e visualizzazione: un utente amministrativo (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 Nel campo **Attivazione account**, selezionare le caselle per gli account che si desidera attivare (l'account amministratore deve essere attivo).

PASSAGGIO 3 (Opzionale) Per modificare l'account amministratore, sotto **Impostazione account amministratore** selezionare **Modifica impostazioni amministratore**. Per modificare l'account ospite, sotto **Impostazioni ospite** selezionare **Modifica impostazioni ospite**. Immettere le seguenti informazioni:

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 64 caratteri.
Digita di nuovo la nuova password	Immettere nuovamente la nuova password.

PASSAGGIO 4 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 5 Immettere la vecchia password.

PASSAGGIO 6 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. Scegliere **mai** per consentire all'amministratore di rimanere sempre connesso.

PASSAGGIO 3 Nel campo **Timeout inattività ospite**, immettere il numero, in minuti, dopo il quale la sessione verrà terminata per inattività. Scegliere **mai** per consentire all'amministratore di rimanere sempre connesso.

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

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

Prima di usare SNMP, installare il software SNMP sul computer. Il dispositivo supporta solo SNMPv3 per la gestione SNMP e SNNPv1/2/3 per i messaggi trap SNMP.

Per attivare SNMP, attenersi alla seguente procedura:

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

PASSAGGIO 2 Selezionare **Attiva** per attivare SNMP.

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 del dispositivo (Amministratore 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 dei 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 i 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

Il dispositivo mette a disposizione diversi strumenti di diagnostica per la risoluzione dei problemi di rete.

- **Strumenti di rete**
- **Configurazione del mirroring delle porte**

Strumenti di rete

Utilizzare gli strumenti di rete per risolvere gli errori di rete.

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**.

Utilizzo di Traceroute

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

Esecuzione di 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" indica 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 evitare problemi con il mirroring delle porte, l'host LAN deve utilizzare un indirizzo IP statico. Se non viene configurato un indirizzo IP statico per l'host LAN, i lease DHCP possono scadere per l'host LAN e provocare errori di mirroring della porta.

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. Se si utilizza una porta per il mirroring, non usarla per altri tipi di traffico.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione della registrazione

Sul router Cisco RV215W è possibile configurare le opzioni di registrazione.

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:

Server di log remoto	Immettere l'indirizzo IP del server che raccoglie i registri.
Gravità log per log locale ed e-mail	Fare clic per selezionare la gravità dei registri da configurare. Tutti i tipi di registri sopra un tipo di registro selezionato vengono inclusi automaticamente e non è possibile deselezionarli. Ad esempio, la scelta di log di errore include automaticamente anche i log di emergenza, allarme e critici. I livelli di gravità degli eventi sono elencati dalla gravità maggiore alla minore, come indicato di seguito: • **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. La selezione di questa gravità prevede la generazione di grandi quantità di registri ed è sconsigliata durante il normale funzionamento del router.
Attiva	Per attivare le informazioni di registrazione, selezionare questa casella.

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 delle impostazioni e-mail

È possibile configurare Cisco RV215W per inviare log di eventi, avvisi di nuovi firmware e avvisi 3G tramite e-mail. Si consiglia di configurare un account e-mail a parte per l'invio e la ricezione degli avvisi tramite e-mail.

Per configurare le impostazioni e-mail, attenersi alla seguente procedura:

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

PASSAGGIO 2 Nella sezione **Configurazione avvisi tramite e-mail**:

- Per abilitare l'invio di eventi 3G tramite e-mail, selezionare la casella di controllo **Abilita avvisi 3G tramite e-mail**.
- Per abilitare l'invio di log tramite e-mail, selezionare la casella di controllo **Log di e-mail Abilita.** Verificare di aver impostato il livello di gravità per gli eventi che si desidera registrare. Per ulteriori informazioni, vedere la sezione **Configurazione delle impostazioni di registrazione**. Il campo **Gravità minima dei log e-mail** indica il livello di gravità dei log che si desidera acquisire. Per modificare il livello di gravità dei log, fare clic su **Configura gravità**.

  Nella sezione **Invia log tramite e-mail in base a pianificazione**, selezionare se si desidera inviare l'e-mail **Ogni ora**, **Ogni giorno** oppure **Ogni settimana**. Se si seleziona **Mai**, i registri non vengono inviati. Se si sceglie un programma settimanale, selezionare il giorno della settimana in cui inviare i log. Se si sceglie un programma settimanale o giornaliero, selezionare l'ora in cui il dispositivo deve inviare i log.

PASSAGGIO 3 Nella sezione **Impostazioni e-mail**, immettere le seguenti informazioni per configurare le impostazioni per gli avvisi tramite e-mail:

Indirizzo server e-mail	Immettere l'indirizzo del server SMTP. Si tratta del server di posta associato all'account e-mail configurato (ad esempio mail.nomeazienda.it).
Porta server e-mail	Immettere la porta del server SMTP. Se il provider di posta richiede una porta speciale per le e-mail, inserirla qui. Altrimenti lasciare l'impostazione predefinita, 25.

Indirizzo e-mail risposta	Inserire l'indirizzo e-mail di risposta al quale Cisco RV215W invierà i messaggi nel caso gli avvisi inviati dal router non venissero recapitati all'indirizzo e-mail di destinazione.
Invia a indirizzo e-mail (1)	Immettere l'indirizzo e-mail a cui inviare gli avvisi (ad esempio, registri@nomeazienda.it).
Invia a indirizzo e-mail (2) (opzionale)	Inserire un indirizzo e-mail alternativo a cui inviare gli avvisi.
Invia a indirizzo e-mail (3) (opzionale)	Inserire un indirizzo e-mail alternativo a cui inviare gli avvisi.
Crittografia e-mail (SSL)	Per abilitare la crittografia delle e-mail, selezionare **Attiva**.
Autenticazione con server SMTP	Se il server (di posta) 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, registri@nomeazienda.it).
Password autenticazione e-mail	Inserire la password di autenticazione e-mail (ad esempio, la password utilizzata per accedere all'account e-mail configurato per ricevere gli avvisi).
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 **Ogni settimana**). 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 annuncio di servizio e di rilevamento. Sul router Cisco RV215W, 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 **Attiva** per attivare Bonjour.

PASSAGGIO 3 Per attivare Bonjour per una VLAN elencata nella **Tabella controlli interfaccia Bonjour**, selezionare la casella **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 Scegliere **Amministrazione** > **Impostazioni ora**. Viene indicata l'ora corrente.

PASSAGGIO 2 Configurare le informazioni seguenti:

Fuso orario	Selezionare il proprio fuso orario in relazione all'ora di Greenwich (GMT).
Regola per l'ora legale	Se applicabile alla propria area geografica, selezionare la casella **Regola per l'ora legale**. Questa casella di controllo viene attivata facendo clic su **Auto** nel campo **Imposta data e ora** sottostante.
Modalità Ora legale	Selezionare **Per data** (immettere la data specifica in cui avviare la modalità Ora legale) o **Ricorrente** (immettere il mese, la settimana, il giorno settimanale e l'ora in cui avviare la modalità Ora legale). Immettere le informazioni appropriate nei campi "da" e "a".
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 **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.
Immetti 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.

CAUTION Durante l'operazione di ripristino non tentare di connettersi 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 il ripristino della configurazione, 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 utilizzata dal dispositivo. Se la configurazione iniziale del 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 Cisco RV215W.
Configurazione mirror	Selezionare questa opzione per comunicare al dispositivo 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 eseguire il download del file di backup sul computer, fare clic su **Scarica**.

Il file (startup.cfg, mirror.cfg o backup.cfg) viene scaricato per impostazione predefinita nella cartella predefinita Download, ad esempio C:\Documents and Settings\Administrator\Documenti\Download\.

Per salvare un file di backup su un'unità USB, fare clic su **Salva su USB.**

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

Ripristino delle impostazioni di configurazione

È possibile ripristinare un file di configurazione salvato in 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 È possibile caricare il file di configurazione dal PC o da un dispositivo USB esterno.

Per caricarlo dal computer, fare clic sul pulsante di scelta **PC**. Fare clic su **Sfoglia** per selezionare il file. Selezionare il file e fare clic su **Apri**.

Per caricarlo su un'unità USB, fare clic sul pulsante di scelta **USB**. Fare clic su **Mostra USB** per visualizzare tutti i dispositivi USB connessi. Mettere il file sull'unità USB e fare clic su **Apri**.

NOTA Il dispositivo supporta NTFS in modalità di sola lettura e supporta i formati file FAT e FAT32 in modalità di lettura/scrittura sui dispositivi USB.

PASSAGGIO 4 Fare clic su **Avvia caricamento**.

Il dispositivo carica il file di configurazione e utilizza le impostazioni contenute per aggiornare la configurazione iniziale. Quindi, il dispositivo viene riavviato e utilizza la nuova configurazione.

Copia delle impostazioni di configurazione

Copiare la configurazione iniziale 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 a Device Manager. In questo caso, l'unico modo per poter accedere a Device Manager consiste nella reimpostazione delle impostazioni di fabbrica.

Il file di configurazione 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

Il router 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 Nella casella, immettere il seed utilizzato per generare la chiave.

PASSAGGIO 4 Fare clic su **Salva**.

Aggiornamento del firmware o modifica della lingua

L'aggiornamento a una nuova versione del firmware o la modifica della lingua del router vengono eseguiti dalla pagina **Amministrazione** > **Aggiornamento firmware/lingua**.

CAUTION Durante l'aggiornamento del firmware, non tentare di connettersi 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.

Aggiornamento automatico del firmware

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

PASSAGGIO 2 Nella sezione **Aggiornamento automatico firmware**, selezionare la frequenza con cui si desidera che il dispositivo ricerchi gli aggiornamenti del firmware, nel campo **Intervallo - Controlla ogni campo**.

PASSAGGIO 3 Nel campo **Aggiorna automaticamente**, selezionare se si desidera installare l'ultimo firmware subito dopo il rilevamento di una nuova versione oppure a una determinata ora.

PASSAGGIO 4 Per ricevere una notifica circa la disponibilità del nuovo firmware o al termine dell'installazione dell'ultimo firmware, selezionare una delle seguenti caselle di controllo:

- **Notifica tramite interfaccia utente amministratore:** l'utente riceve le notifiche sull'interfaccia utente amministratore di RV215W all'accesso successivo.
- **Invia e-mail a** : l'utente riceve le notifiche tramite avvisi di posta elettronica. Per configurare le impostazioni e-mail, fare clic su **Indirizzo e-mail** . Questa casella di controllo non sarà disponibile se l'opzione **Avviso di nuovo firmware tramite e-mail** non è abilitata. Per ulteriori informazioni, vedere la sezione **Configurazione delle impostazioni e-mail**.

PASSAGGIO 5 Fare clic su **Salva**.

Aggiornamento firmware/configurazione automatica da dispositivo USB

Per aggiornare automaticamente il firmware e la configurazione da un dispositivo USB, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Abilita** nel campo **Aggiorna da unità USB quando il dispositivo è acceso** .

Con questa impostazione di distribuzione immediata, se il dispositivo USB è inserito:

- Il firmware sul dispositivo viene aggiornato automaticamente quando il dispositivo è acceso.
- Il file di configurazione viene caricato automaticamente quando il dispositivo è acceso e quando vengono ripristinate le impostazioni di fabbrica del dispositivo.

PASSAGGIO 2 Fare clic su **Salva**.

Aggiornamento manuale del firmware

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

PASSAGGIO 2 Nella sezione **Aggiornamento manuale firmware/lingua**, fare clic sul pulsante di scelta **Immagine firmware** nel campo **Tipo di file**.

PASSAGGIO 3 Scaricare l'ultima versione del firmware sul PC o su un dispositivo USB. Per scaricare l'ultima versione del firmware da cisco.com su un dispositivo USB, fare clic su **Avvia download** in **Salva su USB da cisco.com**.

PASSAGGIO 4 Per installare l'ultima versione del firmware, selezionare una delle seguenti opzioni per aggiornare da:

- **cisco.com:** scaricare il firmware dal sito web cisco.com.
- **PC**: fare clic su **Sfoglia** per individuare e selezionare il firmware scaricato sul computer.
- **USB**: fare clic su **Mostra USB** per visualizzare tutti i file presenti sul dispositivo USB, nella tabella **Contenuto USB**. Individuare e selezionare il file firmware.

NOTA Il dispositivo supporta NTFS in modalità di sola lettura e supporta i formati file FAT e FAT32 in modalità di lettura/scrittura sui dispositivi USB.

CAUTION Il ripristino delle impostazioni predefinite del dispositivo elimina tutte le impostazioni di configurazione.

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

Dopo la convalida, la nuova immagine firmware viene scritta nella memoria flash e il router viene riavviato automaticamente con il nuovo firmware. Nella sezione **Informazioni di sistema**, viene visualizzata l'ultima versione del firmware.

Modifica della lingua

Per modificare la lingua, attenersi alla seguente procedura:

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

PASSAGGIO 2 Nel campo **Tipo di file**, fare clic sul pulsante di scelta **File di lingua**.

PASSAGGIO 3 Fare clic su **Sfoglia** per individuare e selezionare il file della lingua.

PASSAGGIO 4 Per ripristinare i parametri di configurazione predefiniti del dispositivo, selezionare **Ripristina tutte le impostazioni/configurazioni predefinite**.

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

Riavvio dell'unità Cisco RV215W

Per riavviare il router, attenersi alla seguente procedura:

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

PASSAGGIO 2 Fare clic su **Riavvia**.

Ripristino delle impostazioni di fabbrica

CAUTION Durante l'operazione di ripristino non tentare di connettersi 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.

A

Utilizzo di Cisco QuickVPN

Panoramica

In questa appendice viene spiegato 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**
- **Installazione del software QuickVPN di Cisco**
- **Utilizzo del software Cisco QuickVPN**

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**.

PASSAGGIO 2 Creare gli account utente QuickVPN. Vedere la sezione **Configurazione PPTP**. Dopo avere creato un account utente, è possibile utilizzare le credenziali con il client QuickVPN.

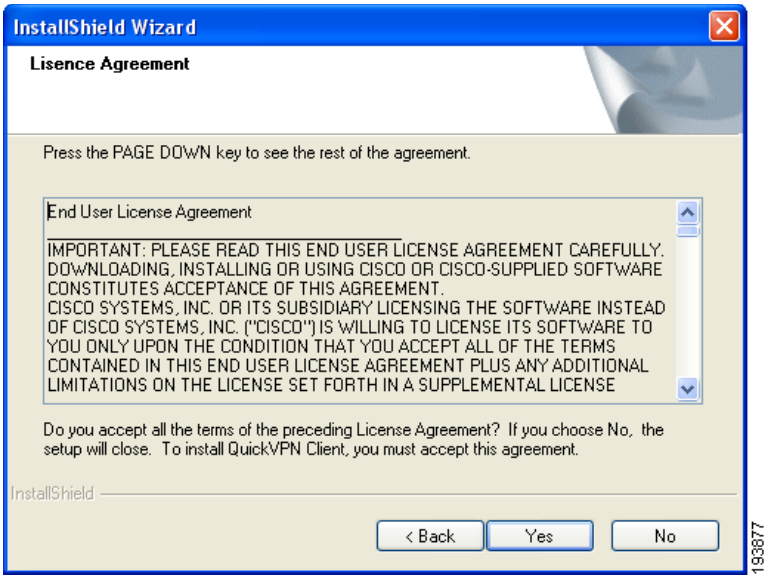
Installazione del software QuickVPN di Cisco

Installazione del software da CD

PASSAGGIO 1 Inserire il CD di installazione del router Cisco RV215W nell'unità CD-ROM. Dopo l'avvio dell'installazione guidata, fare clic sul collegamento **Installa QuickVPN**.

Viene visualizzata la finestra Contratto di licenza.

Contratto di licenza



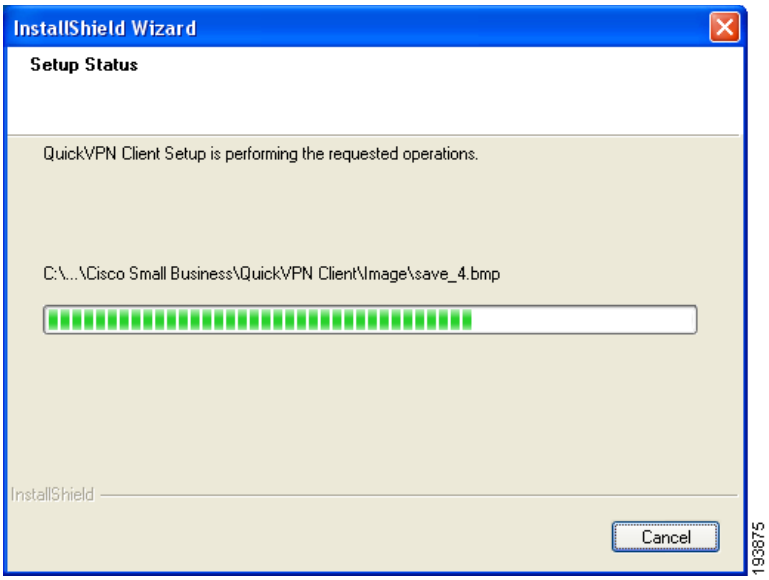
PASSAGGIO 2 Fare clic su **Sì** per accettare il contratto.

PASSAGGIO 3 Fare clic su **Sfoglia** e scegliere la destinazione dei file (ad esempio C:\Cisco Small Business\QuickVPN Client).

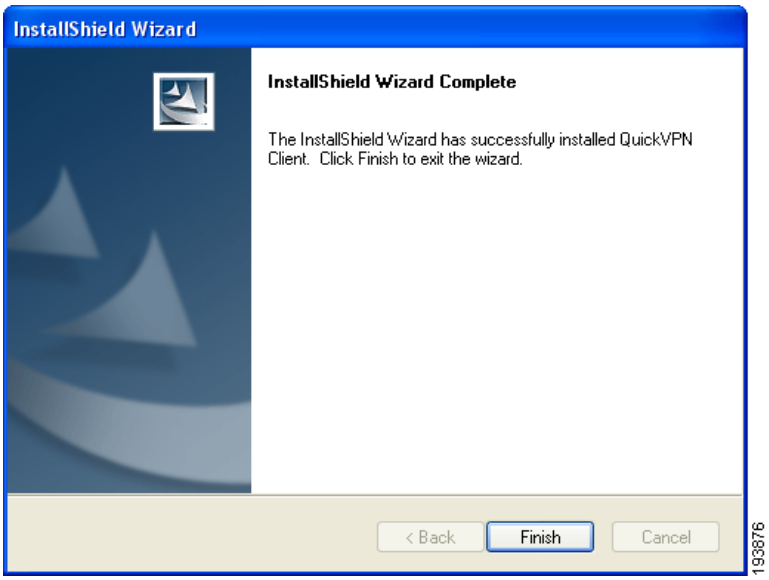
PASSAGGIO 4 Fare clic su **Avanti**.

I file vengono copiati nel percorso selezionato.

Copia dei file



Installazione dei file completata



PASSAGGIO 5 Fare clic su **Fine** per completare l'installazione. Passare alla sezione **"Utilizzo del software Cisco QuickVPN", a pagina 156**.

Download e installazione del software da Internet

PASSAGGIO 1 Nell'**Appendice B, "Risorse aggiuntive",** selezionare il collegamento Download di software.

PASSAGGIO 2 Immettere Cisco RV215W 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.

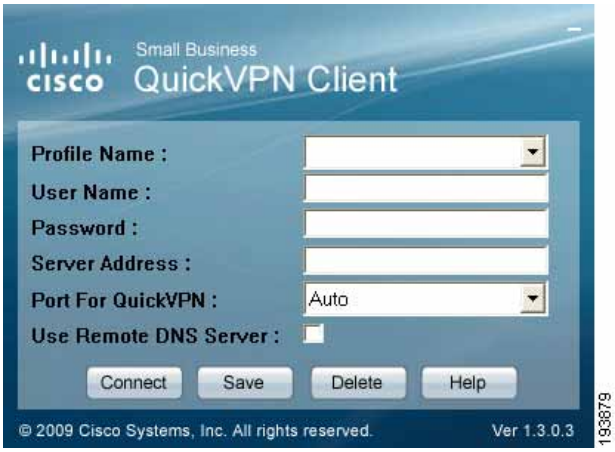
Utilizzo del software Cisco QuickVPN

PASSAGGIO 1 Fare doppio clic sull'icona Cisco QuickVPN sul desktop o nell'area di notifica del sistema.

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

Viene visualizzata la finestra Accesso QuickVPN.



PASSAGGIO 2 Nel campo **Nome profilo**, immettere un nome per il profilo.

PASSAGGIO 3 Nei campi **Nome utente** e **Password**, inserire il nome utente e la password.

PASSAGGIO 4 Nel campo **Indirizzo server**, immettere l'indirizzo IP o il nome di dominio del router Cisco RV215W.

PASSAGGIO 5 Nel campo **Porta per QuickVPN** immettere il numero di porta che viene utilizzata dal client QuickVPN per comunicare con il router VPN remoto oppure mantenere l'impostazione predefinita **Automatico**.

PASSAGGIO 6 Per salvare questo profilo, fare clic su **Salva**.

Per eliminare questo profilo, fare clic su **Elimina**. Per informazioni, fare clic su **Guida**.

NOTA Se è necessario creare un tunnel per più siti, è possibile creare diversi profili, ma può essere attivo un solo tunnel alla volta.

PASSAGGIO 7 Per avviare la connessione QuickVPN, fare clic su **Connetti**.

L'indicatore di avanzamento della connessione visualizza: Collegamento, Provisioning, Criteri di attivazione e Verifica della rete.

PASSAGGIO 8 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.

Per interrompere il tunnel VPN, fare clic sul pulsante **Disconnetti**. Per modificare la password, fare clic su **Modifica password**. Per informazioni, fare clic su **Guida**.

PASSAGGIO 9 Se si dispone dei diritti appropriati per modificare la password, quando si seleziona **Cambia password** viene visualizzata la finestra **Connetti connessione privata virtuale**.

PASSAGGIO 10 Immettere la password corrente nel campo **Vecchia password** e la nuova password nel campo **Nuova password**. Immettere di nuovo la nuova password nel campo **Conferma nuova password**.

PASSAGGIO 11 Fare clic su **OK** per salvare la nuova password.

NOTA È possibile modificare la password solo se la casella **Consenti all'utente di modificare la password** è stata selezionata.

B

Risorse aggiuntive

Assistenza	
Cisco support community	www.cisco.com/go/smallbizsupport
Assistenza tecnica e documentazione online (richiede l'immissione di dati di accesso)	www.cisco.com/support
Contatti per il servizio di assistenza telefonica	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 relativa al prodotto	
Firewall VPN Wireless-N	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Cisco Partner Central (richiede l'immissione di dati di accesso da parte dei partner)	www.cisco.com/web/partners/sell/smb
Marketplace	www.cisco.com/go/marketplace