345139

GUIDA
ALL'AMMINISTRAZIONE

Guida all'amministrazione degli switch gestiti stackable Cisco serie 500 - Versione 1.3.5

Sommario

Sommario

1

Introduzione

Questa sezione fornisce un'introduzione all'utilità di configurazione basata sul Web e include i seguenti argomenti:

- **Avvio dell'utilità di configurazione basata sul Web**
- **Configurazione rapida del dispositivo**
- **Convenzioni relative ai nomi dell'interfaccia**
- **Differenze tra i dispositivi 500**
- **Esplorazione delle finestre**

Avvio dell'utilità di configurazione basata sul Web

In questa sezione viene descritto come esplorare l'utilità di configurazione dello switch basata sul Web.

Se si sta utilizzando un blocco pop-up, accertarsi che sia disattivato.

Limitazioni del browser

Se si utilizzano più interfacce IPv6 nella stazione di gestione, utilizzare l'indirizzo globale IPv6 invece dell'indirizzo locale del collegamento IPv6 per accedere al dispositivo dal browser.

Lancio dell'utilità di configurazione

Per aprire l'utilità di configurazione Web, attenersi alla seguente procedura:

PASSAGGIO 1 Aprire un browser Web.

PASSAGGIO 2 Immettere l'indirizzo IP del dispositivo che si sta configurando nella barra degli indirizzi del browser, quindi premere **Invio**.

NOTA Se il dispositivo utilizza l'indirizzo IP predefinito 192.168.1.254, il LED di alimentazione continua a lampeggiare. Se il dispositivo utilizza un indirizzo IP assegnato da un server DHCP o un indirizzo IP statico configurato dall'amministratore, il LED di alimentazione rimane fisso.

Accesso

Il nome utente predefinito è **cisco** e la password predefinita è **cisco**. La prima volta che si accede con il nome utente e la password predefiniti, è necessario immettere una nuova password.

NOTA Se in precedenza non è stata selezionata una lingua per l'interfaccia utente, la lingua della pagina di accesso viene determinata dalle lingue richieste dal browser e da quelle configurate sul dispositivo. Se, ad esempio, il browser richiede il cinese e tale lingua è stata caricata nel dispositivo, la pagina di accesso viene visualizzata automaticamente in cinese. Se, invece, la lingua cinese non è stata caricata nel dispositivo, la pagina di accesso viene visualizzata in inglese.

Le lingue caricate nel dispositivo sono indicate da un codice lingua/paese (en-US, en-GB e così via). Per visualizzare la pagina di accesso in una determinata lingua, in base alla richiesta del browser, sia il codice lingua che il codice paese della richiesta del browser devono corrispondere a quelli della lingua caricata sul dispositivo. Se la richiesta del browser contiene il codice lingua ma non il codice paese (ad esempio: fr), viene utilizzata la prima lingua integrata con un codice lingua corrispondente (senza associare il codice paese, ad esempio: fr_CA).

Per accedere all'utilità di configurazione del dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Immettere il nome utente/la password. La password può contenere un massimo di 64 caratteri ASCII. Le regole di complessità della password sono descritte nella sezione **Impostazione delle regole di complessità password** del capitolo **Configurazione della protezione**.

PASSAGGIO 2 Se non si utilizza l'inglese, selezionare la lingua desiderata dalla casella a discesa *Lingua*. Per aggiungere una nuova lingua al dispositivo oppure aggiornare quella corrente, fare riferimento alla sezione Aggiornamento/Backup del firmware/ Lingua.

PASSAGGIO 3 Se si tratta del primo accesso con l'ID utente predefinito (**cisco**) e la password predefinita (**cisco**) oppure la password è scaduta, viene visualizzata la pagina Modifica password. Per ulteriori informazioni, vedere Scadenza password.

PASSAGGIO 4 Scegliere se selezionare o meno **Disattiva applicazione complessità della password**. Per ulteriori informazioni sulla complessità della password, vedere la sezione Impostazione delle regole di complessità della password.

PASSAGGIO 5 Immettere la nuova password e fare clic su **Applica**.

Se l'accesso viene completato, viene visualizzata la pagina Introduzione.

Se si immette un nome utente o una password errati, viene visualizzato un messaggio di errore e la pagina Accesso rimane visualizzata nella finestra. Se si riscontrano problemi durante l'accesso, vedere la sezione **Lancio dell'utilità di configurazione** della Guida all'amministrazione per ulteriori informazioni.

Selezionare **Non visualizzare questa pagina durante l'avvio** per impedire che la pagina Introduzione venga visualizzata a ogni accesso al sistema. Se si seleziona questa opzione, viene visualizzata la pagina Riepilogo di sistema invece della pagina Introduzione.

HTTP/HTTPS

È possibile aprire una sessione HTTP (non protetta) selezionando **Accedi** oppure aprire una sessione HTTPS (protetta) selezionando **Navigazione protetta (HTTPS)**. L'utente deve approvare l'accesso con una chiave RSA predefinita; successivamente viene aperta una sessione HTTPS.

NOTA Non è necessario immettere il nome utente/la password prima di fare clic sul pulsante **Navigazione protetta (HTTPS).**

Per informazioni su come configurare l'HTTPS, vedere **Server SSL**.

Scadenza password

La pagina Nuova password viene visualizzata nei casi seguenti:

- Al primo accesso al dispositivo con il nome utente **cisco** e la password **cisco** predefiniti. Questa pagina obbliga a sostituire la password con valori predefiniti.
- Quando la password scade, questa pagina obbliga a selezionarne una nuova.

Disconnessione

Per impostazione predefinita, l'applicazione si disconnette dopo dieci minuti di inattività. È possibile modificare questo valore predefinito come descritto nella sezione **Definizione del timeout della sessione inattiva**.

ATTENZIONE A meno che la configurazione di esecuzione non venga copiata nella configurazione di avvio, quando si riavvia il dispositivo, tutte le modifiche apportate dall'ultimo salvataggio del file vengono rimosse. Salvare la Configurazione di esecuzione nella Configurazione di avvio prima di disconnettersi per conservare le modifiche apportate durante questa sessione.

A sinistra del collegamento dell'applicazione **Salva** viene visualizzata un'icona rossa X lampeggiante per indicare che le modifiche apportate alla configurazione di esecuzione non sono ancora state salvate nel file di configurazione avvio. È possibile fare clic sul pulsante **Disattiva icona di salvataggio lampeggiante** nella pagina **Copia/Salva configurazione** per disattivare il lampeggiamento.

Quando il dispositivo rileva automaticamente un dispositivo, ad esempio un telefono IP (vedere la sezione **Descrizione di uno Smartport**), viene eseguita la configurazione della porta in modo appropriato per il dispositivo. Questi comandi di configurazione vengono scritti nel file Configurazione di esecuzione. In questo modo, l'icona Salva inizia a lampeggiare quando l'utente esegue l'accesso anche senza aver apportato modifiche alla configurazione.

Se si fa clic su **Salva**, viene visualizzata la pagina Copia/Salva configurazione. Salvare il file Configurazione di esecuzione copiandolo nel file Configurazione di avvio. Dopo questo salvataggio, l'icona rossa X e il collegamento all'applicazione Salva non vengono più visualizzati.

Per disconnettersi, fare clic su **Esci** nell'angolo in alto a destra di qualsiasi pagina. Il sistema si disconnette dal dispositivo.

Se si verifica un timeout o ci si disconnette intenzionalmente dal sistema, viene visualizzato un messaggio e viene aperta la pagina Accesso, in cui viene indicato che l'utente è disconnesso. Dopo l'accesso, l'applicazione torna alla pagina iniziale.

La pagina iniziale visualizzata dipende dall'opzione "Non visualizzare questa pagina durante l'avvio" della pagina Introduzione. Se questa opzione non è stata selezionata, la pagina iniziale è la pagina Introduzione. Se, invece, questa opzione è stata selezionata, la pagina iniziale è la pagina Riepilogo di sistema.

Configurazione rapida del dispositivo

Per semplificare la configurazione del dispositivo attraverso una navigazione rapida, la pagina Introduzione fornisce collegamenti alle pagine più utilizzate.

Categoria	Nome collegamento (nella pagina)	Pagina collegata
Installazione iniziale	Modifica di modalità del sistema e gestione dello stack	Pagina Modalità sistema e Gestione stack
	Modifica dei servizi e delle applicazioni di gestione	Pagina Servizi TCP/UDP
	Modifica indirizzo IP dispositivo	Pagina Interfaccia IPv4
	Crea VLAN	Pagina Crea VLAN
	Configura impostazioni porte	Pagina Impostazioni porta
Stato dispositivo	Riepilogo di sistema	Pagina Riepilogo di sistema
	Statistiche porte	Pagina Interfaccia
	Statistiche RMON	Pagina Statistiche
	Visualizza log	Pagina Memoria RAM
Accesso rapido	Modifica password dispositivo	Pagina Account utente
	Aggiorna software dispositivo	Pagina Aggiornamento/ Backup del firmware/Lingua
	Configurazione dispositivo di backup	Pagina Download/ Configurazione backup/Log
	Crea ACL basato su MAC	Pagina ACL basato su MAC
	Crea ACL basato su IP	Pagina ACL basato su IPv4
	Configura QoS	Pagina Proprietà QoS
	Configura mirroring delle porte	Pagina Mirroring di porte e VLAN

Due collegamenti consigliati nella pagina Introduzione conducono a pagine Web di Cisco in cui è possibile ottenere ulteriori informazioni. Se si fa clic sul

collegamento **Supporto**, viene visualizzata la pagina di supporto del prodotto relativa al dispositivo; se, invece, si fa clic sul collegamento **Forum**, viene visualizzata la pagina della Cisco Small Business Support Community.

Convenzioni relative ai nomi dell'interfaccia

All'interno dell'interfaccia utente, le interfacce sono identificate dalla concatenazione dei seguenti elementi:

- **Tipo di interfaccia:** sui vari tipi di dispositivo si trovano i seguenti tipi di interfaccia:
  - **Fast Ethernet (10/100 bit)**: visualizzata come **FE**.
  - **Porte Gigabit Ethernet (10/100/1000 bit)**: visualizzate come **GE**.
  - **Porte 10 Gigabit Ethernet (10000 bit)**: visualizzate come **XG**.
  - **LAG (port channel)**: visualizzati come **LAG**.
  - **VLAN**: visualizzata come **VLAN**.
  - **Tunnel**: visualizzato come **Tunnel**.
- **Numero di unità**: numero dell'unità nello stack. In modalità indipendente è sempre 1.
- **Numero slot**: il numero slot è sempre 1 o 2.
- **Numero interfaccia: porta, LAG, tunnel o ID VLAN.**

Differenze tra i dispositivi 500

Questa guida riguarda i dispositivi Sx500, SG500X,SG500XG e ESW2-550X. Quando una funzione è relativa a un dispositivo, ma non a tutti, vengono fornite delle note esplicative.

Di seguito vengono riassunte le differenze tra questi dispositivi:

- Le funzioni RIP e VRRP sono supportate solo sui dispositivi SG500X, SG500XG, ESW2-550X che operano in modalità indipendente (e in stack ibrido avanzata dei dispositivi SG500X e Sx500. Vedere la sezione **Amministrazione: gestione stack** per ulteriori informazioni).

- Dimensioni TCAM, vedere **Visualizzazione dell'utilizzo di TCAM**
- Le porte stack di questi dispositivi non corrispondono. Vedere **Porte stack**.
- Questi dispositivi dispongono di una diversa disponibilità relativa alla velocità della porta per tipo di cavo. Vedere **Tipi di cavo**.
- L'attivazione del routing IPv4 viene eseguita in modo diverso nei dispositivi:
  - SG500XSG500XG/ESW2-550X: è necessario attivare il routing IPv4 nella pagina Interfaccia IPv4.
  - Sx500: quando il dispositivo viene passato dalla modalità di sistema di livello 2 a livello 3, il routing IPv4 si attiva automaticamente.

Esplorazione delle finestre

In questa sezione vengono descritte le funzioni dell'utilità di configurazione dello switch basata sul Web.

Intestazione applicazione

L'intestazione dell'applicazione viene visualizzata in ogni pagina. Fornisce i seguenti collegamenti all'applicazione:

Nome collegamento all'applicazione	Descrizione
	A sinistra del collegamento dell'applicazione **Salva** viene visualizzata un'icona rossa X indicante che le modifiche a Configurazione di esecuzione apportate non sono ancora state salvate nel file Configurazione di avvio. Il lampeggiare della X rossa può essere disattivato dalla pagina Copia/Salva configurazione. Fare clic su **Salva** per visualizzare la pagina Copia/Salva configurazione. Salvare il file di configurazione esecuzione copiandolo nel tipo di file di configurazione avvio del dispositivo. Dopo questo salvataggio, l'icona rossa X e il collegamento all'applicazione Salva non vengono più visualizzati. Al riavvio del dispositivo, il tipo di file di configurazione avvio viene copiato nella configurazione di esecuzione e i parametri del dispositivo vengono impostati in base ai dati della configurazione di esecuzione.

Nome collegamento all'applicazione	Descrizione
Nome utente	Visualizza il nome dell'utente collegato al dispositivo. Il nome utente predefinito è **cisco** (la password predefinita è **cisco**).
Menu lingua	Nel menu sono disponibili le seguenti opzioni: ▪ **Selezionare una lingua:** consente di selezionare una delle lingue disponibili nel menu. La lingua selezionata diventerà la lingua utilizzata dell'utilità di configurazione Web. ▪ **Scarica lingua:** consente di aggiungere una nuova lingua al dispositivo. ▪ **Elimina lingua:** consente di eliminare la seconda lingua sul dispositivo. La prima lingua (inglese) non può essere eliminata. ▪ **Debug:** utilizzato per le traduzioni. Se si seleziona questa opzione, tutte le etichette dell'utilità di configurazione Web vengono sostituite dagli ID delle stringhe che corrispondono agli ID nel file di lingua. **NOTA** Per aggiornare un file della lingua, utilizzare la pagina Aggiornamento/Backup del firmware/ Lingua.
Esci	Fare clic per disconnettersi dall'utilità di configurazione dello switch basata sul Web.
Informazioni su	Fare clic per visualizzare il nome e il numero di versione del dispositivo.
Guida	Fare clic per visualizzare la guida in linea.
	Quando viene registrato un messaggio SYSLOG sopra il livello di gravità *critico*, viene visualizzata un'icona Stato di avviso SYSLOG. Fare clic sull'icona per aprire la pagina Memoria RAM. Dopo aver avuto accesso a questa pagina, l'icona Stato di avviso SYSLOG non viene più visualizzata. Per visualizzare la pagina quando non è presente nessun messaggio SYSLOG attivo, fare clic su **Stato e statistiche** > **Visualizza log** > **Memoria RAM**.

Pulsanti di gestione

Nella tabella seguente vengono descritti i pulsanti più utilizzati visualizzati nelle diverse pagine del sistema.

Nome pulsante	Descrizione
Showing 1-20 of 20 20 per page	Utilizzare il menu a tendina per configurare il numero di voci per pagina.
	Indica un campo obbligatorio.
Aggiungi	Fare clic per visualizzare la pagina Aggiungi correlata e aggiungere una voce alla tabella. Immettere le informazioni e fare clic su **Applica** per salvarle nella Configurazione di esecuzione. Scegliere **Chiudi** per tornare alla pagina principale. Fare clic su **Salva** per visualizzare la pagina Copia/Salva configurazione e salvare la configurazione di esecuzione nel tipo di file configurazione di avvio del dispositivo.
Applica	Fare clic per applicare le modifiche alla configurazione di esecuzione del dispositivo. Se il dispositivo viene riavviato, la configurazione di esecuzione viene persa a meno che non venga salvata nel tipo di file di configurazione avvio o un altro tipo di file. Fare clic su **Salva** per visualizzare la pagina Copia/Salva configurazione e salvare la configurazione di esecuzione nel tipo di file configurazione di avvio del dispositivo.
Annulla	Fare clic per reimpostare le modifiche apportate nella pagina.
Cancella tutti i contatori interfaccia	Fare clic per cancellare i contatori statistica di tutte le interfacce.
Cancella contatori interfaccia	Fare clic per cancellare i contatori statistica dell'interfaccia selezionata.
Cancella log	Cancella i file di log.
Cancella tabella	Cancella le voci della tabella.

Nome pulsante	Descrizione
Chiudi	Torna alla pagina principale. Se alcune modifiche non sono state applicate alla configurazione di esecuzione, viene visualizzato un messaggio.
Copia impostazioni	Di solito una tabella contiene una o più voci con impostazioni della configurazione. Anziché modificare ogni voce singolarmente, è possibile modificare una voce e copiarla in più voci, come descritto di seguito: 1. Selezionare la voce da copiare. Scegliere **Copia impostazioni** per visualizzare il popup. 2. Immettere i numeri della voce di destinazione nel campo **a**. 3. Scegliere **Applica** per salvare le modifiche e su **Chiudi** per tornare alla pagina principale.
Elimina	Dopo aver selezionato la voce nella tabella, fare clic su **Elimina** per rimuoverla.
Dettagli	Fare clic per visualizzare i dettagli associati alla voce selezionata.
Modifica	Selezionare la voce e fare clic su **Modifica**. Viene visualizzata la pagina Modifica, in cui è possibile modificare la voce. 1. Scegliere **Applica** per salvare le modifiche alla Configurazione di esecuzione. 2. Scegliere **Chiudi** per tornare alla pagina principale.
Vai	Immettere i criteri di filtro e fare clic su **Vai**. I risultati vengono visualizzati nella pagina.
Aggiorna	Fare clic su **Aggiorna** per aggiornare i valori del contatore.
Test	Scegliere **Test** per eseguire i test correlati.

2

Stato e statistiche

In questa sezione viene descritto come visualizzare le statistiche del dispositivo.

Vengono trattati i seguenti argomenti:

- **Riepilogo di sistema**
- **Visualizzazione delle interfacce Ethernet**
- **Visualizzazione delle statistiche Etherlike**
- **Visualizzazione delle statistiche GVRP**
- **Visualizzazione delle statistiche 802.1X EAP**
- **Visualizzazione dell'utilizzo di TCAM**
- **Integrità**
- **Gestione RMON**
- **Visualizza log**

Riepilogo di sistema

Vedere la sezione **Impostazioni di sistema**.

Visualizzazione delle interfacce Ethernet

Nella pagina Interfaccia vengono visualizzate le statistiche del traffico per porta. È possibile selezionare la frequenza di aggiornamento delle informazioni.

Questa pagina è utile per l'analisi della quantità di traffico inviato e ricevuto e della sua dispersione (Unicast, Multicast e Broadcast).

Per visualizzare le statistiche Eternet e/o selezionare una frequenza di aggiornamento, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Stato e statistiche** > **Interfaccia**.

PASSAGGIO 2 Immettere i parametri.

- **Interfaccia**: selezionare il tipo di interfaccia e l'interfaccia specifica di cui è necessario visualizzare le statistiche Ethernet.
- **Frequenza aggiornamento**: selezionare il periodo di tempo che trascorre prima che le statistiche dell'interfaccia Ethernet vengano aggiornate. Le opzioni disponibili sono:
  - *Nessun aggiornamento*: le statistiche non vengono aggiornate.
  - *15 sec.*: le statistiche vengono aggiornate ogni 15 secondi.
  - *30 sec.*: le statistiche vengono aggiornate ogni 30 secondi.
  - *60 sec.*: le statistiche vengono aggiornate ogni 60 secondi.

Nell'area Statistiche ricezione vengono visualizzate le informazioni sui pacchetti in ingresso.

- **Byte totali (ottetti)**: ottetti ricevuti, inclusi i pacchetti danneggiati e gli ottetti FCS, ma non i bit raggruppati in frame.
- **Pacchetti unicast**: pacchetti unicast in buono stato ricevuti.
- **Pacchetti multicast**: pacchetti multicast in buono stato ricevuti.
- **Pacchetti broadcast**: pacchetti broadcast in buono stato ricevuti.
- **Pacchetti con errori**: pacchetti con errori ricevuti.

Nell'area Statistiche di trasmissione vengono visualizzate le informazioni sui pacchetti in uscita.

- **Byte totali (ottetti)**: ottetti trasmessi, inclusi i pacchetti danneggiati e gli ottetti FCS, ma non i bit raggruppati in frame.
- **Pacchetti unicast**: pacchetti unicast in buono stato trasmessi.
- **Pacchetti multicast**: pacchetti multicast in buono stato trasmessi.
- **Pacchetti broadcast**: pacchetti broadcast in buono stato trasmessi.

Per azzerare o visualizzare i contatori delle statistiche, attenersi alla seguente procedura:

- Scegliere **Cancella contatori interfaccia** per cancellare i contatori dell'interfaccia visualizzati.
- Fare clic su **Visualizza tutte le statistiche delle interfacce** per vedere tutte le porte su una singola pagina.

Visualizzazione delle statistiche Etherlike

Nella pagina Etherlike vengono visualizzate le statistiche per porta in base alla definizione standard MIB Etherlike. È possibile selezionare la frequenza di aggiornamento delle informazioni. In questa pagina vengono fornite informazioni più dettagliate relative agli errori nel livello fisico (Livello 1), che potrebbero compromettere il traffico.

Per visualizzare le statistiche Eternet e/o selezionare una frequenza di aggiornamento, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Stato e statistiche** > **Etherlike**.

PASSAGGIO 2 Immettere i parametri.

- **Interfaccia**: selezionare il tipo di interfaccia e l'interfaccia specifica di cui è necessario visualizzare le statistiche Ethernet.
- **Frequenza aggiornamento**: selezionare quanto tempo trascorre prima che le statistiche Etherlike vengano aggiornate.

Vengono visualizzati i campi delle interfacce selezionate.

- **Errori sequenza di controllo frame (FCS)**: frame ricevuti i cui CRC (cyclic redundancy checks) non sono riusciti.
- **Frame di collisione singoli**: i frame interessati in una collisione singola ma trasmessi correttamente.
- **Collisioni ritardate**: collisioni rilevate dopo i primi 512 bit di dati.
- **Numero eccessivo di collisioni**: numero di trasmissioni rifiutate a causa di un numero di collisioni eccessivo.
- **Pacchetti sovradimensionati**: pacchetti ricevuti superiori ai 2000 ottetti.

- **Errori di ricezione MAC interni**: frame rifiutati a causa di errori del ricevitore.
- **Frame di pausa ricevuti**: frame di pausa del controllo di flusso ricevuti.
- **Frame di pausa trasmessi**: frame di pausa del controllo di flusso trasmessi dall'interfaccia selezionata.

Per cancellare i contatori delle statistiche, attenersi alla seguente procedura:

- Fare clic su **Cancella contatori interfaccia** per cancellare i contatori interfaccia selezionati.
- Fare clic su **Visualizza tutte le statistiche delle interfacce** per vedere tutte le porte su una singola pagina.

Visualizzazione delle statistiche GVRP

Nella pagina GVRP vengono visualizzate le informazioni relative ai frame GVRP (GARP VLAN Registration Protocol) inviati o ricevuti da una porta. GVRP è un protocollo di rete Livello 2 basato sugli standard, per la configurazione automatica delle informazioni sulla VLAN degli switch. È stato definito nell'emendamento 802.1ak per 802.1Q-2005.

Le statistiche di GVRP per una porta vengono visualizzate solo se GVRP è attivato a livello globale e nella porta. Vedere la pagina GVRP.

Per visualizzare le statistiche GVRP e/o selezionare una frequenza di aggiornamento, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Stato e statistiche** > **GVRP**.

PASSAGGIO 2 Immettere i parametri.

- **Interfaccia**: selezionare l'interfaccia specifica di cui è necessario visualizzare le statistiche GVRP.
- **Frequenza aggiornamento**: selezionare il periodo di tempo che trascorre prima che le statistiche GVRP vengano aggiornate.

Nel blocco Contatore attributo vengono visualizzati i contatori dei diversi tipi di pacchetti per interfaccia.

- **Includi vuoto**: numero di pacchetti Includi vuoto GVRP ricevuti/trasmessi.
- **Vuoto**: numero di pacchetti Vuoto GVRP ricevuti/trasmessi.

- **Lascia vuoto**: numero di pacchetti Lascia vuoto GVRP ricevuti/trasmessi.
- **Join In**: numero di pacchetti Join in GVRP ricevuti/trasmessi.
- **Leave In**: numero di pacchetti Leave In GVRP ricevuti/trasmessi.
- **Leave All**: numero di pacchetti Leave All GVRP ricevuti/trasmessi.

Nella sezione Statistiche errore GVRP vengono indicati i contatori di errore GVRP.

- **ID protocollo non valido**: errori ID del protocollo non valido.
- **Tipo di attributo non valido**: errori ID attributo non valido.
- **Valore dell'attributo non valido**: errori valore dell'attributo non valido.
- **Lunghezza dell'attributo non valida**: errori lunghezza dell'attributo non valida.
- **Evento non valido**: eventi non validi.

Per cancellare i contatori delle statistiche, attenersi alla seguente procedura:

- Scegliere **Cancella contatori interfaccia** per cancellare i contatori selezionati.
- Fare clic su **Visualizza tutte le statistiche delle interfacce** per vedere tutte le porte su una singola pagina.

Visualizzazione delle statistiche 802.1X EAP

Nella pagina 802.1x EAP vengono visualizzate le informazioni dettagliate sui frame EAP (Extensible Authentication Protocol) inviati o ricevuti. Per configurare la funzione 802.1X, vedere la pagina Proprietà 802.1X.

Per visualizzare le statistiche EAP e/o selezionare una frequenza di aggiornamento, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Stato e statistiche** > **EAP 802.1x**.

PASSAGGIO 2 Selezionare l'**interfaccia** di cui effettuare il polling per le statistiche.

PASSAGGIO 3 Selezionare il periodo di tempo (**Frequenza aggiornamento**) che trascorre prima che le statistiche EAP vengano aggiornate.

Vengono visualizzati i valori dell'interfaccia selezionata.

- **Frame EAPOL ricevuti**: frame EAPOL validi ricevuti nella porta.
- **Frame EAPOL trasmessi**: frame EAPOL validi trasmessi dalla porta.
- **Frame iniziali EAPOL ricevuti**: frame iniziali EAPOL ricevuti nella porta.
- **Frame di disconnessione EAPOL ricevuti**: frame di disconnessione EAPOL ricevuti nella porta.
- **Frame di risposta EAP/ID ricevuti**: frame di risposta EAP/ID ricevuti nella porta.
- **Frame di risposta EAP ricevuti**: frame di risposta EAP ricevuti dalla porta (diversi dai frame di risposta/ID).
- **Frame di richiesta EAP/ID trasmessi**: frame di richiesta EAP/ID trasmessi dalla porta.
- **Frame di richiesta EAP trasmessi**: frame di richiesta EAP trasmessi dalla porta.
- **Frame EAPOL non validi ricevuti**: frame EAPOL non riconosciuti ricevuti in questa porta.
- **Frame di errore lunghezza EAP ricevuti**: frame EAPOL con una Lunghezza corpo del pacchetto non valida ricevuti in questa porta.
- **Ultima versione frame EAPOL**: numero versione di protocollo associato al frame EAPOL ricevuto più di recente.
- **Ultima origine frame EAPOL**: indirizzo MAC di origine associato al frame EAPOL ricevuto più di recente.

Per cancellare i contatori delle statistiche, attenersi alla seguente procedura:

- Fare clic su **Cancella contatori interfaccia** per cancellare i contatori interfaccia selezionati.
- Scegliere **Cancella tutti i contatori interfaccia** per cancellare i contatori di tutte le interfacce.

Visualizzazione dell'utilizzo di TCAM

L'architettura del dispositivo utilizza una TCAM (Ternary Content Addressable Memory) per supportare le azioni del pacchetto a velocità wire-speed.

TCAM mantiene le regole generate da altre applicazioni, come ACL (Access Control Lists), QoS (Quality of Service), routing IP e le regole create dall'utente.

Alcune applicazioni allocano regole al loro avvio. Inoltre i processi inizializzati durante l'avvio del sistema, durante il processo di avvio utilizzano alcune delle loro regole.

Per visualizzare l'utilizzo di TCAM, fare clic su **Stato e statistiche** > **Utilizzo di TCAM**.

I campi seguenti vengono visualizzati per i dispositivi SG500X/SG500XG e per i dispositivi Sx500 nella modalità di sistema Livello 3 e quando il dispositivo fa parte di uno stack (per unità):

- **N. unità**: unità nello stack per le quali viene visualizzato l'utilizzo di TCAM. Questa informazione non viene visualizzata quando il dispositivo è in modalità indipendente.
- **Numero massimo voci TCAM per routing IPv4 e IPv6**: numero massimo di voci TCAM disponibili.
- **Routing IPv4**
  - **In uso**: numero di voci TCAM usate per il routing IPv4.
  - **Massimo**: numero di voci TCAM disponibili che possono essere usate per il routing IPv4.
- **Routing IPv6**: numero di voci TCAM usate per il routing IPv6.
  - **In uso**: numero di voci TCAM usate per il routing IPv6.
  - **Massimo**: numero di voci TCAM disponibili che possono essere usate per il routing IPv6.
- **Numero massimo voci TCAM per regole non IP**: numero massimo di voci TCAM disponibili per regole non IP.
- **Regole non IP**
  - **In uso**: numero di voci TCAM usate per regole non IP.

- **Massimo**: numero di voci TCAM disponibili che possono essere usate per regole non IP.

Per scoprire come modificare l'allocazione tra i vari processi (per la serie 500), vedere la sezione **Risorse router**.

Integrità

Vedere la sezione **Integrità**.

Gestione RMON

RMON (Remote Networking Monitoring) è una specifica SNMP che consente a un agente SNMP nel dispositivo di monitorare in maniera proattiva le statistiche sul traffico per un periodo specifico e di inviare trap a un gestore SNMP. L'agente locale SNMP confronta i contatori effettivi e in tempo reale con le soglie predefinite e genera allarmi, senza dover effettuare il polling da una piattaforma di gestione SNMP centrale. Si tratta di un meccanismo efficace per la gestione preventiva, ammesso che si disponga delle soglie corrette impostate relative alla linea di base della rete.

RMON riduce il traffico tra il gestore e il dispositivo perché il gestore SNMP non deve eseguire spesso il polling del dispositivo per informazioni e consente al gestore di ottenere rapporti sullo stato perché il dispositivo esegue il rapporto di eventi quando si verificano.

Con questa funzione, è possibile eseguire le seguenti azioni:

- Visualizzare le statistiche attuali (dato che i valori del contatore sono stati cancellati). È inoltre possibile raccogliere i valori di questi contatori per un periodo di tempo e visualizzare poi la tabella dei dati raccolti, in cui ogni serie raccolta è una singola riga della scheda *Cronologia*.
- Definire le modifiche interessanti nei valori del contatore come "numero specifico di collisioni ritardate raggiunto" (definisce l'allarme), quindi definire quale azione eseguire quando si verifica questo evento (log, trap o log e trap).

Visualizzazione delle statistiche RMON

Nella pagina Statistiche vengono visualizzate informazioni dettagliate sulle dimensioni dei pacchetti e sugli errori del livello fisico. Le informazioni mostrate seguono lo standard RMON. Un pacchetto sovradimensionato viene definito come un frame Ethernet con i seguenti criteri:

- La lunghezza del pacchetto è superiore alla dimensione in byte di MRU.
- Non è stato rilevato un evento di collisione.
- Non è stato rilevato un evento di collisione ritardata.
- Non è stato rilevato un evento di errore ricevuto (Rx).
- Il pacchetto presenta un CRC valido.

Per visualizzare le statistiche RMON e/o selezionare una frequenza di aggiornamento, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Stato e statistiche> RMON > Statistiche**.

PASSAGGIO 2 Selezionare l'**interfaccia** per cui visualizzare le statistiche Ethernet.

PASSAGGIO 3 Selezionare **Frequenza aggiornamento**, il periodo di tempo che trascorre prima che le statistiche dell'interfaccia vengano aggiornate.

Vengono visualizzate le statistiche dell'interfaccia selezionata.

- **Byte ricevuti**: numero di ottetti ricevuti, inclusi i pacchetti danneggiati e gli ottetti FCS, ma non i bit raggruppati in frame.
- **Eventi di eliminazione**: numero di pacchetti eliminati.
- **Pacchetti ricevuti**: numero di pacchetti correttamente ricevuti, inclusi i pacchetti multicast e broadcast.
- **Pacchetti broadcast ricevuti**: numero di pacchetti broadcast in buono stato ricevuti. Questo numero non include i pacchetti multicast.
- **Pacchetti multicast ricevuti**: numero di pacchetti multicast in buono stato ricevuti.
- **Errori CRC e di allineamento**: numero di errori CRC e di allineamento verificatisi.
- **Pacchetti sottodimensionati**: numero di pacchetti sottodimensionati (meno di 64 ottetti) ricevuti.

- **Pacchetti sovradimensionati**: numero di pacchetti sovradimensionati (più di 2000 ottetti) ricevuti.
- **Frammenti**: numero di frammenti (pacchetti con meno di 64 ottetti, esclusi i bit raggruppati in frame, ma inclusi gli ottetti FCS) ricevuti.
- **Jabber**: numero totale di pacchetti ricevuti con lunghezza superiore ai 1632 ottetti. Questo numero esclude i bit raggruppati in frame, ma include gli ottetti FCS che avevano un FCS (Frame Check Sequence) errato con un numero integrale di ottetti (errore FCS) o un FCS con un numero non integrale di ottetti (errore di allineamento). Un pacchetto Jabber è definito come un frame Ethernet che soddisfa i criteri seguenti:
  - La lunghezza dei dati del pacchetto è maggiore di MRU.
  - Il pacchetto dispone di un CRC non valido.
  - Non è stato rilevato un evento di errore ricevuto (Rx).
- **Collisioni**: numero di collisioni ricevute. Se vengono attivati i frame jumbo, la soglia dei frame jabber raggiunge le dimensioni massime dei frame jumbo.
- **Frame di 64 byte**: numero di frame, contenenti 64 byte, ricevuti.
- **Frame da 65 a 127 byte**: numero di frame, contenenti 65-127 byte, ricevuti.
- **Frame da 128 a 255 byte**: numero di frame, contenenti 128-255 byte, ricevuti.
- **Frame da 256 a 511 byte**: numero di frame, contenenti 256-511 byte, ricevuti.
- **Frame da 512 a 1023 byte**: numero di frame, contenenti 512-1023 byte, ricevuti.
- **Frame superiori o pari a 1024 byte**: numero di frame, contenenti da 1024 a 2000 byte e frame Jumbo, ricevuti.

Per cancellare i contatori delle statistiche, attenersi alla seguente procedura:

- Fare clic su **Cancella contatori interfaccia** per cancellare i contatori interfaccia selezionati.
- Fare clic su **Visualizza tutte le statistiche delle interfacce** per vedere tutte le porte su una singola pagina.

Configurazione della cronologia RMON

La funzione RMON consente il monitoraggio delle statistiche per interfaccia.

Nella pagina Tabella Controllo cronologia viene definita la frequenza di campionamento, la quantità di campioni da memorizzare e la porta da cui raccogliere le informazioni.

I dati campionati e memorizzati vengono visualizzati nella pagina Tabella cronologia, che può essere visualizzata facendo clic sul pulsante **Tabella cronologia**.

Per immettere le informazioni sul controllo RMON, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Stato e statistiche> RMON > Cronologia**. I campi visualizzati in questa pagina sono definiti nella pagina Aggiungi cronologia RMON di seguito. L'unico campo presente in questa pagina e non definito nella pagina Aggiungi è:

- **Numero corrente di campionamenti**: RMON ha il permesso dallo standard di non garantire tutti i campionamenti richiesti ma limita il numero dei campionamenti per richiesta. Pertanto, questo campo indica il numero di campionamenti al momento garantiti alla richiesta uguale o inferiore al valore richiesto.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **Nuova voce cronologia**: indica il numero della nuova voce della tabella Cronologia.
- **Interfaccia origine**: selezionare il tipo di interfaccia da cui sono stati acquisiti i campionamenti cronologici.
- **N. max di campionamenti da conservare**: immettere il numero di campionamenti da memorizzare.
- **Intervallo di campionamento**: immettere il tempo in secondi in cui vengono raccolti i campionamenti dalle porte. Il valore è compreso tra 1 e 3600.
- **Titolare**: immettere la stazione RMON o dell'utente che ha richiesto le informazioni RMON.

PASSAGGIO 4 Fare clic su **Applica**. La voce viene aggiunta alla pagina Tabella Controllo cronologia e il file Configurazione di esecuzione viene aggiornato.

PASSAGGIO 5 Fare clic su **Tabella cronologia** per visualizzare le statistiche attuali.

Visualizzazione della tabella Cronologia RMON

Nella pagina Tabella Cronologia vengono visualizzati i campionamenti di rete statistici specifici di un'interfaccia. I campionamenti sono stati configurati nella tabella Controllo cronologia descritta sopra.

Per visualizzare le statistiche della cronologia RMON, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Stato e statistiche** > **RMON** > **Cronologia**.

PASSAGGIO 2 Scegliere **Tabella Cronologia**.

PASSAGGIO 3 Dall'elenco **N. voce cronologia**, selezionare il numero della voce del campionamento da visualizzare.

Vengono visualizzati i campi del campionamento selezionato.

- **Titolare**: voce della tabella della cronologia.
- **N. campionamento**: statistiche acquisite da questo campionamento.
- **Eventi di eliminazione**: pacchetti eliminati a causa della mancanza di risorse di rete durante l'intervallo di campionamento. Non è possibile indicare il numero esatto di pacchetti eliminati però è possibile indicare il numero di volte in cui sono stati rilevati pacchetti eliminati.
- **Byte ricevuti**: ottetti ricevuti, inclusi i pacchetti danneggiati e gli ottetti FCS, ma non i bit raggruppati in frame.
- **Pacchetti ricevuti**: pacchetti ricevuti, inclusi i pacchetti danneggiati, multicast e broadcast.
- **Pacchetti broadcast**: pacchetti broadcast in buono stato, esclusi i pacchetti multicast.
- **Pacchetti multicast**: pacchetti multicast in buono stato ricevuti.
- **Errori CRC e di allineamento**: errori CRC e di allineamento verificatisi.
- **Pacchetti sottodimensionati**: pacchetti sottodimensionati (meno di 64 ottetti) ricevuti.

- **Pacchetti sovradimensionati**: pacchetti sovradimensionati (più di 2000 ottetti) ricevuti.
- **Frammenti**: frammenti (pacchetti con meno di 64 ottetti) ricevuti, esclusi i bit raggruppati in frame, ma inclusi gli ottetti FCS.
- **Jabber**: numero totale di pacchetti ricevuti con lunghezza superiore ai 2000 ottetti. Questo numero esclude i bit raggruppati in frame, ma include gli ottetti FCS che avevano un FCS (Frame Check Sequence) errato con un numero integrale di ottetti (errore FCS) o un FCS con un numero non integrale di ottetti (errore di allineamento).
- **Collisioni**: collisioni ricevute.
- **Utilizzo**: percentuale di traffico dell'interfaccia corrente confrontato con il traffico massimo gestibile dall'interfaccia.

Definizione di controllo di eventi RMON

È possibile controllare gli eventi in cui viene generato un allarme e il tipo di notifica che si riceve. Ciò viene eseguito nel modo seguente:

- **Pagina Eventi**: configura l'accaduto quando viene generato un allarme. Può trattarsi di una qualsiasi combinazione di log e trap.
- **Pagina Allarmi**: configura gli eventi in cui viene generato un allarme.

Per definire gli eventi RMON, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Stato e statistiche > RMON** > **Eventi**.

In questa pagina vengono visualizzati gli eventi definiti in precedenza.

PASSAGGIO 2 Fare clic su **Aggiungi.**

PASSAGGIO 3 Immettere i parametri.

- **Voce evento**: indica il numero di indice della voce evento della nuova voce.
- **Comunità**: immettere la stringa di comunità SNMP da includere quando vengono inviate le trap (facoltativo). Per definire la comunità, andare alla pagina **Definizione dei destinatari delle notifiche SNMPv1,2** o **Definizione dei Destinatari delle notifiche SNMPv3** in modo tale che il trap raggiunga la stazione di gestione della rete.

- **Descrizione**: immettere un nome per l'evento. Questo nome viene utilizzato nella pagina Aggiungi allarme RMON per associare un allarme a un evento.
- **Tipo di notifica**: selezionare il tipo di azione derivante da questo evento. I valori sono:
  - *Nessuno*: non viene eseguita alcuna azione quando l'allarme si spegne.
  - *Log (Tabella Log evento)*: aggiungere una voce di log alla tabella Log evento quando l'allarme viene attivato.
  - *Trap (SNMP Manager e server Syslog)*: inviare un trap al server di log remoti quando l'allarme si disattiva.
  - *Log e Trap*: aggiungere una voce di log alla tabella Log evento e inviare un trap al server di log remoti quando l'allarme si disattiva.
- **Ora**: mostra l'ora dell'evento (si tratta una tabella di sola lettura nella finestra principale che non può essere definita).
- **Titolare**: immettere il dispositivo o l'utente che ha definito l'evento.

PASSAGGIO 4 Fare clic su **Applica**. L'evento RMON viene salvato nel file di configurazione esecuzione.

PASSAGGIO 5 Scegliere **Tabella Log evento** per visualizzare il log degli allarmi generati e registrati (vedere la descrizione riportata di seguito).

Visualizzazione dei log degli eventi RMON

Nella pagina Tabella Log evento viene mostrato il log degli eventi (azioni) che si sono verificati. È possibile registrare due tipi di eventi: *Log* o *Log e Trap*. L'azione specificata per l'evento viene eseguita quando l'evento è associato a un allarme (vedere la pagina Allarmi) e si sono verificate le condizioni dell'allarme.

PASSAGGIO 1 Scegliere **Stato e statistiche > RMON** > **Eventi**.

PASSAGGIO 2 Fare clic su **Tabella Log evento**.

In questa pagina vengono visualizzati i seguenti campi:

- **N. voce evento**: numero voce log evento.
- **N. log**: numero del log (nell'evento).

- **Ora di log**: ora in cui è stata inserita la voce del log.
- **Descrizione**: descrizione dell'evento che ha generato l'allarme.

Definizione degli allarmi RMON

Gli allarmi RMON forniscono un meccanismo per l'impostazione di soglie e intervalli di campionamento per generare eventi eccezione in qualsiasi contatore o in qualunque contatore oggetto SNMP conservato dall'agente. Nell'allarme è necessario configurare sia la soglia superiore che quella inferiore. Superata la soglia superiore, non viene generato alcun evento superiore fino al superamento della soglia inferiore. Utilizzato un allarme inferiore, l'allarme successivo viene utilizzato quando viene superata una soglia superiore.

Uno o più allarmi vengono associati a un evento che indica l'azione da eseguire quando si verifica l'allarme.

Nella pagina Allarmi viene offerta la possibilità di configurare allarmi e associarli agli eventi. I contatori allarme possono essere monitorati dai valori assoluti o dalle modifiche (delta) nei valori dei contatori.

Per immettere allarmi RMON, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Stato e statistiche > RMON** > **Allarmi**. Vengono visualizzati tutti gli allarmi definiti in precedenza. I campi sono descritti nella pagina Aggiungi allarme RMON di seguito. Oltre a quei campi, viene visualizzato anche il campo seguente:

- **Valore contatore**: visualizza il valore della statistica durante il periodo di campionamento più recente.

PASSAGGIO 2 Fare clic su **Aggiungi.**

PASSAGGIO 3 Immettere i parametri.

- **N. voce allarme**: viene indicato il numero della voce dell'allarme.
- **Interfaccia**: selezionare il tipo di interfaccia di cui vengono visualizzate le statistiche RMON.
- **Nome contatore**: selezionare la variabile MIB che indica il tipo di occorrenza misurata.
- **Tipo di campionamento**: selezionare il metodo di campionamento per generare un allarme. Sono disponibili le seguenti opzioni:

  - *Assoluto*: se la soglia è stata superata, viene generato un allarme.
  - *Delta*: il valore dell'ultimo campionamento viene sottratto dal valore corrente e la differenza viene confrontata con la soglia. Se la soglia è stata superata, viene generato un allarme.
- **Soglia superiore**: immettere il valore che attiva l'allarme della soglia superiore.
- **Evento superiore**: selezionare un evento da eseguire quando si genera un evento superiore. Gli eventi vengono creati nella pagina Eventi.
- **Soglia inferiore**: immettere il valore che attiva l'allarme della soglia inferiore.
- **Evento inferiore**: selezionare un evento da eseguire quando si genera un evento inferiore.
- **Allarme di avvio**: selezionare il primo evento da cui avviare la generazione di allarmi. Con Allarme superiore si intende il superamento di una soglia a causa del passaggio da un valore più basso a uno più alto.
  - *Allarme soglia superiore*: un valore superiore attiva l'allarme della soglia superiore.
  - *Allarme soglia inferiore*: un valore inferiore attiva l'allarme della soglia inferiore.
  - *Definizione di superiore e inferiore*: i valori superiori e inferiori attivano l'allarme.
- **Intervallo**: immettere l'intervallo dell'allarme in secondi.
- **Titolare**: immettere il nome dell'utente o del sistema di gestione di rete che riceve l'allarme.

PASSAGGIO 4 Fare clic su **Applica**. L'allarme RMON viene salvato nel file di configurazione esecuzione.

Visualizza log

Vedere **Visualizzazione dei log memoria**.

3

Amministrazione: log di sistema

In questa sezione viene descritta la funzione Log di sistema che consente al dispositivo di generare più log indipendenti. Ogni log è una serie di messaggi che descrivono gli eventi del sistema.

Il dispositivo genera i seguenti log locali:

- Log inviato all'interfaccia della console.
- Log scritto in un elenco ciclico di eventi registrati nella RAM che viene cancellato quando al riavvio del dispositivo.
- Log scritto in un file di log ciclico salvato nella memoria Flash e che viene conservato dopo il riavvio.

Inoltre, è possibile inviare messaggi a server SYSLOG remoti sotto forma di trap SNMP e messaggi SYSLOG.

In questa sezione vengono trattati i seguenti argomenti:

- **Configurazione delle impostazioni log di sistema**
- **Configurazione delle impostazioni di registrazione remote**
- **Visualizzazione dei log memoria**

Configurazione delle impostazioni log di sistema

È possibile attivare o disattivare l'accesso alla pagina Impostazioni di log e selezionare se aggregare i messaggi di log.

È possibile selezionare gli eventi per livello di gravità. Ogni messaggio di log ha un livello di gravità contrassegnato con la prima lettera del livello di gravità concatenato con un trattino (-) ad ogni lato (tranne per *Emergenza* che è indicato dalla lettera F). Per esempio, il messaggio di log "%INIT-I-InitCompleted: ... " ha un livello di gravità **I**, cioè *Informativo*.

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 per il sistema.
- *Notifica*: il sistema funziona correttamente, ma è stata generata una notifica per il sistema.
- *Informativo*: informazioni sul dispositivo.
- *Debug*: informazioni dettagliate su un evento.

È possibile selezionare diversi livelli di gravità per RAM e log Flash. Questi log vengono visualizzati, rispettivamente, nelle pagine Memoria RAM e Memoria Flash.

La selezione di un livello di gravità da memorizzare in un log provoca la memorizzazione automatica nel log di tutti gli eventi con gravità maggiore. Gli eventi con gravità minore non vengono memorizzati nel log.

Per esempio, se è stato selezionato **Avviso**, tutti i livelli di gravità **Avviso** e con livello di gravità maggiore vengono memorizzati nel log (Emergenza, Preallarme, Critico, Errori e Avviso). Non viene memorizzato nessun livello di gravità inferiore a **Avviso** (Notifica, Informativo e Debug).

Per impostare i parametri globali, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Log di sistema** > **Impostazioni di log**.

PASSAGGIO 2 Immettere i parametri.

- **Registrazione**: selezionare per attivare la registrazione di messaggi.
- **Aggregatore syslog**: selezionare per attivare l'aggregazione di messaggi e trap SYSLOG. Se attivato, vengono aggregati messaggi e trap SYSLOG contigui in un tempo di aggregazione massimo e poi inviati in un singolo messaggio. I messaggi aggregati vengono inviati nell'ordine di arrivo. Ogni messaggio indica il numero di volte che è stato aggregato.
- **Tempo di aggregazione max**: immettere l'intervallo di tempo in cui vengono aggregati i messaggi SYSLOG.

- **Identificatore origine**: consente di aggiungere un identificatore origine ai messaggi SYSLOG. Sono disponibili le seguenti opzioni:
  - *Nessuno*: l'identificatore origine non viene incluso nei messaggi SYSLOG.
  - *Nome host*: il nome host del sistema viene incluso nei messaggi SYSLOG.
  - *Indirizzo IPv4*: include l'indirizzo IPv4 dell'interfaccia di invio nei messaggi SYSLOG.
  - *Indirizzo IPv6*: include l'indirizzo IPv6 dell'interfaccia di invio nei messaggi SYSLOG.
  - *Definito dall'utente*: immettere una descrizione da includere nei messaggi SYSLOG.
- **Registrazione memoria RAM**: selezionare i livelli di gravità dei messaggi da registrare nella RAM.
- **Registrazione memoria Flash**: selezionare i livelli di gravità dei messaggi da registrare nella memoria Flash.

PASSAGGIO 3 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Configurazione delle impostazioni di registrazione remote

Nella pagina Server di log remoti è possibile definire i server SYSLOG remoti in cui vengono inviati i messaggi di log (utilizzando il protocollo SYSLOG). Per ogni server, è possibile configurare la gravità dei messaggi che riceverà.

Per definire i server SYSLOG, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Log di sistema** > **Server di registri remoti**.

PASSAGGIO 2 Immettere informazioni nei seguenti campi:

- Interfaccia IPv4 di origine: selezionare l'interfaccia di origine il cui indirizzo IPv4 verrà utilizzato come indirizzo IPv4 di origine nei messaggi SYSLOG inviati ai server SYSLOG.
- Interfaccia IPv6 di origine: selezionare l'interfaccia di origine il cui indirizzo IPv6 verrà utilizzato come indirizzo IPv6 di origine nei messaggi SYSLOG inviati ai server SYSLOG.

NOTA Se è selezionata l'opzione Auto, il sistema utilizza l'indirizzo IP definito nell'interfaccia in uscita come indirizzo IP di origine.

PASSAGGIO 3 Fare clic su **Aggiungi**.

PASSAGGIO 4 Immettere i parametri.

- **Definizione server**: selezionare se identificare il server di log remoti in base all'indirizzo IP o al nome.
- **Versione IP**: selezionare il formato IP supportato.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se IPv6 viene utilizzato). Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. L'indirizzo locale di un collegamento presenta un prefisso **FE80**, non è reindirizzabile e può essere utilizzato solo per le comunicazioni sulle rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento (se Collega locale - Tipo di indirizzo IPv6 è selezionato) dall'elenco.
- **Indirizzo IP/Nome server dei log**: immettere l'indirizzo IP o il nome di dominio del server dei log.
- **Porta UDP**: immettere la porta UDP a cui vengono inviati i messaggi di log.
- **Infrastruttura**: selezionare il valore di un'infrastruttura da cui i log di sistema vengono inviati al server remoto. È possibile assegnare un solo valore dell'infrastruttura a un server. L'impostazione di un secondo codice di infrastruttura causerà la rimozione del primo.
- **Descrizione**: immettere la descrizione di un server.
- **Gravità minima**: selezionare il livello minimo dei messaggi di log di sistema da inviare al server.

PASSAGGIO 5 Scegliere **Applica**. La pagina Aggiungi server di log remoti viene chiusa, il server SYSLOG viene aggiunto e il file di configurazione esecuzione viene aggiornato.

Visualizzazione dei log memoria

Il dispositivo può scrivere nei seguenti log:

- Log nella RAM (cancellato durante il riavvio).
- Log nella memoria Flash (cancellato solo su comando dell'utente).

È possibile configurare i messaggi scritti in ogni log per gravità e un messaggio può essere inviato a più di un log, inclusi i log che si trovano nei server SYSLOG esterni.

Memoria RAM

Nella pagina Memoria RAM vengono visualizzati tutti i messaggi salvati nella RAM (cache) in ordine cronologico. Le voci vengono memorizzate nel log della RAM in base alla configurazione della pagina Impostazioni di log.

Per visualizzare le voci, fare clic su **Stato e statistiche** > **Visualizza log** > **Memoria RAM**.

Nella parte superiore della pagina è disponibile un pulsante che permette di disattivare l'icona di avviso lampeggiante. **Fare clic** per attivare e disattivare l'opzione correlata.

In questa pagina vengono forniti i seguenti campi:

- **Indice dei log**: numero voce del log.
- **Ora di log**: ora in cui è stato generato il messaggio.
- **Gravità**: gravità evento.
- **Descrizione**: messaggio di testo che descrive l'evento.

Per cancellare i messaggi di log, fare clic su **Cancella log**. I messaggi vengono cancellati.

Memoria FLASH

Nella pagina Memoria Flash vengono visualizzati i messaggi memorizzati nella memoria Flash in ordine cronologico. La gravità minima per la registrazione viene configurata nella pagina Impostazioni di log. Al riavvio del dispositivo i log di Flash vengono conservati. È possibile cancellare i log manualmente.

Per visualizzare i log Flash, fare clic su **Stato e statistiche** > **Visualizza log** > **Memoria Flash**.

In questa pagina vengono forniti i seguenti campi:

- **Indice dei log**: numero voce del log.
- **Ora di log**: ora in cui è stato generato il messaggio.
- **Gravità**: gravità evento.
- **Descrizione**: messaggio di testo che descrive l'evento.

Per cancellare i messaggi, fare clic su **Cancella log**. I messaggi vengono cancellati.

4

Amministrazione: gestione di file

In questa sezione viene descritta la modalità di gestione dei file di sistema

e vengono trattati i seguenti argomenti:

- **File di sistema**
- **Aggiornamento/Backup del firmware/Lingua**
- **Immagine attiva**
- **Download/Configurazione backup/Log**
- **Proprietà dei file di configurazione**
- **Copia/Salva configurazione**
- **Configurazione automatica tramite DHCP**

File di sistema

I file di sistema sono file che contengono le informazioni sulla configurazione, le immagini di firmware e il codice di avvio.

Con questi file si possono eseguire varie operazioni, tra cui selezionare il file del firmware che consente di avviare il dispositivo, copiare i vari tipi di file di configurazione internamente al dispositivo o copiare i file su o da un dispositivo esterno (ad esempio un server esterno).

I possibili metodi di trasferimento di file sono:

- Copia interna.
- HTTP/HTTPS, che utilizza le risorse fornite dal browser.
- Client TFTF/SCP, che richiede un server TFTP/SCP.

I file di configurazione nel dispositivo vengono definiti dal loro *tipo* e contengono le impostazioni e i valori dei parametri per il dispositivo.

Il riferimento a una configurazione nel dispositivo è dato dal *tipo di file di configurazione (ad esempio configurazione di avvio o configurazione di esecuzione)* e non da un nome file che può essere modificato dall'utente.

I contenuti possono essere copiati da un tipo di file di configurazione all'altro ma i nomi dei tipi di file non possono essere modificati dall'utente.

Gli altri file nel dispositivo, che includono firmware, codice di avvio e file di registro, sono denominati *file operativi*.

I file di configurazione sono file di testo e possono essere modificati in un editor di testo come Blocco note dopo essere stati copiati in un dispositivo esterno (ad esempio un PC).

File e tipi di file

Nel dispositivo sono disponibili i seguenti tipi di file di configurazione e di file operativi:

- **Configurazione di esecuzione**: contiene i parametri attualmente utilizzati dal dispositivo per il suo funzionamento. Questo è l'unico tipo di file che viene modificato quando si cambiano i valori dei parametri sul dispositivo.

  Se il dispositivo viene riavviato, la configurazione di esecuzione viene persa. La configurazione di avvio, memorizzata nella memoria Flash, sovrascrive la configurazione di esecuzione memorizzata nella RAM.

  Per mantenere le modifiche apportate al dispositivo, è necessario salvare la configurazione di esecuzione nella configurazione di avvio o in un altro tipo di file.

- **Configurazione di avvio**: i valori del parametro salvati dall'utente copiando un'altra configurazione (di solito la Configurazione di esecuzione) nella Configurazione di avvio.

  La configurazione di avvio è conservata nella memoria Flash e viene mantenuta a ogni riavvio del dispositivo. A questo punto, la Configurazione di avvio viene copiata nella memoria RAM e identificata come la Configurazione di esecuzione.

- **Configurazione mirror**: una copia della configurazione di avvio, creata dal dispositivo nelle seguenti condizioni:

  - Il dispositivo è stato in funzione ininterrottamente per 24 ore.
  - Non è stata apportata nessuna modifica alla Configurazione di esecuzione nelle 24 ore precedenti.

- La Configurazione di avvio è identica alla Configurazione di esecuzione.

Solo il sistema può copiare la Configurazione di avvio nella Configurazione mirror. Tuttavia, è possibile eseguire copie dalla Configurazione mirror in altri tipi di file o in un altro dispositivo.

L'opzione di copia automatica della configurazione di esecuzione nella configurazione mirror può essere disattivata nella pagina Proprietà file di configurazione.

- **Configurazione di backup**: una copia manuale di un file di configurazione utilizzato per la protezione contro l'arresto del sistema o per il mantenimento di uno stato operativo specifico. È possibile copiare la Configurazione mirror, la Configurazione di avvio o la Configurazione di esecuzione in un file di Configurazione di backup. La Configurazione di backup è presente in Flash e viene mantenuta anche se il dispositivo viene riavviato.
- **Firmware**: il programma che controlla il funzionamento e le funzionalità del dispositivo. Comunemente definito *immagine*.
- **Codice di avvio**: controlla l'avvio del sistema di base e lancia l'immagine firmware.
- **File di lingua**: il vocabolario che consente alle finestre dell'utilità di configurazione basata sul Web di essere visualizzate nella lingua selezionata.
- **Log Flash**: messaggi SYSLOG memorizzati in memoria Flash.

Azioni su file

Per gestire firmware e file di configurazione è possibile eseguire le azioni seguenti:

- Aggiornare il firmware o il codice di avvio, oppure sostituire la seconda lingua come descritto nella sezione **Aggiornamento/Backup del firmware/Lingua**.
- Visualizzare l'immagine firmware in uso oppure selezionare l'immagine da utilizzare al riavvio successivo come descritto nella sezione **Immagine attiva**.
- Salvare i file di configurazione nel dispositivo in una posizione in un altro dispositivo come descritto nella sezione **Download/Configurazione backup/Log**.

- Cancellare i tipi di file della Configurazione di avvio o della Configurazione di backup come descritto nella sezione **Proprietà dei file di configurazione**.
- Copiare un tipo di file di configurazione in un altro tipo di file di configurazione come descritto nella sezione **Copia/Salva configurazione**.
- Attivare il caricamento automatico di un file di configurazione da un server DHCP nel dispositivo, come descritto nella sezione **Configurazione automatica tramite DHCP**.

In questa sezione vengono illustrati i seguenti argomenti:

- **Aggiornamento/Backup del firmware/Lingua**
- **Immagine attiva**
- **Download/Configurazione backup/Log**
- **Proprietà dei file di configurazione**
- **Copia/Salva configurazione**
- **Configurazione automatica tramite DHCP**

Aggiornamento/Backup del firmware/Lingua

La procedura di **Aggiornamento/Backup del firmware/Lingua** può essere utilizzata per:

- Eseguire l'aggiornamento o il backup dell'immagine firmware.
- Eseguire l'aggiornamento o il backup del codice di avvio.
- Importare o aggiornare un secondo file di lingua.

Sono supportati i seguenti metodi di trasferimento dei file:

- HTTP/HTTPS, che utilizza le risorse fornite dal browser.
- TFTP, che richiede un server TFTP.
- SCP (Secure Copy Protocol), che richiede un server SCP.

Se è stato caricato un nuovo file di lingua nel dispositivo, la nuova lingua può essere selezionata dalla casella a discesa (non è necessario riavviare il dispositivo). Il file della lingua viene copiato automaticamente in tutti i dispositivi nello stack.

Per garantire il corretto funzionamento dello stack, è necessario che tutte le immagini software nello stack siano uguali. Se si aggiunge un dispositivo a uno stack e la relativa immagine software non è identica all'immagine software dell'unità master, quest'ultima carica automaticamente l'immagine corretta sul nuovo dispositivo.

Esistono due diversi metodi per aggiornare le immagini all'interno dello stack:

- È possibile caricare l'immagine prima di collegare l'unità allo stack (scelta consigliata).
- Aggiornamento dispositivo o stack. Se viene aggiornato lo stack, le unità dipendenti vengono aggiornate automaticamente. Questo viene eseguito nel modo seguente:
  - Utilizzare la pagina Aggiornamento/Backup del firmware/Lingua per copiare l'immagine dal server TFTP/SCP all'unità master.
  - Utilizzare la pagina Immagine attiva per modificare l'immagine attiva.
  - Utilizzare la pagina Riavvia per riavviare.

Nel dispositivo sono memorizzate due immagini firmware. Una delle immagini viene identificata come l'*immagine attiva* e l'altra viene identificata come l'*immagine inattiva*.

Quando si aggiorna il firmware, la nuova immagine sostituisce sempre l'immagine identificata come immagine inattiva.

Anche dopo aver caricato il nuovo firmware, il dispositivo verrà avviato con l'immagine attiva (la versione precedente) fino a quando la nuova immagine non viene impostata come immagine attiva, come descritto nella sezione **Immagine attiva**. Avviare, quindi, il dispositivo.

NOTA Se il dispositivo funziona in modalità stack, il nuovo firmware viene caricato su tutte le unità dello stack. Se allo stack si aggiunge un nuovo dispositivo con una versione firmware diversa, l'unità master sincronizza automaticamente la versione firmware con l'unità appena collegata. Ciò avviene in modo chiaro, senza alcun intervento manuale.

File di aggiornamento/backup del firmware o della lingua

Per aggiornare o eseguire il backup di un'immagine software o di un file della lingua, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Gestione di file** > **Aggiornamento/Backup del firmware/Lingua**.

PASSAGGIO 2 Fare clic sul Metodo di trasferimento. Procedere come indicato:

- Se è stato selezionato il metodo **TFTP**, andare al **PASSAGGIO 3**.
- Se è stato selezionato il metodo **tramite HTTP/HTTPS**, andare al **PASSAGGIO 4**.
- Se è stato selezionato il metodo **SCP**, andare al **PASSAGGIO 5**.

PASSAGGIO 3 Se è stato selezionato il metodo **tramite TFTP**, immettere i parametri come descritto in questo passaggio. Altrimenti, andare al **PASSAGGIO 4**.

Selezionare una delle seguenti **operazioni di salvataggio**:

- **Aggiorna**: specifica che è necessario sostituire il tipo di file nel dispositivo con una nuova versione presente su un server TFTP.
- **Backup**: indica che è necessario salvare una copia del tipo di file in un file su un altro dispositivo.

Immettere informazioni nei seguenti campi:

- **Tipo di file**: selezionare il tipo di file di destinazione. Vengono mostrati solo i tipi di file validi (i tipi di file sono descritti nella sezione **File e tipi di file**).
- **Definizione server TFTP**: selezionare se specificare il server TFTP in base all'indirizzo IP o al nome del dominio.
- **Versione IP**: selezionare se viene utilizzato un indirizzo IPv4 o IPv6.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se IPv6 viene utilizzato). Sono disponibili le seguenti opzioni:
  - **Collega locale**: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale di collegamento presenta un prefisso FE80, non è instradabile e può essere utilizzato solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.

- **Globale**: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.

- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento (se viene utilizzato IPv6) dall'elenco.
- **Indirizzo IP/Nome server TFTP**: immettere l'indirizzo IP o il nome di dominio del server TFTP.
- **(Per aggiornamento) Nome file di origine**: immettere il nome del file di origine.
- **(Per Backup) Nome file di destinazione**: immettere il nome del file di backup.

PASSAGGIO 4 Se è stato selezionato il metodo **tramite HTTP/HTTPS**, è possibile eseguire solo l'**aggiornamento**. Immettere i parametri come descritto in questo passaggio.

- **Tipo di file**: selezionare uno dei seguenti tipi:
  - *Immagine firmware*: selezionare questa opzione per aggiornare l'immagine firmware.
  - *Lingua*: selezionare questa opzione per aggiornare il file di lingua.
- **Nome file**: fare clic su **Sfoglia** per selezionare un file oppure immettere il percorso e il nome del file di origine da utilizzare durante il trasferimento.

PASSAGGIO 5 Se è stato selezionato il metodo tramite **SCP (tramite SSH),** vedere **Autenticazione del client SSH** per le istruzioni, quindi compilare i seguenti campi (vengono descritti solo i campi univoci; per gli altri campi vedere le descrizioni riportate sopra):

- **Autenticazione del server SSH remoto**: per abilitare l'autenticazione del server SSH (per impostazione predefinita non è attiva), scegliere **Modifica**. L'utente verrà reindirizzato alla pagina **Autenticazione del server SSH** per configurare il server SSH e tornare poi alla pagina corrente. Nella pagina **Autenticazione del server SSH**, selezionare un metodo di autenticazione utente SSH (password o chiave pubblica/privata), impostare nome utente e password nel dispositivo (se il metodo password viene selezionato) e, se necessario, creare una chiave RSA o DSA.

Autenticazione del client SSH: l'autenticazione client può essere eseguita in uno dei seguenti modi:

- **Utilizza credenziali di sistema client SSH**: imposta le credenziali utente SSH definitive. Fare clic su **Credenziali di sistema** per accedere alla pagina Autenticazione degli utenti SSH in cui è possibile impostare il nome utente e la password da utilizzare in futuro.
- **Utilizza le credenziali monouso del client SSH**: consente di immettere le informazioni riportate di seguito.
  - *Nome utente*: inserire un nome utente per questa azione di copia.
  - *Password*: immettere una password per questa copia.

  NOTA Il nome utente e la password monouso non verranno salvate nel file di configurazione.

Selezionare una delle seguenti **operazioni di salvataggio**:

- **Aggiorna**: specifica che è necessario sostituire il tipo di file nel dispositivo con una nuova versione presente su un server TFTP.
- **Backup**: indica che è necessario salvare una copia del tipo di file in un file su un altro dispositivo.

Immettere informazioni nei seguenti campi:

- **Tipo di file**: selezionare il tipo di file di destinazione. Vengono mostrati solo i tipi di file validi (i tipi di file sono descritti nella sezione **File e tipi di file**).
- **Definizione server SCP**: selezionare se specificare il server SCP in base all'indirizzo IP o al nome del dominio.
- **Versione IP**: selezionare se viene utilizzato un indirizzo IPv4 o IPv6.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se utilizzato). Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. L'indirizzo locale di un collegamento presenta un prefisso **FE80**, non è reindirizzabile e può essere utilizzato solo per le comunicazioni sulle rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.

- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento dall'elenco.
- **Indirizzo IP/Nome server SCP**: immettere l'indirizzo IP o il nome di dominio del server SCP.
- **(Per aggiornamento) Nome file di origine**: immettere il nome del file di origine.
- **(Per Backup) Nome file di destinazione**: immettere il nome del file di backup.

PASSAGGIO 6 Fare clic su **Applica**. Se i file, le password e gli indirizzi server sono corretti, può verificarsi uno dei seguenti scenari:

- Se l'autenticazione del server SSH è attiva (nella pagina Autenticazione server SSH) e il server SCP è attendibile, l'operazione ha esito positivo. Se il server SCP non è attendibile, l'operazione non sarà completata e verrà visualizzato un errore.
- Se l'autenticazione del server SSH non è attiva, l'operazione andrà a buon fine per tutti i server SCP.

Immagine attiva

Nel dispositivo sono memorizzate due immagini firmware. Una delle immagini viene identificata come l'*immagine attiva* e l'altra viene identificata come l'*immagine inattiva*. Il dispositivo viene avviato dall'immagine impostata come *immagine attiva*. È possibile cambiare l'immagine identificata come l'*immagine inattiva* nell'*immagine attiva* (è possibile riavviare il dispositivo mediante la procedura descritta nella sezione **Interfaccia di gestione**).

Per selezionare l'immagine attiva, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Gestione di file** > **Immagine attiva**.

Nella pagina vengono visualizzati gli elementi seguenti:

- **Immagine attiva**: viene visualizzato il file di immagine attivo al momento nel dispositivo.
- **Numero di versione immagine attiva**: viene visualizzata la versione del firmware dell'immagine attiva.

- **Immagine attiva dopo il riavvio**: viene visualizzata l'immagine attiva dopo il riavvio.
- **Numero di versione immagine attiva dopo il riavvio**: viene visualizzata la versione del firmware dell'immagine attiva dopo il riavvio.

PASSAGGIO 2 Selezionare l'immagine dal menu **Immagine attiva dopo il riavvio** per identificare l'immagine del firmware utilizzata come immagine attiva dopo il riavvio del dispositivo. Nel campo **Numero di versione immagine attiva dopo il riavvio** viene visualizzata la versione dell'immagine attiva utilizzata dopo il riavvio del dispositivo.

PASSAGGIO 3 Fare clic su **Applica**. La selezione dell'immagine attiva viene aggiornata.

Download/Configurazione backup/Log

La pagina Download/Configurazione backup/Log consente di:

- Eseguire il backup dei file di configurazione o dei log dal dispositivo a un dispositivo esterno.
- Ripristinare i file di configurazione da un dispositivo esterno al dispositivo.

NOTA Se il dispositivo funziona in modalità stack, i file di configurazione vengono acquisiti dall'unità master.

Durante il ripristino di un file di configurazione nella configurazione di esecuzione, il file importato *aggiunge* i comandi di configurazione non esistenti nel vecchio file e *sovrascrive* i valori dei parametri dei comandi di configurazione esistenti.

Durante il ripristino di un file di configurazione sulla Configurazione di avvio o di un file di configurazione di backup, il nuovo file *sostituisce* quello precedente.

Durante il ripristino nella configurazione di avvio, è necessario riavviare il dispositivo per poter utilizzare il file di configurazione avvio ripristinato come configurazione di esecuzione. Per riavviare il dispositivo, attenersi alla procedura descritta nella sezione **Interfaccia di gestione**.

Compatibilità all'indietro del file di configurazione

Durante il ripristino dei file di configurazione da un dispositivo esterno al dispositivo, possono verificarsi i seguenti problemi di compatibilità

- **Modifica della modalità code da 4 a 8**: le configurazioni legate alle code devono essere esaminate e impostate per soddisfare gli obiettivi QoS con la nuova modalità code. Per un elenco dei comandi QoS, vedere la *Guida di riferimento CLI*.
- **Modifica della modalità code da 8 a 4**: i comandi di configurazione legati alle code che entrano in conflitto con la nuova modalità code vengono rifiutati; ciò significa che il download del file di configurazione non riesce. Utilizzare la pagina Modalità sistema e Gestione stack per modificare la modalità code.
- **Modifica della modalità di sistema**: se la modalità di sistema è inclusa in un file di configurazione che viene scaricato sul dispositivo e la modalità di sistema del file corrisponde a quella corrente, questa informazione viene ignorata. In caso contrario, se la modalità di sistema è stata modificata, sono possibili i seguenti casi:
  - Se il file di configurazione viene scaricato sul dispositivo (tramite la pagina Download/Configurazione backup/Log), l'operazione viene interrotta e viene visualizzato un messaggio che indica la necessità di cambiare la modalità di sistema nella pagina Modalità sistema e Gestione stack.
  - Se il file di configurazione viene scaricato durante un processo di configurazione automatica, il file di configurazione avvio viene eliminato e il dispositivo viene riavviato automaticamente nella nuova modalità di sistema. Il dispositivo viene configurato con un file di configurazione vuoto. Vedere la sezione **Configurazione automatica tramite DHCP**.
- Per una descrizione di ciò che accade quando si modificano le modalità stack, vedere la sezione **Configurazione dopo il riavvio**.

Download o backup di un file di configurazione o di log

Per eseguire il backup o il ripristino del file di configurazione di sistema, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Gestione di file** > **Download/Configurazione backup/Log**.

PASSAGGIO 2 Selezionare il **Metodo di trasferimento**.

PASSAGGIO 3 Se è stato selezionato il metodo **tramite TFTP**, immettere i parametri. Altrimenti, andare al **PASSAGGIO 4**.

Selezionare il processo di download o backup per **Salva azione**.

Scarica - Salva azione: indica che un tipo di file sul dispositivo viene sostituito dal file di un altro dispositivo. Immettere informazioni nei seguenti campi:

a. **Definizione server**: selezionare se specificare il server TFTP in base all'indirizzo IP o al nome del dominio.

b. **Versione IP**: selezionare se viene utilizzato un indirizzo IPv4 o IPv6.

> **NOTA** Se in Definizione server il server viene selezionato in base al nome, non occorre selezionare le opzioni relative alla versione IP.

c. **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se utilizzato). Sono disponibili le seguenti opzioni:

- *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. L'indirizzo locale di un collegamento presenta un prefisso **FE80**, non è reindirizzabile e può essere utilizzato solo per le comunicazioni sulle rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
- *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.

d. **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento dall'elenco.

e. **Server TFTP**: immettere l'indirizzo IP del server TFTP.

f. **Nome file di origine**: immettere il nome del file di origine. I nomi dei file non possono contenere barre (\ or /), non possono iniziare con un punto (.) e la lunghezza deve essere compresa tra 1 e 160 caratteri (caratteri validi: A-Z, a-z, 0-9, ".", "-", "_").

g. **Tipo file di destinazione**: immettere il tipo di file di configurazione di destinazione. Vengono visualizzati solo i tipi di file validi (i tipi di file sono descritti nella sezione **File e tipi di file**).

Backup - Salva azione: indica che un tipo di file deve essere copiato in un file su un altro dispositivo. Immettere informazioni nei seguenti campi:

a. **Definizione server**: selezionare se specificare il server TFTP in base all'indirizzo IP o al nome del dominio.

b. **Versione IP**: selezionare se viene utilizzato un indirizzo IPv4 o IPv6.

c. **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se utilizzato). Sono disponibili le seguenti opzioni:

- *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. L'indirizzo locale di un collegamento presenta un prefisso **FE80**, non è reindirizzabile e può essere utilizzato solo per le comunicazioni sulle rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
- *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.

d. **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento dall'elenco.

e. **Indirizzo IP/Nome server TFTP**: immettere l'indirizzo IP o il nome di dominio del server TFTP.

f. **Tipo file di origine**: immettere il tipo di file di configurazione di origine. Vengono visualizzati solo i tipi di file validi (i tipi di file sono descritti nella sezione **File e tipi di file**).

g. **Dati sensibili**: selezionare il modo in cui i dati sensibili devono essere inclusi nel file di backup. Sono disponibili le seguenti opzioni:

  - *Escludi*: non includere i dati sensibili nel backup.
  - *Con crittografia*: includere i dati sensibili nel backup in forma crittografata.
  - *Testo normale*: includere i dati sensibili nel backup in forma testo normale.

NOTA Le opzioni disponibili per i dati sensibili sono determinate dalle regole SSD dell'utente corrente. Per i dettagli, consultare la pagina Gestione sicura dei dati sensibili > Regole SSD.

h. **Nome file di destinazione**: immettere il nome del file di destinazione. I nomi dei file non possono contenere barre (\ o /), la prima lettera del nome del file non può essere un punto (.) e la lunghezza dei nomi dei file deve essere compresa tra 1 e 160 caratteri (caratteri validi: A-Z, a-z, 0-9, ".", "-", "_").

i. Fare clic su **Applica**. Viene eseguito l'aggiornamento o il backup del file.

PASSAGGIO 4 Se è stato selezionato il metodo **tramite HTTP/HTTPS**, immettere i parametri come descritto in questo passaggio.

Selezionare **Salva azione**.

Se l'opzione **Salva azione** è impostata su *Scarica* (sostituzione del file nel dispositivo con una nuova versione proveniente da un altro dispositivo), attenersi alla seguente procedura. Altrimenti, andare alla procedura successiva di questo passaggio.

a. **Nome file di origine**: fare clic su **Sfoglia** per selezionare un file oppure immettere il percorso e il nome del file di origine da utilizzare durante il trasferimento.

b. **Tipo file di destinazione**: selezionare il tipo di file di configurazione. Vengono visualizzati solo i tipi di file validi (i tipi di file sono descritti nella sezione **File e tipi di file**).

c. Fare clic su **Applica**. Il file viene trasferito dall'altro dispositivo al dispositivo.

Se **Salva azione** è *Backup* (copia di un file su un altro dispositivo), attenersi alla seguente procedura:

a. **Tipo file di origine**: selezionare il tipo di file di configurazione. Vengono visualizzati solo i tipi di file validi (i tipi di file sono descritti nella sezione **File e tipi di file**).

b. **Dati sensibili**: selezionare il modo in cui i dati sensibili devono essere inclusi nel file di backup. Sono disponibili le seguenti opzioni:

- *Escludi*: non includere i dati sensibili nel backup.
- *Con crittografia*: includere i dati sensibili nel backup in forma crittografata.
- *Testo normale*: includere i dati sensibili nel backup in forma testo normale.

NOTA Le opzioni disponibili per i dati sensibili sono determinate dalle regole SSD dell'utente corrente. Per i dettagli, consultare la pagina Gestione sicura dei dati sensibili > Regole SSD.

c. Fare clic su **Applica**. Viene eseguito l'aggiornamento o il backup del file.

PASSAGGIO 5 Se è stato selezionato il metodo tramite **SCP (tramite SSH)**, vedere **Configurazione del client SSH mediante l'interfaccia utente** per le istruzioni, quindi compilare i seguenti campi:

- **Autenticazione del server remoto SSH**: per abilitare l'autenticazione del server SSH (per impostazione predefinita non è attiva), scegliere **Modifica**; l'utente verrà reindirizzato alla pagina **Autenticazione del server SSH** per eseguire la configurazione e tornare poi alla pagina corrente. Nella pagina **Autenticazione del server SSH**, selezionare un metodo di autenticazione utente SSH (password o chiave pubblica/privata), impostare nome utente e password nel dispositivo (se il metodo password viene selezionato) e, se necessario, creare una chiave RSA o DSA.

Autenticazione del client SSH: l'autenticazione client può essere eseguita in uno dei seguenti modi:

- **Utilizza client SSH**: imposta le credenziali utente SSH definitive. Fare clic su **Credenziali di sistema** per accedere alla pagina Autenticazione degli utenti SSH in cui è possibile impostare il nome utente e la password da utilizzare in futuro.
- **Utilizza le credenziali monouso del client SSH**: consente di immettere le informazioni riportate di seguito.
  - *Nome utente*: inserire un nome utente per questa azione di copia.
  - *Password*: immettere una password per questa copia.
- **Definizione server SCP**: selezionare se specificare il server TFTP in base all'indirizzo IP o al nome del dominio.
- **Versione IP**: selezionare se viene utilizzato un indirizzo IPv4 o IPv6.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se utilizzato). Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. L'indirizzo locale di un collegamento presenta un prefisso **FE80**, non è reindirizzabile e può essere utilizzato solo per le comunicazioni sulle rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.

- *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.

- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento dall'elenco.
- **Indirizzo IP/Nome server SCP**: immettere l'indirizzo IP o il nome di dominio del server TFTP.

Se l'opzione **Salva azione** è impostata su *Scarica* (sostituzione del file nel dispositivo con una nuova versione proveniente da un altro dispositivo), compilare i campi seguenti.

- **Nome file di origine**: immettere il nome del file di origine.
- **Tipo file di destinazione**: selezionare il tipo di file di configurazione. Vengono visualizzati solo i tipi di file validi (i tipi di file sono descritti nella sezione **File e tipi di file**).

Se **Salva azione** è *Backup* (copia di un file su un altro dispositivo), compilare i seguenti campi (oltre a quelli elencati sopra):

- **Tipo file di origine**: selezionare il tipo di file di configurazione. Vengono visualizzati solo i tipi di file validi (i tipi di file sono descritti nella sezione **File e tipi di file**).
- **Dati sensibili**: selezionare il modo in cui i dati sensibili devono essere inclusi nel file di backup. Sono disponibili le seguenti opzioni:
  - *Escludi*: non includere i dati sensibili nel backup.
  - *Con crittografia*: includere i dati sensibili nel backup in forma crittografata.
  - *Testo normale*: includere i dati sensibili nel backup in forma testo normale.

  NOTA Le opzioni disponibili per i dati sensibili sono determinate dalle regole SSD dell'utente corrente. Per i dettagli, consultare la pagina Gestione sicura dei dati sensibili > Regole SSD.
- **Nome file di destinazione**: nome del file su cui viene copiato.

PASSAGGIO 6 Fare clic su **Applica**. Viene eseguito l'aggiornamento o il backup del file.

Proprietà dei file di configurazione

La pagina Proprietà file di configurazione consente di vedere la data di creazione dei vari file di configurazione del sistema. Permette anche di eliminare i file della configurazione di avvio e quelli della configurazione di backup. Non è possibile eliminare gli altri tipi di file di configurazione.

NOTA Se il dispositivo funziona in modalità stack, i file di configurazione vengono acquisiti dall'unità master.

Per decidere se creare i file di configurazione mirror, cancellare i file di configurazione e vedere la relativa data di creazione, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Gestione di file** > **Proprietà file di configurazione**.

In questa pagina vengono visualizzati i seguenti campi:

- **Nome file di configurazione**: il tipo di file di sistema.
- **Data/ora di creazione**: la data e l'ora in cui è stato modificato il file.

PASSAGGIO 2 Se necessario, disattivare **Configurazione mirror automatica**. In questo modo si disattiva la creazione automatica dei file di configurazione mirror. Quando si disabilita tale funzione, il file di configurazione mirror (se esiste) viene eliminato. Vedere **File di sistema** per la descrizione dei file mirror e del perché si potrebbe non voler creare automaticamente i file di configurazione mirror.

PASSAGGIO 3 Se necessario, selezionare i file Configurazione di avvio, Configurazione di backup o entrambi, quindi fare clic su **Elimina file** per eliminarli.

Copia/Salva configurazione

Quando si fa clic su **Applica** in qualsiasi finestra, le modifiche apportate alle impostazioni di configurazione del dispositivo vengono memorizzate *solo* nella configurazione di esecuzione. Per conservare i parametri nella Configurazione di esecuzione, è necessario copiare la Configurazione di esecuzione in un altro tipo di configurazione oppure salvarla in un altro dispositivo.

ATTENZIONE Al riavvio del dispositivo tutte le modifiche apportate dall'ultima volta che il file è stato copiato andranno perse, a meno che la configurazione di esecuzione non venga copiata nella configurazione di avvio o in un altro file di configurazione.

Sono consentite le seguenti combinazioni di copia di tipi di file interni:

- Dalla Configurazione di esecuzione alla Configurazione di avvio o Configurazione di backup.
- Dalla Configurazione di avvio alla Configurazione di esecuzione, Configurazione di avvio o Configurazione di backup.
- Dalla Configurazione di backup alla Configurazione di esecuzione, Configurazione di avvio o Configurazione di backup.
- Dalla Configurazione mirror alla Configurazione di esecuzione, Configurazione di avvio o Configurazione di backup.

Per copiare un tipo di file di configurazione su un altro tipo di file di configurazione, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Gestione di file** > **Copia/Salva configurazione**.

PASSAGGIO 2 Selezionare il **Nome file di origine** da copiare. Solo i tipi di file validi vengono visualizzati (descritti nella sezione **File e tipi di file**).

PASSAGGIO 3 Selezionare il **Nome file di destinazione** da sovrascrivere con il file di origine.

- Se si esegue il backup di un file di configurazione, selezionare uno dei seguenti formati per il file di backup.
  - **Escludi**: i dati sensibili non vengono inclusi nel file di backup.
  - **Con crittografia**: i dati sensibili vengono inclusi nel file di backup in forma crittografata.
  - **Testo normale**: i dati sensibili vengono inclusi nel file di backup in formato testo normale.

  NOTA Le opzioni disponibili per i dati sensibili sono determinate dalle regole SSD dell'utente corrente. Per i dettagli, consultare la pagina Gestione sicura dei dati sensibili > Regole SSD.

PASSAGGIO 4 Il campo **Icona di salvataggio lampeggiante** indica che l'icona lampeggia quando ci sono dati non salvati. Per abilitare/disabilitare tale funzione, scegliere **Attiva/disattiva icona di salvataggio lampeggiante**.

PASSAGGIO 5 Fare clic su **Applica**. Il file viene copiato.

Configurazione automatica tramite DHCP

La configurazione automatica DHCP consente di trasmettere le informazioni sulla configurazione agli host in una rete TCP/IP. In base a questo protocollo, la funzione di configurazione automatica permette al dispositivo di scaricare i file di configurazione da un server TFTP/SCP.

Per utilizzare questa funzione, il dispositivo deve essere configurato come client DHCPv4 che supporta la configurazione automatica da un server DHCPv4 e/o come client DHCPv6 che supporta la configurazione automatica da un server DHCPv6.

Se la funzione di configurazione automatica tramite DHCP è attiva, il dispositivo viene attivato per impostazione predefinita come client DHCP.

Il processo di configurazione automatica supporta inoltre il download di un file di configurazione che includa informazioni sensibili, ad esempio le chiave del server RADIUS e le chiavi SSH/SSL, tramite SCP (Secured Copy Protocol) e SSD (Secure Sensitive Data); vedere **Protezione: gestione sicura dei dati sensibili**.

La procedura di configurazione automatica tramite DHCPv4 viene attivata nei seguenti casi:

- Dopo il riavvio quando viene allocato o rinnovato dinamicamente (tramite DHCPv4) un indirizzo IP.
- Durante un'esplicita richiesta di rinnovo DHCPv4 e se il dispositivo e il server vengono configurati a tale scopo.
- Durante un rinnovo automatico del lease DHCPv4.

La procedura di configurazione automatica tramite DHCPv6 viene attivata quando vengono soddisfatte le seguenti condizioni:

- Quando un server DHCPv6 invia informazioni al dispositivo. Questo avviene nei casi seguenti:
  - Quando un'interfaccia, che consente IPv6, viene definita come client di configurazione stateless DHCPv6.
  - Quando i messaggi DHCPv6 vengono ricevuti dal server, ad esempio quando si fa ci sul pulsante **Riavvia** nella pagina Interfacce IPv6.
  - Quando le informazioni DHCPv6 vengono aggiornate dal dispositivo.
  - Dopo aver riavviato il dispositivo quando è attivato il client DHCPv6 stateless.
- Quando i pacchetti server DHCPv6 contengono l'opzione nome file di configurazione.

Opzioni server DHCP

I messaggi DHCP possono contenere l'indirizzo o il nome del server di configurazione e il percorso o il nome del file di configurazione (opzioni facoltative). Queste opzioni si trovano nel messaggio **Offerta** proveniente dai server DHCPv4 e nei messaggi **Risposta sulle informazioni** provenienti dai server DHCPv6.

Le informazioni di backup (indirizzo/nome del server di configurazione e percorso/nome del file di configurazione) possono essere configurate nella pagina Configurazione automatica. Queste informazioni vengono utilizzate quando il messaggio DHCPv4 non le contiene (ma non sono utilizzate da DHCPv6).

Protocollo di download della configurazione automatica (TFTP o SCP)

È possibile configurare il protocollo di download della configurazione automatica nel modo seguente:

- **Automatico per estensione del file**: (impostazione predefinita) se questa opzione è selezionata, un'estensione del file definita dall'utente indica che i file con tale estensione vengono scaricati tramite SCP (su SSH), mentre i file con altre estensioni vengono scaricati tramite TFTP. Ad esempio, se l'estensione file specificata è *.xyz*, i file con estensione *.xyz* vengono scaricati tramite SCP e i file con altre estensioni tramite TFTP.

- **Solo TFTP**: il download viene eseguito tramite TFTP indipendentemente dall'estensione file del nome del file di configurazione.
- **Solo SCP**: il download viene eseguito tramite SCP (o SSH) indipendentemente dall'estensione file del nome del file di configurazione.

Parametri di autenticazione del client SSH

L'autenticazione del server SSH remoto è disattivata per impostazione predefinita, quindi il dispositivo accetta qualsiasi server SSH remoto out-of-the-box. È possibile attivare l'autenticazione del server SSH remoto per consentire esclusivamente connessioni dai server presenti nell'elenco dei server attendibili.

È necessario inserire i parametri di autenticazione del client SSH per accedere al server SSH dal client (cioè il dispositivo). I parametri predefiniti di autenticazione del client SSH sono:

- Metodo di autenticazione SSH: tramite l'inserimento di nome utente/ password.
- Nome utente SSH: anonima
- Password SSH: anonima

NOTA I parametri di autenticazione client SSH possono essere utilizzati anche quando si scarica un file per il download manuale (un download che non viene eseguito tramite la funzione di configurazione automatica DHCP).

Procedura di configurazione automatica

Quando viene avviata la procedura di configurazione automatica, si verificano i seguenti scenari:

- Si accede al server DHCP per acquisire l'indirizzo/il nome del server TFTP/ SCP e il percorso/il nome del file di configurazione (opzioni DHCPv4: 66,150, e 67; opzioni DHCPv6: 59 e 60).
- Se le opzioni per il server e il file di configurazione non vengono fornite dal server DHCP, allora:
  - **Per DHCPv4:** viene utilizzato il nome del file di configurazione di backup definito dall'utente.
  - **Per DHCPv6:** il processo viene interrotto.

- Se il server DHCP non ha inviato queste opzioni e il parametro dell'indirizzo del server di backup TFTP/SCP è vuoto, allora:
  - **Per DHCPv4:**

    SCP: il processo di configurazione automatica viene interrotto.

    TFTP: il dispositivo invia i messaggi di richiesta TFTP a un indirizzo broadcast limitato (per IPv4) o indirizzo ALL NODES (per IPv6) sulle sue interfacce IP e continua il processo di configurazione automatica con il primo server TFTP che risponde.
  - **Per DHCPv6:** il processo di configurazione automatica viene interrotto.
- Se il nome del file di configurazione è stato fornito dal server DHCP (DHCPv4: opzione 67; DHCPv6: opzione 60), allora viene selezionato il protocollo di copia (SCP/TFTP) come descritto in **Protocollo di download della configurazione automatica (TFTP o SCP)**.
- Quando si esegue un download tramite SCP, il dispositivo accetta qualsiasi server SCP/SSH (senza autenticazione) se sussiste una delle seguenti condizioni:
  - Il processo di autenticazione del server SSH è disattivato. Per impostazione predefinita, l'autenticazione del server SSH è disattivata per agevolare il download del file di configurazione per i dispositivi con configurazione predefinita (ad esempio i dispositivi nuovi).
  - Il server SSH viene configurato nell'elenco dei server SSH attendibili.

  Se il processo di autenticazione del server SSH viene attivato, ma nell'elenco dei server SSH attendibili non viene trovato il server SSH, la procedura di configurazione automatica viene interrotta.
- Se queste informazioni sono disponibili, viene effettuato l'accesso al server TFTP/SCP per scaricare il file.

  Il download viene eseguito solo se il nome del file è diverso da quello utilizzato per il file di configurazione (anche se l'attuale file di configurazione è vuoto).
- Al termine della procedura di configurazione automatica viene generato un messaggio SYSLOG.

Impostazione della configurazione automatica DHCP

Flusso di lavoro

Per definire la configurazione automatica DHCP, attenersi alla seguente procedura:

1. Configurare i server DHCPv4 e/o DHCPv6 per inviare le opzioni richieste. Questo processo non viene descritto in questa guida.
2. Impostare i parametri di configurazione automatica.
3. Definire il dispositivo come client DHCPv4 nelle pagine **Definizione di un'interfaccia IPv4 in modalità di sistema Livello 2** o **Definizione dell'interfaccia IPv4 in modalità di sistema Livello 3** e/o definire il dispositivo come client DHCPv6 nella pagina **Interfaccia IPv6**.

Configurazione Web

La pagina Configurazione automatica DHCP viene utilizzata per eseguire le seguenti azioni quando il messaggio DHCP non fornisce le informazioni necessarie:

- Attivare la funzione di configurazione automatica DHCP.
- Specificare il protocollo di download.
- Configurare il dispositivo per ricevere informazioni sulla configurazione da un file a un server specifico.

Tenere presente le seguenti informazioni relative alla procedura di configurazione automatica di DHCP:

- Un file di configurazione sul server TFTP/SCP deve corrispondere ai requisiti di formato del file di configurazione supportato. Il formato del file viene verificato ma la validità dei *parametri* di configurazione non viene verificata prima che venga caricato nella Configurazione di avvio.
- In IPv4, per garantire che la configurazione del dispositivo funzioni nel modo desiderato, a causa dell'allocazione di indirizzi IP diversi con ogni ciclo di rinnovo di DHCP, si consiglia di associare gli indirizzi IP agli indirizzi MAC nella tabella server DHCP. In questo modo viene garantito che ogni dispositivo ha il suo indirizzo IP riservato personale e altre informazioni importanti.

Per impostare la configurazione automatica, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Gestione di file** > **Configurazione automatica DHCP**.

PASSAGGIO 2 Immettere i valori.

- **Configurazione automatica tramite DHCP**: selezionare questo campo per attivare la configurazione automatica DHCP. Questa funzione è attiva per impostazione predefinita, ma può essere disattivata qui.
- **Protocollo di download**: selezionare una delle opzioni riportate di seguito.
  - *Automatico per estensione del file*: selezionare l'opzione per indicare che la configurazione automatica utilizza il protocollo TFTP o SCP, a seconda dell'estensione del file di configurazione. Selezionando questa opzione, non sarà necessario indicare l'estensione del file di configurazione. Se non indicata, viene utilizzata l'estensione predefinita (come indicato di seguito).
  - *Estensione del file per SCP*: se si seleziona **Automatico per estensione del file**, è possibile indicare l'estensione del file. I file con questa estensione vengono scaricati tramite SCP. Se non si inserisce alcuna estensione, viene utilizzata l'estensione predefinita **.scp**.
  - *Solo TFTP*: selezionare l'opzione per indicare l'utilizzo esclusivo del protocollo TFTP per la configurazione automatica.
  - *Solo SCP*: selezionare l'opzione per indicare l'utilizzo esclusivo del protocollo SCP per la configurazione automatica.
- **Impostazioni SSH per SCP**: se si utilizza SCP per scaricare i file di configurazione, selezionare una delle seguenti opzioni:
  - *Autenticazione del server SSH remoto*: fare clic sul collegamento **Attiva/Disattiva** per passare alla pagina Autenticazione del server SSH. A questo punto, è possibile attivare l'autenticazione del server SSH da utilizzare per il download e, se necessario, specificare il server SSH attendibile.
  - *Autenticazione del client SSH*: fare clic sul collegamento Credenziali del sistema per immettere le credenziali utente nella pagina Autenticazione degli utenti SSH.

PASSAGGIO 3 Immettere le seguenti informazioni facoltative da utilizzare se non è stato ricevuto alcun nome del file di configurazione dal server DHCP.

- **Definizione server di backup**: scegliere **Per indirizzo IP** o **Per nome** per configurare il server.
- **Versione IP**: selezionare se viene utilizzato un indirizzo IPv4 o IPv6.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se IPv6 viene utilizzato). Sono disponibili le seguenti opzioni:
  - **Collega locale**: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale di collegamento presenta un prefisso FE80, non è instradabile e può essere utilizzato solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
  - **Globale**: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento (se viene utilizzato IPv6) dall'elenco.
- **Indirizzo IP/Nome server di backup**: immettere l'indirizzo IP o il nome del server da utilizzare se nel messaggio DHCP non è specificato alcun indirizzo IP del server.
- **Nome del file di configurazione backup**: immettere il percorso e il nome del file da utilizzare se nel messaggio DHCP non è specificato nessun nome di file di configurazione.

PASSAGGIO 4 Fare clic su **Applica**. I parametri vengono copiati nel file di configurazione di esecuzione.

5

Amministrazione: gestione stack

In questa sezione viene descritta la modalità di gestione degli stack Vengono trattati i seguenti argomenti:

- **Panoramica**
- **Tipi di unità in stack**
- **Topologia stack**
- **Assegnazione ID unità**
- **Processo di selezione dell'unità master**
- **Modifiche dello stack**
- **Malfunzionamento dell'unità in stack**
- **Sincronizzazione automatica del software in stack**
- **Modalità dell'unità stack**
- **Porte stack**
- **Configurazione predefinita**
- **Interazioni con altre funzioni**
- **Modalità di sistema**

Panoramica

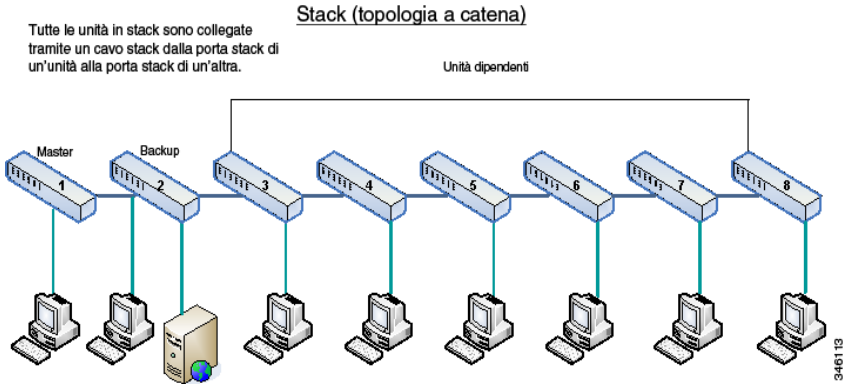
I dispositivi possono funzionare autonomamente (modalità indipendente) oppure possono essere collegati in stack fino a un massimo di 8 dispositivi in varie modalità (vedere la sezione **Modalità dell'unità stack**).

I dispositivi (le unità) in uno stack sono collegate tramite porte stack. Inoltre, questi dispositivi vengono gestiti congiuntamente come se si trattasse di un singolo dispositivo logico.

Lo stack è basato su un modello composto da una singola unità master/backup e più unità dipendenti.

Di seguito viene riportato un esempio di otto dispositivi collegati in stack:

Architettura stack (topologia a catena)



Uno stack offre i seguenti vantaggi:

- La capacità di rete può essere potenziata o ridotta in modo dinamico. Aggiungendo un'unità, l'amministratore può aumentare il numero di porte nello stack in maniera dinamica, mantenendo un unico dispositivo gestito logicamente. In modo analogo, le unità possono essere rimosse per ridurre la capacità di rete.
- Ecco come il sistema in stack supporta la ridondanza:
  - Se il master originale non funziona, l'unità di backup diventa l'unità master dello stack.
  - Il sistema di stack supporta due tipi di topologia: a catena (vedere **"Architettura stack (topologia a catena)"**) e ad anello (vedere **"Stack nella topologia ad anello"**). Nella topologia ad anello, se una delle porte stack non funziona, lo stack continua a funzionare in topologia a catena (vedere **Topologia stack**).
  - Il processo chiamato Rapido failover del collegamento allo stack è supportato nelle porte in stack ad anello per ridurre la durata della perdita dei pacchetti dati quando uno dei collegamenti alle porte stack non funziona. Fino a quando lo stack non ripristina la nuova topologia a catena, la porta stack non funzionante mantiene i pacchetti che

dovevano essere inviati, in modo tale che i pacchetti arrivino a destinazione utilizzando i restanti collegamenti allo stack. Durante il Fast Stack Link failover, le unità master/backup rimangono attive e funzionanti.

Tipi di unità in stack

Uno stack è formato da massimo otto unità. In uno stack l'unità può essere di due tipi:

- **Master**: l'ID dell'unità master deve essere 1 o 2. Lo stack è gestito dall'unità master che si autogestisce, dall'unità di backup e dalle unità dipendenti.
- **Backup**: se l'unità master non funziona, l'unità di backup assume il ruolo di master (commutazione). L'ID dell'unità di backup deve essere 1 o 2.
- **Dipendente**: queste unità sono gestite dall'unità master.

Per consentire a un gruppo di unità di funzionare come uno stack, è necessaria la presenza di un'unità master attiva. Quando l'unità master attivata non funziona, lo stack continua a operare finché c'è un'unità di backup (l'unità attiva che assume il ruolo di master).

Se neanche l'unità di backup funziona e le uniche unità funzionanti sono quelle dipendenti, anche queste verranno bloccate dopo un minuto. Ciò significa, ad esempio, che se dopo un minuto si inserisce un cavo in una delle unità dipendenti che funzionavano senza un'unità master, il collegamento non verrà attivato.

Compatibilità all'indietro del numero di unità in stack

Le versioni precedenti del dispositivo supportavano massimo quattro unità, mentre la versione attuale ne supporta otto. È possibile aggiornare versioni software precedenti senza modificare i file di configurazione.

Quando si carica una versione firmware che non supporta le modalità Stack ibrido e si riavvia lo stack, quest'ultimo passa alla modalità Stack nativo. Se su un dispositivo in modalità stack ibrido viene caricata una versione del firmware che non supporta tale modalità, viene reimpostata la modalità di sistema predefinita (SG500X/EWS2-550X: L3 e L2; Sx500: L2).

In caso di stack con ID unità configurati manualmente, le unità con ID maggiore di 4 passeranno alla numerazione automatica.

LED unità

Il dispositivo presenta 4 LED contrassegnati come 1, 2, 3, 4 che vengono utilizzati per visualizzare l'ID di ciascuna unità ad esempio, sull'ID unità 1, è acceso il LED 1 e gli altri LED sono spenti. Per supportare gli ID unità maggiori di 4, il display LED viene modificato in base alla definizione seguente:

- Unità da 1 a 4: sono accesi, rispettivamente, i LED da 1 a 4.
- Unità 5: sono accesi i LED 1 e 4.
- Unità 6: sono accesi i LED 2 e 4.
- Unità 7: sono accesi i LED 3 e 4.
- Unità 8: sono accesi i LED 1, 3 e 4.

Topologia stack

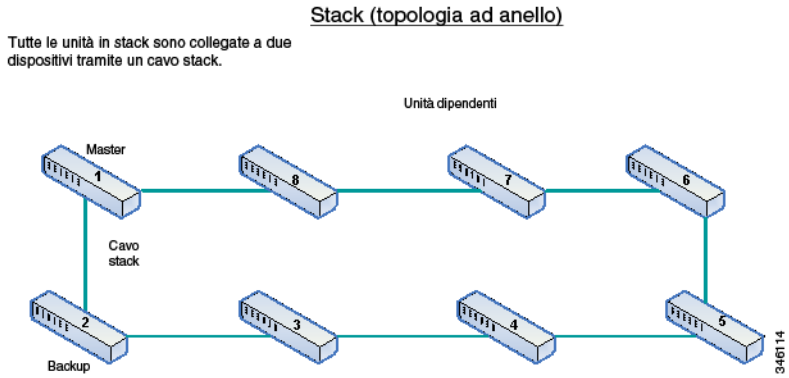
Tipi di topologia stack

Le unità in uno stack possono essere collegate in uno dei seguenti tipi di topologie:

Topologia a catena: la porta stack (destra o sinistra) della prima unità è collegata alla porta stack della seconda unità. Tutte le unità nello stack sono collegate alla porta stack dell'unità successiva, ad eccezione della prima e dell'ultima. Nella figura **“Architettura stack (topologia a catena)”** viene mostrata una topologia a catena.

Topologia ad anello: tutte le unità nello stack sono collegate in modo da formare un anello. L'ultima unità è collegata alla prima. Di seguito viene mostrata una topologia ad anello su uno stack da otto unità:

Stack nella topologia ad anello



La topologia ad anello è più affidabile di quella a catena. In una configurazione ad anello, il mancato funzionamento di un collegamento non influisce sull'attività dello stack, mentre in un collegamento a catena ne provocherebbe la suddivisione.

Rilevamento della topologia

Lo stack viene stabilito tramite un processo chiamato "rilevamento della topologia". Tale processo viene attivato mediante una modifica dello stato attivo/inattivo della porta stack.

Di seguito vengono riportati alcuni esempi di eventi che attivano questo processo:

- Modifica della topologia stack (da anello a catena).
- Unione di due stack in uno stack singolo.
- Suddivisione dello stack.
- Inserimento nello stack di altre unità dipendenti (ad esempio, perché in precedenza le unità non erano collegate allo stack a causa di un malfunzionamento). Ciò può verificarsi in una topologia a catena se un'unità centrale dello stack non funziona.

Durante il rilevamento della topologia, ciascuna unità dello stack procede allo scambio di pacchetti che contengono informazioni relative alla topologia.

Al termine del processo di rilevamento della topologia, in ciascuna unità sono presenti le informazioni di associazione allo stack di tutte le unità.

Assegnazione ID unità

Al termine del rilevamento della topologia, viene assegnato un ID unità a ciascuna unità dello stack.

L'ID unità viene impostato nella pagina Modalità di sistema e Gestione stack in uno dei seguenti modi:

- **Automaticamente (Auto)**: l'ID unità viene assegnato dal processo di rilevamento della topologia. Questa è l'impostazione predefinita.
- **Manualmente**: l'ID unità viene impostato manualmente su un numero intero compreso tra 1 e 8. Inoltre, la numerazione manuale include le seguenti opzioni:
  - **1 - Forza master**: impone l'impostazione dell'unità 1 come master.
  - **2 - Forza master**: impone l'impostazione dell'unità 2 come master.

Duplicare gli ID unità

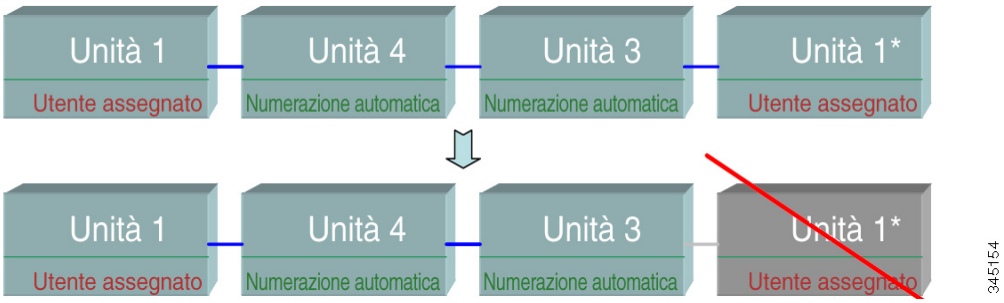
Se si assegna lo stesso ID unità a due unità differenti, solo una di queste può essere collegata allo stack con quell'ID unità.

Se si sceglie la numerazione automatica, l'unità duplicata viene assegnata a un nuovo numero unità. Se non si sceglie la numerazione automatica, l'unità duplicata viene arrestata.

Di seguito vengono riportati alcuni esempi di ID unità duplicato.

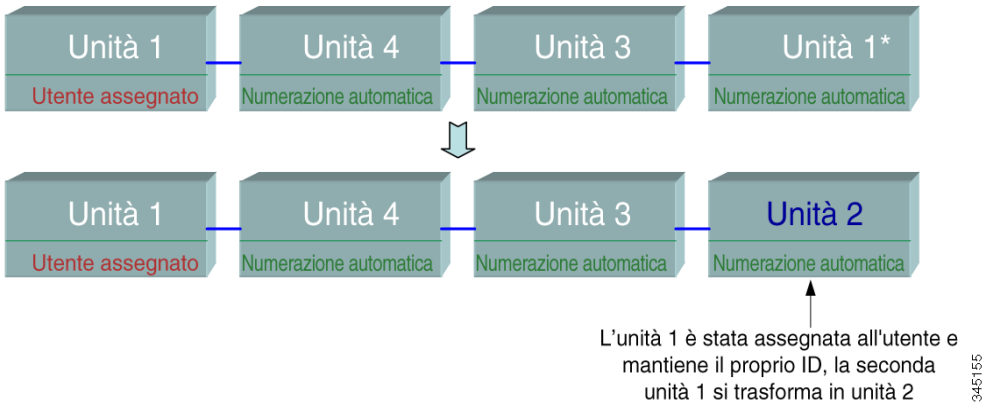
L'esempio seguente mostra un caso in cui è stato assegnato manualmente lo stesso ID a due unità. L'unità 1 non si collega allo stack e viene arrestata. Non è uscita vincitrice dal processo di selezione master tra le unità master attivate (1 o 2).

Unità duplicata arrestata



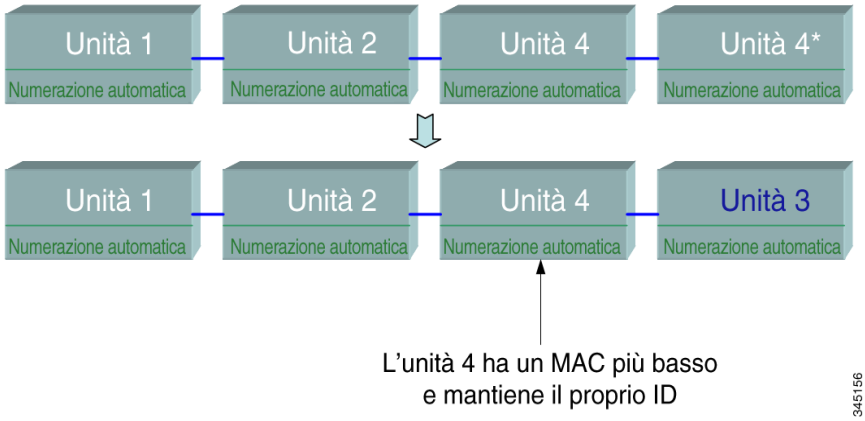
Di seguito viene illustrato il caso in cui una delle unità duplicate (numerate automaticamente) viene rinumerata.

Unità duplicata rinumerata



Di seguito viene illustrato il caso in cui una delle unità duplicate viene rinumerata. Quella con MAC inferiore mantiene il proprio ID unità (vedere **Processo di selezione dell'unità master** per la descrizione di tale processo).

Duplicazione tra due unità con ID unità a numerazione automatica



NOTA Se un nuovo stack dispone di più di 8 unità (numero massimo), tutte le unità supplementari vengono arrestate.

Processo di selezione dell'unità master

L'unità master viene selezionata dalle unità master attivate (1 o 2). I fattori di selezione delle unità master tengono conto del seguente ordine di priorità:

- **Forza master**: se su un'unità è attivata l'opzione Forza master, questa casella è selezionata.
- **Tempo di attività sistema**: le unità master si scambiano il tempo di attività misurato in segmenti di 10 minuti. Viene selezionata l'unità con il maggior numero di segmenti. Se entrambe le unità hanno lo stesso numero di segmenti e l'ID di una delle unità è stato impostato manualmente mentre quello dell'altra unità automaticamente, viene selezionata l'unità con l'ID definito manualmente; in caso contrario, verrà selezionata l'unità con l'ID più basso. Se i due ID unità sono uguali, viene scelta l'unità con l'indirizzo MAC più basso. **Nota:** se l'unità di backup è selezionata come master durante il processo di failover dello switch, il tempo di attività di tale unità viene mantenuto.
- **ID unità**: se entrambe le unità hanno lo stesso numero di segmenti, viene selezionata l'unità con l'ID più basso.
- **Indirizzo MAC**: se i due ID unità sono uguali, viene scelta l'unità con l'indirizzo MAC più basso.

NOTA Per funzionare, uno stack deve disporre di un'unità master. L'unità master viene definita come l'unità attiva che assume il ruolo di master. Dopo il processo di selezione master, lo stack deve contenere un'unità 1 e/o un'unità 2. In caso contrario, lo stack e tutte le unità vengono parzialmente arrestate; non si tratta di un arresto totale, ma le funzionalità di transito del traffico vengono interrotte.

Modifiche dello stack

In questa sezione vengono descritti i vari eventi che possono causare una modifica dello stack. La topologia stack subisce modifiche quando si verifica una delle seguenti situazioni:

- Una o più unità vengono collegate e/o scollegate allo/dallo stack.
- Una delle porte stack ha un collegamento attivo o inattivo.
- Lo stack passa da una struttura ad anello a una struttura a catena.

Quando si aggiungono o rimuovono unità a/da uno stack, vengono apportate modifiche di topologia, viene avviato il processo di selezione master e viene eseguita l'assegnazione dell'ID unità.

Collegamento di una nuova unità

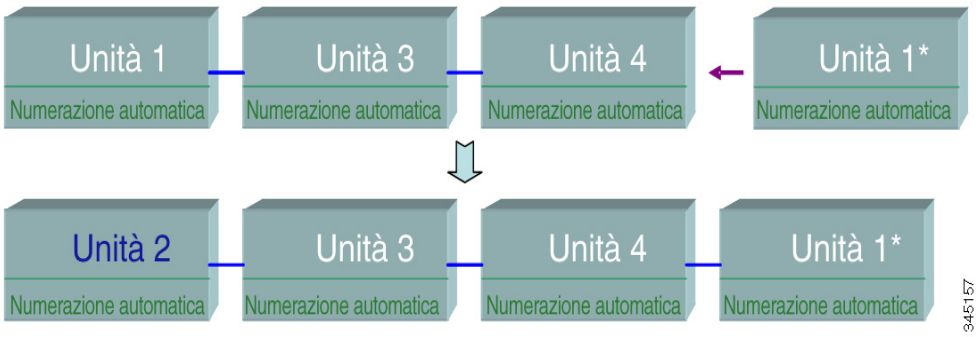
Quando si inserisce un'unità nello stack, la topologia dello stack viene modificata. Viene assegnato l'ID unità (in caso di numerazione automatica) e l'unità viene configurata dal master.

Quando si collega una nuova unità allo stack esistente potrebbe verificarsi uno dei seguenti scenari:

- Non esistono ID unità duplicati.
  - Le unità con ID definito dall'utente mantengono il proprio ID unità.
  - Le unità con ID assegnato automaticamente mantengono il proprio ID unità.
  - Le unità con impostazioni predefinite acquisiscono gli ID unità automaticamente, a partire dall'ID disponibile più basso.
- Esistono uno o più ID unità duplicati. La numerazione automatica risolve i conflitti e assegna gli ID unità. In caso di numerazione manuale, solo un'unità mantiene il proprio ID unità e le altre vengono arrestate.
- Il numero di unità nello stack supera il numero massimo di unità consentito. Le nuove unità collegate allo stack vengono arrestate e viene generato un messaggio SYSLOG visualizzato sull'unità master.

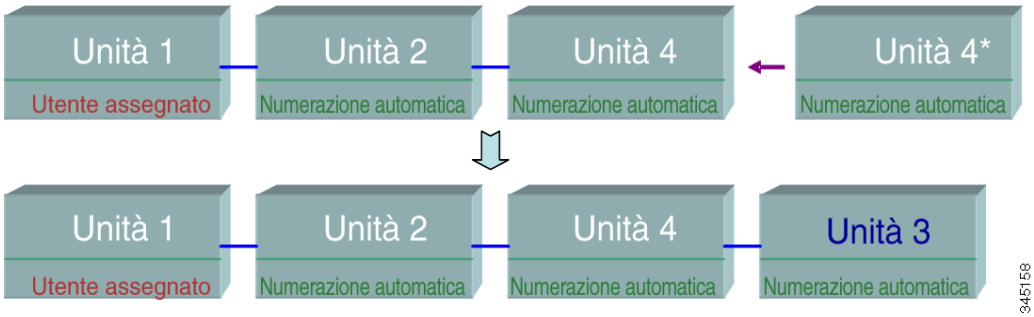
Di seguito viene mostrato un esempio di numerazione automatica quando un'unità master attiva è collegata allo stack. Ci sono due unità con ID = 1. Il processo di selezione master sceglie l'unità più adatta come master. L'unità più adatta è quella con il tempo di attività maggiore in segmenti di 10 minuti. L'altra viene scelta come unità di backup.

Unità master attivata con numerazione automatica



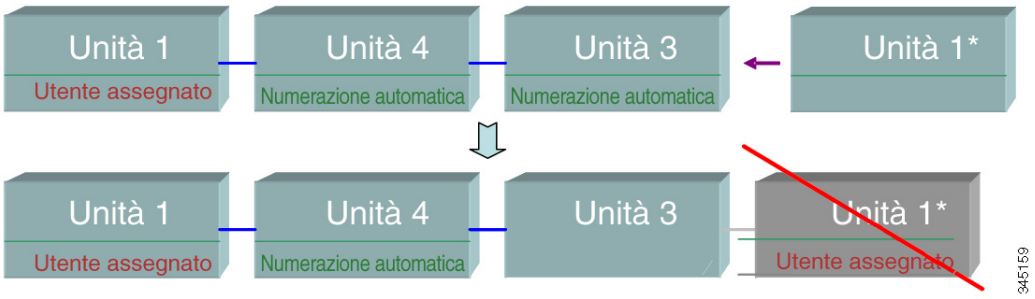
Di seguito viene mostrato un esempio di numerazione automatica quando una nuova unità viene collegata allo stack. Le unità esistenti mantengono il loro ID. La nuova unità acquisisce l'ID disponibile più basso.

Unità a numerazione automatica



Di seguito viene mostrato cosa succede quando un'unità master attiva assegnata dall'utente con ID unità 1 viene collegata a uno stack che dispone già di un'unità master con ID unità assegnato dall'utente pari a 1. L'unità 1 più recente non viene collegata allo stack e subisce un arresto.

Unità master attivata assegnata dall'utente



Malfunzionamento dell'unità in stack

Malfunzionamento dell'unità master

Se l'unità master non funziona, l'unità di backup assume il ruolo di master e continua a far funzionare lo stack regolarmente.

Affinché l'unità di backup possa sostituire l'unità master, entrambe le unità vengono tenute sempre in standby a caldo. In standby a caldo, il master e le relative unità di backup vengono sincronizzate con la configurazione statica (presente nei file di configurazione di avvio e di esecuzione). I file di configurazione backup non vengono sincronizzati. Il file di configurazione backup resta sull'unità master precedente.

Le informazioni sullo stato del processo dinamico, ad esempio la tabella di stato STP, gli indirizzi MAC e i tipi di smartport acquisiti in modo dinamico, le tabelle multicast MAC, LACP e GVRP non sono stati sincronizzati.

Durante la configurazione di un master, il backup viene sincronizzato immediatamente. La sincronizzazione viene avviata non appena si esegue un comando. Si tratta di un'operazione trasparente.

Se un'unità viene inserita in uno stack in esecuzione e viene selezionata come unità di backup, l'unità master la sincronizza in modo da aggiornare la configurazione, quindi genera un messaggio SYSLOG SYNC COMPLETE. Si tratta di un messaggio SYSLOG unico che viene visualizzato soltanto quando il backup converge con l'unità master e ha l'aspetto seguente: %DSYNCH-I-SYNCH_SUCCEEDED: sincronizzazione con l'unità 2 completata.

Commutazione Master/Backup

La commutazione si verifica quando l'unità master non funziona o quando l'opzione Forza master viene configurata sull'unità di backup.

L'unità di backup assume il ruolo di master, tutti i relativi processi e stack del protocollo vengono inizializzati per assumere il controllo di tutto lo stack. Di conseguenza, in questa unità l'inoltro del traffico viene temporaneamente sospeso, mentre le unità dipendenti rimangono attive.

NOTA Quando si utilizza il protocollo STP e le porte hanno un collegamento attivo, lo stato della porta STP viene impostato temporaneamente su Blocco ed è quindi impossibile inoltrare il traffico o rilevare gli indirizzi MAC. Ciò è utile per impedire i loop dell'albero tra le unità attive.

Gestione delle unità dipendenti

Quando l'unità di backup assume il ruolo di master, le unità dipendenti attive rimangono tali e continuano a inoltrare i pacchetti in base alla configurazione del master originale. Ciò riduce al minimo le interruzioni del traffico di dati all'interno delle unità.

Una volta assunto il ruolo di master, l'unità di backup inizializza le unità dipendenti, una alla volta, eseguendo le operazioni indicate di seguito:

- Cancella e ripristina la configurazione predefinita dell'unità dipendente (per evitare una configurazione errata da parte della nuova unità master). Di conseguenza, l'inoltro del traffico non viene eseguito sull'unità dipendente.
- Applica le configurazioni definite dall'utente all'unità dipendente.
- Esegue lo scambio delle informazioni dinamiche, come lo stato della porta in STP, gli indirizzi MAC dinamici e lo stato di collegamento attivo/inattivo tra l'unità master e quella dipendente. L'inoltro dei pacchetti sull'unità dipendente riprende dopo che lo stato delle sue porte è stato impostato per tale operazione dall'unità master in base al protocollo STP.

  NOTA Il flooding dei pacchetti verso indirizzi MAC unicast sconosciuti si verifica fino a quando gli indirizzi MAC non vengono acquisiti o riacquisiti.

Ricollegamento dell'unità master originale dopo il failover

Se dopo il failover l'unità master originale viene collegata di nuovo, si avvia il processo di selezione master. Se l'unità master originale (unità 1) viene riselezionata per assumere tale ruolo, l'unità master corrente (unità 2, che fungeva da unità di backup originale) viene riavviata e torna a essere un'unità di backup.

NOTA Durante il failover master/backup, il tempo di attività dell'unità di backup viene mantenuto.

Sincronizzazione automatica del software in stack

Tutte le unità nello stack devono eseguire la stessa versione del software (firmware e codice di avvio). Ciascuna unità dello stack esegue automaticamente il download del firmware e del codice di avvio dall'unità master se il firmware e/o il codice di avvio utilizzati dall'unità e dal master non coincidono. L'unità si riavvia automaticamente per eseguire la nuova versione.

Modalità dell'unità stack

La modalità dell'unità stack di un dispositivo indica se può far parte di uno stack o se opera in maniera indipendente.

I dispositivi possono funzionare in una delle seguenti modalità dell'unità stack:

- **Indipendente**: un dispositivo in modalità indipendente non è connesso ad altri dispositivi e non dispone di una porta stack.
- **Stack nativo**: un dispositivo che opera in questa modalità può essere collegato ad altri dispositivi *dello stesso tipo* mediante le sue porte stack per formare uno stack. Tutte le unità di uno stack nativo devono essere dello stesso tipo (tutte della serie Sx500, tutte della serie SG500X/ESW2-550X o tutte della serie SG500G).
- **Ibrido di base**: un dispositivo che opera in questa modalità può essere collegato a dispositivi della serie Sx500 e SG500X/ESW2-550X per formare uno stack. La sola limitazione (e il motivo per cui questa modalità viene chiamata Ibrido di base rispetto alla modalità Ibrido avanzata) è data dal fatto che il protocollo VRRP o RIP non è supportato. In questa modalità, l'interfaccia grafica utente mostra le pagine della serie Sx500, anche se il master dello stack appartiene alla serie SG500X/ESW2-550X, dal momento che il set di funzioni è lo stesso della serie Sx500.

  In questa modalità, qualsiasi tipo di dispositivo può assumere il ruolo di master/backup. Solo le porte stack 5G possono essere utilizzate come porte stack.

- **Ibrido avanzata**: un dispositivo che opera in questa modalità può essere collegato a dispositivi della serie Sx500 e SG500X/ESW2-550X per formare uno stack. In questa modalità sono supportati VRRP e/o RIP, ma non la numerazione automatica delle unità dal momento che solo i dispositivi SG500X o ESW2-550X possono funzionare come unità master/backup.

  I dispositivi Sx500 possono essere solo unità dipendenti, quindi è possibile configurare in stack fino a 6 unità Sx500 e due dispositivi SG500X/ESW2-550X.

- **Ibrido avanzata XG**: un dispositivo che opera in questa modalità può essere collegato a dispositivi della serie SG500X/ESW2-550X e SG500XG per formare uno stack.

  Tutte le unità possono essere unità master o dipendenti.

Opzioni di configurazione dello stack

La sezione seguente descrive alcune tradizionali configurazioni dello stack:

Possibile configurazione dello stack	Possibile supporto RIP/ VRRP	Velocità porte stack
Lo stack è composto da tutte unità SG500X in modalità Stack nativo.	Attivato/ Disattivato	1G/10G o 1G/5G
Lo stack è composto da tutte unità ESW2-550X in modalità Stack nativo.	Attivato/ Disattivato	1G/10G o 1G/5G
Lo stack è composto da tutte unità Sx500 in modalità Stack nativo.	Non supportato.	1G/5G (predefinita) o 1G rame/SFP (combo)
Lo stack è costituito da diversi tipi di dispositivi che funzionano in modalità stack ibrido di base. ▪ **Master:** SG500X, ESW2-550X o Sx500 ▪ **Backup:** qualsiasi tipo di dispositivo ▪ **Dipendenti:** qualsiasi tipo di dispositivo	Non supportato.	1G/5G

Possibile configurazione dello stack	Possibile supporto RIP/ VRRP	Velocità porte stack
Lo stack è costituito da diversi tipi di dispositivi che funzionano in modalità Ibrido avanzata. ▪ **Master:** SG500X ▪ **Backup:** SG500X ▪ **Dipendenti:** qualsiasi tipo di dispositivo	Attivato/ Disattivato	1G/5G
Lo stack è costituito da diversi tipi di dispositivi che funzionano in modalità Ibrido avanzata XG. ▪ **Master:** SG500X/ESW2-550X o SG500XG ▪ **Backup:** SG500X/ESW2-550X o SG500XG ▪ **Dipendenti:** qualsiasi tipo di dispositivo	Attivato/ Disattivato	1 G o 10 G

Coerenza delle modalità dell'unità nello stack

Tutte le unità nello stack devono avere la stessa modalità.

Quando lo stack viene inizializzato, esegue un algoritmo di rilevamento della topologia che raccoglie informazioni sulle unità dello stack.

L'unità selezionata come master può rifiutare la richiesta del dispositivo adiacente di collegarsi allo stack se la modalità dell'unità stack non corrisponde. In questo caso il dispositivo rifiutato viene arrestato logicamente (le porte non possono inviare/ricevere traffico) e tutti i suoi LED (sistema, VENTOLA, ID unità, porte di rete e LED porte stack) sono accesi. Le informazioni relative alla modalità dell'unità stack sono visualizzate come errore SYSLOG nell'unità master.

Per ripristinare l'unità da questa modalità è necessario scollegarla dall'alimentazione e ricollegarla.

Modifica della modalità dell'unità stack

Per rimuovere un dispositivo da uno stack, impostare la modalità dell'unità stack su Indipendente; se, invece, si desidera inserire il dispositivo in uno stack, impostare la modalità dell'unità stack su Stack nativo, Configurazione in stack ibrido di base o Configurazione in stack Ibrido avanzata.

Nelle sezioni seguenti vengono descritte la modalità di sistema e la configurazione dei dispositivi dopo il riavvio in seguito al cambiamento di modalità dell'unità stack.

Modalità di sistema (dispositivi 500) dopo il riavvio

Quando si modifica la modalità di stack di un dispositivo, la modalità di sistema del dispositivo dopo il riavvio potrebbe essere modificata:

- **Dispositivi Sx500**: la modalità di sistema (Livello 2 o Livello 3) delle unità Sx500 di backup e dipendenti viene recuperata dall'unità master. Se la modalità di sistema non viene impostata in maniera specifica prima del riavvio, verrà utilizzata la modalità del Livello 2 (impostazione predefinita). Per attivare la modalità Livello 3 dopo il riavvio, è necessario specificarlo prima.
- **Dispositivi SG500X/ESW2-550X**: se il dispositivo è in modalità Indipendente o Stack nativo, la modalità di sistema è sempre Livello 2 e 3. Quando il dispositivo è in modalità Configurazione in stack ibrido di base o avanzata, si comporta come descritto sopra per i dispositivi Sx500. Se il dispositivo è in modalità Ibrido avanzata XG, la modalità di sistema è sempre Livello 2 e 3.
- **Dispositivi SG500XG:** sempre Livello 2 e Livello 3.

Configurazione dopo il riavvio

Se si cambia la modalità stack di un dispositivo e lo si riavvia, il file di configurazione di avvio viene in genere **eliminato**, perché potrebbe contenere informazioni di configurazione non applicabili alla nuova modalità.

Viene mantenuto dopo l'avvio nei seguenti casi:

- **Dispositivi SG500X/ESW2-550X:**
  - **Cambio di modalità da Indipendente a Stack nativo:** mantenuto soltanto se si impone l'impostazione dell'unità come master con ID unità = 1.

- **Cambio di modalità da Ibrido di base a Ibrido avanzata:** mantenuto soltanto se si impone l'impostazione dell'unità come master con ID unità = 1.
- **Cambio di modalità da Ibrido di base a Ibrido avanzata XG:** mantenuto soltanto se si impone l'impostazione dell'unità come master con ID unità = 1.

- **SG500XG:**
  - **Cambio di modalità da Indipendente a Stack nativo:** mantenuto soltanto se si impone l'impostazione dell'unità come master con ID unità = 1.
  - **Cambio di modalità da Nativo a Ibrido avanzata XG:** mantenuto soltanto se si impone l'impostazione dell'unità come master con ID unità = 1.
- **Dispositivi Sx500:**
  - **Cambio di modalità da Indipendente a Stack nativo:** mantenuto soltanto se si impone l'impostazione dell'unità come master con ID unità = 1.
  - **Cambio di modalità da Indipendente a Ibrido di base:** mantenuto soltanto se si impone l'impostazione dell'unità come master con ID unità = 1.
  - **Cambio di modalità da Stack nativo a Ibrido di base:** mantenuto soltanto se si impone l'impostazione dell'unità come master con ID unità = 1.

Porte stack

Le porte di uno stack devono essere riservate per uno dei seguenti tipi di porte:

- **Porte di rete**: note anche come porte di collegamento. Queste porte sono collegate alla rete.
- **Porte stack**: porte che collegano due unità in uno stack. Le porte stack vengono utilizzate per trasferire i dati e i pacchetti di protocollo tra le unità.

È necessario indicare al sistema (riserva) le porte che si prevede di utilizzare come porte stack (nella pagina Modalità Sistema e Gestione stack). Tutte le porte non riservate come porte stack saranno considerate porte di rete.

Porte stack e porte di rete predefinite

Di seguito vengono indicate le porte stack e le porte di rete predefinite:

- **Dispositivi Sx500**: quando un dispositivo Sx500 opera in modalità Stack nativo, S1-S2-1G funzionano come normali porte di rete, mentre S3-S4-5G funzionano come porte stack per impostazione predefinita.
- **Dispositivi SG500X/ESW2-550X**: S1-S2-10G sono porte stack per impostazione predefinita. È possibile configurare manualmente S1-S2-10G e S1-S2-5G come porte di rete o porte stack.
- **Dispositivi SG500XG**: qualsiasi porta può essere usata come porta stack o di rete. Il dispositivo è in modalità indipendente per impostazione predefinita.

Quando si converte un dispositivo da una delle modalità stack alla modalità Indipendente, tutte le porte stack diventano automaticamente normali porte di rete.

Coppie di porte

Nella tabella seguente vengono descritte le coppie di porte disponibili sul dispositivo nelle varie modalità dell'unità stack:

Tipo di dispositivo/ Coppia di porte	Stacking	Indipendente
Sx500 Stack 5G S3-S4	▪ **Modalità Stack nativo:** disponibile sia come porte di rete che come porte stack ▪ **Modalità ibrido:** disponibile come porte stack.	Disponibile come porta di rete
Sx500 Slot combo 1G fibra/rame Stack 1G S1-S2	▪ **Modalità Stack nativo:** disponibile sia come porte di rete che come porte stack ▪ **Modalità ibrido:** disponibile come porte di rete	Disponibile come porta di rete

Tipo di dispositivo/ Coppia di porte	Stacking	Indipendente
SG500X/ESW2-550X Stack 5G S1-S2 Stack 10G S1-S2	▪ **Modalità Stack nativo:** slot 5G o 10G disponibile. ▪ **Modalità ibrido:** disponibile soltanto lo slot 5G.	Disponibile soltanto come slot 10G
SG500XG Porte XG1-XG16. Sono gli slot 10 G.	▪ **Modalità Stack nativo:** porte 1 G o 10 G disponibili. ▪ **Modalità ibrido:** porte 1 G o 10 G disponibili.	Disponibile come porte di rete

Velocità delle porte

La velocità delle porte stack può essere impostata manualmente oppure selezionata automaticamente. Di seguito vengono descritti i tipi di porte stack disponibili e le relative velocità su vari dispositivi:

Tipo di dispositivo	Coppia di porte	Possibili velocità nello stack	Selezione della velocità automatica disponibile
Sx500	S1-S2	1G	No
Sx500	S3-S4	5G/1G	Sì
SG500X/ **ESW2-550X**	S1-S2-XG	10G/1G	Sì
SG500X/ **ESW2-550X**	S1-S2-5G	5G/1G	Sì
SG500XG	**Qualsiasi coppia di porte fra XG1 e XG16**	1G o 10G	Sì

Selezione automatica della velocità delle porte

È possibile impostare il tipo di cavo stack in modo che venga rilevato automaticamente quando viene collegato alla porta (impostazione predefinita). Il sistema identifica automaticamente il tipo di cavo stack e seleziona la velocità più alta supportata dal cavo e dalla porta.

Viene visualizzato un messaggio SYSLOG (livello informativo) che richiede all'utente di configurare manualmente la velocità della porta quando il tipo di cavo non viene riconosciuto.

Connessione di unità

Due unità possono essere connesse in uno stack solo se le porte a entrambe le estremità del collegamento hanno la stessa velocità. A tal fine, è necessario configurare la velocità delle porte stack nel modo seguente:

- Modalità velocità automatica
- Stessa velocità su ogni lato della connessione

Tipi di cavo

Ogni tipo di porta stack può essere utilizzata con tipi di cavi specifici.

Se la modalità stack è impostata su Stack nativo, è possibile utilizzare un cavo in fibra o in rame come cavo di stack. Se sono collegati entrambi i cavi (fibra e rame), scegliere quello in fibra. Per la ridondanza è possibile utilizzare una doppia connessione. Quando si verifica un cambiamento di supporto, ad esempio se si scollega il cavo di stack in fibra e il cavo di stack in rame diventa attivo, il sistema avvia un evento di modifica della topologia.

Di seguito vengono descritte le varie combinazioni tra tipi di cavo e porte.

	Porte stack			Porte di rete		
Tipo di connettore	**S1-S2-5G per SG500X/ ESW2-550X e S3-S4 per Sx500**	**S1, S2 per Sx500**	**S1,S2 - XG per SG500X/ ESW2-550X**	**S1,S2 - 5G per SG500X e S3, S4 per Sx500**	**S1,S2 per Sx500**	**S1,S2 - XG per SG500X**
Cisco SFP-H10GB-CU1M, cavo in rame passivo	5G	1G	10G	1G	1G	10G
Cisco SFP-H10GB-CU3M, cavo in rame passivo	5G	1G	10G	1G	1G	10G
Cisco SFP-H10GB-CU5M, cavo in rame passivo	5G	1G	10G	1G	1G	10G
Cisco SFP-10G-SR	Non supportato	Non supportato	10G	Non supportato	Non supportato	10G
Cisco SFP-10G-LRM	Non supportato	Non supportato	10G	Non supportato	Non supportato	10G
Cisco SFP-10G-LR	Non supportato	Non supportato	10G	Non supportato	Non supportato	10G
1G SFP Modulo MGBSX1	1G	1G	1G	1G	1G	1G
1G SFP Modulo MGBT1	1G	1G	1G	1G	1G	1G
1G SFP Modulo MGBLX1	1G	1G	1G	1G	1G	1G
1G SFP Modulo MGBBX1	1G	1G	1G	1G	1G	1G
100Mbs SFP Modulo MFELX1	Non supportato	Non supportato	Non supportato	Non supportato	100Mbs	Non supportato
100Mbs SFP Modulo MFEFX1	Non supportato	Non supportato	Non supportato	Non supportato	100Mbs	Non supportato

Porte stack				Porte di rete		
Tipo di connettore	**S1-S2-5G per SG500X/ ESW2-550X e S3-S4 per Sx500**	**S1, S2 per Sx500**	**S1,S2 - XG per SG500X/ ESW2-550X**	**S1,S2 - 5G per SG500X e S3, S4 per Sx500**	**S1,S2 per Sx500**	**S1,S2 - XG per SG500X**
100Mbs SFP Modulo MFEBX1	Non supportato	Non supportato	Non supportato	Non supportato	100Mbs	Non supportato
Altri SFP	1G	In base a: Velocità forzata dall'utente Velocità EEPROM Velocità 1G	In base a: Velocità forzata dall'utente Velocità EEPROM Velocità 1G	1G	In base a: Velocità forzata dall'utente Velocità EEPROM Velocità 1G	In base a: Velocità forzata dall'utente Velocità EEPROM Velocità 10G

Porte stack o porte di rete	
Tipo di connettore	**Tutte le porte**
Cisco SFP-H10GB-CU1M, cavo in rame passivo	1G - 10G
Cisco SFP-H10GB-CU3M, cavo in rame passivo	1G - 10G
Cisco SFP-H10GB-CU5M, cavo in rame passivo	1G - 10G
Cisco SFP-10G-SR	Non supportato
Cisco SFP-10G-LRM	Non supportato
Cisco SFP-10G-LR	Non supportato
1G SFP Modulo MGBSX1	1G
1G SFP Modulo MGBT1	1G
1G SFP Modulo MGBLX1	1G
1G SFP Modulo MGBBX1	1G
100Mbs SFP Modulo MFELX1	Non supportato
100Mbs SFP Modulo MFEFX1	Non supportato
100Mbs SFP Modulo MFEBX1	Non supportato
Altri SFP	1G

Configurazione predefinita

Di seguito vengono indicati i valori predefiniti dei dispositivi nelle varie modalità di stack:

Tipo di dispositivo	Modalità stack	Porte stack predefinite	Modalità di sistema predefinita
Sx500	Stack nativo	Stack 5G S3-S4	Livello 2
	Configurazione in stack ibrido di base	Stack 5G S3-S4	Livello 2
	Configurazione in stack ibrido avanzata	Stack 5G S3-S4	Livello 2
SG500X/ ESW2-550X	Stack nativo	Stack 10G S1-S2	Livello 2+Livello 3
	Configurazione in stack ibrido di base	Stack 5G S1-S2	Livello 2
	Configurazione in stack ibrido avanzata	Stack 5G S1-S2	Livello 2
	Configurazione in stack ibrido avanzata XG	Stack 5G S1-S2	Livello 2
SG500XG	Stack nativo	L'utente può scegliere qualsiasi coppia	Livello 2+Livello 3
	Configurazione in stack ibrido avanzata XG	L'utente può scegliere qualsiasi coppia	Livello 2+Livello 3

Interazioni con altre funzioni

RIP e VRRP non sono supportati nella modalità stack Ibrido di base.

Modalità di sistema

Utilizzare la pagina Modalità Sistema e Gestione Stack per eseguire le seguenti operazioni:

- Impostare la modalità stack di un dispositivo su Indipendente.
- Impostare la modalità stack di un dispositivo su una delle modalità di stack, modificare l'ID unità, le porte stack e la velocità delle porte stack di tutti i dispositivi in uno stack.
- Modificare la modalità di sistema (Livello 2-3) di un dispositivo indipendente o dello stack.
- Modificare la modalità code da 4 a 8 code supportate o viceversa.

Le informazioni su queste modalità sono memorizzate nel file di configurazione come segue:

- **Intestazione del file di configurazione**: contiene la modalità di sistema e la modalità code (anche se impostate sui valori predefiniti).
- **Corpo del file di configurazione**: contiene i comandi di configurazione.

Compatibilità all'indietro della modalità di sistema

Le seguenti modalità sono state ampliate nella versione software attuale del dispositivo. Prestare attenzione quando si utilizzano queste funzionalità nelle versioni software precedenti:

- **Modalità Code**: questa modalità può essere modificata da 4 code QoS a 8 code QoS. Se si effettua l'aggiornamento da versioni software precedenti che non supportano 8 code, non si verificano problemi poiché la modalità 4 code è quella predefinita nella versione software attuale. Tuttavia, se si imposta la modalità code su 8 code, è necessario esaminare e adeguare la configurazione per soddisfare gli obiettivi QoS desiderati con la nuova modalità. La modifica della modalità code viene applicata dopo il riavvio del sistema. La configurazione relativa a code in conflitto con la nuova modalità code viene rifiutata.

- **Modalità di stack**: la modalità di stack è stata ampliata per includere le modalità di stack ibrido. L'upgrade dalle versioni software precedenti non presenta alcun problema poiché il dispositivo viene avviato con una modalità di stack esistente (modalità Stack nativo). Se si desidera installare una versione precedente del software da un dispositivo che era configurato in modalità stack ibrido a una versione software che non supporta lo stack ibrido, è necessario configurare prima il dispositivo sulla modalità stack ibrido.

Modalità di sistema e gestione dello stack

Per configurare lo stack, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Modalità sistema e Gestione stack**.

Lo stato operativo di un dispositivo indipendente o di uno stack viene visualizzato in **Stato operativo**:

- **Modalità dell'unità stack**: visualizza uno dei seguenti valori per il dispositivo:
  - *Indipendente*: il dispositivo non fa parte dello stack.
  - *Stack nativo:* il dispositivo fa parte di uno stack che contiene unità dello stesso tipo.
  - *Configurazione in stack Ibrido di base*: il dispositivo fa parte di uno stack composto da dispositivi SG500X e Sx500 con la serie di funzionalità Sx500.
  - *Configurazione in stack Ibrido avanzata*: il dispositivo fa parte di uno stack composto da dispositivi SG500X e Sx500 con la serie di funzionalità SG500X.
  - *Configurazione in stack Ibrido avanzata XG*: il dispositivo fa parte di uno stack composto da dispositivi SG500X/ESW2-550X e SG500XG con la serie di funzionalità SG500X.
- **Topologia stack**: indica la topologia dello stack (a catena o ad anello).
- **Modalità di sistema**: indica se i dispositivi in stack/indipendenti operano in modalità di sistema Livello 2, Livello 3 o Livello 2 e Livello 3.
- **Master dello stack**: indica l'ID dell'unità master dello stack.
- **Stato selezione master**: indica come è stata selezionata l'unità master dello stack. Vedere la sezione **Processo di selezione dell'unità master**.

PASSAGGIO 2 Per configurare la modalità di sistema dopo il riavvio, selezionare la modalità Livello 2 o Livello 3.

PASSAGGIO 3 Per configurare la modalità code dopo il riavvio, selezionare se configurare 4 o 8 code QoS sul dispositivo. Vedere la sezione **Configurazione delle code QoS**.

PASSAGGIO 4 Configurare le unità in uno stack nella **Tabella impostazioni amministrative dello stack.** Tali modifiche diventano effettive dopo il riavvio.

NOTA Se si utilizza un dispositivo Sx500 e la modalità dell'unità stack viene modificata da Stack nativo a Indipendente, il dispositivo sarà in modalità di sistema Livello 2 dopo il riavvio, a meno che non si modifichi il campo **Modalità di sistema** in Livello 3.

Nella tabella viene indicato lo stato operativo di tutte le unità di uno stack.

- **Numero di unità stack**: indica l'ID di un'unità attiva e riconosciuta.
- **Nome modello**: nome del modello di un'unità attiva e riconosciuta.
- **Collegamento 1 stack**: informazioni per il primo collegamento stack:
  - *Porta*: il tipo di porta stack collegata.
  - *Velocità*: la velocità della porta stack collegata.
  - *Router adiacente*: ID dell'unità stack connessa.

6

Amministrazione

In questa sezione viene descritto come visualizzare le informazioni di sistema e come configurare le diverse opzioni nel dispositivo.

Vengono trattati i seguenti argomenti:

- **Modelli dispositivo**
- **Impostazioni di sistema**
- **Impostazioni console (supporto velocità di trasmissione automatico)**
- **Interfaccia di gestione**
- **Gestione di stack e modalità di sistema**
- **Account utente**
- **Definizione di timeout sessione inattiva**
- **Impostazioni ora**
- **Log di sistema**
- **Gestione dei file**
- **Risorse di routing**
- **Integrità**
- **Diagnostica**
- **Rilevamento - Bonjour**
- **Rilevamento - LLDP**
- **Rilevamento - CDP**
- **Ping**
- **Traceroute**

Modelli dispositivo

È possibile gestire completamente tutti i modelli attraverso l'utilità di configurazione dello switch basata sul Web.

NOTA È possibile impostare ogni modello sulla modalità di sistema Livello 3 dalla pagina Modalità di sistema e Gestione stack.

Quando il dispositivo funziona in modalità di sistema Livello 3, il limite di velocità della VLAN e i monitoraggi QoS non funzionano. Le altre funzioni della modalità avanzata QoS funzionano.

Solo i modelli SG500X/SG500XG/ESW2-550X supportano il VRRP (Virtual Router Redundancy Protocol) e il RIP (Routing Information Protocol).

NOTA Vengono utilizzate le seguenti convenzioni di porta:

- GE viene utilizzata per le porte Gigabit Ethernet (10/100/1000).
- FE viene utilizzata per le porte Fast Ethernet (10/100).
- XG viene utilizzata per le porte 10 Gigabit Ethernet.

Nella tabella seguente sono illustrati i vari modelli, il numero e il tipo di porte, oltre alle informazioni sul PoE.

Nome modello	ID prodotto (PID)	Descrizione delle porte sul dispositivo	Alimentazione riservata a PoE	N. di porte che supportano PoE
SF500-24	SF500-24-K9	Switch gestito stackable 10/100 a 24 porte	N/D	N/D
SF500-24P	SF500-24P-K9	Switch gestito stackable PoE 10/100 a 24 porte	180W	24
SF500-48	SF500-48-K9	Switch gestito stackable 10/100 a 48 porte	N/D	N/D
SF500-48P	SF500-48P-K9	Switch gestito stackable PoE 10/100 a 48 porte	375W	48
SG500-28	SG5000-28-K9	Switch gestito stackable Gigabit a 28 porte	N/D	N/D
SG500-28MPP	SG500-28MPP-K9	Switch gestito Gigabit PoE a 28 porte	740W	24

Nome modello	ID prodotto (PID)	Descrizione delle porte sul dispositivo	Alimentazione riservata a PoE	N. di porte che supportano PoE
SG500-28P	SG500-28P-K9	Switch gestito stackable PoE Gigabit a 28 porte	180W	24
SG500-52	SG500-52-K9	Switch gestito stackable Gigabit a 52 porte	N/D	N/D
SG500-52MP	SG500-52MP-K9	Switch gestito Gigabit PoE max a 52 porte	740W	48
SG500-52P	SG500-52P-K9	Switch gestito stackable PoE Gigabit a 52 porte	375W	48
SG500X-24	SG500X-24-K9	Gigabit a 24 porte con switch gestito stackable 10-Gigabit a 4 porte	N/D	N/D
SG500X-24P	SG500X-24P-K9	Gigabit a 24 porte con switch gestito stackable PoE 10-Gigabit a 4 porte	375W	24
SG500X-48	SG500X-48-K9	Gigabit a 48 porte con switch gestito stackable 10-Gigabit a 4 porte	N/D	N/D
SG500X-48P	SG500X-48P-K9	Gigabit a 48 porte con switch gestito stackable PoE 10-Gigabit a 4 porte	375W	48
ESW2-550X-48	ESW2-550X-48-K9	Gigabit a 48 porte con switch gestito stackable 10 Gigabit a 4 porte	N/D	N/D
ESW2-550X-48DC	ESW2-550X-48DC-K9	Gigabit a 48 porte con switch gestito stackable 10 Gigabit a 4 porte	N/D	N/D
SG500XG-8F8T	SG500XG-8F8T-K9	Switch gestito stackable 10-Gigabit a 16 porte	N/D	N/D

Impostazioni di sistema

Nella pagina Riepilogo di sistema viene fornita una visualizzazione grafica del dispositivo e vengono visualizzati lo stato del dispositivo, le informazioni sull'hardware, le informazioni sulla versione firmware, lo stato PoE generale e altre voci.

Visualizzazione del riepilogo di sistema

Per visualizzare le informazioni di sistema, fare clic su **Stato e statistiche** > **Riepilogo di sistema**.

La pagina Riepilogo di sistema contiene le informazioni sul sistema e sull'hardware.

Informazioni di sistema:

- **Indirizzo MAC di base**: indirizzo MAC del dispositivo. Se il sistema è in modalità stack, viene visualizzato l'indirizzo MAC di base dell'unità master.

  NOTA Se il sistema è in modalità stack nativo, il numero di versione del firmware visualizzato si basa sulla versione del master.

- **Versione firmware (non attiva)**: numero di versione firmware dell'immagine non attiva. Se il sistema è in modalità stack nativo, viene visualizzata la versione dell'unità master.
- **Modalità stack del sistema**: indica se il dispositivo fa parte di uno stack **(stack nativo** o **indipendente)**. Sono disponibili le seguenti opzioni:
- **Modalità operativa di sistema**: specifica se il sistema funziona in modalità di sistema Livello 2 o Livello 3 per i dispositivi 500. .
- **Descrizione del sistema**: una descrizione del sistema.
- **Percorso di sistema**: posizione fisica del dispositivo. Fare clic su **Modifica** per aprire la pagina Impostazioni di sistema e immettere questo valore.
- **Contatto del sistema**: nome di una persona di riferimento. Fare clic su **Modifica** per aprire la pagina Impostazioni di sistema e immettere questo valore.

- **Nome host**: nome del dispositivo. Fare clic su **Modifica** per aprire la pagina Impostazioni di sistema e immettere questo valore. Il nome host del dispositivo è composto, per impostazione predefinita, dalla parola *switch* concatenata con gli ultimi tre byte meno significativi dell'indirizzo MAC del dispositivo (le ultime sei cifre esadecimali a destra).
- **ID oggetto del sistema**: identificazione del produttore esclusivo del sottosistema di gestione di rete contenuto nell'entità (utilizzato in SNMP).
- **Disponibilità del sistema**: il tempo trascorso dall'ultimo riavvio.
- **Ora corrente**: ora di sistema corrente.
- **Indirizzo MAC di base**: indirizzo MAC del dispositivo. Se il sistema è in modalità stack, viene visualizzato l'indirizzo MAC di base dell'unità master.
- **Frame jumbo**: stato di supporto del frame jumbo. Questo supporto può essere attivato o disattivato tramite la pagina Impostazioni porta del menu Gestione porte.

  NOTA Il supporto per frame Jumbo diventa effettivo solo dopo l'attivazione e dopo il riavvio del dispositivo.

Informazioni sul software:

- **Versione firmware (immagine attiva)**: numero di versione firmware dell'immagine attiva.

  NOTA Se il sistema è in modalità stack nativo, il numero di versione del firmware visualizzato si basa sulla versione del master. Per ulteriori informazioni sulle modalità stack, consultare la sezione **Modalità dell'unità stack**.
- **Checksum firmware MD5 (immagine attiva)**: checksum MD5 dell'immagine attiva.
- **Versione firmware (immagine non attiva)**: numero di versione firmware dell'immagine non attiva. Se il sistema è in modalità stack, viene visualizzata la versione dell'unità master.
- **Checksum firmware MD5 (immagine non attiva)**: checksum MD5 dell'immagine non attiva.
- **Vers. procedura di avvio**: numero vers. procedura di avvio.
- **Checksum avvio MD5**: checksum MD5 della vers. procedura di avvio.

- **Impostazioni locali**: impostazioni locali della prima lingua (sono sempre Inglese).
- **Versione lingua**: versione pacchetto lingua della prima lingua o di inglese.
- **Checksum lingua MD5**: checksum MD5 del file di lingua.

Stato servizi TCP/UDP:

- **Servizio HTTP**: indica se il servizio HTTP è attivato o disattivato.
- **Servizio HTTPS**: indica se il servizio HTTPS è attivato o disattivato.
- **Servizio SNMP**: indica se il servizio SNMP è attivato o disattivato.
- **Servizio Telnet**: indica se Telnet è attivato o disattivato.
- **Servizio SSH**: indica se il servizio SSH è attivato o disattivato.

Informazioni di alimentazione PoE sull'unità Master:

- **Potenza PoE disponibile massima (W)**: potenza disponibile massima che può essere fornita dal PoE.
- **Assorbimento principale totale PoE (W)**: potenza PoE totale offerta ai dispositivi PoE connessi.
- **Modalità alimentazione PoE**: limite porta o limite classe.

Selezionare il collegamento *Dettagli* accanto a **Informazioni di alimentazione PoE sull'unità Master** per accedere direttamente alla pagina Gestione porte > PoE > Proprietà. In questa pagina vengono fornite le informazioni sull'alimentazione PoE in base all'unità.

Le unità nello stack vengono rappresentate graficamente insieme alle seguenti informazioni su ciascuna unità:

- **ID unità dell'unità Master**
- **Descrizione del modello**: descrizione del modello di dispositivo.
- **Numero di serie**: numero di serie.
- **PID VID**: numero di parte e ID versione.

Impostazioni di sistema

Per immettere le impostazioni di sistema, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Impostazioni di sistema**.

PASSAGGIO 2 Consente di visualizzare o modificare le impostazioni di sistema.

- **Descrizione del sistema**: visualizza una descrizione del dispositivo.
- **Percorso di sistema**: immettere la posizione fisica del dispositivo.
- **Contatto del sistema**: immettere il nome di una persona di riferimento.
- **Nome host**: selezionare il nome host del dispositivo. Viene utilizzato nel prompt dei comandi CLI:
  - *Usa predefinito*: il nome host (nome di sistema) predefinito di questi switch è: *switch123456*, dove 123456 rappresenta gli ultimi tre byte dell'indirizzo MAC del dispositivo in formato esadecimale.
  - *Definito dall'utente*: immettere il nome host. Utilizzare solo lettere, cifre e trattini. I nomi host non possono iniziare o finire con un trattino. Non sono consentiti altri simboli, punteggiatura o spazi bianchi (come specificato in RFC1033, 1034, 1035).
- **Impostazioni banner personalizzate**: è possibile impostare i seguenti banner:
  - **Banner di accesso**: immettere il testo che verrà visualizzato nella pagina di accesso prima di effettuare la procedura di accesso. Scegliere **Anteprima** per visualizzare i risultati.
  - **Banner di benvenuto**: immettere il testo che verrà visualizzato nella pagina di accesso dopo aver effettuato la procedura di accesso. Scegliere **Anteprima** per visualizzare i risultati.

  NOTA Quando l'utente definisce un banner di accesso dall'utilità di configurazione basata sul Web, attiva anche il banner per le interfacce CLI (Console, Telnet e SSH).

PASSAGGIO 3 Fare clic su **Applica** per salvare i valori nel file di configurazione esecuzione.

Impostazioni console (supporto velocità di trasmissione automatico)

La velocità della porta della console può essere impostata su uno dei valori seguenti: 4800, 9600, 19200, 38400, 57600 e 115200 o su Rilevamento automatico.

L'opzione Rilevamento automatico consente al dispositivo di individuare la velocità della console in modo automatico, senza che l'utente sia obbligato a impostarla esplicitamente.

Quando il rilevamento automatico non è attivo, la velocità della porta della console si configura automaticamente sull'ultima impostazione manuale della velocità (115,200 per impostazione predefinita).

Quando il rilevamento automatico è attivo ma la velocità di trasmissione della console non è ancora stata rilevata, il sistema utilizza la velocità 115200 per visualizzare il testo (ad esempio le informazioni sull'avvio).

Dopo aver selezionato il rilevamento automatico nella pagina Impostazioni console, è possibile collegare la console al dispositivo e premere due volte il tasto Invio per attivarlo. Il dispositivo rileva la velocità di trasmissione in modo automatico.

Per attivare il rilevamento automatico o impostare la velocità di trasmissione della console manualmente, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Impostazioni console**.

PASSAGGIO 2 Selezionare una delle seguenti opzioni:

- **Rilevamento automatico**: la velocità di trasmissione della console viene rilevata automaticamente.
- **Statica**: selezionare una delle velocità disponibili.

Interfaccia di gestione

Vedere **Interfacce e gestione IPv4**.

Gestione di stack e modalità di sistema

Vedere **Amministrazione: gestione stack**.

Account utente

Vedere **Definizione degli utenti**.

Definizione di timeout sessione inattiva

L'opzione *Timeout sessione inattiva* configura gli intervalli di tempo in cui le sessioni di gestione possono rimanere inattive prima che avvenga il timeout e che l'utente acceda di nuovo per ristabilire una delle seguenti sessioni:

- **Timeout sessione HTTP**
- **Timeout sessione HTTPS**
- **Timeout sessione Console**
- **Timeout sessione Telnet**
- **Timeout sessione SSH**

Per impostare il timeout sessione inattiva di diversi tipi di sessione, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Timeout sessione inattiva**.

PASSAGGIO 2 Selezionare il timeout per ciascuna sessione dall'elenco corrispondente. Il valore di timeout predefinito è 10 minuti.

PASSAGGIO 3 Fare clic su **Applica** per definire le impostazioni di configurazione sul dispositivo.

Impostazioni ora

Vedere **Amministrazione: impostazione ora**.

Log di sistema

Vedere **Amministrazione: log di sistema**.

Gestione dei file

Vedere **Amministrazione: gestione di file**.

Riavvio del dispositivo

Alcune modifiche della configurazione, come l'attivazione del supporto del frame jumbo, affinché diventino effettive richiedono il riavvio del sistema. Tuttavia, se si riavvia il dispositivo, la configurazione di esecuzione viene eliminata, quindi è importante salvarla nella configurazione di avvio prima di riavviare. Facendo clic su **Applica** la configurazione non viene salvata nella Configurazione di avvio. Per ulteriori informazioni sui file e sui tipi di file, vedere la sezione **File di sistema**.

È possibile eseguire il backup della configurazione da *Amministrazione > Gestione file > Salva/Copia configurazione*, oppure facendo clic su **Salva** nella parte superiore della finestra. È anche possibile caricare la configurazione da un dispositivo remoto. Vedere la sezione **Download/Configurazione backup/Log**.

In alcuni casi si preferisce impostare il riavvio in un determinato momento nel futuro, come nelle situazioni seguenti:

- Si stanno eseguendo azioni su un dispositivo remoto e queste azioni possono provocare una perdita della connessione sul dispositivo remoto. Pianificando in anticipo un riavvio si ripristina la configurazione in uso ed è possibile ripristinare la connessione sul dispositivo remoto. Se queste azioni vengono completate, è possibile cancellare il riavvio ritardato.
- Ricaricando il dispositivo verrà persa la connessione alla rete, perciò grazie al riavvio ritardato è possibile programmare il riavvio in un momento più conveniente per gli utenti, ad esempio di notte.

Per riavviare il dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Riavvio**.

PASSAGGIO 2 Fare clic su uno dei pulsanti **Riavvia** per riavviare il dispositivo.

- **Riavvia**: riavvia il dispositivo. Dato che al riavvio del dispositivo tutte le informazioni non salvate nella configurazione di esecuzione vengono eliminate, è necessario fare clic su **Salva** nell'angolo superiore destro della finestra per mantenere la configurazione corrente durante l'avvio. Se l'opzione Salva non viene visualizzata, la Configurazione di esecuzione corrisponde alla Configurazione di avvio e non è necessario eseguire alcuna azione.

  Sono disponibili le seguenti opzioni:

  - *Immediato*: riavvio immediato.
  - *Data*: immettere la data (mese/giorno) e l'orario (ora e minuti) per il riavvio pianificato. Ciò permette di ricaricare in modo pianificato il software in un momento specifico (utilizzando il formato a 24 ore). Se si specifica il mese e il giorno, il riavvio verrà eseguito nel giorno e nell'orario specificati. Se, invece, non si specifica il mese e il giorno, il riavvio avrà luogo nell'orario specificato del giorno corrente (se l'orario specificato è successivo all'orario corrente) oppure del giorno successivo (se l'orario specificato è precedente all'orario attuale). Se si immette 00:00 il riavvio verrà pianificato per mezzanotte. Il riavvio deve avere luogo entro 24 giorni.

    NOTA Questa opzione può essere utilizzata soltanto se l'ora di sistema è stata impostata manualmente o mediante SNTP.
  - *Tra*: riavvia il dispositivo entro un numero di ore e minuti specifico. Possono trascorrere al massimo 24 giorni.

- **Riavvio con impostazioni predefinite**: il dispositivo viene riavviato utilizzando la configurazione predefinita. Tale processo elimina il file della configurazione di avvio e quello della configurazione di backup.

  L'ID dell'unità stack è impostato su automatico; sui dispositivi Sx500 la modalità di sistema è impostata su Livello 2.

  Il file di configurazione mirror non viene eliminato durante il ripristino delle impostazioni predefinite.

- **Cancellare il file della configurazione di avvio**: consente di cancellare la configurazione di avvio sul dispositivo per l'avvio successivo.

NOTA Se il dispositivo è in modalità stack nativo, questo pulsante consente di ripristinare le impostazioni predefinite sull'intero stack.

NOTA Cancellare il file della configurazione di avvio e riavviare non è come eseguire il riavvio con impostazioni predefinite. Il riavvio con impostazioni predefinite è un'operazione molto più invasiva.

Risorse di routing

L'allocazione TCAM viene gestita in modo differente nei dispositivi Sx500 e SG500X/ESW2-550X. I dispositivi Sx500 dispongono di una TCAM singola utilizzata per il routing e le regole ACL. I dispositivi SG500X/SG500XG/ESW2-550X possiedono due TCAM: una per il routing e l'altra per le regole ACL.

Quando i dispositivi SG500X/ESW2-550X sono in modalità stack ibrido hanno soltanto una TCAM (come i dispositivi Sx500). Vedere **Modalità dell'unità stack**.

Le voci TCAM sono suddivise nei seguenti gruppi:

- **Voci IP**: voci TCAM riservate a percorsi statici IP, interfacce IP e host IP.
- **Voci non IP**: voci TCAM riservate per altre applicazioni, quali regole ACL, monitoraggi CoS e limiti di velocità VLAN.

Se il routing IPv4 è abilitato sul dispositivo, nella tabella seguente viene indicato il numero di voci TCAM utilizzate dalle diverse funzioni:

Entità logica	IPv4
Router adiacente IP	1 voce
Indirizzo IP su un'interfaccia	2 voci
Percorso remoto IP	1 voce

Se il routing IPv6 è abilitato sul dispositivo, nella tabella seguente viene indicato il numero di voci TCAM utilizzate dalle diverse funzioni:

Entità logica	IPv4	IPv6 (TCAM PCL)	IPv6 (TCAM router)
Router adiacente IP	1 voce	1 voce	4 voci
Indirizzo IP su un'interfaccia	2 voci	2 voci	8 voci

Entità logica	IPv4	IPv6 (TCAM PCL)	IPv6 (TCAM router)
Percorso remoto IP	1 voce	1 voce	4 voci
Prefisso On-Link		1 voce	4 voci

La pagina Risorse di routing consente di regolare l'allocazione TCAM.

Se si modifica l'assegnazione TCAM in modo non corretto, viene visualizzato un messaggio di errore. Se l'allocazione TCAM è fattibile, viene visualizzato un messaggio che informa che sarà effettuato un riavvio automatico con le nuove impostazioni. Le risorse di routing possono essere modificate in modo errato in uno dei seguenti modi:

- Il numero di voci TCAM che si allocano è inferiore al numero attualmente in uso.
- Il numero di voci TCAM che si allocano è superiore al numero massimo disponibile per quella categoria (i valori massimi sono indicati nella pagina).

Per visualizzare e modificare le risorse di routing, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Risorse di routing**.

Per il routing IPv4 vengono visualizzati i campi seguenti:

- **Router adiacenti**: **Conteggio** indica il numero di router adiacenti registrati sul dispositivo e **Voci TCAM** indica il numero di voci TCAM usate per i router adiacenti.
- **Interfacce**: **Conteggio** indica il numero di indirizzi IP sulle interfacce sul dispositivo e **Voci TCAM** indica il numero di voci TCAM usate per gli indirizzi IP.
- **Percorsi**: **Conteggio** indica il numero di percorsi registrati sul dispositivo e **Voci TCAM** indica il numero di voci TCAM usate per i percorsi.
- **Totale**: visualizza il numero di voci TCAM che sono attualmente in uso.
- **Voci massime**: selezionare una delle seguenti opzioni:
  - *Usa predefinito*: sui dispositivi Sx500, il numero di voci TCAM è pari al 25% delle dimensioni TCAM. Sui dispositivi SG500X/SG500XG il numero di voci TCAM Router è pari al 50% delle dimensioni router TCAM.

- *Definito dall'utente*: immettere un valore.

Per il routing IPv6 vengono visualizzati i campi seguenti:

- **Router adiacenti**: **Conteggio** indica il numero di router adiacenti registrati sul dispositivo e **Voci TCAM** indica il numero di voci TCAM usate per i router adiacenti.
- **Interfacce**: **Conteggio** indica il numero di indirizzi IP sulle interfacce sul dispositivo e **Voci TCAM** indica il numero di voci TCAM usate per gli indirizzi IP.
- **Prefissi On Link**: **Conteggio** indica il numero di prefissi definiti sul dispositivo e **Voci TCAM** indica il numero di voci TCAM usate per i prefissi.
- **Percorsi**: **Conteggio** indica il numero di percorsi registrati sul dispositivo e **Voci TCAM** indica il numero di voci TCAM usate per i percorsi.
- **Totale**: visualizza il numero di voci TCAM che sono attualmente in uso.
- **Voci massime**: selezionare una delle seguenti opzioni:
  - *Usa predefinito*: sui dispositivi Sx500, il numero di voci TCAM è pari al 25% delle dimensioni TCAM. Sui dispositivi SG500X/SG500XG il numero di voci TCAM Router è pari al 50% delle dimensioni router TCAM.
  - *Definito dall'utente*: immettere un valore.

PASSAGGIO 2 Per salvare le nuove impostazioni, fare clic su **Applica**. In questo modo viene verificata l'applicabilità delle impostazioni delle risorse di routing. Se l'impostazione non è corretta, viene visualizzato un messaggio di errore. Se, invece, è corretta, le impostazioni vengono copiate nel file di configurazione esecuzione.

NOTA Nella parte inferiore di questa pagina viene visualizzato un riepilogo delle voci TCAM attualmente in uso e disponibili. Per la descrizione di questi campi, vedere **Visualizzazione dell'utilizzo di TCAM**.

PASSAGGIO 3 Per salvare le nuove impostazioni, fare clic su **Applica**. In questo modo viene verificata l'applicabilità dell'allocazione TCAM. Se l'impostazione non è corretta, viene visualizzato un messaggio di errore. Se, invece, è corretta, l'allocazione viene salvata nel file di configurazione esecuzione e il dispositivo viene riavviato.

Integrità

Dalla pagina Salute è possibile monitorare lo stato della ventola su tutti i dispositivi dotati di ventola. A seconda del modello, un dispositivo può avere una o più ventole. Alcuni modelli, invece, sono privi di ventola.

Nei dispositivi con sensore di temperatura, per proteggere l'hardware in caso di surriscaldamento, il dispositivo esegue le seguenti azioni se la temperatura è troppo alta e durante il periodo di raffreddamento che segue:

Evento	Azione
Almeno un sensore di temperatura supera la soglia di avviso	Viene generato quanto segue: ▪ Messaggio SYSLOG ▪ Trap SNMP
Almeno un sensore di temperatura supera la soglia critica	Viene generato quanto segue: ▪ Messaggio SYSLOG ▪ Trap SNMP Vengono eseguite le seguenti azioni: ▪ Il LED di sistema è impostato su ambra fisso (se l'hardware lo supporta). ▪ Disattivazione delle porte: se la temperatura critica è stata superata per due minuti, tutte le porte verranno arrestate. ▪ (Sui dispositivi che supportano PoE) Disattivazione del circuito PoE affinché venga consumata meno energia e venga emesso meno calore.
Periodo di raffreddamento dopo aver superato la soglia critica (tutti i sensori sono al di sotto della soglia di avviso - 2°C)	Una volta riportata la temperatura di tutti i sensori al valore di soglia di avviso -2°C, il PHY e tutte le porte vengono riattivati. Se lo stato della VENTOLA è OK, le porte vengono attivate. (Sui dispositivi che supportano PoE) Il circuito PoE viene attivato.

Per visualizzare i parametri di integrità del dispositivo, fare clic su **Stato e statistiche** > **Salute**.

Se il dispositivo è in modalità indipendente vengono visualizzati i campi seguenti:

- **Stato della ventola**: stato della ventola. I valori selezionabili sono:
  - OK: le ventole funzionano normalmente.
  - Guasto: le ventole non funzionano correttamente.
  - N/D: la ventola non è applicabile al modello specifico.
- **Direzione ventola**: la direzione in cui lavorano le ventole.

Se il dispositivo è in modalità stack nativo, nella pagina Salute vengono visualizzati i campi seguenti per ogni unità:

- **Unità**: numero dell'unità.
- **Stato della ventola**: stato delle ventole. Sono disponibili colonne per 4 ventole, ma le informazioni vengono mostrate soltanto per le ventole esistenti sul modello specifico del dispositivo. I valori selezionabili sono:
  - OK: le ventole funzionano normalmente.
  - Guasto: le ventole non funzionano correttamente.
  - N/D: gli ID ventola non sono applicabili al modello specifico.
- **Direzione ventola**: la direzione in cui lavorano le ventole.

Diagnostica

Vedere **Amministrazione: diagnostica**.

Rilevamento - Bonjour

Vedere **Bonjour**.

Rilevamento - LLDP

Vedere **Configurazione di LLDP**.

Rilevamento - CDP

Vedere **Configurazione CDP**.

Ping

Ping è un'utilità volta a verificare se un host remoto possa essere raggiunto e a misurare il tempo di andata e ritorno dei pacchetti inviati dal dispositivo a un dispositivo di destinazione.

Ping opera inviando pacchetti di richiesta Echo Internet Control Message Protocol (ICMP) all'host di destinazione e attendendo una risposta ICMP, a volte definita "pong". Calcola il tempo di round trip e registra le eventuali perdite di pacchetti.

Per eseguire il ping di un host, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere**Amministrazione > Ping**.

PASSAGGIO 2 Configurare il ping immettendo i campi seguenti:

- **Definizione host**: selezionare se specificare l'interfaccia di origine in base all'indirizzo IP o al nome. Questo campo influenza le interfacce visualizzate nel campo IP di origine, come descritto di seguito.
- **Versione IP**: se l'interfaccia di origine viene identificata tramite l'indirizzo IP, selezionare IPv4 o IPv6 per indicare che verrà inserita nel formato selezionato.
- **IP di origine**: selezionare l'interfaccia di origine il cui indirizzo IPv4 verrà utilizzato come indirizzo IPv4 di origine per comunicare con la destinazione. Se il campo Definizione host era Per nome, tutti gli indirizzi IPv4 e IPv6 verranno visualizzati in questo campo a discesa. Se il campo Definizione host era Per indirizzo IP, nel campo Versione IP verranno visualizzati solo gli indirizzi IP esistenti del tipo specificato.

  NOTA Se si seleziona l'opzione Automatico, il sistema calcola l'indirizzo di origine in base all'indirizzo di destinazione.

- **Tipo di indirizzo IPv6 di destinazione**: selezionare Collega locale o Globale per il tipo di indirizzo IPv6 da inserire come indirizzo IP di destinazione.
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale collegamento presenta un prefisso **FE80** non reindirizzabile, che è possibile utilizzare solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questa voce sostituisce l'indirizzo nella configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: se il tipo di indirizzo IPv6 è Collegamento locale, selezionare l'origine da cui riceverlo.
- **Nome/indirizzo IP di destinazione**: indirizzo o nome host del dispositivo di cui deve essere eseguito il ping. La scelta tra indirizzo IP o nome host dipende dall'impostazione Definizione host.
- **Intervallo ping**: tempo di attesa prima che il sistema esegua il ping dei pacchetti. Il ping viene ripetuto un determinato numero di volte in base all'impostazione del campo "Numero ping", che vada a buon fine o meno. Scegliere di utilizzare l'intervallo predefinito o specificare il valore desiderato.
- **Numero ping**: numero di volte in cui verrà eseguita l'operazione di ping. Scegliere di utilizzare il valore predefinito o specificare il valore desiderato.
- **Stato**: permette di visualizzare se il ping è andato a buon fine o meno.

PASSAGGIO 3 Scegliere **Attiva ping** per eseguire il ping dell'host. Viene visualizzato lo stato del ping e viene aggiunto un altro messaggio all'elenco dei messaggi a indicare il risultato dell'operazione.

PASSAGGIO 4 Visualizzare i risultati del ping nella sezione **Contatori ping e stato** della pagina.

Traceroute

Traceroute rileva i percorsi IP lungo i quali sono stati reindirizzati i pacchetti con l'invio di un pacchetto IP all'host di destinazione e di nuovo al dispositivo. La pagina Traceroute mostra ogni hop tra il dispositivo e un host di destinazione e il tempo di andata e ritorno per ciascun hop di questo tipo.

PASSAGGIO 1 Scegliere **Amministrazione > Traceroute**.

PASSAGGIO 2 Configurare Traceroute immettendo le informazioni nei campi seguenti:

- **Definizione host**: selezionare l'opzione per identificare gli host in base all'indirizzo IP o al nome.
- **Versione IP**: se l'host viene identificato tramite l'indirizzo IP, selezionare IPv4 o IPv6 per indicare che verrà inserito nel formato selezionato.
- **IP origine**: selezionare l'interfaccia di origine il cui indirizzo IPv4 verrà utilizzato come indirizzo IPv4 di origine per i messaggi di comunicazione. Se il campo Definizione host field era Per nome, tutti gli indirizzi IPv4 e IPv6 verranno visualizzati in questo campo a discesa. Se il campo Definizione host era Per indirizzo IP, nel campo Versione IP verranno visualizzati solo gli indirizzi IP esistenti del tipo specificato.

  NOTA Se si seleziona l'opzione Automatico, il sistema calcola l'indirizzo di origine in base all'indirizzo di destinazione.
- **Tipo di indirizzo IPv6 di destinazione**: selezionare Collega locale o Globale per il tipo di indirizzo IPv6 da inserire.
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale collegamento presenta un prefisso **FE80** non reindirizzabile, che è possibile utilizzare solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questa voce sostituisce l'indirizzo nella configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: se il tipo di indirizzo IPv6 è Collegamento locale, selezionare l'origine da cui riceverlo.
- **Indirizzo IP/Nome host**: immettere l'indirizzo o il nome dell'host.

- **TTL**: immettere il numero massimo di hop consentiti da Traceroute. In questo modo è possibile impedire a un frame trasmesso di entrare in un loop infinito. Il comando Traceroute termina quando si raggiunge la destinazione o questo valore. Per utilizzare il valore predefinito (30) selezionare **Usa predefinito**.
- **Timeout**: immettere l'intervallo di tempo durante il quale il sistema attende il ritorno di un frame prima di dichiararne lo smarrimento, oppure selezionare **Usa predefinito**.

PASSAGGIO 3 Scegliere **Attiva Traceroute**. L'operazione viene eseguita.

Viene visualizzata una pagina che mostra il tempo di andata e ritorno (RTT, Round Trip Time) e lo stato per ogni andata e ritorno nei campi seguenti:

- **Indice**: viene visualizzato il numero di hop.
- **Host**: visualizza un arresto lungo il percorso verso la destinazione.
- **Tempo andata e ritorno** *(1-3)*: visualizza il tempo di andata e ritorno in (ms) per i frame dal primo al terzo e lo stato delle operazioni dalla prima alla terza.

7

Amministrazione: impostazione ora

Gli orologi di sistema sincronizzati forniscono un frame di riferimento tra tutti i dispositivi della rete. La sincronizzazione dell'ora di rete è importante perché ogni aspetto della gestione, della protezione, della pianificazione e del debug di una rete comporta la determinazione di quando avverranno gli eventi. Senza orologi sincronizzati, non è possibile mettere in relazione in modo preciso i file di log tra i dispositivi, quando si rilevano violazioni della sicurezza o l'uso della rete.

Inoltre, la sincronizzazione dell'ora riduce la confusione nei file system condivisi, poiché è importante che gli orari delle modifiche siano coerenti, indipendentemente dalla macchina in cui risiedono i file system.

Per questi motivi è importante che l'ora configurata su tutti i dispositivi della rete sia precisa.

NOTA Il dispositivo supporta il protocollo SNTP (Simple Network Time Protocol) e, se attivato, il dispositivo sincronizza in modo dinamico il suo orario con l'ora del server SNTP. Il dispositivo funziona solo come client SNTP e non può fornire servizi temporali ad altri dispositivi.

In questa sezione vengono descritte le opzioni per la configurazione dell'ora di sistema, del fuso orario e dell'ora legale (Daylight Savings Time, DST). Vengono trattati i seguenti argomenti:

- **Opzioni Ora di sistema**
- **Modalità SNTP**
- **Configurazione dell'ora di sistema**

Opzioni Ora di sistema

L'ora di sistema può essere impostata manualmente dall'utente, dinamicamente tramite un server SNTP oppure eseguendo la sincronizzazione con il PC su cui viene eseguita l'interfaccia utente. Se viene scelto un server SNTP, le impostazioni manuali dell'ora vengono sovrascritte quando vengono stabilite le comunicazioni con il server.

Come parte del processo di avvio, il dispositivo configura sempre l'ora, il fuso orario e l'ora legale. Questi parametri sono ottenuti dal PC sul quale viene eseguita l'interfaccia utente, dall'SNTP, dai valori impostati manualmente oppure dalle impostazioni predefinite, se tutto il resto non funziona.

Ora

Per impostare l'ora di sistema sul dispositivo, sono disponibili i seguenti metodi:

- **Manuale**: consente di impostare l'ora manualmente.
- **Dal PC**: l'ora può essere ricevuta dal PC utilizzando le informazioni del browser.

  La configurazione dell'ora dal computer viene salvata nel file Configurazione di esecuzione. È necessario copiare la Configurazione di esecuzione nella configurazione di avvio al fine di consentire al dispositivo di utilizzare l'ora dal computer dopo il riavvio. Dopo il riavvio l'ora viene impostata al primo accesso Web del dispositivo.

  Alla prima configurazione di questa funzione, se l'ora non è ancora stata impostata, il dispositivo imposta l'ora dal PC.

  Questo metodo di impostazione dell'ora funziona sia con connessioni HTTP che HTTPS.
- **SNTP**: l'ora può essere ricevuta dai time server SNTP. SNTP garantisce una sincronizzazione dell'ora di rete del dispositivo precisa al millisecondo utilizzando un server SNTP come origine dell'orario. Quando si specifica un server SNTP, se lo si cerca per nome host, nell'interfaccia grafica utente vengono fornite tre opzioni:
  - time-a.timefreq.bldrdoc.gov
  - time-b.timefreq.bldrdoc.gov
  - time-c.timefreq.bldrdoc.gov

Una volta impostata tramite una qualsiasi delle origini sopra riportate, non viene impostata di nuovo dal browser.

NOTA SNTP rappresenta il metodo consigliato per l'impostazione dell'ora.

Fuso orario e ora legale (DST)

Per impostare il fuso orario e l'ora legale sul dispositivo, attenersi alla seguente procedura:

- Configurazione dinamica del dispositivo tramite un server DHCP, in cui:
  - DST dinamica, quando attivata e disponibile, ha sempre la precedenza sulla configurazione manuale dell'ora legale.
  - Se il server che fornisce i parametri di origine è guasto o la configurazione dinamica viene disattivata dall'utente, vengono utilizzate le impostazioni manuali.
  - Configurazione dinamica del fuso orario e dell'ora legale continua dopo la scadenza del periodo di validità dell'indirizzo IP.
- La configurazione manuale del fuso orario e dell'ora legale viene utilizzata come configurazione del fuso orario e dell'ora legale operativi solo se la configurazione dinamica del fuso orario e dell'ora legale è disattivata o non funziona.

  NOTA Il server DHCP deve fornire l'opzione 100 DHCP affinché venga eseguita la configurazione dinamica del fuso orario.

Modalità SNTP

Il dispositivo riceve l'ora di sistema da un server SNTP in uno dei seguenti modi:

- Ricezione broadcast client (modalità passiva)

  I server SNTP trasmettono l'ora e il dispositivo ascolta questi broadcast. Quando il dispositivo è in questa modalità, non è necessario definire un server SNTP unicast.

- **Trasmissione broadcast client (modalità attiva)**: il dispositivo, in quanto client SNTP, necessita di aggiornare periodicamente l'ora SNTP. Questa modalità funziona nei seguenti modi:
  - **Modalità client anycast SNTP**: il dispositivo trasmette i pacchetti con la richiesta dell'ora a tutti i server SNTP della sottorete e attende la risposta.
  - **Modalità server unicast SNTP**: il dispositivo invia le query unicast a un elenco di server SNTP configurati manualmente e attende la risposta.

Il dispositivo supporta contemporaneamente tutte le modalità attive precedenti e seleziona l'ora di sistema migliore ricevuta da un server SNTP, secondo un algoritmo basato sullo strato più vicino (distanza dall'orologio di riferimento).

Configurazione dell'ora di sistema

Selezione dell'origine dell'ora di sistema

Utilizzare la pagina Ora di sistema per selezionare l'origine dell'ora di sistema. Se l'origine è manuale, è possibile immettere l'ora qui.

ATTENZIONE Se l'ora di sistema viene impostata manualmente e il dispositivo viene riavviato, è necessario immettere di nuovo le impostazioni manuali dell'ora.

Per definire l'ora di sistema, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione**> **Impostazione ora** > **Ora di sistema**.

Vengono visualizzati i seguenti campi:

- **Ora corrente (statica)**: ora di sistema indicata sul dispositivo. Viene mostrato il fuso orario DHCP o l'acronimo del fuso orario definito dall'utente, se disponibile.
- **Ultimo server sincronizzato**: indirizzo, strato e tipo del server SNTP da cui è stata recuperata l'ora l'ultima volta.

PASSAGGIO 2 Immettere i seguenti parametri:

Impostazioni origine orario: selezionare l'origine utilizzata per impostare l'orologio di sistema.

- **Origine orario principale (server SNTP)**: selezionando tale opzione, l'ora di sistema viene ottenuta da un server SNTP. Per utilizzare questa funzione, è necessario configurare anche una connessione a un server SNTP nella pagina Impostazioni interfaccia SNTP. Facoltativamente, applicare l'autenticazione delle sessioni SNTP nella pagina Autenticazione SNTP.
- **Origine orario alternativo (PC tramite sessioni HTTP/HTTPS attive)**: selezionare questa opzione per impostare la data e l'ora dal computer di configurazione tramite il protocollo HTTP.

  NOTA Per eseguire l'autenticazione MD5 RIP è necessario impostare l'origine orario. È utile anche per le funzioni relative all'ora, ad esempio: ACL basato sul tempo, porta e autenticazione della porta 802.1, supportate su alcuni dispositivi.

Impostazioni manuali: impostare la data e l'ora manualmente. L'ora locale viene utilizzata quando non c'è un'origine alternativa, ad esempio un server SNTP:

- **Data**: immettere la data di sistema.
- **Ora locale**: immettere l'ora di sistema.

Impostazioni fuso orario: l'ora locale viene utilizzata tramite server DHCP o differenza di fuso orario.

- **Fuso orario da DHCP**: selezionare questa opzione per attivare la configurazione dinamica del fuso orario e di DST dal server DHCP. La configurazione o meno di questi parametri dipende dalle informazioni trovate nel pacchetto DHCP. Se questa opzione è attivata, *è necessario attivare anche il client DHCP sul dispositivo*.

  NOTA Il client DHCP supporta l'opzione 100 con impostazione dinamica del fuso orario.

- **Fuso orario da DHCP**: in questo campo viene visualizzato l'acronimo del fuso orario configurato sul server DHCP. L'acronimo mostrato qui, viene visualizzato nel campo **Ora corrente**.
- **Differenza fuso orario**: selezionare la differenza in ore tra l'*ora di Greenwich* (GMT) e quella locale. Per esempio, la differenza di fuso orario di Parigi è GMT +1, mentre quella di New York è GMT -5.

- **Acronimo fuso orario**: immettere un nome definito dall'utente che rappresenta il fuso orario configurato. L'acronimo mostrato qui, viene visualizzato nel campo **Ora corrente**.

Impostazioni Ora legale: selezionare come viene definito il tipo di ora legale:

- **Ora legale**: selezionare questa opzione per abilitare l'ora legale.
- **Differenza impostazione ora**: immettere il numero di minuti di differenza da GMT, nell'intervallo compreso fra 1 e 1440 (il valore predefinito è 60).
- **Tipo di Ora legale**: fare clic su una delle seguenti opzioni:
  - *USA*: l'ora legale viene impostata in base alle date utilizzate negli Stati Uniti.
  - *Europeo*: l'ora legale viene impostata in base alle date utilizzate dall'Unione Europea e da altri Paesi che utilizzano questo standard.
  - *Per date*: l'ora legale viene impostata manualmente, di solito per un Paese diverso dagli Stati Uniti o da un Paese europeo. Immettere i parametri seguenti.
  - *Ricorrente*: DST si verifica nella stessa data ogni anno.

  La selezione *Per date* consente di personalizzare la data di inizio e di fine dell'ora legale:

  - **Da**: giorno e ora di inizio di DST.
  - **A**: giorno e ora di fine di DST.

  La selezione *Ricorrente* consente una diversa personalizzazione della data di inizio e di fine dell'ora legale:

- **Da**: data in cui ogni anno inizia DST.
  - *Giorno*: giorno della settimana in cui ogni anno inizia DST.
  - *Settimana*: settimana del mese in cui ogni anno inizia DST.
  - *Mese*: mese dell'anno in cui ogni anno inizia DST.
  - *Ora*: l'ora in cui ogni anno inizia DST.
- **A**: data in cui ogni anno finisce DST. Per esempio, DST finisce localmente ogni quarto venerdì di ottobre alle 5:00. I parametri sono:
  - *Giorno*: giorno della settimana in cui ogni anno finisce DST.
  - *Settimana*: settimana del mese in cui ogni anno finisce DST.

- *Mese*: mese dell'anno in cui ogni anno finisce DST.
- *Ora*: l'ora in cui ogni anno finisce DST.

PASSAGGIO 3 Fare clic su **Applica**. I valori dell'ora di sistema vengono scritti nel file Configurazione di esecuzione.

Aggiunta di un server unicast SNTP

È possibile configurare massimo 16 server unicast SNTP.

NOTA Per specificare un server unicast SNTP in base al nome, è necessario configurare i server DNS sul dispositivo (vedere la sezione **Impostazioni DNS**). Per aggiungere un server unicast SNTP, selezionare la casella per attivare **Unicast client SNTP**.

Per aggiungere un server unicast SNTP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Impostazioni ora** > **Unicast SNTP**.

PASSAGGIO 2 Immettere informazioni nei seguenti campi:

- **Unicast client SNTP**: selezionare questa opzione per consentire al dispositivo di utilizzare unicast client SNTP predefiniti con server Unicast SNTP.
- **Interfaccia IPv4 di origine**: selezionare l'interfaccia IPv4 il cui indirizzo IPv4 verrà utilizzato come indirizzo IPv4 di origine in messaggi utilizzati per comunicazioni con il server SNTP.
- **Interfaccia IPv6 di origine**: selezionare l'interfaccia IPv6 il cui indirizzo IPv6 verrà utilizzato come indirizzo IPv6 di origine in messaggi utilizzati per comunicazioni con il server SNTP.

  NOTA Se viene selezionata l'opzione Automatica, il sistema prende l'indirizzo IP di origine dall'indirizzo IP definito nell'interfaccia di uscita.

In questa pagina vengono visualizzate le seguenti informazioni per ogni server SNTP unicast:

- **Server SNTP**: indirizzo IP del server SNTP. Il server preferito, o nome host, viene scelto in base al suo livello di strato.
- **Intervallo di polling**: visualizza se il polling è abilitato o meno.
- **ID chiave di autenticazione**: chiave di identificazione utilizzata per comunicare tra il server SNTP e il dispositivo.

- **Livello strato**: la distanza dall'orologio di riferimento espresso come valore numerico. Un server SNTP non può essere il server primario (strato livello 1) a meno che l'intervallo di polling non sia abilitato.
- **Stato**: stato del server SNTP. I valori selezionabili sono:
  - *Su*: server SNTP al momento funzionante normalmente.
  - *Giù*: server SNTP al momento non disponibile.
  - *Sconosciuto*: sul dispositivo è in corso la ricerca del server SNTP.
  - *In corso*: si verifica quando il server SNTP non ha ancora verificato completamente l'attendibilità del proprio time server, ovvero al primo avvio del server SNTP.
- **Ultima risposta**: data e ora dell'ultima volta che è stata ricevuta una risposta da questo server SNTP.
- **Differenza**: la differenza stimata dell'orologio del server relativo all'orologio locale, in millisecondi. L'host determina il valore di questo offset utilizzando l'algoritmo descritto in RFC 2030.
- **Ritardo**: il ritardo di trasmissione stimato dell'orologio del server relativo all'orologio locale nel percorso di rete tra di essi, in millisecondi. L'host determina il valore di questo ritardo utilizzando l'algoritmo descritto in RFC 2030.
- **Origine**: modalità di definizione del server, ad esempio manuale o da server DHCPv6.
- **Interfaccia**: interfaccia che riceve i pacchetti.

PASSAGGIO 3 Per aggiungere un server unicast SNTP, attivare **Unicast client SNTP**.

PASSAGGIO 4 Fare clic su **Aggiungi**.

PASSAGGIO 5 Immettere i parametri seguenti.

- **Definizione server**: selezionare se il server SNTP è in fase di identificazione da parte del suo indirizzo IP oppure se sta scegliendo un server SNTP noto per nome dall'elenco.

  NOTA Per specificare un server SNTP noto, il dispositivo deve essere connesso a Internet e configurato con un server DNS o configurato in modo che un server DNS venga identificato utilizzando DHCP (vedere la sezione **Impostazioni DNS**).

- **Versione IP**: selezionare la versione dell'indirizzo IP: **Versione 6** o **Versione 4**.

- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se IPv6 viene utilizzato). Le opzioni sono
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale collegamento presenta un prefisso **FE80** non reindirizzabile, che è possibile utilizzare solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questa voce sostituisce l'indirizzo nella configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento (se Collega locale - Tipo di indirizzo IPv6 è selezionato) dall'elenco.
- **Indirizzo IP del server SNTP**: immettere l'indirizzo IP del server SNTP. Il formato dipende dal tipo di indirizzo selezionato.
- **Server SNTP**: selezionare il nome del server SNTP da un elenco di server NTP noti. Se viene selezionata l'opzione **altro**, immettere il nome del server SNTP nel campo adiacente.
- **Intervallo di polling**: selezionare per attivare il polling del server SNTP per le informazioni sull'ora di sistema. Di tutti i server NTP registrati per il polling viene effettuato il polling e l'orologio viene selezionato dal server con il livello di strato più basso (distanza dall'orologio di riferimento) raggiungibile. Il server con lo strato più basso viene considerato il server primario. Il server con lo strato più basso successivo viene considerato un server secondario e così via. Se il server primario è disattivato, il dispositivo effettua il polling di tutti i server con l'impostazione di polling attivata e seleziona un nuovo server primario con lo strato più basso.
- **Autenticazione**: selezionare la casella di controllo per attivare l'autenticazione.
- **ID chiave di autenticazione**: se autenticazione è attivata, selezionare il valore dell'ID della chiave; per creare le chiavi di autenticazione, utilizzare la pagina Autenticazione SNTP.

PASSAGGIO 6 Fare clic su **Applica**. Il server STNP viene aggiunto e si viene ricondotti alla pagina principale.

Configurazione della modalità SNTP

Il dispositivo può essere in modalità attiva e/o passiva (vedere **Modalità SNTP** per ulteriori informazioni).

Per abilitare la ricezione dei pacchetti SNTP da tutti i server della sottorete e/o attivare la trasmissione delle richieste dell'ora ai server SNTP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Impostazioni ora** > **Multicast/Anycast SNTP**.

PASSAGGIO 2 Scegliere tra le seguenti opzioni:

- **Modalità client multicast SNTP IPv4 (ricezione broadcast client)**: selezionare questa opzione per ricevere le trasmissioni multicast IPv4 dell'ora di sistema da qualsiasi server SNTP.
- **Modalità client multicast SNTP IPv6 (ricezione broadcast client)**: selezionare questa opzione per ricevere le trasmissioni multicast IPv6 dell'ora di sistema da qualsiasi server SNTP.
- **Modalità client anycast SNTP IPv4 (trasmissione broadcast client)**: selezionare questa opzione per trasmettere i pacchetti di sincronizzazione SNTP IPv4 che richiedono informazioni sull'ora di sistema. I pacchetti vengono trasmessi a tutti i server SNTP della sottorete.
- **Modalità client anycast SNTP IPv6 (trasmissione broadcast client)**: selezionare questa opzione per trasmettere i pacchetti di sincronizzazione SNTP IPv6 che richiedono informazioni sull'ora di sistema. I pacchetti vengono trasmessi a tutti i server SNTP della sottorete.

PASSAGGIO 3 Se il sistema è in modalità di sistema Livello 3, fare clic su **Aggiungi** per selezionare l'interfaccia di ricezione/trasmissione SNTP.

Scegliere un'interfaccia e selezionare le opzioni di ricezione/trasmissione.

PASSAGGIO 4 Fare clic su **Applica** per salvare le impostazione nel file di configurazione esecuzione.

Definizione di autenticazione SNTP

I client SNTP possono autenticare le risposte tramite HMAC-MD5. Un server SNTP viene associato a una chiave, che viene utilizzata insieme alla risposta stessa come accesso alla funzione MD5; il risultato dell'MD5 è incluso nel pacchetto di risposta.

Nella pagina Autenticazione SNTP è possibile configurare le chiavi di autenticazione utilizzate durante la comunicazione con un server SNTP che richiede l'autenticazione.

La chiave di autenticazione viene creata sul server SNTP in un processo separato che dipende dal tipo di server SNTP in uso. Per maggiori informazioni, consultare l'amministratore di sistema del server SNTP.

Flusso di lavoro

PASSAGGIO 1 Attivare l'autenticazione nella pagina Autenticazione SNTP.

PASSAGGIO 2 Creare una chiave nella pagina Autenticazione SNTP.

PASSAGGIO 3 Associare la chiave a un server SNTP nella pagina Unicast SNTP.

Per attivare l'autenticazione SNTP e definire le chiavi, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Impostazione ora** > **Autenticazione SNTP**.

PASSAGGIO 2 Selezionare **Autenticazione SNTP** per supportare l'autenticazione di una sessione SNTP tra il dispositivo e un server SNTP.

PASSAGGIO 3 Fare clic su **Applica** per aggiornare il dispositivo.

PASSAGGIO 4 Fare clic su **Aggiungi.**

PASSAGGIO 5 Immettere i parametri seguenti.

- **ID chiave di autenticazione**: immettere il numero utilizzato per identificare questa chiave di identificazione SNTP internamente.
- **Chiave di autenticazione**: immettere la chiave utilizzata per l'autenticazione (massimo otto caratteri). Per la sincronizzazione con il dispositivo, è necessario che il server SNTP invii questa chiave.

- **Chiave affidabile**: selezionare questa opzione per consentire al dispositivo di ricevere informazioni sulla sincronizzazione solo da un server SNTP utilizzando questa chiave di autenticazione.

PASSAGGIO 6 Fare clic su **Applica**. I parametri di autenticazione SNTP vengono scritti nel file Configurazione di esecuzione.

Intervallo di tempo

È possibile definire e associare gli intervalli di tempo ai tipi di comando riportati di seguito, affinché vengano applicati solo in quell'intervallo di tempo:

- ACL
- Autenticazione della porta 8021X
- Stato della porta
- PoE basato sul tempo

Sono disponibili due tipi di intervallo di tempo:

- **Assoluto**: questo tipo di intervallo di tempo inizia in una data specifica o nell'immediato e termina in una data specifica o mai. Viene generato nelle pagine Intervallo di tempo. A questo può essere aggiunto un elemento ricorrente.
- **Ricorrente**: questo tipo di intervallo di tempo contiene un elemento che viene aggiunto a un intervallo assoluto; inizia e termina su base regolare. Viene definito nelle pagine Intervallo ricorrente.

Se un intervallo di tempo include intervalli assoluti e ricorrenti, la procedura a cui è associato viene attivata solo se sono stati raggiunti sia l'ora di inizio assoluta sia l'intervallo di tempo ricorrente. La procedura viene disattivata se entrambi gli intervalli di tempo sono stati raggiunti.

Il dispositivo supporta massimo 10 intervalli di tempo assoluti.

Tutte le specifiche di tempo vengono interpretate come ora locale (l'ora legale non influisce). Per garantire che le voci dell'intervallo di tempo diventino effettive nelle ore desiderate, l'ora del sistema deve essere impostata.

È possibile utilizzare la funzione Intervallo di tempo nei casi seguenti:

- Limitare, ad esempio, l'accesso dei computer alla rete durante l'orario di lavoro, dopo il quale le porte di rete vengono bloccate impedendo l'accesso alla rete (vedere **Capitolo 10, “Configurazione delle porte”** e **Capitolo 10, “Configurazione delle impostazioni LAG”**).

- L'imitare l'attività PoE a un determinato periodo.

Intervallo di tempo assoluto

Per definire un intervallo di tempo assoluto, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Impostazione ora** > **Ora Intervallo**.

Vengono visualizzati gli intervalli di tempo esistenti.

PASSAGGIO 2 Per aggiungere un nuovo intervallo di tempo, fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere informazioni nei seguenti campi:

- **Nome intervallo di tempo**: immettere un nuovo nome intervallo di tempo.
- **Ora di inizio assoluta**: per definire l'ora di inizio, immettere le seguenti informazioni:
  - *Immediato*: selezionare l'opzione per fare iniziare immediatamente l'intervallo di tempo.
  - *Data e ora*: immettere la data e l'ora di inizio dell'intervallo di tempo.
- **Ora di fine assoluta**: per definire l'ora di inizio, immettere le seguenti informazioni:
  - *Infinito*: selezionare l'opzione per applicare un intervallo di tempo infinito.
  - *Data e ora*: immettere la data e l'ora di fine dell'intervallo di tempo.

PASSAGGIO 4 Per aggiungere un intervallo di tempo ricorrente, fare clic su **Intervallo ricorrente**.

Intervallo di tempo ricorrente

È possibile aggiungere un elemento dell'intervallo di tempo ricorrente a un intervallo assoluto. Ciò limita l'operazione a determinati periodi di tempo che rientrano nell'intervallo assoluto.

Per aggiungere un elemento dell'intervallo di tempo ricorrente a un intervallo assoluto, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Impostazioni ora** > **Intervallo ricorrente**.

Vengono visualizzati gli intervalli di tempo ricorrenti esistenti (filtrati per uno specifico intervallo di tempo assoluto)

PASSAGGIO 2 Selezionare l'intervallo di tempo assoluto a cui aggiungere l'intervallo ricorrente.

PASSAGGIO 3 Per aggiungere un nuovo intervallo di tempo ricorrente, fare clic su **Aggiungi**.

PASSAGGIO 4 Immettere informazioni nei seguenti campi:

- **Ora di inizio ricorrente**: immettere la data e l'ora di inizio dell'intervallo di tempo su base regolare.

Ora di fine ricorrente: immettere la data e l'ora di fine dell'intervallo di tempo su base regolare.

8

Amministrazione: diagnostica

In questo capitolo vengono presentate le informazioni per la configurazione del mirroring delle porte, per l'esecuzione dei test sui cavi e per la visualizzazione delle informazioni operative sul dispositivo.

Vengono trattati i seguenti argomenti:

- **Test delle porte in rame**
- **Visualizzazione dello stato Modulo ottico**
- **Configurazione del mirroring di porte e VLAN**
- **Visualizzazione dell'utilizzo di CPU e della tecnologia Secure Core Technology**

Test delle porte in rame

Nella pagina Test rame vengono visualizzati i risultati dei test sui cavi integrati eseguiti su cavi in rame dal Virtual Cable Tester (VCT).

VCT esegue due tipi di test:

- La tecnologia TDR (Time Domain Reflectometry) verifica la qualità e le caratteristiche di un cavo in rame collegato a una porta. È possibile provare cavi con una lunghezza massima di 140 metri. Questi risultati sono visualizzati nel blocco Risultati test della pagina Test rame.
- I test basati su DSP vengono eseguiti in collegamenti attivi GE per misurare la lunghezza. Questi risultati sono visualizzati nel blocco Informazioni avanzate della pagina Test rame.

Requisiti per l'esecuzione del test delle porte in rame

Prima di eseguire il test, attenersi alla seguente procedura:

- (Obbligatorio) Disattivare la modalità Portata breve (vedere la pagina Gestione porte > Ethernet verde > Proprietà).
- (Facoltativo) Disattivare EEE (vedere la pagina Gestione porte > Ethernet verde > Proprietà).

Utilizzare un cavo dati CAT5 quando si eseguono i test sull'utilizzo dei cavi (VCT).

La precisione dei risultati dei test può avere un intervallo di errore di +/- 10 per i test avanzati e +/- 2 per i test di base.

ATTENZIONE Quando viene provata una porta, viene impostata sullo stato Inattivo e le comunicazioni vengono interrotte. Dopo il test, la porta torna allo stato Attivo. Non si consiglia di eseguire il test sulle porte in rame in una porta che si sta utilizzando per eseguire l'utilità di configurazione dello switch basata sul Web, perché le comunicazioni con quel dispositivo sono compromesse.

Per provare i cavi in rame collegati alle porte, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Diagnostica** > **Test rame**.

PASSAGGIO 2 Selezionare la porta sulla quale eseguire il test rame.

PASSAGGIO 3 Scegliere **Test rame**.

PASSAGGIO 4 Quando viene visualizzato il messaggio, fare clic su **OK** per confermare che il collegamento può essere interrotto oppure su **Annulla** per bloccare il test.

Nel blocco Risultati test vengono visualizzati i campi seguenti:

- **Ultimo aggiornamento**: ora dell'ultimo test condotto nella porta.
- **Risultati test**: risultati del test sui cavi. È possibile scegliere fra i valori seguenti:
  - *OK*: il cavo ha superato il test.
  - *Nessun cavo*: non è presente un cavo collegato alla porta.
  - *Cavo aperto*: il cavo è collegato solo a una estremità.
  - *Cortocircuito cavo*: si è verificato un cortocircuito sul cavo.

  - *Risultato test sconosciuto*: si è verificato un errore di sistema.
- **Distanza dal guasto**: distanza dalla porta alla posizione del cavo in cui è stato rilevato l'errore.
- **Stato porta operativa**: visualizza se la porta è attiva o inattiva.

Se viene sottoposta a test una porta Giga, il blocco **Informazioni avanzate** visualizza le seguenti informazioni, che vengono aggiornate ogni volta che si accede alla pagina:

- **Lunghezza del cavo:** fornisce una stima della lunghezza.
- **Coppia**: coppia di cavi elettrici in fase di verifica.
- **Stato**: stato della coppia di cavi elettrici. Il rosso indica l'errore e il verde indica lo stato OK.
- **Canale**: canale del cavo che indica se i cavi sono dritti o incrociati.
- **Polarità**: indica se il rilevamento e la correzione automatici della polarità sono stati attivati per la coppia di cavi elettrici.
- **Differenza ritardo coppia**: differenza del ritardo tra le coppie di cavi elettrici.

NOTA I test TDR non possono essere eseguiti quando la velocità della porta è 10Mbit/Sec.

Visualizzazione dello stato Modulo ottico

Nella pagina Stato modulo ottico vengono visualizzate le condizioni operative riportate dal ricetrasmettitore SFP (Small Form-factor Pluggable). Alcune informazioni potrebbero non essere disponibili per gli SFP che non supportano lo standard SFF-8472 del monitoraggio della diagnostica digitale.

SFP compatibili con MSA

Sono supportati i seguenti ricetrasmettitori FE SFP (100 Mbps):

- MFEBX1: ricetrasmettitore 100BASE-BX-20U SFP per cavo in fibra ottica monomodale, lunghezza d'onda 1310 nm, supporta fino a 20 km.
- MFEFX1: ricetrasmettitore 100BASE-FX SFP per cavo in fibra ottica multimodale, lunghezza d'onda 1310 nm, supporta fino a 2 km.

- MFELX1: ricetrasmettitore 100BASE-LX SFP per cavo in fibra ottica monomodale, lunghezza d'onda 1310 nm, supporta fino a 10 km.

Sono supportati i seguenti ricetrasmettitori GE SFP (1000 Mbps):

- MGBBX1: ricetrasmettitore 1000BASE-BX-20U SFP per cavo in fibra ottica monomodale, lunghezza d'onda 1310 nm, supporta fino a 40 km.
- MGBLH1: ricetrasmettitore 1000BASE-LH SFP per cavo in fibra ottica monomodale, lunghezza d'onda 1310 nm, supporta fino a 40 km.
- MGBLX1: ricetrasmettitore 1000BASE-LX SFP per cavo in fibra ottica monomodale, lunghezza d'onda 1310 nm, supporta fino a 10 km.
- MGBSX1: ricetrasmettitore 1000BASE-SX SFP per cavo in fibra ottica multimodale, lunghezza d'onda 850 nm, supporta fino a 550 m.
- MGBT1: ricetrasmettitore 1000BASE-T SFP per cavo in rame della categoria 5, supporta fino a 100 m.

Per visualizzare i risultati dei test ottici, fare clic su **Amministrazione** > **Diagnostica** > **Stato modulo ottico**.

In questa pagina vengono visualizzati i seguenti campi:

- **Porta**: numero della porta su cui è connesso SFP.
- **Descrizione**: la descrizione del ricetrasmettitore ottico.
- **Numero di serie**: numero di serie del ricetrasmettitore ottico.
- **PID**: ID VLAN.
- **VID**: ID del ricetrasmettitore ottico.
- **Temperatura**: temperatura (Celsius) a cui opera l'SFP.
- **Tensione**: tensione operativa dell'SFP.
- **Corrente**: assorbimento corrente dell'SFP.
- **Potenza di uscita**: potenza ottica trasmessa.
- **Potenza di entrata**: potenza ottica ricevuta.
- **Errore trasmettitore**: SFP remoto segnala perdita di segnale. I valori sono Vero, Falso e Nessun segnale (N/S).

- **Perdita del segnale**: SFP locale segnala perdita di segnale. I valori sono Vero e Falso.
- **Data Ready**: SFP è operativo. I valori sono Vero e Falso.

Configurazione del mirroring di porte e VLAN

Il mirroring delle porte è utilizzato su un dispositivo di rete per inviare una copia dei pacchetti di rete visualizzati in una porta dello switch, in più porte del dispositivo o su una VLAN intera per una connessione di monitoraggio di rete in un'altra porta del dispositivo. In genere, questa funzione viene utilizzata per i dispositivi di rete che richiedono il monitoraggio del traffico di rete, ad esempio un sistema di rilevamento delle intrusioni. Un analizzatore di rete connesso alla porta di monitoraggio elabora i pacchetti di dati per la diagnosi, il debug e il monitoraggio delle prestazioni. È possibile eseguire il mirroring di un massimo di otto fonti. Può essere qualsiasi combinazione di otto porte singole e/o VLAN.

È possibile eseguire il mirroring di un massimo di otto fonti.

Di un pacchetto ricevuto in una porta di rete assegnata a una VLAN soggetta al mirroring, viene eseguito il mirroring nella porta dell'analizzatore anche se per il pacchetto è stato eseguito il trap o l'eliminazione. Quando è attivato il mirroring Tx (Transmit) viene eseguito il mirroring dei pacchetti inviati.

Il mirroring non garantisce che tutto il traffico delle porte di origine venga ricevuto nella porta dell'analizzatore (di destinazione). Se alla porta dell'analizzatore vengono inviati più dati di quelli che può supportare, alcuni dati potrebbero andare persi.

Il mirroring VLAN non è attivo in una VLAN che non è stata creata manualmente. Ad esempio, se VLAN 23 è stata creata da GVRP ed è stata creata manualmente VLAN 34 e si crea il mirroring della porta che include VLAN 23, VLAN 34 o entrambe e poi si elimina VLAN 34, lo stato nel mirroring della porta è impostato su **Non pronto** perché VLAN 34 non si trova più nel database e VLAN 23 non è stata creata manualmente.

Viene supportata solo un'istanza di mirroring a livello di sistema. La porta dell'analizzatore (o porta di destinazione per il mirroring di VLAN o di porte) è la stessa per tutte le VLAN o le porte di cui è stato eseguito il mirroring.

Per attivare il mirroring, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Diagnostica** > **Mirroring di porte e VLAN**.

Vengono visualizzati i seguenti campi:

- **Porta di destinazione**: porta in cui deve essere copiato il traffico; la porta dell'analizzatore.
- **Interfaccia origine**: interfaccia, porta o VLAN da cui viene inviato il traffico alla porta dell'analizzatore.
- **Tipo**: tipo di monitoraggio: in ingresso nella porta (Rx), in uscita dalla porta (Tx) o entrambi.
- **Stato**: visualizza uno dei seguenti valori:
  - *Attivo*: le interfacce di origine e di destinazione sono attive e reindirizzano il traffico.
  - *Non pronto*: l'origine o la destinazione (o entrambe) sono inattive e per qualche motivo non reindirizzano il traffico.

PASSAGGIO 2 Scegliere **Aggiungi** per aggiungere una porta o una VLAN di cui eseguire il mirroring.

PASSAGGIO 3 Immettere i seguenti parametri:

- **Porta di destinazione**: selezionare la porta dell'analizzatore in cui vengono copiati i pacchetti. Un analizzatore di rete, come un PC che esegue Wireshark, è connesso a questa porta. Se una porta è stata identificata come la porta di destinazione di un analizzatore, essa rimane la porta di destinazione dell'analizzatore fino a quando tutte le voci non vengono rimosse.
- **Interfaccia origine**: selezionare la porta o la VLAN di origine da cui deve essere eseguito il mirroring del traffico.
- **Tipo**: selezionare se viene eseguito il mirroring in entrata, in uscita o di entrambi i tipi di traffico nella porta dell'analizzatore. Se **Porta** è selezionato, le opzioni sono:
  - *Solo Rx*: mirroring della porta nei pacchetti in entrata.
  - *Solo Tx*: mirroring della porta nei pacchetti in uscita.
  - *Tx e Rx*: mirroring della porta in entrambi i pacchetti in entrata e in uscita.

PASSAGGIO 4 Fare clic su **Applica**. Il mirroring della porta viene aggiunto alla Configurazione di esecuzione.

Visualizzazione dell'utilizzo di CPU e della tecnologia Secure Core Technology

In questa sezione sono descritte la Secure Core Technology (SCT) e le procedure per la visualizzazione dell'utilizzo di CPU.

Il dispositivo gestisce i seguenti tipi di traffico, oltre al traffico dell'utente finale:

- Traffico di gestione
- Traffico di protocollo
- Traffico di snooping

Il traffico eccessivo affatica la CPU e potrebbe impedire il normale funzionamento del dispositivo. Il dispositivo utilizza la tecnologia Secure Core Technology (SCT); questa tecnologia garantisce che il dispositivo riceva ed elabori il traffico di gestione e di protocollo, a prescindere dal volume di traffico totale ricevuto. SCT viene attivata per impostazione predefinita e non può essere disattivata.

Non vi sono interazioni con altre funzioni.

Per visualizzare l'utilizzo di CPU, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione> Diagnostica > Utilizzo della CPU**.

Viene visualizzata la pagina Utilizzo della CPU.

Nel campo Velocità ingresso CPU viene visualizzata la velocità dei frame in ingresso nella CPU al secondo.

Nella finestra viene visualizzato un grafico dell'utilizzo della CPU. L'asse Y rappresenta la percentuale di utilizzo mentre l'asse X è il numero di campionamenti.

PASSAGGIO 2 Selezionare la **Frequenza aggiornamento** (periodo di tempo in secondi) che trascorre prima che le statistiche vengano aggiornate. Per ogni periodo di tempo viene creato un nuovo campione.

9

Amministrazione: rilevamento

In questa sezione vengono fornite le informazioni per la configurazione del rilevamento.

Vengono trattati i seguenti argomenti:

- **Bonjour**
- **LLDP e CDP**
- **Configurazione di LLDP**
- **Configurazione CDP**

Bonjour

Come client Bonjour, il dispositivo trasmette periodicamente i pacchetti del protocollo Rilevamento Bonjour alle sottoreti IP a connessione diretta, dichiarando la sua esistenza e i servizi che fornisce, per esempio HTTP, HTTPS e Telnet (utilizzare la pagina Protezione > Servizi TCP/UDP per attivare o disattivare i servizi del dispositivo). Il dispositivo può essere rilevato da un sistema di gestione di rete o da altre applicazioni di terze parti. Per impostazione predefinita, Bonjour è attivato nella VLAN di gestione. La console Bonjour rileva automaticamente il dispositivo e lo visualizza.

Bonjour in modalità di sistema Livello 2

Se il dispositivo è in modalità di sistema Livello 2, Rilevamento Bonjour è attivato a livello globale e non è possibile attivarlo in base alla porta o alla VLAN. Il dispositivo dichiara tutti i servizi che sono stati attivati da parte dell'amministratore in base alla configurazione della pagina Servizi.

Se Rilevamento Bonjour e IGMP sono entrambi attivati, l'indirizzo multicast IP di Bonjour viene visualizzato nella pagina Indirizzo IP gruppo multicast.

Se Rilevamento Bonjour è disattivato, il dispositivo interrompe gli annunci di qualsiasi tipo di servizio e non risponde alle richieste di servizio da parte delle applicazioni di gestione di rete.

Per attivare Bonjour a livello globale quando il sistema è in modalità Livello 2, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Rilevamento - Bonjour**.

PASSAGGIO 2 Selezionare **Attiva** per attivare il Rilevamento Bonjour a livello globale sul dispositivo.

PASSAGGIO 3 Fare clic su **Applica**. Bonjour viene attivato o disattivato sul dispositivo in base alla selezione.

Bonjour in modalità di sistema Livello 3

In modalità di sistema Livello 3, a ogni interfaccia (VLAN, porta o LAG) può essere assegnato un indirizzo IP. Se Bonjour è attivato, il dispositivo può inviare i pacchetti Rilevamento Bonjour su tutte le interfacce con indirizzi IP. Bonjour può essere assegnato individualmente in base alla porta e/o alla VLAN. Se Bonjour è attivato, il dispositivo può inviare i pacchetti Rilevamento Bonjour a tutte le interfacce con indirizzi IP associati a Bonjour presenti nella tabella Controllo interfaccia rilevamento Bonjour. Se il dispositivo funziona in modalità di sistema Livello 3, accedere a **Configurazione IP** > **Interfacce di gestione e IP** > **Interfaccia IPv4** per configurare un indirizzo IP su una interfaccia.

Se un'interfaccia, ad esempio una VLAN, viene eliminata, vengono inviati pacchetti Goodbye per annullare la registrazione dei servizi che il dispositivo sta dichiarando dalla tabella della cache all'interno della rete locale. La tabella Controllo interfaccia rilevamento Bonjour mostra le interfacce con gli indirizzi IP associati alla funzione Bonjour. Gli annunci Bonjour possono essere trasmessi unicamente sulle interfacce elencate nella tabella (vedere la tabella Controllo interfaccia rilevamento Bonjour nella pagina Amministrazione > Rilevamento Bonjour). Se i servizi disponibili vengono modificati, queste modifiche vengono dichiarate, annullando la registrazione dei servizi disattivati e registrando i servizi attivi. Se un indirizzo IP viene modificato, questa modifica viene dichiarata.

Se Bonjour è disattivato, il dispositivo non invia annunci Rilevamento Bonjour e non ascolta gli annunci Rilevamento Bonjour inviati da altri dispositivi.

Per configurare Bonjour quando il dispositivo è in modalità di sistema Livello 3, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Rilevamento Bonjour**.

PASSAGGIO 2 Selezionare **Attiva** per attivare Rilevamento Bonjour a livello globale.

PASSAGGIO 3 Fare clic su **Applica** per aggiornare il file Configurazione di esecuzione.

PASSAGGIO 4 Per abilitare Bonjour su un'interfaccia, fare clic su **Aggiungi**.

PASSAGGIO 5 Selezionare un'interfaccia e fare clic su **Applica**.

NOTA Fare clic su **Elimina** per disabilitare Bonjour su un'interfaccia; in questo caso verrà eseguita l'operazione di eliminazione senza operazioni aggiuntive, come Applica.

LLDP e CDP

LLDP (Link Layer Discovery Protocol) e CDP (Cisco Discovery Protocol) sono protocolli di livello di collegamento per router adiacenti LLDP e CDP connessi direttamente per dichiarare se stessi e le loro funzionalità a vicenda. Per impostazione predefinita, il dispositivo invia periodicamente un annuncio LLDP/CDP a tutte le sue interfacce, quindi termina ed elabora i pacchetti in entrata LLDP e CDP, come richiesto dai protocolli. Nei protocolli LLDP e CDP, gli annunci sono codificati come TLV (Type, Length, Value; tipo, lunghezza, valore) nel pacchetto.

Vengono applicate le seguenti regole di configurazione CDP/LLDP:

- I protocolli CDP/LLDP possono essere attivati o disattivati a livello globale e per porta. Le funzionalità CDP/LLDP di una porta sono rilevanti solo se i protocolli CDP/LLDP sono attivati globalmente.
- Se i protocolli CDP/LLDP sono abilitati a livello globale, il dispositivo filtra i pacchetti CDP/LLDP in ingresso dalle porte con protocolli CDP/LLDP disattivati.
- Se i protocolli CDP/LLDP sono disattivati a livello globale, il dispositivo può essere configurato in modo da eliminare il traffico in grado di rilevare reti VLAN o il traffico non in grado di rilevare reti VLAN di tutti i pacchetti CDP/LLDP in arrivo. Il traffico in grado di rilevare reti VLAN distribuisce un pacchetto CDP/LLDP in arrivo alla VLAN sulla quale viene ricevuto il pacchetto esclusa la porta di ingresso. Il traffico non in grado di rilevare reti VLAN distribuisce un pacchetto CDP/LLDP in arrivo a tutte le porte esclusa

la porta di ingresso. L'impostazione predefinita è quella di eliminare i pacchetti CDP/LLDP quando i protocolli CDP/LLDP sono disabilitati a livello globale. È possibile configurare l'eliminazione/il traffico dei pacchetti CDP e LLDP in entrata nella pagina delle proprietà CDP e nella pagina delle proprietà LLDP, rispettivamente.

- SmartPort Automatico richiede che i protocolli CDP e/o LLDP siano attivati. SmartPort Automatico configura automaticamente un'interfaccia basata sull'annuncio CDP/LLDP ricevuto dall'interfaccia.
- I dispositivi terminali CDP e LLDP, quali telefoni IP, apprendono la configurazione VLAN voce dagli annunci CDP e LLDP. Per impostazione predefinita, il dispositivo può inviare un annuncio CDP e LLDP basato sulla VLAN voce configurata sul dispositivo. Fare riferimento alle sezioni relative alla VLAN voce e alla VLAN voce automatica per ulteriori dettagli.

NOTA I protocolli CDP/LLDP non capiscono se una porta si trova in un LAG. Se in un LAG sono presenti più porte, i protocolli CDP/LLDP trasmettono i pacchetti su ogni porta, senza tener conto del fatto che le porte sono in un LAG.

Il funzionamento dei protocolli CDP/LLDP è indipendente dallo stato STP di un'interfaccia.

Se il controllo di accesso delle porte 802.1x è attivato su un'interfaccia, il dispositivo trasmette e riceve pacchetti CDP/LLDP dall'interfaccia solo se questa è autenticata e autorizzata.

Se una porta è la destinazione del mirroring, i protocolli CDP/LLDP sono considerati non funzionanti.

NOTA CDP e LLDP sono protocolli di livello di collegamento per dispositivi CDP/LLDP collegati direttamente per dichiarare se stessi e le loro funzionalità. Nelle implementazioni in cui i dispositivi CDP/LLDP non sono collegati direttamente e sono separati con dispositivi non CDP/LLDP, i primi potrebbero essere in grado di ricevere l'annuncio da altri dispositivi solo se i dispositivi non CDP/LLDP distribuiscono i pacchetti CDP/LLDP che ricevono. Se i dispositivi non CDP/LLDP eseguono traffico in grado di rilevare reti VLAN, allora i dispositivi CDP/LLDP sono in grado di ascoltarsi solo se si trovano nella stessa VLAN. Un dispositivo CDP/LLDP può ricevere un annuncio da più dispositivi se i dispositivi non CDP/LLDP distribuiscono i pacchetti CDP/LLDP.

Configurazione di LLDP

In questa sezione viene descritto come configurare LLDP. Vengono trattati i seguenti argomenti:

- **Panoramica di LLDP**
- **Impostazione delle proprietà LLDP**
- **Modifica delle impostazioni della porta LLDP**
- **Criteri di rete LLDP MED**
- **Configurazione delle impostazioni delle porte LLDP MED**
- **Visualizzazione dello stato delle porte LLDP**
- **Visualizzazione di informazioni locali LLDP**
- **Visualizzazione di informazioni sui router LLDP adiacenti**
- **Accesso alle statistiche LLDP**
- **Sovraccarico LLDP**

Panoramica di LLDP

LLDP è un protocollo che consente ai manager di rete di risolvere i problemi e migliorare la gestione di rete in ambienti multi-vendor. LLDP standardizza i metodi con cui i dispositivi di rete si dichiarano ad altri sistemi e memorizzano le informazioni rilevate.

LLDP consente a un dispositivo di dichiarare la propria identificazione, configurazione e le proprie funzionalità ai dispositivi adiacenti che memorizzano poi i dati in un MIB (Management Information Base). Il sistema di gestione di rete modella la topologia della rete interrogando questi database MIB.

LLDP è un protocollo di livello di collegamento. Per impostazione predefinita, il dispositivo termina ed elabora tutti i pacchetti LLDP in entrata come richiesto dal protocollo.

Il protocollo LLDP ha un'estensione chiamata LLDP-MED (LLDP Media Endpoint Discovery) che fornisce e accetta le informazioni dei dispositivi terminali multimediali, come telefoni VoIP e videotelefoni. Per ulteriori informazioni su LLDP-MED, vedere la sezione **Criteri di rete LLDP MED**.

Flusso di lavoro della configurazione di LLDP

Di seguito sono presentati esempi delle azioni che è possibile eseguire con la funzione LLDP in un ordine suggerito. È possibile fare riferimento alla sezione LLDP/CDP per ulteriori istruzioni sulla configurazione di LLDP. Le pagine di configurazione LLDP sono accessibili tramite il menu **Amministrazione > Rilevamento - LLDP**.

1. Utilizzare la pagina Proprietà LLDP per immettere i parametri globali LLDP, come l'intervallo di tempo per l'invio di aggiornamenti LLDP.
2. Utilizzare la pagina Impostazioni porta per configurare LLDP in base alla porta. In questa pagina, le interfacce possono essere configurate per ricevere/trasmettere PDU LLDP, inviare notifiche SNMP, specificare quali TLV dichiarare e dichiarare l'indirizzo di gestione del dispositivo.
3. Per creare criteri di rete LLDP MED, utilizzare la pagina Criteri di rete LLDP MED.
4. Utilizzare la pagina Impostazioni porta LLDP MED per associare criteri di rete LLDP MED e TLV LLDP-MED opzionali alle interfacce desiderate.
5. Se SmartPort automatico deve individuare le funzionalità dei dispositivi LLDP, abilitare LLDP nella pagina delle proprietà SmartPort.
6. Per visualizzare le informazioni relative al sovraccarico, utilizzare la pagina Sovraccarico LLDP.

Impostazione delle proprietà LLDP

La pagina *Proprietà LLDP* consente di immettere i parametri generali di LLDP, come l'attivazione/disattivazione della funzione a livello globale e l'impostazione dei timer.

Per immettere le proprietà LLDP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Rilevamento - LLDP** > **Proprietà**.

PASSAGGIO 2 Immettere i parametri.

- **Stato LLDP**: selezionare questa opzione per attivare LLDP sul dispositivo (opzione attiva per impostazione predefinita).
- **Gestione dei frame LLDP**: se LLDP non è abilitato, selezionare l'azione da intraprendere se viene ricevuto un pacchetto corrispondente ai criteri selezionati:
  - *Filtro*: elimina il pacchetto.
  - *Traffico*: reindirizza il pacchetto a tutti i membri della VLAN.

- **Intervallo dichiarazione TLV**: immettere la velocità in secondi con cui vengono inviati gli aggiornamenti degli annunci LLDP oppure utilizzare le impostazioni predefinite.
- **Intervallo di notifica SNMP della modifica alla topologia**: immettere l'intervallo di tempo minimo tra le notifiche SNMP.
- **Moltiplicatore di sospensione**: immettere il tempo per il quale i pacchetti LLDP vengono conservati prima di essere eliminati, misurato in multipli dell'intervallo dichiarazione TLV. Per esempio, se l'Intervallo dichiarazione TLV è di 30 secondi e il Moltiplicatore di sospensione è 4, i pacchetti LLDP vengono eliminati dopo 120 secondi.
- **Ritardo di reinizializzazione**: immettere l'intervallo di tempo in secondi che trascorre tra la disattivazione e la reinizializzazione di LLDP, seguendo un ciclo di attivazione/disattivazione di LLDP.
- **Ritardo di trasmissione**: immettere quanto tempo in secondi trascorre tra le trasmissioni di frame LLDP successivi a causa di modifiche nel MIB dei sistemi locali LLDP.
- **Annuncio ID chassis**: selezionare una delle seguenti opzioni per l'annuncio nei messaggi LLDP:
  - *Indirizzo MAC*: annuncia l'indirizzo MAC del dispositivo locale.
  - *Nome host*: annuncia il nome host del dispositivo.

PASSAGGIO 3 Nel campo **Numero di ripetizione avvio rapido**, immettere il numero di volte che i pacchetti LLDP vengono inviati durante l'inizializzazione del meccanismo Avvio rapido di LLDP-MED. Avviene quando un nuovo dispositivo di punto terminale si collega al dispositivo. Per una descrizione di LLDP MED, fare riferimento alla sezione Criteri di rete LLDP MED.

PASSAGGIO 4 Fare clic su **Applica**. Le proprietà LLDP vengono aggiunte al file Configurazione di esecuzione.

Modifica delle impostazioni della porta LLDP

Nella pagina Impostazioni porta viene consentita l'attivazione della notifica LLDP e SNMP in base alla porta e l'immissione dei TLV che vengono inviati alla PDU LLDP.

È possibile selezionare i TLV LLDP-MED da dichiarare nella pagina Impostazioni porta LLDP MED ed è possibile configurare l'indirizzo di gestione TLV del dispositivo.

Per definire le impostazioni della porta LLDP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Rilevamento - LLDP** > **Impostazioni porta**.

In questa pagina vengono mostrate le informazioni LLDP della porta.

PASSAGGIO 2 Selezionare una porta e fare clic su **Modifica**.

In questa pagina vengono forniti i seguenti campi:

- **Interfaccia**: selezionare la porta da modificare.
- **Stato amministrativo**: selezionare l'opzione di pubblicazione di LLDP della porta. I valori sono:
  - *Solo Tx*: esegue solo pubblicazioni ma non rilevamenti.
  - *Solo Rx*: esegue rilevamenti ma non pubblicazioni.
  - *Tx e Rx*: esegue pubblicazioni e rilevamenti.
  - *Disattiva*: indica che LLDP è disattivato sulla porta.
- **Notifica SNMP**: selezionare **Attiva** per inviare le notifiche ai destinatari delle notifiche SNMP, per esempio un sistema di gestione SNMP, quando avviene una modifica alla topologia.

  L'intervallo di tempo tra le notifiche viene immesso nel campo Intervallo di notifica SNMP della modifica alla topologia della pagina Proprietà LLDP. Utilizzare SNMP > Destinatari delle notifiche SNMPv1,2 e/o SNMP > Destinatari delle notifiche SNMPv3 per definire i destinatari delle notifiche SNMP.
- **TLV facoltativi disponibili**: selezionare le informazioni che possono essere pubblicate dal dispositivo spostando il TLV nell'elenco **TLV facoltativi selezionati**. I TLV disponibili contengono le seguenti informazioni:
  - *Descrizione della porta*: informazioni sulla porta, inclusi il produttore, il nome del prodotto e la versione hardware/software.
  - *Nome del sistema*: nome assegnato del sistema (in formato alfanumerico). Il valore è uguale all'oggetto sysName.
  - *Descrizione del sistema*: descrizione dell'entità di rete (in formato alfanumerico). Include il nome del sistema e le versioni dell'hardware, il sistema operativo e il software di rete supportato dal dispositivo. Il valore è uguale all'oggetto sysDescr.

- *Funzionalità del sistema*: funzioni principali del dispositivo; viene indicato, inoltre, se queste funzioni sono attivate o meno nel dispositivo. Le funzionalità sono indicate da due ottetti. I bit da 0 a 7 indicano rispettivamente Altro, Repeater, Bridge, access point WLAN, Router, Telefono, Dispositivo cavo DOCSIS e stazione. I bit da 8 a 15 sono riservati.
- *802.3 MAC-PHY*: la funzionalità duplex e velocità bit e le impostazioni correnti duplex e velocità bit del dispositivo di invio. Indica inoltre se le impostazioni correnti sono dovute alla negoziazione automatica o alla configurazione manuale.
- *Aggregazione collegamenti 802.3*: se è possibile aggregare il collegamento (associato alla porta in cui viene trasmessa PDU LLDP). Indica inoltre se il collegamento è attualmente aggregato e, in caso affermativo, fornisce l'identificatore della porta aggregata.
- *Dimensioni massime frame 802.3*: funzionalità delle dimensioni massime del frame dell'implementazione MAC/PHY.

I seguenti campi sono correlati all'Indirizzo di gestione:

- **Modalità di annuncio**: selezionare uno dei seguenti modi per dichiarare l'indirizzo di gestione IP del dispositivo:
  - *Dichiarazione automatica*: il software sceglie automaticamente un indirizzo di gestione da dichiarare fra tutti gli indirizzi IP del prodotto. In caso di più indirizzi IP il software sceglie l'indirizzo IP più basso tra gli indirizzi IP dinamici. Se non sono presenti indirizzi dinamici, il software sceglie l'indirizzo IP più basso tra gli indirizzi IP statici.
  - *Nessuno*: non dichiarare l'indirizzo IP di gestione.
  - *Dichiarazione manuale*: selezionare questa opzione e l'indirizzo IP di gestione da dichiarare. Si consiglia di selezionare questa opzione quando il dispositivo è in modalità di sistema Livello 3 e il dispositivo è configurato con indirizzi IP multipli (questa condizione è sempre vera per i dispositivi SG500X/ESW2-550X).
- **Indirizzo IP**: se è stata selezionata l'opzione Dichiarazione manuale, selezionare l'indirizzo IP di gestione dagli indirizzi forniti.

PASSAGGIO 3 Immettere le informazioni richieste e fare clic su **Applica**. Le impostazioni della porta vengono scritte nel file Configurazione di esecuzione.

Criteri di rete LLDP MED

LLDP-MED (LLDP Media Endpoint Discovery) è un'estensione di LLDP che fornisce ulteriori funzionalità per supportare i dispositivi multimediali terminali. Di seguito vengono elencate alcune delle caratteristiche dei criteri di rete LLDP Med:

- Consente la dichiarazione e il rilevamento di criteri di rete per applicazioni in tempo reale quali voce e/o video.
- Rilevamento della posizione del dispositivo per consentire la creazione di database e, nel caso di Voice over Internet Protocol (VoIP), Emergency Call Service (E-911) utilizzando le informazioni sulla posizione del telefono IP.
- Informazioni per la risoluzione dei problemi. LLDP MED invia avvisi ai responsabili di rete nei casi seguenti:
  - Conflitti tra velocità della porta e modalità duplex
  - Errori di configurazione dei criteri QoS

Impostazione dei criteri di rete LLDP MED

Un criterio di rete LLDP-MED è un insieme correlato di impostazioni di configurazione per una specifica applicazione in tempo reale, come voce o video. Un criterio di rete, se configurato, può essere incluso nei pacchetti LLDP in uscita da associare al dispositivo multimediale terminale LLDP. Il dispositivo multimediale terminale deve inviare il proprio traffico come specificato nel criterio di rete che riceve. Per esempio, è possibile creare un criterio per il traffico VoIP che istruisce il telefono VoIP di eseguire le seguenti azioni:

- Inviare il traffico voce su VLAN 10 come pacchetto con tag e 802.1p priorità 5.
- Inviare il traffico voce con DSCP 46.

Per associare i criteri di rete alle porte, utilizzare la pagina Impostazioni porte LLDP MED. Un amministratore può configurare manualmente uno o più criteri di rete e le interfacce alle quali i criteri devono essere inviati. È responsabilità dell'amministratore creare manualmente le VLAN e le loro appartenenze di porta in conformità ai criteri di rete e alle loro interfacce associate.

Inoltre, un amministratore può istruire il dispositivo in modo da generare e dichiarare automaticamente un criterio di rete per un'applicazione voce basata sulla VLAN voce mantenuta dal dispositivo. Consultare la sezione relativa alla VLAN voce automatica per i dettagli su come il dispositivo mantiene la VLAN voce.

Per definire un criterio di rete LLDP MED, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Rilevamento - LLDP** > **Criteri di rete LLDP MED**.

In questa pagina vengono visualizzati i criteri di rete creati in precedenza.

PASSAGGIO 2 Selezionare **Automatico** per i criteri di rete LLDP MED per un'applicazione voce se il dispositivo deve generare e dichiarare automaticamente un criterio di rete per un'applicazione voce basata sulla VLAN voce mantenuta dallo switch.

NOTA Selezionando questa casella non sarà più possibile configurare manualmente un criterio di rete voce.

PASSAGGIO 3 Fare clic su **Applica** per aggiungere l'impostazione al file Configurazione di esecuzione.

PASSAGGIO 4 Per aggiungere un nuovo criterio, fare clic su **Aggiungi**.

PASSAGGIO 5 Immettere i valori:

- **Numero criterio di rete**: selezionare il numero del criterio da creare.
- **Applicazione**: selezionare dall'elenco il tipo di applicazione (tipo di traffico) per cui è stato definito il criterio di rete.
- **ID VLAN**: immettere l'ID VLAN a cui inviare il traffico.
- **Tag VLAN**: decidere se il traffico è Con tag o Senza tag.
- **Priorità utente**: selezionare la priorità di traffico applicata al traffico definito da questo criterio di rete. Questo è il valore CoS.
- **Valore DSCP**: selezionare il valore DSCP da associare ai dati dell'applicazione inviati dai router adiacenti. In questo modo vengono informati su come dovrebbero contrassegnare il traffico dell'applicazione che inviano al dispositivo.

PASSAGGIO 6 Fare clic su **Applica**. Il criterio di rete viene definito.

NOTA È necessario configurare manualmente le interfacce per includere i criteri di rete desiderati definiti manualmente per i pacchetti LLDP in uscita utilizzando la pagina Impostazioni porte LLDP MED.

Configurazione delle impostazioni delle porte LLDP MED

La pagina Impostazioni porte LLDP MED consente di selezionare i TLV LLDP MED e/o i criteri di rete da includere nell'annuncio LLDP in uscita per le interfacce desiderate. I criteri di rete vengono configurati tramite la pagina Criteri di rete LLDP MED.

NOTA Se il criterio di rete LLDP-MED per applicazione voce (pagina Criteri di rete LLDP MED) è impostato su Automatico e la VLAN voce automatica è in funzione, il dispositivo genera automaticamente un criterio di rete LLDP-MED per applicazione voce per tutte le porte LLDP- MED che fanno parte della VLAN voce.

Per configurare LLDP MED su ogni porta, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Rilevamento - LLDP** > **Impostazioni porte LLDP MED**.

In questa pagina vengono visualizzate le impostazioni LLDP MED, inclusi i TLV attivati, per tutte le porte.

PASSAGGIO 2 Il messaggio nella parte superiore della pagina indica se la generazione del criterio di rete LLDP MED per l'applicazione voce è automatico o meno (vedere **Panoramica di LLDP).** Fare clic sul collegamento per modificare la modalità.

PASSAGGIO 3 Per associare ulteriori TLV LLDP MED e/o uno o più criteri di rete LLDP MED definiti dall'utente a una porta, selezionarla e fare clic su **Modifica**.

PASSAGGIO 4 Immettere i seguenti parametri:

- **Interfaccia**: selezionare l'interfaccia da configurare.
- **Stato LLDP MED**: attivare/disattivare LLDP MED in questa porta.
- **Notifica SNMP**: decidere se una notifica SNMP deve essere inviata in base alle porte quando viene rilevata una stazione terminale che supporta MED, per esempio un sistema di gestione SNMP, nel caso in cui ci sia una modifica alla topologia.
- **TLV facoltativi disponibili**: selezionare i TLV che possono essere pubblicati dal dispositivo spostandoli nell'elenco *TLV facoltativi selezionati*.
- **Criteri di rete disponibili**: selezionare i criteri LLDP MED pubblicati da LLDP, spostandoli nell'elenco Criteri di rete selezionati. Questi sono stati creati nella pagina Criteri di rete LLDP MED. Per includere uno o più criteri di rete definiti dall'utente nella dichiarazione. può essere necessario selezionare anche *Criteri di rete* in TLV facoltativi disponibili.

NOTA I seguenti campi devono essere compilati in caratteri esadecimali nel formato dati esatto definito nello standard LLDP-MED (ANSI-TIA-1057_final_for_publication.pdf).

- **Coordinate posizione**: immettere le coordinate posizione da far pubblicare a LLDP.
- **Indirizzo civico posizione**: immettere l'indirizzo civico da far pubblicare a LLDP.
- **Collegamento (ECS) ELIN**: immettere il collegamento Emergency Call Service (ECS) ELIN da far pubblicare a LLDP.

PASSAGGIO 5 Fare clic su **Applica**. Le impostazioni della porta LLDP MED vengono scritte nel file Configurazione di esecuzione.

Visualizzazione dello stato delle porte LLDP

Nella pagina Tabella Stato porte LLDP vengono visualizzate le informazioni globali LLDP per ogni porta.

PASSAGGIO 1 Per visualizzare lo stato delle porte LLDP, fare clic su **Amministrazione** > **Rilevamento - LLDP** > **Stato porte LLDP**.

PASSAGGIO 2 Fare clic su **Dettagli informazioni locali LLDP** per visualizzare i dettagli dei TLV di LLDP e di LLDP-MED inviati al router adiacente.

PASSAGGIO 3 Fare clic su **Dettagli informazioni router LLDP contigui** per visualizzare i dettagli dei TLV di LLDP e di LLDP-MED ricevuti dal router adiacente.

Informazioni generali sullo stato delle porte LLDP

- **Sottotipo ID chassis**: tipo di ID chassis (per esempio, indirizzo MAC).
- **ID chassis**: identificatore di chassis. Se il sottotipo ID chassis è un indirizzo MAC, viene visualizzato l'indirizzo MAC del dispositivo.
- **Nome del sistema**: il nome del dispositivo.
- **Descrizione del sistema**: la descrizione del dispositivo (in formato alfanumerico).
- **Funzionalità del sistema supportate**: funzioni principali del dispositivo, come Bridge, WLAN AP o Router.

- **Funzionalità del sistema attivate**: funzioni principali del dispositivo attivate.
- **Sottotipo ID porta**: tipo di identificatore della porta mostrato.

Tabella Stato porte LLDP

- **Interfaccia**: identificatore della porta.
- **Stato LLDP**: opzione di pubblicazione di LLDP.
- **Stato LLDP MED**: attivato o disattivato.
- **PoE locale**: informazioni sul PoE locale dichiarate.
- **PoE remoto**: informazioni sul PoE dichiarate dal router adiacente.
- **N. di router adiacenti**: numero di router adiacenti rilevati.
- **Funzionalità router adiacente del primo dispositivo**: vengono visualizzate le funzioni primarie del router adiacente, ad esempio bridge o router.

Visualizzazione di informazioni locali LLDP

Per visualizzare lo stato delle porte locale LLDP dichiarato su una porta, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Rilevamento - LLDP** > **Informazioni locali LLDP**.

PASSAGGIO 2 Nella parte inferiore della pagina, fare clic su **Tabella Stato porte LLDP**.

Fare clic su **Dettagli informazioni locali LLDP** per visualizzare i dettagli dei TLV di LLDP e di LLDP-MED inviati al router adiacente.

Fare clic su **Dettagli informazioni router LLDP adiacenti** per visualizzare i dettagli dei TLV di LLDP e di LLDP-MED ricevuti dal router adiacente.

PASSAGGIO 3 Selezionare la porta desiderata dall'elenco **Porta**.

In questa pagina vengono visualizzati i seguenti campi:

Globale

- **Sottotipo ID chassis**: tipo di ID chassis (per esempio, l'indirizzo MAC).
- **ID chassis**: identificatore di chassis. Se il sottotipo ID chassis è un indirizzo MAC, viene visualizzato l'indirizzo MAC del dispositivo.
- **Nome del sistema**: il nome del dispositivo.

- **Descrizione del sistema**: la descrizione del dispositivo (in formato alfanumerico).
- **Funzionalità del sistema supportate**: funzioni principali del dispositivo, come Bridge, WLAN AP o Router.
- **Funzionalità del sistema attivate**: funzioni principali del dispositivo attivate.
- **Sottotipo ID porta**: tipo di identificatore della porta mostrato.
- **ID porta**: identificatore della porta.
- **Descrizione della porta**: informazioni sulla porta, inclusi il produttore, il nome del prodotto e la versione hardware/software.

Indirizzo di gestione

Viene visualizzata la tabella degli indirizzi dell'agente LLDP locale. Gli altri responsabili remoti possono utilizzare questo indirizzo per ottenere informazioni relative al dispositivo locale. L'indirizzo consiste negli elementi seguenti:

- **Sottotipo indirizzo**: tipo di indirizzo IP di gestione elencato nel campo Indirizzo di gestione, per esempio, IPv4.
- **Indirizzo**: indirizzo restituito più appropriato per l'utilizzo di gestione, di solito un indirizzo di Livello 3.
- **Sottotipo interfaccia**: metodo di numerazione utilizzato per definire il numero di interfaccia.
- **Numero interfaccia**: interfaccia specifica associata a questo indirizzo di gestione.

Dettagli MAC/PHY

- **Negoziazione automatica supportata**: stato di supporto della negoziazione automatica della velocità della porta.
- **Negoziazione automatica attivata**: stato attivo della negoziazione automatica della velocità della porta.
- **Funzionalità dichiarate della negoziazione automatica**: funzionalità di negoziazione automatica della velocità della porta, per esempio, modalità 1000BASE-T half duplex, modalità 100BASE-TX full duplex.

- **Tipo MAU operativo**: tipo di MAU (Medium Attachment Unit). La MAU esegue funzioni di livello fisico, inclusa la conversione di dati digitali dal rilevamento di collisioni delle interfacce Ethernet e l'inserimento di bit nella rete (per esempio, modalità 100BASE-TX full duplex).

Dettagli 802.3

- **Dimensioni massime frame 802.3**: le dimensioni IEEE 802.3 massime supportate.

Aggregazione collegamenti 802.3

- **Funzionalità di aggregazione**: indica se è possibile aggregare l'interfaccia.
- **Stato di aggregazione**: indica se l'interfaccia è aggregata.
- **ID porta di aggregazione**: ID interfaccia aggregata dichiarato.

Energy Efficient Ethernet (EEE) 802.3 (se il dispositivo supporta EEE)

- **Tx locale**: indica il tempo (in microsecondi) che il partner di collegamento di trasmissione attende prima di iniziare a trasmettere i dati all'uscita dalla modalità LPI (Low Power Idle).
- **Rx locale**: indica il tempo (in microsecondi) che il partner di collegamento di ricezione chiede al partner di collegamento di trasmissione di attendere prima di iniziare con la trasmissione dei dati all'uscita dalla modalità LPI (Low Power Idle).
- **Eco TX remoto**: indica il modo in cui il partner di collegamento locale riflette il valore Tx del partner di collegamento remoto.
- **Eco RX remoto**: indica il modo in cui il partner di collegamento locale riflette il valore Rx del partner di collegamento remoto.

Dettagli MED

- **Funzionalità supportate**: funzionalità MED supportate sulla porta.
- **Funzionalità correnti**: funzionalità MED attivate sulla porta.
- **Classe del dispositivo**: classe del dispositivo del punto terminale LLDP-MED. Le possibili classi del dispositivo sono:
  - *Classe punto terminale 1*: indica una classe del punto terminale generica, che offre servizi LLDP di base.

- *Classe punto terminale 2*: indica una classe del punto terminale del supporto, che offre funzionalità di flusso multimediale e tutte le funzioni della Classe 1.
- *Classe punto terminale 3*: indica una classe di dispositivi di comunicazione che offre tutte le funzioni della Classe 1 e 2 più località 911, supporto per lo switch di Livello 2 e funzionalità di gestione delle informazioni sul dispositivo.

- **Tipo di dispositivo PoE**: tipo di porta PoE, per esempio, alimentata.
- **Origine alimentazione PoE**: origine di alimentazione della porta.
- **Priorità alimentazione PoE**: priorità di alimentazione della porta.
- **Valore alimentazione PoE**: valore di alimentazione della porta.
- **Revisione hardware**: versione hardware.
- **Revisione firmware**: versione firmware.
- **Revisione software**: versione software.
- **Numero di serie**: numero di serie del dispositivo.
- **Nome produttore**: nome del produttore del dispositivo.
- **Nome modello**: nome del modello del dispositivo.
- **ID asset**: ID asset.

Informazioni sulla posizione

- **Civico**: indirizzo.
- **Coordinate**: coordinate della mappa: latitudine, longitudine e altitudine.
- **ECS ELIN**: numero ELIN (Emergency Location Identification Number) del servizio ECS (Emergency Call Service).

Tabella Criteri di rete

- **Tipo di applicazione**: tipo di applicazione dei criteri di rete, per esempio Voce.
- **ID VLAN**: ID VLAN per cui viene definito il criterio di rete.

- **Tipo VLAN**: tipo di VLAN per cui viene definito il criterio di rete. Le opzioni disponibili sono:
  - *Con tag*: indica che il criterio di rete è definito per le VLAN con tag.
  - *Senza tag*: indica che il criterio di rete è definito per le VLAN senza tag.
- **Priorità utente**: priorità utente dei criteri di rete.
- **DSCP**: DSCP criteri di rete.

Visualizzazione di informazioni sui router LLDP adiacenti

La pagina delle informazioni sui router LLDP adiacenti visualizza informazioni che sono state ricevute da dispositivi adiacenti.

Dopo il timeout (basato sul valore acquisito dal campo Time To Live TLV del router adiacente nel quale non è stata ricevuta alcuna PDU LLDP da un router adiacente), le informazioni vengono eliminate.

Per visualizzare le informazioni sui router LLDP adiacenti, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Rilevamento - LLDP** > **Informazioni contigui LLDP**.

In questa pagina vengono forniti i seguenti campi:

- **Porta locale**: numero della porta locale a cui è connesso il router adiacente.
- **Sottotipo ID chassis**: tipo di ID chassis (per esempio, indirizzo MAC).
- **ID chassis**: identificatore di chassis del dispositivo adiacente 802 LAN.
- **Sottotipo ID porta**: tipo di identificatore della porta mostrato.
- **ID porta**: identificatore della porta.
- **Nome del sistema**: nome del dispositivo pubblicato.
- **Durata**: intervallo di tempo (in secondi) dopo il quale le informazioni di questo router adiacente vengono eliminate.

PASSAGGIO 2 Selezionare una porta locale e fare clic su **Dettagli**.

Nella pagina Informazioni sui router LLDP adiacenti vengono visualizzati i seguenti campi:

Dettagli porta

- **Porta locale**: numero della porta.
- **Voce MSAP**: numero della voce MSAP (Media Service Access Point) del dispositivo.

Dettagli di base

- **Sottotipo ID chassis**: tipo di ID chassis (per esempio, indirizzo MAC).
- **ID chassis**: identificatore di chassis del dispositivo adiacente 802 LAN.
- **Sottotipo ID porta**: tipo di identificatore della porta mostrato.
- **ID porta**: identificatore della porta.
- **Descrizione della porta**: informazioni sulla porta, inclusi il produttore, il nome del prodotto e la versione hardware/software.
- **Nome del sistema**: nome del sistema pubblicato.
- **Descrizione del sistema**: descrizione dell'entità di rete (in formato alfanumerico). Include il nome del sistema e le versioni dell'hardware, il sistema operativo e il software di rete supportati dal dispositivo. Il valore è uguale all'oggetto sysDescr.
- **Funzionalità del sistema supportate**: funzioni principali del dispositivo. Le funzionalità sono indicate da due ottetti. I bit da 0 a 7 indicano rispettivamente Altro, Repeater, Bridge, access point WLAN, Router, Telefono, Dispositivo cavo DOCSIS e stazione. I bit da 8 a 15 sono riservati.
- **Funzionalità del sistema attivate**: funzioni principali del dispositivo attivate.

Tabella Indirizzo di gestione

- **Sottotipo indirizzo**: sottotipo di indirizzo di gestione, per esempio MAC o IPv4.
- **Indirizzo**: indirizzo di gestione.
- **Sottotipo interfaccia**: sottotipo di porta.
- **Numero interfaccia**: numero di porta.

Dettagli MAC/PHY

- **Negoziazione automatica supportata**: stato di supporto della negoziazione automatica della velocità della porta. I possibili valori sono Vero e Falso.
- **Negoziazione automatica attivata**: stato attivo della negoziazione automatica della velocità della porta. I possibili valori sono Vero e Falso.
- **Funzionalità dichiarate della negoziazione automatica**: funzionalità di negoziazione automatica della velocità della porta, per esempio, modalità 1000BASE-T half duplex, modalità 100BASE-TX full duplex.
- **Tipo MAU operativo**: tipo di MAU (Medium Attachment Unit). La MAU esegue funzioni di livello fisico, inclusa la conversione di dati digitali dal rilevamento di collisioni delle interfacce Ethernet e l'inserimento di bit nella rete (per esempio, modalità 100BASE-TX full duplex).

Alimentazione 802.3 tramite MDI

- **Classe porta di supporto alimentazione MDI**: classe porta di supporto alimentazione dichiarata.
- **Supporto alimentazione MDI PSE**: indica se l'alimentazione MDI è supportata sulla porta.
- **Stato alimentazione MDI PSE**: indica se l'alimentazione MDI è attivata sulla porta.
- **Capacità di controllo coppia alimentazione PSE**: indica se il controllo coppia alimentazione è supportato sulla porta.
- **Coppia alimentazione PSE**: tipo di controllo coppia alimentazione supportato sulla porta.
- **Classe di alimentazione PSE**: valore di alimentazione della porta dichiarato.

Dettagli 802.3

- **Dimensioni massime frame 802.3**: le dimensioni massime dichiarate supportate nella porta.

Aggregazione collegamenti 802.3

- **Funzionalità di aggregazione**: indica se è possibile aggregare la porta.
- **Stato di aggregazione**: indica se la porta è correntemente aggregata.
- **ID porta di aggregazione**: ID porta aggregata dichiarato.

Energy Efficient Ethernet (EEE) 802.3

- **Tx remoto**: indica il tempo (in microsecondi) che il partner di collegamento di trasmissione attende prima di iniziare a trasmettere i dati all'uscita dalla modalità LPI (Low Power Idle).
- **Rx remoto**: indica il tempo (in microsecondi) che il partner di collegamento di ricezione chiede al partner di collegamento di trasmissione di attendere prima di iniziare con la trasmissione dei dati all'uscita dalla modalità LPI (Low Power Idle).
- **Eco TX locale**: indica il modo in cui il partner di collegamento locale riflette il valore Tx del partner di collegamento remoto.
- **Eco RX locale**: indica il modo in cui il partner di collegamento locale riflette il valore Rx del partner di collegamento remoto.

Dettagli MED

- **Funzionalità supportate**: funzionalità MED attivate sulla porta.
- **Funzionalità correnti**: TLV MED dichiarati dalla porta.
- **Classe del dispositivo**: classe del dispositivo del punto terminale LLDP-MED. Le possibili classi del dispositivo sono:
  - *Classe punto terminale 1*: indica una classe del punto terminale generica, che offre servizi LLDP di base.
  - *Classe punto terminale 2*: indica una classe del punto terminale del supporto, che offre funzionalità di flusso multimediale e tutte le funzioni della Classe 1.
  - *Classe punto terminale 3*: indica una classe di dispositivi di comunicazione che offre tutte le funzioni della Classe 1 e 2 più collegamento, 911, supporto per lo switch di Livello 2 e funzionalità per la gestione delle informazioni sul dispositivo.
- **Tipo di dispositivo PoE**: tipo di porta PoE, per esempio, alimentata.
- **Origine alimentazione PoE**: origine di alimentazione della porta.
- **Priorità alimentazione PoE**: priorità di alimentazione della porta.
- **Valore alimentazione PoE**: valore di alimentazione della porta.
- **Revisione hardware**: versione hardware.
- **Revisione firmware**: versione firmware.

- **Revisione software**: versione software.
- **Numero di serie**: numero di serie del dispositivo.
- **Nome produttore**: nome del produttore del dispositivo.
- **Nome modello**: nome del modello del dispositivo.
- **ID asset**: ID asset.

VLAN e protocollo 802.1

- **PVID**: ID VLAN della porta dichiarato.

Tabella PPVID

- **VID**: ID VLAN del protocollo.
- **Supportato**: ID VLAN del protocollo e della porta supportati.
- **Attivato**: ID VLAN del protocollo e della porta attivati.

ID VLAN

- **VID**: ID VLAN del protocollo e della porta.
- **Nome VLAN**: nomi della VLAN dichiarati.

ID protocollo

- **Tabella ID protocollo**: ID del protocollo dichiarati.

Informazioni sulla posizione

Immettere le seguenti strutture di dati in esadecimali come descritto nella sezione 10.2.4 dello standard ANSI-TIA-1057:

- **Civico**: civico o indirizzo.
- **Coordinate**: coordinate della mappa posizione (latitudine, longitudine e altitudine).
- **ECS ELIN**: numero ELIN (Emergency Location Identification Number) del servizio ECS (Emergency Call Service) del dispositivo.
- **Sconosciuto**: informazioni sulla posizione sconosciute.

Criteri di rete

- **Tipo di applicazione**: tipo di applicazione dei criteri di rete, per esempio Voce.
- **ID VLAN**: ID VLAN per cui viene definito il criterio di rete.
- **Tipo di VLAN**: tipo di VLAN, Con tag o Senza tag, per cui viene definito il criterio di rete.
- **Priorità utente**: priorità utente dei criteri di rete.
- **DSCP**: DSCP criteri di rete.

Accesso alle statistiche LLDP

Nella pagina Statistiche LLDP vengono visualizzate le informazioni statistiche LLDP in base alla porta.

Per visualizzare le statistiche LLDP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Rilevamento - LLDP** > **Statistiche LLDP**.

Per ogni porta, vengono visualizzati i seguenti campi.

- **Interfaccia**: identificatore dell'interfaccia.
- **Frame Tx totali**: numero di frame trasmessi.
- **Frame Rx**
  - *Totale*: numero di frame ricevuti.
  - *Eliminato*: numero totale di frame ricevuti che sono stati eliminati.
  - *Errori*: numero totale di frame ricevuti con errori.
- **TLV Rx**
  - *Eliminato*: numero totale di TLV ricevuti che sono stati eliminati.
  - *Non riconosciuto*: numero totale di TLV ricevuti che non sono stati riconosciuti.
- **Numero di eliminazioni di informazioni sui router adiacenti**: numero di scadenze di router adiacenti sull'interfaccia.

PASSAGGIO 2 Fare clic su **Aggiorna** per visualizzare le ultime statistiche.

Sovraccarico LLDP

LLDP aggiunge informazioni come LLDP e TLV LLDP MED ai pacchetti LLDP. Il sovraccarico LLDP si verifica quando la quantità totale di informazioni da includere in un pacchetto LLDP eccede la dimensione massima PDU supportata da un'interfaccia.

Nella pagina Sovraccarico LLDP viene visualizzato il numero di byte di informazioni LLDP/LLDP-MED, il numero di byte disponibili per ulteriori informazioni LLDP e lo stato di sovraccarico di ogni interfaccia.

Per visualizzare le informazioni sul sovraccarico di LLDP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione** > **Rilevamento - LLDP** > **Sovraccarico LLDP**.

In questa pagina vengono visualizzati i seguenti campi per ogni porta.

- **Interfaccia**: identificatore della porta.
- **Totale (byte)**: numero totale di byte di informazioni LLDP in ogni pacchetto.
- **Da inviare (byte)**: numero totale di byte disponibili rimasti in ogni pacchetto per ulteriori informazioni LLDP.
- **Stato**: se i TLV sono in fase di trasmissione o se sono sovraccarichi.

PASSAGGIO 2 Per visualizzare i dettagli del sovraccarico di una porta, selezionarla e fare clic su **Dettagli**.

In questa pagina vengono visualizzate le seguenti informazioni per ogni TLV inviato nella porta:

- **TVL obbligatori LLDP**
  - *Dimensioni (byte)*: dimensioni in byte dei TLV obbligatori totali.
  - *Stato*: se il gruppo TLV obbligatorio è in fase di trasmissione oppure se è stato sovraccaricato.
- **Funzionalità LLDP MED**
  - *Dimensioni (byte)*: dimensioni totali in byte dei pacchetti delle funzionalità LLDP MED.

- *Stato*: se i pacchetti delle funzionalità LLDP MED sono stati inviati oppure se sono stati sovraccaricati.

- **Posizione LLDP MED**
  - *Dimensioni (byte)*: dimensioni totali in byte dei pacchetti della posizione di LLDP MED.
  - *Stato*: se i pacchetti delle posizioni LLDP MED sono stati inviati oppure se sono stati sovraccaricati.
- **Criteri di rete LLDP MED**
  - *Dimensioni (byte)*: dimensioni totali in byte dei pacchetti dei criteri di rete LLDP MED.
  - *Stato*: se i pacchetti dei criteri di rete LLDP MED sono stati inviati oppure se sono stati sovraccaricati.
- **Alimentazione estesa LLDP MED tramite MDI**
  - *Dimensioni (byte)*: dimensioni totali in byte dei pacchetti con alimentazione estesa LLDP MED tramite MDI.
  - *Stato*: se l'alimentazione estesa LLDP MED è stata inviata tramite pacchetti MDI oppure se è stata sovraccaricata.
- **TLV 802.3**
  - *Dimensioni (byte)*: dimensioni totali in byte dei pacchetti di TLV LLDP MED 802.3.
  - *Stato*: se i pacchetti di TLV LLDP MED 802.3 sono stati inviati oppure se sono stati sovraccaricati.
- **TLV facoltativi LLDP**
  - *Dimensioni (byte)*: dimensioni totali in byte dei pacchetti di TLV LLDP MED facoltativi.
  - *Stato*: se i pacchetti di TLV LLDP MED facoltativi sono stati inviati oppure se sono stati sovraccaricati.
- **Inventario LLDP MED**
  - *Dimensioni (byte)*: dimensioni totali in byte dei pacchetti di TLV dell'inventario LLDP MED.
  - *Stato*: se i pacchetti dell'inventario LLDP MED sono stati inviati oppure se sono stati sovraccaricati.

- **Totale (byte)**: numero totale di byte di informazioni LLDP in ogni pacchetto.
- **Da inviare (byte)**: numero totale di byte disponibili rimasti in ogni pacchetto per ulteriori informazioni LLDP.

Configurazione CDP

In questa sezione viene descritto come configurare CDP.

Vengono trattati i seguenti argomenti:

- **Impostazione delle proprietà CDP**
- **Modifica delle impostazioni dell'interfaccia CDP**
- **Visualizzazione delle informazioni locali CDP**
- **Visualizzazione delle informazioni dei router adiacenti CDP**
- **Visualizzazione delle statistiche CDP**

Impostazione delle proprietà CDP

Analogamente a LLDP, CDP (Cisco Discovery Protocol) è un protocollo di livello di collegamento per router adiacenti collegati direttamente per dichiarare se stessi e le loro funzionalità a vicenda. A differenza di LLDP, CDP è un protocollo proprietario di Cisco.

Flusso di lavoro della configurazione di CDP

Di seguito viene riportato un esempio di flusso di lavoro per la configurazione del protocollo CDP sul dispositivo. Ulteriori linee guida sono disponibili nella sezione LLDP/CDP.

PASSAGGIO 1 Immettere i parametri globali CDP tramite la pagina delle proprietà CDP

PASSAGGIO 2 Configurare CDP per l'interfaccia tramite la pagina di impostazione dell'interfaccia

PASSAGGIO 3 Se SmartPort automatico deve individuare le funzionalità dei dispositivi CDP, abilitare CDP nella pagina Proprietà SmartPort.

Vedere la sezione **Identificazione del tipo di Smartport** per una descrizione di come viene utilizzato CDP per identificare i dispositivi per la funzione SmartPort.

Per immettere i parametri generali di CDP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Rilevamento - CDP** > **Proprietà**.

PASSAGGIO 2 Immettere i parametri.

- **Stato CDP**: selezionare questa opzione per attivare CDP sul dispositivo.
- **Gestione frame CDP**: se CDP non è abilitato, selezionare l'azione da intraprendere quando viene ricevuto un pacchetto corrispondente ai criteri selezionati:
  - *Bridging*: reindirizza il pacchetto in base alla VLAN.
  - *Filtro*: elimina il pacchetto.
  - *Traffico*: il traffico non in grado di rilevare reti VLAN reindirizza i pacchetti CDP in arrivo a tutte le porte esclusa la porta di ingresso.
- **Annuncio VLAN voce CDP**: selezionare questa opzione per consentire al dispositivo di attivare la dichiarazione della VLAN voce in CDP su tutte le porte idonee CDP che fanno parte della VLAN voce. La VLAN voce viene configurata nella pagina Proprietà VLAN voce.
- **Convalida TLV obbligatoria CDP**: se selezionata, i pacchetti CDP in ingresso che non contengono TLV obbligatori vengono eliminati e il contatore degli errori "non valido" viene incrementato.
- **Versione CDP:** selezionare la versione di CDP da usare.
- **Tempo di attesa CDP**: immettere il tempo per il quale i pacchetti CDP vengono conservati prima di essere eliminati, misurato in multipli dell'intervallo di dichiarazione TLV. Per esempio, se l'Intervallo dichiarazione TLV è di 30 secondi e il Moltiplicatore di sospensione è 4, i pacchetti LLDP vengono eliminati dopo 120 secondi. Sono disponibili le seguenti opzioni:
  - *Usa predefinito*: usa il tempo predefinito (180 secondi).
  - *Definito dall'utente*: inserire il tempo in secondi.
- **Velocità di trasmissione CDP**: immettere la velocità in secondi con cui vengono inviati gli aggiornamenti degli annunci CDP. Sono disponibili le seguenti opzioni:
  - *Usa predefinito*: usare la velocità predefinita (60 secondi).

- *Definito dall'utente*: inserire la velocità in secondi.

- **Formato ID dispositivo**: il formato dell'ID del dispositivo (indirizzo MAC o numero di serie). Sono disponibili le seguenti opzioni:
  - *Indirizzo MAC*: utilizza l'indirizzo MAC del dispositivo come ID dispositivo.
  - *Numero di serie*: utilizza il numero di serie del dispositivo come ID dispositivo.
  - *Nome host*: utilizza il nome host del dispositivo come ID dispositivo.
- **Interfaccia origine** indirizzo IP da utilizzare nel TLV dei frame. Sono disponibili le seguenti opzioni:
  - *Usa predefinito*: usa l'indirizzo IP dell'interfaccia di uscita.
  - *Definito dall'utente*: usa l'indirizzo IP dell'interfaccia (nel campo **Interfaccia**) nell'indirizzo TLV.
- **Interfaccia**: se per *Interfaccia origine* è stata selezionata l'opzione **Definito dall'utente**, selezionare l'interfaccia.
- **Syslog VLAN voce non corrispondente**: selezionare questa opzione per inviare un messaggio SYSLOG quando viene rilevata una mancata corrispondenza VLAN voce. Ciò significa che le informazioni della VLAN voce nel frame in ingresso non hanno corrispondenza con la dichiarazione del dispositivo locale.
- **Syslog VLAN nativa non corrispondente**: selezionare questa opzione per inviare un messaggio SYSLOG quando viene rilevata una mancata corrispondenza VLAN nativa. Ciò significa che le informazioni della VLAN nativa nel frame in ingresso non hanno corrispondenza con la dichiarazione del dispositivo.
- **Syslog Duplex non corrispondente**: selezionare questa opzione per inviare un messaggio SYSLOG quando le informazioni duplex non corrispondono. Ciò significa che le informazioni duplex nel frame in ingresso non hanno corrispondenza con la dichiarazione del dispositivo.

PASSAGGIO 3 Fare clic su **Applica**. Vengono definite le proprietà LLDP.

Modifica delle impostazioni dell'interfaccia CDP

La pagina Impostazioni interfaccia consente agli amministratori di abilitare/disabilitare il protocollo CDP per porta. Le notifiche possono essere attivate anche quando ci sono conflitti con i router adiacenti CDP. Il conflitto può essere VLAN voce dati, VLAN nativa o duplex.

Impostando queste proprietà è possibile selezionare i tipi di informazioni da fornire ai dispositivi che supportano il protocollo LLDP.

I TLV di LLDP-MED da dichiarare possono essere selezionati nella pagina delle impostazioni dell'interfaccia LLDP MED.

Per definire le impostazioni dell'interfaccia CDP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Rilevamento - CDP** > **Impostazioni interfaccia**.

In questa pagina vengono visualizzate le seguenti informazioni CDP per ogni interfaccia.

- **Stato CDP**: opzione di pubblicazione CDP per la porta.
- **Reporting dei conflitti con i router contigui CDP**: visualizza lo stato delle opzioni di reporting che sono attivati/disattivati nella pagina **Modifica** (VLAN voce/VLAN nativo/Duplex).
- **N. di router contigui**: numero di router contigui rilevati.

Nella parte inferiore della pagina sono disponibili quattro pulsanti:

- **Copia impostazioni**: consente di copiare una configurazione da una porta all'altra.
- **Modifica**: campi spiegati al punto 2 sotto.
- **Dettagli informazioni locali CDP**: consente di visualizzare la pagina Amministrazione > Rilevamento - CDP > Informazioni locali CDP.
- **Dettagli informazioni router adiacenti CDP**: consente di visualizzare la pagina Amministrazione > Rilevamento - CDP > Informazioni sui router CDP adiacenti.

PASSAGGIO 2 Selezionare una porta e fare clic su **Modifica**.

In questa pagina vengono forniti i seguenti campi:

- **Interfaccia**: selezionare l'interfaccia da definire.

- **Stato CDP**: selezionare questa opzione per attivare/disattivare l'opzione di pubblicazione CDP per la porta.

  NOTA I successivi tre campi sono disponibili se il dispositivo è stato impostato per l'invio di trap alla stazione di gestione.

- **Syslog VLAN voce non corrispondente**: selezionare questa opzione per inviare un messaggio SYSLOG quando viene rilevata una mancata corrispondenza VLAN voce. Ciò significa che le informazioni VLAN voce nel frame in ingresso non corrispondono alla dichiarazione del dispositivo locale.
- **Syslog VLAN nativa non corrispondente**: selezionare questa opzione per inviare un messaggio SYSLOG quando viene rilevata una mancata corrispondenza VLAN nativa. Ciò significa che le informazioni della VLAN nativa nel frame in ingresso non hanno corrispondenza con la dichiarazione del dispositivo.
- **Syslog Duplex non corrispondente**: selezionare questa opzione per inviare un messaggio SYSLOG quando viene rilevata una mancata corrispondenza duplex. Ciò significa che le informazioni duplex nel frame in ingresso non hanno corrispondenza con la dichiarazione del dispositivo.

PASSAGGIO 3 Immettere le informazioni richieste e fare clic su **Applica**. Le impostazioni della porta vengono definite nel file Configurazione di esecuzione.

Visualizzazione delle informazioni locali CDP

Per informazioni sul dispositivo locale dichiarate dal protocollo CDP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Rilevamento - CDP** > **Informazioni locali CPD**.

PASSAGGIO 2 Selezionare una porta locale per visualizzare i seguenti campi:

- **Interfaccia**: numero della porta locale.
- **Stato CDP**: visualizza se CDP è abilitato o meno.
- **Dispositivo ID TLV**
  - **Tipo dispositivo ID**: tipo di ID del dispositivo dichiarato nel TLV dell'ID dispositivo.
  - **ID dispositivo**: ID del dispositivo dichiarato nel TLV dell'ID dispositivo.

- Nome del sistema TLV
  - **Nome sistema**: nome del sistema del dispositivo.
- Indirizzo TLV
  - **Indirizzi 1-3**: gli indirizzi IP (dichiarati nel TLV dell'indirizzo del dispositivo).
- TLV Porta
  - **ID porta**: identificativo della porta dichiarata nel TLV della porta.
- TLV funzionalità
  - **Funzionalità**: funzionalità dichiarate nel TLV della porta.
- TLV versione
  - **Versione**: informazioni sulla versione del software su cui viene eseguito il dispositivo.
- TLV piattaforma
  - **Piattaforma**: identificativo della piattaforma dichiarata nel TLV della piattaforma.
- VLAN TLV nativa
  - **VLAN nativa**: l'identificatore della VLAN nativa dichiarato nel TLV della VLAN nativa.
- TLV Full/Half Duplex
  - **Duplex**: se la porta dichiarata nel TLV full/half duplex è half o full duplex.
- TLV Applicazione
  - **ID applicazione**: tipo di dispositivo collegato alla porta dichiarata nel TLV dell'applicazione.
  - **ID VLAN applicazione**: VLAN sul dispositivo utilizzato dall'applicazione, per esempio se l'apparecchio è un telefono IP, si tratta della VLAN voce.

- TLV Trust esteso
  - **Trust esteso**: se si seleziona questa opzione la porta è attendibile; questo significa che l'host/il server dal quale viene ricevuto il pacchetto è attendibile per contrassegnare i pacchetti. In questo caso, i pacchetti ricevuti su una porta non sono nuovamente contrassegnati. Se questa opzione è deselezionata significa che la porta non è attendibile; in questo caso, il campo seguente è rilevante.
- CoS per porte non attendibili TLV
  - **CoS per porte non attendibili**: se per la porta è stata selezionata l'opzione Trust esteso, questo campo mostra il valore Livello 2 CoS; questo significa che 802.1D/802.1p ha valore prioritario. Questo è il valore COS con cui tutti i pacchetti ricevuti su una porta non attendibile vengono nuovamente contrassegnati dal dispositivo.
- Power TLV
  - **ID richiesta**: l'ultimo ID richiesta alimentazione ricevuto esegue l'eco del campo ID richiesta ricevuto per ultimo in un TLV richiesta alimentazione. È pari a 0 se non è stato ricevuto un TLV richiesta alimentazione dall'ultima transizione dell'interfaccia a Su.
  - **ID gestione alimentazione**: valore incrementato di 1 (o 2, per evitare 0) ogni volta che si verifica uno qualsiasi dei seguenti eventi:

    I campi Potenza disponibile o Livello gestione alimentazione cambiano valore

    Viene ricevuto un TLV richiesta alimentazione con campo ID richiesta diverso dall'ultima serie ricevuta (o quando il primo valore è stato ricevuto)

    Transizione dell'interfaccia su Giù
  - **Potenza disponibile**: quantità di energia consumata dalla porta.
  - **Livello gestione alimentazione**: visualizza la richiesta del fornitore al dispositivo alimentato per il TLV di assorbimento. In questo campo il dispositivo visualizza sempre "Nessuna preferenza".

Visualizzazione delle informazioni dei router adiacenti CDP

Nella pagina Dettagli informazioni router CDP adiacenti vengono visualizzate le informazioni CPD ricevute da dispositivi adiacenti.

Dopo il timeout (basato sul valore acquisito dal TLV Durata del router adiacente nel quale non è stata ricevuta alcuna PDU LLDP da un router adiacente), le informazioni vengono eliminate.

Per visualizzare le informazioni dei router adiacenti CDP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Rilevamento - CDP** > **Informazioni router contiguiCPD**.

In questa pagina vengono visualizzati i seguenti campi per ogni partner di collegamento (router adiacente):

- **ID dispositivo**: identificativo del dispositivo del router adiacente.
- **Nome del sistema**: nome del sistema del router adiacente.
- **Interfaccia locale**: numero della porta locale a cui è connesso il router adiacente.
- **Versione annuncio**: versione del protocollo CDP.
- **Durata (sec)**: intervallo di tempo (in secondi) dopo il quale le informazioni del router adiacente vengono eliminate.
- **Funzionalità**: funzionalità dichiarate dal router adiacente.
- **Piattaforma**: informazioni del TLV della piattaforma del router adiacente.
- **Interfaccia router adiacente**: interfaccia di uscita del router adiacente.

PASSAGGIO 2 Selezionare un dispositivo e fare clic su **Dettagli**.

In questa pagina vengono visualizzati i seguenti campi relativi al router adiacente:

- **ID dispositivo**: identificativo dell'ID dispositivo del router adiacente.
- **Nome sistema**: nome dell'ID dispositivo del router adiacente.
- **Interfaccia locale**: numero di interfaccia della porta da cui è arrivato il frame.
- **Versione annuncio**: versione del protocollo CDP.
- **Durata**: intervallo di tempo (in secondi) dopo il quale le informazioni di questo router adiacente vengono eliminate.

- **Funzionalità**: funzioni principali del dispositivo. Le funzionalità sono indicate da due ottetti. I bit da 0 a 7 indicano rispettivamente Altro, Repeater, Bridge, access point WLAN, Router, Telefono, Dispositivo cavo DOCSIS e stazione. I bit da 8 a 15 sono riservati.
- **Piattaforma**: identificatore della piattaforma del router adiacente.
- **Interfaccia router adiacente**: numero di interfaccia del router adiacente da cui è arrivato il frame.
- **VLAN nativa**: VLAN nativa del router adiacente.
- **Duplex**: se l'interfaccia è half-duplex o full-duplex.
- **Indirizzi**: indirizzi dei router adiacenti.
- **Energia assorbita**: quantità di energia assorbita dal router adiacente sull'interfaccia.
- **Versione**: versione software del router adiacente.

NOTA Se si fa clic sul pulsante **Cancella tabella** tutti i dispositivi connessi vengono scollegati dal protocollo CDP e, se l'opzione SmartPort automatico è attivata, tutti i tipi di porta vengono impostati su predefinito.

Visualizzazione delle statistiche CDP

Nella pagina Statistiche CDP vengono visualizzate le informazioni relative ai frame del protocollo CDP (Cisco Discovery Protocol) inviati o ricevuti da una porta. I pacchetti CDP vengono ricevuti da dispositivi collegati alle interfacce switch e sono utilizzati per la funzione SmartPort. Vedere la sezione **Configurazione CDP** per ulteriori informazioni.

Le statistiche CDP per una porta vengono visualizzate solo se CDP è attivato a livello globale e nella porta. A tal fine utilizzare la pagina Proprietà di CDP e la pagina Impostazioni interfaccia CDP.

Per visualizzare le statistiche CDP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione > Rilevamento - CDP > Statistiche CDP**.

Per ogni interfaccia vengono visualizzati i campi seguenti:

Pacchetti ricevuti/trasmessi:

- **Versione 1**: numero di pacchetti CDP versione 1 ricevuti/trasmessi.

- **Versione 2**: numero di pacchetti CDP versione 2 ricevuti/trasmessi.
- **Totale**: numero complessivo di pacchetti CDP ricevuti/trasmessi.

Nella sezione Statistiche errore CDP vengono indicati i contatori degli errori CDP.

- **Checksum non valido**: numero di pacchetti ricevuti con valore di checksum non valido.
- **Altri errori**: numero di pacchetti ricevuti con errori diversi da checksum non valido.
- **Router adiacenti superano il massimo**: numero di volte che le informazioni del pacchetto non possono essere memorizzate nella cache per mancanza di spazio.

Per azzerare i contatori per tutte le interfacce, fare clic su **Azzera tutti i contatori interfaccia**. Per azzerare i contatori per tutte le interfacce, fare clic su **Azzera tutti i contatori interfaccia**.

10

Gestione porte

In questa sezione vengono illustrate la configurazione delle porte, l'aggregazione collegamenti e la funzione Ethernet verde.

Vengono trattati i seguenti argomenti:

- **Configurazione delle porte**
- **Definire la configurazione delle porte**
- **Aggregazione collegamenti**
- **UDLD**
- **Configurazione di Ethernet verde**

Configurazione delle porte

Per configurare le porte, effettuare le seguenti operazioni:

1. Configurare la porta nella pagina Impostazioni porta.
2. Attivare/disattivare il protocollo LAG (Link Aggregation Control) e configurare le possibili porte membro sui LAG desiderati nella pagina Gestione LAG. Per impostazione predefinita, tutti i LAG sono vuoti.
3. Configurare i parametri Ethernet, ad esempio la velocità e la negoziazione automatica per i LAG, nella pagina Impostazioni LAG.
4. Configurare i parametri LACP per le porte che sono membri o candidate di un LAG dinamico nella pagina LACP.
5. Configurare Ethernet verde ed Energy Efficient Ethernet 802.3 nella pagina Proprietà.
6. Configurare la modalità energetica Ethernet verde ed Energy Efficient Ethernet 802.3 per porta tramite la pagina Impostazioni porta.

7. Se la funzione PoE è supportata ed è attiva sul dispositivo, configurare il dispositivo come riportato nella sezione **Gestione delle porte: PoE**.

Definire la configurazione delle porte

È possibile configurare le porte nelle seguenti pagine.

Impostazioni della porta

Nella pagina Impostazioni porta vengono visualizzate le impostazioni generali e per porta relative a tutte le porte. In questa pagina è possibile selezionare le porte desiderate e configurarle nella pagina di modifica delle impostazioni della porta.

Per configurare le impostazioni della porta, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione porte** > **Impostazioni porta**.

PASSAGGIO 2 Selezionare **Frame jumbo** per supportare pacchetti di dimensioni fino a 10 Kb. Se l'opzione **Frame jumbo** non è selezionata (impostazione predefinita), il sistema supporta pacchetti con dimensioni massime di 2.000 byte. Per utilizzare i frame jumbo, è necessario attivare la relativa funzione e riavviare il dispositivo.

PASSAGGIO 3 Scegliere **Applica** per aggiornare l'impostazione generale.

Le modifiche alla configurazione dei frame jumbo vengono applicate *solo* dopo aver salvato esplicitamente la Configurazione di esecuzione nel file di configurazione avvio nella pagina Copia/Salva configurazione e dopo aver riavviato il dispositivo.

PASSAGGIO 4 Per aggiornare le impostazioni delle porte, selezionare la porta desiderata e fare clic su **Modifica**.

PASSAGGIO 5 Modificare i seguenti parametri:

- **Porta**: selezionare il numero della porta.
- **Descrizione della porta**: immettere il nome della porta o i commenti definiti dall'utente.
- **Tipo di porta**: indica il tipo di porta e la velocità. Le opzioni possibili sono:
  - *Porte in rame*: quelle regolari, non combo, supportano i valori seguenti: 10M, 100M e 1000M (tipo: rame).

- *Porte in rame combinate*: le porte Combo collegate tramite il cavo CAT5 in rame supportano i valori seguenti: 10M, 100M e 1000M (tipo: ComboC)
- *Fibra combinata*: *la Porta di conversione dell'interfaccia Gigabit con Fibra SFP* supporta i seguenti valori: 100M e 1000M (tipo: ComboF).
- Porte in fibra ottica 10 G: porte con velocità 1G o 10G.

NOTA Quando si utilizzano entrambe le porte, Fibra SFP avrà la precedenza nelle porte combo.

- **Stato amministrativo**: selezionare se, dopo il riavvio del dispositivo, la porta deve essere attiva o inattiva.
- **Stato operativo**: in questo campo viene mostrato se la porta è attualmente attiva o inattiva. Se la porta è inattiva a causa di un errore, viene visualizzata la descrizione dell'errore.
- **Stato del collegamento Trap SNMP**: selezionare questa opzione per consentire la generazione di Trap SNMP che avvertono dei cambiamenti allo stato del collegamento della porta.
- **Intervallo di tempo**: selezionare questa opzione per attivare l'intervallo di tempo durante il quale la porta è attiva. Quando l'intervallo di tempo non è attivo, la porta viene bloccata. Un intervallo di tempo configurato diventa effettivo solo quando la porta viene attivata dall'amministratore. Se l'intervallo di tempo non è stato ancora definito, fare clic su **Modifica** per accedere alla pagina Intervallo di tempo.
- **Nome intervallo di tempo**: selezionare il profilo che specifica l'intervallo di tempo.
- **Stato intervallo di tempo operativo**: indica se l'intervallo di tempo è attualmente attivo o inattivo.
- **Riattiva porta sospesa**: consente di riattivare una porta precedentemente sospesa. Una porta può essere sospesa in vari modi, ad esempio tramite la funzione di sicurezza basata sul blocco della porta, la violazione host singolo dot1x, il rilevamento di loopback, la protezione loopback STP o le configurazioni dell'Access Control List (ACL). L'operazione di riattivazione attiva la porta senza considerare i motivi per i quali la porta era stata sospesa.

- **Negoziazione automatica**: selezionare questa funzione per attivare la negoziazione automatica sulla porta. La negoziazione automatica consente a una porta di dichiarare la propria velocità di trasmissione, la modalità duplex e le capacità di controllo del flusso ai partner di collegamento della porta.
- **Negoziazione automatica operativa**: indica lo stato corrente della negoziazione automatica della porta.
- **Velocità porta amministrativa**: configurare la velocità della porta. Il tipo di porta determina le velocità disponibili. È possibile specificare la *Velocità amministrativa* solo quando la negoziazione automatica della porta è disattivata.
- **Velocità porta operativa**: indica la velocità attuale della porta ottenuta dalla negoziazione.
- **Modalità Duplex amministrativa**: selezionare la modalità duplex sulla porta. Questo campo può essere configurato solo quando la negoziazione automatica è disattivata e la velocità della porta è impostata su 10M o 100M. Alla velocità porta di 1G, la modalità è sempre full duplex. Le opzioni possibili sono:
  - *Completo*: l'interfaccia supporta la trasmissione tra il dispositivo e il client contemporaneamente in entrambe le direzioni.
  - *Half*: l'interfaccia supporta la trasmissione tra il dispositivo e il client in una sola direzione alla volta.
- **Modalità Duplex operativa**: visualizza la modalità duplex corrente della porta.
- **Annuncio automatico**: selezionare le funzionalità dichiarate tramite negoziazione automatica quando questa è attivata. Sono disponibili le seguenti opzioni:
  - *Capacità massima*: vengono accettate tutte le velocità e le impostazioni della modalità duplex della porta.
  - *10 Half*: velocità a 10 Mbps in modalità half-duplex.
  - *10 Full*: velocità a 10 Mbps in modalità full-duplex.
  - *100 Half*: velocità a 100 Mbps in modalità half-duplex.
  - *100 Full*: velocità a 100 Mbps in modalità full-duplex.
  - *1000 Full*: velocità a 1000 Mbps in modalità full-duplex.

- **Annuncio operativo**: indica le funzionalità attualmente dichiarate ai dispositivi adiacenti. Le opzioni possibili sono riportate nel campo *Annuncio amministrativo*.
- **Annuncio router adiacente**: visualizza le funzionalità dichiarate dal dispositivo adiacente (partner di collegamento).
- **Congestione**: selezionare la modalità di congestione sulla porta (utilizzata con la modalità half-duplex) per ridurre la velocità di ricezione dei pacchetti quando il dispositivo è congestionato. Questo consente di disattivare la porta remota, impedendo l'invio di pacchetti congestionando il segnale.
- **Controllo del flusso**: attivare o disattivare il Controllo del flusso 802.3x, oppure attivare la negoziazione automatica del controllo del flusso della porta (solo in modalità full-duplex).
- **MDI/MDIX**: lo stato della *Media Dependent Interface* (MDI)/*Media Dependent Interface crossover* (MDIX) sulla porta.

  Sono disponibili le seguenti opzioni:

  - *MDIX*: selezionare l'opzione per scambiare le coppie di trasmissione e ricezione della porta.
  - *MDI*: selezionare MDI per collegare il dispositivo a una stazione tramite un cavo dritto.
  - *Automatico*: consente al dispositivo di rilevare automaticamente i pinout corretti per collegarsi a un altro dispositivo.
- **MDI/MDIX operativi**: indica l'impostazione attuale della MDI/MDIX.
- **Porta protetta**: consente di impostare la porta come porta protetta, nota anche come PVE (Private VLAN Edge). Le caratteristiche di una porta protetta sono le seguenti:

  - Le porte protette forniscono un isolamento tra le interfacce di Livello 2 (porte Ethernet e LAG) che condividono la stessa VLAN.
  - I pacchetti ricevuti da porte protette possono essere reindirizzati solo su porte di uscita non protette. Ai pacchetti reindirizzati dal software, come le applicazioni snooping, vengono applicate le regole del filtro porta protetta.
  - La protezione della porta non è soggetta all'appartenenza VLAN. I dispositivi collegati alle porte protette non possono comunicare con gli altri, anche se appartengono alla stessa VLAN.

- Sia le porte che i LAG possono essere definiti come protetti o non protetti. I LAG sono descritti nella sezione **Configurazione delle impostazioni LAG**.

- **Membro in LAG**: se la porta è membro di un LAG, viene visualizzato il numero del LAG; in caso contrario il campo è vuoto.

PASSAGGIO 6 Fare clic su **Applica**. Le impostazioni della porta vengono scritte nel file di configurazione esecuzione.

Impostazioni ripristino errore

Questa pagina consente di riattivare automaticamente una porta che è stata bloccata a causa di una condizione di errore.

Per configurare le impostazioni ripristino errore, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione porte** > **Impostazioni ripristino errore**.

PASSAGGIO 2 Immettere informazioni nei seguenti campi:

- **Intervallo ripristino automatico**: selezionare questa opzione per attivare il meccanismo di ripristino errore per lo stato disattivato dell'errore della sicurezza della porta.
- **Sicurezza porta**: selezionare questa opzione per attivare il meccanismo di ripristino errore per lo stato disattivato dell'errore della sicurezza della porta.
- **Violazione host singolo 802.1x**: selezionare questa opzione per attivare il meccanismo di ripristino errore per lo stato disattivato dell'errore di 802.1x.
- **Negazione ACL**: selezionare questa opzione per attivare il meccanismo di ripristino errore per lo stato disattivato dell'errore della negazione ACL.
- **Guardia BPDU STP**: selezionare questa opzione per attivare il meccanismo di ripristino errore per lo stato disattivato dell'errore della guardia BPDU STP.
- **UDLD**: selezionare questa opzione per attivare il meccanismo di ripristino errore per lo stato di arresto di UDLD.

PASSAGGIO 3 Scegliere **Applica** per aggiornare l'impostazione generale.

Per riattivare manualmente una porta, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione porte** > **Impostazioni ripristino errore**.

Viene visualizzato l'elenco delle interfacce inattive e il relativo **motivo di sospensione**.

PASSAGGIO 2 Selezionare l'interfaccia da riattivare.

PASSAGGIO 3 Fare clic su **Riattiva**.

Aggregazione collegamenti

In questa sezione viene descritto come configurare i LAG. Vengono trattati i seguenti argomenti:

- **Panoramica dell'aggregazione dei collegamenti**
- **Flusso di lavoro del LAG statico e dinamico**
- **Definizione della Gestione LAG**
- **Configurazione delle impostazioni LAG**
- **Configurazione del LACP**

Panoramica dell'aggregazione dei collegamenti

Il LACP (Link Aggregation Control Protocol) appartiene a una specifica IEEE (802.3az) che consente di raggruppare diverse porte fisiche formando un unico canale logico (LAG). I LAG consentono di aumentare la larghezza di banda e la flessibilità della porta e forniscono collegamenti ridondanti tra due dispositivi.

Sono utilizzati due tipi di LAG:

- *Statico*: un LAG è statico se LACP è disattivato su di esso. Il gruppo di porte assegnate ad un LAG statico sono sempre membri attivi. Dopo la creazione manuale di un LAG, l'opzione LACP non può essere aggiunta o rimossa fino a quando il LAG non viene modificato e un membro non viene rimosso (può essere aggiunto prima dell'applicazione), solo allora il pulsante LACP sarà disponibile per le modifiche.

- *Dinamico*: un LAG è dinamico se il LACP su di esso è attivato. Il gruppo di porte assegnate a un LAG dinamico è un gruppo di porte candidate. Il LACP determina quali porte candidate sono porte membro attive. Le porte candidate non attive sono porte in *standby* pronte per sostituire qualsiasi porta membro attiva mancante.

Bilanciamento del carico

Il carico del traffico reindirizzato a un LAG è bilanciato su tutte le porte membro attive, pertanto si ottiene un'effettiva larghezza di banda simile a quella di tutte le porte membro attive aggregate su un LAG.

Il bilanciamento del carico del traffico su porte membro attive di un LAG viene gestito da una funzione di distribuzione basata su hash che consente di distribuire traffico unicast e multicast sulla base delle informazioni relative all'intestazione di un pacchetto di livello 2 o di livello 3.

Il dispositivo supporta due modalità di bilanciamento del carico:

- **Tramite indirizzi MAC**: basato sugli indirizzi MAC di origine e di destinazione di tutti i pacchetti.
- **Tramite indirizzi IP e MAC**: secondo gli indirizzi IP di origine e di destinazione dei pacchetti IP e gli indirizzi MAC di origine e di destinazione dei pacchetti non IP.

Gestione LAG

Generalmente, il sistema tratta un LAG come una singola porta logica. Nello specifico, gli attributi delle porte di un LAG, quali stato e velocità, sono simili a quelli di una porta regolare.

Il dispositivo supporta 32 LAG con un massimo di 8 porte per gruppo LAG.

ciascuno dei quali presenta le caratteristiche seguenti:

- Tutte le porte di un LAG devono avere lo stesso tipo di supporto.
- Per aggiungere una porta al LAG, questo non può appartenere a nessuna VLAN se non a quella predefinita.
- Le porte di un LAG devono essere assegnate a un altro LAG.
- Su un LAG statico è possibile assegnare non più di otto porte e per un LAG dinamico è possibile sceglierne massimo 16.
- Su tutte le *porte* di un LAG la negoziazione automatica deve essere disattivata, sebbene sul *LAG* sia possibile attivarla.

- Quando una porta viene aggiunta a un LAG, la configurazione del LAG viene applicata alla porta. Quando la porta viene rimossa dal LAG, viene nuovamente applicata la configurazione originaria.
- I protocolli, quali lo Spanning Tree, trattano tutte le porte di un LAG come un'unica porta.

Impostazioni predefinite e configurazione

Le porte non fanno parte di un LAG e non sono candidate a diventarlo.

Flusso di lavoro del LAG statico e dinamico

Dopo la creazione manuale di un LAG, LACP non può essere aggiunto o rimosso fino a quando il LAG non viene modificato e un membro non viene rimosso. Solo allora il pulsante LACP sarà disponibile per le modifiche.

Per configurare un LAG **statico**, eseguire le seguenti operazioni:

1. Disattivare LACP sul LAG per renderlo statico. Assegnare al LAG statico un massimo di otto porte membro selezionando e spostando le porte dall'**Elenco delle porte** all'elenco **Membri LAG**. Selezionare l'algoritmo di bilanciamento del carico per il LAG. Eseguire queste azioni nella pagina Gestione LAG.
2. Configurare i vari aspetti del LAG, ad esempio la velocità e il controllo del flusso, nella pagina Impostazioni LAG.

Per configurare un LAG **dinamico**, eseguire le seguenti operazioni:

1. Abilitare LACP sul LAG. Nella pagina Gestione LAG, selezionare le porte candidate (massimo 16) da assegnare al LAG dinamico nell'**Elenco delle porte** e spostarle nell'elenco **Membri LAG**.
2. Configurare i vari aspetti del LAG, ad esempio la velocità e il controllo del flusso, nella pagina Impostazioni LAG.
3. Impostare la priorità LACP e il timeout delle porte del LAG nella pagina LACP.

Definizione della Gestione LAG

Nella pagina Gestione LAG vengono visualizzate sia le impostazioni generali che quelle dei LAG. Inoltre, la pagina consente di configurare le impostazioni generali e selezionare il LAG desiderato per modificarlo nella pagina Modifica appartenenza a LAG.

Per selezionare l'algoritmo di bilanciamento del carico per il LAG, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione porte** > **Aggregazione collegamenti** > **Gestione LAG.**

PASSAGGIO 2 Selezionare uno dei seguenti **Algoritmi di bilanciamento del carico**:

- *Indirizzo MAC*: eseguire il bilanciamento del carico tramite gli indirizzi MAC di origine e di destinazione su tutti i pacchetti.
- *Indirizzo IP/MAC*: eseguire il bilanciamento del carico tramite gli indirizzi IP di origine e destinazione sui pacchetti IP e gli indirizzi MAC di origine e di destinazione sui pacchetti non IP.

PASSAGGIO 3 Fare clic su **Applica**. L'algoritmo di bilanciamento del carico viene salvato nel file di configurazione esecuzione.

Per definire le porte membro o candidato in un LAG, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare il LAG da configurare e fare clic su **Modifica.**

PASSAGGIO 2 Immettere i valori dei seguenti campi:

- **LAG**: selezionare il numero del LAG.
- **Nome LAG**: immettere il nome LAG o un commento.
- **LACP**: selezionare LACP per attivarlo sul LAG selezionato. Questo consente di creare un LAG dinamico. Questo campo può essere attivato solo dopo lo spostamento di una porta al LAG nel campo successivo.
- **Unità/Slot**: indica il membro dello stack per cui vengono definite le informazioni LAG.
- **Elenco delle porte**: spostare le porte da assegnare al LAG dall'**Elenco delle porte** all'elenco **Membri LAG**. È possibile assegnare un massimo di otto porte per LAG statico e 16 su un LAG dinamico.

PASSAGGIO 3 Fare clic su **Applica**. L'appartenenza al LAG viene salvata nel file di configurazione esecuzione.

Configurazione delle impostazioni LAG

Nella pagina Impostazioni LAG viene visualizzata una tabella in cui sono riportate le impostazioni attuali di tutti i LAG. È possibile configurare le impostazioni dei LAG selezionati e riattivare quelli sospesi nella pagina Modifica impostazioni LAG.

Per configurare le impostazioni LAG o riattivare un LAG sospeso, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione porte** > **Aggregazione collegamenti** > **Impostazioni LAG**.

PASSAGGIO 2 Selezionare un LAG e fare clic su **Modifica**.

PASSAGGIO 3 Immettere i valori dei seguenti campi:

- **LAG**: selezionare il numero ID del LAG.
- **Descrizione**: immettere il nome LAG o un commento.
- **Tipo di LAG**: indica il tipo di porta che in cui è incluso il LAG.
- **Stato amministrativo**: impostare il LAG selezionato su Su o Giù.
- **Stato operativo**: indica se il LAG è al momento operativo.
- **Stato del collegamento Trap SNMP**: selezionare questa opzione per consentire la generazione di Trap SNMP che avvertono dei cambiamenti allo stato del collegamento delle porte nel LAG.
- **Intervallo di tempo**: selezionare questa opzione per attivare l'intervallo di tempo durante il quale la porta è attiva. Quando l'intervallo di tempo non è attivo, la porta viene bloccata. Un intervallo di tempo configurato diventa effettivo solo quando la porta viene attivata dall'amministratore. Se l'intervallo di tempo non è stato ancora definito, fare clic su **Modifica** per accedere alla pagina Intervallo di tempo.
- **Nome intervallo di tempo**: selezionare il profilo che specifica l'intervallo di tempo.
- **Stato intervallo di tempo operativo**: indica se l'intervallo di tempo è attualmente attivo o inattivo.

- **Riattiva LAG sospeso**: consente di riattivare una porta se il LAG è stato disattivato tramite la funzione di protezione basata sul blocco della porta o tramite le configurazioni ACL.
- **Negoziazione automatica amministrativa**: consente di attivare o disattivare la negoziazione automatica sul LAG. La negoziazione automatica è un protocollo utilizzato da due parti di un collegamento che consente a un LAG di dichiarare la propria velocità di trasmissione e il controllo del flusso (per impostazione predefinita il Controllo del flusso è *disattivato*). Si consiglia di tenere la negoziazione automatica attivata su entrambe le parti di un collegamento aggregato, oppure disattivata se le velocità dei collegamenti sono identiche.
- **Negoziazione automatica operativa**: indica l'impostazione della negoziazione automatica.
- **Velocità amministrativa**: selezionare la velocità del LAG.
- **Velocità LAG operativa**: indica la velocità attuale dell'operatività del LAG.
- **Annuncio amministrativo**: selezionare la velocità di trasmissione raggiungibile dichiarata dal LAG. Sono disponibili le seguenti opzioni:
  - *Capacità massima*: sono disponibili le velocità e le modalità duplex di tutti i LAG.
  - *10 Full*: il LAG dichiara una velocità a 10 Mbps in modalità full-duplex.
  - *100 Full*: il LAG dichiara una velocità a 100 Mbps in modalità full-duplex.
  - *1000 Full*: il LAG dichiara una velocità a 1000 Mbps in modalità full-duplex.
- **Annuncio operativo**: indica lo stato dell'Annuncio operativo. Per avviare il processo di negoziazione un LAG dichiara le proprie capacità al LAG adiacente. I valori possibili sono riportati nel campo *Annuncio amministrativo*.
- **Controllo del flusso amministrativo**: consente di impostare il controllo del flusso su **Attivo** o **Inattivo** oppure di attivare la **negoziazione automatica** del controllo del flusso del LAG.
- **Controllo del flusso operativo**: indica l'impostazione attuale del Controllo del flusso.

- **LAG protetto**: consente di impostare il LAG come porta protetta per l'isolamento di livello 2. Vedere la descrizione relativa alla configurazione delle porte nella sezione **Impostazione della configurazione base della porta** per i dettagli relativi alle porte e ai LAG protetti.

PASSAGGIO 4 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Configurazione del LACP

Un LAG dinamico è abilitato al LACP e LACP viene eseguito su ogni porta candidata definita nel LAG.

Priorità e regole sul LACP

La priorità sul sistema e quella sulla porta LACP sono entrambe utilizzate per determinare quale delle porte candidate diventerà porta membro attiva in un LAG dinamico configurato con più di otto porte candidate.

Le porte candidate selezionate del LAG sono tutte collegate allo stesso dispositivo remoto. Entrambi gli switch locale e remoto hanno una priorità di sistema LACP.

Il seguente algoritmo viene utilizzato per determinare se le priorità porta LACP sono tratte dal dispositivo locale o remoto: la priorità di sistema LACP viene confrontata con la priorità di sistema LACP remota. Il dispositivo con la priorità più bassa controlla la selezione delle porte candidate al LAG. Se le priorità sono identiche, vengono confrontati gli indirizzi MAC locali e remoti e la priorità del dispositivo con l'indirizzo MAC più basso controlla la selezione delle porte candidate al LAG.

Un LAG dinamico può avere fino a 16 porte Ethernet dello stesso tipo. Possono essere attive o in modalità di standby massimo otto porte. Se nel LAG dinamico sono presenti più di otto porte, il dispositivo all'estremità di controllo del collegamento utilizza le priorità della porta per determinare le porte che vengono raggruppate nel LAG e quelle che vengono inserite nella modalità standby. Le priorità delle porte sull'altro dispositivo, ovvero l'estremità non di controllo del collegamento, vengono ignorate.

Le seguenti sono regole aggiuntive per la selezione di porte attive o in standby in un LACP dinamico:

- Qualsiasi collegamento che opera ad una velocità diversa rispetto al membro attivo con la massima velocità o che opera in modalità half-duplex viene resa standby. Tutte le porte attive di un LAG dinamico operano alla stessa velocità di trasmissione.
- Se la priorità del collegamento della porta LACP è inferiore rispetto a quella delle porte membro del collegamento correntemente attive e che presentano il numero massimo, il collegamento viene reso inattivo e posto in modalità standby.

LACP senza partner di collegamento

Affinché un LACP crei un LAG, le porte su entrambe le estremità del collegamento devono essere configurate per LACP; questo significa che le porte inviano PDU LACP e gestiscono le PDU ricevute.

Tuttavia, in alcuni casi un partner di collegamento non è temporaneamente configurato per LACP. Questo accade, ad esempio, quando il partner di collegamento è su un dispositivo che sta ricevendo la sua configurazione tramite il protocollo di configurazione automatica. Le porte del dispositivo non sono ancora configurate per LACP. Se non è possibile attivare il collegamento LAG, non è possibile configurare il dispositivo. Un caso simile si verifica su computer con due schede di rete NIC, ad esempio PXE, che ricevono la loro configurazione LAG soltanto dopo l'avvio.

Se sono presenti più porte configurate con LACP e il collegamento viene attivato in una o più porte, ma non vengono ricevute risposte LACP dal partner di collegamento per tali porte, la prima porta con il collegamento attivo viene aggiunta al LAG LACP e diventa attiva, mentre le altre porte diventano non candidate. In questo modo, il dispositivo adiacente può ottenere, ad esempio, il suo indirizzo IP utilizzando DHCP e ottenere la sua configurazione tramite la configurazione automatica.

Impostazioni dei parametri LACP

Utilizzare la pagina LACP per configurare le porte candidate per il LAG e per configurare i parametri LACP per porta.

Se tutti i fattori sono impostati in modo identico, quando il LAG è configurato con più porte candidate rispetto al numero massimo di porte attive consentite (8), verranno selezionate come attive le porte del LAG dinamico sul dispositivo con la priorità più alta.

NOTA L'impostazione LACP non è fondamentale sulle porte non appartenenti a un LAG dinamico.

Per definire le impostazioni LACP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione porte** > **Aggregazione collegamenti** > **LACP**.

PASSAGGIO 2 Immettere la priorità di sistema LACP. Vedere **Priorità e regole sul LACP**.

PASSAGGIO 3 Selezionare una porta e fare clic su **Modifica.**

PASSAGGIO 4 Immettere i valori dei seguenti campi:

- **Porta**: selezionare il numero della porta a cui sono assegnati i valori di timeout e priorità.
- **Priorità porta LACP**: immettere il valore della priorità LACP della porta. Vedere **Impostazioni dei parametri LACP**.
- **Timeout LACP**: intervallo di tempo tra l'invio e la ricezione di PDU LACP consecutive. Sselezionare le PDU LACP trasmesse periodicamente a una velocità di trasmissione **lunga** o **breve**, in base alle preferenze di timeout LACP indicate.

PASSAGGIO 5 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

UDLD

Vedere **Gestione delle porte: rilevamento del collegamento unidirezionale**.

PoE

Vedere **Gestione delle porte: PoE**.

Configurazione di Ethernet verde

In questa sezione viene illustrata la funzione Ethernet verde, realizzata per risparmiare energia sul dispositivo.

Vengono trattate le seguenti sezioni:

- **Panoramica di Ethernet verde**
- **Impostazione delle proprietà generali di Ethernet verde**
- **Impostazione delle proprietà Ethernet verde per le porte**

Panoramica di Ethernet verde

Ethernet verde è un nome comune che indica una serie di funzioni ideate per creare un ambiente ecologico e per ridurre l'assorbimento di un dispositivo. Ciò che differenzia Ethernet verde da EEE è che il rilevamento energia su Ethernet verde è attivato su tutti i dispositivi e non solo sulle porte Gigabyte come nel caso di EEE.

La funzione Ethernet verde consente di ridurre l'utilizzo energetico complessivo nei modi seguenti:

- **Modalità di rilevamento energia**: (non disponibile su SG500XG) su un collegamento inattivo, la porta passa in modalità inattiva risparmiando energia e mantenendo contemporaneamente attivo lo stato amministrativo della porta. Il passaggio da questa modalità a quella completamente operativa avviene in modo rapido e trasparente senza comportare la perdita di frame. Questa modalità viene supportata sia su porte GE che su porte FE.
- **Raggiungimento breve**: questa funzione garantisce risparmi energetici su un breve tratto di cavo. Dopo avere analizzato la lunghezza del cavo, l'utilizzo energetico viene regolato per le varie lunghezze dei cavi. Se il cavo è più corto di 50 metri, il dispositivo utilizza meno energia per inviare i frame sul cavo, consentendo così un risparmio energetico. Questa modalità è supportata solo su porte RJ45 GE e non si applica a porte combo.

  Questa modalità è disattivata globalmente per impostazione predefinita. Non può essere attivata se la modalità EEE è attivata (vedi sotto).

In aggiunta alle caratteristiche Ethernet verde di cui sopra, **Energy Efficient Ethernet (EEE) 802.3az** si trova su dispositivi che supportano le porte GE. EEE riduce l'assorbimento di energia quando non c'è traffico sulla porta. Vedere **Funzione Energy Efficient Ethernet 802.3az** per ulteriori informazioni (disponibile solo su modelli GE).

EEE è attivo globalmente per impostazione predefinita. Su una determinata porta, se EEE è attivata, la modalità di raggiungimento breve sarà disattivata. Se la modalità di raggiungimento breve è abilitata, EEE verrà disattivata.

Queste modalità sono configurate per porta, senza tener conto delle appartenenze LAG delle porte.

I LED del dispositivo consumano energia. Dato che la maggior parte delle volte i dispositivi si trovano in stanze inutilizzate, tenere accesi questi LED è uno spreco di energia. La funzione Ethernet verde consente di disattivare i LED della porta (collegamento, velocità e PoE) quando non sono necessari e di attivarli quando necessari (debug, connessione di altri dispositivi...).

Se nella pagina Riepilogo di sistema vengono disattivati i LED, i LED presenti sulle immagini della scheda del dispositivo non vengono disattivati.

È possibile monitorare il risparmio energetico, il consumo energetico corrente e il totale dell'energia risparmiata. È possibile visualizzare la quantità totale di energia risparmiata tramite una percentuale dell'eventuale alimentazione consumata dalle interfacce fisiche non eseguite in modalità Ethernet verde.

L'energia risparmiata visualizzata è solo relativa all'Ethernet verde. La quantità di energia risparmiata da EEE non viene visualizzata.

Risparmio energetico tramite la disattivazione dei LED porta

La funzionalità Disattiva LED porta consente all'utente di disattivare i LED del dispositivo per risparmiare ulteriore energia. Dato che la maggior parte delle volte i dispositivi si trovano in stanze inutilizzate, tenere accesi questi LED è uno spreco di energia. La funzione Ethernet verde consente di disattivare i LED della porta (collegamento, velocità e PoE) quando non sono necessari e di attivarli quando necessari (debug, connessione di altri dispositivi...).

Se nella pagina Riepilogo di sistema vengono disattivati i LED, i LED presenti sulle immagini della scheda del dispositivo non vengono disattivati.

Nella pagina Ethernet verde > Proprietà, il è possibile disattivare i LED delle porte per risparmiare energia.

Funzione Energy Efficient Ethernet 802.3az

In questa sezione viene illustrata la funzione Energy Efficient Ethernet (EEE) 802.3az.

Vengono trattati i seguenti argomenti:

- **Panoramica di EEE 802.3az**
- **Negoziazione delle funzionalità di annuncio**
- **Rilevamento livello collegamento per EEE 802.3az**
- **Disponibilità di EEE 802.3az**
- **Configurazione predefinita**
- **Interazioni tra funzioni**
- **Flusso di lavoro configurazione di EEE 802.3az**

Panoramica di EEE 802.3az

EEE 802.3az è stato creato per risparmiare energia quando non c'è traffico sul collegamento. Con Ethernet verde, la potenza è ridotta quando porta è disattivata. Con EEE 802.3az, la potenza è ridotta quando la porta è attiva, ma su di essa non c'è traffico.

EEE 802.3az è supportato solo su dispositivi con porte GE.

Quando si utilizza EEE 802.3az, i sistemi su entrambi i lati del collegamento possono disabilitare parti della loro funzionalità e risparmiare energia durante i periodi di assenza di traffico.

EEE 802.3az è compatibile con il funzionamento MAC IEEE 802.3 a 100 Mbps e 1000 Mbps.

Per selezionare il set ideale di parametri per entrambi i dispositivi viene utilizzato LLDP. Se LLDP non è supportato dal partner di collegamento o è disattivato, EEE 802.3az sarà ancora operativo, ma potrebbe non essere nella modalità operativa ottimale.

La funzione EEE 802.3az è implementata utilizzando una modalità porta denominata modalità Low Power Idle (LPI). Quando non c'è traffico e questa funzione è attivata sulla porta, tale porta è posta in modalità LPI, che riduce drasticamente il consumo di energia.

Per poter utilizzare questa funzione è necessario che entrambi i lati di una connessione (porta del dispositivo e dispositivo di collegamento) la supportino. Quando il traffico è assente, entrambe le parti inviano segnali che indicano che la potenza sta per essere ridotta. Quando vengono ricevuti segnali da entrambi i lati, il segnale Mantieni connessione attiva indica che le porte sono in stato LPI (e non in stato Giù) e l'alimentazione viene ridotta.

Per consentire alle porte di rimanere in modalità LPI, il segnale Mantieni connessione attiva deve pervenire continuamente da entrambi i lati.

Negoziazione delle funzionalità di annuncio

Il supporto per EEE 802.3az viene dichiarato durante la fase di negoziazione automatica. La negoziazione automatica fornisce un dispositivo collegato con la capacità di rilevare le funzionalità (modalità di funzionamento) supportate dal dispositivo all'altro capo del collegamento, di determinare le funzionalità comuni e di autoconfigurarsi per il funzionamento congiunto. La negoziazione automatica viene eseguita al momento del collegamento, su comando dalla gestione, o al rilevamento di un errore di collegamento. Durante il processo di creazione del collegamento, entrambi i partner di collegamento scambiano le proprie funzionalità EEE 802.3az. Quando è abilitata sul dispositivo, la negoziazione automatica funziona automaticamente senza necessità di intervento da parte dell'utente.

> **NOTA** Se la negoziazione automatica non è abilitata su una porta, la funzione EEE è disabilitata. L'unica eccezione si presenta se la velocità di collegamento è 1GB; in questo caso, l'opzione EEE sarà ancora abilitata anche se la negoziazione automatica è disabilitata.

Rilevamento livello collegamento per EEE 802.3az

In aggiunta alle funzionalità sopra descritte, le funzionalità e le impostazioni di EEE 802.3az sono anche dichiarate utilizzando frame basati sui TLV specifici da un punto organizzativo come definito nell'Appendice G del protocollo IEEE Std 802.1AB (LLDP). LLDP viene utilizzato per ottimizzare ulteriormente il funzionamento di EEE 802.3az dopo il completamento della negoziazione automatica. Il TLV di EEE 802.3az viene utilizzato per affinare la riattivazione del sistema e la durata degli aggiornamenti.

Disponibilità di EEE 802.3az

Controllare le note di rilascio per un elenco completo dei prodotti che supportano EEE.

Configurazione predefinita

Per impostazione predefinita, EEE 802.3az e LLDP EEE sono attivati a livello globale e per porta.

Interazioni tra funzioni

Di seguito sono descritte le interazioni di EEE 802.3az con altre funzioni:

- Se la negoziazione automatica non è abilitata sulla porta, lo stato operativo di EEE 802.3az è disattivato. L'unica eccezione a questa regola è che se la velocità di collegamento è pari a 1GB, EEE sarà ancora abilitata anche se la negoziazione automatica è disabilitata.
- Se EEE 802.3az è abilitato e la porta è in via di attivazione, l'opzione inizia a funzionare immediatamente in conformità con il valore massimo di tempo di riattivazione della porta.
- Nell'interfaccia grafica, il campo EEE per la porta non è disponibile se l'opzione Raggiungimento breve e selezionata sulla porta.
- Se la velocità della porta sulla porta GE è passata a 10Mbit, EEE 802.3az è disabilitato. Questa funzione è supportata solo nei modelli GE.

Flusso di lavoro configurazione di EEE 802.3az

In questa sezione viene illustrato come configurare la funzione EEE 802.3az e visualizzarne i contatori.

PASSAGGIO 1 Assicurarsi che la negoziazione automatica sia attivata sulla porta visualizzando la pagina **Gestione porte > Impostazioni porta**.

a. Selezionare una porta e visualizzare la pagina Modifica impostazione porta.

b. Selezionare il campo **Negoziazione automatica** per verificare che sia abilitato.

PASSAGGIO 2 Nella pagina Gestione porte > Ethernet verde > Proprietà, assicurarsi che l'opzione **Energy Efficient Ethernet (EEE) 802.3** sia attivata a livello globale; questa opzione è selezionata per impostazione predefinita. Su questa pagina è visualizzata anche la quantità di energia risparmiata.

PASSAGGIO 3 Aprire la pagina Ethernet verde > Impostazioni porta per verificare che l'opzione EEE 802.3az sia attiva per una porta.

a. Selezionare una porta e aprire la pagina Modifica impostazione porta.

b. Selezionare la modalità **Energy Efficient Ethernet (EEE) 802.3** sulla porta (è attivata per impostazione predefinita).

c. Selezionare se abilitare o disabilitare la dichiarazione delle funzionalità EEE 802.3az tramite LLDP in **LLDP Energy Efficient Ethernet (EEE) 802.3 (EEE)** (è attivata per impostazione predefinita).

PASSAGGIO 4 Per visualizzare le informazioni relative a EEE 802.3 sul dispositivo locale, aprire la pagina Amministrazione > Rilevamento - LLDP >Informazioni locali LLDP e visualizzare le informazioni nel blocco Energy Efficient Ethernet (EEE) 802.3.

PASSAGGIO 5 Per visualizzare le informazioni relative a EEE 802.3az sul dispositivo remoto, aprire le pagine Amministrazione > Rilevamento - LLDP > Informazioni sui router LLDP adiacenti e visualizzare le informazioni nel blocco Energy Efficient Ethernet (EEE) 802.3.

Impostazione delle proprietà generali di Ethernet verde

Nella pagina Proprietà è possibile visualizzare e attivare la configurazione della modalità Ethernet verde per il dispositivo. Inoltre, è possibile visualizzare il risparmio energetico attuale.

Per abilitare Ethernet verde e EEE e visualizzare il risparmio energetico, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione porte** > **Ethernet verde** > **Proprietà**.

PASSAGGIO 2 Immettere i valori dei seguenti campi:

- **Modalità di rilevamento energia**: (non disponibile in SG500XG) disabilitata per impostazione predefinita. Fare clic sulla casella di controllo per attivarla.
- **Portata breve**: se sul dispositivo sono presenti porte GE, attivare o disattivare la modalità Portata breve a livello globale.

  NOTA Se la modalità di raggiungimento breve è abilitata, è necessario disattivare EEE.

- **LED della porta**: selezionare l'opzione per attivare i LED della porta. Quando queste vengono disattivate, non vengono visualizzati lo stato del collegamento, l'attività ecc...
- **Risparmio energetico**: viene indicata la percentuale di energia risparmiata operando con Ethernet verde e Raggiungimento breve. Il risparmio energetico visualizzato riguarda esclusivamente l'energia risparmiata grazie alle modalità di raggiungimento breve e di rilevamento energia. Il risparmio energetico EEE è dinamico per natura poiché si basa sull'utilizzo della porta,

pertanto non viene preso in considerazione. Il calcolo del risparmio energetico viene eseguito confrontando il consumo energetico massimo senza risparmio energetico con il consumo attuale.

- **Energia totale risparmiata**: viene indicata la quantità di energia risparmiata dall'ultimo riavvio del dispositivo. Questo valore viene aggiornato ogni volta che si verifica un evento che incide sul risparmio energetico.
- **Energy Efficient Ethernet (EEE) 802.3**: attivare o disattivare la modalità EEE a livello globale (disponibile solo se sul dispositivo sono presenti porte GE).

PASSAGGIO 3 Fare clic su **Applica**. Le proprietà di Ethernet verde vengono scritte nel file Configurazione di esecuzione.

Impostazione delle proprietà Ethernet verde per le porte

Nella pagina Impostazioni porta sono visualizzate le modalità Ethernet verde e EEE correnti per ogni porta; inoltre, è possibile selezionare una porta e aprire la pagina Modifica impostazione porta per configurare la modalità Ethernet verde. Per consentire a una porta di operare in modalità Ethernet verde, nella pagina Proprietà è necessario attivare le modalità corrispondenti a livello globale.

Tenere presente che le impostazioni EEE sono visualizzate solo per i dispositivi che dispongono di porte GE. EEE funziona solo quando le porte sono impostate su Negoziazione automatica. L'eccezione è che EEE è ancora funzionante, anche con la negoziazione automatica disabilitata, quando la porta è a 1GB o superiore.

Per definire le impostazioni di Ethernet verde per porta, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione porte** > **Ethernet verde**> **Impostazioni porta**.

Nella pagina Impostazioni porta vengono visualizzati gli elementi seguenti:

- **Stato parametro globale**: descrive le funzioni attive.

Per ogni porta, vengono descritti i seguenti campi:

- **Porta**: il numero della porta.
- **Rilevamento energia**: stato delle porte relativo alla modalità Rilevamento energia. Lo stato può essere:
  - *Amministrativo*: indica se la modalità Rilevamento energia è stata attivata.

- *Operativo*: indica se la modalità Rilevamento energia è al momento operativa.
- *Motivo*: se la modalità Rilevamento energia non è operativa, ne indica il motivo.

- **Raggiungimento breve**: stato delle porte relativo alla modalità Raggiungimento breve. Lo stato può essere:
  - *Amministrativo*: indica se la modalità Raggiungimento breve è stata attivata.
  - *Operativo*: indica se la modalità Raggiungimento breve è al momento operativa.
  - *Motivo*: se la modalità Raggiungimento breve non è operativa, ne indica il motivo.
  - *Lunghezza del cavo*: indica la lunghezza del cavo VCT restituito in metri.

  NOTA La modalità Raggiungimento breve viene supportata solo su porte RJ45 GE e non su porte combo.

- **Energy Efficient Ethernet (EEE) 802.3**: stato della porta relativo alla funzione EEE:
  - *Amministrativo*: indica se la modalità EEE è stata attivata.
  - *Operativo*: indica se la modalità EEE è attualmente operativa sulla porta locale. Indica se è stata attivata (stato amministrativo), se è stata attivata sulla porta locale e se è operativa sulla porta locale.
  - *LLDP amministrativo*: visualizza se i contatori EEE di annuncio tramite LLDP sono stati attivati.
  - *LLDP operativo*: visualizza se i contatori EEE di annuncio tramite LLDP sono attualmente in funzione.
  - *Supporto EEE su remoto*: visualizza se EEE è supportato sul partner di collegamento. EEE deve essere supportato sia sul partner di collegamento locale che su quello remoto.

  NOTA Nella finestra vengono visualizzate le impostazioni Portata breve, Rilevamento energia ed EEE per ogni porta; queste impostazioni, però, sono attivate sulle porte solo se sono state attivate a livello globale nella pagina Proprietà. Per attivare il raggiungimento breve e la EEE a livello globale, vedere **Impostazione delle proprietà generali di Ethernet verde**.

PASSAGGIO 2 Selezionare una **Porta** e fare clic su **Modifica**.

PASSAGGIO 3 Selezionare la modalità **Rilevamento energia** per attivarla o disattivarla sulla porta.

PASSAGGIO 4 Selezionare la modalità **Raggiungimento breve** per attivarla o disattivarla sulla porta se sul dispositivo sono presenti porte GE.

PASSAGGIO 5 Selezionare la modalità **Energy Efficient Ethernet (EEE) 802.3** per attivarla o disattivarla sulla porta se sul dispositivo sono presenti porte GE.

PASSAGGIO 6 Selezionare la modalità LLDP **Energy Efficient Ethernet (EEE) 802.3** per attivarla o disattivarla sulla porta (dichiarazione delle funzionalità EEE tramite LLDP) se sul dispositivo sono presenti porte GE.

PASSAGGIO 7 Fare clic su **Applica**. Le impostazioni della porta Ethernet verde vengono scritte nel file Configurazione di esecuzione.

11

Gestione delle porte: rilevamento del collegamento unidirezionale

In questa sezione viene descritta la funzione Rilevamento del collegamento unidirezionale (UDLD).

Vengono trattati i seguenti argomenti:

- **Panoramica della funzione UDLD**
- **Operazione UDLD**
- **Indicazioni di utilizzo**
- **Dipendenze da altre funzioni**
- **Impostazioni predefinite e configurazione**
- **Operazioni preliminari**
- **Attività UDLD comuni**
- **Configurazione della funzione UDLD**

Panoramica della funzione UDLD

La funzione UDLD è un protocollo di Livello 2 che consente ai dispositivi connessi con cavo Ethernet in fibra ottica o doppino di rilevare i collegamenti unidirezionali. Si verifica un collegamento unidirezionale ogni volta che il traffico proveniente da un dispositivo adiacente viene ricevuto dal dispositivo locale, ma il traffico proveniente dal dispositivo locale non viene ricevuto da quello adiacente.

Lo scopo della funzione UDLD è quello di rilevare le porte su cui il dispositivo adiacente non riceve il traffico che proviene dal dispositivo locale (collegamento unidirezionale) e di arrestarle.

Tutti i dispositivi collegati devono supportare la funzione UDLD per consentire al protocollo di rilevare correttamente i collegamenti unidirezionali. Se la funzione UDLD viene supportata soltanto dal dispositivo locale, tale dispositivo non sarà in grado di rilevare lo stato del collegamento. In questo caso, lo stato del collegamento è impostato su indeterminato. L'utente può configurare se le porte in stato indeterminato vengono arrestate o se inviano semplicemente delle notifiche.

Operazione UDLD

Stati e modalità UDLD

Nel protocollo della funzione UDLD, alle porte sono assegnati i seguenti stati:

- **Rilevamento**: il sistema sta tentando di determinare se il collegamento è di tipo bidirezionale o unidirezionale. Si tratta di uno stato temporaneo.
- **Bidirezionale**: il traffico inviato da un dispositivo locale viene in genere ricevuto dal suo dispositivo adiacente e il traffico inviato dal dispositivo adiacente viene ricevuto dal dispositivo locale.
- **Arresto**: il collegamento è unidirezionale. Il traffico inviato da un dispositivo locale viene ricevuto dal suo dispositivo adiacente, ma il traffico inviato dal dispositivo adiacente non viene ricevuto dal dispositivo locale.
- **Indeterminato**: il sistema non è in grado di determinare lo stato della porta, poiché si è verificata una delle seguenti condizioni:
  - Il dispositivo adiacente non supporta la funzione UDLD.

    oppure
  - Il dispositivo adiacente non riceve il traffico dal dispositivo locale.

  In questo caso, l'operato della funzione UDLD dipende dalla modalità UDLD del dispositivo, come spiegato di seguito.

La funzione UDLD supporta le seguenti modalità operative:

- **Normale**
  - Se il collegamento è unidirezionale, la porta viene arrestata.
  - Se il collegamento è indeterminato, la porta non viene arrestata. Il suo stato viene modificato in indeterminato e viene inviata una notifica.

- **Aggressiva**

  Se il collegamento è unidirezionale o indeterminato, la porta viene arrestata.

La funzione UDLD viene attivata su una porta quando si verifica una delle seguenti situazioni:

- La porta è una porta per cavi in fibra ottica e la funzione UDLD viene attivata a livello globale.
- La porta è una porta in rame e la funzione UDLD viene attivata specificamente su di essa.

Funzionamento UDLD

Quando la funzione UDLD viene attivata su una porta, vengono eseguite le seguenti azioni:

- La funzione UDLD avvia lo stato di rilevamento sulla porta.

  In questo stato, la funzione UDLD invia periodicamente dei messaggi su ogni interfaccia attiva a tutti i dispositivi adiacenti. Questi messaggi contengono l'ID dispositivo di tutti i dispositivi adiacenti rilevati. La funzione UDLD invia questi messaggi in base al tempo del messaggio definito dall'utente.

- La funzione UDLD riceve messaggi di tipo UDLD dai dispositivi adiacenti. Questi messaggi vengono conservati nella cache fino al superamento del periodo di scadenza (3 volte il tempo del messaggio). Se viene ricevuto un nuovo messaggio prima del periodo di scadenza, l'informazione presente in quel messaggio sostituisce la precedente.
- Al termine del periodo di scadenza, il dispositivo esegue le seguenti operazioni con le informazioni ricevute:
  - **Se il messaggio inviato dal dispositivo adiacente contiene l'ID del dispositivo locale**: lo stato del collegamento delle porta viene impostato su bidirezionale.
  - **Se il messaggio inviato dal dispositivo adiacente non contiene l'ID del dispositivo locale**: lo stato del collegamento della porta viene impostato su unidirezionale e la porta viene arrestata.

- Se i messaggi inviati dalla funzione UDLD non vengono ricevuti dal dispositivo adiacente durante il frame del periodo di scadenza, lo stato del collegamento viene impostato su indeterminato e si verificano le seguenti situazioni:
  - **Il dispositivo è in modalità UDLD normale:** viene inviata una notifica.
  - **Il dispositivo è in modalità UDLD aggressiva.** La porta viene arrestata.

Mentre l'interfaccia è in stato bidirezionale o indeterminato, il dispositivo invia periodicamente un messaggio per ogni secondo del tempo del messaggio. I passaggi descritti sopra vengono eseguiti ripetutamente.

È possibile riattivare manualmente una porta arrestata nella pagina Gestione delle porte > Impostazioni ripristino errore. Per ulteriori informazioni, vedere la sezione **Riattivazione di una porta arrestata**.

Se un'interfaccia è inattiva e la funzione UDLD è abilitata, il dispositivo rimuove tutte le informazioni dei dispositivi adiacenti e invia loro almeno un messaggio UDLD per informarli che la porta risulta essere inattiva. Quando la porta viene attivata, lo stato UDLD viene modificato su rilevamento.

Funzione UDLD non supportata o disattivata su un dispositivo adiacente

Se la funzione UDLD non è supportata o risulta disattivata su un dispositivo adiacente, tale dispositivo non riceve nessun messaggio UDLD. In questo caso, il dispositivo non è in grado di determinare se il collegamento è di tipo unidirezionale o bidirezionale. Lo stato dell'interfaccia viene quindi impostato su indeterminato. Le azioni eseguite dal dispositivo dipendono dalla modalità UDLD (normale o aggressiva).

Modalità UDLD incoerente nei dispositivi locali e adiacenti

È possibile che per il dispositivo locale e per il suo dispositivo adiacente sia impostata una modalità UDLD diversa (normale o aggressiva). Poiché la modalità UDLD non è contenuta nei messaggi UDLD, il dispositivo locale non è a conoscenza della modalità UDLD del dispositivo adiacente e viceversa.

Se le modalità UDLD del dispositivo locale e di quello adiacente sono diverse, il funzionamento dei dispositivi è il seguente:

- Quando lo stato UDLD del collegamento è bidirezionale o unidirezionale, entrambi i dispositivi arrestano le porte.

- Quando lo stato UDLD della porta è indeterminato, il dispositivo in modalità UDLD normale si limita ad attivare una notifica, mentre il dispositivo in modalità UDLD aggressiva arresta la porta.

Se entrambi i dispositivi sono in modalità normale, la porta non viene arrestata quando il suo stato risulta essere indeterminato.

Riattivazione di una porta arrestata

È possibile riattivare una porta arrestata da una funzione UDLD in uno dei seguenti modi:

- **Automaticamente**: è possibile configurare il sistema affinché riattivi automaticamente le porte arrestate dalla funzione UDLD, andando alla pagina Gestione delle porte > Impostazioni ripristino errore. In questo caso, una porta arrestata da una funzione UDLD viene automaticamente riattivata alla scadenza dell'intervallo di ripristino automatico. La funzione UDLD torna operativa sulla porta. Ad esempio, se il collegamento è ancora unidirezionale, la funzione UDLD lo arresta nuovamente dopo il termine del periodo di scadenza della funzione UDLD
- **Manualmente**: è possibile riattivare una porta nella pagina Gestione delle porte > Impostazioni ripristino errore.

Indicazioni di utilizzo

Cisco consiglia di non attivare la funzione UDLD sulle porte collegate a dispositivi sui quali la funzione UDLD risulta non supportata o disattivata. L'invio di pacchetti UDLD a una porta collegata a un dispositivo che non supporta la funzione UDLD causa semplicemente più traffico sulla porta senza apportare alcun beneficio.

Si consiglia inoltre di considerare le seguenti informazioni durante la configurazione della funzione UDLD:

- Impostare il tempo del messaggio in base al livello di urgenza di arresto delle porte con collegamento unidirezionale. Minore è l'intervallo del tempo del messaggio, maggiore sarà la quantità di pacchetti UDLD inviati e analizzati, ma l'arresto della porta verrà eseguito più rapidamente in caso di collegamento unidirezionale.
- Se si desidera attivare la funzione UDLD su una porta in rame, questa deve essere attivata su ciascuna porta. Quando la funzione UDLD viene attivata a livello globale, risulta essere attiva solo sulle porte in fibra ottica.

- Impostare la modalità UDLD su normale quando non si desidera arrestare le porte finché non si è certi che il collegamento sia unidirezionale.
- Impostare la modalità UDLD su aggressiva quando si desidera arrestare le porte ogni volta che si presenta la possibilità che il collegamento sia indeterminato.

Dipendenze da altre funzioni

- UDLD e Livello 1.

  Quando la funzione UDLD è abilitata su una porta, tale funzione viene eseguita attivamente sulla porta quando quest'ultima è attiva. Quando la porta è inattiva, la funzione UDLD passa allo stato di arresto UDLD. In questo stato, la funzione UDLD rimuove tutti i dispositivi adiacenti conosciuti. Quando lo stato della porta passa da inattivo ad attivo, la funzione UDLD riprende a operare attivamente.
- UDLD e protocolli di Livello 2

  La funzione UDLD viene eseguita su una porta indipendentemente da altri protocolli di Livello 2 eseguiti sulla stessa porta, come STP o LACP. Ad esempio, la funzione UDLD assegna uno stato alla porta indipendentemente dallo stato STP della porta o dal fatto che la porta appartenga o meno a un LAG.

Impostazioni predefinite e configurazione

Per questa funzione esistono i seguenti valori predefiniti:

- La funzione UDLD viene disattivata per impostazione predefinita su tutte le porte del dispositivo.
- Il tempo del messaggio predefinito è 15 secondi.
- Il periodo di scadenza predefinito è 45 secondi (3 volte il tempo del messaggio).
- Stato UDLD della porta predefinito:
  - Le interfacce in fibra ottica sono impostate sullo stato UDLD globale.
  - Le interfacce non in fibra ottica sono impostate sullo stato disattivato.

Operazioni preliminari

Nessuna attività preliminare richiesta.

Attività UDLD comuni

In questa sezione vengono illustrate alcune attività comuni per l'impostazione della funzione UDLD.

Flusso di lavoro 1: *per attivare a livello globale la funzione UDLD sulle porte in fibra ottica, attenersi alla seguente procedura:*

PASSAGGIO 1 Aprire la pagina Gestione delle porte > Impostazioni generali UDLD.

a. Immettere il **tempo del messaggio**.

b. Selezionare **Disattivato**, **Normale** o **Aggressivo** come stato globale della funzione UDLD.

PASSAGGIO 2 Fare clic su **Applica**.

Flusso di lavoro 2: *per modificare la configurazione UDLD di una porta in fibra ottica o per attivare la funzione UDLD su una porta di rame, attenersi alla seguente procedura:*

PASSAGGIO 1 Aprire la pagina **Gestione delle porte > Impostazioni generali UDLD**.

a. Selezionare una porta.

b. Selezionare **Predefinito**, **Disattivato**, **Normale** o **Aggressivo** come stato della porta UDLD. Se si seleziona Predefinito, la porta riceve l'impostazione generale.

PASSAGGIO 2 Fare clic su **Applica**.

Flusso di lavoro 3: *per attivare una porta arrestata dalla funzione UDLD quando la riattivazione automatica non è configurata, attenersi alla seguente procedura:*

PASSAGGIO 1 Aprire la pagina **Gestione delle porte** > **Impostazioni ripristino errore**.

a. Selezionare una porta.

b. Fare clic su **Riattiva**.

Configurazione della funzione UDLD

La funzione UDLD può essere configurata contemporaneamente per tutte le porte in fibra ottica (nella pagina Impostazioni generali UDLD) o separatamente per ciascuna porta (nella pagina Impostazioni interfaccia UDLD).

Impostazioni generali UDLD

Lo stato predefinito UDLD della porta in fibra ottica è applicabile solo alle porte in fibra ottica.

Il campo relativo al tempo del messaggio è applicabile sia alle porte in rame sia a quelle in fibra ottica.

Per configurare la funzione UDLD a livello globale, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione delle porte > UDLD** > **Impostazioni generali UDLD**.

PASSAGGIO 2 Immettere informazioni nei seguenti campi:

- **Tempo del messaggio**: immettere l'intervallo di tempo tra l'invio di due messaggi UDLD. Questo campo è rilevante sia per le porte in rame sia per quelle in fibra ottica.
- **Stato predefinito della funzione UDLD della porta in fibra ottica**: questo campo è rilevante soltanto per le porte in **fibra ottica**. Lo stato della funzione UDLD delle porte in rame deve essere impostato singolarmente nella pagina Impostazioni interfaccia UDLD. I possibili stati sono:
  - *Disattivato*: la funzione UDLD è disattivata su tutte le porte del dispositivo.

- *Normale*: il dispositivo arresta un'interfaccia se il collegamento è unidirezionale. Se il collegamento è indeterminato, viene inviata una notifica.
- *Aggressivo*: il dispositivo arresta un'interfaccia se il collegamento è unidirezionale o indeterminato.

PASSAGGIO 3 Fare clic su **Applica** per salvare le impostazione sul file Configurazione di esecuzione.

Impostazioni interfaccia UDLD

Utilizzare la pagina Impostazioni interfaccia UDLD per modificare lo stato della funzione UDLD per una porta specifica. In questa pagina lo stato può essere impostato per porte in fibra ottica o in rame.

Per copiare una specifica serie di valori in più di una porta, impostare il valore per una porta e utilizzare il pulsante **Copia** per copiarlo nelle altre porte.

Per configurare la funzione UDLD per un'interfaccia, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione delle porte> UDLD** > **Impostazioni interfaccia UDLD**.

Le informazioni vengono visualizzate per tutte le porte sulle quali è attiva la funzione UDLD, oppure, se è stato applicato un filtro per un determinato gruppo di porte, le informazioni vengono visualizzate solo per quel gruppo.

- **Porta**: l'identificatore della porta.
- **Stato UDLD**: i possibili stati sono:
  - *Disattivato*: la funzione UDLD è disattivata su tutte le porte in fibra ottica del dispositivo.
  - *Normale*: il dispositivo arresta un'interfaccia se rileva che il collegamento è unidirezionale. Invia una notifica se il collegamento è indeterminato.
  - *Aggressivo*: il dispositivo arresta una porta se il collegamento è unidirezionale o indeterminato.

- **Stato bidirezionale**: selezionare il valore di questo campo per la porta selezionata. I possibili stati sono:
  - *Rilevamento*: il più recente stato UDLD della porta è in corso di determinazione. Il periodo di scadenza non scade fino all'ultima determinazione (se ce n'è stata una) oppure fino a quando la funzione UDLD riprende l'esecuzione sulla porta, in modo che lo stato non risulti ancora stabilito.
  - *Bidirezionale*: il traffico inviato dal dispositivo locale viene ricevuto dal suo dispositivo adiacente e il traffico inviato dal dispositivo adiacente viene ricevuto dal dispositivo locale.
  - *Indeterminato*: lo stato del collegamento tra la porta e la sua porta collegata non può essere stabilito perché nessun messaggio UDLD è stato ricevuto oppure perché il messaggio UDLD non conteneva l'ID del dispositivo locale.
  - *Disattivato*: la funzione UDLD è stata disattivata su questa porta.
  - *Arresto*: la porta è stata arrestata poiché in modalità aggressiva, il collegamento con il dispositivo collegato risulta unidirezionale o indeterminato.
- **Numero di dispositivi adiacenti**: numero di dispositivi collegati rilevato.

PASSAGGIO 2 Per modificate lo stato UDLD per una porta specifica, selezionarla e fare clic su **Modifica**.

PASSAGGIO 3 Modificare il valore dello stato UDLD. Se viene selezionato **Predefinito**, la porta riceve il valore dello **Stato predefinito UDLD della porta in fibra ottica** nella pagina Impostazioni generali UDLD.

PASSAGGIO 4 Fare clic su **Applica** per salvare le impostazione sul file Configurazione di esecuzione.

Adiacenti UDLD

Per visualizzare tutti i dispositivi collegati al dispositivo locale, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione delle porte> UDLD** > **UDLD dispositivi adiacenti**.

I seguenti campi vengono visualizzati per tutte le porte con funzione UDLD attivata.

- **Nome interfaccia**: nome della porta locale con funzione UDLD attivata.

- **Informazioni sui router adiacenti:**
  - *ID dispositivo*: ID del dispositivo remoto.
  - *Dispositivo MAC*: indirizzo MAC del dispositivo remoto.
  - *Nome dispositivo*: nome del dispositivo remoto.
  - *ID porta*: nome della porta remota.
- **Stato**: stato del collegamento tra il dispositivo locale e quello adiacente sulla porta locale. I valori selezionabili sono:
  - *Rilevamento*: il più recente stato UDLD della porta è in corso di determinazione. Il periodo di scadenza non scade fino all'ultima determinazione (se ce n'è stata una) oppure fino a quando la funzione UDLD riprende l'esecuzione sulla porta, in modo che lo stato non risulti ancora stabilito.
  - *Bidirezionale*: il traffico inviato dal dispositivo locale viene ricevuto dal suo dispositivo adiacente e il traffico inviato dal dispositivo adiacente viene ricevuto dal dispositivo locale.
  - *Indeterminato*: lo stato del collegamento tra la porta e la sua porta collegata non può essere stabilito perché nessun messaggio UDLD è stato ricevuto oppure perché il messaggio UDLD non conteneva l'ID del dispositivo locale.
  - *Disattivato*: la funzione UDLD è stata disattivata su questa porta.
  - *Arresto*: la porta è stata arrestata poiché in modalità aggressiva, il collegamento con il dispositivo collegato risulta unidirezionale o indeterminato.
- **Periodo di scadenza dispositivo adiacente (sec)**: consente di visualizzare il tempo che deve trascorrere prima di poter determinare lo stato UDLD della porta. Corrisponde a tre volte il valore del tempo del messaggio.
- **Tempo del messaggio del dispositivo adiacente (sec)**: consente di visualizzare il tempo trascorso tra i messaggi UDLD.

12

Smartport

Nel presente documento viene descritta la funzionalità Smartport e vengono trattati i seguenti argomenti:

- Panoramica
- Descrizione di uno Smartport
- Tipi di Smartport
- Macro Smartport
- Errore delle macro e operazione di reimpostazione
- Funzionamento di Smartport
- Smartport automatico
- Gestione degli errori
- Configurazione predefinita
- Relazioni con altre funzioni e retrocompatibilità
- Attività comuni con Smartport
- Configurare Smartport tramite l'interfaccia basata su Web
- Macro Smartport integrate

Panoramica

La funzione Smartport offre un metodo semplice per salvare e condividere configurazioni comuni. Se si applica la stessa macro Smartport a più interfacce, esse condivideranno un insieme comune di configurazioni. Una macro Smartport è uno script di comandi CLI (Command Line Interface).

Una macro Smartport può essere applicata a un'interfaccia tramite il nome macro o tramite il tipo di Smartport associato alla macro. L'applicazione di una macro Smartport tramite il nome macro può essere eseguita solo attraverso la CLI. Per i dettagli, consultare la guida CLI.

Esistono due modi per applicare a un'interfaccia una macro Smartport tramite il tipo Smartport:

- **Smartport statico**: si assegna manualmente un tipo Smartport a un'interfaccia. Il risultato è l'applicazione della macro Smartport corrispondente all'interfaccia.
- **Smartport automatico**: Smartport automatico attende il collegamento di un dispositivo all'interfaccia prima di applicare una configurazione. Quando un dispositivo viene rilevato da un'interfaccia, la macro Smartport (se assegnata) che corrisponde al tipo Smartport del dispositivo in collegamento viene applicata automaticamente.

La funzione Smartport è costituita da vari componenti e funziona in combinazione con altre funzioni del dispositivo. Questi componenti e caratteristiche sono descritti nelle sezioni seguenti:

- Smartport, tipi di Smartport e macro Smartport, descritti in questa sezione.
- VLAN voce e Smartport, descritti nella sezione **VLAN voce**.
- LLDP/CDP per Smartport descritti, rispettivamente, nelle sezioni **Configurazione di LLDP** e **Configurazione CDP**.

Inoltre, i flussi di lavoro tipici sono descritti nella sezione **Attività comuni con Smartport**.

Descrizione di uno Smartport

Uno Smartport è un'interfaccia alla quale può essere applicata una macro integrata (o definita dall'utente). Queste macro sono ideate per fornire un mezzo di configurazione rapida del dispositivo al fine di supportare i requisiti di comunicazione e utilizzare le caratteristiche dei vari tipi di dispositivi di rete. La rete di accesso e requisiti QoS variano se l'interfaccia è collegata a un telefono IP, a una stampante o a un router e/o punto di accesso (AP).

Tipi di Smartport

Con tipi di Smartport si intendono i tipi di dispositivi collegati o da collegare agli Smartport. Il dispositivo supporta i seguenti tipi di Smartport:

- Stampante
- Desktop
- Ospite
- Server
- Host
- Camera IP
- Telefono IP
- Telefono IP + Desktop
- Switch
- Router
- Access point wireless

I tipi di Smartport sono denominati in modo da descrivere il tipo di dispositivo collegato a un'interfaccia. Ogni tipo di Smartport è associato a due macro Smartport. Una macro, chiamata "la macro", serve per applicare la configurazione desiderata. L'altra, chiamata "l'anti-macro", serve per annullare tutte le configurazioni eseguite da "la macro", quando quell'interfaccia diventa un diverso tipo di Smartport.

È possibile applicare una macro Smartport utilizzando i metodi seguenti:

- Il tipo di Smartport associato.
- Staticamente da una macro Smartport tramite il nome solo dalla CLI.

Una macro Smartport può essere applicata staticamente tramite suo tipo Smartport dalla CLI e dall'interfaccia grafica, e dinamicamente da Smartport automatico. Smartport automatico ottiene i tipi Smartport dei dispositivi collegati sulla base delle funzionalità CDP, delle funzionalità di sistema LLDP e/o delle funzionalità LLDP-MED.

Di seguito viene descritta la relazione tra tipi di Smartport e Smartport automatico.

Tipo Smartport	Supportato da Smartport automatico	Supportato da Smartport automatico per impostazione predefinita
Sconosciuto	No	No
Predefinito	No	No
Stampante	No	No
Desktop	No	No
Ospite	No	No
Server	No	No
Host	Sì	No
Camera IP	No	No
Telefono IP	Sì	Sì
Telefono IP + desktop	Sì	Sì
Switch	Sì	Sì
Router	Sì	No
Access point wireless	Sì	Sì

Tipi di Smartport speciali

Esistono due tipi di Smartport speciali: *predefinito* e *sconosciuto*. Questi due tipi non sono associati alle macro, ma esistono per indicare lo stato dell'interfaccia che riguarda Smartport.

Di seguito sono descritti i tipi di Smartport speciali:

- **Predefinito**

  Un'interfaccia che non ha (ancora) un tipo di Smartport assegnato presenta lo stato Smartport predefinito.

  Se Smartport automatico assegna un tipo di Smartport a un'interfaccia e tale interfaccia non è configurata per essere Smartport automatico persistente, allora il tipo di Smartport corrispondente sarà reinizializzato su Predefinito nei seguenti casi:

  - Sull'interfaccia viene eseguita un'operazione di attivazione/disattivazione del collegamento.
  - Il dispositivo viene riavviato.
  - Tutti i dispositivi collegati all'interfaccia sono scaduti: questo viene definito come l'assenza di annuncio CDP e/o LLDP dal dispositivo per un periodo di tempo specificato.

- **Sconosciuto**

  Se una macro Smartport viene applicata a un'interfaccia e si verifica un errore, all'interfaccia viene assegnato lo stato Sconosciuto. In questo caso, le funzioni Smartport e Smartport automatico verranno riattivate solo dopo aver corretto l'errore e aver applicato l'azione di reimpostazione (eseguita nella pagina Impostazioni interfaccia) che ripristina lo stato dello Smartport.

  Per la risoluzione dei problemi vedere l'area del flusso di lavoro nella sezione **Attività comuni con Smartport**.

NOTA In questa sezione, il termine "scaduto" viene utilizzato per descrivere i messaggi LLDP e CDP tramite il relativo TTL. Se è attivato Smartport automatico, lo stato persistente è disattivato e sull'interfaccia non vengono ricevuti più messaggi CDP o LLDP prima che entrambi i TTL dei pacchetti CDP e LLDP più recenti scendano a 0, allora verrà eseguita l'anti-macro e il tipo di Smartport tornerà al valore predefinito.

Macro Smartport

Una macro Smartport è uno script di comandi CLI che configurano un'interfaccia in modo appropriato per un particolare dispositivo di rete.

Le macro Smartport non devono essere confuse con le macro globali. Le macro globali configurano il dispositivo a livello globale; tuttavia, la portata di una macro Smartport è limitata all'interfaccia su cui viene applicata.

Per trovare la sorgente macro, eseguire il comando show parser macro name [nome_macro] in modalità di esecuzione privilegiata della CLI oppure fare clic sul pulsante **Visualizza sorgente macro** nella pagina Impostazioni tipo Smartport.

Una macro e la corrispondente anti-macro sono accoppiate in associazione con ogni tipo di Smartport. La macro applica la configurazione e l'anti-macro la rimuove.

Esistono due tipi di macro Smartport:

- **Integrata**: queste sono le macro fornite dal sistema. Una macro applica il profilo di configurazione e l'altra lo rimuove. I nomi macro delle macro Smartport integrate e il tipo di Smartport cui sono associati vengono rappresentati come segue:
  - macro-name (ad esempio: printer)
  - no_macro-name (ad esempio: no_printer)
- **Definita dall'utente**: queste sono macro scritte dagli utenti. Per ulteriori informazioni su questo argomento, vedere la Guida di riferimento CLI. Per associare una macro definita dall'utente ad un tipo di Smartport, è necessario definire anche la rispettiva anti-macro.
  - smartport-type-name (ad esempio: my_printer)
  - no_smartport-type-name (ad esempio: no_my_printer)

Le macro Smartport sono legate ai tipi di Smartport specificati nella pagina Modifica impostazione tipo Smartport.

Vedere **Macro Smartport integrate** per ottenere un elenco delle macro Smartport integrate per ogni tipo di dispositivo.

Applicazione di un tipo di Smartport a un'interfaccia

Quando vengono applicati alle interfacce, i tipi di Smartport e la configurazione delle macro Smartport associate vengono salvati nel file Configurazione di esecuzione. Se l'amministratore salva il file di configurazione esecuzione nel file di configurazione avvio, il dispositivo applica i tipi di Smartport e le macro Smartport alle interfacce dopo il riavvio nel seguente modo:

- Se il file Configurazione di avvio non specifica un tipo di Smartport per un'interfaccia, il relativo tipo di Smartport è impostato Predefinito.
- Se il file Configurazione di avvio specifica un tipo Smartport statico, il tipo Smartport dell'interfaccia è impostato su tale tipo statico.
- Se il file Configurazione di avvio specifica un tipo Smartport che è stato assegnato dinamicamente da Smartport automatico:
  - Se lo stato operativo globale di Smartport automatico, l'interfaccia Smartport automatico e lo stato Persistente sono tutti **attivi**, il tipo di Smartport è impostato su questo tipo dinamico.
  - In caso contrario, l'anti-macro corrispondente viene applicata e lo stato delle interfacce viene impostato su Predefinito.

Errore delle macro e operazione di reimpostazione

Una macro Smartport potrebbe non funzionare in caso di conflitto tra la configurazione esistente dell'interfaccia e una macro Smartport.

Quando una macro Smartport non funziona, viene inviato un messaggio SYSLOG contenente i seguenti parametri:

- Numero della porta
- Tipo di Smartport
- Il numero di riga del comando CLI non riuscito nella macro.

Quando una macro Smartport genera un errore su un'interfaccia, lo stato dell'interfaccia è impostato su *Sconosciuto*. Il motivo dell'errore può essere visualizzato nella finestra a comparsa **Mostra diagnostica** della finestra Impostazioni interfaccia.

Dopo aver determinato l'origine del problema e corretto la configurazione esistente o la macro SmartPort, è necessario eseguire un'operazione di reimpostazione dell'interfaccia prima che questa possa essere riapplicata con un tipo di Smartport (nelle pagine Impostazioni interfaccia). Per la risoluzione dei problemi vedere l'area del flusso di lavoro nella sezione **Attività comuni con Smartport**.

Funzionamento di Smartport

Una macro Smartport può essere applicata a un'interfaccia tramite il nome della macro o il tipo di Smartport associato alla macro. L'applicazione di una macro Smartport tramite il nome macro può essere eseguita solo attraverso la CLI. Consultare la Guida di riferimento CLI per ulteriori dettagli.

Poiché viene fornito supporto per i tipi di Smartport che corrispondono a dispositivi che non si lasciano rilevare attraverso CDP e/o LLDP, questi tipi di Smartport devono essere assegnati staticamente alle interfacce desiderate. A tal fine, accedere alla pagina Impostazioni interfaccia Smartport, selezionare il pulsante corrispondente all'interfaccia desiderata e fare clic su **Modifica**. Quindi, selezionare il tipo di Smartport che si desidera assegnare e regolare i parametri come richiesto prima di fare clic su **Applica**.

Esistono due modi per applicare a una interfaccia una macro Smartport tramite il tipo Smartport:

- **Smartport statico**

  Si assegna manualmente un tipo Smartport a un'interfaccia. La macro Smartport corrispondente viene applicata all'interfaccia. È possibile assegnare manualmente un tipo di Smartport a un'interfaccia nella pagina Impostazioni interfaccia Smartport.

- **Smartport automatico**

  Quando un dispositivo viene rilevato da un'interfaccia, la macro Smartport, se presente, che corrisponde al tipo Smartport del dispositivo in collegamento viene applicata automaticamente. Smartport automatico è attivato per impostazione predefinita a livello globale e a livello di interfaccia.

In entrambi i casi, l'anti-macro associata viene eseguita quando il tipo di Smartport viene rimosso dall'interfaccia: viene eseguita esattamente nello stesso modo, eliminando tutta la configurazione di interfaccia.

Smartport automatico

Affinché possa assegnare automaticamente i tipi di Smartport alle interfacce, la funzione Smartport automatico deve essere abilitata a livello globale e sulle interfacce rilevanti che deve poter configurare. Per impostazione predefinita, Smartport automatico è attivato ed è autorizzato a configurare tutte le interfacce. Il tipo di Smartport assegnato a ciascuna interfaccia viene determinato dai pacchetti CDP e LLDP ricevuti, rispettivamente, su ogni interfaccia.

- Se più dispositivi sono collegati a un'interfaccia, se possibile viene applicato all'interfaccia un profilo di configurazione appropriato per tutti i dispositivi.
- Se un dispositivo è scaduto (non riceve più annunci da altri dispositivi), la configurazione dell'interfaccia viene modificata in base al suo Stato persistente. Se Stato persistente è attivato, la configurazione dell'interfaccia viene mantenuta. In caso contrario, il tipo di Smartport ritorna all'impostazione predefinita.

Attivazione di Smartport automatico

La funzione Smartport automatico può essere attivata a livello globale nella pagina Proprietà nei seguenti modi:

- **Attivato**: attiva manualmente Smartport automatico e lo mette subito in funzione.
- **Attiva con VLAN voce automatica**: consente a Smartport automatico di funzionare se la VLAN voce automatica è abilitata e in funzione. L'impostazione predefinita è Attiva con VLAN voce automatica.

NOTA Oltre ad attivarlo a livello globale, è necessario attivare Smartport automatico anche a livello dell'interfaccia desiderata. Per impostazione predefinita, Smartport automatico è abilitato su tutte le interfacce.

Vedere la sezione **VLAN voce** per ulteriori informazioni su come attivare la VLAN voce automatica.

Identificazione del tipo di Smartport

Se la funzione Smartport automatico è abilitata a livello globale (nella pagina Proprietà e su un'interfaccia (nella pagina Impostazioni interfaccia), il dispositivo applica una macro Smartport all'interfaccia in base al tipo di Smartport del dispositivo che si sta collegando. Smartport automatico ottiene i tipi di Smartport dei dispositivi in collegamento sulla base del CDP e/o LLDP che i dispositivi annunciano.

Se, ad esempio, un telefono IP è collegato a una porta, trasmetterà i pacchetti CDP o LLDP che dichiarano le sue funzionalità. Dopo la ricezione di questi pacchetti CDP e/o LLDP, il dispositivo ottiene il tipo di Smartport appropriato per il telefono e applica la macro Smartport corrispondente all'interfaccia a cui si collega il telefono IP.

A meno che Smartport automatico persistente sia attivato su un'interfaccia, il tipo di Smartport e la configurazione risultante applicata da Smartport automatico saranno rimossi se i dispositivi in collegamento scadono, perdono il collegamento, si riavviano o se vengono ricevute funzionalità in conflitto. I tempi di scadenza sono determinati dall'assenza di annunci CDP e/o LLDP dal dispositivo per un periodo di tempo specificato.

Utilizzo delle informazioni CDP/LLDP per l'identificazione dei tipi di Smartport

Il dispositivo rileva il tipo di dispositivo collegato alla porta in base alle funzionalità CDP/LLDP.

Tale associazione viene mostrata nelle tabelle di seguito:

Associazione delle funzionalità CDP al tipo di Smartport

Nome funzionalità	Bit CDP	Tipo Smartport
Router	0x01	Router
Bridge TB	0x02	Access point wireless
Bridge SR	0x04	Ignora
Switch	0x08	Switch
Host	0x10	Host
Filtro IGMP condizionale	0x20	Ignora
Ripetitore	0x40	Ignora
Telefono VoIP	0x80	ip_phone

Associazione delle funzionalità CDP al tipo di Smartport (Continua)

Nome funzionalità	Bit CDP	Tipo Smartport
Dispositivo gestito in remoto	0x100	Ignora
Porta telefono CAST	0x200	Ignora
Relay MAC due porte	0x400	Ignora

Associazione delle funzionalità LLDP al tipo di Smartport

Nome funzionalità	Bit LLDP	Tipo Smartport
Altro	1	Ignora
Repeater IETF RFC 2108	2	Ignora
Bridge MAC IEEE Std. 802.1D	3	Switch
Access point WLAN IEEE Std. 802.11 MIB	4	Access point wireless
Router IETF RFC 1812	5	Router
Telefono IETF RFC 4293	6	ip_phone
Dispositivo cavo DOCSIS IETF RFC 4639 e IETF RFC 4546	7	Ignora
Solo stazione IETF RFC 4293	8	Host
Componente C-VLAN di un bridge VLAN IEEE Std. 802.1Q	9	Switch
Componente S-VLAN di un bridge VLAN IEEE Std. 802.1Q	10	Switch
Relay MAC due porte (TPMR) IEEE Std. 802.1Q	11	Ignora
Riservato	12-16	Ignora

NOTA Se vengono impostati solo i bit Telefono IP e Host, allora il tipo SmartPort è ip_phone_desktop.

Più dispositivi collegati alla porta

Il dispositivo ottiene il tipo di Smartport di un dispositivo collegato tramite le funzionalità che il dispositivo annuncia nei propri pacchetti CDP e/o LLDP.

Se più dispositivi sono collegati al dispositivo tramite un'unica interfaccia, la funzione Smartport automatico prende in considerazione ogni annuncio di funzionalità che riceve attraverso l'interfaccia designata al fine di assegnare il tipo di Smartport corretto. L'assegnazione avviene in base al seguente algoritmo:

- Se tutti i dispositivi su un'interfaccia annunciano la stessa funzionalità (non c'è conflitto), il tipo di Smartport corrispondente viene applicato all'interfaccia.
- Se uno dei dispositivi è uno switch, viene utilizzato il tipo di Smartport *Switch*.
- Se uno dei dispositivi è un punto di accesso, viene utilizzato il tipo di Smartport *Punto di accesso wireless*.
- Se uno dei dispositivi è un telefono IP e un altro è un host, viene utilizzato il tipo di Smartport *ip_phone_desktop*.
- Se uno dei dispositivi è un telefono IP desktop e l'altro è un telefono IP o un host, viene utilizzato il tipo di Smartport *ip_phone_desktop*.
- In tutti gli altri casi viene utilizzato il tipo di Smartport predefinito.

Per ulteriori informazioni su LLDP/CDP vedere, rispettivamente, le sezioni **Configurazione di LLDP** e **Configurazione CDP**.

Interfaccia Smartport automatico persistente

Se per un'interfaccia è attivata l'opzione Stato persistente, il relativo tipo di Smartport e la configurazione che è stata già applicata in modo dinamico dalla funzione Smartport automatico rimarranno sull'interfaccia anche dopo la scadenza del dispositivo collegato, la disattivazione dell'interfaccia e il riavvio del dispositivo (presupponendo che la configurazione venga salvata). Il tipo di Smartport e la configurazione dell'interfaccia non sono cambiati a meno che Smartport automatico rilevi un dispositivo in collegamento con un tipo di Smartport diverso. Se per un'interfaccia è stata attivata l'opzione Stato persistente, l'interfaccia ritorna al tipo di Smartport predefinito quando il dispositivo collegato scade, l'interfaccia viene disattivata o il dispositivo viene riavviato. L'attivazione dello Stato persistente su un'interfaccia elimina il ritardo nel rilevamento del dispositivo, che altrimenti si verificherebbe.

NOTA La persistenza dei tipi di Smartport applicati alle interfacce è effettiva tra i riavvii solo se la configurazione di esecuzione con il tipo di Smartport applicato alle interfacce è salvata nel file Configurazione di avvio.

Gestione degli errori

Se l'applicazione di una macro Smartport a un'interfaccia fallisce, è possibile esaminare il punto di errore nella pagina Impostazioni interfaccia, quindi reimpostare la porta e riapplicare la macro dopo avere corretto l'errore nelle pagine Impostazioni interfaccia e Modifica impostazioni.

Configurazione predefinita

Smartport è sempre disponibile. Per impostazione predefinita, Smartport automatico è abilitato per VLAN voce automatica, utilizza sia CDP che LLDP per rilevare il tipo di Smartport del dispositivo in collegamento e rileva i tipi di Smartport Telefono IP, Telefono IP + desktop, Switch e Punto di accesso wireless.

Vedere **VLAN voce** per una descrizione delle impostazioni predefinite della voce.

Relazioni con altre funzioni e retrocompatibilità

Smartport automatico è abilitato per impostazione predefinita e può essere disattivato. OUI telefonia non può funzionare in concomitanza con Smartport automatico e VLAN voce automatica. Smarport automatico deve essere disattivato prima di abilitare OUI telefonia.

Attività comuni con Smartport

In questa sezione vengono illustrate alcune attività comuni per impostare Smartport e Smartport automatico.

Flusso di lavoro 1: per attivare globalmente la funzione Smartport automatico sul dispositivo e per configurare una porta con funzione Smartport automatico, attenersi alla seguente procedura:

PASSAGGIO 1 Per attivare la funzione Smartport automatico sul dispositivo, aprire la pagina Smartport > Proprietà. Impostare **Smartport automatico amministrativo** su **Attiva** o **Attiva con VLAN voce automatica**.

PASSAGGIO 2 Selezionare se il dispositivo debba elaborare gli annunci CDP e/o LLDP provenienti da dispositivi collegati.

PASSAGGIO 3 Selezionare quale tipo di dispositivo sarà rilevato nel campo **Rilevamento dispositivo Smartport automatico**.

PASSAGGIO 4 Fare clic su **Applica**.

PASSAGGIO 5 Per attivare la funzione Smartport automatico su una o più interfacce, aprire la pagina Smartport > Impostazioni interfaccia.

PASSAGGIO 6 Selezionare l'interfaccia e fare clic su **Modifica**.

PASSAGGIO 7 Selezionare Smartport automatico nel campo **Applicazione Smartport.**

PASSAGGIO 8 Selezionare o deselezionare **Stato persistente**, se lo si desidera.

PASSAGGIO 9 Fare clic su **Applica**.

Flusso di lavoro 2: per configurare un'interfaccia come Smartport statico, attenersi alla seguente procedura:

PASSAGGIO 1 Per attivare la funzione Smartport sull'interfaccia, aprire la pagina Smartport > Impostazioni interfaccia.

PASSAGGIO 2 Selezionare l'interfaccia e fare clic su **Modifica**.

PASSAGGIO 3 Selezionare il tipo di Smartport che deve essere assegnato all'interfaccia nel campo **Applicazione Smartport**.

PASSAGGIO 4 Impostare i parametri macro come richiesto.

PASSAGGIO 5 Fare clic su **Applica**.

Flusso di lavoro 3: per regolare le impostazioni predefinite per i parametri macro Smartport e/o associare una coppia macro definita dall'utente a un tipo di Smartport, attenersi alla seguente procedura:

Seguendo tale procedura, è possibile ottenere quanto segue:

- Visualizzare la sorgente macro.
- Modificare le impostazioni predefinite dei parametri.
- Ripristinare le impostazioni predefinite dei parametri alle impostazioni di fabbrica.
- Associare una coppia macro definita dall'utente (una macro e l'anti-macro corrispondente) a un tipo di Smartport.

1. Aprire la pagina Smartport > Impostazioni tipo Smartport.
2. Selezionare il tipo di Smartport.
3. Scegliere **Visualizza sorgente macro** per visualizzare la macro Smartport corrente associata al tipo di Smartport selezionato.
4. Fare clic su **Modifica** per aprire una nuova finestra in cui è possibile associare macro definite dall'utente al tipo di Smartport selezionato e/o modificare i valori predefiniti dei parametri nelle macro associate a quel tipo di Smartport. Tali valori predefiniti dei parametri vengono utilizzati quando Smartport automatico applica il tipo di Smartport selezionato (se applicabile) a un'interfaccia.
5. Nella pagina Modifica, modificare i campi.
6. Scegliere **Applica** per eseguire nuovamente la macro se i parametri sono stati modificati, oppure **Ripristina impostazioni predefinite** per ripristinare i valori predefiniti dei parametri per le macro incorporate, se richiesto.

Flusso di lavoro 4: per eseguire nuovamente una macro Smartport che ha generato un errore, attenersi alla seguente procedura:

PASSAGGIO 1 Nella pagina Impostazioni interfaccia, selezionare un'interfaccia con tipo di Smartport sconosciuto.

PASSAGGIO 2 Scegliere **Mostra Diagnostica** per visualizzare il problema.

PASSAGGIO 3 Risolvere il problema e correggerlo. Vedere il suggerimento sulla risoluzione dei problemi indicato di seguito.

PASSAGGIO 4 Scegliere **Modifica.** Viene visualizzata una nuova finestra nella quale è possibile fare clic su **Ripristina** per reimpostare l'interfaccia.

PASSAGGIO 5 Tornare alla pagina principale e riapplicare la macro selezionando **Riapplica** (per qualsiasi dispositivo al di fuori di switch, router o AP) o **Riapplica macro Smartport** (per switch, router o AP) per eseguire la macro Smartport sull'interfaccia.

Un secondo metodo per reimpostare interfacce sconosciute singole o multiple è il seguente:

PASSAGGIO 1 Nella pagina Impostazioni interfaccia, selezionare la casella di controllo Tipo di porta uguale a.

PASSAGGIO 2 Selezionare *Sconosciuto* e fare clic su **Vai**.

PASSAGGIO 3 Scegliere **Ripristina tutti gli Smartport sconosciuti**. Quindi riapplicare la macro come descritto sopra.

SUGGERIMENTO Il problema alla macro potrebbe derivare da un conflitto con una configurazione sull'interfaccia precedente all'applicazione della macro (si rileva spesso con le impostazioni di sicurezza e i controlli storm), da un tipo di porta errato, da un errore di battitura o di comando nella macro definita dall'utente, oppure da un'impostazione di parametro non valida. Né il tipo né il limite dei parametri vengono verificati prima del tentativo di applicare la macro; quindi, un input errato o non valido per il valore di un parametro sarà quasi certamente causa di errore al momento di applicare la macro.

Configurare Smartport tramite l'interfaccia basata su Web

La funzione Smartport viene configurata nelle pagine Smartport > Proprietà Impostazioni tipo SmartPort e Impostazioni interfaccia.

Per la configurazione della VLAN voce, vedere **VLAN voce**.

Per la configurazione di LLDP/CDP vedere, rispettivamente, le sezioni **Configurazione di LLDP** e **Configurazione CDP**.

Proprietà Smartport

Per configurare la funzione Smartport a livello globale, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Smartport > Proprietà**.

PASSAGGIO 2 Immettere i parametri.

- **Smartport automatico amministrativo**: consente di abilitare o disabilitare a livello globale Smartport automatico. Sono disponibili le seguenti opzioni:
  - *Disattiva*: selezionare questa opzione per disattivare la funzione Smartport automatico sul dispositivo.
  - *Attiva*: selezionare questa opzione per attivare la funzione Smartport automatico sul dispositivo.
  - *Attiva con VLAN voce automatica*: questa opzione attiva la funzione Smartport automatico ma la attiva solo quando viene abilitata la VLAN voce automatica. L'impostazione predefinita è Attiva con VLAN voce automatica.
- **Smartport automatico operativo**: indica lo stato dello smartport automatico.
- **Metodo rilevamento dispositivo Smartport automatico**: scegliere se i pacchetti CDP, LLDP o entrambi i tipi in arrivo sono utilizzati per rilevare il tipo di Smartport dei dispositivi in collegamento. Deve esserne selezionato almeno uno per consentire a Smartport automatico di identificare i dispositivi.
- **Stato CDP operativo**: visualizza lo stato operativo di CDP. Attiva CDP se Smartport automatico deve rilevare il tipo di Smartport basato sull'annuncio CDP.
- **Stato LLDP operativo**: visualizza lo stato operativo di LLDP. Attiva LLDP se Smartport automatico deve rilevare il tipo di Smartport basato sull'annuncio LLDP/LLDP-MED.
- **Rilevamento dispositivo Smartport automatico**: selezionare ogni tipo di dispositivo per il quale Smartport automatico può assegnare tipi di Smartport alle interfacce. Se questa opzione non è selezionata, Smartport automatico non assegnerà quel tipo di Smartport ad alcuna interfaccia.

PASSAGGIO 3 Fare clic su **Applica**. In questo modo si impostano i parametri globali Smartport sul dispositivo.

Impostazioni tipo Smartport

Utilizzare la pagina Impostazioni tipo Smartport per modificare le impostazioni relative al tipo di Smartport e visualizzare la sorgente macro.

Per impostazione predefinita, ogni tipo di Smartport è associato a una coppia di macro Smartport integrate. Vedere **Tipi di Smartport** per ulteriori informazioni sulle macro a confronto con le anti-macro. In alternativa, è possibile associare al tipo di Smartport la propria coppia di macro definite dall'utente con configurazioni personalizzate. Le macro definite dall'utente possono essere preparate solo tramite CLI. Per i dettagli, vedere la Guida di riferimento rapido CLI.

Le macro integrate o definite dall'utente possono presentare dei parametri. Le macro integrate possono avere fino a tre parametri.

La modifica di questi parametri per i tipi di Smartport applicati dalla funzione Smartport automatico nella pagina Impostazioni tipo Smartport configura i valori predefiniti per questi parametri. Tali valori predefiniti vengono utilizzati da Smartport automatico.

NOTA Modifiche ai tipi di Smartport automatico provocano l'applicazione delle nuove impostazioni alle interfacce che sono già state assegnate a quel tipo da Smartport automatico. In questo caso, l'associazione di una macro non valida o l'impostazione di un parametro predefinito non valido fa passare allo stato Sconosciuto tutte le porte di questo tipo di Smartport.

PASSAGGIO 1 Scegliere **Smartport > Impostazioni tipo Smartport**.

PASSAGGIO 2 Per visualizzare la macro Smartport associata a un tipo di Smartport, selezionare un tipo di Smartport e fare clic su **Visualizza sorgente macro**.

PASSAGGIO 3 Per modificare i parametri di una macro o assegnare una macro definita dall'utente, selezionare un tipo di Smartport e fare clic su **Modifica**.

PASSAGGIO 4 Immettere i campi:

- **Tipo di porta**: selezionare un tipo di Smartport.
- **Nome macro**: visualizza il nome della macro Smartport attualmente associata al tipo di Smartport.
- **Tipo di macro**: indicare se la coppia macro e anti-macro associata a questo tipo di Smartport è di tipo integrata o definita dall'utente.
- **Macro definita dall'utente**: se lo si desidera, selezionare la macro definita dall'utente che deve essere associata al tipo di Smartport selezionato. La macro deve essere già stata accoppiata con un'anti-macro.

L'accoppiamento delle due macro viene eseguito in base al nome e viene descritto nella sezione Macro Smartport.

- **Parametri macro**: mostra i seguenti campi per i tre parametri della macro:
  - *Nome parametro*: nome del parametro nella macro.
  - *Valore parametro*: valore corrente del parametro nella macro. È modificabile.
  - *Descrizione parametro*: descrizione del parametro.

  È possibile ripristinare i valori predefiniti dei parametri facendo clic su **Ripristina impostazioni predefinite**.

PASSAGGIO 5 Scegliere **Applica** per salvare le modifiche alla Configurazione di esecuzione. Se la macro Smartport e/o i valori dei parametri associati con il tipo di Smartport vengono modificati, Smartport automatico riapplica automaticamente la macro alle interfacce attualmente assegnate con il tipo di Smartport tramite Smartport automatico. Smartport automatico non applica le modifiche alle interfacce che sono state assegnate staticamente a un tipo di Smartport.

NOTA Non esiste un metodo per convalidare i parametri delle macro perché non presentano un'associazione per tipo. Di conseguenza, a questo punto ogni voce è valida. Tuttavia, i valori non validi dei parametri possono provocare errori quando il tipo di Smartport viene assegnato a un'interfaccia, applicando la macro associata.

Impostazioni interfaccia Smartport

Utilizzare la pagina Impostazioni interfaccia per eseguire le seguenti operazioni:

- Applicare staticamente un tipo di Smartport specifico a un'interfaccia con valori interfaccia specifici per i parametri della macro.
- Abilitare Smartport automatico su un'interfaccia.
- Eseguire la diagnosi di una macro Smartport che ha generato un errore al momento dell'applicazione e ha causato il passaggio del tipo di Smartport allo stato Sconosciuto.
- Riapplicare una macro Smartport dopo che questa ha generato un errore su uno dei seguenti tipi di interfaccia: switch, router e AP. È previsto che le necessarie correzioni siano state apportate prima di fare clic su **Riapplica**. Per la risoluzione dei problemi vedere l'area del flusso di lavoro nella sezione **Attività comuni con Smartport**.

- Riapplicare una macro Smartport a un'interfaccia. In alcune circostanze, può essere necessario applicare nuovamente una macro Smartport in modo che la configurazione di una interfaccia sia aggiornata. Ad esempio, se si riapplica una macro Smartport dispositivo su un'interfaccia dispositivo, l'interfaccia diventa membro delle VLAN create dopo l'ultima applicazione della macro. Per determinare se la riapplicazione di una macro ha effetto sull'interfaccia, è necessario conoscere le configurazioni attuali del dispositivo e la definizione della macro.
- Reimpostare interfacce sconosciute. Consente di impostare la modalità delle interfacce sconosciute su Predefinita.

Per applicare una macro Smartport, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Smartport > Impostazioni interfaccia**.

Riapplicare la macro Smartport associata nei seguenti modi:

- Selezionare un gruppo di tipi di Smartport (switch, router o AP) e fare clic su **Riapplica macro Smartport.** Le macro vengono applicate a tutti i tipi di interfaccia selezionati.
- Selezionare un'interfaccia attiva e fare clic su **Riapplica** per riapplicare l'ultima macro applicata all'interfaccia.

  L'operazione **Riapplica** consente di aggiungere l'interfaccia a tutte le VLAN appena create.

PASSAGGIO 2 Diagnostica Smartport.

Se una macro Smartport non funziona correttamente, il tipo di Smartport dell'interfaccia sarà Sconosciuto. Selezionare un'interfaccia di tipo Sconosciuto e fare clic su **Mostra diagnostica.** In questo modo verrà visualizzato il comando durante il quale l'applicazione della macro non è riuscita. Per la risoluzione dei problemi vedere l'area del flusso di lavoro nella sezione **Attività comuni con Smartport**. Dopo aver risolto il problema, si può procedere con la riapplicazione della macro.

PASSAGGIO 3 Ripristino delle impostazioni predefinite su tutte le interfacce sconosciute.

- Selezionare la casella di controllo *Tipo di porta uguale a*.
- Selezionare *Sconosciuto* e fare clic su **Vai**.

- Scegliere **Ripristina tutti gli Smartport sconosciuti**. Quindi riapplicare la macro come descritto sopra. Questa operazione consente di ripristinare il tipo Sconosciuto su tutte le interfacce, di conseguenza su tutte le interfacce vengono ripristinate le impostazioni predefinite. Dopo aver corretto l'errore nella macro o nella configurazione dell'interfaccia corrente o in entrambe, può essere applicata una nuova macro.

NOTA La reimpostazione dell'interfaccia di tipo Sconosciuto non ripristina la configurazione eseguita dalla macro che ha generato un errore. Questo intervento di pulitura deve essere eseguito manualmente.

Per assegnare un tipo di Smartport a un'interfaccia o attivare Smartport automatico nell'interfaccia, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare un'interfaccia e fare clic su **Modifica**.

PASSAGGIO 2 Immettere i campi:

- **Interfaccia**: selezionare una porta o un LAG.
- **Tipo Smartport**: visualizza il tipo di Smartport attualmente assegnato alla porta/al LAG.
- **Applicazione Smartport**: selezionare il tipo di Smartport dalla casella a discesa Applicazione Smartport.
- **Metodo applicazione Smartport**: se è selezionato, Smartport automatico assegna automaticamente il tipo di Smartport in base all'annuncio CDP e/o LLDP ricevuto dai dispositivi in collegamento. Inoltre, applica la corrispondente macro Smartport. Per assegnare staticamente un tipo di Smartport e applicare la macro Smartport corrispondente all'interfaccia, selezionare il tipo di Smartport desiderato.
- **Stato persistente**: selezionare questa opzione per attivare lo Stato persistente. Se questa opzione è attivata, l'associazione di un tipo di Smartport a un'interfaccia viene mantenuta anche se l'interfaccia viene disattivata o il dispositivo viene riavviato. Lo Stato persistente è applicabile solo se l'applicazione Smartport dell'interfaccia è Smartport automatico. L'attivazione dello Stato persistente su un'interfaccia elimina il ritardo nel rilevamento del dispositivo, che altrimenti si verificherebbe.
- **Parametri macro**: presenta i seguenti campi fino a tre parametri nella macro:
  - *Nome parametro*: nome del parametro nella macro.
  - *Valore parametro*: valore corrente del parametro nella macro. È modificabile.

- *Descrizione parametro*: descrizione del parametro.

PASSAGGIO 3 Scegliere **Ripristina** per ripristinare le impostazioni predefinite di un'interfaccia, se è in stato Sconosciuto (a seguito di un'applicazione macro non riuscita). La macro non può essere riapplicata sulla pagina principale.

PASSAGGIO 4 Scegliere **Applica** per aggiornare le modifiche e assegnare il tipo di Smartport all'interfaccia.

Macro Smartport integrate

Di seguito viene descritta la coppia di macro integrate per ogni tipo di Smartport. Per ogni tipo di Smartport esistono una macro per configurare l'interfaccia e una anti-macro per rimuovere la configurazione.

Viene fornito il codice macro per i seguenti tipi di Smartport:

- **desktop**
- **printer**
- **ospite**
- **server**
- **host**
- **ip_camera**
- **ip_phone**
- **ip_phone_desktop**
- **switch**
- **router**
- **ap**

desktop

```
[desktop]
#interface configuration, for increased network security and reliability when
connecting a desktop device, such as a PC, to a switch port.
#macro description Desktop
#macro keywords $native_vlan $max_hosts
#
```

```
#macro key description:   $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
#                         $max_hosts: Il numero massimo di dispositivi
consentiti sulla porta
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_desktop

```
[no_desktop]
#macro description No Desktop
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

printer

```
[printer]
#macro description printer
#macro keywords $native_vlan
#
```

```
#macro key description: $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_printer

```
[no_printer]
#macro description No printer
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

guest

```
[guest]
#macro description guest
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
#Default Values are
```

```
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_guest]]

```
[no_guest]
#macro description No guest
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

server

```
[server]
#macro description server
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
#                         $max_hosts: Il numero massimo di dispositivi
consentiti sulla porta
#Default Values are
#$native_vlan = Default VLAN
```

```
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_server

```
[no_server]
#macro description No server
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
spanning-tree portfast auto
#
@
```

host

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
#                         $max_hosts: Il numero massimo di dispositivi
consentiti sulla porta
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
```

```
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_host

```
[no_host]
#macro description No host
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_camera

```
[ip_camera]
#macro description ip_camera
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
#Default Values are
#$native_vlan = Default VLAN
#
switchport mode access
switchport access vlan $native_vlan
#
```

```
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_camera

```
[no_ip_camera]
#macro description No ip_camera
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone

```
[ip_phone]
#macro description ip_phone
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
#                        $voice_vlan: L'identificativo voce VLAN
#                         $max_hosts: Il numero massimo di dispositivi
consentiti sulla porta
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
```

```
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone

```
[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: L'identificativo voce VLAN
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone_desktop

```
[ip_phone_desktop]
#macro description ip_phone_desktop
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
#                        $voice_vlan: L'identificativo voce VLAN
#                         $max_hosts: Il numero massimo di dispositivi
consentiti sulla porta
```

```
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone_desktop

```
[no_ip_phone_desktop]
#macro description no ip_phone_desktop
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: L'identificativo voce VLAN
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

switch

```
[switch]
#macro description switch
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
#                        $voice_vlan: L'identificativo voce VLAN
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_switch

```
[no_switch]
#macro description No switch
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: L'identificativo voce VLAN
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

router

```
[router]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
#                        $voice_vlan: L'identificativo voce VLAN
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
```

```
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree link-type point-to-point
#
@
```

no_router

```
[no_router]

#macro description No router

#macro keywords $voice_vlan

#

#macro key description:   $voice_vlan: L'identificativo voce VLAN

#

no smartport switchport trunk native vlan

smartport switchport trunk allowed vlan remove all

#

no smartport storm-control broadcast enable

no smartport storm-control broadcast level

#

no spanning-tree link-type

#

@
```

ap

```
[ap]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: Il messaggio elimina tag da VLAN che
verrà configurato sulla porta
```

13

Gestione delle porte: PoE

La funzione PoE (Power over Ethernet) è disponibile solo nei dispositivi basati su PoE. Per un elenco dei dispositivi basati su PoE, fare riferimento alla sezione **Modelli dispositivo**.

In questa sezione viene descritto come utilizzare la funzione PoE

NOTA La funzione PoE non è abilitata sui dispositivi SG500XG/ESW2-550X.

Vengono trattati i seguenti argomenti:

- **PoE sul dispositivo**
- **Configurazione delle proprietà di PoE**
- **Configurazione delle impostazioni PoE**

PoE sul dispositivo

Un dispositivo PoE è un PSE (Power Sourcing Equipment) che fornisce alimentazione elettrica ai dispositivi PD (Powered Devices) connessi tramite cavi in rame esistenti senza interferire con il traffico di rete, aggiornare la rete fisica o modificare l'infrastruttura di rete.

Per informazioni sul supporto PoE ai vari modelli, vedere **Modelli dispositivo**.

Funzioni PoE

PoE fornisce le seguenti funzioni:

- Elimina la necessità di eseguire alimentazione 110/220 V CA su tutti i dispositivi di una LAN cablata.
- Rimuove la necessità di posizionare tutti i dispositivi di rete accanto a fonti di alimentazione.

- Elimina la necessità di distribuire sistemi di cablaggio doppi in un'azienda riducendo notevolmente i costi di installazione.

Power over Ethernet può essere utilizzato in qualsiasi rete aziendale che distribuisce dispositivi a relativamente bassa alimentazione connessi alla LAN Ethernet, come:

- Telefoni IP
- Access point wireless
- Gateway IP
- Dispositivi di monitoraggio remoti audio e video

Funzionamento di PoE

PoE viene implementato nelle seguenti fasi:

- Rilevamento: invia impulsi speciali nel cavo in rame. Quando un dispositivo PoE viene posizionato sull'altra estremità, quel dispositivo risponde a questi impulsi.
- Classificazione: la negoziazione tra PSE (Power Sourcing Equipment) e PD (Powered Device) ha inizio dopo la fase di Rilevamento. Durante la negoziazione, il PD specifica la sua classe, cioè la quantità di alimentazione massima che consuma il PD.
- Assorbimento: al termine della fase di classificazione, PSE fornisce alimentazione al PD. Se il PD supporta PoE ma senza classificazione, si assume che sia di classe 0 (il massimo). Se un dispositivo PD cerca di consumare più alimentazione di quella consentita dallo standard, PSE interrompe la fornitura di alimentazione alla porta.

PoE supporta due modalità:

- **Limite porta**: l'alimentazione massima che il dispositivo può fornire è limitata al valore configurato dall'amministratore di sistema, indipendentemente dal risultato di classificazione.
- **Limite di alimentazione classe**: l'alimentazione massima che il dispositivo può fornire viene determinata dai risultati della fase Classificazione. Significa che viene impostato come in base alla richiesta del client.

Considerazioni sulla configurazione di PoE

Nella funzione PoE è necessario tenere in considerazione due fattori:

- La quantità di alimentazione che PSE può fornire
- La quantità di alimentazione che PD sta cercando di consumare al momento

È possibile decidere quanto segue:

- Alimentazione massima che un PSE può fornire a PD.
- Durante il funzionamento del dispositivo, è possibile passare da Limite di alimentazione classe a Limite porta e vice versa. I valori di alimentazione per porta configurati per la modalità Limite porta vengono conservati.

  NOTA Se si cambia la modalità da Limite di alimentazione classe a Limite porta e viceversa quando il dispositivo è operativo, il dispositivo alimentato verrà riavviato.
- Il limite della porta massimo consentito come il limite numerico in base alla porta in mW (modalità Limite porta).
- Per generare una trap quando PD cerca di consumare troppo e a quale percentuale di alimentazione massima viene generata questa trap.

L'hardware specifico di PoE rileva automaticamente la classe PD e il suo limite di alimentazione in base alla classe del dispositivo connesso a ogni porta specifica (modalità Limite classe).

Se in qualsiasi momento della connessione un PD associato richiede più energia al dispositivo rispetto a quanto consentito dall'allocazione configurata (a prescindere dal fatto che sia selezionata la modalità Limite classe o Limite porta), il dispositivo esegue quanto segue:

- Mantiene lo stato attivo/inattivo del collegamento alla porta PoE
- Disattiva la distribuzione di alimentazione alla porta PoE
- Registra il motivo della disattivazione dell'alimentazione
- Genera una trap SNMP

  NOTA Quando un dispositivo PoE di tensione inferiore è collegato a un dispositivo della serie SG500 con PoE ed è collegato tramite porte abilitate per PoE alle due estremità della connessione, il dispositivo di tensione inferiore smette di alimentare qualsiasi dispositivo supportato. Per evitare che ciò accada, disattivare il supporto PoE su SG500 o utilizzare una porta non-PoE.

ATTENZIONE Durante il collegamento di switch in grado di erogare PoE, tenere presente quanto segue:

I modelli PoE degli switch delle serie Sx200, Sx300 e SF500 sono i dispositivi PSE (Power Sourcing Equipment, apparecchiature di alimentazione elettrica), capaci di erogare corrente in CC verso dispositivi PD (Powered Devices, dispositivi alimentati) collegati. Tali dispositivi includono telefoni VoIP, fotocamere IP e access point wireless. Gli switch PoE sono in grado di rilevare e fornire corrente a dispositivi alimentati PoE precedenti allo standard. Considerato il supporto di PoE preesistenti, un dispositivo PoE che agisce da PSE potrebbe erroneamente rilevare e alimentare un PSE collegato, compresi altri switch PoE, come un dispositivo PD preesistente.

Sebbene gli switch PoE Sx200/300/500 siano PSE (e come tali devono essere alimentati in CA), potrebbero essere alimentati come dispositivi PD preesistenti da un altro PSE a causa di rilevamenti errati. In tal caso, il dispositivo PoE non funziona correttamente e potrebbe non riuscire ad alimentare in modo appropriato i dispositivi PD collegati.

Per impedire i rilevamenti errati, disattivare il PoE sulle porte degli switch PoE utilizzate per collegare i PSE. Prima di collegarlo a un dispositivo PoE, accendere il dispositivo PSE. Quando un dispositivo viene erroneamente rilevato come dispositivo PD, scollegarlo dalla porta PoE, quindi spegnere e accendere l'alimentazione CA del dispositivo prima di ricollegarlo alle porte PoE.

Configurazione delle proprietà di PoE

Nella pagina Proprietà PoE è possibile selezionare la modalità PoE Limite porta o Limite classe e specificare le trap PoE da generare.

Queste impostazioni vengono immesse in anticipo. Quando PD si connette e consuma alimentazione, potrebbe consumare molto meno rispetto all'alimentazione massima consentita.

Durante il riavvio dell'accensione, l'inizializzazione e la configurazione di sistema, la potenza di uscita viene disattivata per garantire che i PD non vengano danneggiati.

Per configurare PoE sul dispositivo e monitorare l'utilizzo dell'alimentazione corrente, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione porte> PoE > Proprietà**.

PASSAGGIO 2 Immettere i valori dei seguenti campi:

- **Modalità di alimentazione**: selezionare una delle seguenti opzioni:
  - *Limite porta*: il limite di alimentazione massimo per ogni porta configurato dall'utente.
  - *Limite classe*: il limite di alimentazione massima per porta viene determinato dalla classe del dispositivo, risultante dalla fase Classificazione.

  NOTA Se si passa dalla modalità Limite porta alla modalità Limite classe o viceversa, è necessario disattivare le porte PoE e riattivarle dopo aver modificato la configurazione di alimentazione.
- **Trap**: attivare o disattivare trap. Se le trap sono attivate, è necessario attivare anche SNMP e configurare almeno un Destinatario notifica SNMP.
- **Soglia trap di alimentazione**: immettere la soglia di utilizzo, cioè una percentuale del limite di alimentazione. Se l'alimentazione supera questo valore, viene attivato un allarme.

I seguenti contatori vengono visualizzati per ciascun dispositivo o per tutte le unità dello stack:

- **Potenza nominale**: la quantità totale di potenza che il dispositivo può fornire a tutti i PD connessi.
- **Potenza assorbita**: quantità di alimentazione che le porte PoE stanno consumando.
- **Potenza disponibile**: potenza nominale meno la quantità di alimentazione consumata.

PASSAGGIO 3 Scegliere **Applica** per salvare le proprietà PoE.

Configurazione delle impostazioni PoE

Nella pagina Impostazioni PoE vengono visualizzate le informazioni PoE di sistema per l'attivazione di PoE nelle interfacce e il monitoraggio dell'utilizzo corrente dell'alimentazione e il limite di alimentazione massimo per porta.

NOTA È possibile configurare PoE sul dispositivo per un periodo specifico. Questa funzione consente di definire per ogni porta i giorni della settimana e gli orari in cui PoE è attivato. Al di fuori dei giorni e degli orari stabiliti, PoE è disattivato. Per utilizzare questa funzione, è necessario specificare prima un intervallo temporale nella pagina **Intervallo di tempo**.

Fare clic su **Gestione porte > PoE > Impostazioni**.

In questa pagina l'alimentazione per porta viene limitata in due modi in base alla modalità di alimentazione:

- **Limite porta:** l'alimentazione è limitata a un wattaggio specifico. Affinché queste impostazioni siano attive, il sistema deve essere in modalità Limite porta PoE. Questa modalità è configurata nella pagina Proprietà PoE.

  Quando l'alimentazione consumata nella porta supera il limite porta, l'alimentazione della porta viene disattivata.

- **Limite classe:** l'alimentazione viene limitata in base alla classe del PD connesso. Affinché queste impostazioni siano attive, il sistema deve essere in modalità Limite classe PoE. Questa modalità è configurata nella pagina Proprietà PoE.

  Quando l'alimentazione consumata nella porta supera il limite classe, l'alimentazione della porta viene disattivata.

Esempio di priorità PoE:

Dato: un dispositivo a 48 porte eroga corrente per un totale di 375 Watt.

L'amministratore configura tutte le porte per allocare fino a 30 Watt. Per 48 volte si verifica che 30 porte raggiungono 1440 Watt, ossia un valore troppo alto. Non riuscendo ad alimentare a sufficienza tutte le porte, il dispositivo fornisce alimentazione in base alla priorità.

L'amministratore determina la priorità di ogni porta, assegnando la quantità di alimentazione da erogare.

La priorità viene specificata nella pagina Impostazioni PoE.

Vedere **Modelli dispositivo** per la descrizione dei modelli di dispositivo che supportano PoE e la potenza massima che può essere assegnata alle porte PoE.

Per configurare le impostazioni della porta PoE, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione porte > PoE > Impostazioni**. Di seguito viene riportato l'elenco dei campi per la modalità di alimentazione Limite porta. I campi cambiano leggermente per la Modalità di alimentazione Limite classe.

PASSAGGIO 2 Selezionare una porta e Scegliere **Modifica.** Di seguito viene riportato l'elenco dei campi per la Modalità di alimentazione Limite porta. I campi cambiano leggermente per la Modalità di alimentazione Limite classe.

PASSAGGIO 3 Immettere il valore del seguente campo:

- **Interfaccia**: selezionare la porta da configurare.
- **Stato amministrativo PoE**: attivare o disattivare PoE nella porta.
- **Intervallo di tempo**: selezionare questa opzione per attivare PoE sulla porta.
- **Nome intervallo di tempo**: se l'opzione Intervallo di tempo è selezionata, scegliere l'intervallo di tempo desiderato. Gli intervalli di tempo vengono definiti nella pagina **Intervallo di tempo**.
- **Livello di priorità alimentazione**: selezionare la priorità della porta: bassa, alta o critica da utilizzare quando l'alimentazione è bassa. Per esempio, se l'alimentazione viene eseguita al 99% di utilizzo e la porta 1 ha una priorità alta ma la porta 3 ha una priorità bassa, la porta 1 riceve alimentazione mentre alla porta 3 potrebbe essere negata l'alimentazione.
- **Distribuzione alimentazione amministrativa**: questo campo viene visualizzato solo se la modalità di alimentazione impostata nella pagina Proprietà PoE è Limite porta. Se la modalità di alimentazione è Limite alimentazione, inserire la potenza assegnata alla porta in milliwatt.
- **Distribuzione alimentazione massima**: questo campo viene visualizzato solo se la modalità di alimentazione impostata nella pagina Proprietà PoE è Limite alimentazione. Indica la massima quantità di alimentazione consentita su questa porta.

- **Classe**: questo campo viene visualizzato solo se la modalità di alimentazione impostata nella pagina Proprietà PoE è Limite classe. La classe determina il livello di alimentazione:

Classe	Alimentazione massima distribuita dalla porta del dispositivo
0	15,4 watt
1	4,0 watt
2	7,0 watt
3	15,4 watt
4	30,0 watt

- **Assorbimento**: viene visualizzata la quantità di alimentazione in milliwatt assegnata al dispositivo alimentato connesso all'interfaccia selezionata.
- **Contatore sovraccarico**: viene visualizzato il numero totale di volte in cui si verifica un sovraccarico di alimentazione.
- **Contatore breve**: visualizza il numero totale di volte in cui si verifica un calo di alimentazione.
- **Contatore respinto**: visualizza il numero di volte in cui il dispositivo alimentato è stato respinto.
- **Contatore assente**: visualizza il numero di volte in cui l'alimentazione al dispositivo alimentato è stata interrotta perché il dispositivo non è stato più rilevato.
- **Contatore firme non valido**: visualizza le volte in cui è stata ricevuta una firma non valida. Le firme sono il mezzo attraverso cui il dispositivo alimentato identifica se stesso nel PSE. Le firme vengono generate durante il rilevamento, la classificazione o la manutenzione del dispositivo alimentato.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni PoE della porta vengono scritte nel file di Configurazione di esecuzione.

14

Gestione VLAN

In questa sezione vengono illustrati i seguenti argomenti:

- **Reti VLAN**
- **Configurazione delle impostazioni VLAN predefinite**
- **Creazione di VLAN**
- **Configurazione delle impostazioni interfaccia VLAN**
- **Definizione di Appartenenza a VLAN**
- **Impostazioni GVRP**
- **Gruppi VLAN**
- **VLAN voce**
- **VLAN TV multicast basata su porta di accesso**
- **VLAN TV multicast basata su porta del cliente**

Reti VLAN

Una VLAN è un gruppo logico di porte che consente ai dispositivi ad essa associati di comunicare l'uno con l'altro sul livello MAC di Ethernet, indipendentemente dal segmento LAN fisico della rete connessa a cui sono collegati.

Descrizione VLAN

Ogni VLAN è configurata con un VID (ID VLAN) univoco con un valore compreso tra 1 e 4094. Una porta di un dispositivo in una rete connessa è un membro di una VLAN se può inviare dati a e ricevere dati dalla VLAN. Una porta è un membro senza tag di una VLAN se tutti i pacchetti destinati a quella porta della VLAN non hanno nessun tag VLAN. Una porta è un membro con tag di una VLAN se tutti i pacchetti destinati a quella porta della VLAN hanno un tag VLAN. Una porta può essere membro di una VLAN senza tag e anche di varie VLAN con tag.

Una porta in modalità Accesso VLAN può far parte solo di una VLAN. Se è in modalità Generale o Trunk, la porta può far parte di una o più VLAN.

Le VLAN affrontano problemi relativi alla sicurezza e alla scalabilità. Il traffico di una VLAN rimane all'interno della VLAN e termina nei dispositivi della VLAN. Facilita inoltre la configurazione di rete connettendo logicamente dispositivi senza riposizionarli fisicamente.

Se un frame ha tag VLAN, a ogni frame Ethernet viene aggiunto un tag VLAN a quattro byte. Il tag contiene un ID VLAN tra 1 e 4094 e un tag di priorità VLAN (VPT) tra 0 e 7. Per i dettagli su VPT, vedere **QoS**.

Quando un frame immette un dispositivo in grado di rilevare reti VLAN, viene classificato come appartenente a una VLAN, in base al tag VLAN a quattro byte del frame.

Se nel frame non ci sono tag VLAN o se il frame ha solo tag di priorità, il frame viene classificato per la VLAN basata sul PVID (identificatore VLAN della porta) configurato sulla porta d'ingresso in cui il frame viene ricevuto.

Il frame viene eliminato sulla porta d'ingresso se Filtro traffico in ingresso è attivato e la porta d'ingresso non è un membro della VLAN a cui appartiene il pacchetto. Un frame viene considerato come con tag di priorità solo se VID nel suo tag VLAN è 0.

I frame che appartengono a una VLAN rimangono nella VLAN. A questo scopo è necessario inviare o reindirizzare un frame solo alle porte di uscita membri della VLAN di destinazione. Una porta di uscita può essere un membro con tag o senza tag di una VLAN.

La porta di uscita:

- Aggiunge un tag VLAN al frame se la porta di uscita è un membro con tag della VLAN di destinazione e il frame originale non ha un tag VLAN.
- Rimuove il tag VLAN dal frame se la porta di uscita è un membro senza tag della VLAN di destinazione e il frame originale ha un tag VLAN.

Ruoli VLAN

Le VLAN funzionano a Livello 2. Tutto il traffico della VLAN (unicast/broadcast/multicast) rimane in quella VLAN. I dispositivi associati a diverse VLAN non hanno una connettività diretta l'uno verso l'altro sul livello MAC di Ethernet. I dispositivi di VLAN diverse possono comunicare l'un l'altro solo tramite i router Livello 3. Un router IP, per esempio, deve eseguire il routing del traffico IP tra le VLAN se ogni VLAN rappresenta una subnet IP.

Il router IP deve essere un router tradizionale in cui ogni interfaccia si connette solo a una VLAN. Il traffico verso e da un router IP tradizionale deve essere una VLAN senza tag. Il router IP può essere un router in grado di rilevare reti VLAN in cui ogni interfaccia può connettersi a una o più VLAN. Il traffico verso e da un router IP in grado di rilevare reti VLAN può essere una VLAN con o senza tag.

I dispositivi in grado di rilevare VLAN si scambiano l'un l'altro informazioni su VLAN utilizzando il protocollo GVRP (Generic VLAN Registration Protocol). Di conseguenza, le informazioni sulla VLAN vengono propagate tramite una rete connessa.

È possibile creare VLAN in un dispositivo dinamicamente o statisticamente in base alle informazioni su GVRP scambiate dai dispositivi. Una VLAN può essere statica o dinamica (da GRVP), ma non entrambe. Per ulteriori informazioni su GVRP, fare riferimento alla sezione Impostazioni GVRP.

Alcune VLAN possono avere altri ruoli, inclusi:

- VLAN voce: per ulteriori informazioni, fare riferimento alla sezione VLAN voce.
- VLAN ospite: impostata nella pagina Modifica autenticazione VLAN.
- VLAN predefinita: per ulteriori informazioni, fare riferimento alla sezione Configurazione delle impostazioni VLAN predefinite.
- Gestione VLAN (nei sistemi in modalità di sistema Livello 2): per ulteriori informazioni, fare riferimento alla sezione Indirizzo IP di livello 2.

QinQ

QinQ fornisce isolamento tra le reti dei service provider e le reti dei clienti. Il dispositivo è un bridge provider che supporta un'interfaccia di servizio con c-tag basata su porta.

Con QinQ, il dispositivo aggiunge un tag ID noto come S-tag (Service Tag) per reindirizzare il traffico sulla rete. L'S-tag viene utilizzato per separare il traffico tra clienti diversi, pur mantenendo i tag VLAN del cliente.

Il traffico dei clienti è incapsulato con un S-tag con TPID 0x8100, indipendentemente dal fatto di essere all'origine con c-tag o senza tag. L'S-tag consente a questo traffico di essere trattato come un aggregato nell'ambito di una rete connessa provider, dove il bridging è basato solo sul S-VID (VID dell'S-tag).

L'S-Tag viene conservato, mentre il traffico è reindirizzato attraverso le infrastrutture del provider di servizi di rete e viene successivamente rimosso da un dispositivo di uscita.

Un ulteriore vantaggio di QinQ è che non vi è alcuna necessità di configurare i dispositivi edge dei clienti.

La funzione QinQ viene abilitata nella pagina Gestione VLAN > Impostazioni interfaccia.

Flusso di lavoro della configurazione di VLAN

Per configurare le VLAN, attenersi alla seguente procedura:

1. Se richiesto, modificare la VLAN predefinita utilizzando la sezione **Configurazione delle impostazioni VLAN predefinite**.
2. Creare le VLAN richieste utilizzando la sezione **Creazione di VLAN**.
3. Impostare la configurazione desiderata relativa alla VLAN per le porte e abilitare QinQ su un'interfaccia utilizzando la sezione **Configurazione delle impostazioni interfaccia VLAN**.
4. Assegnare le interfacce alle VLAN utilizzando la sezione **Configurazione di Porta a VLAN** o la sezione **Configurazione dell'appartenenza a VLAN**.
5. Visualizzare l'appartenenza alla porta VLAN corrente di tutte le interfacce della sezione **Configurazione dell'appartenenza a VLAN**.
6. Se necessario, configurare i gruppi VLAN come descritto nelle sezioni **Gruppi basati su MAC** e **VLAN basate su protocollo**.
7. Se necessario, configurare la VLAN TV come descritto nelle sezioni **VLAN TV multicast basata su porta di accesso** e **VLAN TV multicast basata su porta del cliente**.

Configurazione delle impostazioni VLAN predefinite

Se si utilizzano le impostazioni predefinite di fabbrica, il dispositivo crea automaticamente la VLAN 1 come la VLAN predefinita, lo stato dell'interfaccia predefinita di tutte le porte è Trunk e tutte le porte sono configurate come membri senza tag della VLAN predefinita.

La VLAN predefinita presenta le seguenti caratteristiche:

- È distinta, non statica/non dinamica e tutte le porte sono membri senza tag per impostazione predefinita.
- Non si può eliminare.
- Non si può darle un'etichetta.
- Non può essere utilizzata per un ruolo speciale come una VLAN non autenticata o una VLAN vocale. Questo è rilevante solo per la VLAN voce attivata per OUI.
- Se una porta non fa più parte di una VLAN, il dispositivo configura automaticamente la porta come membro senza tag della VLAN predefinita. Una porta non è più un membro di una VLAN se questa viene eliminata oppure se la porta viene rimossa dalla VLAN.
- I server RADIUS non possono utilizzare l'assegnazione VLAN dinamica per assegnare la VLAN predefinita ai richiedenti 802.1x.

Quando il VID della VLAN predefinita viene modificato, dopo il salvataggio della configurazione e il riavvio, il dispositivo esegue le azioni seguenti in tutte le porte della VLAN:

- Rimuove l'appartenenza a VLAN delle porte della VLAN predefinita originale (possibile solo dopo il riavvio).
- Modifica il PVID (identificatore VLAN porta) delle porte nel VID della nuova VLAN predefinita.
- L'ID VLAN predefinito originale viene rimosso dal dispositivo. Per essere utilizzato, deve essere creato di nuovo.
- Aggiunge le porte come membri VLAN senza tag della nuova VLAN predefinita.

Per modificare la VLAN predefinita, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **Impostazioni VLAN predefinite**.

PASSAGGIO 2 Immettere il valore del seguente campo:

- **ID VLAN predefinito corrente**: indica l'ID VLAN predefinito corrente.
- **ID VLAN predefinito dopo il riavvio**: immettere un nuovo ID VLAN per sostituire l'ID VLAN predefinito dopo il riavvio.

PASSAGGIO 3 Fare clic su **Applica**.

PASSAGGIO 4 Scegliere **Salva** (nell'angolo superiore destro della finestra) e salvare la Configurazione di esecuzione in Configurazione di avvio.

L'**ID VLAN predefinito dopo il ripristino** diventa l'**ID VLAN predefinito corrente** dopo il riavvio del dispositivo.

Creazione di VLAN

È possibile creare una VLAN che però non ha effetto fino a quando la VLAN non viene associata ad almeno una porta, manualmente o dinamicamente. Le porte devono appartenere sempre a una o più VLAN.

Ogni VLAN deve essere configurata con un VID (ID VLAN) univoco con un valore compreso tra 1 e 4094. Il dispositivo riserva il VID 4095 come VLAN di scarto. Tutti i pacchetti classificati per la VLAN di scarto vengono eliminati all'ingresso e non vengono reindirizzati a una porta.

Per creare una VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **Impostazioni VLAN**.

In questa pagina vengono visualizzati i seguenti campi per ogni VLAN.

- **ID VLAN**: ID VLAN definito dall'utente.
- **Nome VLAN**: nome VLAN definito dall'utente.
- **Identificatori origine**: tipo di VLAN:
  - *GVRP*: VLAN creata dinamicamente attraverso il protocollo GVRP (Generic VLAN Registration Protocol).

- *Statico*: VLAN definita dall'utente.
- *Predefinito*: VLAN è la VLAN predefinita.

PASSAGGIO 2 Fare clic su **Aggiungi** per aggiungere una nuova VLAN.

In questa pagina viene consentita la creazione di una VLAN singola o di un intervallo di VLAN.

PASSAGGIO 3 Per creare una VLAN singola, selezionare il pulsante di opzione **VLAN**, immettere l'**ID VLAN (VID)** e se si desidera il **Nome VLAN**.

Per creare un intervallo di VLAN, selezionare il pulsante di opzione **Intervallo** e specificare l'intervallo di VLAN da creare immettendo il VID iniziale e il VID finale, inclusi. Quando si utilizza la funzione **Intervallo**, il numero massimo di VLAN che è possibile creare ogni volta è 100.

PASSAGGIO 4 Scegliere **Applica** per creare le VLAN.

Configurazione delle impostazioni interfaccia VLAN

Nella pagina Impostazioni interfaccia viene visualizzata e consentita la configurazione di parametri relativi a VLAN per tutte le interfacce.

Per configurare le impostazioni della VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione VLAN** > **Impostazioni interfaccia**.

PASSAGGIO 2 Selezionare un tipo di interfaccia (porta o LAG) e fare clic su **Vai**. Vengono visualizzate le porte o i LAG e i rispettivi parametri VLAN.

PASSAGGIO 3 Per configurare una porta o un LAG, selezionarlo e fare clic su **Modifica.**

PASSAGGIO 4 Immettere i valori dei seguenti campi:

- **Interfaccia**: selezionare una porta/un LAG.
- **Modalità VLAN interfaccia**: selezionare la modalità dell'interfaccia della VLAN. Sono disponibili le seguenti opzioni:
  - *Generale*: l'interfaccia può supportare tutte le funzioni come definito nella specifica IEEE 802.1q. L'interfaccia può essere un membro con o senza tag di una o più VLAN.

- *Accesso*: l'interfaccia è un membro senza tag di una VLAN singola. Una porta configurata in questa modalità è conosciuta come una porta di accesso.
- *Trunk*: l'interfaccia è un membro senza tag di una VLAN al massimo ed è un membro con tag di zero o più VLAN. Una porta configurata in questa modalità è conosciuta come una porta di trunk.
- *Cliente*: selezionando questa opzione, l'interfaccia viene posta in modalità QinQ. Ciò permette all'utente di utilizzare le proprie impostazioni VLAN (PVID) attraverso la rete del provider. Se il dispositivo dispone di una o più porte del cliente, sarà in modalità Q-in-Q. Vedere **QinQ**.

- **PVID amministrativo**: immettere l'ID VLAN della porta (PVID) della VLAN in base a cui sono classificati i frame con tag di priorità e senza tag in ingresso. I possibili valori sono compresi tra 1 e 4094.
- **Tipo di frame**: selezionare il tipo di frame che l'interfaccia può ricevere. I frame che non fanno parte del tipo di frame configurato vengono eliminati all'ingresso. Questi tipi di frame sono disponibili solo in modalità Generale. È possibile scegliere fra i valori seguenti:
  - *Ammetti tutti*: l'interfaccia accetta tutti i tipi di frame: frame senza tag, frame con tag e frame con tag di priorità.
  - *Ammetti solo con tag*: l'interfaccia accetta solo i frame con tag.
  - *Ammetti solo senza tag*: l'interfaccia accetta solo i frame senza tag e di priorità.
- **Filtro traffico in ingresso**: (disponibile solo in modalità Generale) selezionare per attivare il filtro traffico in ingresso. Quando un'interfaccia ha il filtro traffico in ingresso attivato, l'interfaccia elimina tutti i frame in ingresso classificati come VLAN la cui interfaccia non è un membro. Il filtro del traffico in ingresso può essere disattivato o attivato nelle porte generali. È sempre attivato nelle porte di accesso e di trunk.

PASSAGGIO 5 Fare clic su **Applica**. I parametri vengono scritti nel file Configurazione di esecuzione.

Definizione di Appartenenza a VLAN

Nelle pagine Porta a VLAN e Appartenenza a VLAN basata su porta vengono visualizzate le appartenenze VLAN delle porte nelle varie presentazioni. È possibile utilizzarle per aggiungere o rimuovere appartenenze alle o dalle VLAN.

Quando una porta ha l'appartenenza a VLAN predefinita vietata, questa porta non ha un'appartenenza autorizzata in nessun'altra VLAN. Un VID interno di 4095 viene assegnato alla porta.

Per reindirizzare i pacchetti correttamente, i dispositivi in grado di rilevare reti VLAN intermedi che trasmettono il traffico VLAN lungo il percorso tra i nodi finali devono essere configurati manualmente o devono rilevare dinamicamente le VLAN e le loro appartenenze alla porta dal protocollo GVRP (Generic VLAN Registration Protocol).

L'appartenenza alla porta senza tag tra due dispositivi in grado di rilevare reti VLAN senza l'intervento di dispositivi in grado di rilevare reti VLAN deve essere nella stessa VLAN. In altre parole, il PVID nelle porte tra i due dispositivi deve essere lo stesso se le porte devono inviare e ricevere pacchetti senza tag alla e dalla VLAN. Altrimenti, il traffico può fuoriuscire da una VLAN all'altra.

I frame con tag VLAN possono passare attraverso altri dispositivi di rete in grado o meno di rilevare reti VLAN. Se un nodo finale di destinazione non è in grado di rilevare reti VLAN ma è in grado di ricevere traffico da una VLAN, l'ultimo dispositivo in grado di rilevare reti VLAN (se presente) deve inviare frame della VLAN di destinazione al nodo finale senza tag.

Configurazione di Porta a VLAN

Utilizzare la pagina Porta a VLAN per visualizzare e configurare le porte all'interno di una specifica VLAN.

Per associare porte o LAG a una VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **Porta a VLAN**.

PASSAGGIO 2 Selezionare una VLAN e il tipo di interfaccia (porta o LAG) e fare clic su **Vai** per visualizzare o modificare le caratteristiche della porta per quanto riguarda la VLAN.

La modalità porta di ogni porta o LAG viene visualizzata con la sua modalità porta corrente (Accesso, Trunk, Generale o Cliente) configurata dalla pagina Impostazioni interfaccia.

Ogni porta o LAG viene visualizzata con la sua registrazione corrente alla VLAN.

PASSAGGIO 3 Modificare la registrazione di un'interfaccia nella VLAN selezionando l'opzione desiderata dal seguente elenco:

- **Vietato**: l'interfaccia non è autorizzata a includere la VLAN, neanche dalla registrazione GVRP. Quando una porta non è un membro di altre VLAN, attivare questa opzione nella porta fa diventare la porta parte della VLAN 4095 interna (un VID riservato).
- **Esclusa**: l'interfaccia al momento non è un membro della VLAN. Si tratta dell'impostazione predefinita di tutte le porte e di tutti i LAG. La porta può includere la VLAN tramite la registrazione GVRP.
- **Con tag**: l'interfaccia è un membro con tag della VLAN.
- **Senza tag**: l'interfaccia è un membro senza tag della VLAN. I frame della VLAN vengono inviati senza tag alla VLAN interfaccia.
- **VLAN TV multicast**: l'interfaccia utilizzata per la TV digitale con IP multicast. La porta si connette alla VLAN con tag VLAN di VLAN TV multicast. Per ulteriori informazioni, vedere la sezione **VLAN TV multicast basata su porta di accesso**.
- **PVID**: selezionare per impostare il PVID dell'interfaccia sul VID della VLAN. PVID è un'impostazione basata sulla porta.

PASSAGGIO 4 Fare clic su **Applica**. Le interfacce vengono assegnate alla VLAN e scritte nel file Configurazione di esecuzione.

È possibile continuare a visualizzare e/o configurare l'appartenenza alla porta di un'altra VLAN selezionando un altro ID VLAN.

Configurazione dell'appartenenza a VLAN

Nella pagina Appartenenza a VLAN basata su porta vengono visualizzate tutte le porte sul dispositivo insieme a un elenco delle VLAN a cui appartiene ogni porta.

Se il metodo di autenticazione basato sulla porta di un'interfaccia è 802.1x e Controllo porta amministrativa è impostato su Automatico, allora si verifica quanto segue:

- Fino all'autenticazione, la porta è esclusa da tutte le reti VLAN, ad eccezione delle VLAN ospite o non autenticate. Nella pagina VLAN a porta, la porta sarà contrassegnata dalla lettera "P".
- Quando la porta viene autenticata, ottiene l'appartenenza alla VLAN nella quale è stata configurata.

Per assegnare una porta a una o più VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **Appartenenza a VLAN basata su porta**.

PASSAGGIO 2 Selezionare un tipo di interfaccia (porta o LAG) e fare clic su **Vai**. Per tutte le interfacce del tipo selezionato vengono visualizzati i campi seguenti:

- **Interfaccia**: ID porta/LAG.
- **Modalità**: la modalità VLAN dell'interfaccia che è stata selezionata nella pagina Impostazioni interfaccia.
- **VLAN amministrative**: elenco a discesa che visualizza tutte le VLAN di cui l'interfaccia può essere un membro.
- **VLAN operative**: elenco a discesa che visualizza tutte le VLAN di cui l'interfaccia è attualmente un membro.
- **LAG**: se l'interfaccia selezionata è Porta, viene visualizzato il LAG di cui è un membro.

PASSAGGIO 3 Selezionare una porta e fare clic sul pulsante **Includi VLAN**.

PASSAGGIO 4 Immettere i valori dei seguenti campi:

- **Interfaccia**: selezionare una porta o un LAG. Selezionare l'unità o lo slot su un dispositivo della serie 500.
- **Modalità**: indica la modalità VLAN della porta selezionata nella pagina Impostazioni interfaccia.

- **Seleziona VLAN**: per associare una porta con VLAN, spostare gli ID VLAN dall'elenco di sinistra all'elenco di destra utilizzando i pulsanti frecce. La VLAN predefinita può apparire nell'elenco di destra se con tag ma non può essere selezionata.
- **Tag**: selezionare una delle seguenti opzioni di tag/PVID:
  - **Con tag**: selezionare se la porta è con tag. Non è importante per le porte di accesso.
  - **Senza tag**: selezionare se la porta è senza tag. Non è importante per le porte di accesso.
  - **PVID**: PVID è impostato su questa VLAN. Se l'interfaccia è in modalità di accesso o trunk, il dispositivo trasforma automaticamente l'interfaccia in un membro senza tag della VLAN. Se l'interfaccia è in modalità generale, è necessario configurare manualmente l'appartenenza a VLAN.

PASSAGGIO 5 Fare clic su **Applica**. Le impostazioni sono modificate e vengono scritte nel file Configurazione di esecuzione.

Per vedere le VLAN amministrative e operative su un'interfaccia, fare clic su **Dettagli**.

Impostazioni GVRP

I dispositivi adiacenti in grado di rilevare reti VLAN possono scambiarsi l'un l'altro informazioni su VLAN utilizzando il protocollo GVRP (Generic VLAN Registration Protocol). GVRP si basa sul protocollo GARP (Generic Attribute Registration Protocol) e divulga informazioni su VLAN su una rete connessa.

Dato che GVRP richiede assistenza per l'assegnazione di tag, la porta deve essere configurata in modalità Trunk o Generale.

Una porta che si unisce a una VLAN tramite GVRP viene aggiunta come un membro dinamico, a meno che ciò non sia espressamente vietato nella pagina Appartenenza a VLAN basata su porta. Se la VLAN non esiste, viene creata in maniera dinamica, se per la porta è stata attivata la creazione dinamica della VLAN dinamica (nella pagina Impostazioni GVRP).

GVRP deve essere attivato a livello globale e su ogni porta. Quando attivato, trasmette e riceve GPDU (GARP Packet Data Units). Le VLAN definite ma non attive non vengono divulgate. Per divulgare la VLAN, deve essere attiva su almeno una porta.

Per impostazione predefinita, GVRP è disattivato globalmente e sulle porte.

Definizione delle impostazioni GVRP

Per definire le impostazioni GVRP per un'interfaccia, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **Impostazioni GVRP**.

PASSAGGIO 2 Selezionare **Stato generale GVRP** per attivare GVRP a livello globale.

PASSAGGIO 3 Scegliere **Applica** per impostare lo stato GVRP globale.

PASSAGGIO 4 Selezionare un tipo di interfaccia (porta o LAG), e fare clic su **Vai** per visualizzare tutte le interfacce di quel tipo.

PASSAGGIO 5 Per definire le impostazioni GVRP per una porta, selezionarla e fare clic su **Modifica.**

PASSAGGIO 6 Immettere i valori dei seguenti campi:

- **Interfaccia**: selezionare l'interfaccia (porta o LAG) da modificare.
- **Stato GVRP**: selezionare per attivare GVRP su questa interfaccia.
- **Creazione VLAN dinamica**: selezionare per attivare Creazione VLAN dinamica su questa interfaccia.
- **Registrazione GVRP**: selezionare per attivare Registrazione VLAN utilizzando GVRP su questa interfaccia.

PASSAGGIO 7 Fare clic su **Applica**. Le impostazioni GVRP sono modificate e vengono scritte nel file Configurazione di esecuzione.

Gruppi VLAN

I gruppi VLAN vengono utilizzati per il bilanciamento del carico di traffico sulla rete Livello 2.

I pacchetti vengono assegnati alla VLAN in base alle varie classificazioni configurate (ad esempio, i gruppi VLAN).

Se vengono definiti numerosi schemi di classificazione, i pacchetti vengono assegnati alla VLAN nel seguente ordine:

- **TAG:** se il pacchetto è dotato di tag, la VLAN viene tratta dal tag.
- **VLAN basata su MAC:** se è stata definita una VLAN basata su MAC, la VLAN viene tratta dall'associazione MAC a VLAN di origine dell'interfaccia di ingresso.
- **VLAN basata su protocollo:** se è stata definita una VLAN basata su protocollo, la VLAN viene tratta dall'associazione protocollo-VLAN (di tipo Ethernet) dell'interfaccia di ingresso.
- **PVID:** la VLAN viene tratta dall'ID VLAN predefinito della porta.

Gruppi basati su MAC

La classificazione VLAN basata su MAC consente di classificare pacchetti secondo il rispettivo indirizzo MAC di origine. È quindi possibile definire l'associazione MAC a VLAN per interfaccia.

È possibile definire vari gruppi VLAN basati su MAC, ognuno dei quali contiene diversi indirizzi MAC.

Questi gruppi basati su MAC possono essere assegnati a porte o a LAG specifici. I gruppi VLAN basati su MAC non possono contenere campi sovrapposti di indirizzi MAC sulla stessa porta.

Nella seguente tabella è illustrata la disponibilità di gruppi VLAN basati su MAC in vari SKU.

Tabella 1 Disponibilità gruppi VLAN basati su MAC

SKU	Modalità di sistema	Gruppi VLAN basati su MAC supportati
Sx300	**Livello 2**	Sì
	Livello 3	No
Sx500, Sx500ESW2-550X	**Livello 2**	Sì
	Livello 3	No
SG500X	**Nativa**	Sì
	Ibrido di base - Livello 2	Sì
	Ibrido di base - Livello 3	No
SG500XG	**Come Sx500**	Sì

Flusso di lavoro

Per definire un gruppo VLAN basato su MAC, attenersi alla seguente procedura:

1. Assegnare l'indirizzo MAC a un ID gruppo VLAN (nella pagina Gruppi basati su MAC).
2. Per ogni interfaccia necessaria:
   a. Assegnare il gruppo VLAN a una VLAN (nella pagina Gruppi basati su Mac a VLAN). Le interfacce devono essere in modalità Generale.
   b. Se l'interfaccia non appartiene alla VLAN, assegnarla manualmente alla VLAN dalla pagina Porta a VLAN.

Assegnazione di gruppi VLAN basate su MAC

Vedere **Tabella 1** per una descrizione della disponibilità di questa funzione.

Per assegnare un indirizzo MAC a un gruppo VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **Gruppi VLAN** > **Gruppi basati su MAC**.

PASSAGGIO 2 Fare clic su **Aggiungi.**

PASSAGGIO 3 Immettere i valori dei seguenti campi:

- **Indirizzo MAC**: immettere un indirizzo MAC da assegnare a un gruppo VLAN.

NOTA Questo indirizzo MAC non può essere assegnato a qualsiasi altro gruppo VLAN.

- **Maschera**: immettere una delle seguenti opzioni:
  - *Host*: host di origine dell'indirizzo MAC
  - *Lunghezza*: *prefisso* dell'indirizzo MAC
- **ID gruppo**: immettere un numero ID gruppo VLAN creato dall'utente.

PASSAGGIO 4 Fare clic su **Applica**. L'indirizzo MAC viene assegnato a un gruppo VLAN.

Associazione di un gruppo VLAN a VLAN per interfaccia

Vedere **Tabella 1** per una descrizione della disponibilità di questa funzione.

Le porte e i LAG devono essere in modalità generale.

Per assegnare un gruppo VLAN basato su MAC a VLAN su un'interfaccia, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione VLAN** > **Gruppi VLAN** > **Gruppi basati su MAC a VLAN**.

PASSAGGIO 2 Fare clic su **Aggiungi.**

PASSAGGIO 3 Immettere i valori dei seguenti campi:

- **Tipo di gruppo**: indica che il gruppo è basato su MAC.
- **Interfaccia**: immettere un'interfaccia generica (porta o LAG) attraverso cui ricevere il traffico.
- **ID gruppo**: selezionare un gruppo VLAN definito nella pagina Gruppi basati su MAC.
- **ID VLAN**: selezionare la VLAN a cui viene reindirizzato il traffico dal gruppo VLAN.

PASSAGGIO 4 Scegliere **Applica** per impostare l'associazione del gruppo VLAN alla VLAN Questa associazione non collega l'interfaccia alla VLAN in modo dinamico; è necessario aggiungere manualmente l'interfaccia alla VLAN.

VLAN basate su protocollo

I gruppi di protocollo possono essere definiti e successivamente associati a una porta. Dopo aver associato il gruppo di protocollo a una porta, a ciascun pacchetto proveniente da un protocollo del gruppo viene assegnata la VLAN, configurata nella pagina Gruppi basati su protocollo.

Flusso di lavoro

Per definire un gruppo VLAN basato su protocollo, attenersi alla seguente procedura:

1. Definire un gruppo di protocollo (nella pagina Gruppi basati su protocollo).
2. Per ogni interfaccia necessaria, assegnare il gruppo di protocollo a una VLAN (nella pagina Gruppi basati su protocolli a VLAN). Le interfacce devono essere in modalità Generale e non devono essere associate a nessuna VLAN dinamica (DVA).

Gruppi basati su protocollo

Per definire un insieme di protocolli, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **Gruppi VLAN** > **Gruppi basati su protocollo**.

Nella pagina Gruppi basati su protocollo sono presenti i seguenti campi:

- **Incapsulamento**: indica il protocollo su cui è basato il gruppo VLAN.
- **Valore del protocollo (esadecimale):** indica il valore del protocollo esadecimale.
- **ID gruppo**: indica l'ID del gruppo di protocolli a cui viene aggiunta l'interfaccia.

PASSAGGIO 2 Fare clic sul pulsante **Aggiungi**. Viene visualizzata la pagina Aggiungi gruppo basato su protocollo.

PASSAGGIO 3 Immettere informazioni nei campi indicati di seguito.

- **Incapsulamento**: tipo di pacchetto del protocollo. Sono disponibili le seguenti opzioni:
  - *Ethernet V2*: se selezionata, scegliere il **tipo di Ethernet**.
  - *LLC-SNAP (rfc1042)*: se selezionata, immettere il **valore del protocollo**.
  - *LLC*: se selezionata, scegliere i **valori DSAP-SSAP**.

- **Tipo Ethernet:** selezionare il tipo di Ethernet per l'incapsulamento di Ethernet V2. Si tratta del campo a due ottetti nel frame Ethernet utilizzato per indicare il protocollo che viene incapsulato nel carico del pacchetto Ethernet per il gruppo VLAN.
- **Valore del protocollo:** inserire il protocollo per l'incapsulamento LLC-SNAP (rfc 1042).
- **DSAP-SSAP:** inserire questi valori per l'incapsulamento LLC.
- **ID gruppo**: immettere l'ID del gruppo di protocolli.

PASSAGGIO 4 Fare clic su **Applica**. Il gruppo di protocolli viene aggiunto e definito nel file Configurazione di esecuzione.

Gruppi basati su protocollo ad associazione VLAN

Per associare un gruppo di protocolli a una porta, quest'ultima deve essere in modalità Generale e non deve essere associata a nessuna DVA (vedere **Configurazione delle impostazioni interfaccia VLAN**).

È possibile associare più gruppi a una singola porta, purché ciascuna porta sia associata alla propria VLAN.

È inoltre possibile associare più gruppi a una singola VLAN.

Per associare la porta di protocollo a una VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **Gruppi VLAN** > **Gruppi basati su protocollo a VLAN.**

Vengono visualizzate le associazioni attualmente definite.

PASSAGGIO 2 Per associare un'interfaccia a una VLAN e un gruppo basato su protocollo, fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere informazioni nei campi indicati di seguito.

- **Interfaccia**: numero della porta o del LAG assegnato alla VLAN in base al gruppo basato su protocollo.
- **ID gruppo**: ID del gruppo di protocolli.
- **ID VLAN**: consente di collegare l'interfaccia all'ID VLAN definito dall'utente.

PASSAGGIO 4 Fare clic su **Applica**. Le porte di protocollo vengono associate alle VLAN e definite nel file Configurazione di esecuzione.

VLAN voce

In una LAN i dispositivi vocali, quali telefoni IP, terminali VoIP e sistemi vocali vengono inseriti nella stessa VLAN. Questa VLAN viene definita VLAN voce. Se i dispositivi vocali sono in VLAN voce diverse, vengono richiesti dei router IP (Livello 3) per garantire la comunicazione.

In questa sezione vengono illustrati i seguenti argomenti:

- **Panoramica della VLAN voce**
- **Configurazione della VLAN voce**

Panoramica della VLAN voce

In questa sezione vengono illustrati i seguenti argomenti:

- **Modalità VLAN voce dinamiche**
- **VLAN voce automatica, Smartport automatico, CDP e LLDP**
- **QoS VLAN voce**
- **Vincoli di VLAN voce**
- **Flussi di lavoro della VLAN voce**

Di seguito sono descritti tipici scenari di distribuzione vocali, con le configurazioni appropriate:

- **UC3xx/UC5xx hosted:** tutti i telefoni Cisco e punti terminali VoIP supportano questo modello di distribuzione. Per questo modello, UC3xx/UC5xx , i telefoni Cisco e i terminali VoIP si trovano nella stessa VLAN voce. La VLAN voce di UC3xx/UC5xx passa a VLAN 100 per impostazione predefinita.
- **IP di terze parti su host PBX:** Cisco SBTG CP-79xx, i telefoni SPA5xx e i terminali SPA8800 supportano questo modello di distribuzione. In questo modello, la VLAN utilizzata dai telefoni viene determinata dalla configurazione di rete. Ci possono essere o non essere VLAN voce e dati separate. I telefoni e i terminali VoIP si registrano su PBX IP locale.
- **IP Centrex/ITSP hosted:** Cisco CP-79xx, i telefoni SPA5xx e i terminali SPA8800 supportano questo modello di distribuzione. Per questo modello, la VLAN utilizzata dai telefoni viene determinata dalla configurazione di rete. Ci possono essere o non essere VLAN voce e dati separate. I telefoni e i terminali VoIP si registrano con un proxy SIP esterno nel "cloud".

Dal punto di vista della VLAN, i modelli di cui sopra operano sia negli ambienti in grado di rilevare le VLAN che negli ambienti che non sono in grado di farlo. Nell'ambiente in grado di rilevare VLAN, la VLAN voce è una delle tante VLAN configurate di un'installazione. Lo scenario di ambiente non in grado di rilevare una VLAN è equivalente a quello di un ambiente in grado di farlo, ma con una sola VLAN.

Il dispositivo funziona sempre come switch in grado di rilevare reti VLAN.

Il dispositivo supporta una singola VLAN voce, che viene configurata per impostazione predefinita su VLAN 1. È possibile configurare manualmente una VLAN voce diversa. Si può anche apprendere dinamicamente quando è attivata una VLAN voce automatica.

Le porte possono essere aggiunte manualmente alla VLAN voce tramite la configurazione VLAN di base come descritto nella sezione Configurazione delle impostazioni interfaccia VLAN oppure manualmente applicando alle porte la macro Smartport relativa alla voce. In alternativa, possono essere aggiunte dinamicamente se il dispositivo è in modalità OUI telefonia o ha attivato Smartport automatici.

Modalità VLAN voce dinamiche

Il dispositivo supporta due modalità VLAN voce dinamiche: la modalità OUI (Organization Unique Identifier) telefonia e la modalità VLAN voce automatica. Le due modalità influenzano il modo in cui la VLAN voce e/o le appartenenze alla porta VLAN voce sono configurate. Le due modalità si escludono a vicenda.

- **OUI telefonia**

  In modalità OUI telefonia, la VLAN voce deve essere una VLAN configurata manualmente e non può essere la VLAN predefinita.

  Quando il dispositivo è in modalità OUI telefonia e una porta viene configurata manualmente come candidato all'inclusione sulla VLAN voce, il dispositivo aggiunge in modo dinamico la porta alla VLAN voce se riceve un pacchetto con un indirizzo MAC di origine corrispondente a uno degli OUI telefonia configurati. Un OUI è costituito dai primi tre byte di un indirizzo MAC Ethernet. Per ulteriori informazioni sulla pagina OUI telefonia, vedere **Configurazione OUI telefonia**.

- **VLAN voce automatica**

  In modalità VLAN voce automatica, la VLAN voce può essere sia la VLAN voce predefinita, configurata manualmente, sia appresa da dispositivi esterni come UC3xx/5xx e da switch che dichiarano la VLAN voce in CDP o VSDP. VSDP è un protocollo Cisco definito per il rilevamento del servizio vocale.

  A differenza della modalità OUI telefonia, in grado di rilevare i dispositivi vocali basati su OUI telefonia, la modalità VLAN voce automatica dipende da SmartPort automatico per aggiungere dinamicamente le porte alla VLAN voce. SmartPort automatico, se attivato, aggiunge una porta alla VLAN voce se viene rilevato un dispositivo di collegamento sulla porta che si dichiara come punto terminale telefonico o multimediale tramite CDP e/o LLDP-MED.

Punti terminali voce

Affinché una VLAN voce funzioni in modo corretto, i dispositivi vocali, quali telefoni Cisco e punti terminali VoIP, devono essere assegnati alla VLAN voce nel punto in cui essa invia e riceve il traffico vocale. Alcuni degli scenari possibili sono i seguenti:

- Un telefono/punto terminale può essere configurato staticamente con la VLAN voce.
- Un telefono/punto terminale può ottenere la VLAN voce nel file di avvio che scarica da un server TFTP. Un server DHCP può specificare il file di avvio e il server TFTP quando assegna un indirizzo IP al telefono.
- Un telefono/punto terminale può ottenere le informazioni sulla VLAN voce dagli annunci CDP e LLDP-MED che riceve dai sistemi vocali e dagli switch adiacenti.

Il dispositivo si aspetta che i dispositivi vocali connessi inviino pacchetti VLAN voce con tag. Sulle porte dove la VLAN voce è anche la VLAN nativa, è possibile la presenza di pacchetti VLAN voce senza tag.

VLAN voce automatica, Smartport automatico, CDP e LLDP

Impostazioni predefinite

Per impostazione predefinita di fabbrica sul dispositivo sono abilitati CDP, LLDP e LLDP-MED, la modalità Smartport automatico e QoS di base con DSCP attendibile; inoltre, tutte le porte sono membri della VLAN 1 predefinita, che è anche la VLAN voce predefinita.

Inoltre, la modalità VLAN voce dinamica è l'impostazione predefinita sulla VLAN voce automatica con abilitazione basata su trigger e SmartPort automatico è l'impostazione predefinita da attivare a seconda della VLAN voce automatica.

Trigger VLAN voce

Quando per la VLAN voce dinamica viene impostata la modalità Attiva VLAN con voce automatica, la VLAN voce automatica diventerà operativa solo se si verificano uno o più trigger. Possibili trigger sono la configurazione della VLAN voce statica, le informazioni VLAN voce ricevute negli annunci CDP adiacenti e le informazioni VLAN voce ricevute nel VSDP (VLAN Voice Discovery Protocol). Se lo si desidera, si può attivare immediatamente la VLAN voce automatica senza attendere un trigger.

Quando Smartport automatico è abilitato in base alla modalità VLAN voce automatica, Smartport automatico sarà abilitato quando la VLAN voce automatica diventa operativa. Se lo si desidera, si può abilitare Smartport automatico indipendentemente dalla VLAN voce automatica.

NOTA L'elenco di configurazione predefinito si applica agli switch le cui versioni firmware supportano VLAN voce automatica come preimpostazione. Si applica anche agli switch non configurati che sono stati aggiornati alla versione firmware che supporta la VLAN voce automatica.

NOTA Le impostazioni predefinite e i trigger VLAN voce sono realizzati in modo da non avere alcun effetto sulle installazioni senza VLAN voce e sugli switch che sono già stati configurati. È possibile disattivare manualmente e abilitare VLAN voce automatica e/o Smartport automatico per adattarli alla distribuzione, se necessario.

VLAN voce automatica

La VLAN voce automatica è responsabile del mantenimento della VLAN voce, ma è compito di Smartport automatico mantenere l'appartenenza delle porte alla VLAN voce. VLAN voce automatica svolge le seguenti funzioni quando è in funzione:

- Rileva informazioni sulla VLAN voce negli annunci CDP dei dispositivi adiacenti connessi direttamente.
- Se più switch e/o router contigui, ad esempio dispositivi Cisco UC (Unified Communication), dichiarano la propria VLAN voce, viene utilizzata la VLAN voce del dispositivo con l'indirizzo MAC più basso.

NOTA Quando si collega il dispositivo a un dispositivo Cisco UC, potrebbe essere necessario configurare la porta sul dispositivo UC mediante il comando `switchport voice vlan` per garantire che il dispositivo UC dichiari la propria VLAN voce in CDP sulla porta.

- In questo modo vengono sincronizzati i parametri relativi alla VLAN voce con altri switch abilitati alla VLAN voce automatica tramite il protocollo VSDP (Voice Service Discovery Protocol). Il dispositivo si configura sempre con la VLAN voce proveniente dall'origine con la massima priorità di cui è a conoscenza. La priorità è basata sul tipo di origine e sull'indirizzo MAC dell'origine che fornisce le informazioni sulla VLAN voce. Tipi di origine elencati secondo priorità in ordine decrescente sono configurazione VLAN statica, dichiarazione CDP, configurazione predefinita basata sulla VLAN predefinita modificata e VLAN voce predefinita. Un indirizzo numerico MAC basso ha una priorità maggiore rispetto a un indirizzo numerico MAC alto.
- Mantiene la VLAN voce finché una nuova VLAN voce con un'origine di priorità più alta non viene rilevata oppure finché la VLAN voce automatica non viene riavviata dall'utente. Al riavvio, il dispositivo reimposta la VLAN voce sulla VLAN voce predefinita e riavvia il rilevamento della VLAN voce automatica.
- Quando viene configurata/rilevata una nuova VLAN voce, il dispositivo la crea automaticamente e sostituisce tutte le appartenenze di porta della VLAN voce esistente con la nuova VLAN voce. Questo può interrompere le sessioni vocali esistenti, fatto previsto quando la topologia di rete viene alterata.

  NOTA Se il dispositivo è in modalità di sistema Livello 2, può sincronizzarsi solo con switch idonei per VSDP nella stessa VLAN di gestione. Se il dispositivo è in modalità di sistema Livello 3, può sincronizzarsi con switch idonei per VSDP che siano nelle sottoreti IP a connessione diretta configurate sul dispositivo.

Smartport automatico funziona con CDP/LLDP per mantenere le appartenenze di porta della VLAN voce quando sulle porte vengono rilevati punti terminali vocali:

- Se CDP e LLDP sono attivati, il dispositivo invia i pacchetti CDP e LLDP periodicamente per annunciare la VLAN voce ai punti terminali vocali da utilizzare.
- Quando un dispositivo che si collega a una porta si annuncia come punto terminale vocale tramite CDP e/o LLDP, la funzione Smartport automatico aggiunge automaticamente la porta alla VLAN voce, applicando la macro Smartport corrispondente alla porta (se non vi sono altri dispositivi dalla porta che dichiarano capacità in conflitto o superiore). Se un dispositivo si

annuncia come telefono, il valore predefinito della macro Smartport è telefono. Se un dispositivo si annuncia come telefono e host o telefono e bridge, il valore predefinito della macro Smartport è telefono+desktop.

QoS VLAN voce

La VLAN voce può propagare le impostazioni CoS/802.1p e DSCP utilizzando i criteri di rete LLDP-MED. LLDP-MED viene impostato in modo predefinito per rispondere con l'impostazione QoS voce se un dispositivo invia pacchetti LLDP-MED. I dispositivi con supporto MED devono inviare il proprio traffico vocale con gli stessi valori CoS/802.1p e DSCP, come ricevuti con la risposta LLDP-MED.

È possibile disabilitare l'aggiornamento automatico tra VLAN voce e LLDP-MED e utilizzare i propri criteri di rete.

Lavorando in modalità OUI, il dispositivo può inoltre configurare l'associazione e la contrassegnazione (CoS/802.1p) del traffico vocale basato su OUI.

Per impostazione predefinita, tutte le interfacce sono attendibili per CoS/802.1p. Il dispositivo applica la qualità del servizio in base al valore CoS/802.1p rilevato nel flusso vocale. In VLAN voce automatica, è possibile sovrascrivere il valore dei flussi vocali tramite un QoS avanzato. Per i flussi vocali di OUI telefonia, è possibile sovrascrivere la qualità del servizio ed eventualmente contrassegnare il valore 802.1p dei flussi vocali specificando i valori CoS/802.1p desiderati e utilizzando l'opzione di contrassegnazione in OUI telefonia.

Vincoli di VLAN voce

Esistono i seguenti vincoli:

- È supportata una sola VLAN voce.
- Non è possibile rimuovere una VLAN definita come una VLAN voce.

Inoltre, i seguenti vincoli sono applicabili a OUI telefonia:

- La VLAN voce non può essere VLAN1 (la VLAN predefinita).
- La VLAN voce non può essere abilitata per Smartport.
- La VLAN voce non supporta l'assegnazione DVA (Dynamic VLAN Assignment).
- La VLAN voce non può essere la VLAN ospite se la modalità VLAN voce è OUI. Se la modalità VLAN voce è automatica, allora la VLAN voce può essere la VLAN ospite.

- La decisione della QoS della VLAN voce ha priorità su qualsiasi altra decisione QoS tranne che per la decisione della QoS del criterio/di ACL.
- È possibile configurare un nuovo ID VLAN per la VLAN voce solo se quella corrente non ha porte candidate.
- La VLAN interfaccia di una porta candidata deve essere in modalità Generale o Trunk.
- La QoS della VLAN voce viene applicata alle porte candidate con la VLAN voce inclusa e alle porte statiche.
- Il flusso vocale viene accettato se è possibile rilevare l'indirizzo MAC da FDB (se non c'è spazio libero in FDB, non si verifica nessuna azione).

Flussi di lavoro della VLAN voce

La configurazione predefinita del dispositivo sulla VLAN voce automatica, gli Smartport automatici, CDP e LLDP riguarda gli scenari di distribuzione vocale più comuni. In questa sezione viene illustrato come distribuire la VLAN voce quando non si applica la configurazione predefinita.

Flusso di lavoro 1: per configurare la VLAN voce automatica, attenersi alla seguente procedura:

PASSAGGIO 1 Aprire la pagina Gestione VLAN > VLAN voce > Proprietà.

PASSAGGIO 2 Selezionare l'ID VLAN voce, che non può essere impostato su ID VLAN 1 (questo passaggio non è necessario per la VLAN voce dinamica).

PASSAGGIO 3 Impostare la **VLAN voce dinamica** su Attiva VLAN voce automatica.

PASSAGGIO 4 Selezionare il metodo **Attivazione VLAN voce automatica**.

> **NOTA** Se il dispositivo è attualmente in modalità OUI telefonia, è necessario disattivare tale modalità prima di poter configurare la VLAN voce automatica.

PASSAGGIO 5 Fare clic su **Applica**.

PASSAGGIO 6 Configurare le Smartport come descritto nella sezione **Attività comuni con Smartport**.

PASSAGGIO 7 Configurare LLDP/CDP come descritto, rispettivamente, nelle sezioni **Configurazione di LLDP** e **Configurazione CDP**.

PASSAGGIO 8 Attivare la funzione Smartport sulle porte pertinenti tramite la pagina Smartport > Impostazioni interfaccia.

NOTA I passaggi 7 e 8 sono facoltativi in quanto attivati per impostazione predefinita.

Flusso di lavoro 2: per configurare il metodo OUI telefonia, attenersi alla seguente procedura:

PASSAGGIO 1 Aprire la pagina Gestione VLAN > VLAN voce > Proprietà. Impostare **VLAN voce dinamica** su Attiva OUI telefonia.

NOTA Se il dispositivo è attualmente in modalità VLAN voce automatica, è necessario disattivare tale modalità prima di poter attivare OUI telefonia.

PASSAGGIO 2 Configurare OUI telefonia nella pagina omonima.

PASSAGGIO 3 Configurare l'appartenenza della VLAN OUI telefonia per le porte nella pagina Interfaccia OUI telefonia.

Configurazione della VLAN voce

In questa sezione viene illustrato come configurare la VLAN voce. Vengono trattati i seguenti argomenti:

- **Configurazione delle proprietà della VLAN voce**
- **Visualizzazione delle impostazioni di VLAN voce automatica**
- **Configurazione OUI telefonia**

Configurazione delle proprietà della VLAN voce

Utilizzare la pagina Proprietà VLAN voce per eseguire le attività seguenti:

- Visualizzare la configurazione corrente della VLAN voce.
- Configurare l'ID VLAN della VLAN voce.
- Configurare le impostazioni QoS della VLAN voce.
- Configurare la modalità VLAN voce (OUI telefonia o VLAN voce automatica).
- Configurare le modalità di attivazione della VLAN voce automatica.

Per visualizzare e configurare le proprietà della VLAN voce, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **VLAN voce** > **Proprietà**.

- Le impostazioni della VLAN voce configurate sul dispositivo vengono visualizzate nel blocco **Impostazioni VLAN voce (Stato amministrativo)**.
- Le impostazioni della VLAN voce che vengono correntemente applicate alla distribuzione della VLAN voce vengono visualizzate nel blocco **Impostazioni VLAN voce (Stato operativo)**.

PASSAGGIO 2 Immettere i valori dei seguenti campi:

- **ID VLAN voce**: selezionare la VLAN che dovrà essere la VLAN voce.

  NOTA Cambiamenti relativi a ID VLAN voce, CoS/802.1p e/o DSCP portano il dispositivo a dichiarare la VLAN voce amministrativa come VLAN voce statica. Se l'opzione *Attivazione VLAN voce automatica* attivata dalla VLAN voce esterna è selezionata, i valori predefiniti devono essere mantenuti.

- **CoS/802.1p**: selezionare un valore CoS/802.1p che verrà utilizzato da LLDP-MED come criterio di rete voce. Fare riferimento a *Amministrazione > Rilevamento > LLDP > Criteri di rete LLDP MED* per ulteriori dettagli.
- **DSCP**: selezione dei valori DSCP che verranno utilizzati da LLDP-MED come criteri di rete voce. Fare riferimento a *Amministrazione > Rilevamento > LLDP > Criteri di rete LLDP MED* per ulteriori dettagli.
- **VLAN voce dinamica**: selezionare questo campo per disattivare o attivare funzionalità VLAN voce in uno dei seguenti modi:
  - *Attiva VLAN voce automatica*: attiva la VLAN voce dinamica in modalità VLAN voce automatica.
  - *Attiva OUI telefonia*: attiva la VLAN voce dinamica in modalità OUI telefonia.
  - *Disattiva*: disattiva VLAN voce automatica o OUI telefonia.
- **Attivazione VLAN voce automatica**: se la VLAN voce automatica è stata abilitata, selezionare una delle seguenti opzioni per attivare VLAN voce automatica:
  - *Immediato*: la VLAN voce automatica sul dispositivo deve essere attivata e messa immediatamente in funzione se abilitata.

- *Tramite attivazione VLAN voce esterna*: la VLAN voce automatica sul dispositivo deve essere attivata e messa in funzione solo se il dispositivo rileva un dispositivo che dichiara la VLAN voce.

NOTA La riconfigurazione manuale di ID VLAN voce, CoS/802.1p e/o DSCP rispetto ai valori predefiniti si traduce in una VLAN voce statica, che ha una priorità maggiore rispetto alla VLAN voce automatica appresa da origini esterne.

PASSAGGIO 3 Fare clic su **Applica**. Le proprietà della VLAN vengono aggiunte al file Configurazione di esecuzione.

Visualizzazione delle impostazioni di VLAN voce automatica

Se è attivata la modalità VLAN voce automatica, utilizzare la pagina VLAN voce automatica per visualizzare i parametri globali e di interfaccia pertinenti.

È inoltre possibile utilizzare questa pagina per riavviare manualmente la VLAN voce automatica, facendo clic su **Riavvio VLAN voce automatica**. Dopo una breve attesa, la VLAN voce viene reimpostata sulla VLAN voce predefinita e riavvia il rilevamento della VLAN voce automatica e il processo di sincronizzazione su tutti gli switch della LAN che sono abilitati per la VLAN voce automatica.

NOTA In questo modo si reimposta solo la VLAN voce a quella predefinita se il tipo di origine è in stato *Inattivo*.

Per visualizzare i parametri della VLAN voce automatica, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **VLAN voce** > **VLAN voce automatica**.

Il blocco di stato operativo in questa pagina mostra le informazioni relative alla VLAN voce corrente e la sua origine:

- **Stato VLAN voce automatica**: indica se la VLAN voce automatica è attivata o meno.
- **ID VLAN voce**: l'identificativo della VLAN voce corrente.
- **Tipo origine**: visualizza il tipo di origine in cui la VLAN voce viene rilevata dal dispositivo root.
- **CoS/802.1p**: visualizza i valori CoS/802.1p che verranno utilizzati da LLDP-MED come criterio di rete voce.

- **DSCP**: visualizza i valori DSCP che verranno utilizzati da LLDP-MED come criteri di rete voce.
- **Indirizzo MAC switch root**: l'indirizzo MAC del dispositivo root VLAN voce automatica che rileva o viene configurato con la VLAN voce da cui viene appresa la VLAN voce.
- **Indirizzo MAC switch**: l'indirizzo MAC di base del dispositivo. Se l'indirizzo MAC switch del dispositivo è l'indirizzo MAC switch root, il dispositivo è il root VLAN voce automatica.
- **Ora modifica ID VLAN voce**: l'ultima volta in cui la VLAN voce è stata aggiornata.

PASSAGGIO 2 Scegliere **Riavvio VLAN voce automatica** per riportare la VLAN voce alla VLAN voce predefinita e riavviare il rilevamento della VLAN voce automatica su tutti gli switch nella LAN abilitati per VLAN voce automatica.

La Tabella origine locale VLAN voce mostra la VLAN voce configurata sul dispositivo, oltre a tutte le eventuali configurazioni VLAN voce dichiarate da dispositivi contigui direttamente connessi. Contiene i seguenti campi:

- **Interfaccia**: visualizza l'interfaccia su cui viene eseguita o ricevuta la configurazione della VLAN voce. Se viene visualizzato N/D, la configurazione è stata eseguita sul dispositivo stesso. Se viene visualizzata un'interfaccia, significa che è stata ricevuta una configurazione vocale da un dispositivo contiguo.
- **Indirizzo MAC di origine**: indirizzo MAC di un UC da cui è stata ricevuta la configurazione vocale.
- **Tipo di origine**: tipo di UC da cui è stata ricevuta la configurazione vocale. Sono disponibili le seguenti opzioni:
  - *Predefinito*: configurazione della VLAN voce predefinita sul dispositivo.
  - *Statico*: configurazione della VLAN voce definita dall'utente sul dispositivo.
  - *CDP*: l'UC che ha dichiarato la configurazione della VLAN voce esegue il protocollo CDP.
  - *LLDP*: l'UC che ha dichiarato la configurazione della VLAN voce esegue il protocollo LLDP.
  - *ID VLAN voce*: l'identificativo della VLAN voce dichiarata o configurata.
- **ID VLAN voce**: l'identificativo della VLAN voce corrente.

- **CoS/802.1p**: i valori CoS/802.1p dichiarati o configurati che verranno utilizzati da LLDP-MED come criterio di rete voce.
- **DSCP**: i valori DSCP dichiarati o configurati che verranno utilizzati da LLDP-MED come criteri di rete voce.
- **Migliore origine locale**: indica se la VLAN voce è stata utilizzata dal dispositivo. Sono disponibili le seguenti opzioni:
  - *Sì*: il dispositivo utilizza la VLAN voce per la sincronizzazione con altri switch abilitati per VLAN voce automatica. Questa VLAN voce è la VLAN voce per la rete a meno che venga rilevata una VLAN voce da una origine con priorità superiore. Una sola origine locale è la migliore origine locale.
  - *No*: questa non è la migliore origine locale.

PASSAGGIO 3 Scegliere **Aggiorna** per aggiornare le informazioni sulla pagina.

Configurazione OUI telefonia

Gli OUI vengono assegnati dall'autorità di registrazione IEEE (Institute of Electrical and Electronics Engineers, Incorporated). Dato che il numero di produttori di telefoni IP è limitato e noto, i valori OUI noti provocano l'assegnazione automatica dei frame selezionati e della porta su cui vengono visualizzati a una VLAN vocale.

La tabella OUI globali può contenere un massimo di 128 OUI.

In questa sezione vengono illustrati i seguenti argomenti:

- **Aggiunta di OUI alla Tabella OUI telefonia**
- **Aggiunta di interfacce alla VLAN voce sulla base di OUI**

Aggiunta di OUI alla Tabella OUI telefonia

Utilizzare la pagina OUI telefonia per configurare le proprietà QoS di OUI telefonia. Inoltre, è possibile configurare la validità temporale appartenenza automatica. Se il periodo di tempo specificato passa senza attività di telefonia, la porta viene rimossa dalla VLAN voce.

Utilizzare la pagina OUI telefonia per visualizzare gli OUI esistenti e aggiungerne di nuovi.

Per configurare OUI telefonia e/o aggiungere una nuova OUI VLAN voce, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **VLAN vocale** > **OUI telefonia**.

Nella pagina OUI telefonia vengono visualizzati i seguenti campi:

- **Stato operativo OUI telefonia**: indica se gli OUI vengono utilizzati per identificare il traffico vocale.
- **CoS/802.1p**: selezionare la coda CoS da assegnare al traffico vocale.
- **Contrassegna CoS/802.1p**: selezionare se contrassegnare il traffico in uscita.
- **Validità temporale appartenenza automatica**: immettere il ritardo per rimuovere una porta dalla VLAN voce dopo la scadenza di tutti gli indirizzi MAC dei telefoni rilevati sulle porte.

PASSAGGIO 2 Fare clic su **Applica** per aggiornare la Configurazione di esecuzione del dispositivo con questi valori.

Viene visualizzata la tabella OUI telefonia:

- **OUI telefonia**: le prime sei cifre dell'indirizzo MAC riservate per gli OUI.
- **Descrizione**: descrizione OUI assegnato dall'utente.

PASSAGGIO 3 Scegliere **Ripristina OUI predefiniti** per eliminare tutti gli OUI creati dall'utente e lasciare solo gli OUI predefiniti nella tabella.

Per eliminare tutti gli OUI, selezionare la casella di controllo in alto. Tutti gli OUI sono selezionati e possono essere eliminati facendo clic su **Elimina**. Se poi si fa clic su **Ripristina OUI predefiniti**, il sistema recupera gli OUI noti.

PASSAGGIO 4 Per aggiungere un nuovo OUI, fare clic su **Aggiungi**.

PASSAGGIO 5 Immettere i valori dei seguenti campi:

- **OUI telefonia**: immettere un nuovo OUI.
- **Descrizione**: immettere il nome di un OUI.

PASSAGGIO 6 Fare clic su **Applica**. L'OUI viene aggiunto alla tabella OUI telefonia.

Aggiunta di interfacce alla VLAN voce sulla base di OUI

È possibile assegnare gli attributi QoS in base alla porta ai pacchetti vocali in uno dei seguenti modi:

- **Tutti**: valori di QoS (Quality of Service) configurati per la VLAN vocale applicati a tutti i frame in ingresso ricevuti nell'interfaccia e classificati per la VLAN vocale.
- **Indirizzo MAC origine telefonia**: i valori QoS configurati per la VLAN voce vengono applicati ad ogni frame in ingresso classificato sulla VLAN voce e contenente un OUI nell'indirizzo MAC di origine che corrisponde a un OUI telefonia configurato.

Utilizzare la pagina Interfaccia OUI telefonia per aggiungere un'interfaccia alla VLAN voce sulla base dell'identificatore OUI e per configurare la modalità QoS OUI della VLAN voce.

Per configurare OUI telefonia su un'interfaccia, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **VLAN voce** > **Interfaccia OUI telefonia**.

Nella pagina Interfaccia OUI telefonia vengono visualizzati i parametri OUI VLAN voce per tutte le interfacce.

PASSAGGIO 2 Per configurare un'interfaccia come porta candidata di una VLAN voce basata su OUI telefonia, fare clic su **Modifica.**

PASSAGGIO 3 Immettere i valori dei seguenti campi:

- **Interfaccia**: selezionare un'interfaccia.
- **Appartenenza VLAN OUI telefonia**: se questa opzione è attivata, l'interfaccia è una porta candidata della VLAN voce basata su OUI telefonia. Quando vengono ricevuti i pacchetti che corrispondono a uno degli OUI telefonia configurati, la porta viene aggiunta alla VLAN voce.
- **Modalità QoS OUI telefonia**: selezionare una delle opzioni seguenti:
  - *Tutti*: gli attributi QoS vengono applicati su tutti i pacchetti classificati alla VLAN voce.
  - *Indirizzo MAC origine telefonia*: gli attributi QoS sono applicati solo ai pacchetti provenienti dai telefoni IP.

PASSAGGIO 4 Fare clic su **Applica**. L'OUI è stato aggiunto.

VLAN TV multicast basata su porta di accesso

Le VLAN TV multicast attivano le trasmissioni multicast per gli abbonati che non si trovano sulla stessa VLAN dati (isolata a Livello 2), senza dover duplicare i frame di trasmissione multicast per ciascun abbonato VLAN.

Gli abbonati che non sono sulla stessa VLAN dati (isolata a Livello 2) e sono connessi al dispositivo con un'appartenenza ID VLAN differente possono condividere lo stesso flusso multicast includendo le porte allo stesso ID VLAN multicast.

La porta di rete, connessa al serve multicast, viene configurata staticamente come un membro nell'ID VLAN multicast.

Le porte di rete, tramite cui gli abbonati comunicano con il server multicast (inviando messaggi IGMP), ricevono i flussi multicast dal server multicast, includendo la VLAN TV multicast nell'intestazione del pacchetto multicast. Per questo motivo, le porte di rete devono essere configurate staticamente nel modo seguente:

- Tipo di porta trunk o generica (vedere **Configurazione delle impostazioni interfaccia VLAN**)
- Membro sulla VLAN TV multicast

Le porte di ricezione dell'abbonato possono essere associate alla VLAN TV multicast solo se questa viene definita in uno dei tipi seguenti:

- Porta di accesso
- Porta del cliente (vedere **VLAN TV multicast basata su porta del cliente**)

È possibile associare uno o più gruppi di indirizzi multicast IP alla stessa VLAN TV multicast.

Qualsiasi VLAN è configurabile come VLAN TV multicast. Una porta assegnata alla VLAN TV multicast:

- La VLAN TV multicast viene inclusa.
- i pacchetti che passano dalle porte di uscita nella VLAN TV multicast non hanno tag.
- Il parametro relativo al tipo di frame della porta è impostato su **Ammetti tutti**, consentendo i pacchetti senza tag (vedere **Configurazione delle impostazioni interfaccia VLAN**).

La configurazione VLAN TV multicast viene definita per porta. Le porte del cliente vengono configurate in modo che appartengano alle VLAN TV multicast, utilizzando la pagina VLAN TV multicast.

Snooping IGMP

La VLAN TV multicast si basa sullo snooping IGMP, vale a dire che:

- gli abbonati utilizzano i messaggi IGMP per accedere o abbandonare un gruppo multicast;
- Il dispositivo esegue lo snooping IGMP e configura la porta di accesso in base all'appartenenza multicast sulla VLAN TV multicast.

Il dispositivo decide per ciascun pacchetto IGMP ricevuto su una porta di accesso se associarlo alla VLAN di accesso o alla VLAN TV multicast, in base alle seguenti regole:

- Se un messaggio IGMP viene ricevuto su una porta di accesso, con indirizzo IP multicast di destinazione associato alla VLAN TV multicast della porta, il software associa il pacchetto IGMP alla VLAN TV multicast.
- In caso contrario, il messaggio IGMP viene associato alla VLAN di accesso e il messaggio IGMP viene inoltrato soltanto all'interno di quella VLAN.
- Il messaggio IGMP viene respinto se:
  - Lo stato STP/RSTP sulla porta di accesso è impostato su **respingi**.
  - Lo stato MSTP per la VLAN di accesso è impostato su **respingi**.
  - Lo stato MSTP per la VLAN TV multicast è impostato su **respingi** e il messaggio IGMP viene associato a questa VLAN TV multicast.

Differenze tra VLAN TV regolari e multicast

Confronto delle caratteristiche delle VLAN TV multicast e regolari

	VLAN regolare	VLAN TV multicast
Appartenenza a VLAN	Le porte di origine e tutte quelle di ricezione devono essere membri statici della stessa VLAN dati.	Le porte di origine e di ricezione non possono essere membri nella stessa VLAN dati.

	VLAN regolare	VLAN TV multicast
Registrazione gruppi	La registrazione di tutti i gruppi multicast è dinamica.	I gruppi devono essere associati alla VLAN multicast in modo statico, ma la registrazione effettiva delle stazioni è dinamica.
Porte di ricezione	La VLAN può essere utilizzata per inviare e ricevere traffico (multicast e unicast).	La VLAN multicast può essere utilizzata solo per ricevere il traffico dalle stazioni sulla porta (solo multicast).
Protezione e isolamento	I ricevitori dello stesso flusso multicast sono sulla stessa VLAN dati e possono comunicare tra loro.	I ricevitori dello stesso flusso multicast si trovano in diverse VLAN di accesso e sono isolati gli uni dagli altri.

Configurazione

Flusso di lavoro

Configurare la VLAN TV attenendosi alla seguente procedura:

1. Definire una VLAN TV associando un gruppo multicast a una VLAN (nella pagina Gruppo multicast a VLAN).
2. Specificare le porte di accesso in ciascuna VLAN multicast (nella pagina Appartenenza VLAN multicast basata su porta).

Gruppo TV multicast a VLAN

Per definire la configurazione della VLAN TV multicast, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **VLAN TV multicast basata su porta di accesso > Gruppo multicast a VLAN**.

Vengono visualizzati i seguenti campi:

- **Gruppo multicast**: indirizzo IP del gruppo multicast.
- **VLAN TV multicast**: VLAN a cui assegnare i pacchetti multicast.

PASSAGGIO 2 Scegliere **Aggiungi** per associare una VLAN a un gruppo multicast. È possibile selezionare qualsiasi VLAN. Una volta selezionata, la VLAN si trasforma in VLAN TV multicast.

PASSAGGIO 3 Fare clic su **Applica**. Le impostazioni della VLAN TV multicast vengono modificate e definite nel file Configurazione di esecuzione.

Appartenenza a VLAN multicast basata su porta

Per definire la configurazione della VLAN TV multicast, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Gestione VLAN** > **VLAN TV multicast basata su porta di accesso > Appartenenza VLAN multicast basata su porta**.

PASSAGGIO 2 Scegliere una VLAN dal campo **VLAN TV multicast**.

PASSAGGIO 3 Nell'elenco **Porte di accesso candidato** sono comprese tutte le porte di accesso configurate sul dispositivo. Spostare le porte desiderate dal campo **Porte di accesso candidato** al campo **Porte di accesso membro**.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni della VLAN TV multicast vengono modificate e definite nel file Configurazione di esecuzione.

VLAN TV multicast basata su porta del cliente

Un servizio a riproduzione tripla offre tre servizi a banda larga, oltre a un singola connessione a banda larga:

- Accesso Internet ad alta velocità
- Sorveglianza
- Voce

Il servizio a riproduzione tripla viene fornito agli abbonati di un provider di servizi, garantendo tra i due l'isolamento del Livello 2.

Ciascun abbonato dispone di una casella MUX CPE. Il MUX è dotato di più porte di accesso collegate ai dispositivi dell'abbonato (PC, telefono e così via) e di una porta di rete collegata al dispositivo di accesso.

La casella inoltra i pacchetti dalla porta di rete ai dispositivi dell'abbonato in base al tag VLAN del pacchetto. Ciascuna VLAN è associata a una delle porte di accesso MUX.

I pacchetti che dagli abbonati giungono alla rete del provider di servizi vengono inoltrati come frame con tag VLAN per fare una distinzione tra i tipi di servizio; ciò significa che nella casella CPE a ciascun tipo di servizio corrisponde un unico ID VLAN.

Tutti i pacchetti provenienti dall'abbonato che giungono alla rete del provider di servizi vengono incapsulati dal dispositivo di accesso con la VLAN dell'abbonato configurata come VLAN del cliente (tag esterno o S-VID), ad eccezione dei messaggi di snooping IGMP provenienti dai ricevitori TV che sono associati alla VLAN TV multicast. Inoltre, le informazioni VOD trasmesse dai ricevitori TV vengono inviate come se si trattasse di un qualsiasi altro tipo di traffico.

I pacchetti provenienti dalla rete del provider di servizi e ricevuti sulla porta di rete dell'abbonato vengono inviati sulla rete del provider di servizi come pacchetti con doppio tag, mentre il tag più esterno (S-Tag o Service Tag) costituisce uno dei due tipi di VLAN elencati di seguito:

- VLAN dell'abbonato (include Internet e telefoni IP)
- VLAN TV multicast

La VLAN interna (C-Tag) rappresenta il tag che determina la destinazione nella rete dell'abbonato (da MUX CPE).

Flusso di lavoro

1. Configurare una porta di accesso come porta del cliente (nella pagina Gestione VLAN > Impostazioni interfaccia). Per ulteriori informazioni, vedere la sezione **QinQ**.
2. Configurare la porta di rete come porta di trunk o generica con l'abbonato e la VLAN TV multicast come VLAN con tag (nella pagina Gestione VLAN > Impostazioni interfaccia).
3. Creare una VLAN TV multicast utilizzando fino a 4094 VLAN differenti (le VLAN vengono create tramite la configurazione della gestione di VLAN regolari).
4. Associare la porta del cliente a una VLAN TV multicast nella pagina Appartenenza VLAN multicast basata su porta.
5. Associare la VLAN CPE (C-TAG) alla VLAN TV multicast (S-Tag) nella pagina VLAN CPE a VLAN.

Associazione di VLAN CPE a VLAN TV multicast

Per supportare MUX CPE con le VLAN degli abbonati, questi ultimi potrebbero richiedere più provider di video e a ciascun provider viene assegnata una VLAN esterna differente.

Le VLAN multicast CPE (interne) devono essere associate alle VLAN del provider multicast (esterne).

Una volta che la VLAN CPE è stata associata alla VLAN multicast può prendere parte allo snooping IGMP.

Per associare le VLAN CPE, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione VLAN** > **VLAN TV multicast basata su porta del cliente > VLAN CPE a VLAN**.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere informazioni nei seguenti campi:

- **VLAN CPE**: immettere la VLAN definita nella casella CPE.
- **VLAN TV multicast**: selezionare la VLAN TV multicast da associare alla VLAN CPE.

PASSAGGIO 4 Fare clic su **Applica**. L'associazione VLAN CPE viene modificata e definita nel file Configurazione di esecuzione.

Appartenenza a VLAN multicast basata su porta CPE

Le porte associate alle VLAN multicast devono essere configurate come porte del cliente (vedere **Configurazione delle impostazioni interfaccia VLAN**).

Utilizzare la pagina relativa all'appartenenza VLAN multicast basata su porta per associare tali porte alle VLAN TV multicast come descritto in **Appartenenza a VLAN multicast basata su porta**.

15

Spanning Tree

In questa sezione viene descritto il protocollo Spanning Tree (STP) (IEEE802.1D e IEEE802.1Q) e vengono illustrati i seguenti argomenti:

- **Aspetti del protocollo STP**
- **Configurazione dello Stato STP e delle Impostazioni generali**
- **Definizione delle impostazioni dell'interfaccia di Spanning Tree**
- **Configurazione delle impostazioni di Rapid Spanning Tree**
- **Multiple Spanning Tree**
- **Definizione delle proprietà MSTP**
- **Associazione delle VLAN a un'istanza MSTP.**
- **Definizione delle impostazioni istanza MSTP.**
- **Definizione delle impostazioni interfaccia MSTP**

Aspetti del protocollo STP

Il protocollo STP consente di proteggere un dominio di broadcast di Livello 2 dagli storm broadcast impostando in modo selettivo i collegamenti in modalità standby per impedire il verificarsi di loop. In modalità standby, questi collegamenti eseguono un'interruzione temporanea del trasferimento dei dati utente. Dopo aver modificato la topologia, rendendo possibile il trasferimento dei dati, i collegamenti vengono riattivati automaticamente.

I loop si verificano quando esistono percorsi alternativi tra gli host. In una rete estesa la presenza di loop può causare l'inoltro ciclico di traffico da parte degli switch, con un conseguente incremento del carico di traffico e una riduzione dell'efficienza della rete.

Il protocollo STP fornisce una topologia ad albero per qualsiasi configurazione di switch e una connessione tra i collegamenti, creando un percorso unico tra le stazioni terminali di una rete ed eliminando i loop.

Il dispositivo supporta le seguenti versioni del protocollo STP (Spanning Tree Protocol):

- STP tradizionale, che fornisce un percorso unico tra due stazioni finali qualsiasi, evitando ed eliminando i loop.
- STP rapido (RSTP), che rileva le topologie di rete per fornire una convergenza dello spanning tree più rapida. Quest'ultimo risulta chiaramente il più conveniente quando la topologia di rete è strutturata ad albero, pertanto è possibile rendere una convergenza più rapida. Per impostazione predefinita, RSTP è attivo.
- STP multiplo (MSTP): MSTP è basato sul protocollo RSTP. Rileva i loop di Livello 2 e tenta di diminuirli impedendo la trasmissione del traffico sulla porta interessata. Poiché i loop si verificano in base a un dominio di livello 2, può accadere che ci siano loop nella VLAN A e non nella VLAN B. Se entrambe le VLAN sono poste sulla Porta X e il protocollo STP desidera diminuire il loop, il traffico viene interrotto sull'intera porta, compreso il traffico nella VLAN B.

  MSTP risolve questo problema attivando diverse istanze STP in modo tale da poter rilevare e ridurre i loop separatamente in ciascuna istanza. Associando le istanze alle VLAN, ciascuna istanza viene associata al dominio di livello 2 su cui esegue le operazioni di rilevamento e riduzione dei loop. In questo modo, è possibile bloccare una porta in un'istanza, come il traffico proveniente dalla VLAN A che causa un loop, mentre il traffico rimane attivo in un altro dominio in cui non sono stati rilevati loop, ad esempio sulla VLAN B.

Configurazione dello Stato STP e delle Impostazioni generali

La pagina Stato STP e Impostazioni generali contiene i parametri per l'attivazione di STP, RSTP o MSTP.

Utilizzare la pagina Impostazioni interfaccia STP, la pagina Impostazioni interfaccia RSTP e la pagina Proprietà MSTPper configurare ogni modalità

Per impostare lo stato STP e le impostazioni generali, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Spanning Tree** > **Stato STP e impostazioni generali**.

PASSAGGIO 2 Immettere i parametri.

Impostazioni generali:

- **Stato Spanning Tree**: attivare o disattivare il protocollo STP sul dispositivo.
- **Modalità operativa STP**: selezionare una modalità STP.
- **Gestione BPDU**: selezionare la modalità di gestione dei pacchetti BPDU (Bridge Protocol Data Unit) se STP è disattivato sulla porta o sul dispositivo. I BPDU vengono utilizzati per trasmettere informazioni sull'albero.
  - *Filtro*: i pacchetti BPDU vengono filtrati se lo Spanning Tree è disattivato su un'interfaccia.
  - *Traffico*: i pacchetti BPDU vengono distribuiti se lo Spanning Tree è disattivato su un'interfaccia.
- **Valori predefiniti costo del percorso**: indica il metodo utilizzato per assegnare i costi dei percorsi predefiniti alle porte STP. Il costo dei percorsi predefiniti assegnato a un'interfaccia varia a seconda del metodo selezionato.
  - *Breve*: viene assegnato un valore compreso tra 1 e 65.535 per i costi dei percorsi delle porte.
  - *Lungo*: viene assegnato un valore compreso tra 1 e 200.000.000 per i costi dei percorsi delle porte.

Impostazioni bridge:

- **Priorità**: impostare il valore di priorità del bridge. Dopo lo scambio dei BPDU, il dispositivo con la priorità più bassa diventa il bridge root. Laddove tutti i bridge presentino la stessa priorità vengono utilizzati gli indirizzi MAC per determinare quale rappresenta il bridge root. Il valore di priorità del bridge viene fornito in incrementi di 4096. Ad esempio, 4096, 8192, 12288 e così via.
- **Hello Time**: impostare l'intervallo (in secondi) atteso dal bridge root tra l'invio dei messaggi di configurazione.
- **Tempo massimo**: impostare l'intervallo (in secondi) durante il quale il dispositivo può attendere senza ricevere un messaggio di configurazione, prima di provare a ridefinire la propria configurazione.
- **Ritardo reindirizzamento**: impostare l'intervallo (in secondi) durante il quale un bridge rimane in uno stato di rilevamento prima di reindirizzare i pacchetti. Per ulteriori informazioni, fare riferimento alla **Definizione delle impostazioni dell'interfaccia di Spanning Tree**.

Root designato:

- **ID bridge**: indica la priorità del bridge concatenata con l'indirizzo MAC del dispositivo.
- **ID bridge root**: indica la priorità del bridge root concatenata con l'indirizzo MAC del bridge root.
- **Porta root**: indica la porta che offre il percorso di costo più basso dal bridge al bridge root. Questo valore è importante se il bridge non è il bridge root.
- **Costo percorso root**: indica il costo del percorso dal bridge al root.
- **Numero di modifiche alla topologia**: il numero totale delle modifiche alla topologia STP che si sono verificate.
- **Ultima modifica alla topologia**: indica l'intervallo di tempo trascorso dall'ultima modifica alla topologia verificatasi. Questo intervallo viene visualizzato nel formato giorni/ore/minuti/secondi.

PASSAGGIO 3 Fare clic su **Applica**. Le impostazioni globali STP vengono scritte nel file Configurazione di esecuzione.

Definizione delle impostazioni dell'interfaccia di Spanning Tree

Nella pagina Impostazioni interfaccia STP è possibile configurare il protocollo STP per singola porta e visualizzare le informazioni rilevate dal protocollo, ad esempio il bridge designato.

La configurazione effettuata sarà valida per tutti gli aspetti del protocollo STP.

Per configurare il protocollo STP su un'interfaccia, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Spanning Tree** > **Impostazioni interfaccia STP**.

PASSAGGIO 2 Selezionare un'interfaccia e fare clic su **Modifica**.

PASSAGGIO 3 Immettere i parametri

- **Interfaccia**: selezionare la porta o il LAG sul quale viene configurato lo Spanning Tree.
- **STP**: è possibile attivare o disattivare il protocollo STP sulla porta.
- **Porta Edge**: è possibile attivare Collegamento rapido sulla porta. Se viene attivata la modalità Collegamento rapido su una porta, quest'ultima viene automaticamente impostata sulla modalità di reindirizzamento quando il collegamento della porta è attivo. La modalità Collegamento rapido ottimizza la convergenza del protocollo STP. Sono disponibili le seguenti opzioni:
  - *Attiva*: è possibile attivare subito il Collegamento rapido.
  - *Automatico*: consente di attivare Collegamento rapido pochi secondi dopo che l'interfaccia diventa attiva. Questo consente al protocollo STP di evitare i loop prima di attivare Collegamento rapido.
  - *Disattiva*: consente di disattivare il Collegamento rapido.

    NOTA Si consiglia di impostare il valore su Automatica in modo che la porta venga attivata dal dispositivo in modalità di collegamento rapido se c'è un host collegato oppure che venga attivata come porta STP tradizionale se connessa a un altro dispositivo. Ciò aiuta a evitare i loop.
- **Guardia root**: consente di attivare o disattivare la guardia root sul dispositivo. L'opzione Guardia root offre un modo per applicare la posizione del bridge root nella rete.

Questa opzione garantisce inoltre che tale funzione venga attivata sulla porta designata. In genere, tutte le porte del bridge root sono porte designate, a meno che non ci siano collegate due o più porte del bridge root. Se il bridge riceve un numero maggiore di BPDU su una porta abilitata per la Guardia root, quest'ultima imposta la porta su uno stato STP di incoerenza root. Lo stato di incoerenza root è l'equivalente dello stato di ascolto. Su questa porta il traffico non viene reindirizzato, così la Guardia root applica la posizione del bridge root.

- **Guardia BPDU**: consente di attivare o disattivare la funzione di Guardia BPDU (Bridge Protocol Data Unit) sulla porta.

  La Guardia BPDU consente di applicare i confini del dominio STP e mantiene prevedibile la topologia. I dispositivi dietro le porte abilitate per la Guardia BPDU non possono influenzare la topologia STP. Quando si ricevono i BPDU, il funzionamento della guardia BPDU disattiva la porta configurata con BPDU. In questo caso, oltre a ricevere un messaggio BPDU, viene generato un trap SNMP appropriato.

- **Gestione BPDU**: selezionare la modalità di gestione dei pacchetti BPDU quando STP è disattivato sulla porta o sul dispositivo. I BPDU vengono utilizzati per trasmettere informazioni sull'albero.
  - *Usa Impostazioni generali*: consente di utilizzare le impostazioni definite nella pagina Stato STP e Impostazioni generali.
  - *Filtro*: i pacchetti BPDU vengono filtrati se lo Spanning Tree è disattivato su un'interfaccia.
  - *Traffico*: i pacchetti BPDU vengono distribuiti se lo Spanning Tree è disattivato su un'interfaccia.

- **Costo del percorso**: impostare il contributo della porta al costo del percorso root oppure utilizzare il costo predefinito generato dal sistema.

- **Priorità**: specificare il valore di priorità della porta. Questo valore influenza la scelta della porta quando un bridge dispone di due porte collegate in un loop. La priorità è un valore compreso tra 0 e 240, impostato in incrementi di 16.

- **Stato delle porte**: viene indicato lo stato STP corrente della porta.
  - *Disattivato*: indica che il protocollo STP è correntemente disattivato sulla porta. La porta reindirizza il traffico e rileva gli indirizzi MAC.
  - *Blocco*: la porta è al momento bloccata e non può reindirizzare il traffico (eccetto dati BDPU) o rilevare indirizzi MAC.

- *Ascolto*: la porta è in modalità di ascolto e non è in grado di reindirizzare traffico né di rilevare gli indirizzi MAC.
- *Rilevamento*: indica che la porta è in modalità di rilevamento e non è in grado di reindirizzare il traffico, ma solo di rilevare gli indirizzi MAC.
- *Reindirizzamento*: indica che la porta è in modalità di reindirizzamento ed è in grado di reindirizzare traffico e di rilevare nuovi indirizzi MAC.

- **ID bridge designato**: indica la priorità del bridge e l'indirizzo MAC del bridge designato.
- **ID porta designata**: viene indicata la priorità e l'interfaccia della porta selezionata.
- **Costo designato**: viene indicato il costo della porta che partecipa alla topologia STP. Le porte con un costo inferiore presentano un minor rischio di blocco nel caso in cui STP rilevi dei loop.
- **Reindirizza transizioni**: viene indicato il numero di volte in cui la porta è passata dallo stato di **Blocco** a quello di **Reindirizzamento**.
- **Velocità**: viene visualizzata la velocità della porta.
- **LAG**: indica il LAG a cui appartiene la porta. Se una porta appartiene a un LAG, le impostazioni del LAG annulleranno quelle della porta.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni di interfaccia vengono scritte nel file Configurazione di esecuzione.

Configurazione delle impostazioni di Rapid Spanning Tree

Il protocollo RSTP (Rapid Spanning Tree Protocol) consente una convergenza STP più rapida, senza creare loop di inoltro.

La pagina Impostazioni interfaccia RSTP consente di configurare il protocollo RSTP per porta. Qualsiasi configurazione effettuata in questa pagina sarà attiva se la modalità STP a livello globale è impostata su RSTP o MSTP.

Per immettere le impostazioni RSTP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Spanning Tree** > **Stato STP e impostazioni generali**. Attivare **RSTP**.

PASSAGGIO 2 Scegliere **Spanning Tree** > **Impostazioni interfaccia RSTP**. Viene visualizzata la pagina Impostazioni interfaccia RSTP.

PASSAGGIO 3 Selezionare una porta.

NOTA Attiva migrazione protocollo è disponibile solo dopo aver selezionato la porta collegata al bridge associato su cui viene eseguito il test.

PASSAGGIO 4 Se tramite il protocollo STP si rileva un collegamento associato, fare clic su **Attiva migrazione protocollo** per eseguire un test della migrazione del protocollo. Il test consente di rilevare se il collegamento associato che utilizza il protocollo STP è ancora presente e, in caso affermativo, se è stato trasferito a RSTP o MSTP. Se presente, il dispositivo continua a comunicare con il collegamento STP usando il protocollo STP. Altrimenti, se è passato a RSTP o MSTP, il dispositivo comunicherà utilizzando rispettivamente RSTP o MSTP.

PASSAGGIO 5 Selezionare un'interfaccia e fare clic su **Modifica**.

PASSAGGIO 6 Immettere i seguenti parametri:

- **Interfaccia**: impostare l'interfaccia e specificare la porta o il LAG su cui configurare il protocollo RSTP.
- **Stato amministrativo Point to Point**: definisce lo stato del collegamento point to point. Le porte in modalità full duplex sono considerate collegamenti point to point della porta.
  - *Attiva*: quando la funzione è attiva, la porta diventa una porta edge RSTP e ritorna rapidamente alla modalità di inoltro (generalmente entro 2 secondi).
  - *Disattiva*: la porta non è considerata un point to point per motivi legati al protocollo RSTP, ovvero STP funziona solo ad una velocità regolare, non ad alta velocità.
  - *Automatico*: determina automaticamente lo stato del dispositivo tramite i BPDU RSTP.
- **Stato operativo Point to Point**: indica lo stato operativo point to point se **Stato amministrativo Point to Point** è impostato su automatico.

- **Ruolo**: viene indicato il ruolo della porta assegnato dal protocollo STP per fornire percorsi STP. I ruoli possibili sono:
  - *Root*: percorso con il costo più basso per reindirizzare pacchetti al bridge root.
  - *Designato*: l'interfaccia tramite cui il bridge è connesso alla LAN, che fornisce il percorso dalla LAN al bridge root con il costo più basso.
  - *Alternativo*: fornisce un percorso alternativo dall'interfaccia root al bridge root.
  - *Backup*: fornisce un percorso di backup per la porta designata verso le ramificazioni dell'albero. Fornisce una configurazione in cui due porte sono collegate ad anello tramite un collegamento point to point. Le porte di backup possono essere utilizzate anche quando la rete LAN dispone di due o più connessioni stabilite con un segmento condiviso.
  - *Disattivato*: indica che la porta non fa parte dello Spanning Tree.
- **Modalità**: viene indicata la modalità corrente dell'albero, STP tradizionale o RSTP.
- **Stato operativo collegamento rapido**: indica se il Collegamento rapido (porta edge) dell'interfaccia è attivato, disattivato o automatico. I valori sono:
  - *Attivato*: il Collegamento rapido è attivato.
  - *Disattivato*: il Collegamento rapido è disattivato.
  - *Automatico*: la modalità Collegamento rapido viene attivata pochi secondi dopo che l'interfaccia diventa attiva.
- **Stato delle porte**: indica lo stato RSTP sulla porta specificata.
  - *Disattivato*: indica che il protocollo STP è correntemente disattivato sulla porta.
  - *Blocco*: la porta è correntemente bloccata e non è in grado di reindirizzare il traffico o rilevare indirizzi MAC.
  - *Ascolto*: la porta è in modalità di ascolto e non è in grado di reindirizzare traffico né di rilevare gli indirizzi MAC.
  - *Rilevamento*: indica che la porta è in modalità di rilevamento e che non è in grado di reindirizzare il traffico, ma solo di rilevare gli indirizzi MAC.
  - *Reindirizzamento*: indica che la porta è in modalità di reindirizzamento ed è in grado di reindirizzare traffico e di rilevare nuovi indirizzi MAC.

PASSAGGIO 7 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Multiple Spanning Tree

MSTP (Multiple Spanning Tree Protocol) viene utilizzato per separare lo stato della porta STP tra i vari domini (su VLAN diverse). Ad esempio, se la porta A viene bloccata in un'istanza STP a causa di un loop sulla VLAN A, sulla stessa porta viene attivata la modalità di inoltro in un'altra istanza STP. Nella pagina Proprietà MSTP è possibile definire le impostazioni globali di MSTP.

Per configurare la modalità MSTP, attenersi alla seguente procedura:

1. Impostare la Modalità operativa STP su MSTP, come riportato nella pagina **Configurazione dello Stato STP e delle Impostazioni generali**.
2. Definire le istanze MSTP. Ciascuna istanza MSTP calcola e crea una topologia libera da loop per consentire il passaggio dei pacchetti dalle VLAN associate all'istanza. Fare riferimento alla sezione **Associazione delle VLAN a un'istanza MSTP.**.
3. Decidere quali istanze MSTP attivare in quale VLAN, quindi associarle alle VLAN di conseguenza.
4. Configurare gli attributi MST da:
   - **Definizione delle proprietà MSTP**
   - **Definizione delle impostazioni istanza MSTP.**
   - **Associazione delle VLAN a un'istanza MSTP.**

Definizione delle proprietà MSTP

Il protocollo MSTP a livello globale consente di configurare uno spanning tree diverso in ciascun gruppo VLAN e di bloccare tutti i percorsi alternativi all'interno di ciascuno spanning tree lasciandone disponibile uno. MSTP consente la creazione di regioni MST in grado di eseguire più istanze MST (MSTI). Le regioni e gli altri bridge STP sono connessi tra di loro tramite un albero comune (CST, Common spanning tree).

MSTP è del tutto compatibile con i bridge RSTP, in cui è possibile interpretare un BDPU MSTP come un BDPU RSTP tramite un bridge RSTP. Inoltre, non solo è compatibile con i bridge RSTP senza dover modificare la configurazione, ma consente anche di visualizzare tutti i bridge RSTP esterni a una regione MSTP come un singolo bridge RSTP, indipendentemente dal numero di bridge MSTP che si trovano nella regione.

I due o più switch che si trovano nella stessa regione MSTP devono presentare un'associazione delle stesse VLAN all'istanza MST, lo stesso numero di versione della configurazione e lo stesso nome della regione.

Gli switch che si trovano nella stessa regione MST non vengono mai separati dagli switch posti in un'altra regione MST, altrimenti la regione si divide in due, creando due regioni separate.

Questa associazione può essere effettuata nella pagina VLAN a istanza MST.

Utilizzare questa pagina se il sistema funziona in modalità MSTP.

Per definire la modalità MSTP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Spanning Tree** > **Stato STP e impostazioni generali**. Attivare la modalità MSTP.

PASSAGGIO 2 Scegliere **Spanning Tree** > **Proprietà MSTP**.

PASSAGGIO 3 Immettere i parametri.

- **Nome regione**: definire un nome per la regione MSTP.
- **Revisione**: viene indicato il numero senza segno a 16 bit che identifica la versione della configurazione MST corrente, specificando un valore compreso tra 0 e 65535.
- **Passaggi max**: impostare il numero totale di passaggi che si verificano in una regione specifica prima che il pacchetto BPDU venga eliminato. In tal caso le informazioni sulla porta diventano obsolete, specificando un valore compreso tra 1 e 40.
- **Master IST**: indica l'IST principale della regione.

PASSAGGIO 4 Fare clic su **Applica**. Le proprietà MSTP vengono definite e il file di Configurazione di esecuzione viene aggiornato.

Associazione delle VLAN a un'istanza MSTP.

Nella pagina VLAN a istanza MSTP è possibile associare ciascuna VLAN a un'istanza Multiple Spanning Tree (MSTI). I dispositivi che si trovano nella stessa regione devono avere la stessa associazione tra VLAN e MSTI.

NOTA È possibile associare la stessa MSTI a più VLAN, ma ciascuna di queste può essere associata a un'unica istanza MST.

La configurazione effettuata su questa pagina (e in tutte le pagine MSTP) viene applicata se la modalità STP del sistema è MSTP.

Sugli switch della serie 500 è possibile definire massimo 16 istanze MST, oltre all'istanza zero.

Per le VLAN non esplicitamente associate a una delle istanze MST, il dispositivo le associa automaticamente all'istanza CIST (Core and Internal Spanning Tree). L'istanza CIST è un'istanza MST 0.

Per associare VLAN a istanze MST, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Spanning Tree** > **VLAN a istanza MSTP**.

La pagina VLAN a istanza MSTP include i campi seguenti:

- **ID istanza MSTP**: vengono visualizzate tutte le istanze MST.
- **VLAN**: vengono visualizzate tutte le VLAN appartenenti all'istanza MST.

PASSAGGIO 2 Per aggiungere una VLAN a un'istanza MSTP, selezionare l'istanza MST e fare clic su **Modifica**.

PASSAGGIO 3 Immettere i parametri.

- **ID istanza MSTP**: selezionare l'istanza MST.
- **VLAN**: definire le VLAN associate a questa istanza MST.
- **Azione**: definire se **Aggiungere** (associare) la VLAN all'istanza MST o **rimuoverla**.

PASSAGGIO 4 Fare clic su **Applica**. Le associazioni MSTP VLAN sono definite e il file di Configurazione di esecuzione viene aggiornato.

Definizione delle impostazioni istanza MSTP.

Nella pagina Impostazioni istanza MSTP è possibile configurare e visualizzare i parametri di ciascuna istanza MST. Questa configurazione equivale alla configurazione per istanza della pagina di *configurazione dello stato STP e delle impostazioni globali*.

Per immettere l'istanza MSTP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Spanning Tree** > **MSTP Impostazioni istanza**.

PASSAGGIO 2 Immettere i parametri.

- **ID istanza**: selezionare un'istanza MST da visualizzare e specificare.
- **VLAN incluse**: vengono indicate le VLAN associate all'istanza selezionata. L'associazione predefinita è quella tra tutte le VLAN all'istanza (istanza 0) dell'albero interno comune (CIST).
- **Priorità bridge**: impostare la priorità del bridge per l'istanza MST selezionata.
- **ID bridge root designato**: indica la priorità e l'indirizzo MAC del bridge root per l'istanza MST.
- **Porta root**: viene indicata la porta root dell'istanza selezionata.
- **Costo percorso root**: viene indicato il costo del percorso root dell'istanza selezionata.
- **ID bridge**: indica la priorità del bridge e l'indirizzo MAC del dispositivo per l'istanza selezionata.
- **Passaggi restanti**: viene indicato il numero di passaggi restanti necessari per raggiungere la destinazione successiva.

PASSAGGIO 3 Fare clic su **Applica**. La configurazione istanza MST viene definita e il file di Configurazione di esecuzione viene aggiornato.

Definizione delle impostazioni interfaccia MSTP

Nella pagina Impostazioni interfaccia MSTP è possibile configurare le impostazioni MSTP della porta per ciascuna istanza MST e visualizzare le informazioni correntemente rilevate dal protocollo, come quelle relative al bridge designato per istanza MST.

Per configurare le porte in un'istanza MST, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Spanning Tree** > **MSTP Impostazioni interfaccia**.

PASSAGGIO 2 Immettere i parametri.

- **Istanza uguale a**: selezionare un'istanza MSTP da configurare.
- **Tipo di interfaccia uguale a**: scegliere se visualizzare l'elenco delle porte o dei LAG.

PASSAGGIO 3 Scegliere **Vai**. Vengono visualizzati i parametri MSTP per le interfacce dell'istanza.

PASSAGGIO 4 Selezionare un'interfaccia e fare clic su **Modifica**.

PASSAGGIO 5 Immettere i parametri.

- **ID istanza**: selezionare un'istanza MST da configurare.
- **Interfaccia**: selezionare l'interfaccia per cui definire le impostazioni MSTI.
- **Priorità interfaccia**: impostare la priorità della porta e l'istanza MST per l'interfaccia specificata.
- **Costo del percorso**: immettere il contributo della porta al costo del percorso root nella casella di testo **Definito dall'utente** oppure selezionare **Usa predefinito** per utilizzare il valore predefinito.
- **Stato della porta**: indica lo stato MSTP della porta specificata su una determinata istanza MST. I parametri vengono definiti come:
  - *Disattivato*: il protocollo STP è correntemente disattivato.
  - *Blocco*: la porta sull'istanza è al momento bloccata e non può reindirizzare traffico (eccetto dati BDPU) o rilevare indirizzi MAC.
  - *Ascolto*: la porta sull'istanza è in modalità di ascolto e non è in grado di reindirizzare traffico né di rilevare gli indirizzi MAC.
  - *Rilevamento*: la porta sull'istanza è in modalità di rilevamento e non è in grado di reindirizzare il traffico, ma solo di rilevare gli indirizzi MAC.

- *Inoltro*: indica che la porta sull'istanza è in modalità di inoltro ed è in grado di reindirizzare traffico e di rilevare nuovi indirizzi MAC.
- *Confine*: la porta sull'istanza è una porta di confine. Il suo stato dipende dall'istanza 0 ed è possibile visualizzarlo nella pagina Impostazioni interfaccia STP.

- **Ruolo della porta**: viene indicato il ruolo della porta o del LAG di ciascuna istanza, assegnato tramite l'algoritmo MSTP al fine di fornire i percorsi STP:
  - *Root*: il reindirizzamento dei pacchetti tramite questa interfaccia fornisce il percorso con il costo più basso per reindirizzare pacchetti al dispositivo root.
  - *Designato*: l'interfaccia tramite cui il bridge è connesso alla LAN, che fornisce il percorso dalla LAN al bridge root dell'istanza MST con il costo più basso.
  - *Alternativo*: l'interfaccia fornisce un percorso alternativo per raggiungere il dispositivo root dall'interfaccia root.
  - *Backup*: l'interfaccia fornisce un percorso di backup per la porta designata verso le ramificazioni dell'albero. È possibile impostare una porta di backup se due porte sono collegate ad anello tramite un collegamento point to point. Le porte di backup possono essere create anche quando la rete LAN dispone di due o più connessioni stabilite con un segmento condiviso.
  - *Disattivato*: indica che l'interfaccia non fa parte dell'albero.
  - *Confine*: la porta sull'istanza è una porta di confine. Il suo stato dipende dall'istanza 0 ed è possibile visualizzarlo nella pagina Impostazioni interfaccia STP.
- **Modalità**: viene indicata la modalità corrente dell'albero dell'interfaccia.
  - Se il partner di collegamento sta utilizzando MSTP o RSTP, la modalità della porta visualizzata sarà RSTP.
  - Se il partner di collegamento sta utilizzando STP, la modalità della porta visualizzata sarà STP.
- **Tipo**: viene visualizzato il tipo MSTP della porta.
  - *Confine* : una porta di confine consente di collegare bridge MST a una LAN in una regione remota. Se la porta è di confine, indica anche se il dispositivo sull'altro lato del collegamento funziona in modalità RSTP o STP.

- *Interno*: indica che la porta è interna.

- **ID bridge designato**: viene indicato il numero ID del bridge che connette il collegamento o la rete LAN condivisa alla root.
- **ID porta designata**: viene indicato il numero ID della porta sul bridge designato che connette il collegamento o la rete LAN condivisa alla root.
- **Costo designato**: viene indicato il costo della porta che partecipa alla topologia STP. Le porte con un costo inferiore presentano un minor rischio di blocco nel caso in cui STP rilevi dei loop.
- **Passaggi restanti**: vengono indicati i passaggi restanti necessari per raggiungere la destinazione successiva.
- **Reindirizza transizioni**: viene indicato il numero di volte che la porta è passata dallo stato di inoltro a quello di blocco.

PASSAGGIO 6 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

16

Gestione tabelle Indirizzi MAC

In questa sezione viene spiegato come aggiungere gli indirizzi MAC al sistema. Vengono trattati i seguenti argomenti:

- **Configurazione di indirizzi MAC statici**
- **Gestione degli indirizzi MAC dinamici**
- **Definizione di Indirizzi MAC riservati**

Tipi di indirizzi MAC

Ci sono due tipi di indirizzi MAC: statico e dinamico. A seconda del tipo, gli indirizzi MAC vengono memorizzati nella tabella *Indirizzi statici* o nella tabella *Indirizzi dinamici* insieme alle informazioni sulla VLAN e sulla porta.

Gli indirizzi statici vengono configurati dall'utente, pertanto non hanno una scadenza.

Un nuovo indirizzo MAC di origine, visualizzato in un frame che arriva al dispositivo, viene aggiunto alla tabella degli indirizzi dinamici. Questo indirizzo MAC viene mantenuto per un periodo di tempo configurabile. Se al dispositivo non arriva nessun altro frame con lo stesso indirizzo MAC di origine prima che il tempo scada, la voce MAC viene eliminata dalla tabella.

Quando riceve un frame, il dispositivo cerca una voce di indirizzo MAC di destinazione corrispondente nella tabella dinamica o statica. Se viene trovata una corrispondenza, il frame viene contrassegnato per l'uscita in una porta specifica della tabella. Se i frame vengono inviati a un indirizzo MAC che non viene trovato nelle tabelle, vengono trasmessi/distribuiti a tutte le porte della VLAN selezionata. Questi frame sono detti anche frame unicast sconosciuti.

Il dispositivo supporta massimo 8.000 indirizzi MAC statici e dinamici.

Configurazione di indirizzi MAC statici

È possibile assegnare indirizzi MAC statici a un'interfaccia fisica e una VLAN specifiche sul dispositivo. Se un indirizzo viene rilevato su un'altra interfaccia, viene ignorato e non viene definito nella tabella degli indirizzi.

Per definire un indirizzo statico, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Tabelle Indirizzi MAC > Indirizzi statici**.

Nella pagina Indirizzi statici vengono visualizzati gli indirizzi statici definiti.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **ID VLAN**: selezionare l'ID VLAN della porta.
- **Indirizzo MAC**: immettere l'indirizzo MAC dell'interfaccia.
- **Interfaccia**: selezionare un'interfaccia (unità/slot, porta o LAG) per la voce.
- **Stato**: selezionare come viene trattata la voce. Sono disponibili le seguenti opzioni:
  - *Permanente*: l'indirizzo MAC non viene mai rimosso dal sistema. Se l'indirizzo MAC statico viene salvato nella configurazione di avvio, verrà mantenuto anche dopo il riavvio.
  - *Elimina durante il ripristino*: l'indirizzo MAC statico viene eliminato al ripristino del dispositivo.
  - *Elimina durante il timeout*: l'indirizzo MAC viene eliminato quando diventa obsoleto.
  - *Sicuro*: l'indirizzo MAC è sicuro quando l'interfaccia è in modalità bloccata tradizionale (vedere **Configurazione della sicurezza della porta**).

PASSAGGIO 4 Fare clic su **Applica**. Nella tabella viene aggiunta una nuova voce.

Gestione degli indirizzi MAC dinamici

La tabella degli indirizzi dinamici (tabella di bridging) contiene gli indirizzi MAC acquisiti durante il monitoraggio degli indirizzi di origine dei frame in arrivo sul dispositivo.

Per impedire l'overflow della tabella e per fare spazio a nuovi indirizzi, viene eliminato un indirizzo se per un determinato periodo di tempo non si rileva traffico corrispondente. Questo periodo di tempo è l'intervallo temporale.

Configurazione della validità temporale dell'indirizzo MAC dinamico

Per configurare l'intervallo temporale degli indirizzi dinamici, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Tabelle Indirizzi MAC > Impostazioni indirizzo dinamico**.

PASSAGGIO 2 Immettere **Validità temporale**. La validità temporale è un valore compreso tra il valore configurato dall'utente e il doppio di quel valore meno 1. Per esempio, se si immette 300 secondi, la validità temporale è compresa tra 300 e 599 secondi.

PASSAGGIO 3 Fare clic su **Applica**. La validità temporale viene aggiornata.

Ricerca di indirizzi dinamici

Per eseguire ricerche di indirizzi dinamici, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Tabelle Indirizzi MAC > Indirizzi dinamici**.

PASSAGGIO 2 Nel blocco *Filtra*, è possibile immettere i seguenti criteri di ricerca:

- **ID VLAN**: immettere l'ID VLAN ricercato nella tabella.
- **Indirizzo MAC**: immettere l'indirizzo MAC ricercato nella tabella.
- **Interfaccia**: selezionare l'interfaccia ricercata nella tabella. È possibile cercare unità/slot, porte o LAG specifici.

PASSAGGIO 3 Immettere la **Chiave di ordinamento tabella Indirizzi dinamici**: compilare il campo in base al quale è ordinata la tabella. La tabella degli indirizzi può essere ordinata per ID VLAN, indirizzo MAC o interfaccia.

PASSAGGIO 4 Scegliere **Vai**. La ricerca viene eseguita nella tabella Indirizzi MAC dinamici e i risultati vengono visualizzati.

Scegliere **Cancella tabella** per eliminare tutti gli indirizzi MAC dinamici.

Definizione di Indirizzi MAC riservati

Se il dispositivo riceve un frame con un indirizzo MAC di destinazione appartenente a un intervallo riservato (in base allo standard IEEE), il frame può essere eliminato o connesso. La voce nella tabella Indirizzi MAC riservati può indicare l'indirizzo MAC riservato o l'indirizzo MAC riservato e un tipo di frame.

Per aggiungere una voce per un indirizzo MAC riservato, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Tabelle Indirizzi MAC > Indirizzi MAC riservati**. Viene visualizzata la pagina Indirizzi MAC riservati.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i valori dei seguenti campi:

- **Indirizzo MAC**: selezionare l'indirizzo MAC da riservare.
- **Tipo di frame**: selezionare un tipo di frame in base ai seguenti criteri:
  - *Ethernet V2*: si applica ai pacchetti Ethernet V2 con l'indirizzo MAC specifico.
  - *LLC*: si applica ai pacchetti LLC (Logical Link Control) con l'indirizzo MAC specifico.
  - *LLC-SNAP*: si applica ai pacchetti LLC-SNAP (Logical Link Control/Sub-Network Access Protocol) con l'indirizzo MAC specifico.
  - *Tutti*: si applica a tutti i pacchetti con l'indirizzo MAC specifico.
- **Azione**: selezionare una delle seguenti azioni da eseguire alla ricezione del pacchetto corrispondente ai criteri selezionati:
  - *Elimina*: eliminare il pacchetto.
  - *Crea bridge*: reindirizzare il pacchetto a tutti i membri VLAN.

Fare clic su **Applica**. Viene riservato un nuovo indirizzo MAC.

17

Multicast

In questa sezione viene descritta la funzione di reindirizzamento multicast e vengono trattati i seguenti argomenti:

- **Inoltro multicast**
- **Definizione delle proprietà multicast**
- **Aggiunta dell'indirizzo MAC di gruppo**
- **Aggiunta dell'indirizzo IP gruppo Multicast**
- **Configurazione dello snooping IGMP**
- **Snooping MLD**
- **Ricerca gruppo IP Multicast IGMP/MLD**
- **Definizione delle porte router multicast**
- **Definizione dell'inoltro di tutti i multicast**
- **Definizione delle impostazioni Multicast non registrato**

Inoltro multicast

Il reindirizzamento multicast consente una distribuzione delle informazioni di tipo "uno a molti". Le applicazioni multicast sono utili per diffondere informazioni su più client che non richiedono la ricezione dell'intero contenuto. Una tipica applicazione è un servizio simile al cavo TV, in cui i client possono raggiungere un canale durante la trasmissione e abbandonarlo prima che questa giunga al termine.

I dati vengono inviati solo a specifiche porte. Il reindirizzamento di dati solo a specifiche porte consente di mantenere la larghezza di banda e le risorse dell'host sui collegamenti.

Per poter utilizzare il reindirizzamento multicast è necessario che tutte le sottoreti IP, i nodi e i router siano abilitati al multicast. Un nodo abilitato al multicast deve essere in grado di eseguire le seguenti operazioni:

- Inviare e ricevere pacchetti multicast.
- Registrare gli indirizzi multicast in ascolto dal nodo con i router locali, in modo che i router locali e remoti siano in grado di instradare il pacchetto multicast verso i nodi.

Tipica configurazione multicast

Mentre i router multicast instradano pacchetti multicast tra le sottoreti IP, gli switch di livello 2 abilitati al multicast reindirizzano i pacchetti multicast ai nodi registrati all'interno di una LAN o una VLAN.

In una configurazione tipica, un router reindirizza i flussi multicast tra reti IP private e/o pubbliche, un dispositivo con funzionalità snooping IGMP (Internet Group Membership Protocol) o MLD (Multicast Listener Discovery) e un client multicast che deve ricevere un flusso multicast. In questa configurazione, il router invia periodicamente query IGMP.

NOTA MLD per IPv6 deriva dalla versione 2 di IGMP per IPv4. Nonostante in questa sezione gran parte delle istruzioni facciano riferimento all'IGMP, dove richiesto, vengono affrontati anche argomenti legati a MLD.

Le query raggiungono il dispositivo che, a sua volta, le inoltra alla VLAN e acquisisce la porta in cui si trova un router multicast (MRouter). Quando un host riceve una query IGMP, risponde con un messaggio IGMP Join che riporta che l'host vuole ricevere un flusso multicast specifico e, se possibile, da una specifica origine. Il dispositivo con snooping IGMP analizza i messaggi Join e rileva che il flusso multicast richiesto dall'host deve essere reindirizzato su una porta specifica, quindi reindirizzerà il messaggio IGMP Join soltanto all'MRouter. Analogamente, quando l'MRouter riceve un messaggio IGMP Join, rileva l'interfaccia da cui ha ricevuto i messaggi Join e che deve ricevere un flusso Multicast. L'MRouter reindirizza all'interfaccia il flusso multicast richiesto.

In un servizio multicast di livello 2, uno switch di livello 2 riceve un singolo frame destinato a un determinato indirizzo multicast e crea copie del frame da trasmettere su ciascuna porta selezionata.

Quando il dispositivo con snooping IGMP/MLD attivato riceve un frame per un flusso multicast, lo reindirizza a tutte le porte registrate per ricevere il flusso multicast tramite i messaggi IGMP Join.

Il dispositivo può reindirizzare i flussi multicast in base a una delle seguenti opzioni:

- Indirizzo gruppo MAC Multicast
- Indirizzo IP gruppo Multicast (G)
- Una combinazione dell'indirizzo IP di origine (S) e l'indirizzo IP gruppo multicast di destinazione (G) del pacchetto multicast.

È possibile configurare una di queste in base alla VLAN.

Il sistema conserva elenchi di gruppi multicast per ciascuna VLAN, e questo consente di gestire le informazioni multicast ricevute da ogni porta. I gruppi multicast e le porte di ricezione possono essere configurate staticamente o acquisite dinamicamente tramite lo snooping dei protocolli IGMP o Multicast Listener Discovery (MLD).

La registrazione multicast è il processo di ascolto e risposta ai protocolli di registrazione multicast. I protocolli disponibili sono IGMP per IPv4 e MLD per IPv6.

Se su un dispositivo che si trova su una VLAN viene attivato lo snooping IGMP/MLD, vengono analizzati i pacchetti IGMP/MLD ricevuti dalla VLAN collegata allo switch e ai router multicast della rete.

Quando un dispositivo rileva che un host utilizza messaggi IGMP/MLD per registrare e ricevere un flusso multicast, facoltativamente da un'origine specifica, aggiunge la registrazione nel database MFDB (Multicast Forwarding Data Base).

Lo snooping IGMP/MLD consente effettivamente di ridurre il traffico multicast dal flusso delle applicazioni IP che utilizzano un'ampia larghezza di banda. Un dispositivo con snooping IGMP/MLD abilitato reindirizza il traffico multicast solo agli host coinvolti. La riduzione del traffico multicast riduce l'elaborazione dei pacchetti sul dispositivo e il carico di lavoro sugli host finali, che non devono ricevere e filtrare tutto il traffico multicast generato nella rete.

Le versioni supportate sono le seguenti:

- IGMP v1/v2/ v3
- MLD v1/v2
- Un interrogante snooping IGMP semplice

Un interrogante IGMP consente di semplificare il protocollo IGMP su una determinata sottorete. Generalmente, un router multicast è anche un interrogante GMP. Quando in una sottorete ci sono più interroganti IGMP, le query ne selezionano uno come principale.

È possibile configurare il dispositivo come interrogante IGMP di backup o in mancanza di un regolare interrogante IGMP. Il dispositivo non è un interrogante IGMP con funzionalità complete.

Se il dispositivo viene attivato come interrogante IGMP, viene avviato 60 secondi dopo il suo passaggio da un router multicast senza aver individuato traffico IGMP (query). Se sono presenti altri interroganti IGMP, il dispositivo potrebbe o meno bloccare l'invio di query, a seconda dei risultati ottenuti dal processo di selezione dell'interrogante standard.

Proprietà indirizzo multicast

Gli indirizzi multicast presentano le proprietà seguenti:

- Ciascun indirizzo multicast IPv4 è compreso nell'intervallo di indirizzi tra 224.0.0.0 e 239.255.255.255.
- L'indirizzo multicast IPv6 è FF00:/8.
- Per associare un indirizzo IP gruppo multicast a un indirizzo multicast di livello 2, attenersi alla seguente procedura:
  - Per quanto riguarda IPv4, l'associazione avviene ottenendo 23 bit di ordine basso dall'indirizzo IPv4 e aggiungendoli al prefisso 01:00:5e. Per impostazione predefinita, i nove bit più alti dell'indirizzo IP vengono ignorati e tutti gli indirizzi IP che differiscono soltanto nel valore di questi bit più alti vengono associati allo stesso indirizzo di livello 2, poiché i 23 bit più bassi utilizzati sono gli stessi. Ad esempio, 234.129.2.3 viene associato a un indirizzo gruppo MAC multicast 01:00:5e:01:02:03. Allo stesso indirizzo di livello 2, è possibile associare un massimo di 32 indirizzi gruppo IP multicast.
  - Per l'IPv6, l'associazione avviene ottenendo i 32 bit di ordine basso dell'indirizzo multicast e aggiungendoli con il prefisso 33:33. Ad esempio, l'indirizzo multicast IPv6, ovvero FF00:1122:3344, viene associato al multicast di livello 2, che è 33:33:11:22:33:44.

Definizione delle proprietà multicast

Nella pagina *Proprietà* è possibile configurare lo stato del filtro multicast bridge.

Per impostazione predefinita, tutti i frame multicast vengono distribuiti a tutte le porte della VLAN. Per eseguire il reindirizzamento in modo selettivo, quindi soltanto alle porte selezionate, e per filtrare (eliminare) il multicast sulle porte rimanenti, attivare lo stato di filtro multicast bridge nella pagina Proprietà.

Se il filtro è attivato, i frame multicast vengono reindirizzati a un subset di porte all'interno della VLAN selezionata, come definito nel database MFDB. Il filtro multicast viene applicato su tutto il traffico. Per impostazione predefinita, tale traffico viene distribuito a tutte le porte selezionate, ma è possibile limitare il reindirizzamento a una sottoserie più piccola.

Un modo comune per indicare l'appartenenza multicast è la notazione (S,G) in cui "S" è l'origine (singola) da cui viene inviato un flusso di dati multicast e "G" è l'indirizzo del gruppo IPv4 o IPv6. Un client multicast in grado di ricevere traffico multicast da qualsiasi origine di un gruppo multicast specifico viene salvato come (*,G).

Il reindirizzamento dei frame multicast può avvenire nei modi seguenti:

- **Indirizzo MAC di gruppo**: in base all'indirizzo MAC di destinazione all'interno del frame Ethernet.

  NOTA Come specificato in precedenza, è possibile associare uno o più indirizzi IP di gruppo multicast a un indirizzo MAC di gruppo. Il reindirizzamento basato su indirizzi MAC di gruppo può comportare il reindirizzamento di un flusso multicast IP a porte che non dispongono di ricevitori per quel flusso.

- **Indirizzo IP di gruppo**: in base all'indirizzo IP di destinazione del pacchetto IP (*,G).
- **Indirizzo IP di gruppo specifico dell'origine**: in base sia all'indirizzo IP di destinazione che all'indirizzo IP di origine del pacchetto IP (S,G).

Se si seleziona la modalità di reindirizzamento, è possibile definire il metodo usato dall'hardware per identificare il flusso multicast in base a una delle seguenti opzioni : Indirizzo MAC di gruppo, Indirizzo IP di gruppo o Indirizzo IP di gruppo specifico dell'origine.

(S,G) è supportato da IGMPv3 e MLDv2, mentre IGMPv1/2 e MLDv1 supportano solo (*.G) che corrisponde solo all'ID del gruppo.

Il dispositivo supporta massimo 256 indirizzi di gruppo multicast statici e dinamici.

Per attivare il filtro multicast e selezionare il metodo di reindirizzamento, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Multicast> Proprietà**.

PASSAGGIO 2 Immettere i parametri.

- **Stato filtro multicast bridge**: selezionare questa opzione per attivare il filtro.
- **ID VLAN**: selezionare ID VLAN per impostare il metodo di reindirizzamento.
- **Metodo di reindirizzamento per IPv6**: impostare uno dei seguenti metodi di reindirizzamento per gli indirizzi IPv6. Indirizzo MAC di gruppo, Indirizzo IP di gruppo o Indirizzo IP di gruppo specifico dell'origine.
- **Metodo di reindirizzamento per IPv4**: impostare uno dei seguenti metodi di reindirizzamento per gli indirizzi IPv4. Indirizzo MAC di gruppo, Indirizzo IP di gruppo o Indirizzo IP di gruppo specifico dell'origine.

PASSAGGIO 3 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Aggiunta dell'indirizzo MAC di gruppo

Il dispositivo supporta il reindirizzamento del traffico multicast in ingresso sulla base delle informazioni del gruppo multicast. Tali informazioni provengono dai pacchetti IGMP/MLD ricevuti o dalla configurazione manuale e vengono conservati nel Multicast Forwarding Database (MFDB).

Quando si riceve un frame da una VLAN configurata per reindirizzare i flussi multicast sulla base degli indirizzi MAC di gruppo e il cui indirizzo di destinazione è un indirizzo multicast di livello 2, il frame viene reindirizzato a tutte le porte appartenenti all'indirizzo MAC di gruppo.

La pagina Indirizzo MAC di gruppo ha le seguenti funzioni:

- Richiedere e visualizzare informazioni contenute nel database MFDB a un ID VLAN o un gruppo di indirizzi MAC specifico. I dati vengono acquisiti dinamicamente attraverso lo snooping IGMP/MLD oppure staticamente tramite un inserimento manuale.
- Aggiungere o eliminare voci statiche dal database MFDB che forniscono informazioni sul reindirizzamento statico sulla base degli indirizzi MAC di destinazione.

- Visualizzare un elenco di tutte le porte/LAG appartenenti a ciascun ID VLAN e gruppo di indirizzi MAC e indicare l'eventuale reindirizzamento del traffico.

Per visualizzare le informazioni sul reindirizzamento quando la modalità è *Indirizzo IP di gruppo* o *Gruppo IP e di origine*, utilizzare la pagina Indirizzo IP gruppo multicast.

Per definire e visualizzare i gruppi MAC multicast, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Multicast> Indirizzo MAC di gruppo**.

PASSAGGIO 2 Immettere i parametri.

- **ID VLAN uguale a**: impostare l'ID VLAN del gruppo da visualizzare.
- **Indirizzo MAC di gruppo uguale a**: impostare l'indirizzo MAC del gruppo multicast da visualizzare. Se non è stato specificato un indirizzo MAC di gruppo, nella pagina verranno visualizzati tutti gli indirizzi MAC di gruppo della VLAN selezionata.

PASSAGGIO 3 Scegliere **Vai** e gli indirizzi MAC di gruppo multicast verranno visualizzati nell'area in basso.

Vengono visualizzate le voci che sono state create sia in questa pagina che nella pagina Indirizzo IP gruppo multicast. Per le voci create nella pagina Indirizzo IP gruppo Multicast, gli indirizzi IP vengono convertiti in indirizzi MAC.

PASSAGGIO 4 Scegliere **Aggiungi** per aggiungere un indirizzo MAC di gruppo statico.

PASSAGGIO 5 Immettere i parametri.

- **ID VLAN**: indica l'ID VLAN del nuovo gruppo multicast.
- **Indirizzo MAC di gruppo**: indica l'indirizzo MAC del nuovo gruppo multicast.

PASSAGGIO 6 Fare clic su **Applica** per salvare il gruppo MAC multicast nel file di configurazione esecuzione.

Per configurare e visualizzare la registrazione delle interfacce all'interno del gruppo, selezionare un indirizzo e fare clic su **Dettagli**.

Nella pagina sono visualizzati i campi seguenti:

- **ID VLAN**: l'ID VLAN del gruppo multicast.
- **Indirizzo MAC di gruppo**: l'indirizzo MAC del gruppo.

PASSAGGIO 7 Selezionare la porta o il LAG da visualizzare dal menu **Filtra: Tipo di interfaccia**.

PASSAGGIO 8 Scegliere **Vai** per visualizzare l'appartenenza alla porta o al LAG.

PASSAGGIO 9 Selezionare il modo in cui associare ciascuna interfaccia con il gruppo multicast:

- **Statico**: collega l'interfaccia al gruppo multicast come membro statico.
- **Dinamico**: indica che, in seguito allo snooping IGMP/MLD, l'interfaccia è stata aggiunta al gruppo multicast.
- **Vietato**: specifica che la porta non può essere associata a questo gruppo su questa VLAN.
- **Nessuno**: indica che la porta attualmente non appartiene a questo gruppo multicast della VLAN.

PASSAGGIO 10 Scegliere **Applica** e il file con la Configurazione di esecuzione viene aggiornato.

NOTA Le voci che sono state create nella pagina Indirizzo IP gruppo multicast non possono essere eliminate in questa pagina (anche se sono selezionate).

Aggiunta dell'indirizzo IP gruppo Multicast

La pagina Indirizzo IP gruppo multicast è simile alla pagina Indirizzo MAC di gruppo; l'unica differenza consiste nel fatto che i gruppi multicast sono identificati dagli indirizzi IP.

La pagina Indirizzo IP gruppo multicast consente l'interrogazione e l'aggiunta di gruppi multicast IP.

Per definire e visualizzare i gruppi IP multicast, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Multicast> Indirizzo IP gruppo Multicast**.

Nella pagina vengono visualizzati tutti gli indirizzi IP gruppo Multicast acquisiti dallo snooping.

PASSAGGIO 2 Immettere i parametri necessari per il filtro.

- **ID VLAN uguale a**: indicare l'ID VLAN del gruppo da visualizzare.
- **Versione IP uguale a**: selezionare IPv6 o IPv4.

- **Indirizzo IP gruppo Multicast uguale a**: indicare l'indirizzo IP del gruppo multicast da visualizzare. Questa operazione è utile solo per la modalità di reindirizzamento (S,G).
- **Indirizzo IP di origine uguale a**: indicare l'indirizzo IP di origine del dispositivo di invio. Se la modalità è (S,G), immettere il mittente S che, insieme all'Indirizzo IP di gruppo, costituisce l'ID del gruppo multicast (S,G) da visualizzare. Se la modalità è (*.G), inserire un * per indicare che il gruppo multicast viene definito soltanto tramite la destinazione.

PASSAGGIO 3 Fare clic su **Vai**. I risultati verranno visualizzati nell'area sottostante. Se su un dispositivo in modalità di sistema Livello 2 sono attivati Bonjour e IGMP, viene visualizzato l'indirizzo multicast IP di Bonjour. Per i dispositivi SG500X/ESW2-550X, l'indirizzo viene visualizzato sempre.

PASSAGGIO 4 Fare clic su **Vai**. I risultati verranno visualizzati nell'area sottostante.

PASSAGGIO 5 Scegliere **Aggiungi** per aggiungere un indirizzo IP gruppo Multicast statico.

PASSAGGIO 6 Immettere i parametri.

- **ID VLAN**: indica l'ID VLAN del gruppo da aggiungere.
- **Versione IP**: selezionare il tipo di indirizzo IP.
- **Indirizzo IP gruppo Multicast**: indica l'indirizzo IP del nuovo gruppo multicast.
- **Specifico dell'origine**: indica che la voce contiene un'origine specifica e aggiunge l'indirizzo nel campo Indirizzo IP di origine. In caso contrario, la voce viene aggiunta come voce di (*,G), un indirizzo IP di gruppo acquisito da qualsiasi origine IP.
- **Indirizzo IP di origine**: definisce l'indirizzo di origine da includere.

PASSAGGIO 7 Fare clic su **Applica**. Il gruppo IP multicast viene aggiunto e il dispositivo viene aggiornato.

PASSAGGIO 8 Per configurare e visualizzare la registrazione di un indirizzo IP di gruppo, selezionare un indirizzo e fare clic su **Dettagli**.

L'ID VLAN, la versione IP, l'indirizzo IP gruppo multicast e l'indirizzo IP di origine selezionati vengono visualizzati in sola lettura nella parte superiore della finestra. È possibile selezionare il tipo di filtro:

- **Tipo di interfaccia uguale a**: scegliere se visualizzare porte o LAG.

PASSAGGIO 9 Selezionare il tipo di associazione per ciascuna interfaccia. Le opzioni disponibili sono:

- **Statico**: collega l'interfaccia al gruppo multicast come membro statico.
- **Vietato**: specifica che la porta non può essere associata al gruppo presente su questa VLAN.
- **Nessuno**: indica che la porta attualmente non appartiene a questo gruppo multicast della VLAN. Questa opzione è selezionata per impostazione predefinita fino a quando non si seleziona Statico o Vietato.

PASSAGGIO 10 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Configurazione dello snooping IGMP

Per supportare il reindirizzamento multicast selettivo (IPv4), è necessario attivare il filtro bridge multicast (nella pagina Proprietà e lo snooping IGMP a livello globale e per ogni VLAN selezionata (nella pagina Snooping IGMP).

Per impostazione predefinita, un dispositivo di livello 2 inoltra frame multicast a tutte le porte della VLAN selezionata, in pratica trattando il frame come se fosse un broadcast. Tramite lo snooping IGMP, il dispositivo reindirizza i frame multicast alle porte che riportano client multicast registrati.

NOTA Il dispositivo supporta lo snooping IGMP solo sulle VLAN statiche e non su quelle dinamiche.

Se la funzione Snooping IGMP è attivata a livello globale o su una VLAN, tutti i pacchetti IGMP vengono reindirizzati alla CPU, che li analizza e determina i seguenti elementi:

- Quali porte richiedono di partecipare ai gruppi multicast e su quale VLAN.
- Quali porte sono collegate ai router multicast (MRouter) che generano query IGMP.
- Quali porte ricevono protocolli per le query PIM, DVMRP o IGMP.

Queste vengono visualizzate nella pagina Snooping IGMP.

Le porte che chiedono di partecipare a un gruppo multicast specifico rilasciano un report IGMP in cui vengono specificati i gruppi a cui l'host si vuole connettere. Questo comporta la creazione di un'opzione di reindirizzamento nel database MFDB.

In mancanza di un router multicast, viene utilizzato l'interrogante snooping IGMP per supportare il dominio multicast di livello 2 degli switch con snooping attivo. È il caso, ad esempio, in cui il contenuto multicast viene fornito da un server locale ma il router (se presente) che si trova su quella rete non supporta il multicast.

La velocità dell'attività di un interrogante IGMP deve essere allineata con gli switch abilitati allo snooping IGMP. Le query devono essere inviate in un intervallo di tempo corrispondente alla validità temporale della tabella Snooping. Se le query vengono inviate in un intervallo di tempo inferiore alla validità temporale, l'interrogante selezionato non può ricevere pacchetti multicast. Questo viene definito nella pagina Modifica snooping IGMP.

Per attivare lo snooping IGMP e identificare il dispositivo come interrogante snooping IGMP su una VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Multicast** > **Snooping IGMP**.

PASSAGGIO 2 Attivare o disattivare lo stato Snooping IGMP.

L'attivazione di snooping IGMP a livello globale consente al dispositivo di monitorare il traffico di rete e di determinare quali host hanno richiesto la ricezione del traffico multicast.

Il dispositivo esegue lo snooping IGMP solo se sono attivi sia lo snooping IGMP che il filtro bridge multicast.

PASSAGGIO 3 Selezionare una VLAN e fare clic su **Modifica**.

In una rete è consentito un solo interrogante IGMP. Il dispositivo supporta la selezione di interroganti IGMP basati sugli standard. Alcuni valori dei parametri operativi di questa tabella vengono inviati dall'interrogante selezionato. Gli altri valori provengono dal dispositivo.

PASSAGGIO 4 Immettere i parametri.

- **ID VLAN**: selezionare l'ID VLAN in cui viene definito lo snooping IGMP.
- **Stato snooping IGMP**: attivare o disattivare il monitoraggio del traffico di rete per la VLAN selezionata.
- **Stato operativo snooping IGMP**: consente di visualizzare lo stato attuale dello Snooping IGMP per la VLAN selezionata.

- **Rilevamento automatico porte MRouter:** attivare o disattivare il rilevamento automatico delle porte a cui è collegato l'MRouter.
- **Affidabilità query**: immettere il valore della variabile di affidabilità da utilizzare se il dispositivo viene definito come interrogante.
- **Affidabilità query operativa**: visualizza la variabile di affidabilità inviata dall'interrogante selezionato.
- **Intervallo query**: immettere l'intervallo tra le query generali da utilizzare se il dispositivo viene impostato come interrogante.
- **Intervallo query operativa**: l'intervallo di tempo in secondi tra le query generali inviate dall'interrogante selezionato.
- **Intervallo risposta max query**: immettere il ritardo usato per calcolare il Numero massimo risposte inserito nelle Query generali periodiche.
- **Intervallo risposta max query operativa**: visualizza l'Intervallo risposta max query incluso nelle Query generali inviate dall'interrogante selezionato.
- **Contatore query ultimo membro**: immettere il numero di query IGMP specifiche di un gruppo inviate prima che il dispositivo, se rappresenta l'interrogante selezionato, indichi l'eventuale mancanza di ulteriori membri del gruppo.
- **Contatore query ultimo membro operativo**: visualizza il valore operativo del Contatore query ultimo membro.
- **Intervallo query ultimo membro**: immettere il ritardo risposta massimo da utilizzare se il dispositivo non è in grado di leggere il valore del tempo massimo di risposta dalle query specifiche del gruppo inviate dall'interrogante selezionato.
- **Intervallo query ultimo membro operativo**: visualizza l'Intervallo query ultimo membro inviato dall'interrogante selezionato.
- **Uscita immediata**: attivare Uscita immediata per ridurre il tempo necessario per bloccare un flusso multicast inviato su una porta membro durante la ricezione di un messaggio di Uscita gruppo IGMP.
- **Stato interrogante IGMP**: consente di attivare o disattivare l'Interrogante IGMP.
- **Indirizzo IP di origine interrogante amministrativo**: selezionare l'indirizzo IP di origine dell'interrogante IGMP, che può essere l'indirizzo IP della VLAN o l'indirizzo IP di gestione.

- **Indirizzo IP di origine interrogante operativo**: indica l'indirizzo IP di origine dell'interrogante selezionato.
- **Versione interrogante IGMP**: selezionare la versione IGMP usata se il dispositivo diventa l'interrogante selezionato. Se nella VLAN sono presenti switch e/o router multicast che eseguono il reindirizzamento multicast di IP specifici dell'origine, selezionare IGMPv3.

PASSAGGIO 5 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Snooping MLD

Gli host utilizzano il protocollo MLD per riportare la loro partecipazione alle sessioni multicast e il dispositivo utilizza lo snooping MLD per sviluppare elenchi di appartenenza multicast. Tali elenchi vengono poi utilizzati per reindirizzare i pacchetti multicast solo alle porte del dispositivo in cui ci sono nodi host appartenenti ai gruppi multicast. Il dispositivo non supporta l'interrogante MLD.

Gli host utilizzano il protocollo MLD per riportare la loro partecipazione a sessioni multicast.

Il dispositivo supporta due versioni di snooping MLD:

- Lo snooping MLDv1 rileva pacchetti di controllo MLDv1 e imposta il bridging del traffico sulla base degli indirizzi multicast IPv6 di destinazione.
- Lo snooping MLDv2 usa i pacchetti di controllo MLDv2 per reindirizzare il traffico sulla base dell'indirizzo IPv6 di origine e l'indirizzo multicast IPv6 di destinazione.

La versione MLD che verrà utilizzata viene selezionata dal router multicast della rete.

Analogamente allo snooping IGMP, viene eseguito lo snooping dei frame MLD che il dispositivo reindirizza dalle stazioni a un router multicast upstream e viceversa. Questa funzione consente a un dispositivo di stabilire i seguenti elementi:

- su quali porte sono posizionate le stazioni interessate all'associazione a un gruppo multicast specifico
- su quali porte sono posizionati i router multicast che inviano frame multicast

Queste informazioni vengono utilizzate per escludere porte non selezionate (porte sulle quali non sono registrate stazioni per la ricezione di un gruppo multicast specifico) dal reindirizzamento di un frame multicast in ingresso impostato.

Se oltre ai gruppi multicast configurati manualmente si attiva lo snooping MLD, il risultato sarà un'unione dei gruppi multicast e delle appartenenze alle porte derivate dalla configurazione manuale e il rilevamento dinamico tramite lo snooping MLD. Al riavvio del sistema, vengono mantenute solo le definizioni statiche.

Per attivare lo snooping MLD e configurarlo su una VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Multicast** > **Snooping MLD**.

PASSAGGIO 2 Attivare o disattivare lo **Stato snooping MLD**. L'attivazione dello snooping MLD a livello globale consente al dispositivo di monitorare il traffico di rete e di determinare quali host hanno richiesto la ricezione del traffico multicast. Il dispositivo esegue lo snooping MLD solo se sono attivi sia lo snooping MLD che il filtro bridge multicast.

PASSAGGIO 3 Selezionare una VLAN e fare clic su **Modifica**.

PASSAGGIO 4 Immettere i parametri.

- **ID VLAN**: selezionare l'ID VLAN.
- **Stato snooping MLD**: attivare o disattivare lo snooping MLD sulla VLAN. Il dispositivo monitora il traffico di rete per determinare quali host hanno richiesto l'invio di traffico multicast. Il dispositivo esegue lo snooping MLD solo se sono attivi sia lo snooping MLD che il filtro bridge multicast.
- **Stato snooping MLD operativo**: consente di visualizzare lo stato attuale dello Snooping MLD per la VLAN selezionata.
- **Rilevamento automatico porte MRouter**: attivare o disattivare il rilevamento automatico del router multicast.
- **Affidabilità query**: immettere il valore della variabile di affidabilità da utilizzare se il dispositivo non è in grado di leggere tale valore dai messaggi inviati dall'interrogante selezionato.
- **Affidabilità query operativa**: visualizza la variabile di affidabilità inviata dall'interrogante selezionato.
- **Intervallo query**: immettere il valore dell'Intervallo query che verrà utilizzato dal dispositivo nel caso in cui non riuscisse a ricavarlo dai messaggi inviati dall'interrogante selezionato.

- **Intervallo query operativa**: l'intervallo di tempo in secondi tra le Query generali ricevute dall'interrogante selezionato.
- **Intervallo risposta max query**: immettere il ritardo massimo di risposta alle query da utilizzare se il dispositivo in grado di leggere il valore del tempo massimo di risposta alle query generali inviate dall'interrogante selezionato.
- **Intervallo risposta max query operativa**: indica il ritardo usato per calcolare il Numero massimo risposte inserito nelle Query generali.
- **Contatore query ultimo membro**: immettere il contatore query ultimo membro da utilizzare se il dispositivo non è in grado di ricavare il valore dai messaggi inviati dall'interrogante selezionato.
- **Contatore query ultimo membro operativo**: visualizza il valore operativo del Contatore query ultimo membro.
- **Intervallo query ultimo membro**: immettere il ritardo massimo di risposta da utilizzare se il dispositivo non è in grado di leggere il valore del tempo massimo di risposta dalle query specifiche del gruppo inviate dall'interrogante selezionato.
- **Intervallo query ultimo membro operativo**: l'Intervallo query ultimo membro inviato dall'interrogante selezionato.
- **Uscita immediata**: se selezionata, questa opzione consente di ridurre il tempo necessario per bloccare il traffico MLD non necessario inviato da una porta del dispositivo.

PASSAGGIO 5 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Ricerca gruppo IP Multicast IGMP/MLD

Nella pagina Gruppo IP Multicast IGMP/MLD viene visualizzato l'indirizzo di gruppo IPv4 e IPv6 acquisito tramite i messaggi IGMP/MLD.

Le informazioni riportate in questa pagina potrebbero risultare diverse rispetto a quelle visualizzate, ad esempio, nella pagina Indirizzo MAC di gruppo. Immaginando che il sistema si trovi in gruppi basati su MAC e una porta che ha richiesto l'associazione ai seguenti gruppi multicast, 224.1.1.1 e 225.1.1.1, entrambi vengono associati all'indirizzo multicast MAC 01:00:5e:01:01:01. In questo caso, la pagina MAC Multicast riporta una voce, mentre in quella relativa a IP Multicast ne vengono visualizzate due.

Per ricercare un gruppo IP Multicast, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Multicast** > **Gruppo IP Multicast IGMP/MLD**.

PASSAGGIO 2 Impostare il tipo di gruppo di snooping da cercare: IGMP o MLD.

PASSAGGIO 3 Immettere alcuni o tutti i seguenti criteri sul filtro della query:

- **Indirizzo gruppo uguale a**: indica l'indirizzo MAC del gruppo Multicast o l'indirizzo IP su cui eseguire la ricerca.
- **Indirizzo di origine uguale a**: indica l'indirizzo del mittente su cui eseguire la ricerca.
- **ID VLAN uguale a**: indica l'ID VLAN su cui eseguire la ricerca.

PASSAGGIO 4 Scegliere **Vai**. Per ogni gruppo multicast vengono visualizzati i campi seguenti:

- **VLAN**: l'ID VLAN.
- **Indirizzo gruppo**: l'indirizzo MAC del gruppo multicast o l'indirizzo IP.
- **Indirizzo di origine**: l'indirizzo del mittente per tutte le porte del gruppo specificato.
- **Porte incluse**: l'elenco delle porte di destinazione del flusso multicast.
- **Porte escluse**: l'elenco delle porte non incluse nel gruppo.
- **Modalità di compatibilità**: la versione IGMP/MLD di registrazione meno recente degli host ricevuti dal dispositivo sull'indirizzo IP di gruppo.

Definizione delle porte router multicast

Una porta router Multicast (MRouter) è una porta che si connette a un router multicast. Il dispositivo include i numeri delle porte del router multicast di destinazione dei flussi multicast e i messaggi di registrazione IGMP/MLD. Questo è necessario affinché tutti i router multicast possano reindirizzare, a loro volta, flussi multicast e distribuire i messaggi di registrazione alle altre sottoreti.

Per configurare in modo statico o vedere porte rilevate dinamicamente connesse al router multicast, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Multicast** > **Porta router Multicast**.

PASSAGGIO 2 Immettere alcuni o tutti i seguenti criteri sul filtro della query:

- **ID VLAN uguale a**: selezionare l'ID VLAN per le porte router indicate.
- **Versione IP uguale a**: selezionare la versione IP supportata dal router multicast.
- **Tipo di interfaccia uguale a**: scegliere se visualizzare porte o LAG.

PASSAGGIO 3 Scegliere **Vai**. Vengono visualizzate le interfacce corrispondenti ai criteri della query.

PASSAGGIO 4 Selezionare il tipo di associazione per ciascuna porta o LAG. Le opzioni disponibili sono:

- **Statico**: la porta viene configurata staticamente come una porta router multicast.
- **Dinamico** (solo visualizzazione): la porta viene configurata come porta router multicast dinamicamente attraverso una query MLD/IGMP. Per attivare il rilevamento dinamico delle porte router multicast, visualizzare la pagina **Multicast** > **Snooping IGMP** e la pagina **Multicast** > **Snooping MLD**.
- **Vietato**: la porta selezionata non è stata configurata come porta router multicast, nonostante qui vengano ricevute le query IGMP o MLD. Se la porta è impostata sull'opzione Vietato, Mrouter non viene rilevato (ad esempio il rilevamento automatico delle porte di Mrouter non è attivo sulla porta).
- **Nessuno**: la porta non è al momento una porta router multicast.

PASSAGGIO 5 Fare clic su **Applica** per aggiornare il dispositivo.

Definizione dell'inoltro di tutti i multicast

Nella pagina Inoltra tutto è possibile attivare e visualizzare la configurazione delle porte e/o dei LAG che devono ricevere i flussi multicast da una VLAN specifica. Per utilizzare questa funzione, è necessario attivare il filtro bridge multicast nella pagina Proprietà Se il filtro è disattivato, tutto il traffico multicast viene distribuito alle porte del dispositivo.

Se i dispositivi collegati alla porta non supportano IGMP e/o MLD, è possibile configurare (manualmente) staticamente una porta su Inoltra tutto.

I messaggi IGMP o MLD non vengono reindirizzati alle porte su cui viene impostato *Inoltra tutto*.

NOTA La configurazione incide solo sulle porte appartenenti alla VLAN selezionata.

Per definire il reindirizzamento di tutti i multicast, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Multicast** > **Inoltra tutto**.

PASSAGGIO 2 Definire quanto segue:

- **ID VLAN uguale a**: l'ID VLAN delle porte/LAG da visualizzare.
- **Tipo di interfaccia uguale a**: indicare se visualizzare porte o LAG.

PASSAGGIO 3 Scegliere **Vai**. Viene visualizzato lo stato di tutte le porte/LAG.

PASSAGGIO 4 Selezionare la porta/il LAG da definire come Inoltra tutto usando i metodi seguenti:

- **Statico**: la porta riceve tutti i flussi multicast.
- **Vietato**: le porte non possono ricevere flussi multicast, anche se dallo snooping IGMP/MLP risultano associate a un gruppo multicast.
- **Nessuno**: la porta non è al momento una porta Inoltra tutto.

PASSAGGIO 5 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Definizione delle impostazioni Multicast non registrato

Generalmente, i frame multicast vengono reindirizzati a tutte le porte presenti nella VLAN. Se lo snooping IGMP/MLD è attivo, il dispositivo rileva la presenza di gruppi multicast e monitora le porte indicando a quale gruppo multicast sono state associate. I gruppi multicast possono essere configurati anche staticamente. Quelli acquisiti dinamicamente o configurati staticamente, vengono considerati come registrati.

Il dispositivo reindirizza i frame multicast (da un gruppo multicast registrato) solo alle porte registrate a quel gruppo multicast.

Nella pagina Multicast non registrato è possibile gestire i frame multicast appartenenti a gruppi non riconosciuti dal dispositivo (gruppi multicast non registrati). Generalmente, i frame multicast vengono reindirizzati a tutte le porte presenti nella VLAN.

È possibile selezionare una porta su cui ricevere o filtrare i flussi multicast non registrati. La configurazione è valida per qualsiasi VLAN cui appartiene (o apparterrà).

La funzione garantisce al cliente di ricevere solo i gruppi multicast richiesti e non gli altri eventualmente trasmessi nella rete.

Per definire le impostazioni dei multicast non registrati, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Multicast** > **Multicast non registrato**.

PASSAGGIO 2 Definire quanto segue:

- **Tipo di interfaccia uguale a**: il modo in cui vengono visualizzate tutte le porte/LAG.
- **Porta/LAG**: visualizza l'ID della porta o del LAG.
- **Multicast non registrato**: indica lo stato di reindirizzamento dell'interfaccia selezionata. I valori selezionabili sono:
  - *Reindirizzamento*: consente di reindirizzare i frame multicast non registrati all'interfaccia selezionata.
  - *Filtro*: consente di filtrare (eliminare) i frame multicast non registrati sull'interfaccia selezionata.

PASSAGGIO 3 Fare clic su **Applica**. Le impostazioni vengono salvate e il file Configurazione di esecuzione viene aggiornato.

18

Configurazione IP

Gli indirizzi IP di interfaccia vengono configurati manualmente dall'utente oppure automaticamente da un server DHCP. In questa sezione vengono fornite le informazioni per definire gli indirizzi IP del dispositivo manualmente o impostandolo come client DHCP.

In questa sezione vengono illustrati i seguenti argomenti:

- **Panoramica**
- **Interfacce e gestione IPv4**
- **Server DHCP**
- **Interfacce e gestione IPv6**
- **Nome di dominio**

Panoramica

NOTA I dispositivi SG500X funzionano sempre in modalità L3 avanzata a meno che non siano in modalità Ibrido (vedere la sezione **Modalità dell'unità stack**) quando agiscono da dispositivi Sx500. I dispositivi Sx500, invece, devono sempre essere impostati per il funzionamento in modalità di sistema Livello 2 o Livello 3. Pertanto, quando nella sezione si parla di dispositivi che operano in modalità di sistema Livello 3, si fa riferimento a tutti i dispositivi SG500X in modalità Stack nativo e ai dispositivi su cui è stata impostata manualmente la modalità di sistema Livello 3. Quando si parla di dispositivi che operano in modalità di sistema Livello 2, invece, si fa riferimento a tutti i dispositivi Sx500 e SG500X (in modalità Ibrido) su cui è stata impostata manualmente la modalità di sistema Livello 2.

Alcune funzioni sono disponibili solo in modalità di sistema Livello 2 o 3, come descritto di seguito:

- In modalità di sistema Livello 2 (solo per dispositivi Sx500), il dispositivo è in grado di rilevare una VLAN di Livello 2 e non include funzioni di routing.

- In modalità di sistema Livello 3, il dispositivo dispone di funzioni di routing IP e delle funzionalità della modalità di sistema Livello 2. In questa modalità di sistema, una porta di Livello 3 mantiene gran parte delle funzionalità di Livello 2, ad esempio l'STP (Spanning Tree Protocol) e l'appartenenza VLAN.
- In modalità di sistema Livello 3 (solo per dispositivi Sx500), il dispositivo non supporta le VLAN basate su MAC, l'assegnazione dinamica delle VLAN, il limite di velocità VLAN, la protezione DoS velocità SYN e il monitoraggio QoS avanzato.

Per configurare la modalità di sistema (Livello 2 o Livello 3) per i dispositivi Sx500, vedere la pagina Modalità di sistema e Gestione stack.

NOTA Se si passa da una modalità di sistema (livello) a un'altra (sui dispositivi Sx500) è necessario riavviare il dispositivo e la configurazione di avvio verrà eliminata.

Indirizzamento IP di livello 2

NOTA Questa sezione riguarda soltanto i dispositivi Sx500.

In modalità di sistema Livello 2, il dispositivo può avere un indirizzo IPv4 e due interfacce IPv6 (interfaccia "nativa" o Tunnel) nella VLAN di gestione. Questo indirizzo IP e il gateway predefinito possono essere configurati manualmente o tramite DHCP. L'indirizzo IP statico e il gateway predefinito per la modalità di sistema Livello 2 vengono configurati nelle pagine Interfaccia IPv4 e Interfaccia IPv6. In modalità di sistema Livello 2, il dispositivo utilizza il gateway predefinito, se configurato, per comunicare con i dispositivi che non si trovano nella stessa subnet IP. Per impostazione predefinita, VLAN1 corrisponde alla VLAN di gestione, ma può essere modificata. Quando si opera in modalità di sistema Livello 2, il dispositivo può essere raggiunto soltanto all'indirizzo IP configurato tramite la relativa VLAN di gestione.

L'impostazione predefinita per la configurazione dell'indirizzo IPv4 è *DHCPv4*. Questo significa che il dispositivo funge da client DHCPv4 e durante la procedura di avvio invia una richiesta DHCPv4.

Se il dispositivo riceve una risposta DHCPv4 dal server DHCPv4 con un indirizzo IPv4, invierà pacchetti ARP (Address Resolution Protocol) per confermare l'univocità dell'indirizzo IP. Se nella risposta ARP viene indicato che l'indirizzo IPv4 è in uso, il dispositivo invia un messaggio DHCPDECLINE al server DHCP e un altro pacchetto DHCPDISCOVER per riavviare il processo.

Se il dispositivo non riceve una risposta DCHPv4 entro 60 secondi, continuerà a inviare query DHCPDISCOVER e utilizzerà l'indirizzo IPv4 predefinito: 192.168.1.254/24.

Le collisioni dell'indirizzo IP si verificano quando più di un dispositivo utilizza lo stesso indirizzo IP nella medesima subnet. Per risolvere tali collisioni, è necessario un intervento amministrativo sul server DHCP e/o sui dispositivi che sono in conflitto con il dispositivo.

Quando si configura una VLAN per utilizzare indirizzi IPv4 dinamici, il dispositivo rilascia richieste DHCPv4 fino a quando un server DHCPv4 non assegna un indirizzo IPv4. In modalità di sistema Livello 2, è possibile configurare un indirizzo IP statico o dinamico soltanto per la VLAN di gestione. In modalità di sistema Livello 3, è possibile configurare con un indirizzo IP statico o dinamico tutti i tipi di interfaccia (porte, LAG, e/o VLAN) sul dispositivo.

Di seguito vengono riportate le regole di assegnazione degli indirizzi IP per il dispositivo:

- Se è attiva la modalità di sistema Livello 2 e non è stato configurato un indirizzo IP statico, il dispositivo rilascia richieste DHCPv4 finché non riceve una risposta dal server DHCP.
- Se l'indirizzo IP sul dispositivo viene modificato, il dispositivo rilascia pacchetti ARP ingiustificati alla VLAN corrispondente per verificare la presenza di collisioni tra gli indirizzi IP. Questa regola viene applicata anche quando sul dispositivo viene ripristinato l'indirizzo IP predefinito.
- Quando il server DHCP fornisce un nuovo indirizzo IP univoco, il LED dello stato del sistema diventa di colore verde fisso. Allo stesso modo, anche quando si imposta un indirizzo IP statico, il LED diventa di colore verde fisso. Se il dispositivo utilizza l'indirizzo IP predefinito 192.168.1.254 e sta acquisendo un indirizzo IP, il LED lampeggia.
- Le stesse regole si applicano quando un client deve rinnovare il periodo di validità prima di ricevere notifica sulla scadenza tramite un messaggio DHCPREQUEST.
- Con le impostazioni predefinite, quando non è disponibile un indirizzo IP definito staticamente o acquisito dal DCHP, viene utilizzato quello predefinito. Quando gli altri indirizzi IP diventano disponibili, verranno utilizzati automaticamente. L'indirizzo IP predefinito si trova sempre nella VLAN di gestione.

Indirizzamento IP di livello 3

In modalità di sistema Livello 3, il dispositivo può avere più indirizzi IP. È possibile assegnare ciascun indirizzo IP su porte, LAG o VLAN specificati. Tali indirizzi IP vengono configurati nella pagine Interfaccia IPv4 e Interfacce IPv6 in modalità di sistema Livello 3. Rispetto alla modalità di sistema Livello 2, in cui è possibile configurare un singolo indirizzo IP, questa fornisce una maggiore flessibilità della rete. Lavorando in modalità di sistema Livello 3, è possibile raggiungere il dispositivo su tutti i suoi indirizzi IP dalle interfacce corrispondenti.

In modalità di sistema Livello 3 non viene fornito un percorso predefinito. Per gestire il dispositivo in remoto, è necessario indicare un percorso predefinito. Tutti i gateway predefiniti assegnati da DHCP vengono memorizzati come percorsi predefiniti. Inoltre è possibile definire percorsi predefiniti manualmente. A tal fine, utilizzare le pagine Percorso statico IPv4 e Routing IPv6.

Tutti gli indirizzi IP configurati o assegnati al dispositivo sono definiti indirizzi IP di gestione nella presente guida.

Se le pagine per Livello 2 e Livello 3 sono diverse, vengono visualizzate entrambe le versioni.

Interfaccia loopback

Panoramica

L'interfaccia loopback è un'interfaccia virtuale il cui stato operativo è sempre attivo. Se l'indirizzo IP configurato su questa interfaccia virtuale viene utilizzato come indirizzo locale quando comunica con applicazioni IP remote, la comunicazione non viene annullata anche se l'attuale percorso all'applicazione remota è stato modificato.

Lo stato operativo di un'interfaccia loopback è sempre attivo. Definire un indirizzo IP (IPv4 o IPv6) nell'interfaccia e utilizzare tale indirizzo IP come indirizzo IP locale per la comunicazione IP con applicazioni IP remote.

Un'interfaccia loopback non supporta il bridging; non può appartenere a nessuna VLAN e nessun protocollo di Livello 2 può essere attivato in essa.

L'identificatore di interfaccia locale di collegamento IPv6 è 1.

Quando lo switch è in modalità di sistema Livello 2, sono supportate le seguenti regole:

- È supportata una sola interfaccia loopback.
- Possono essere configurate due interfacce IPv4: una su una porta VLAN o Ethernet e una sull'interfaccia loopback.

- Se l'indirizzo IPv4 è stato configurato sulla VLAN predefinita ma questa è stata modificata, lo switch trasferisce l'indirizzo IPv4 sulla nuova VLAN predefinita.

Configurazione di un'interfaccia loopback

Per configurare un'interfaccia loopback IPv4, attenersi alla seguente procedura:

- Nel Livello 2, abilitare l'interfaccia loopback e configurare il suo indirizzo nella pagina Amministrazione > Interfaccia di gestione > Interfaccia IPv4. Questa pagina non è disponibile per i dispositivi SG500X, ESW2-550X e SG500XG.
- Nel Livello 3, aggiungere un'interfaccia loopback in Configurazione IP > Interfacce e gestione IPv4 > Interfaccia IPv4.

Per configurare un'interfaccia loopback IPv6, attenersi alla seguente procedura:

- Nel Livello 2, aggiungere un'interfaccia loopback nella pagina Amministrazione > Interfaccia di gestione > Interfacce IPv6. Configurare l'indirizzo IPv6 di tale interfaccia nella pagina Amministrazione > Interfaccia di gestione > Indirizzi IPv6. Questa pagina non è disponibile per i dispositivi SG500X, ESW2-550X e SG500XG.
- Nel Livello 3, aggiungere un'interfaccia loopback in Configurazione IP > Interfacce e gestione IPv6 > Interfaccia IPv6. Configurare l'indirizzo IPv6 di tale interfaccia nella pagina Configurazione IP > Interfacce e gestione IPv6 > Indirizzi IPv6.

Interfacce e gestione IPv4

Interfaccia IPv4

È possibile definire interfacce IPv4 sul dispositivo se è attiva la modalità di sistema Livello 2 o Livello 3.

Definizione di un'interfaccia IPv4 in modalità di sistema Livello 2

Questa sezione non è rilevante per i dispositivi SG500X, ESW2-550X o SG500XG.

Per gestire il dispositivo tramite l'utilità di configurazione basata sul Web, è necessario che l'indirizzo IP di gestione del dispositivo IPv4 venga definito e riconosciuto. L'indirizzo IP del dispositivo può essere configurato manualmente o ricevuto automaticamente da un server DHCP.

Per configurare l'indirizzo IP del dispositivo IPv4, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione > Interfaccia di gestione > Interfaccia IPv4**.

PASSAGGIO 2 Immettere i valori dei seguenti campi:

- **VLAN di gestione**: selezionare la VLAN di gestione utilizzata per accedere al dispositivo tramite Telnet o l'interfaccia utente Web. VLAN1 rappresenta la VLAN di gestione predefinita.
- **Tipo di indirizzo IP**: selezionare una delle seguenti opzioni:
  - *Dinamico*: rilevare l'indirizzo IP dal DHCP della VLAN di gestione.
  - *Statico*: definire manualmente un indirizzo IP statico.

  NOTA L'opzione 12 DHCP (opzione Nome host) è supportata quando il dispositivo è un client DHCP. Se si riceve l'Opzione 12 DHCP da un server DHCP, questa viene salvata come nome host del server. L'opzione 12 DHCP non è richiesta dal dispositivo. Per poter inviare l'opzione 12, è necessario configurare il server DHCP indipendentemente da ciò che viene richiesto affinché la funzione venga eseguita.

Per configurare un indirizzo IP statico, configurare i seguenti campi.

- **Indirizzo IP**: immettere l'indirizzo IP e configurare uno dei campi **Maschera** seguenti:
  - **Maschera di rete**: selezionare e immettere la maschera dell'indirizzo IP.
  - **Lunghezza prefisso**: selezionare e immettere la lunghezza del prefisso dell'indirizzo IPv4.
- **Interfaccia loopback**: selezionare per consentire la configurazione di un'interfaccia loopback (vedere **Interfaccia loopback**).
- **Indirizzo IP loopback**: immettere l'indirizzo IPv4 dell'interfaccia loopback.

Immettere uno dei seguenti campi per l'interfaccia loopback:

- *Maschera loopback*: immettere la maschera dell'indirizzo IPv4 nell'interfaccia loopback.
- *Lunghezza prefisso*: immettere la lunghezza prefisso dell'indirizzo IPv4 dell'interfaccia loopback.

- **Gateway amministrativo predefinito**: selezionare **Definito dall'utente** e immettere l'indirizzo IP del gateway predefinito oppure selezionare **Nessuno** per rimuovere dall'interfaccia quello selezionato.
- **Gateway predefinito operativo**: indica lo stato corrente del gateway predefinito.

  NOTA Se il dispositivo non è stato configurato con un gateway predefinito, non può comunicare con altri dispositivi che non si trovano nella stessa subnet IP.

Se il server DHCP recupera un indirizzo IP dinamico, selezionare i campi attivi tra i seguenti:

- **Rinnova indirizzo IP ora**: l'indirizzo IP dinamico del dispositivo assegnato da un server DHCP può essere rinnovato in qualsiasi momento. A seconda della configurazione del server DHCP, dopo il rinnovo il dispositivo potrebbe ricevere un nuovo indirizzo IP che deve essere specificato nell'utilità di configurazione basata sul Web.
- **Configurazione automatica tramite DHCP**: visualizza lo stato della funzione di configurazione automatica. La Configurazione automatica DHCP può essere configurata da *Amministrazione* > *Gestione di file* > *Configurazione automatica DHCP*.

PASSAGGIO 3 Fare clic su **Applica**. Le impostazioni dell'interfaccia IPv4 vengono scritte nel file Configurazione di esecuzione.

Definizione dell'interfaccia IPv4 in modalità di sistema Livello 3

La pagina Interfaccia IPv4 viene utilizzata quando il dispositivo è in modalità di sistema Livello 3. Questa modalità permette di configurare più indirizzi IP per la gestione del dispositivo e fornisce servizi di routing.

È possibile configurare l'indirizzo IP su una porta, un LAG, un'interfaccia loopback o VLAN.

Utilizzando la modalità Livello 3, il dispositivo indirizza il traffico tra le sottoreti IP configurate connesse direttamente e continua a indirizzare il traffico tra i dispositivi che si trovano nella stessa VLAN. Nella pagina Percorso statico IPv4 è possibile configurare ulteriori percorsi IPv4 del routing su sottoreti non collegate direttamente.

NOTA Il software del dispositivo utilizza un ID VLAN (VID) per ciascun indirizzo IP configurato su una porta o un LAG. Il dispositivo prende il primo VID disponibile a partire da 4094.

Per configurare gli indirizzi IPv4, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv4**> **Interfaccia IPv4**.

Solo per i dispositivi SG500X, selezionare la casella **Attiva** per attivare il routing IPv4. Nei dispositivi Sx500, quando si modifica la modalità di sistema da Livello 2 a Livello 3, il routing IP viene eseguito automaticamente.

PASSAGGIO 2 Selezionare **Routing IPv4** per impostare il dispositivo come router IPv4.

PASSAGGIO 3 Fare clic su **Applica**. Il parametro viene salvato nel file di configurazione esecuzione.

In questa pagina vengono visualizzati i seguenti campi della tabella Interfaccia IPv4:

- **Interfaccia**: interfaccia per cui è definito l'indirizzo IP.
- **Tipo di indirizzo IP**: indirizzo IP definito come statico o DHCP.
  - *Indirizzo IP dinamico*: ricevuto dal server DHCP.
  - *Statico*: viene inserito manualmente.
- **Indirizzo IP**: l'indirizzo IP configurato per l'interfaccia.
- **Maschera**: maschera dell'indirizzo IP configurato.
- **Stato**: risultati della verifica sulla duplicazione dell'indirizzo IP.
  - *Provvisorio*: la verifica di indirizzi IP duplicati non ha prodotto risultati finali.
  - *Valido*: la verifica delle collisioni tra gli indirizzi IP è stata completata e non sono state rilevate collisioni.
  - *Duplicato valido*: la verifica della duplicazione degli indirizzi IP è stata completata e non sono stati rilevati indirizzi IP duplicati.

- *Duplicato*: è stato rilevato un indirizzo IP duplicato per l'indirizzo IP predefinito.
- *Ritardato*: se il client DHCP è abilitato, l'assegnazione dell'indirizzo IP è ritardata di 60 secondi all'avvio in modo da dare il tempo di rilevare l'indirizzo DHCP.
- *Non ricevuto*: pertinente all'indirizzo DHCP. Quando un client DHCP avvia un processo di rilevamento, assegna un indirizzo IP fittizio 0.0.0.0 prima di ottenere l'indirizzo reale. Questo indirizzo fittizio presenta lo stato "Non ricevuto".

PASSAGGIO 4 Fare clic su **Aggiungi.**

PASSAGGIO 5 Selezionare uno dei seguenti campi:

- **Interfaccia**: selezionare Porta, LAG o VLAN come interfaccia associata alla configurazione IP e scegliere un'interfaccia dall'elenco.
- **Tipo di indirizzo IP**: selezionare una delle seguenti opzioni:
  - *Indirizzo IP dinamico*: ottenere l'indirizzo IP da un server DHCP.
  - *Indirizzo IP statico*: immettere l'indirizzo IP.

PASSAGGIO 6 Selezionare **Indirizzo dinamico o Indirizzo statico**.

PASSAGGIO 7 Se è stato selezionato **Indirizzo statico**, immettere l'indirizzo IP per questa interfaccia e inserire uno dei seguenti:

- **Maschera di rete**: maschera IP dell'indirizzo.
- **Lunghezza prefisso**: lunghezza del prefisso IPv4.

PASSAGGIO 8 Fare clic su **Applica**. Le impostazioni dell'indirizzo IPv4 vengono definite nel file Configurazione di esecuzione.

ATTENZIONE Se nel sistema è attiva una modalità di stack con un master di backup, si consiglia di configurare l'indirizzo IP come indirizzo statico per impedire la disconnessione dalla rete durante una commutazione master dello stack. Questo perché quando il master backup prende il controllo dello stack, se si utilizza DHCP, potrebbe ricevere un indirizzo IP diverso da quello ricevuto dall'unità master originale dello stack.

Percorsi IPv4

Se il dispositivo è in modalità di sistema Livello 3, in questa pagina è possibile configurare e visualizzare i percorsi statici IPv4 sul dispositivo. Quando si indirizza il traffico, il passaggio successivo viene stabilito in base al prefisso più lungo (algoritmo LPM). Un indirizzo IPv4 di destinazione può riportare più percorsi nella tabella Percorso statico IPv4. Il dispositivo utilizza il percorso corrispondente con la subnet mask più alta, ovvero la corrispondenza con il prefisso più lungo.

Per definire un percorso IP statico, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv4**> **Percorsi IPv4**.

PASSAGGIO 2 Fare clic su **Aggiungi.**

PASSAGGIO 3 Immettere i valori dei seguenti campi:

- **Prefisso IP di destinazione**: immettere il prefisso dell'indirizzo IP di destinazione.
- **Maschera**: selezionare e immettere le informazioni in uno dei seguenti elementi:
  - **Maschera di rete**: il prefisso del percorso IP per l'IP di destinazione.
  - **Lunghezza prefisso**: il prefisso del percorso IP per l'IP di destinazione.
- **Tipo di routing**: selezionare il tipo di routing.
  - *Rifiuta*: rifiuta il percorso e blocca il routing in tutti i gateway verso la rete di destinazione. Questo garantisce l'eliminazione di un frame contenente l'IP di destinazione di questo percorso.
  - *Remoto*: indica che il percorso è remoto.
- **Indirizzo IP router del passaggio successivo**: immettere sul percorso un indirizzo IP del passaggio successivo o un alias IP.

  NOTA Quando il dispositivo acquisisce l'indirizzo IP da un server DHCP, non è possibile configurare un percorso statico tramite una subnet IP connessa direttamente.
- **Metrico**: immettere la distanza amministrativa relativa al passaggio successivo L'intervallo è compreso tra 1 e 255.

PASSAGGIO 4 Fare clic su **Applica**. Il percorso statico IP viene salvato nel file di configurazione esecuzione.

RIPv2

Vedere la sezione **Configurazione IP: RIPv2**.

Elenco di accesso

Vedere la sezione **Elenchi di accesso**.

VRRP

Vedere la sezione **Configurazione IP: VRRP**

ARP

Il dispositivo gestisce una tabella ARP (Address Resolution Protocol) per tutti i dispositivi conosciuti che si trovano nelle sottoreti IP collegate direttamente. Una subnet IP connessa direttamente è la subnet alla quale è connessa un'interfaccia IPv4 del dispositivo. Quando il dispositivo deve inviare/reindirizzare pacchetti su un dispositivo locale, cerca nella tabella ARP l'indirizzo MAC del dispositivo. La tabella ARP contiene sia indirizzi statici che dinamici. Gli indirizzi statici vengono configurati manualmente e mantenuti. Il dispositivo crea indirizzi dinamici dai pacchetti ARP ricevuti che, dopo un periodo di tempo configurato, non sono più validi.

NOTA In modalità Livello 2, il dispositivo utilizza le informazioni relative all'associazione degli indirizzi IP/MAC presenti nella Tabella ARP per reindirizzare il traffico proveniente dal dispositivo stesso. In modalità Livello 3, tali informazioni vengono utilizzate per il routing di Livello 3 e per reindirizzare il traffico generato.

Per definire le tabelle ARP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP > Interfacce e gestione IPv4**> **ARP**.

PASSAGGIO 2 Immettere i parametri.

- **Tempo alla scadenza voce ARP**: immettere il numero di secondi durante i quali è possibile mantenere gli indirizzi dinamici nella tabella ARP. Un indirizzo dinamico non è più considerato valido quando la sua presenza nella tabella supera l'impostazione di Voce ARP scaduta. Quando un indirizzo dinamico non è più valido, viene eliminato dalla tabella e viene reinserito solo se acquisito di nuovo.

- **Cancella voci tabella ARP**: selezionare il tipo di voci ARP da cancellare dal sistema.
  - *Tutte*: elimina subito tutti gli indirizzi statici e dinamici.
  - *Dinamiche*: elimina subito tutti gli indirizzi dinamici.
  - *Statiche*: elimina subito tutti gli indirizzi statici.
  - *Normali scadute*: elimina gli indirizzi dinamici in base all'impostazione di Voce ARP scaduta.

PASSAGGIO 3 Scegliere **Applica**. Le impostazioni globali ARP vengono scritte nel file Configurazione di esecuzione.

Nella tabella ARP vengono visualizzati i seguenti campi:

- **Interfaccia**: corrisponde all'interfaccia IPv4 della subnet IP connessa direttamente in cui si trova il dispositivo IP.
- **Indirizzo IP**: l'indirizzo IP del dispositivo IP.
- **Indirizzo MAC**: l'indirizzo MAC del dispositivo IP.
- **Stato**: indica se la voce è stata inserita manualmente o acquisita dinamicamente.

PASSAGGIO 4 Scegliere **Aggiungi**.

PASSAGGIO 5 Immettere i seguenti parametri:

- **Versione IP**: il formato dell'indirizzo IP supportato dall'host. È supportato solo l'IPv4.
- **Interfaccia**: (solo Livello 3) interfaccia IPv4 del dispositivo.
- **VLAN**: (solo Livello 2) nel Livello 2, visualizza l'ID della VLAN di gestione.

  Per i dispositivi in modalità Livello 2, è disponibile una sola subnet IP connessa direttamente che si trova sempre nella VLAN di gestione. Tutti gli indirizzi statici e dinamici riportati nella Tabella ARP si trovano nella VLAN di gestione.

  Interfaccia: per i dispositivi in modalità di sistema Livello 3, è possibile configurare un'interfaccia IPv4 su una porta, un LAG o una VLAN. Selezionare l'interfaccia desiderata dall'elenco delle interfacce IPv4 configurate sul dispositivo.
- **Indirizzo IP**: immettere l'indirizzo IP del dispositivo locale.
- **Indirizzo MAC**: immettere l'indirizzo MAC del dispositivo locale.

PASSAGGIO 6 Fare clic su **Applica**. La voce ARP viene salvata nel file di configurazione esecuzione.

Proxy ARP

La tecnica Proxy ARP viene utilizzata da un dispositivo su una determinata subnet IP per rispondere alle query ARP relative a un indirizzo di rete non presente sulla rete.

NOTA La funzione Proxy ARP è disponibile solo se il dispositivo è in modalità Livello 3.

Questa funzione rileva la destinazione del traffico e fornisce un altro indirizzo MAC come risposta. L'utilizzo di un proxy ARP per un host diverso consente effettivamente di indirizzare sull'host una destinazione del traffico LAN. Il percorso del traffico ottenuto viene quindi in genere indirizzato dal proxy alla destinazione stabilita tramite un'altra interfaccia o un tunnel.

Quando in seguito a una query ARP di richiesta di un indirizzo IP diverso, per motivi legati al proxy, il nodo risponde con il proprio indirizzo MAC si parla di "pubblicazione".

Per attivare la funzione Proxy ARP su tutte le interfacce IP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP > Interfacce e gestione IPv4**> **Proxy ARP**.

PASSAGGIO 2 Selezionare **Proxy ARP** per consentire al dispositivo di rispondere alle richieste ARP di nodi remoti con l'indirizzo MAC del dispositivo.

PASSAGGIO 3 Fare clic su **Applica**. Il proxy ARP è attivato e il file di Configurazione di esecuzione viene aggiornato.

Inoltro UDP/Helper IP

Inoltro UDP/Helper IP è l'unica funzione disponibile quando il dispositivo è in modalità di sistema Livello 3. Generalmente gli switch non instradano pacchetti broadcast IP tra sottoreti IP. Tuttavia, se questa funzionalità è attivata, il dispositivo può inoltrare pacchetti broadcast UDP specifici, ricevuti dalle interfacce IPv4, a indirizzi IP di destinazione specifici.

Per configurare l'inoltro di pacchetti UDP ricevuti da un'interfaccia IPv4 specifica con una specifica porta UDP di destinazione, aggiungere un Inoltro UDP:

PASSAGGIO 1 Fare clic su **Configurazione IP > Interfacce e gestione IPv4**> **Inoltro UDP/ Helper IP**.

PASSAGGIO 2 Fare clic su **Aggiungi.**

PASSAGGIO 3 Selezionare l'interfaccia IP di origine di destinazione dei pacchetti broadcast UDP inoltrati dal dispositivo sulla base di una porta di destinazione UDP configurata. È necessario selezionare un'interfaccia IPv4 configurata sul dispositivo.

PASSAGGIO 4 Immettere il numero di **Porta di destinazione UDP** per i pacchetti che verranno inoltrati dal dispositivo. Selezionare dall'elenco a discesa una porta nota oppure fare clic sul pulsante di opzione della porta per immettere il numero manualmente.

PASSAGGIO 5 Immettere l'**Indirizzo IP di destinazione** a cui verranno inoltrati i pacchetti UDP. Se il campo è 0.0.0.0, i pacchetti UDP verranno eliminati. Se il campo è 255.255.255.255, i pacchetti UDP verranno distribuiti su tutte le interfacce IP.

PASSAGGIO 6 Fare clic su **Applica**. Le impostazioni dell'inoltro UDP vengono scritte nel file Configurazione di esecuzione.

Snooping/inoltro DHCPv4

Snooping DHCPv4

Lo Snooping DHCP fornisce un meccanismo di sicurezza per impedire la ricezione di falsi pacchetti di risposta DHCP e registrare gli indirizzi DHCP. Il meccanismo funziona trattando le porte sul dispositivo come attendibili o non attendibili.

Una porta attendibile è una porta connessa a un server DHCP e autorizzata ad assegnare indirizzi DHCP. I messaggi DHCP ricevuti sulle porte attendibili possono passare nel dispositivo.

Una porta non attendibile è una porta non autorizzata ad assegnare indirizzi DHCP. Tutte le porte sono considerate non attendibili per impostazione predefinita, finché non vengono dichiarate attendibili (nella pagina Impostazioni delle interfacce per snooping DHCP).

Inoltro DHCPv4

L'Inoltro DHCP trasmette i pacchetti DHCP al server DHCP.

DHCPv4 nel Livello 2 e Livello 3

In modalità di sistema Livello 2, il dispositivo trasmette i messaggi DHCP ricevuti dalle VLAN con la funzionalità Inoltro DHCP abilitata.

In modalità di sistema Livello 3, il dispositivo è anche in grado di trasmettere messaggi DHCP ricevuti da VLAN prive di indirizzi IP. Ogni volta che l'Inoltro DHCP è attivo su una VLAN senza indirizzo IP, viene inserita automaticamente l'Opzione 82. Questo inserimento riguarda la specifica VLAN e non influenza lo stato di amministrazione globale relativo all'inserimento dell'Opzione 82.

Inoltro DHCP trasparente

Per l'Inoltro DHCP trasparente, dove viene utilizzato un agente di Inoltro DHCP esterno:

- Attivare lo Snooping DHCP.
- Attivare l'inserimento dell'Opzione 82.
- Disattivare l'Inoltro DHCP.

Per l'Inoltro DHCP normale:

- Attivare l'Inoltro DHCP.
- Non è necessario attivare l'inserimento dell'Opzione 82.

Option 82

L'Opzione 82 (opzione informazioni sull'agente di Inoltro DHCP) trasmette le informazioni sulla porta e sull'agente a un server DHCP centrale, indicando il punto in cui un indirizzo IP assegnato si connette fisicamente alla rete.

L'obiettivo principale dell'Opzione 82 è di supportare il server DHCP nella scelta della migliore subnet IP (pool di rete) da cui ottenere un indirizzo IP.

Sul dispositivo sono disponibili le seguenti opzioni per l'Opzione 82:

- **Inserimento DHCP**: aggiunge le informazioni dell'Opzione 82 ai pacchetti senza informazioni esterne sull'Opzione 82.
- **Passthrough DHCP**: inoltra o respinge i pacchetti DHCP che contengono informazioni sull'Opzione 82 da porte non attendibili. Sulle porte attendibili, i pacchetti DHCP contenenti informazioni sull'Opzione 82 vengono sempre inoltrati.

La tabella seguente mostra il flusso di pacchetti attraverso i moduli Inoltro DHCP, Snooping DHCP e Opzione 82.

Possono verificarsi i seguenti casi:

- Un Client DHCP e un server DHCP sono connessi alla stessa VLAN. In questo caso, un normale bridging trasmette i messaggi DHCP tra il client DHCP e il server DHCP.
- Un Client DHCP e un server DHCP sono connessi a VLAN diverse. In questo caso, solo l'Inoltro DHCP consente di trasmettere i messaggi DHCP tra il client DHCP e il server DHCP. I messaggi unicast DHCP sono trasmessi da router normali; pertanto, se l'Inoltro DHCP è attivato su una VLAN senza indirizzo IP o se il dispositivo non è un router (dispositivo di Livello 2), è necessario un router esterno.

Solo l'Inoltro DHCP trasmette i messaggi DHCP al server DHCP.

Interazioni tra Snooping DHCPv4, Inoltro DHCPv4 e Opzione 82

Nelle tabelle seguenti viene descritto il funzionamento del dispositivo con varie combinazioni di Snooping DHCP, Inoltro DHCP e Opzione 82.

La seguente tabella descrive in che modo vengono gestiti i pacchetti DHCP quando lo Snooping DHCP non è attivo e l'Inoltro DHCP è attivo.

	Inoltro DHCP **VLAN con indirizzo IP**		**Inoltro DHCP** **VLAN senza indirizzo IP**	
	Il pacchetto arriva senza l'Opzione 82	Il pacchetto arriva con l'Opzione 82	Il pacchetto arriva senza l'Opzione 82	Il pacchetto arriva con l'Opzione 82

	Inoltro DHCP VLAN con indirizzo IP		Inoltro DHCP VLAN senza indirizzo IP	
L'inserimento Opzione 82 non è attivo	Il pacchetto viene inviato senza l'Opzione 82	Il pacchetto viene inviato con l'Opzione 82 originale	Inoltro: l'Opzione 82 viene inserita Bridge: non viene inserita nessuna Opzione 82	Inoltro: il pacchetto viene eliminato Bridge: il pacchetto viene inviato con l'Opzione 82 originale
L'inserimento Opzione 82 è attivo	Inoltro: viene inviato con l'Opzione 82 Bridge: non viene inviata nessuna Opzione 82	Il pacchetto viene inviato con l'Opzione 82 originale	Inoltro: viene inviato con l'Opzione 82 Bridge: non viene inviata nessuna Opzione 82	Inoltro: il pacchetto viene eliminato Bridge: il pacchetto viene inviato con l'Opzione 82 originale

La seguente tabella descrive in che modo vengono gestiti i pacchetti di richiesta DHCP quando lo Snooping DHCP e l'Inoltro DHCP sono entrambi attivi:

	Inoltro DHCP VLAN con indirizzo IP		Inoltro DHCP VLAN senza indirizzo IP	
	Il pacchetto arriva senza l'Opzione 82	Il pacchetto arriva con l'Opzione 82	Il pacchetto arriva senza l'Opzione 82	Il pacchetto arriva con l'Opzione 82
L'inserimento Opzione 82 non è attivo	Il pacchetto viene inviato senza l'Opzione 82	Il pacchetto viene inviato con l'Opzione 82 originale	Inoltro: l'Opzione 82 viene inserita Bridge: non viene inserita nessuna Opzione 82	Inoltro: il pacchetto viene eliminato Bridge: il pacchetto viene inviato con l'Opzione 82 originale

	Inoltro DHCP VLAN con indirizzo IP		Inoltro DHCP VLAN senza indirizzo IP	
L'inserimento Opzione 82 è attivo	Inoltro: viene inviato con l'Opzione 82 Bridge: l'Opzione 82 viene aggiunta (se la porta è attendibile, si comporta come se lo Snooping DHCP fosse attivo)	Il pacchetto viene inviato con l'Opzione 82 originale	Inoltro: viene inviato con l'Opzione 82 Bridge: l'Opzione 82 viene inserita (se la porta è attendibile, si comporta come se lo Snooping DHCP fosse attivo)	Inoltro: il pacchetto viene eliminato Bridge: il pacchetto viene inviato con l'Opzione 82 originale

La seguente tabella descrive in che modo vengono gestiti i pacchetti di risposta DHCP quando lo Snooping DHCP non è attivo:

	Inoltro DHCP VLAN con indirizzo IP		Inoltro DHCP VLAN senza indirizzo IP	
	Il pacchetto arriva senza l'Opzione 82	Il pacchetto arriva con l'Opzione 82	Il pacchetto arriva senza l'Opzione 82	Il pacchetto arriva con l'Opzione 82

	Inoltro DHCP VLAN con indirizzo IP		Inoltro DHCP VLAN senza indirizzo IP	
L'inserimento Opzione 82 non è attivo	Il pacchetto viene inviato senza l'Opzione 82	Il pacchetto viene inviato con l'Opzione 82 originale	Inoltro: l'Opzione 82 viene ignorata Bridge: il pacchetto viene inviato senza l'Opzione 82	Inoltro: 1. Se la risposta ha origine nel dispositivo, il pacchetto viene inviato senza l'Opzione 82. 2. Se la risposta non ha origine nel dispositivo, il pacchetto viene eliminato. Bridge: il pacchetto viene inviato con l'Opzione 82 originale
L'inserimento Opzione 82 è attivo	Il pacchetto viene inviato senza l'Opzione 82	Inoltro: il pacchetto viene inviato senza l'Opzione 82 Bridge: il pacchetto viene inviato con l'Opzione 82	Inoltro: l'Opzione 82 viene ignorata Bridge: il pacchetto viene inviato senza l'Opzione 82	Inoltro: il pacchetto viene inviato senza l'Opzione 82 Bridge: il pacchetto viene inviato con l'Opzione 82

La seguente tabella descrive in che modo vengono gestiti i pacchetti di risposta DHCP quando lo Snooping DHCP e l'Inoltro DHCP sono entrambi attivi:

	Inoltro DHCP **VLAN con indirizzo IP**		**Inoltro DHCP** **VLAN senza indirizzo IP**	
	Il pacchetto arriva senza l'Opzione 82	Il pacchetto arriva con l'Opzione 82	Il pacchetto arriva senza l'Opzione 82	Il pacchetto arriva con l'Opzione 82
L'inserimento Opzione 82 non è attivo	Il pacchetto viene inviato senza l'Opzione 82	Il pacchetto viene inviato con l'Opzione 82 originale	Inoltro: elimina l'Opzione 82 Bridge: il pacchetto viene inviato senza l'Opzione 82	Inoltro 1. Se la risposta ha origine nel dispositivo, il pacchetto viene inviato senza l'Opzione 82. 2. Se la risposta non ha origine nel dispositivo, il pacchetto viene eliminato. Bridge: il pacchetto viene inviato con l'Opzione 82 originale
L'inserimento Opzione 82 è attivo	Il pacchetto viene inviato senza l'Opzione 82	Il pacchetto viene inviato senza l'Opzione 82	Inoltro: l'Opzione 82 viene ignorata Bridge: il pacchetto viene inviato senza l'Opzione 82	Il pacchetto viene inviato senza l'Opzione 82

Database di binding per snooping DHCP

Lo Snooping DHCP crea un database (noto come Database di binding per snooping DHCP) ricavato dalle informazioni prese dai pacchetti DHCP in ingresso nel dispositivo tramite porte attendibili.

Il database di binding per snooping DHCP contiene i seguenti dati: porta di ingresso, VLAN di ingresso, indirizzo MAC del client e indirizzo IP del client, se esiste.

Il database di binding per snooping DHCP è utilizzato anche dalle funzioni di Guardia origine IP e Esame ARP dinamico per determinare le origini autorizzate dei pacchetti.

Porte attendibili DHCP

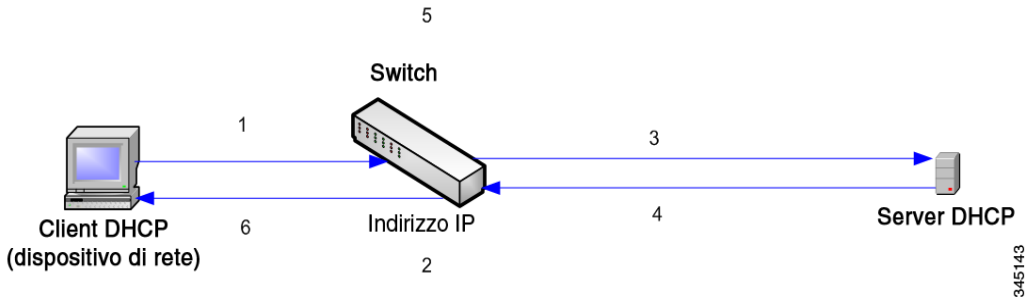
Le porte DHCP possono essere attendibili e non attendibili. Per impostazione predefinita, tutte le porte sono non attendibili. Per creare una porta attendibile, utilizzare la pagina Impostazioni delle interfacce per snooping DHCP. I pacchetti provenienti da queste porte vengono inoltrati automaticamente. I pacchetti dalle porte attendibili vengono utilizzati per creare il database di binding e sono gestiti nel modo descritto di seguito.

Se lo Snooping DHCP non è attivo, tutte le porte sono attendibili per impostazione predefinita.

Creazione del database di binding per snooping DHCP

Nel seguente paragrafo viene descritto il modo in cui il dispositivo gestisce i pacchetti DHCP quando sia il client DHCP che il server DHCP sono attendibili. In questa fase viene creato il database di binding per snooping DHCP.

Gestione dei pacchetti DHCP attendibili



Le operazioni sono:

PASSAGGIO 1 Il dispositivo invia DHCPDISCOVER per richiedere un indirizzo IP o DHCPREQUEST per accettare un indirizzo IP e un lease.

PASSAGGIO 2 Il dispositivo esegue lo snooping del pacchetto e aggiunge le informazioni IP-MAC al database di binding per snooping DHCP.

PASSAGGIO 3 Il dispositivo inoltra i pacchetti DHCPDISCOVER o DHCPREQUEST.

PASSAGGIO 4 Il server DHCP invia il pacchetto DHCPOFFER per offrire un indirizzo IP, DHCPACK per assegnarne uno o DHCPNAK per negare una richiesta di indirizzo.

PASSAGGIO 5 Il dispositivo esegue lo snooping del pacchetto. Se nella tabella Binding per snooping DHCP esiste una voce che corrisponde al pacchetto, il dispositivo la sostituisce con il binding IP-MAC alla ricezione del pacchetto DHCPACK.

PASSAGGIO 6 Il dispositivo inoltra DHCPOFFER, DHCPACK o DHCPNAK.

Di seguito viene riassunta la modalità di gestione dei pacchetti DHCP da porte attendibili e non attendibili. Il database di binding per snooping DHCP viene memorizzato nella memoria non volatile.

Gestione dei pacchetti snooping DHCP

Tipo di pacchetto	In arrivo da un'interfaccia di ingresso non attendibile	In arrivo da un'interfaccia di ingresso attendibile
DHCPDISCOVER	Inoltra solo a interfacce attendibili.	Inoltrato solo a interfacce attendibili.
DHCPOFFER	Filtro.	Inoltra il pacchetto in base alle informazioni DHCP. Se l'indirizzo di destinazione è sconosciuto, il pacchetto viene filtrato.
DHCPREQUEST	Inoltra solo a interfacce attendibili.	Inoltra solo a interfacce attendibili.
DHCPACK	Filtro.	Come per il pacchetto DHCPOFFER; viene anche aggiunta una voce al database di binding per snooping DHCP.

Tipo di pacchetto	In arrivo da un'interfaccia di ingresso non attendibile	In arrivo da un'interfaccia di ingresso attendibile
DHCPNAK	Filtro.	Come per il pacchetto DHCPOFFER. Rimuove la voce (se esiste).
DHCPDECLINE	Verifica la presenza di informazioni nel database. Se le informazioni esistono e non corrispondono a quelle dell'interfaccia su cui è stato ricevuto il messaggio, il pacchetto viene filtrato. In caso contrario, il pacchetto viene inoltrato a interfacce attendibili e la voce viene rimossa dal database.	Inoltra solo a interfacce attendibili.
DHCPRELEASE	Come per il pacchetto DHCPDECLINE.	Come per il pacchetto DHCPDECLINE.
DHCPINFORM	Inoltra solo a interfacce attendibili.	Inoltra solo a interfacce attendibili.
DHCPLEASEQUERY	Filtrato.	Inoltra.

Snooping DHCP e Inoltro DHCP

Se lo Snooping DHCP e l'Inoltro DHCP sono stati attivati globalmente e se lo Snooping DHCP è attivo sulla VLAN del client, vengono applicate le regole dello Snooping DHCP contenute nel database di binding per snooping DHCP e il database di binding per snooping DHCP viene aggiornato sulla VLAN del client e del server DHCP per i pacchetti inoltrati.

Configurazione predefinita DHCP

Di seguito vengono descritte le opzioni predefinite per lo Snooping DHCP e l'Inoltro DHCP.

Opzioni predefinite DHCP

Opzione	Stato predefinito
Snooping DHCP	**Attivato**
Inserimento Opzione 82	**Non attivato**
Passthrough opzione 82	**Non attivato**
Verifica indirizzo MAC	**Attivato**
Backup del database di binding per snooping DHCP	**Non attivato**
Inoltro DHCP	**Disattivato**

Configurazione del flusso di lavoro DHCP

Per configurare l'Inoltro DHCP e lo Snooping DHCP, attenersi alla seguente procedura:

PASSAGGIO 1 Attivare l'opzione Snooping DHCP e/o Inoltro DHCP nella pagina **Configurazione IP > DHCP > Proprietà** o nella pagina **Protezione > Snooping DHCP > Proprietà**.

PASSAGGIO 2 Specificare le interfacce su cui attivare lo Snooping DHCP nella pagina **Configurazione IP > DHCP > Impostazioni interfaccia**.

PASSAGGIO 3 Configurare le interfacce come attendibili o non attendibili nella pagina **Configurazione IP > DHCP > Interfaccia Snooping DHCP**.

PASSAGGIO 4 Facoltativo. Aggiungere voci al database di binding per snooping DHCP nella pagina **Configurazione IP > DHCP > Database di binding per snooping DHCP**.

Snooping/Inoltro DHCP

In questa sezione viene descritta l'implementazione delle funzioni Inoltro DHCP e Snooping DHCP tramite l'interfaccia basata sul Web.

Proprietà

Per configurare l'Inoltro DHCP, lo Snooping DHCP e l'Opzione 82, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP**> **Interfacce e gestione IPv4**> **Snooping/Inoltro DHCP> Proprietà** o **Protezione** > **Snooping DHCP**.

Immettere informazioni nei seguenti campi:

- **Opzione 82**: selezionare **Opzione 82** per inserire le informazioni dell'Opzione 82 nei pacchetti.
- **Inoltro DHCP**: selezionare questa opzione per attivare l'Inoltro DHCP.
- **Stato snooping DHCP**: selezionare questa opzione per attivare lo Snooping DHCP. Se lo Snooping DHCP è attivato, è possibile abilitare le seguenti opzioni:
  - *Opzione 82 Pass Through*: selezionare questa opzione per lasciare le informazioni esterne dell'Opzione 82 durante l'inoltro dei pacchetti.
  - *Verifica indirizzo MAC*: selezionare questa opzione per verificare che l'indirizzo MAC di origine dell'intestazione di Livello 2 corrisponda all'indirizzo hardware del client dell'intestazione DHCP (parte del carico) sulle porte DHCP non attendibili.
  - *Database di backup*: selezionare questa opzione per eseguire il backup del database di binding per snooping DHCP nella memoria flash del dispositivo.
  - *Intervallo di aggiornamento del database di backup*: inserire la frequenza di backup del database di binding per snooping DHCP (**se è stata selezionata l'opzione Database di backup**).

PASSAGGIO 2 Fare clic su **Applica**. Le impostazioni vengono scritte nel file Configurazione di esecuzione.

PASSAGGIO 3 Per definire un server DHCP, fare su **Aggiungi**.

PASSAGGIO 4 Immettere l'indirizzo IP del server DHCP e fare clic su **Applica**. Le impostazioni vengono scritte nel file Configurazione di esecuzione.

Impostazioni interfaccia

A livello 2, l'Inoltro DHCP e lo Snooping DHCP possono essere attivati solo su VLAN con indirizzi IP.

A livello 3, l'Inoltro DHCP e lo Snooping DHCP possono essere attivati su qualsiasi interfaccia con un indirizzo IP e su VLAN con o senza indirizzo IP.

Per attivare Snooping DHCP/Inoltro DHCP su specifiche interfacce, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP**> **Interfacce e gestione IPv4** > **Inoltro/Snooping UDP > Impostazioni interfaccia**.

PASSAGGIO 2 Per attivare l'Inoltro DHCP o lo Snooping DHCP su un'interfaccia, fare clic su **AGGIUNGI**.

PASSAGGIO 3 Selezionare l'interfaccia e le funzioni da attivare: **Inoltro DHCP** o **Snooping DHCP**.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni vengono scritte nel file Configurazione di esecuzione.

Interfacce attendibili per snooping DHCP

I pacchetti in ingresso da LAG/porte non attendibili vengono controllati a fronte del database di binding per snooping DHCP (vedere la pagina Database di binding per snooping DHCP).

Per impostazione predefinita, le interfacce sono attendibili.

Per specificare un'interfaccia come non attendibile, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP**> **Interfacce e gestione IPv4** > **Inoltro/Snooping DHCP > Interfacce attendibili per snooping DHCP**.

PASSAGGIO 2 Selezionare l'interfaccia e fare clic su **Modifica**.

PASSAGGIO 3 Selezionare **Interfaccia attendibile** (**Sì** o **No**).

PASSAGGIO 4 Fare clic su **Applica** per salvare le impostazione sul file Configurazione di esecuzione.

Database di binding per snooping DHCP

Per una descrizione del modo in cui aggiungere delle voci dinamiche al database di binding per snooping DHCP, vedere **Creazione del database di binding per snooping DHCP**.

Considerare i seguenti punti sulla manutenzione del database di binding per snooping DHCP:

- Il dispositivo non aggiorna il database di binding per snooping DHCP quando una stazione passa a un'altra interfaccia.
- Se una porta è inattiva, le voci per quella porta vengono eliminate.
- Quando lo Snooping DHCP è disattivato per una VLAN, le voci di binding raccolte per quella VLAN vengono rimosse.
- Se il database è pieno, lo Snooping DHCP continua a inoltrare i pacchetti, ma non vengono create nuove voci. Se le funzioni di Guardia origine IP e/o Esame di ARP sono attive, i client non registrati nel database di binding per snooping DHCP non possono connettersi alla rete.

Per aggiungere voci al database di binding per snooping DHCP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP**> **Interfacce e gestione IPv4** >**Inoltro/Snooping DHCP** > **Database di binding per snooping DHCP**.

Per vedere un sottoinsieme di voci nel database di binding per snooping DHCP, immettere i criteri di ricerca rilevanti e fare clic su **Vai**.

Vengono visualizzati i campi nel database di binding per snooping DHCP: sono descritti nella pagina Aggiungi ad eccezione del campo **Guardia origine IP**:

- **Stato:**
  - Attivo: Guardia origine IP è attivo sul dispositivo.
  - Inattivo: Guardia origine IP non è attivo sul dispositivo.
- **Motivo:**
  - Nessun problema
  - Nessuna risorsa
  - Nessuna VLAN snoop
  - Porta attendibile

PASSAGGIO 2 Per aggiungere una voce, fare clic su **Aggiungi**.

PASSAGGIO 3 Completare i seguenti campi:

- **ID VLAN:** VLAN sulla quale è atteso il pacchetto.

- **Indirizzo MAC**: indirizzo MAC del pacchetto.
- **Indirizzo IP**: indirizzo IP del pacchetto.
- **Interfaccia**: unità slot/interfaccia sulla quale è atteso il pacchetto.
- **Tipo**: i possibili valori del campo sono:
  - *Dinamico*: durata del lease limitata per la voce.
  - *Statico:* la voce è stata configurata in maniera statica.
- **Durata lease**: se la voce è di tipo dinamico, immettere l'intervallo di tempo durante il quale la voce deve essere attiva nel database DHCP Se il lease non ha durata, selezionare Infinita.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni vengono definite e il dispositivo viene aggiornato.

Server DHCP

La funzionalità Server DHCPv4 consente di configurare il dispositivo come server DHCPv4. Il server DHCPv4 viene utilizzato per assegnare indirizzi IPv4 e altre informazioni a un altro dispositivo (client DHCP).

Il server DHCPv4 assegna indirizzi IPv4 da un pool di indirizzi IPv4 definiti dall'utente.

Questi possono essere nelle seguenti modalità:

- **Assegnazione statica**: l'indirizzo hardware o l'identificatore client di un host viene associato manualmente a un indirizzo IP. Ciò avviene nella pagina Host statici.
- **Assegnazione dinamica**: un client ottiene un indirizzo IP con lease per un periodo di tempo specificato (che può essere infinito). Se il client DHCP non rinnova l'indirizzo IP assegnato, quest'ultimo viene revocato al termine del periodo e il client deve richiederne un altro. Ciò avviene nella pagina Pool di reti.

Dipendenze tra funzioni

- È impossibile configurare contemporaneamente il server DHCP e il client DHCP sul sistema, ossia: se in un'interfaccia è presente un client DHCP attivo, non è possibile attivare il server DHCP a livello globale.
- Se è attivo l'Inoltro DHCPv4, il dispositivo non può essere configurato come server DHCP.

Impostazioni predefinite e configurazioni

- Il dispositivo non è configurato come server DHCPv4 per impostazione predefinita.
- Se il dispositivo è abilitato come server DHCPv4, non vi sono pool di indirizzi di rete definiti per impostazione predefinita.

Flusso di lavoro per abilitare la funzione server DHCP

Per configurare il dispositivo come server DHCPv4, attenersi alla seguente procedura:

PASSAGGIO 1 Abilitare il dispositivo come server DHCP nella pagina Server DHCP > Proprietà.

PASSAGGIO 2 Utilizzare la pagina Indirizzi esclusi per selezionare eventuali indirizzi IP che non devono essere assegnati.

PASSAGGIO 3 Definire fino a 8 pool di rete di indirizzi IP nella pagina Pool di reti.

PASSAGGIO 4 Configurare i client che riceveranno un indirizzo IP permanente nella pagina Host statici.

PASSAGGIO 5 Configurare le opzioni DHCP richieste nella pagina Opzioni DHCP. Questo consente di configurare i valori che devono essere restituiti per ogni opzione DHCP rilevante.

PASSAGGIO 6 Aggiungere un'interfaccia IP nell'intervallo di uno dei pool DHCP configurati nella pagina Pool di rete. Il dispositivo risponde alle query DHCP da questa Interfaccia IP. Ad esempio: se l'intervallo di pool è 1.1.1.1 -1.1.1.254, aggiungere un indirizzo IP in questo intervallo affinché i client direttamente collegati ricevano gli indirizzi IP dal pool configurato. Eseguire questa operazione nella pagina Configurazione IP > Interfaccia IPv4.

PASSAGGIO 7 Visualizzare gli indirizzi IP assegnati nella pagina Binding dell'indirizzo. In questa pagina è possibile eliminare gli indirizzi IP.

Server DHCPv4

Per configurare il dispositivo come server DHCPv4, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv4**> **Server DHCP** > **Proprietà** per visualizzare la pagina Proprietà.

PASSAGGIO 2 Selezionare **Attiva** per configurare il dispositivo come server DHCPv4.

PASSAGGIO 3 Fare clic su **Applica**. Il dispositivo inizia immediatamente a funzionare come server DHCP. Tuttavia, inizia ad assegnare indirizzi IP ai client solo dopo la creazione di un pool.

Pool di reti

Quando il dispositivo funge da server DHCP, è necessario definire uno o più pool di indirizzi IP da utilizzare per assegnare gli indirizzi IP ai client. Ciascun pool di reti contiene un intervallo di indirizzi che appartengono a una subnet specifica. Questi indirizzi sono assegnati a vari client in tale subnet.

Quando un client richiede un indirizzo IP, il dispositivo che funge da server DHCP assegna un indirizzo IP in base a quanto segue:

- **Client direttamente collegato**: il dispositivo assegna un indirizzo dal pool di reti con subnet corrispondente a quella configurata sull'interfaccia IP del dispositivo da cui è stata ricevuta la richiesta DHCP.
- **Client remoto**: i dispositivi prendono un indirizzo IP dal primo pool di reti con subnet di inoltro, collegata direttamente al client, corrispondente alla subnet configurata su una delle interfacce IP dello switch.

È possibile definire massimo otto pool di reti.

Per creare un pool di indirizzi IP e definire la durata del lease, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv4** > **Server DHCP** > **Pool di reti** per visualizzare la pagina Pool di reti.

Vengono visualizzati i pool di reti definiti in precedenza.

PASSAGGIO 2 Fare clic su **Aggiungi** per aggiungere un nuovo pool di reti. È possibile immettere l'indirizzo IP della subnet e la maschera oppure la maschera, il primo indirizzo e l'ultimo indirizzo del pool di indirizzi.

PASSAGGIO 3 Completare i seguenti campi:

- **Nome pool**: immettere il nome del pool.
- **Indirizzo IP subnet**: immettere la subnet in cui si trova il pool di reti.
- **Maschera**: immettere una delle seguenti opzioni:
  - **Maschera di rete**: selezionare questa opzione e immettere la maschera di rete del pool.
  - **Lunghezza prefisso**: selezionare questa opzione e immettere il numero di bit che compongono il prefisso dell'indirizzo.
- **Inizio pool indirizzi:** immettere il primo indirizzo IP dell'intervallo del pool di reti.
- **Fine pool indirizzi:** immettere l'ultimo indirizzo IP dell'intervallo del pool di reti.
- **Durata lease**: immettere l'intervallo di tempo durante il quale un client DHCP può utilizzare un indirizzo IP da questo pool. È possibile configurare una durata del lease fino a 49.710 giorni o una durata infinita.
  - **Infinita**: la durata del lease è illimitata.
  - **Giorni**: la durata del lease in numero di giorni. L'intervallo è compreso tra 0 e 49.710 giorni.
  - **Ore**: la durata del lease in numero di ore. Per poter aggiungere un valore in questo campo, è necessario immettere un valore nel campo Giorni.
  - **Minuti**: la durata del lease in numero di minuti. Per poter aggiungere un valore in questo campo, è necessario immettere un valore nei campi Giorni e Ore.
- **Indirizzo IP router predefinito (opzione 3):** immettere il router predefinito per il client DHCP.
- **Indirizzo IP server dei nomi di dominio (opzione 6)**: selezionare uno dei dispositivi dei server DNS (se già configurati) oppure selezionare **Altro** e immettere l'indirizzo IP del server DNS disponibile per il client DHCP.
- **Nome di dominio (opzione 15)**: immettere il nome del dominio per un client DHCP.
- **Indirizzo IP server WINS NetBIOS (opzione 44)**: immettere il server dei nomi NetBIOS disponibile per un client DHCP.

- **Tipo nodo NetBIOS (opzione 46):** selezionare come risolvere il nome NetBIOS. I tipi di nodi validi sono:
  - *Ibrido*: si utilizza una combinazione ibrida di nodo B e nodo P. Se configurato per utilizzare un nodo H, un computer tenta sempre prima con il nodo P e utilizza il nodo B soltanto se il primo tentativo fallisce. Questa è l'impostazione predefinita.
  - *Misto*: si utilizza una combinazione di comunicazioni nodo B e nodo P per registrare e risolvere i nomi NetBIOS. Il nodo M utilizza per primo il nodo B; quindi, se necessario, utilizza il nodo P. Generalmente il nodo M non è la soluzione migliore per reti di grandi dimensioni poiché la sua preferenza per le trasmissioni del nodo B aumenta il traffico di rete.
  - *Peer-to-Peer*: vengono utilizzate le comunicazioni Point-to-Point con un server dei nomi NetBIOS per registrare e risolvere i nomi dei computer in indirizzi IP.
  - *Broadcast*: vengono utilizzati messaggi broadcast IP per registrare e risolvere i nomi NetBIOS in indirizzi IP.
- **Indirizzo IP server SNTP (opzione 4):** selezionare uno dei server SNTP del dispositivo (se già configurati) oppure selezionare **Altro** e immettere l'indirizzo IP del server di riferimento dell'ora per il client DHCP.
- **Indirizzo IP server file (siaddr)**: immettere l'indirizzo IP del server TFTP/SCP da cui viene scaricato il file di configurazione.
- **Nome host server file (sname)**: immettere il nome del server TFTP/SCP.
- **Nome file configurazione (file):** immettere il nome del file utilizzato come file di configurazione.

Indirizzi esclusi

Per impostazione predefinita, il server DHCP presume che tutti gli indirizzi del pool possano essere assegnati ai client. È possibile escludere un singolo indirizzo IP o un intervallo di indirizzi IP. Gli indirizzi sono esclusi da tutti i pool DHCP.

Per definire un intervallo di indirizzi esclusi, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv4** > **Server DHCP** > **Indirizzi esclusi** per visualizzare la pagina Indirizzi esclusi.

Vengono visualizzati tutti gli indirizzi IP esclusi definiti in precedenza.

PASSAGGIO 2 Per aggiungere un intervallo di indirizzi IP da escludere, fare clic su **Aggiungi** e compilare i campi seguenti:

- **Indirizzo IP iniziale**: il primo indirizzo IP nell'intervallo di indirizzi IP esclusi.
- **Indirizzo IP finale**: l'ultimo indirizzo IP nell'intervallo di indirizzi IP esclusi.

Host statici

In alcuni casi è necessario assegnare ad alcuni client DHCP un indirizzo IP fisso, che non cambi mai. Questi client sono noti come host statici.

Per assegnare manualmente un indirizzo IP permanente a un client specifico, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv4** > **Server DHCP** > **Host statici** per visualizzare la pagina Host statici.

Vengono visualizzati gli host statici.

PASSAGGIO 2 Per aggiungere un host statico, fare clic su **Aggiungi** e compilare i seguenti campi:

- **Indirizzo IP**: immettere l'indirizzo IP assegnato staticamente all'host.
- **Nome host**: immettere il nome host, che può essere una stringa di simboli e un numero intero.
- **Maschera**: immettere la maschera di rete dell'host statico.
  - *Maschera di rete*: selezionare questa opzione e immettere la maschera di rete dell'host.
  - *Lunghezza prefisso*: selezionare questa opzione e immettere il numero di bit che compongono il prefisso dell'indirizzo.
- **Tipo di identificatore**: specificare come deve essere identificato un determinato host statico.
  - *Identificatore client*: immettere un identificatore univoco del client specificato in notazione esadecimale come: 01b60819681172.

oppure:

- *Indirizzo MAC*: immettere l'indirizzo MAC del client.

- **Nome client**: immettere il nome dell'host statico utilizzando un set standard di caratteri ASCII. Il nome client non deve includere il nome di dominio.
- **Indirizzo IP router predefinito (opzione 3)**: immettere il router predefinito per l'host statico.
- **Indirizzo IP server dei nomi di dominio (opzione 6)**: selezionare uno dei dispositivi dei server DNS (se già configurati) oppure selezionare **Altro** e immettere l'indirizzo IP del server DNS disponibile per il client DHCP.
- **Nome di dominio (opzione 15)**: immettere il nome del dominio per l'host statico.
- **Indirizzo IP server WINS NetBIOS (opzione 44)**: immettere il server dei nomi NetBIOS disponibile per l-host statico.
- **Tipo nodo NetBIOS (opzione 46)**: selezionare come risolvere il nome NetBIOS. I tipi di nodi validi sono:
  - *Ibrido*: si utilizza una combinazione ibrida di nodo B e nodo P. Se configurato per utilizzare un nodo H, un computer tenta sempre prima con il nodo P e utilizza il nodo B soltanto se il primo tentativo fallisce. Questa è l'impostazione predefinita.
  - *Misto*: si utilizza una combinazione di comunicazioni nodo B e nodo P per registrare e risolvere i nomi NetBIOS. Il nodo M utilizza per primo il nodo B; quindi, se necessario, utilizza il nodo P. Generalmente il nodo M non è la soluzione migliore per reti di grandi dimensioni poiché la sua preferenza per le trasmissioni del nodo B aumenta il traffico di rete.
  - *Peer-to-Peer*: vengono utilizzate le comunicazioni Point-to-Point con un server dei nomi NetBIOS per registrare e risolvere i nomi dei computer in indirizzi IP.
  - *Broadcast*: vengono utilizzati messaggi broadcast IP per registrare e risolvere i nomi NetBIOS in indirizzi IP.
- **Indirizzo IP server SNTP (opzione 4)**: selezionare uno dei server SNTP del dispositivo (se già configurati) oppure selezionare **Altro** e immettere l'indirizzo IP del server di riferimento dell'ora per il client DHCP.
- **Indirizzo IP server file (siaddr)**: immettere l'indirizzo IP del server TFTP/SCP da cui viene scaricato il file di configurazione.

- **Nome host server file (sname)**: immettere il nome del server TFTP/SCP.
- **Nome file configurazione (file)**: immettere il nome del file utilizzato come file di configurazione.

Opzioni DHCP

Quando il dispositivo opera come server DHCP, le opzioni DHCP possono essere configurate tramite l'utilizzo dell'opzione HEX. È possibile trovare la descrizione di una di queste opzioni in RFC2131.

La configurazione di queste opzioni determina la risposta inviata ai client DHCP, i cui pacchetti includono una richiesta (utilizzando l'opzione 55) per le opzioni DHCP configurate.

Le opzioni configurate specificamente nelle pagine Server DHCP > Pool di rete e Server DHCP > Host statici (Opzione 3-6, 15, 44, 46, 66, 67) non possono essere configurate mediante la pagina Opzioni DHCP.

Esempio: l'opzione DHCP 66 è configurata con il nome di un server TFTP nella pagina Opzioni DHCP. Quando viene ricevuto il pacchetto DHCP di un client contenente l'opzione 66, il server TFTP viene restituito come valore di opzione 66.

Per configurare una o più opzioni DHCP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP**> **Interfacce e gestione IPv4**> **Server DHCP** > **Opzioni DHCP**.

Vengono visualizzate le opzioni DHCP configurate in precedenza.

PASSAGGIO 2 Configurazione di un'opzione non ancora configurata e inserimento del campo:

- **Nome pool server DHCP**: selezionare uno dei pool degli indirizzi di rete definiti nella pagina Pool di rete.

PASSAGGIO 3 Fare clic su **Aggiungi** e compilare i campi:

- **Codice**: immettere il codice opzione DHCP.
- **Tipo**: il pulsante di opzione per questo campo viene modificato in base al tipo di parametro dell'opzione DHCP. Selezionare uno dei seguenti codici e immettere il valore per i parametri di opzione DHCP:
  - *Hex*: selezionare se si desidera immettere il valore hex del parametro per l'opzione DHCP. Un valore hex può essere fornito in sostituzione di qualsiasi altro tipo di valore. Ad esempio, è possibile fornire un codice hex di un indirizzo IP al posto dell'indirizzo IP stesso.

Siccome per il valore hex non viene eseguita nessuna convalida, quando si inserisce un valore HEX, che rappresenta un valore non valido, non viene visualizzato nessun messaggio di errore e il client potrebbe non essere in grado di gestire il pacchetto DHCP dal server.

- *IP*: selezionare se si desidera immettere un indirizzo IP quando questo risulta rilevante per l'opzione DHCP selezionata.
- *Elenco IP*: immettere un elenco IP separato da virgole.
- *Intero*: selezionare se si desidera immettere un valore intero del parametro per l'opzione DHCP selezionata.
- *Booleano*: selezionare se il parametro per l'opzione DHCP selezionata è booleano.

- **Valore booleano**: se è di tipo booleano, selezionare il valore da restituire: **Vero** o **Falso**.
- **Valore**: se non è di tipo booleano, immettere il valore da inviare per questo codice.
- **Descrizione**: immettere una descrizione scritta per la documentazione.

Binding dell'indirizzo

Utilizzare la pagina Binding dell'indirizzo per visualizzare ed eliminare indirizzi IP assegnati dal dispositivo e i corrispondenti indirizzi MAC.

Per visualizzare e/o rimuovere binding dell'indirizzo:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv4** > **Server DHCP** > **Binding dell'indirizzo** per visualizzare la pagina Binding dell'indirizzo.

Per i binding dell'indirizzo vengono visualizzati i seguenti campi:

- **Indirizzo IP**: gli indirizzi IP dei client DHCP.
- **Tipo di indirizzo**: indica se l'indirizzo del client DHCP viene visualizzato come indirizzo MAC o tramite un identificatore client.
- **Indirizzo MAC/Identificatore client**: identificatore univoco del client specificato come Indirizzo MAC o in notazione esadecimale, ad esempio 01b60819681172.
- **Scadenza lease**: la data e l'ora di scadenza del lease dell'indirizzo IP dell'host oppure Infinita, se è stata definita una durata senza termine.

- **Tipo**: il modo in cui l'indirizzo IP è stato assegnato al client. Le opzioni possibili sono:
  - *Statica*: l'indirizzo hardware dell'host è stato associato a un indirizzo IP.
  - *Dinamica*: l'indirizzo IP, ottenuto dinamicamente dal dispositivo, è di proprietà del client per un periodo di tempo specificato. L'indirizzo IP viene revocato al termine di questo periodo e il client dovrà richiederne un altro.
- **Stato**: le opzioni possibili sono:
  - *Assegnato*: l'indirizzo IP è stato assegnato. Quando un host statico è configurato, il suo stato risulta allocato.
  - *Rifiutato*: l'indirizzo IP è stato offerto ma non accettato, risulta quindi non allocato.
  - *Scaduto*: il lease dell'indirizzo IP è scaduto.
  - *Assegnato in anticipo*: su una voce verrà impostato lo stato Assegnato in anticipo relativamente al tempo trascorso dall'offerta all'invio dell'ACK DHCP da parte del client. Lo stato diventa quindi assegnato.

Interfacce e gestione IPv6

L'Internet Protocol versione 6 (IPv6) è un protocollo a livello di rete per le interreti su cui vengono veicolati i pacchetti. IPv6 è stato ideato per sostituire l'IPv4, il protocollo Internet prevalentemente distribuito.

IPv6 presenta una maggiore flessibilità nelle assegnazioni degli indirizzi IP poiché la dimensione degli indirizzi aumenta da 32 bit a 128 bit. Gli indirizzi IPv6 sono otto gruppi composti da quattro cifre esadecimali, ad esempio FE80:0000:0000:0000:0000:9C00:876A:130B. Viene inoltre accettata la forma abbreviata, in cui è possibile tralasciare un gruppo di zeri e sostituirlo con '::', ad esempio ::-FE80::9C00:876A:130B.

Affinché i nodi IPv6 comunichino con altri nodi IPv6 su una rete basata solo su IPv4, è necessario un meccanismo di associazione intermedio. Tale meccanismo, denominato tunnel, consente agli host solo di tipo IPv6 di accedere ai servizi IPv4 e permette agli host IPv6 isolati e alle reti di utilizzare sull'infrastruttura IPv4 un nodo IPv6.

Il tunneling utilizza un meccanismo ISATAP o manuale (vedere la sezione **Tunnel IPv6**). Il tunneling tratta la rete IPv4 come se fosse un collegamento locale IPv6 virtuale tramite l'associazione di ciascun indirizzo IPv4 a un collegamento dell'indirizzo IPv6 locale.

Il dispositivo rileva i frame IPv6 tramite il tipo di connessione Ethernet IPv6.

Routing statico IPv6

Come accade nel routing IPv4, i frame inviati all'indirizzo MAC del dispositivo, ma a un indirizzo IPv6 di destinazione sconosciuto al dispositivo, vengono inoltrati a un dispositivo dell'hop successivo. Questo dispositivo può essere la stazione finale di destinazione o un router più vicino alla destinazione. Il meccanismo di inoltro comporta la ricostruzione di un frame L2 attorno al pacchetto L3 (essenzialmente) non modificato ricevuto, con l'indirizzo MAC del dispositivo dell'hop successivo come indirizzo MAC di destinazione.

Il sistema utilizza messaggi Routing statico e Rilevamento dei router adiacenti (simili ai messaggi ARP IPv4) per costruire le tabelle di inoltro appropriate e gli indirizzi dell'hop successivo.

Un percorso definisce il "tracciato" fra due dispositivi di rete. Le voci di routing aggiunte dall'utente sono statiche e vengono conservate e utilizzate dal sistema fino a quando non vengono esplicitamente rimosse dall'utente e non vengono modificate dai protocolli di routing. L'aggiornamento dei percorsi statici deve essere eseguito in maniera esplicita dall'utente. È responsabilità dell'utente prevenire i loop di routing nella rete.

I percorsi IPv6 statici possono essere:

- Direttamente collegati: la destinazione è direttamente collegata a un'interfaccia sul dispositivo in modo che la destinazione del pacchetto (che è l'interfaccia) sia utilizzata come indirizzo dell'hop successivo.
- Ricorsivi: viene specificato soltanto l'hop successivo e l'interfaccia in uscita è derivata dall'hop successivo.

Allo stesso modo, l'indirizzo MAC dei dispositivi dell'hop successivo (inclusi i sistemi finali direttamente collegati) viene derivato automaticamente tramite la funzione di rilevamento della rete. Tuttavia, l'utente può annullare e integrare tale impostazione aggiungendo manualmente voci alla tabella Router adiacenti.

Configurazione globale IPv6

Per definire i parametri globali IPv6 e le impostazioni client DHCPv6, attenersi alla seguente procedura:

PASSAGGIO 1 In modalità di sistema Livello 2, fare clic su **Amministrazione** > **Interfaccia di gestione** > **Configurazione globale IPv6**.

In modalità di sistema Livello 3, fare clic su **Configurazione IP** > **Interfacce e gestione IPv6** > **Configurazione globale IPv6**.

PASSAGGIO 2 Immettere i valori dei seguenti campi:

- **Routing IPv6**: (solo Livello 3) selezionare questa opzione per attivare il routing IPv6. Se tale impostazione non è attivata, il dispositivo agisce come host (non come router) e può ricevere pacchetti di gestione, ma non può inoltrare pacchetti. Se il routing è attivato, il dispositivo può inoltrare pacchetti IPv6.
- **Intervallo limite di velocità ICMPv6**: indicare la frequenza con cui i messaggi ICMP di errore vengono generati.
- **Dimensioni bucket limite di velocità ICMPv6**: immettere il numero massimo di messaggi di errore ICMP inviati dal dispositivo per intervallo.
- **Limite hop IPv6**: (solo Livello 3) immettere il numero massimo di router intermedi sul percorso verso la destinazione finale che un pacchetto può superare. Ogni volta che un pacchetto viene inoltrato a un altro router, il limite hop si riduce. Quando il limite hop si azzera, il pacchetto viene eliminato. Ciò impedisce che i pacchetti vengano trasferiti in maniera illimitata.

Impostazioni client DHCPv6

- **Formato identificatore univoco (DUID)**: l'identificatore del client DHCP utilizzato dal server DHCP per localizzare il client. Può essere in uno dei seguenti formati:
  - *Link Layer*: (opzione predefinita). Se si seleziona questa opzione, si utilizza l'indirizzo MAC del dispositivo.
  - *Codice aziendale*: se si seleziona questa opzione, immettere i valori nei campi seguenti.
- **Codice aziendale**: il codice Private Enterprise registrato e gestito da IANA.

- **Identificatore**: la stringa esadecimale definita dal fornitore (fino a 64 caratteri esadecimali). Se il numero di caratteri non è pari, viene aggiunto uno zero a destra. Ogni due caratteri esadecimali è possibile inserire una separazione con un punto o due punti.
- **Identificatore univoco DHCPv6 (DUID)**: visualizza l'identificatore selezionato.

Interfaccia IPv6

È possibile configurare un'interfaccia IPv6 su una porta, un LAG, una VLAN, un'interfaccia loopback o un tunnel.

Un'interfaccia tunnel viene configurata con un indirizzo IPv6 in base alle impostazioni definite nella pagina Tunnel IPv6.

Per definire un'interfaccia IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 In modalità di sistema Livello 2, fare clic su **Amministrazione** > **Interfaccia di gestione** > **Interfacce IPv6**.
In modalità di sistema Livello 3, fare clic su **Configurazione IP** > **Interfacce e gestione IPv6** > **Interfacce IPv6**.

PASSAGGIO 2 Immettere i parametri.

- **Zona predefinita locale collegamento IPv6**: (solo Livello 3) selezionare questa opzione per attivare la definizione di una zona predefinita. Si tratta di un'interfaccia da utilizzare per l'uscita di un pacchetto locale di collegamento in arrivo senza un'interfaccia specifica o con la zona predefinita 0.
- **Interfaccia zona predefinita locale collegamento IPv6**: (solo Livello 3) selezionare un'interfaccia da utilizzare come zona predefinita. Può trattarsi di un tunnel o di un'altra interfaccia definita in precedenza.

PASSAGGIO 3 Fare clic su **Aggiungi** per aggiungere una nuova interfaccia sulla quale è attivata l'interfaccia IPv6.

PASSAGGIO 4 Immettere nei campi:

- **Interfaccia IPv6**: selezionare una porta, un LAG, una VLAN o un tunnel specifico per l'indirizzo IPv6. Per i dispositivi Sx500 è possibile configurare soltanto tunnel **ISATAP**. Per gli altri dispositivi 500, è possibile configurare sia tunnel manuali che ISATAP.
- **Tipo di tunnel**: (non presente per Sx500) se l'interfaccia IPv6 è un tunnel, selezionare il tipo: **Manuale** o **ISATAP** (vedere la sezione **Tunnel IPv6**).

PASSAGGIO 5 Per configurare l'interfaccia come client DHCPv6, ovvero per consentire all'interfaccia di ricevere informazioni dal server DHCPv6, quali configurazione SNTP e informazioni DNS, compilare i campi **Client DHCPv6**:

- **Stateless**: selezionare questa opzione per attivare l'interfaccia come client DHCPv6 stateless. Questa procedura consente di attivare la ricezione di informazioni sulla configurazione da un server DHCP.
- **Tempo minimo aggiornamento informazioni**: questo valore è utilizzato per impostare un intervallo minimo di aggiornamento. Se il server invia un'opzione di aggiornamento minore di questo valore, verrà utilizzato il valore specificato qui. Selezionare **Infinito** (l'aggiornamento avviene soltanto se il server invia questa opzione) oppure **Definito dall'utente** per impostare un valore.
- **Tempo aggiornamento informazioni**: questo valore indica la frequenza di aggiornamento delle informazioni sul dispositivo ricevute dal server DHCPv6. Se questa opzione non viene ricevuta dal server, viene utilizzato il valore immesso qui. Selezionare **Infinito** (l'aggiornamento avviene soltanto se il server invia questa opzione) oppure **Definito dall'utente** per impostare un valore.

PASSAGGIO 6 Per configurare parametri IPv6 aggiuntivi, compilare i seguenti campi:

- **Configurazione automatica indirizzo IPv6**: selezionare questa opzione per attivare la configurazione automatica dell'indirizzo dagli annunci del router inviati dai dispositivi adiacenti.

  NOTA Il dispositivo non supporta la configurazione automatica stateful dell'indirizzo da un server DHCPv6.

- **Numero di tentativi DAD**: immettere il numero di messaggi di richiesta adiacenti consecutivi inviati durante l'esecuzione del Duplicate Address Detection (DAD) sugli indirizzi IPv6 unicast dell'interfaccia. Il DAD verifica l'univocità di un nuovo indirizzo IPv6 unicast prima che venga assegnato. Durante la verifica DAD, i nuovi indirizzi rimangono in uno stato provvisorio. Se si immette **0** in questo campo, la procedura di rilevamento degli indirizzi duplicati sull'interfaccia indicata viene disabilitata. Se si immette **1** in questo campo, viene indicata una singola trasmissione senza riportare quelle successive.
- **Invia messaggi ICMPv6**: attiva la generazione di messaggi con destinazione non raggiungibile.
- **Versione MLD**: (solo Livello 3) versione MLD IPv6.

- **Reindirizzamenti IPv6**: (solo Livello 3) selezionare questa opzione per attivare l'invio di messaggio di reindirizzamento IPv6 ICMP. Questi messaggi informano gli altri dispositivi di non inviare traffico al dispositivo, ma a un altro.

PASSAGGIO 7 Fare clic su **Applica** per attivare l'elaborazione IPv6 sull'interfaccia selezionata. Le interfacce IPv6 standard presentano i seguenti indirizzi configurati automaticamente:

- Indirizzo locale collegamento tramite un ID interfaccia di formato EUI-64 basato su un indirizzo MAC del dispositivo.
- Tutti gli indirizzi multicast locali del collegamento del nodo (FF02::1)
- Indirizzo multicast del nodo richiesto (formato FF02::1:FFXX:XXXX)

PASSAGGIO 8 Scegliere **Tabella Indirizzo IPv6** per assegnare, se richiesto, indirizzi IPv6 all'interfaccia. Questa pagina viene descritta nella sezione **Definizione indirizzi IPv6**.

PASSAGGIO 9 Selezionare **Riavvia** per avviare l'aggiornamento delle informazioni stateless ricevute dal server DHCPv6.

Dettagli client DHCPv6

Il pulsante **Dettagli client DHCPv6** visualizza le informazioni ricevute sull'interfaccia da un server DHCPv6.

Questo pulsante è attivo quando l'interfaccia selezionata è definita come client stateless DHCPv6.

Se si fa clic su questo pulsante, vengono visualizzati i campi seguenti (per le informazioni ricevute dal server DHCP):

- **Modalità operativa DHCPv6**: viene visualizzato Attivata se sono soddisfatte le condizioni seguenti:
  - L'interfaccia è attiva.
  - IPv6 è abilitato.
  - Il client stateless DDHCPv6 è abilitato.
- **Servizio Stateless**: indica se il client è definito come stateless (riceve le informazioni di configurazione da un server DHCP) o meno.
- **Indirizzo server DHCPv6**: indirizzo del server DHCPv6.
- **DUID server DHCPv6**: identificatore univoco del server DHCPv6.

- **Preferenza server DHCPv6**: priorità del server DHCPv6.
- **Tempo minimo aggiornamento informazioni**: vedere sopra.
- **Tempo aggiornamento informazioni**: vedere sopra.
- **Tempo aggiornamento informazioni ricevute**: tempo di aggiornamento ricevuto dal server DHCPv6.
- **Tempo rimanente aggiornamento informazioni**: tempo rimanente fino all'aggiornamento successivo.
- **Server DNS**: elenco dei server DNS ricevuti dal server DHCPv6.
- **Elenco di ricerca dominio DNS**: elenco dei domini ricevuti dal server DHCPv6.
- **Server SNTP**: elenco dei server SNTP ricevuti dal server DHCPv6.
- **Stringa fuso orario POSIX**: fuso orario ricevuto dal server DHCPv6.
- **Server configurazione**: server contenente il file di configurazione ricevuto dal server DHCPv6.
- **Nome percorso di configurazione**: percorso al file di configurazione sul server di configurazione ricevuto dal server DHCPv6.

Tunnel IPv6

I tunnel consentono la trasmissione di pacchetti IPv6 su reti IPv4. Ogni tunnel ha un indirizzo IPv4 di origine e un indirizzo IPv4 di destinazione. Il pacchetto IPv6 è incapsulato tra questi indirizzi.

NOTA I tunnel ISATAP possono essere attivati sul dispositivo solo se il routing IPv6 non è attivato ed è possibile eseguire il tunneling della sola interfaccia di gestione IPv6. Per creare un tunnel IPv6, definire un'interfaccia IPv6 come tunnel nella pagina Interfacce IPv6, quindi configurare il tunnel nella pagina Tunnel IPv6.

Tipi di tunnel

Sul dispositivo è possibile configurare due tipi di tunnel, come segue:

- Tunnel ISATAP

  Il protocollo ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) è un tunnel point-to-multi-point. L'indirizzo di origine è l'indirizzo IPv4 (o uno degli indirizzi IPv4) del dispositivo.

Quando si configura un tunnel ISATAP, l'indirizzo IPv4 di destinazione è fornito dal router. Nota:

- Nell'interfaccia ISATAP viene assegnato un indirizzo locale collegamento IPv6. Nell'interfaccia viene assegnato l'indirizzo IP iniziale e quindi attivato.
- Se risulta attiva un'interfaccia ISATAP, l'indirizzo IPv4 del router ISATAP viene determinato tramite DNS attraverso l'associazione di ISATAP a IPv4. Se non si ottiene il registro DNS di ISATAP, l'associazione del nome host di ISATAP all'indirizzo viene ricercata nella tabella di associazione degli host.
- Quando non viene determinato l'indirizzo IPv4 del router ISATAP tramite il processo DNS, l'interfaccia IP dell'ISATAP rimane attiva. Il sistema non presenterà un router predefinito per il traffico ISATAP fino al completamento del processo DNS.

▪ Tunnel manuale

Si tratta di una definizione point-to-point. Quando si crea un tunnel manuale, si immette sia l'indirizzo IP di origine (uno degli indirizzi IP del dispositivo) sia l'indirizzo IPv4 di destinazione.

È possibile definire fino a 16 tunnel (uno dei quali può essere ISATAP).

Configurazione dei tunnel

NOTA Per configurare un tunnel, è necessario configurare prima un'interfaccia IPv6 come tunnel nella pagina Interfacce IPv6.

Per configurare un tunnel IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 In modalità di sistema Livello 2, fare clic su **Amministrazione > Interfaccia di gestione > Tunnel IPv6**.

La modalità Livello 2 è disponibile soltanto sui dispositivi Sx500 e SG500X quando sono in modalità stack Ibrido.

PASSAGGIO 2 In modalità di sistema Livello 3, fare clic su **Configurazione IP** > **Interfacce e gestione IPv6** > **Tunnel IPv6**.

PASSAGGIO 3 Immettere i **parametri ISATAP**.

▪ **Intervallo richiesta**: il numero di secondi che intercorre tra i messaggi di richiesta del router ISATAP, in assenza di router ISATAP attivi. L'intervallo può essere un valore predefinito oppure definito dall'utente.

- **Affidabilità**: serve a calcolare l'intervallo delle query di richiesta del router. Più il numero è grande, più frequenti saranno le query.

  NOTA Il tunnel ISATAP non risulta attivo se l'interfaccia IPv4 basilare non è operativa.

PASSAGGIO 4 Fare clic su **Applica** per salvare i parametri ISATAP nel file di configurazione esecuzione.

PASSAGGIO 5 Per modificare un tunnel, selezionare un'interfaccia (definita come tunnel nella pagina Interfacce IPv6) nella tabella Tunnel IPv6 e fare clic su **Modifica**.

PASSAGGIO 6 Immettere informazioni nei seguenti campi:

- **Tipo**: visualizza il tipo di tunnel: **Manuale** o **ISATAP**.
- **Tipo tunnel**: selezionare questa opzione per attivare il tunnel.
- **Trap SNMP sullo stato del collegamento**: selezionare per attivare la generazione di una trap quando viene modificato lo stato del collegamento di una porta. Se non si desidera ricevere tali trap su porte specifiche (ad esempio, l'ISP richiede i trap solo sulle porte connesse alle sua infrastruttura e non li richiede per le porte connesse al dispositivo dell'utente), la funzione può essere disattivata.
- **Origine**: impostare l'indirizzo IPv4 (di origine) locale di un'interfaccia tunnel. L'indirizzo IPv4 dell'interfaccia IPv4 selezionata viene utilizzato per creare una parte dell'indirizzo IPv6 sull'interfaccia tunnel ISATAP. L'indirizzo IPv6 presenta un prefisso di rete a 64 bit di fe80:: e il resto dei 64 bit risultati dalla concatenazione di 0000:5EFE e l'indirizzo IPv4.
  - *Automatico*: seleziona automaticamente l'indirizzo IPv4 più basso tra tutte le interfacce IPv4 configurate come indirizzo di origine per i pacchetti inviati sull'interfaccia tunnel.
  - Se si modifica l'indirizzo IPv4, viene modificato anche l'indirizzo locale dell'interfaccia tunnel.
  - *Indirizzo IPv4*: specifica l'indirizzo IPv4 da utilizzare come indirizzo di origine per i pacchetti inviati sull'interfaccia tunnel. L'indirizzo locale dell'interfaccia tunnel non viene modificato quando si sposta l'indirizzo IPv4 su un'altra interfaccia.

    NOTA Se si modifica l'indirizzo IPv4, l'indirizzo locale dell'interfaccia tunnel non viene modificato.
  - *Interfaccia*: selezionare l'interfaccia il cui indirizzo IPv4 sarà utilizzato come indirizzo di origine del tunnel.

Se l'interfaccia presenta più indirizzi IPv4, come indirizzo di origine verrà utilizzato l'indirizzo IPv4 più basso. Se l'indirizzo IPv4 più basso viene rimosso dall'interfaccia (eliminato o spostato su un'altra interfaccia), si sceglie l'indirizzo IPv4 più basso successivo come indirizzo IPv4 locale.

- **Destinazione**: (solo per tunnel manuale) selezionare una delle seguenti opzioni per specificare l'indirizzo di destinazione del tunnel:
  - *Nome host*: nome DNS dell'host remoto.
  - *Indirizzo IPv4*: indirizzo IPv4 dell'host remoto.
- **Nome router ISATAP**: (solo per tunnel ISATAP) selezionare una delle seguenti opzioni per configurare una stringa globale che rappresenta il nome di dominio del router di un tunnel automatico specifico.
  - *Usa predefinito*: sempre ISATAP.
  - *Definito dall'utente*: immettere il nome di dominio del router.

PASSAGGIO 7 Fare clic su **Applica**. Il tunnel viene salvato nel file di configurazione esecuzione.

Definizione indirizzi IPv6

Per assegnare un indirizzo IPv6 su un'interfaccia IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 In modalità di sistema Livello 2, fare clic su **Amministrazione** > **Interfaccia di gestione** > **Indirizzi IPv6**.
In modalità di sistema Livello 3, fare clic su **Configurazione IP** > **Interfacce e gestione IPv6** > **Indirizzi IPv6**.

PASSAGGIO 2 Per applicare un filtro alla tabella, selezionare il nome di un'interfaccia e fare clic su **Vai**. L'interfaccia viene visualizzata nella Tabella Indirizzo IPv6.

PASSAGGIO 3 Fare clic su **Aggiungi**.

PASSAGGIO 4 Immettere i valori per i campi.

- **Interfaccia IPv6**: visualizza l'interfaccia su cui viene definito l'indirizzo IPv6. Se viene visualizzato un asterisco (*) significa che l'interfaccia IPv6 non è abilitata ma è stata configurata.

- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 da aggiungere.
  - *Collegamento locale*: un indirizzo IPv6 che identifica in modo univoco gli host in un singolo collegamento di rete. L'indirizzo locale di un collegamento presenta un prefisso **FE80**, non è reindirizzabile e può essere utilizzato solo per le comunicazioni sulle rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
  - *Globale*: un indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
  - *Anycast*: (solo Livello 3) l'indirizzo IPv6 è un indirizzo Anycast. Si tratta di un indirizzo assegnato a una serie di interfacce che generalmente appartengono a nodi diversi. Un pacchetto inviato a un indirizzo Anycast viene consegnato all'interfaccia più vicina, definita dai protocolli di routing in uso, identificata dall'indirizzo Anycast.

  NOTA Se l'indirizzo IPv6 è su un'interfaccia ISATAP non è possibile utilizzare Anycast.

- **Indirizzo IPv6**: nel Livello 2, il dispositivo supporta un'unica interfaccia IPv6. Oltre agli indirizzi locali di collegamento predefiniti e multicast, il dispositivo aggiunge automaticamente all'interfaccia anche indirizzi globali, sulla base degli annunci router ricevuti. Il dispositivo supporta un massimo di 128 indirizzi nell'interfaccia. Ciascun indirizzo deve essere un indirizzo IPv6 valido, specificato in formato esadecimale da valori a 16 bit separati da due punti.Non è possibile configurare indirizzi IPv6 direttamente su un'interfaccia tunnel ISATAP.
- **Lunghezza prefisso**: è la lunghezza del prefisso dell'IPv6 globale, espresso da un valore da 0 a 128 che indica il numero di bit contigui più significativi che formano il prefisso dell'indirizzo (la parte dell'indirizzo che indica la rete).
- **EUI-64**: utilizzare il parametro EUI-64 per identificare la parte dell'ID dell'interfaccia dell'indirizzo IPv6 globale attraverso il formato EUI-64, sulla base dell'indirizzo MAC di un dispositivo.

PASSAGGIO 5 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Configurazione router IPv6

Le sezioni seguenti descrivono come configurare i router IPv6.

Annuncio router

I router IPv6 possono annunciare i propri prefissi ai dispositivi adiacenti. Per attivare o disattivare questa funzionalità per ogni interfaccia, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv4** > **Configurazione router IPv6 > Annuncio router**.

PASSAGGIO 2 Per configurare un'interfaccia elencata nella tabella Annuncio router, selezionarla e fare clic su **Modifica**.

PASSAGGIO 3 Immettere informazioni nei seguenti campi:

- **Sopprimi annuncio router**: selezionare **Sì** per sopprimere le trasmissioni degli annunci router IPv6 sull'interfaccia. Se questa opzione è disattivata, immettere i valori nei campi seguenti.
- **Preferenza router**: selezionare la preferenza (**Bassa**, **Media** o **Alta**) per il router. I messaggi RA vengono inviati con la preferenza configurata in questo campo. Se questo campo non viene impostato, i messaggi vengono inviati con una preferenza media.

L'associazione di una preferenza a un router è utile quando, ad esempio, due router su un collegamento forniscono routing equivalente, ma a costi diversi, e le direttive possono imporre che gli host preferiscano uno dei router.

- **Includi opzione intervallo annuncio**: selezionare questa opzione per indicare che il sistema utilizzerà un'opzione annuncio. Questa opzione indica a un nodo mobile in visita l'intervallo al quale il nodo può aspettarsi di ricevere annunci router. Il nodo può utilizzare queste informazioni nel suo algoritmo di rilevamento del movimento.
- **Limite hop**: il valore dichiarato dal router. Se questo valore è diverso da zero viene usato dall'host come limite di hop.
- **Flag configurazione indirizzo gestito**: selezionare questo flag per indicare agli host collegati che devono utilizzare la configurazione automatica stateful per ottenere gli indirizzi. Gli host possono utilizzare simultaneamente la configurazione automatica degli indirizzi stateful e stateless.

- **Altro flag configurazione stateful**: selezionare questo flag per indicare agli host collegati che devono utilizzare la configurazione automatica stateful per ottenere altre informazioni (non indirizzi).

  NOTA Se si imposta il flag Configurazione indirizzo gestito, un host collegato può utilizzare la configurazione automatica stateful per ottenere le altre informazioni (diverse dall'indirizzo) indipendentemente dall'impostazione di questo flag.

- **Intervallo ritrasmissioni richieste router adiacente**: impostare l'intervallo per determinare il tempo che deve trascorrere tra due ritrasmissioni dei messaggi di richiesta adiacenti a un dispositivo adiacente quando si risolve l'indirizzo o si verifica la raggiungibilità di un dispositivo adiacente.

- **Intervallo massimo annuncio router**: immettere il tempo massimo che può trascorrere tra due annunci del router.

L'intervallo tra trasmissioni deve essere minore o uguale alla durata dell'annuncio router IPv6 se si configura il router come predefinito utilizzando questo comando. Per impedire la sincronizzazione con altri nodi IPv6, l'intervallo effettivo utilizzato viene selezionato a caso da un valore compreso tra quello minimo e quello massimo.

- **Intervallo minimo annuncio router**: immettere il tempo minimo che può trascorrere tra due annunci del router (**Definito dall'utente**) oppure selezionare **Usa predefinito** per utilizzare l'impostazione predefinita del sistema.

  NOTA L'intervallo RA minimo non può mai essere superiore al 75% dell'intervallo RA massimo e mai inferiore a 3 secondi.

- **Durata annuncio router**: immettere il tempo residuo in secondi durante il quale il router continuerà a fungere da router predefinito. Un valore pari a zero indica che non funge più da router predefinito.

- **Tempo raggiungibile**: immettere la quantità di tempo (in millisecondi) durante il quale un nodo IPv6 remoto è considerato raggiungibile (**Definito dall'utente**) oppure selezionare **Usa predefinito** per utilizzare l'impostazione predefinita del sistema.

PASSAGGIO 4 Fare clic su **Applica** per salvare la configurazione nel file di configurazione esecuzione.

Prefissi IPv6

Per definire i prefissi da dichiarare sulle interfacce del dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv6** > **Configurazione router IPv6 > Prefissi IPv6**.

PASSAGGIO 2 Se richiesto, attivare il campo **Filtro** e fare clic su **Vai**. Viene visualizzato il gruppo di interfacce corrispondenti al filtro.

PASSAGGIO 3 Per aggiungere un'interfaccia, fare clic su **Aggiungi**.

PASSAGGIO 4 Selezionare l'interfaccia IPv6 richiesta a cui aggiungere un prefisso.

PASSAGGIO 5 Immettere informazioni nei seguenti campi:

- **Prefisso IPv6**: selezionare **Predefinito** per modificare la configurazione per i prefissi predefiniti creati quando si definisce un indirizzo sull'interfaccia. Utilizzare **Definito dall'utente** per immettere quanto segue:
  - *Indirizzo prefisso*: la rete IPv6. Questo argomento deve essere nella forma documentata in RFC 4293, dove l'indirizzo è specificato in formato esadecimale da valori a 16 bit separati da due punti.
  - *Lunghezza prefisso*: la lunghezza del prefisso IPv6. Un valore decimale che indica il numero di bit di ordine superiore adiacenti dell'indirizzo che costituiscono il prefisso (la porzione di rete dell'indirizzo). Il valore decimale deve essere preceduto da una barra.
- **Annuncio prefisso**: selezionare questa opzione per dichiarare il prefisso.
- **Durata valida**: tempo residuo (in secondi) durante il quale il prefisso continuerà a essere valido, ovvero fino all'invalidazione. L'indirizzo generato da un prefisso invalidato non deve essere indicato come indirizzo di destinazione o di origine di un pacchetto.
  - *Infinita*: selezionare questo valore per impostare il campo su 4.294.967.295, che rappresenta l'infinito.
  - *Definito dall'utente*: immettere un valore.

- **Durata preferita**: tempo residuo, in secondi, durante il quale il prefisso continuerà a essere preferito. Trascorso l'intervallo specificato qui, il prefisso non dovrà più essere utilizzato come indirizzo di origine nelle nuove comunicazioni, ma i pacchetti ricevuti su tale interfaccia saranno elaborati secondo le attese. La durata preferita non deve essere superiore alla durata valida.
  - *Infinita*: selezionare questo valore per impostare il campo su 4.294.967.295, che rappresenta l'infinito.
  - *Definito dall'utente*: immettere un valore.
- **Configurazione automatica**: attivare la configurazione automatica degli indirizzi IPv6 tramite la configurazione automatica stateless su un'interfaccia e attivare l'elaborazione IPv6 sull'interfaccia. Gli indirizzi sono configurati a seconda dei prefissi ricevuti nei messaggi Annuncio router.
- **Stato prefisso**: selezionare una delle seguenti opzioni:
  - *On-link*: configura il prefisso specificato come on-link. I nodi che inviano traffico a indirizzi che contengono il prefisso specificato considerano la destinazione raggiungibile localmente sul collegamento. Un prefisso on-link viene inserito nella tabella di routing come prefisso connesso (bit L impostato).
  - *No on-link*: configura il prefisso specificato come no on-link. Un prefisso no on-link viene inserito nella tabella di routing come prefisso connesso, ma dichiarato con bit L cancellato.
  - *Off-link*: configura il prefisso specificato come off-link. Il prefisso sarà dichiarato con bit L cancellato. Un prefisso non sarà inserito nella tabella di routing come prefisso connesso. Se il prefisso è già presente nella tabella di routing come prefisso connesso (ad esempio perché il prefisso è stato configurato anche aggiungendo un indirizzo IPv6), sarà rimosso.

PASSAGGIO 6 Fare clic su **Applica** per salvare la configurazione nel file di configurazione esecuzione.

Elenco router predefiniti IPv6

La pagina Elenco router predefiniti IPv6 consente la configurazione e la visualizzazione degli indirizzi dei router IPv6 predefiniti. L'elenco contiene i router che potrebbero diventare il router predefinito del dispositivo per il traffico non locale; questo elenco può essere vuoto. Il dispositivo seleziona casualmente un router dall'elenco. Inoltre, supporta un unico router IPv6 statico predefinito. I router dinamici predefiniti inviano annunci router all'interfaccia IPv6 del dispositivo.

Quando si aggiungono o si eliminano indirizzi IP, si verificano gli eventi seguenti:

- Quando si rimuove un'interfaccia IP, vengono rimossi tutti gli indirizzi IP del router predefinito. Non è possibile rimuovere gli indirizzi IP dinamici.
- Dopo aver tentato di inserire più di un singolo indirizzo definito dall'utente, viene visualizzato un messaggio di avviso.
- Quando si tenta di inserire un indirizzo diverso dal tipo di indirizzo locale collegamento, ovvero 'fe80:', viene visualizzato un messaggio di avviso.

Per definire un router predefinito, attenersi alla seguente procedura:

PASSAGGIO 1 In modalità di sistema Livello 2, fare clic su **Amministrazione > Gestione interfaccia > Elenco router predefiniti IPv6**.
In modalità di sistema Livello 3, fare clic su **Configurazione IP** > **Interfacce e gestione IPv6** > **Elenco router predefiniti IPv6**.

In questa pagina vengono visualizzati i seguenti campi per ogni router predefinito:

- **Indirizzo IPv6 router predefinito**: indirizzo IP locale collegamento del router predefinito.
- **Interfaccia**: interfaccia IPv6 esterna in cui si trova il router predefinito.
- **Tipo**: configurazione del router predefinito che include le opzioni seguenti:
  - *Statico*: il router predefinito è stato aggiunto manualmente nella tabella con il pulsante **Aggiungi**.
  - *Dinamico*: il router predefinito è stato configurato dinamicamente.
- **Metrica**: costo dell'hop.

PASSAGGIO 2 Fare clic su **Aggiungi** per aggiungere un router predefinito statico.

PASSAGGIO 3 Immettere informazioni nei seguenti campi:

- **Hop successivo**: l'indirizzo IP della destinazione successiva a cui viene inviato il pacchetto. È composto da:
  - *Globale*: un indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
  - *Collegamento locale*: un'interfaccia e un indirizzo IPv6 che identificano in modo univoco gli host in un singolo collegamento di rete. L'indirizzo locale di un collegamento presenta un prefisso **FE80**, non è reindirizzabile e può essere utilizzato solo per le comunicazioni sulle rete locale. È supportato

soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.

- *Point-to-Point*: un tunnel Point-to-point.

- **Interfaccia**: visualizza l'interfaccia locale collegamento in uscita.
- **Indirizzo IPv6 router predefinito**: indirizzo IP del router statico predefinito.
- **Metrica**: immettere il costo dell'hop.

PASSAGGIO 4 Fare clic su **Applica**. Il router predefinito viene salvato nel file di configurazione esecuzione.

Definizione delle informazioni sui router IPv6 adiacenti

Nella pagina Router IPv6 adiacenti è possibile configurare e visualizzare l'elenco di router IPv6 adiacenti sull'interfaccia IPv6. La tabella Router IPv6 adiacenti (nota anche come cache di rilevamento dei router adiacenti IPv6) consente di visualizzare gli indirizzi MAC dei router adiacenti IPv6 che si trovano nella stessa subnet del dispositivo. È l'equivalente IPv6 della Tabella ARP IPv4. Quando il dispositivo deve comunicare con i router adiacenti, utilizza la Tabella router adiacenti IPv6 per determinare gli indirizzi MAC, sulla base dei loro indirizzi IPv6.

In questa pagina vengono riportati i router adiacenti rilevati automaticamente o le voci configurate manualmente. Ciascuna voce consente di visualizzare l'interfaccia a cui è collegato il router adiacente, i relativi indirizzi IPv6 e MAC, il tipo di voce (statico o dinamico) e lo stato del router.

Per definire i router IPv6 adiacenti, attenersi alla seguente procedura:

PASSAGGIO 1 In modalità di sistema Livello 2, fare clic su **Amministrazione > Interfaccia di gestione > Router IPv6 adiacenti**.
In modalità di sistema Livello 3, fare clic su **Configurazione IP** > **Interfacce e gestione IPv6** > **Router IPv6 adiacenti**.

È possibile selezionare un'opzione **Cancella tabella** per cancellare alcuni o tutti gli indirizzi IPv6 della Tabella IPv6 Adiacenti.

- **Solo statico**: elimina le voci relative all'indirizzo IPv6 statico.
- **Solo dinamico**: elimina le voci relative all'indirizzo IPv6 dinamico.

- **Tutti dinamici e statici**: elimina le voci relative all'indirizzo IPv6 statico e dinamico.

Per le interfacce adiacenti vengono visualizzati i campi seguenti:

- **Interfaccia**: tipo di interfaccia IPv6 adiacente.
- **Indirizzo IPv6**: indirizzo IPv6 di un router adiacente.
- **Indirizzo MAC**: indirizzo MAC associato all'indirizzo IPv6 specificato.
- **Tipo**: tipo di voce (statico o dinamico) relativo alle informazioni contenute nella cache di rilevamento dei router adiacenti.
- **Stato**: indica lo stato del router adiacente IPv6. I valori sono:
  - *Incompleto*: risoluzione dell'indirizzo in corso. Il router adiacente non ha ancora fornito risposta.
  - *Raggiungibile*: il router adiacente è stato riconosciuto, quindi è raggiungibile.
  - *Non aggiornato*: il router adiacente precedentemente riconosciuto non è raggiungibile. Non vengono intraprese azioni per verificare la sua raggiungibilità fino a quando non risulta necessario inviare traffico.
  - *Ritardo*: il router adiacente precedentemente riconosciuto non è raggiungibile. L'interfaccia presenta lo stato Ritardo in base a un Tempo di ritardo predefinito. Se non si riceve conferma sulla raggiungibilità, lo stato diventerà Sonda.
  - *Sonda*: il router adiacente non è più raggiungibile e vengono inviate sonde di tipo Unicast Neighbor Solicitation per verificarne la raggiungibilità.
- **Router**: specifica se il dispositivo adiacente è un router (**Sì** o **No**).

PASSAGGIO 2 Per aggiungere un router contiguo alla tabella, fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i valori dei seguenti campi:

- **Interfaccia**: l'interfaccia IPv6 adiacente da aggiungere.
- **Indirizzo IPv6**: immettere l'indirizzo di rete IPv6 assegnato all'interfaccia. L'indirizzo deve essere un indirizzo IPv6 valido.
- **Indirizzo MAC**: immettere l'indirizzo MAC associato all'indirizzo IPv6 specificato.

PASSAGGIO 4 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

PASSAGGIO 5 Per modificare il tipo di indirizzo IP da **Dinamico** a **Statico**, selezionare l'indirizzo, fare clic su **Modifica** e utilizzare la pagina Modifica router adiacenti IPv6.

Elenco prefissi IPv6

Se la protezione del primo hop viene configurata, è possibile definire le regole per il filtro basato sui prefissi IPv6. Questi elenchi possono essere definiti nella pagina Elenco prefissi IPv6.

Gli elenchi dei prefissi sono configurati con le parole chiave **consenti** o **nega** per consentire o negare in base a una condizione corrispondente. Un rifiuto implicito viene applicato al traffico che non corrisponde a nessuna delle voci presenti nell'elenco dei prefissi.

Una voce di un elenco di prefissi è formata da un indirizzo IP e da una maschera di bit. L'indirizzo IP può essere destinato a una rete basata sulla classe, a una subnet o a un percorso host singolo. La maschera di bit corrisponde a un numero compreso tra 1 e 32.

Gli elenchi dei prefissi sono configurati per filtrare il traffico in base alla corrispondenza di un'esatta lunghezza del prefisso o alla corrispondenza in un intervallo, quando vengono utilizzate le parole chiave ge e le.

I parametri **Maggiore di** e **Minore di** vengono utilizzati per specificare un intervallo di lunghezze del prefisso e offrire una configurazione più flessibile rispetto al solo utilizzo dell'argomento rete/lunghezza. Un elenco di prefissi viene elaborato utilizzando una corrispondenza esatta quando i parametri **Maggiore di** e **Minore di** non sono specificati. Se viene specificato solo il parametro **Maggiore di**, l'intervallo è compreso tra il valore immesso per il parametro **Maggiore di** e la lunghezza complessiva di 32 bit. Se viene specificato solo il parametro **Minore di**, l'intervallo è compreso tra il valore immesso per l'argomento rete/lunghezza e quello attribuito al parametro **Minore di**. Se vengono immessi dei valori per entrambi gli argomenti **Maggiore di** e **Minore di**, l'intervallo è dato dai valori utilizzato per **Maggiore di** e **Minore di**.

Per creare un elenco di prefissi, attenersi alla seguente procedura:

PASSAGGIO 1 (Nel Livello 3) Fare clic su **Configurazione IP> Interfacce di gestione IPv6 > Elenco prefissi IPv6**.

oppure

(Nel Livello 2) Fare clic su **Amministrazione > Interfacce di gestione IPv6 > Elenco prefissi IPv6**.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere informazioni nei seguenti campi:

- **Nome elenco**: selezionare una delle seguenti opzioni:
  - *Utilizza elenco esistente*: selezionare un elenco definito in precedenza a cui aggiungere un prefisso.
  - *Crea nuovo elenco*: immettere un nome per creare un nuovo elenco.
- **Numero sequenza**: specifica la posizione del prefisso all'interno dell'elenco prefissi. Selezionare una delle seguenti opzioni:
  - *Numerazione automatica*: inserisce il nuovo prefisso IPV6 dopo l'ultima voce dell'elenco prefissi. Il numero sequenza è uguale all'ultimo numero sequenza più 5. Se l'elenco è vuoto, alla prima voce dell'elenco prefissi viene assegnato il numero 5 e alle voci successive vengono assegnati gli incrementi di 5.
  - *Definito dall'utente*: inserire il nuovo prefisso IPV6 nella posizione specificata dal parametro. Se esiste già una voce numerata, questa viene sostituita da quella nuova.
- **Tipo di regola**: immettere la regola per l'elenco prefissi:
  - *Consenti*: consente le reti che soddisfano la condizione.
  - *Nega*: nega le reti che soddisfano la condizione.
  - *Descrizione*: testo.
- **Prefisso IPv6**: prefisso percorso IP.
- **Lunghezza prefisso**: lunghezza prefisso del percorso IP.

- **Maggiore di**: lunghezza minima del prefisso da utilizzare per la corrispondenza. Selezionare una delle seguenti opzioni:
  - *Nessun limite*: nessuna lunghezza minima del prefisso da utilizzare per la corrispondenza.
  - *Definito dall'utente*: lunghezza minima del prefisso da soddisfare.
- **Minore di**: lunghezza massima del prefisso da utilizzare per la corrispondenza. Selezionare una delle seguenti opzioni:
  - *Nessun limite*: nessuna lunghezza massima del prefisso da utilizzare per la corrispondenza.
  - *Definito dall'utente*: lunghezza massima del prefisso da soddisfare.
- **Descrizione**: immettere una descrizione dell'elenco prefissi.

PASSAGGIO 4 Fare clic su **Applica** per salvare la configurazione nel file di configurazione esecuzione.

Visualizzazione delle tabelle Percorso IPv6

La tabella di inoltro IPv6 contiene i vari percorsi configurati. Uno di questi è un percorso predefinito (indirizzo IPv6 ::0) che usa il percorso predefinito selezionato dall'Elenco router predefiniti IPv6 per inviare pacchetti ai dispositivi di destinazione che non si trovano nella stessa subnet IPv6 del dispositivo. Oltre al percorso predefinito, la tabella include anche i percorsi dinamici che consistono in reindirizzamenti ICMP ricevuti dai router IPv6 tramite i messaggi di reindirizzamento ICMP. Questo si può verificare quando il router predefinito utilizzato dal dispositivo non corrisponde al router al quale intende comunicare il traffico delle sottoreti IPv6.

Per visualizzare i router IPv6 o aggiungere manualmente un percorso, attenersi alla seguente procedura:

Per visualizzare le voci di routing IPv6 nella modalità di sistema Livello 2, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Amministrazione > Interfaccia di gestione > Percorsi IPv6**.

oppure

Per visualizzare le voci di routing IPv6 nella modalità di sistema Livello 3, attenersi alla seguente procedura: Fare clic su **Configurazione IP** > **Interfacce e gestione IPv6** > **Percorsi IPv6**.

In questa pagina vengono visualizzati i seguenti campi:

- **Prefisso IPv6**: prefisso del percorso IP relativo all'indirizzo di destinazione della subnet IPv6.
- **Lunghezza prefisso**: lunghezza del prefisso del percorso IP relativo all'indirizzo di destinazione della subnet IPv6. Esso è preceduto da una barra in avanti.
- **Interfaccia**: interfaccia utilizzata per il reindirizzamento dei pacchetti.
- **Passaggio successivo**: indirizzo a cui viene reindirizzato il pacchetto. Generalmente, corrisponde all'indirizzo di un router adiacente Può essere di uno dei seguenti tipi:
  - *Collegamento locale*: un'interfaccia e un indirizzo IPv6 che identificano in modo univoco gli host in un singolo collegamento di rete. L'indirizzo locale di un collegamento presenta un prefisso **FE80**, non è reindirizzabile e può essere utilizzato solo per le comunicazioni sulle rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
  - *Globale*: un indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
  - *Point-to-Point*: un tunnel Point-to-point.
- **Metrico**: valore utilizzato per confrontare questo percorso con altri che presentano nella tabella dei router IPv6 la stessa destinazione. Tutti i percorsi predefiniti presentano lo stesso valore.
- **Durata**: periodo entro il quale è possibile inviare il pacchetto e reinviarlo prima che venga eliminato.
- **Tipo di routing**: indica il modo in cui la destinazione è collegata e il metodo usato per ottenere la query. I valori sono i seguenti:
  - *Locale*: una rete a connessione diretta il cui prefisso è ricavato da un indirizzo IPv6 del dispositivo configurato manualmente.
  - *Dinamico*: la destinazione è indirettamente collegata (remoto) all'indirizzo della subnet IPv6. La voce è stata determinata dinamicamente tramite il protocollo ND o ICMP.
  - *Statico*: la voce è stata configurata manualmente da un utente.

Inoltro DHCPv6

L'inoltro DHCPv6 è utilizzato per l'inoltro dei messaggi DHCPv6 ai server DHCPv6. È definito in RFC 3315.

Quando il client DHCPv6 non è direttamente collegato al server DHCPv6, un agente di inoltro DHCPv6 (il dispositivo) a cui il client DHCPv6 è direttamente collegato incapsula i messaggi ricevuti dal client DHCPv6 direttamente collegato e li inoltra al server DHCPv6.

In direzione opposta, l'agente di inoltro decapsula i pacchetti ricevuti dal server DHCPv6 e li inoltra al client DHCPv6.

L'utente deve configurare l'elenco di server DHCP a cui vengono inoltrati i pacchetti. È possibile configurare due serie di server DHCPv6:

- **Destinazioni globali**: i pacchetti vengono sempre inoltrati a questi server DHCPv6.
- **Elenco interfacce**: elenco per interfaccia dei server DHCPv6. I pacchetti DHCPv6 ricevuti su un'interfaccia vengono inoltrati sia ai server sull'elenco delle interfacce (se esistente) che ai server sull'elenco di destinazioni globali.

Dipendenze con altre funzioni

Le funzioni client e di inoltro DHCPv6 si escludono a vicenda su un'interfaccia.

Destinazioni globali

Per configurare un elenco di server DHCPv6 a cui vengono inoltrati tutti i pacchetti DHCPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP > Interfacce e gestione IPv6 > Inoltro DHCPv6 > Destinazioni globali**.

PASSAGGIO 2 Per aggiungere un server DHCPv6 predefinito, fare clic su **Aggiungi**.

PASSAGGIO 3 Completare i seguenti campi:

- **Tipo di indirizzo IPv6**: immettere il tipo di indirizzo di destinazione a cui inoltrare i messaggi client. Il tipo di indirizzo può essere **Collegamento locale**, **Globale** o **Multicast** (All_DHCP_Relay_Agents_and_Servers).
- **Indirizzo IP del server DHCPv6**: immettere l'indirizzo del server DHCPv6 a cui inoltrare i pacchetti.

- **Interfaccia IPv6 di destinazione**: immettere l'interfaccia sulla quale vengono trasmessi i pacchetti quando il tipo di indirizzo del server DHCPv6 è **Collegamento locale** o **Multicast**.

PASSAGGIO 4 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Impostazioni interfaccia

Utilizzare la pagina Impostazioni interfaccia per attivare la funzionalità Inoltro DHCPv6 su un'interfaccia e per configurare un elenco di server DHCPv6 a cui inoltrare i pacchetti DHCPv6 quando vengono ricevuti sull'interfaccia.

PASSAGGIO 1 Fare clic su **Configurazione IP > Interfacce e gestione IPv6 > Inoltro DHCPv6 > Impostazioni interfaccia**.

PASSAGGIO 2 Per attivare DHCPv6 su un'interfaccia e, facoltativamente, aggiungere un server DHCPv6 per un'interfaccia, fare clic su **Aggiungi**.

Completare i seguenti campi:

- **Interfaccia di origine**: selezionare l'interfaccia (porta, LAG, VLAN o tunnel) per la quale è attivato l'Inoltro DHCPv6.
- **Usa solo destinazioni globali**: selezionare questa opzione per inoltrare i pacchetti soltanto ai server di destinazione globali DHCPv6.
- **Tipo di indirizzo IPv6**: immettere il tipo di indirizzo di destinazione a cui inoltrare i messaggi client. Il tipo di indirizzo può essere **Collegamento locale**, **Globale** o **Multicast** (All_DHCP_Relay_Agents_and_Servers).
- **Indirizzo IP del server DHCPv6**: immettere l'indirizzo del server DHCPv6 a cui inoltrare i pacchetti.
- **Interfaccia IPv6**: immettere l'interfaccia sulla quale vengono trasmessi i pacchetti quando il tipo di indirizzo del server DHCPv6 è **Collegamento locale** o **Multicast**.

PASSAGGIO 3 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Nome di dominio

Il DNS (Domain Name System) consente di convertire i nomi di dominio in indirizzi IP per poterli localizzare e indirizzare.

In quanto client DNS, il dispositivo converte i nomi di dominio in indirizzi IP tramite l'uso di uno o più server DNS configurati.

Impostazioni DNS

Utilizzare la pagina Impostazioni DNS per attivare la funzione DNS, configurare i server DNS e impostare il dominio predefinito utilizzato dal dispositivo.

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Nome dominio** > **Impostazioni DNS**.

PASSAGGIO 2 Immettere i parametri.

- **DNS**: scegliere di impostare il dispositivo come client DNS in grado di convertire i nomi DNS in indirizzi IP tramite uno o più server DNS configurati.
- **Tentativi di polling**: immettere il numero di volte in cui inviare una query DNS a un server DNS prima che il dispositivo decida che il server DNS non esiste.
- **Timeout di polling**: immettere il numero di secondi durante i quali il dispositivo attenderà una risposta a una query DNS.
- **Intervallo di polling**: immettere la frequenza (in secondi) con la quale il dispositivo invia pacchetti di interrogazione DNS dopo aver esaurito il numero di tentativi.
  - *Usa predefinito*: consente di utilizzare il valore predefinito.

    Questo valore = 2*(Tentativi polling + 1)* Timeout polling
  - *Definito dall'utente*: selezionare questa opzione per immettere un valore definito dall'utente.
- **Parametri predefiniti**: immettere i seguenti parametri predefiniti:
  - **Nome dominio predefinito**: immettere il nome di dominio DNS utilizzato per completare nomi host non qualificati. Il dispositivo lo aggiunge a tutti i nomi di dominio non completamente qualificati (NFQDN), trasformandoli in FQDN.

    NOTA Non includere il punto iniziale che separa il nome non qualificato dal nome di dominio (come cisco.com).

- **Elenco di ricerca dominio DHCP**: fare clic su **Dettagli** per visualizzare l'elenco di server DNS configurati sul dispositivo.

PASSAGGIO 3 Fare clic su **Applica.** Il file Configurazione di esecuzione viene aggiornato.

Tabella Server DNS: per ogni server DNS vengono visualizzati i campi seguenti:

- **Server DNS**: l'indirizzo IP del server DNS.
- **Preferenza**: ciascun server ha un valore di preferenza; un valore basso indica una maggiore possibilità di essere utilizzato.
- **Origine**: origine dell'indirizzo IP del server (statico o DHCPv4 oppure DHCPv6).
- **Interfaccia**: interfaccia dell'indirizzo IP del server.

PASSAGGIO 4 È possibile definire un massimo di otto server DNS. Per aggiungere un server DNS fare clic su **Aggiungi.**

Immettere i parametri.

- **Versione IP**: selezionare Versione 6 per IPv6 o Versione 4 per IPv4.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se IPv6 viene utilizzato). Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. L'indirizzo locale di un collegamento presenta un prefisso **FE80**, non è reindirizzabile e può essere utilizzato solo per le comunicazioni sulle rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: se il tipo di indirizzo IPv6 è Collegamento locale, selezionare l'interfaccia attraverso la quale viene ricevuto.
- **Indirizzo IP server DNS**: immettere l'indirizzo IP del server DNS.
- **Preferenza**: selezionare un valore che determina l'ordine di utilizzo dei domini (dal basso all'alto). Ciò determina in maniera efficace l'ordine in cui i nomi non qualificati vengono completati durante le query DNS.

PASSAGGIO 5 Fare clic su **Applica**. Il server DNS viene salvato nel file di configurazione esecuzione.

Elenco di ricerca

L'elenco di ricerca può contenere una voce statica definita dall'utente nella pagina Impostazioni DNS e voci dinamiche ricevute dai server DHCPv4 e DHCPv6.

Per visualizzare i nomi di dominio che sono stati configurati sul dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Nome dominio** > **Elenco di ricerca**.

Per ogni server DNS configurato sul dispositivo vengono visualizzati i campi seguenti.

- **Nome dominio**: nome di dominio che è possibile utilizzare sul dispositivo.
- **Origine**: origine dell'indirizzo IP del server (statico o DHCPv4 oppure DHCPv6) per questo dominio.
- **Interfaccia**: interfaccia dell'indirizzo IP del server per questo dominio.
- **Preferenza**: l'ordine di utilizzo dei domini (dal basso all'alto). Ciò determina in maniera efficace l'ordine in cui i nomi non qualificati vengono completati durante le query DNS.

Associazione host

Le associazioni nome host/indirizzo IP sono memorizzate nella Tabella Associazione host (cache DNS).

Questa cache può contenere i seguenti tipi di voci:

- **Voci statiche**: coppie di associazioni aggiunte manualmente alla cache. È possibile immettere fino a un massimo di 64 voci statiche.
- **Voci dinamiche**: coppie di associazioni aggiunte al sistema poiché utilizzate dall'utente o immesse per ciascun indirizzo IP configurato sul dispositivo da DHCP. È possibile inserire 256 voci dinamiche.

La risoluzione dei nomi inizia sempre con la verifica delle voci statiche, prosegue con il controllo delle voci dinamiche e termina inviando richieste al server DNS esterno.

Sono supportati otto indirizzi IP per nome host server DNS.

Per aggiungere un nome host e il relativo indirizzo IP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Domain Name System** > **Associazione host**.

PASSAGGIO 2 Se richiesto, è possibile selezionare l'opzione **Cancella tabella** per cancellare alcune o tutte le voci nella Tabella Associazione host.

- **Solo statico**: elimina gli host statici.
- **Solo dinamico**: elimina gli host dinamici.
- **Dinamici e statici**: elimina gli host statici e dinamici.

Nella Tabella Associazione host vengono visualizzati i seguenti campi:

- **Nome host**: nome host definito dall'utente o completo.
- **Indirizzo IP**: l'indirizzo IP dell'host.
- **Versione IP**: selezionare la versione IP dell'indirizzo IP host:
- **Tipo**: indica se la voce aggiunta alla cache è **Dinamica** o **Statica**.
- **Stato**: visualizza i risultati dei tentativi di accedere all'host.
  - *OK*: tentativo riuscito.
  - *Cache negativa*: tentativo fallito, non riprovare.
  - *Nessuna risposta*: nessuna risposta ricevuta, ma il sistema può riprovare in futuro.
- **TTL**: intervallo di tempo durante il quale le voci dinamiche rimangono nella cache.
- **TTL restante**: l'intervallo di tempo di permanenza delle voci dinamiche nella cache.

PASSAGGIO 3 Per aggiungere un'associazione host fare clic su **Aggiungi**.

PASSAGGIO 4 Immettere i parametri.

- **Versione IP**: selezionare **Versione 6** per IPv6 o **Versione 4** per IPv4.

- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se IPv6 viene utilizzato). Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. L'indirizzo locale di un collegamento presenta un prefisso **FE80**, non è reindirizzabile e può essere utilizzato solo per le comunicazioni sulle rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: se il tipo di indirizzo IPv6 è Collegamento locale, selezionare l'interfaccia attraverso la quale viene ricevuto.
- **Nome host**: immettere un nome host definito dall'utente o completo. I nomi host sono limitati alle lettere ASCII dalla A alla Z (senza distinzione tra maiuscole e minuscole), alle cifre da 0 a 9, al carattere di sottolineatura e al trattino. Per separare le etichette, utilizzare il punto (.).
- **Indirizzi IP**: immettere un indirizzo oppure un massimo di otto indirizzi IP associati (IPv4 o IPv6).

È possibile selezionare l'opzione **Cancella tabella** per cancellare alcune o tutte le voci nella Tabella Associazione host.

- **Solo statico**: elimina gli host statici.
- **Solo dinamico**: elimina gli host dinamici.
- **Dinamici e statici**: elimina gli host statici e dinamici.

19

Configurazione IP: RIPv2

In questa sezione viene descritta la funzione RIP (Routing Information Protocol) versione 2.

Vengono trattati i seguenti argomenti:

- **Panoramica**
- **Funzionamento del protocollo RIP sul dispositivo**
- **Configurazione del RIP**

NOTA Il protocollo RIP è supportato nei seguenti dispositivi:

- SG500X/SG500XG in modalità stack indipendente.
- SG500X/SG500XG in modalità stack ibrido avanzata nel livello 3.

Panoramica

Il protocollo RIP è l'implementazione di un protocollo di vettore di distanza per reti LAN e WAN che classifica i router come *attivi* o *passivi* (silenzioso). I router attivi dichiarano i propri percorsi agli altri, mentre quelli passivi ascoltano e aggiornano i propri percorsi sulla base delle dichiarazioni altrui, senza però dichiarare nulla. In genere, i router eseguono il RIP in modalità attiva, mentre gli host utilizzano la modalità passiva.

Il gateway predefinito è un percorso statico e, se attivato dalla configurazione, viene dichiarato dal RIP come tutti gli altri router statici.

Quando il routing IP viene attivato, il RIP funziona perfettamente. Quando il routing IP è disattivato, il RIP funziona in modalità passiva, vale a dire che apprende i percorsi dai messaggi RIP ricevuti e non li invia.

NOTA Il controllo del routing IP è disponibile solo per i modelli SG500X/ESW2-550X. Per attivare il routing IP, accedere alla pagina **Configurazione > Interfacce di gestione e IP > Interfaccia IPv4**.

Il dispositivo supporta la versione 2 di RIP, che si basa sui seguenti standard:

- RFC2453 Versione 2 del RIP, novembre 1998
- RFC2082 Autenticazione MD RIP-2, gennaio 1997
- RFC1724 Estensione MIB versione 2 del RIP

I pacchetti RIPv1 ricevuti vengono eliminati.

Funzionamento del protocollo RIP sul dispositivo

Nella sezione seguente viene descritto come attivare il protocollo RIP e vengono presentate altre funzioni, come la configurazione della differenza, la modalità passiva, l'autenticazione, i contatori statistici e i database paritetici.

Attivazione del RIP

Attivazione del RIP

- Il RIP deve essere attivato per interfaccia e a livello globale.
- Il RIP è configurabile solo previa attivazione.
- Se il RIP viene disattivato a livello globale, la configurazione RIP sul sistema viene rimossa.
- Se il RIP viene disattivato su un'interfaccia, la configurazione RIP viene rimossa dall'interfaccia specificata.
- Se il routing IP viene disattivato, i messaggi RIP non vengono inviati, ma quelli ricevuti vengono utilizzati per aggiornare le informazioni della tabella di routing.

NOTA È possibile definire il RIP solo su interfacce IP configurate manualmente; questo significa che il RIP non può essere definito su un'interfaccia che dispone di un indirizzo IP predefinito o il cui indirizzo IP ricevuto è stato inviato da un server DHCP.

Configurazione offset

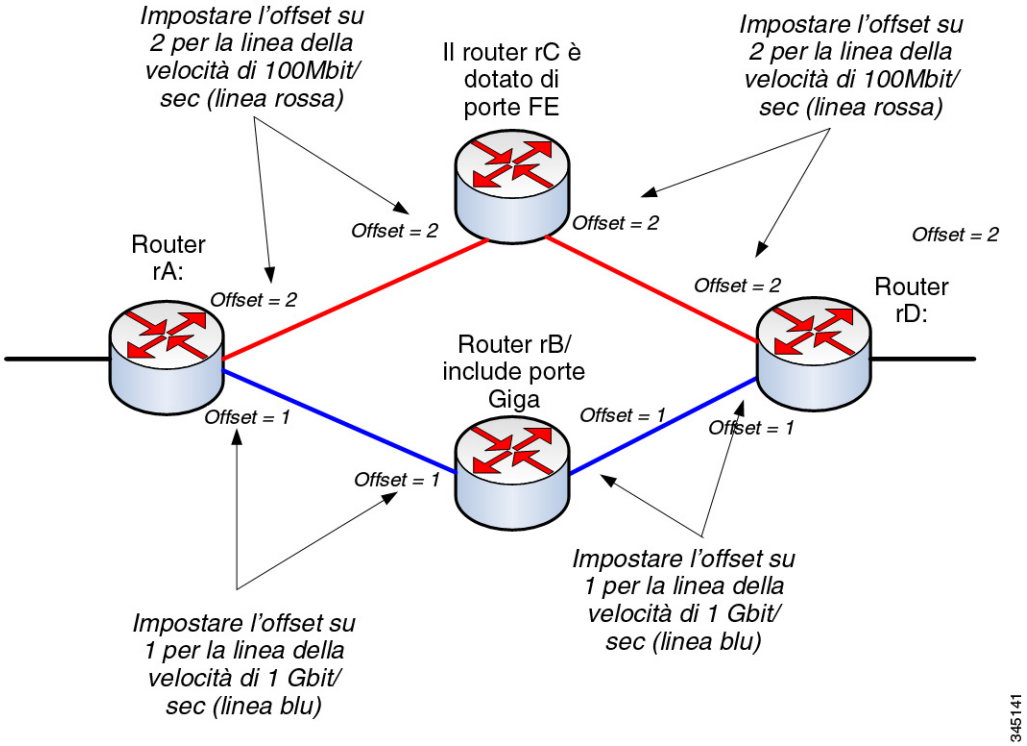
Un messaggio RIP include una metrica (numero di hop) per ciascun percorso.

Un offset è un numero supplementare che viene aggiunto alla metrica per influire sul costo dei percorsi. L'offset viene impostato per interfaccia ed è in grado di indicare la velocità, il ritardo e altre qualità di quella determinata interfaccia. In questo modo, il costo relativo delle interfacce può essere regolato secondo necessità.

È necessario impostare l'offset per ciascuna interfaccia (1 per impostazione predefinita).

Di seguito viene illustrata la configurazione dell'offset per le varie interfacce in base alla velocità della porta.

Configurazione dell'offset (in base alla velocità della porta)



Il router rD può inviare dati a rA tramite rB o rC. Poiché rC supporta solo le porte Fast Ethernet (FE) mentre rB supporta le porte Gigabit Ethernet (GE), il costo del percorso dal router rD al router rA è maggiore se effettuato tramite il router rC (un'aggiunta di 4 al costo del percorso) al contrario di quanto avviene per il

percorso tramite il router rB (un'aggiunta di 2 al costo del percorso). Di conseguenza, è preferibile eseguire l'inoltro del traffico tramite il routing rB. Per fare ciò, configurare un offset (valore di metrica) diverso per ogni interfaccia in base alla sua velocità di linea.

Per ulteriori informazioni, vedere la sezione **Configurazione offset**.

Modalità passiva

È possibile disattivare la trasmissione dei messaggi di aggiornamento del routing su una determinata interfaccia IP. In questo caso, il router è passivo e riceve sull'interfaccia solo le informazioni RIP aggiornate. Per impostazione predefinita, la trasmissione degli aggiornamenti di routing su un'interfaccia IP è attiva.

Per ulteriori informazioni, vedere la sezione **Impostazioni RIPv2 su interfaccia IP**.

Applicazione del filtro agli aggiornamenti di routing

È possibile applicare il filtro ai percorsi in entrata e in uscita di una determinata interfaccia IP utilizzando due elenchi di accesso standard: uno per quelli in entrata e uno per quelli in uscita.

L'elenco di accesso standard è un elenco con nome e ordinato di coppie di prefissi IP (indirizzo IP e lunghezza maschera IP) e azioni. L'azione può essere negata o consentita.

Se si definisce un elenco di accesso, ogni percorso dal messaggio RIP viene confrontato con l'elenco a partire dalla prima coppia: se esiste una corrispondenza con la prima coppia e l'azione è consentita, il percorso viene trasmesso; se invece l'azione viene negata, il percorso non viene trasmesso. Se il percorso non corrisponde, si passa alla coppia successiva.

Se il percorso non trova corrispondenza con nessuna delle coppie, l'azione viene negata.

Dichiarazione delle voci di percorso predefinito su interfacce IP

L'indirizzo speciale 0.0.0.0 viene utilizzato per descrivere un percorso predefinito. Si utilizza un percorso predefinito per evitare di elencare tutte le reti possibili negli aggiornamenti di routing, quando uno o più router strettamente collegati nel sistema sono pronti a trasferire il traffico sulle reti non espressamente elencate. Questi router generano voci RIP per l'indirizzo 0.0.0.0, proprio come se ci fosse una rete a cui sono connessi.

È possibile attivare la dichiarazione di un percorso predefinito e configurarla con una determinata metrica.

Funzione di ridistribuzione

Sono disponibili i seguenti tipi di percorso, che possono essere distribuiti dai RIP:

- **Connesso**: i percorsi RIP che corrispondono a interfacce IP definite sulle quali non è attivato il RIP (definito localmente). La tabella di routing RIP include, per impostazione predefinita, solo i percorsi che corrispondono alle interfacce IP sulle quali è attivato il RIP.
- **Statico**: percorsi (remoti) definiti manualmente.

È possibile stabilire se il RIP deve distribuire i percorsi statici o connessi impostando rispettivamente la funzione **Ridistribuisci percorso statico** o **Ridistribuisci percorso connesso**.

Queste funzioni sono disattivate per impostazione predefinita, ma possono essere attivate a livello globale.

Se queste funzioni sono attivate, i percorsi rifiutati vengono annunciati dai percorsi con metrica 16.

Le configurazioni di un percorso possono essere distribuite tramite una delle seguenti opzioni:

- **Metrica predefinita**

  Consente al RIP di utilizzare un valore di metrica predefinito per la configurazione distribuita dei percorsi.

- **Trasparente** (opzione predefinita)

  Consente al RIP di utilizzare la metrica della tabella di routing come metrica RIP per la configurazione distribuita dei percorsi.

  Ne consegue il comportamento seguente:

  - Se il valore di metrica di un percorso è minore o uguale a 15, il valore viene utilizzato nel protocollo RIP quando si annuncia il percorso.
  - Se il valore di metrica di un percorso statico è maggiore di 15, il percorso non viene annunciato agli altri router tramite RIP.

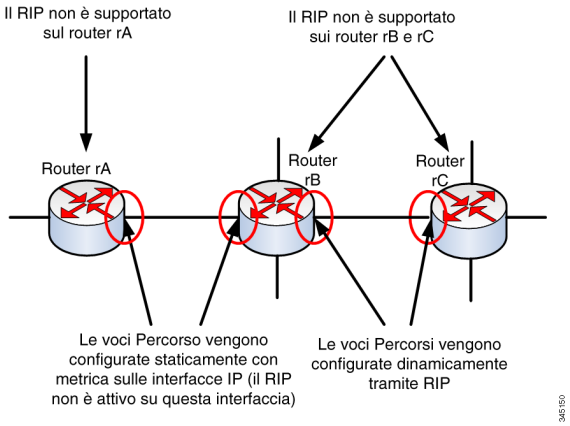
- **Metrica definita dall'utente**

  Fa in modo che il RIP utilizzi il valore di metrica immesso dall'utente.

Utilizzo del RIP in una rete con dispositivi senza RIP

Quando si utilizza la funzione RIP è opportuno tenere conto della configurazione del percorso statico e delle interfacce connesse. Ciò viene descritto nella seguente figura, in cui viene rappresentata una rete con alcuni router che supportano il protocollo RIP e altri che non lo supportano.

Una rete con router RIP e router senza RIP



Il router rA non supporta il protocollo RIP. Di conseguenza, le voci di routing con una metrica adeguata vengono configurate in modo statico su questo router. Sul router rB, invece, il percorso al router rA è considerato un percorso connesso. Al contrario, i router rB e rC acquisiscono e distribuiscono le voci di routing tramite protocollo RIP.

La configurazione del percorso connesso del router rB può essere distribuita al router rC mediante la metrica predefinita o il sistema trasparente. Un percorso statico/connesso viene *ridistribuito* con la metrica del percorso (metrica trasparente) o con la metrica definita dal comando di metrica predefinita.

Per ulteriori informazioni, vedere la sezione **Funzione di ridistribuzione**.

Autenticazione RIP

È possibile disattivare l'autenticazione dei messaggi RIP tramite l'interfaccia IP oppure attivare uno dei seguenti tipi di autenticazione:

- **Testo normale o password**: utilizza una password (stringa) che viene inviata insieme al percorso a un altro router. Il router ricevente confronta questa chiave con quella configurata. Se sono uguali, il percorso viene accettato.

- **MD5**: utilizza l'autenticazione digest MD5. Ciascun router viene configurato con un set di chiavi segrete. Questo set viene denominato **keychain**. Ogni keychain è composto da una o più chiavi. Ogni chiave ha un numero di identificazione (**identificatore di chiavi**), una **stringa di chiavi** ed eventualmente un valore di **send-lifetime** e di **accept-lifetime**. Il send-lifetime indica il lasso di tempo durante il quale la chiave di autenticazione di un keychain viene considerata valida per l'invio; l'accept-lifetime rappresenta invece il periodo di tempo in cui la chiave di autenticazione di un keychain che viene ricevuta è considerata valida.

  Tutti i messaggi RIP trasmessi includono il digest MD5 calcolato del messaggio (contenente il keychain), oltre all'identificatore di chiavi della stringa di chiavi utilizzata. Il ricevitore ha configurato al suo interno anche il keychain. L'identificatore di chiavi è utilizzato dal ricevitore per selezionare la chiave per la convalida del digest MD5.

Contatori statistici RIP

È possibile monitorare le operazioni RIP esaminando i contatori statistici per interfaccia IP. Per una descrizione di questi contatori, vedere **Visualizzazione dei contatori statistici RIPv2**.

Database paritetici RIP

È possibile monitorare il database paritetico RIP per interfaccia IP. Per una descrizione di questi contatori, vedere **Visualizzazione del database paritetico RIP**.

Configurazione del RIP

È possibile eseguire le operazioni indicate di seguito.

- Operazioni obbligatorie:
  - Attivare/disattivare il protocollo RIP a livello globale nella pagina Proprietà RIPv2.
  - Attivare/disattivare il protocollo RIP su un'interfaccia IP nella pagina Impostazioni RIPv2.

- Operazioni opzionali (se non vengono eseguite, il sistema imposta i valori predefiniti)
  - Attivare/disattivare il protocollo RIP per annunciare i percorsi statici o connessi e la relativa metrica su un'interfaccia IP nella pagina Proprietà RIPv2.
  - Configurare l'offset aggiunto alla metrica per i percorsi in entrata su un'interfaccia IP nella pagina Impostazioni RIPv2.
  - Attivare la modalità passiva su un'interfaccia IP nella pagina Impostazioni RIPv2.
  - Controllare quali percorsi vengono elaborati negli aggiornamenti di routing in entrata e in uscita specificando un elenco di indirizzo IP sull'interfaccia IP (vedere **Elenchi di accesso**).
  - Dichiarare le voci di percorso predefinite sull'interfaccia IP nella pagina Impostazioni RIPv2.
  - Attivare l'autenticazione RIP su un'interfaccia IP nella pagina Impostazioni RIPv2.

Proprietà RIPv2

Per attivare/disattivare il RIP sul dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Configurazione IP**> **RIPv2 > Proprietà RIPv2**.

PASSAGGIO 2 Selezionare le seguenti opzioni come richiesto:

- **RIP**: sono disponibili le opzioni riportate di seguito.
  - *Attiva*: consente di attivare il RIP.
  - *Disattiva*: consente di disattivare il RIP. Se il RIP viene disattivato, la configurazione RIP sul sistema viene rimossa.
  - *Arresta*: consente di eseguire l'arresto globale del RIP.
- **Annuncio RIP**: selezionare questa opzione per attivare l'invio di aggiornamenti di routing su tutte le interfacce IP RIP.
- **Annuncio percorso predefinito**: selezionare questa opzione per attivare l'invio del percorso predefinito al dominio RIP. Questo percorso funge da router predefinito.

- **Metrica predefinita**: immettere il valore della metrica predefinita (fare riferimento a **Funzione di ridistribuzione**).

PASSAGGIO 3 **Ridistribuisci percorso statico**: selezionare questa opzione per attivare la funzione corrispondente (descritta in **Funzione di ridistribuzione**).

PASSAGGIO 4 Se l'opzione **Ridistribuisci percorso statico** è attiva, selezionare un'opzione per il campo **Ridistribuisci metrica statica**. Sono disponibili le seguenti opzioni:

- **Metrica predefinita**: consente al RIP di utilizzare un valore di metrica predefinito per la configurazione distribuita di percorsi statici (consultare **Funzione di ridistribuzione**).
- **Trasparente**: consente al RIP di utilizzare la metrica della tabella di routing come metrica RIP per la configurazione distribuita di percorsi statici. Ne consegue il comportamento seguente:
  - Se il valore di metrica di un percorso statico è minore o uguale a 15, il valore viene utilizzato nel protocollo RIP quando si annuncia il percorso statico.
  - Se il valore di metrica di un percorso statico è maggiore di 15, il percorso statico non viene annunciato agli altri router tramite RIP.
- **Metrica definita dall'utente**: immettere il valore della metrica.

PASSAGGIO 5 **Ridistribuisci percorso connesso**: selezionare questa opzione per attivare la funzione corrispondente (descritta in Ridistribuzione della configurazione di un percorso statico).

PASSAGGIO 6 Se l'opzione **Ridistribuisci percorso connesso** è attiva, selezionare un'opzione per il campo **Ridistribuisci metrica statica**. Sono disponibili le seguenti opzioni:

- **Metrica predefinita**: consente al RIP di utilizzare un valore di metrica predefinito per la configurazione distribuita di percorsi statici (consultare **Funzione di ridistribuzione**).
- **Trasparente**: consente al RIP di utilizzare la metrica della tabella di routing come metrica RIP per la configurazione distribuita di percorsi statici. Ne consegue il comportamento seguente:
  - Se il valore di metrica di un percorso statico è minore o uguale a 15, il valore viene utilizzato nel protocollo RIP quando si annuncia il percorso statico.
  - Se il valore di metrica di un percorso statico è maggiore di 15, il percorso statico non viene annunciato agli altri router tramite RIP.
- **Metrica definita dall'utente**: immettere il valore della metrica.

PASSAGGIO 7 Fare clic su **Applica**. Le impostazioni vengono scritte nel file Configurazione di esecuzione.

Impostazioni RIPv2 su interfaccia IP

Per configurare il protocollo RIP su un'interfaccia IP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Configurazione IP** > **RIPv2 > Impostazioni RIPv2**.

PASSAGGIO 2 I parametri RIP vengono visualizzati per interfaccia IP.

Per aggiungere una nuova interfaccia IP, fare clic su **Aggiungi** per aprire la pagina Aggiungi impostazioni RIPv2 e compilare i seguenti campi:

- **Indirizzo IP**: selezionare un'interfaccia IP definita su un'interfaccia di Livello 2.
- **Arresta**: selezionare questa opzione per attivare il RIP sull'interfaccia anche nello stato di arresto.
- **Passivo**: questa opzione specifica se inviare i messaggi di aggiornamento del percorso RIP su una determinata interfaccia IP. Se questo campo non è attivo, gli aggiornamenti RIP non vengono inviati (passivo).
- **Offset**: specifica il numero della metrica di una determinata interfaccia IP. Ciò rispecchia il costo aggiuntivo dell'utilizzo dell'interfaccia, basato sulla velocità dell'interfaccia stessa.
- **Annuncio percorso predefinito**: questa opzione è definita a livello globale nella pagina **Proprietà RIPv2**. È possibile utilizzare la definizione globale oppure definire questo campo per l'interfaccia specifica. Sono disponibili le seguenti opzioni:
  - *Globale*: usare le impostazioni globali definite nella schermata **Proprietà RIPv2**.
  - *Disattiva*: il percorso predefinito non viene dichiarato su questa interfaccia RIP.
  - *Attiva*: il percorso predefinito viene dichiarato su questa interfaccia RIP.
- **Metrica annuncio percorso predefinito**: immettere la metrica del percorso predefinito per questa interfaccia.

- **Modalità di autenticazione**: stato di autenticazione del RIP (attivo/inattivo) su una determinata interfaccia IP. Sono disponibili le seguenti opzioni:
  - *Nessuna*: non è stata eseguita alcuna autenticazione.
  - *Testo*: la password chiave inserita di seguito viene utilizzata per l'autenticazione.
  - *MD5*: il digest MD5 del keychain selezionato di seguito viene utilizzato per l'autenticazione.
- **Password chiave**: se l'opzione **Testo** è stata selezionata come tipo di autenticazione, inserire la password da utilizzare.
- **Keychain**: se come modalità di autenticazione è stata selezionata l'opzione **MD5**, inserire il keychain da utilizzare. Questo keychain viene creato nel modo descritto nella sezione **Gestione delle chiavi**.
- **Elenco di distribuzione in ingresso**: selezionare questa opzione per configurare il filtro sui percorsi RIP in ingresso per l'indirizzo o gli indirizzi IP specificati nel nome dell'elenco di accesso. Se questo campo è attivo, selezionare il nome dell'elenco di accesso di seguito:
- **Nome elenco di accesso**: selezionare il nome dell'elenco di accesso (che include un elenco di indirizzi IP) dei percorsi RIP in ingresso che applica un filtro per una determinata interfaccia IP. Per una descrizione degli elenchi di accesso, vedere **Creazione di un elenco di accesso**.
- **Elenco di distribuzione in uscita**: selezionare questa opzione per configurare il filtro sui percorsi RIP in uscita per l'indirizzo o gli indirizzi IP specificati nel nome dell'elenco di accesso. Se questo campo è attivo, selezionare il nome dell'elenco di accesso di seguito:
- **Nome elenco di accesso**: selezionare il nome dell'elenco di accesso (che include un elenco di indirizzi IP) dei percorsi RIP in uscita che applica un filtro per una determinata interfaccia IP. Per una descrizione degli elenchi di accesso, vedere **Creazione di un elenco di accesso**.

PASSAGGIO 3 Fare clic su **Applica**. Le impostazioni vengono scritte nel file Configurazione di esecuzione.

Visualizzazione dei contatori statistici RIPv2

Per visualizzare i contatori statistici RIP di ciascun indirizzo IP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Configurazione IP** > **RIPv2 > Statistiche RIPv2**.

Vengono visualizzati i seguenti campi:

- **Interfaccia IP**: l'interfaccia IP definita su un'interfaccia di Livello 2.
- **Pacchetti danneggiati ricevuti**: specifica il numero di pacchetti danneggiati identificati dal RIP sull'interfaccia IP.
- **Percorsi danneggiati ricevuti**: specifica il numero di percorsi danneggiati ricevuti e identificati dal RIP sull'interfaccia IP. Un percorso danneggiato è un percorso che presenta parametri non corretti. Ad esempio, l'indirizzo IP di destinazione è un indirizzo broadcast, quindi la metrica deve essere 0 o maggiore di 16.
- **Aggiornamenti inviati**: specifica il numero di pacchetti inviati dal RIP sull'interfaccia IP.

PASSAGGIO 2 Per azzerare tutti i contatori dell'interfaccia, fare clic su **Cancella tutti i contatori interfaccia**.

Visualizzazione del database paritetico RIP

Per visualizzare il database paritetici (contigui) RIP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Configurazione IP** > **RIPv2 > Database router paritetico RIPv2**.

Per il database router paritetico vengono visualizzati i seguenti campi:

- **Indirizzo IP del router**: l'interfaccia IP definita su un'interfaccia di Livello 2.
- **Pacchetti danneggiati ricevuti**: specifica il numero di pacchetti danneggiati identificati dal RIP sull'interfaccia IP.
- **Percorsi danneggiati ricevuti**: specifica il numero di percorsi danneggiati ricevuti e identificati dal RIP sull'interfaccia IP. Un percorso danneggiato è un percorso che presenta parametri non corretti. Ad esempio, la destinazione IP di è un broadcast, oppure la metrica è uguale a 0 o maggiore di 16.

- **Ultimo aggiornamento**: indica l'ultima volta in cui il RIP ha ricevuto i percorsi RIP dall'indirizzo IP remoto.

PASSAGGIO 2 Per azzerare tutti i contatori, fare clic su **Azzera tutti i contatori interfaccia**.

Elenchi di accesso

Per una descrizione degli elenchi di accesso, vedere **Applicazione del filtro agli aggiornamenti di routing**.

Per creare gli elenchi di accesso, attenersi alla seguente procedura:

1. Creare un elenco di accesso con indirizzo IP univoco nella pagina Impostazioni dell'elenco di accesso.
2. Se necessario, aggiungere ulteriori indirizzi IP nella pagina Elenco dell'indirizzo IPv4 di origine.

Creazione di un elenco di accesso

Per impostare la configurazione globale di un elenco di accesso, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Configurazione IP** > **Elenco di accesso** > **Impostazioni elenco di accesso**.

PASSAGGIO 2 Per aggiungere un nuovo elenco di accesso, fare clic su **Aggiungi** per aprire la pagina Aggiungi elenco di accesso e compilare i seguenti campi:

- **Nome**: specificare un nome per l'elenco di accesso.
- **Indirizzo IPv4 di origine**: immettere l'indirizzo IPv4 di origine. Sono disponibili le seguenti opzioni:
  - *Tutti*: vengono inclusi tutti gli indirizzi IP.
  - *Definito dall'utente*: immettere l'indirizzo IP.
- **Maschera IPv4 di origine**: immettere il valore e il tipo di maschera dell'indirizzo IPv4 di origine. Sono disponibili le seguenti opzioni:
  - *Maschera di rete*: immettere la maschera di rete.
  - *Lunghezza prefisso*: immettere la lunghezza del prefisso.

- **Azione**: selezionare un'azione per l'elenco di accesso. Sono disponibili le seguenti opzioni:
  - *Consenti*: consente l'ingresso di pacchetti provenienti da indirizzi IP presenti nell'elenco di accesso.
  - *Rifiuta*: rifiuta l'ingresso di pacchetti provenienti da indirizzi IP presenti nell'elenco di accesso.

Compilare un elenco di accesso

Per compilare un elenco di accesso con indirizzi IP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Configurazione IP** > **Elenco di accesso** > **Elenco di accesso IPv4 di origine**.

PASSAGGIO 2 Per modificare i parametri di un elenco di accesso, fare clic su **Aggiungi** per aprire la pagina Modifica elenco di accesso e modificare i seguenti campi:

- **Nome elenco di accesso**: immettere il nome dell'elenco di accesso.
- **Indirizzo IPv4 di origine**: immettere l'indirizzo IPv4 di origine. Sono disponibili le seguenti opzioni:
  - *Tutti*: vengono inclusi tutti gli indirizzi IP.
  - *Definito dall'utente*: immettere l'indirizzo IP.
- **Maschera IPv4 di origine**: il valore e il tipo di maschera dell'indirizzo IPv4 di origine. Sono disponibili le seguenti opzioni:
  - *Maschera di rete*: immettere la maschera di rete (ad esempio 255.255.0.0).
  - *Lunghezza prefisso*: immettere la lunghezza del prefisso.
- **Azione**: l'azione per l'elenco di accesso. Sono disponibili le seguenti opzioni:
  - *Consenti*: consente l'ingresso di pacchetti provenienti da indirizzi IP presenti nell'elenco di accesso.
  - *Rifiuta*: rifiuta l'ingresso di pacchetti provenienti da indirizzi IP presenti nell'elenco di accesso.

20

Configurazione IP: VRRP

In questo capitolo viene descritto il funzionamento del protocollo VRRP (Virtual Router Redundancy Protocol, protocollo di ridondanza router virtuale), oltre alle modalità di configurazione dei router virtuali con VRRP tramite interfaccia utente Web.

NOTA I modelli SF500 non supportano la funzione VRRP.

Vengono trattati i seguenti argomenti:

- **Panoramica**
- **Elementi configurabili di VRRP**
- **Configurazione del protocollo VRRP**

Panoramica

VRRP è un protocollo di elezione e ridondanza che assegna dinamicamente la responsabilità di un router virtuale a uno dei router fisici sulla LAN. In questo modo aumentano disponibilità e affidabilità dei percorsi di routing nella rete.

Nel protocollo VRRP, un router fisico in un router virtuale viene eletto come master, con un altro router fisico dello stesso router virtuale che agisce da backup in caso di errori o guasti del master. I router fisici sono detti anche router VRRP.

Il gateway predefinito di un host partecipante viene assegnato al router virtuale piuttosto che al router fisico. Se il router fisico che inoltra i pacchetti per conto del router virtuale non funziona, viene selezionato automaticamente un altro router fisico per sostituirlo. Il router fisico che inoltra pacchetti in un dato momento è detto router master.

Il protocollo VRRP permette anche la condivisione del carico di traffico. Il traffico è condivisibile allo stesso modo tra router disponibili configurando il protocollo VRRP in modo tale che il traffico verso/dai client della LAN venga condiviso da più router.

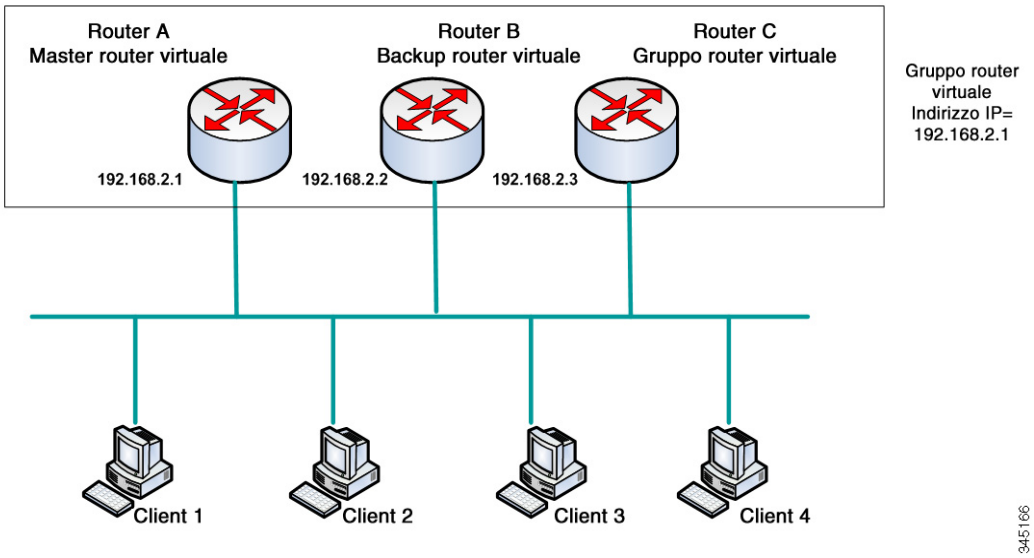
Vincoli

VRRP è supportato solo sugli switch SG500X/ESW2-550X.

Topologia VRRP

L'immagine sotto mostra una topologia LAN in cui è configurato il protocollo VRRP. In questo esempio, i router A, B e C sono VRRP e comprendono un router virtuale. L'indirizzo IP del router virtuale è lo stesso di quello configurato per l'interfaccia Ethernet del router A (198.168.2.1).

Topologia base VRRP



Dato che il router virtuale utilizza l'indirizzo IP dell'interfaccia Ethernet fisica del router A, il router A assume il ruolo di *router virtuale master* ed è anche noto come *proprietario dell'indirizzo IP*. In qualità di router virtuale master, il router A controlla l'indirizzo IP del router virtuale ed è responsabile dell'inoltro dei pacchetti per conto del router virtuale. I client da 1 a 3 sono configurati con l'indirizzo IP del gateway predefinito 198.168.2.1. Il client 4 è configurato con l'indirizzo IP del gateway predefinito 198.168.2.2.

NOTA Il router VRRP proprietario dell'indirizzo IP risponde/elabora i pacchetti aventi come destinazione l'indirizzo IP. Il router VRRP corrispondente al router virtuale master, ma non proprietario dell'indirizzo IP, non risponde/elabora tali pacchetti.

I router B e C funzionano da *backup del router virtuale*. Se il router virtuale master non funziona, il router configurato con la priorità più alta diventa il router virtuale master e fornisce servizi agli host della LAN con interruzioni minime.

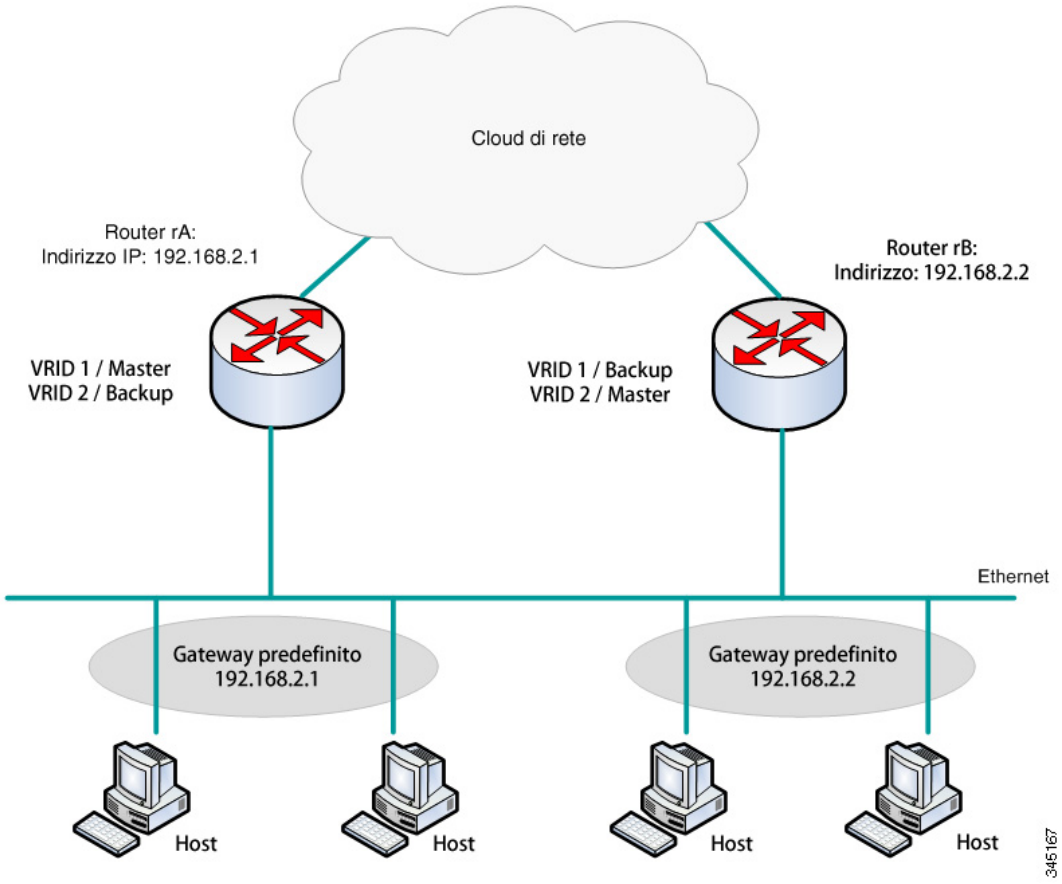
> **NOTA** La priorità del router VRRP dipende da quanto segue: se il router VRRP è il proprietario, la sua priorità è 255 (massimo), se non è proprietario, la priorità viene configurata manualmente (sempre inferiore a 255).

Una volta ripristinato, il router A torna a essere il router virtuale master. Durante il periodo in cui il master viene ripristinato, entrambi i master inoltrano pacchetti e di conseguenza sono riscontrabili duplicati (comportamento normale), ma senza interruzioni.

Per ulteriori dettagli sui ruoli svolti dai router VRRP e sugli eventi successivi al guasto di un master del router virtuale, vedere **Priorità e annullamento router VRRP**.

L'immagine sotto mostra una topologia LAN in cui è configurato il protocollo VRRP. I router A e B condividono traffico verso/dai client da 1 a 4 e i router A e B agiscono da backup del router virtuale tra di loro, nel caso in cui uno dei router si guasti.

Topologia VRRP con condivisione del carico



In questa topologia, sono configurati due router virtuali. Per il router virtuale 1, rA è il proprietario dell'indirizzo IP 192.168.2.1 ed è il master del router virtuale, mentre rB è il backup del router virtuale su rA. I client 1 e 2 sono configurati con l'indirizzo IP del gateway predefinito 192.168.2.1.

Per il router virtuale 2, rB è il proprietario dell'indirizzo IP 192.168.2.2 ed è il master del router virtuale, mentre rA è il backup del router virtuale rB. I client 3 e 4 sono configurati con l'indirizzo IP del gateway predefinito 192.168.2.2.

Elementi configurabili di VRRP

È necessario assegnare a ogni router virtuale della stessa LAN un identificatore router virtuale unico (VRID). Tutti i router VRRP che supportano lo stesso router virtuale devono essere configurati con ogni informazione relativa al router virtuale, incluso il suo VRID. I router virtuali devono essere attivi sul dispositivo solo quando anche il routing IP è attivo sul dispositivo.

L'utente può configurare un router VRRP per la partecipazione a uno o più router virtuali, sia con i comandi dell'interfaccia da linea di comando, che tramite l'interfaccia utente Web, come descritto nella sezione **Configurazione del protocollo VRRP**.

Per configurare un router virtuale, configurare le sue informazioni, quali ID router virtuale, e i suoi indirizzi IP, su ogni router VRRP che supporta il router virtuale. I seguenti elementi sono configurabili e personalizzabili.

Identificazione del router virtuale

È necessario assegnare un identificatore (VRID); se si desidera, è possibile assegnare anche una descrizione. Le seguenti sezioni descrivono i vari attributi di un router virtuale.

Il protocollo VRRP supporta fino a 255 router virtuali (gruppi VRRP).

Versioni VRRP

Il dispositivo supporta i seguenti tipi di versione VRRP:

- IPv4 VRRPv3 basato su RFC5798. I messaggi VRRPv3 vengono inviati.
- IPv4 VRRPv3 e VRRPv2 basati su RFC5798. I messaggi VRRPv3 e VRRP v2 vengono inviati.
- IPv4 VRRPv2 basato su RC3768. I messaggi VRRPv2 vengono inviati.

La configurazione della versione VRRP è per ogni router virtuale. La versione predefinita è VRRPv2.

Durante la configurazione di un router virtuale si possono verificare i seguenti casi:

- Tutti i router VRRP esistenti del router virtuale funzionano in VRRPv3. In questo caso, configurare il nuovo router VRRP in modo che funzioni in VRRPv3.
- Tutti i router VRRP esistenti del router virtuale funzionano in VRRPv2. In questo caso, configurare il nuovo router VRRP in modo che funzioni in VRRPv2.
- Esiste almeno un router VRRP del router virtuale che funziona sia in VRRPv2, che VRRPv3. In questo caso, configurare il router VRRP in modo che funzioni in VRRPv3, sebbene supporti anche VRRPv2.

  NOTA Se sono presenti router solo VRRPv2 e router solo VRRPv3 nel router virtuale, è necessario configurare almeno un router VRRPv2 e uno VRRPv3.

NOTA Se sul router VRRP sono attivati sia VRRPv2 che VRRPv3, il router VRRP trasmette pacchetti sia in formato VRRPv2, che VRRPv3. Conformemente agli standard VRRPv3, l'attivazione di entrambe le versioni VRRPv2 e VRRPv3 deve avvenire durante l'aggiornamento da v2 a v3. La combinazione delle due versioni non deve essere considerata una soluzione definitiva. Per i dettagli sull'interoperabilità di VRRPv2 e VRRPv3, vedere lo standard VRRPv3.

Indirizzi IP del router virtuale

Ad ogni router virtuale vengono assegnati uno o più indirizzi IP, per i quali il master corrente si assume la responsabilità.

Un router VRRP che supporta un router virtuale deve avere un'interfaccia IP sulla stessa sottorete IP rispetto agli indirizzi IP configurati sul router virtuale.

L'assegnazione degli indirizzi IP a un router virtuale avviene conformemente alle seguenti regole:

- Tutti i router VRRP che supportano il router virtuale devono essere configurati con gli stessi indirizzi IP presenti nella configurazione del router virtuale.
- Nessuno degli indirizzi IP è utilizzabile in un altro router virtuale o in router VRRP che non supportano il router virtuale.

- Uno dei router VRRP che supporta il router virtuale deve essere il proprietario di tutti gli indirizzi IP del router virtuale. Un router VRRP è il proprietario degli indirizzi IP, se gli indirizzi sono indirizzi reali configurati sull'interfaccia IP.
- Se un router VRRP (il router fisico) è il proprietario degli indirizzi IP del router virtuale, l'indirizzo IP del router virtuale deve essere configurato manualmente sul router VRRP e non assegnato dal DHCP.
- Se un router VRRP non è proprietario degli indirizzi IP del router virtuale:
  - I router VRRP non proprietari devono essere configurati con un'interfaccia IP sulla stessa sottorete IP degli indirizzi IP del router virtuale.
  - Le corrispondenti sottoreti IP devono essere configurate manualmente nel router VRRP e non assegnate dal DHCP.

Tutti i router VRRP che supportano lo stesso router virtuale devono avere la stessa configurazione. Se le configurazioni sono diverse, viene utilizzata quella del master. Un router VRRP di backup trasmette un syslog quando la sua configurazione è diversa da quella del master.

Indirizzo IP di origine in un router VRRP

Ogni router VRRP che supporta un router virtuale utilizza il proprio indirizzo IP come indirizzo IP di origine nei messaggi VRRP in uscita per il router virtuale. I router VRRP dello stesso router virtuale comunicano tra di loro con messaggi VRRP. Se il router VRRP è il proprietario dell'indirizzo IP del router virtuale, allora l'indirizzo IP è uno di quelli del router virtuale. Se un router VRRP non è proprietario dell'indirizzo IP del router virtuale, allora l'indirizzo IP corrisponde all'indirizzo IP dell'interfaccia del router VRRP verso la stessa sottorete IP del router virtuale.

Se l'indirizzo IP è stato configurato manualmente, la configurazione viene rimossa e reimpostato l'indirizzo IP sorgente predefinito (indirizzo IP del router VRRP minimo definito sull'interfaccia). Se l'indirizzo IP di origine era un indirizzo predefinito, viene preso un nuovo indirizzo IP di origine predefinito.

Priorità e annullamento router VRRP

Un aspetto importante dello schema di ridondanza VRRP è la capacità di assegnare a ogni router VRRP una priorità VRRP. La priorità VRRP deve esprimere l'efficienza di un router VRRP in termini di router di backup per un router virtuale definito nel router VRRP. Se sono presenti più router VRRP per il router virtuale, la priorità determina quale router VRRP di backup sarà il master, se quello attuale non funziona.

Se un router virtuale è il proprietario dell'indirizzo IP, la sua priorità VRRP viene assegnata automaticamente dal sistema con priorità 255 e il router VRRP (sul quale questo router virtuale viene assegnato) funziona automaticamente come master del router virtuale, se è attivo.

In **Figura** , se il router A, il router virtuale master non funziona, si avvia un processo di selezione per determinare se i backup del router virtuale B o C devono prendere il suo posto. Se i router B e C sono configurati con priorità di 101 e 100 rispettivamente, il router B viene eletto a master del router virtuale in quanto dotato della priorità maggiore. Se entrambi hanno la stessa priorità, viene scelto quello con valore di indirizzo IP maggiore per diventare il master del router virtuale.

Per impostazione predefinita, è attiva una funzione di annullamento che opera nel seguente modo:

- Attivata: quando un router VRRP è configurato con priorità maggiore del master corrente attivo, sostituisce il master corrente.
- Disattivata: anche se un router VRRP con priorità maggiore del master corrente è attivo, non sostituisce il master corrente. Solo il master originale (quando ridiventa disponibile) sostituisce il router di backup.

Annunci VRRP

Il master del router virtuale invia annunci VRRP ai router che si trovano nello stesso gruppo (configurati con lo stesso identificatore router virtuale).

Gli annunci VRRP sono incapsulati nei pacchetti IP e inviati all'indirizzo multicast IPv4 assegnato al gruppo VRRP. Gli annunci sono inviati ogni secondo per impostazione predefinita; l'intervallo di annuncio è configurabile.

L'intervallo di annuncio è in ms (intervallo: 50 - 40950, predefinito: 1000). Non è possibile non inserire valori.

- In VRRP versione 3, l'intervallo annuncio operativo viene arrotondato per difetto ai 10 ms più prossimi.

- In VRRP versione 2, l'intervallo annuncio operativo viene arrotondato per difetto al secondo più vicino. Il valore minimo operativo è di 1 secondo.

Configurazione del protocollo VRRP

Questa funzione può essere configurata nelle pagine seguenti.

Router virtuali

È possibile configurare e personalizzare le proprietà VRRP nella pagina *Router VRRP virtuali*.

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv4 > Router virtuali**.

PASSAGGIO 2 Per aggiungere un router virtuale, fare clic su **AGGIUNGI**.

PASSAGGIO 3 Immettere informazioni nei seguenti campi:

- **Interfaccia**: interfaccia sulla quale è definito il router virtuale.
- **Identificatore router virtuale**: numero definito dall'utente che identifica il router virtuale.
- **Descrizione**: stringa definita dall'utente che identifica il router virtuale.
- **Stato**: selezionare questa opzione per attivare il VRRP sul dispositivo.
- **Versione**: selezionare la versione di VRRP da utilizzare sul router.
- **Titolare indirizzo IP**: se è selezionata l'opzione **Sì**, l'indirizzo IP del dispositivo corrisponde all'indirizzo IP del router virtuale. Selezionare gli indirizzi IP del proprietario dall'elenco **Indirizzo IP disponibile** e spostarlo nell'elenco **Indirizzo IP del proprietario**.
- Se è selezionata l'opzione **No**, è necessario inserire gli indirizzi del router virtuale nel campo **Indirizzo IP del router virtuale**. Nel caso in cui qui vengano aggiunti più indirizzi IP, separarli nel seguente modo: 1.1.1.1, 2.2.2.2.
- **Indirizzo IP di origine**: selezionare l'indirizzo IP da utilizzare nei messaggi VRRP. L'indirizzo IP di origine predefinito è quello minore tra gli indirizzi IP definiti sull'interfaccia.

- **Priorità**: se questo dispositivo è il proprietario, nel campo viene visualizzato il valore 255, che non può essere modificato. In caso contrario, immettere la priorità del dispositivo, in base alla sua capacità di funzionare come master. 100 è la priorità predefinita per un dispositivo non proprietario.
- **Superamento priorità**: selezionare vero/falso per attivare/disattivare il superamento priorità, come descritto nella sezione **Priorità e annullamento router VRRP**.
- **Intervallo annuncio**: immettere l'intervallo di tempo, come descritto nella sezione **Annunci VRRP**.

  NOTA Se questi parametri vengono modificati (**Modifica**), il router virtuale risulta modificato e viene inviato un nuovo messaggio con nuovi parametri.

PASSAGGIO 4 Per visualizzare ulteriori informazioni su un router virtuale, fare clic su **Dettagli**.

PASSAGGIO 5 Per il router virtuale selezionato vengono visualizzati i seguenti campi:

- **Interfaccia**: l'interfaccia di livello 2 (porta, LAG o VLAN) sulla quale è definito il router virtuale.
- **Identificatore router virtuale**: il numero di identificazione del router virtuale.
- **Indirizzo MAC router virtuale**: l'indirizzo MAC virtuale del router virtuale.
- **Tabella indirizzo IP del router virtuale**: gli indirizzi IP associati a questo router virtuale.
- **Descrizione**: il nome del router virtuale.
- **Versione**: la versione del router virtuale.
- **Stato**: VRRP attivato.
- **Titolare indirizzo IP**: il titolare dell'indirizzo IP del router virtuale.
- **Stato master/backup**: è il master o il backup del router virtuale.
- **Sfasamento temporale**: tempo impiegato nel calcolo dell'intervallo di disattivazione del master.
- **Intervallo disattivazione master**: intervallo di tempo del Backup per dichiarare la disattivazione del master.
- **Superamento priorità**: superamento priorità attivato.

- **I miei parametri** del router virtuale selezionato:
  - *Priorità*: priorità del dispositivo di questo router virtuale, in base alla sua capacità di funzionare come master.
  - *Intervallo annuncio*: intervallo di tempo, come descritto nella sezione **Annunci VRRP**.
  - *Indirizzo IP di origine*: indirizzo IP da utilizzare nei messaggi VRRP.
- **Parametri master** del dispositivo master:
  - *Priorità*: 255
  - *Intervallo annuncio*: intervallo di tempo, come descritto nella sezione **Annunci VRRP**.
  - *Indirizzo IP di origine*: indirizzo IP da utilizzare nei messaggi VRRP.

Statistiche VRRP

Per visualizzare le statistiche VRRP e per azzerare i contatori dell'interfaccia:

PASSAGGIO 1 Fare clic su **Configurazione IP** > **Interfacce e gestione IPv4 > Statistiche VRRP**.

Per ogni interfaccia su cui è stato attivato VRRP vengono visualizzati i campi seguenti:

- **Interfaccia**: specificare l'interfaccia su cui VRRP viene attivato.
- **Checksum non valido**: mostra il numero di pacchetti con checksum non validi.
- **Lunghezza pacchetto non valida**: mostra il numero di pacchetti con lunghezze di pacchetto non valide.
- **TTL non valido**: mostra il numero di pacchetti con valori TTL non validi.
- **Tipo di pacchetto VRRP non valido**: mostra il numero di pacchetti con tipi di pacchetti VRRP non validi.
- **ID VRRP non valido**: mostra il numero di pacchetti con ID VRRP non validi.
- **Numero protocollo non valido**: mostra il numero di pacchetti con numeri di protocollo non validi.
- **Elenco IP non valido**: mostra il numero di pacchetti con elenchi IP non validi.
- **Intervallo non valido**: mostra il numero di pacchetti con intervalli non validi.

- **Autenticazione non valida**: mostra il numero di pacchetti la cui autenticazione non è riuscita.

PASSAGGIO 2 Selezionare un'interfaccia.

PASSAGGIO 3 Fare clic su **Azzera contatori interfaccia** per azzerare i contatori dell'interfaccia.

21

Protezione

Questa sezione descrive la sicurezza del dispositivo e il controllo degli accessi. Il sistema gestisce diversi tipi di sicurezza.

Nel seguente elenco di argomenti vengono descritti i diversi tipi di funzioni di sicurezza presenti in questa sezione. Alcune funzioni vengono utilizzate per più di un tipo di sicurezza o controllo e quindi compaiono due volte nell'elenco degli argomenti di seguito.

L'autorizzazione alla gestione del dispositivo viene descritta nelle seguenti sezioni:

- **Definizione degli utenti**
- **Configurazione del protocollo TACACS+**
- **Configurazione del RADIUS**
- **Metodo di accesso a gestione**
- **Gestione delle chiavi**
- **Gestione sicura dei dati sensibili**
- **Server SSL**

La protezione da attacchi rivolti alla CPU del dispositivo viene descritta nelle seguenti sezioni:

- **Configurazione dei servizi TCP/UDP**
- **Definizione del controllo storm**
- **Controllo di accesso**

Il controllo degli accessi degli utenti finali alla rete attraverso il dispositivo viene descritto nelle seguenti sezioni:

- **Metodo di accesso a gestione**
- **Configurazione del protocollo TACACS+**
- **Configurazione del RADIUS**

- Configurazione della sicurezza della porta
- 802.1X
- Definizione degli intervalli di tempo

La protezione da altri utenti di rete viene descritta nelle seguenti sezioni. Si tratta di attacchi che passano attraverso il dispositivo, ma che non sono destinati al dispositivo stesso.

- Blocco da attacchi DoS
- Snooping DHCP
- Server SSL
- Definizione del controllo storm
- Configurazione della sicurezza della porta
- Guardia origine IP
- Esame di ARP
- Controllo di accesso
- Protezione primo hop

Definizione degli utenti

Il nome utente e la password predefiniti sono **cisco/cisco**. La prima volta che si accede con il nome utente e la password predefiniti, è necessario immettere una nuova password. La complessità della password è abilitata per impostazione predefinita. Se la password scelta non è sufficientemente complessa (opzione **Impostazioni complessità password** selezionata nella pagina Complessità password), verrà chiesto di creare una nuova password.

Impostazione degli account utente

La pagina Account utente consente di aggiungere altri utenti che hanno l'autorizzazione ad accedere al dispositivo (solo lettura o lettura e scrittura) o di modificare le password degli utenti esistenti.

Quando viene aggiunto un utente di livello 15 (come descritto di seguito), l'utente predefinito viene eliminato dal sistema.

NOTA Non è consentito eliminare tutti gli utenti. Se tutti gli utenti sono selezionati, il pulsante **Elimina** è disattivato.

Per aggiungere un nuovo utente, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Account utente**.

In questa pagina vengono visualizzati gli utenti definiti nel sistema e il relativo livello di privilegio.

PASSAGGIO 2 Selezionare **Servizio di recupero password** per attivare la funzione. Una volta attivata, l'utente finale con accesso fisico alla porta della console del dispositivo può accedere al menu di avvio e avviare la procedura di recupero password. Al termine della procedura del sistema di avvio, è possibile accedere al dispositivo senza dover eseguire l'autenticazione della password. È possibile accedere al dispositivo solo tramite la console e solo quando questa è collegata al dispositivo con accesso fisico.

È possibile accedere al menu di avvio ed eseguire la procedura di recupero password anche quando la funzione di recupero password non è attiva. La differenza sta nel fatto che in questo caso tutti i file utente e di configurazione vengono eliminati durante la procedura di avvio del sistema e sul terminale viene visualizzato un messaggio di registro appropriato.

PASSAGGIO 3 Scegliere **Aggiungi** per aggiungere un nuovo utente o fare clic su **Modifica** per modificare un utente.

PASSAGGIO 4 Immettere i parametri.

- **Nome utente**: immettere un nuovo nome utente di lunghezza compresa tra 0 e 20 caratteri. I caratteri UTF-8 non sono consentiti.
- **Password**: immettere una password (i caratteri UTF-8 non sono consentiti). Se viene definita la complessità della password, la password dell'utente deve rispettare i criteri configurati nella sezione **Impostazione delle regole di complessità password**.
- **Conferma password**: immettere di nuovo la password.
- **Indicatore di complessità password**: visualizza la complessità della password. I criteri per la complessità della password vengono configurati nella pagina Complessità password.

- **Livello utente**: selezionare il livello di privilegi dell'utente che viene aggiunto/modificato.
  - *Accesso CLI solo lettura (1)*: l'utente non può accedere all'interfaccia grafica; può accedere soltanto ai comandi CLI che non cambiano la configurazione del dispositivo.
  - *Accesso CLI lettura/scrittura limitata (7)*: l'utente non può accedere all'interfaccia grafica; può accedere soltanto ad alcuni comandi CLI che cambiano la configurazione del dispositivo. Vedere la *Guida di riferimento CLI* per ulteriori informazioni.
  - *Accesso gestione lettura/scrittura (15)*: l'utente può accedere all'interfaccia grafica e può configurare il dispositivo.

PASSAGGIO 5 Fare clic su **Applica**. L'utente viene aggiunto al file di configurazione esecuzione del dispositivo.

Impostazione delle regole di complessità password

Le password vengono utilizzate per autenticare gli utenti che accedono al dispositivo. Password semplici comportano potenziali pericoli per la sicurezza. Pertanto, i requisiti di complessità della password vengono applicati per impostazione predefinita e possono essere configurati secondo necessità. I requisiti di complessità della password vengono configurati nella pagina **Complessità password** a cui si accede dal menu a discesa Protezione. Inoltre, in questa pagina è possibile configurare la validità temporale della password.

Per definire le regole di complessità password, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Complessità password**.

PASSAGGIO 2 Inserire i seguenti parametri di validità temporale per le password:

- **Scadenza password**: se selezionato, all'utente viene richiesto di cambiare la password quando la **Validità temporale password** scade.
- **Validità temporale password**: immettere il numero di giorni che possono trascorrere prima che all'utente venga richiesto di cambiare la password.

  NOTA Le impostazioni di validità temporale della password sono applicabili anche alle password di lunghezza pari a zero (nessuna password).

PASSAGGIO 3 Selezionare **Impostazioni complessità password** per applicare le regole di complessità per le password.

Se la complessità delle password è abilitata, le nuove password devono essere conformi alle seguenti impostazioni predefinite:

- Avere una lunghezza minima di otto caratteri.
- Contenere caratteri da almeno tre classi di carattere (lettere maiuscole, lettere minuscole, numeri e caratteri speciali disponibili sulla tastiera standard).
- Essere diverse dalla password corrente.
- Non contenere alcun carattere che venga ripetuto più di tre volte consecutivamente.
- Non ripetere o invertire il nome dell'utente ed evitare qualsiasi variante ottenuta cambiando le lettere minuscole in maiuscole e viceversa.
- Non ripetere o invertire il nome del produttore ed evitare qualsiasi variante ottenuta cambiando le lettere minuscole in maiuscole e viceversa.

PASSAGGIO 4 Se sono attivate le **Impostazioni complessità password**, possono essere configurati i seguenti parametri:

- **Lunghezza minima password**: immettere il numero minimo di caratteri richiesti per le password.

  NOTA Sono consentite password di lunghezza pari a zero (nessuna password), ed è comunque possibile assegnare ad esse la validità temporale della password.

- **Ripetizione caratteri consentita**: immettere il numero di ripetizioni di un carattere consentite.
- **Numero minimo classi di caratteri**: immettere il numero di classi di caratteri che devono essere presenti in una password. Le classi di caratteri sono minuscolo (1), maiuscolo (2), cifre (3) e simboli o caratteri speciali (4).
- **La nuova password deve essere diversa da quella attuale**: se selezionato, la nuova password non può essere uguale a quella attuale nel momento in cui viene modificata.

PASSAGGIO 5 Fare clic su **Applica**. Le impostazioni della password vengono scritte nel file Configurazione di esecuzione.

NOTA La configurazione dell'equivalenza nome utente-password e dell'equivalenza produttore-password può essere eseguita attraverso la CLI. Vedere la *Guida di riferimento CLI* per ulteriori informazioni.

Configurazione del protocollo TACACS+

Un'azienda può configurare un server TACACS+ (*Terminal Access Controller Access Control System*) per fornire protezione centralizzata a tutti i suoi dispositivi. In questo modo, è possibile gestire l'autenticazione e l'autorizzazione su un singolo server per tutti i dispositivi dell'azienda.

Il dispositivo può agire come client TACACS+ che utilizza il server TACACS+ per i seguenti servizi:

- **Autenticazione**: fornisce l'autenticazione degli utenti che accedono al dispositivo utilizzando nomi utente e password definiti dall'utente.
- **Autorizzazione**: eseguita al momento dell'accesso. Terminata la sessione di autenticazione, viene avviata una sessione di autorizzazione utilizzando il nome utente autenticato. Il server TACACS+ verifica quindi i privilegi utente.
- **Accounting**: attivare l'accounting delle sessioni di accesso tramite il server TACACS+. Ciò consente a un amministratore di sistema di generare report di accounting dal server TACACS+.

Oltre a fornire servizi di autenticazione e autorizzazione, il protocollo TACACS+ contribuisce a garantire la protezione dei messaggi TACACS attraverso messaggi con corpo TACACS crittografati.

TACACS+ è supportato solo con IPv4.

Alcuni server TACACS+ supportano una sola connessione che consente al dispositivo di ricevere tutte le informazioni in una sola connessione. Se il server TACACS+ non la supporta, il dispositivo torna a più connessioni.

Accounting tramite un server TACACS+

L'utente può attivare l'accounting delle sessioni di accesso utilizzando un server RADIUS o TACACS+.

La porta TCP configurabile dall'utente e utilizzata per l'accounting del server TACACS+ è la stessa porta TCP utilizzata per l'autenticazione e l'autorizzazione del server TACACS+.

Quando un utente effettua l'accesso o il logout, il dispositivo invia le seguenti informazioni al server TACACS+:

Tabella 2:

Argomento	Descrizione	Messaggio In Start	Messaggio In Stop
task_id	Un identificatore univoco della sessione di accounting.	Sì	Sì
utente	Nome utente immesso per l'autenticazione dell'accesso.	Sì	Sì
rem-addr	L'indirizzo IP dell'utente.	Sì	Sì
elapsed-time	Indica la durata della sessione dell'utente.	No	Sì
reason	Indica il motivo per il quale la sessione è stata terminata.	No	Sì

Impostazioni predefinite

Di seguito vengono descritti i valori predefiniti per questa funzionalità:

- Per impostazione predefinita non è definito alcun server TACACS+.
- Se si configura un server TACACS, la funzionalità di accounting sarà disattivata per impostazione predefinita.

Interazioni con altre funzioni

Non è possibile attivare l'accounting sia su un server RADIUS che su un server TACACS+.

Flusso di lavoro

Per utilizzare un server TACACS+, attenersi alla seguente procedura:

PASSAGGIO 1 Creare un account per un utente sul server TACACS+.

PASSAGGIO 2 Configurare il server con gli altri parametri nelle pagine TACACS+ e Aggiungi server TACACS+.

PASSAGGIO 3 Selezionare **TACACS+** nella pagina Autenticazione di accesso a gestione in modo che quando un utente accede al dispositivo, l'autenticazione venga eseguita sul server TACACS+ invece che nel database locale.

NOTA Se sono stati configurati più server TACACS+, il dispositivo utilizza le priorità configurate dei server TACACS+ disponibili per selezionare il server TACACS+ che il dispositivo dovrà utilizzare.

Configurazione di un server TACACS+

Nella pagina TACACS+ è possibile configurare i server TACACS+.

Il dispositivo può essere gestito solo gli utenti con livello di privilegi 15 sul server TACACS+. Il livello di privilegio 15 viene assegnato a un utente o a un gruppo di utenti sul server TACACS+ tramite la seguente stringa nella definizione di gruppo o utente:

```
service = exec {
priv-lvl = 15
}
```

Per configurare i parametri del server TACACS+, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **TACACS+**.

PASSAGGIO 2 Se necessario, attivare l'accounting TACACS+. Vedere la spiegazione nella sezione **Accounting tramite un server TACACS+**.

PASSAGGIO 3 Immettere i seguenti parametri predefiniti:

- **Stringa di chiavi**: immettere la **stringa di chiavi** predefinita utilizzata per comunicare con tutti i server TACACS+ in modalità **Con crittografia** o **Testo normale**. Il dispositivo può essere configurato per utilizzare questa chiave o una chiave immessa per un server specifico (immessa nella pagina Aggiungi server TACACS+).

  Se non si immette una stringa di chiavi in questo campo, la chiave del server inserita nella pagina Aggiungi server TACACS+ deve corrispondere alla chiave di crittografia utilizzata dal server TACACS+.

  Se si immette una stringa di chiavi qui e una per un singolo server TACACS+, la stringa di chiavi configurata per il singolo server TACACS+ ha la precedenza.

- **Timeout per risposta**: immettere l'intervallo di tempo che deve trascorrere prima che si verifichi il timeout della connessione tra il dispositivo e il server TACACS+. Se non viene immesso un valore nella pagina Aggiungi server TACACS+ per un server specifico, verrà utilizzato il valore immesso in questo campo.
- **IPv4 di origine**: (solo in modalità di sistema Livello 3) selezionare l'interfaccia di origine IPv4 del dispositivo che verrà utilizzato nei messaggi inviati per la comunicazione con il server TACACS+.
- **IPv6 di origine**: (solo in modalità di sistema Livello 3) selezionare l'interfaccia di origine IPv6 del dispositivo che verrà utilizzato nei messaggi inviati per la comunicazione con il server TACACS+.

  NOTA Se viene selezionata l'opzione Automatica, il sistema prende l'indirizzo IP di origine dall'indirizzo IP definito nell'interfaccia di uscita.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni TACACS+ predefinite vengono aggiunte al file di configurazione esecuzione. Queste impostazioni vengono utilizzate se nella pagina Aggiungi non sono stati impostati i parametri equivalenti.

PASSAGGIO 5 Per aggiungere un server TACACS+ fare clic su **Aggiungi**.

PASSAGGIO 6 Immettere i parametri.

- **Definizione server**: selezionare uno dei seguenti metodi per identificare il server TACACS+:
  - *Per indirizzo IP*: se questa opzione è selezionata, inserire l'indirizzo IP del server nel campo **Indirizzo IP/Nome del server**.
  - *Per nome*: se questa opzione è selezionata, inserire il nome del server nel campo **Indirizzo IP/Nome server**.
- **Versione IP**: selezionare la versione IP supportata dell'indirizzo di origine: IPv6 o IPv4.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se IPv6 viene utilizzato). Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale collegamento presenta un prefisso **FE80** non reindirizzabile, che è possibile utilizzare solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questa voce sostituisce l'indirizzo nella configurazione.

- *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.

- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento (se Collega locale - Tipo di indirizzo IPv6 è selezionato) dall'elenco.
- **Indirizzo IP/Nome server**: immettere l'indirizzo IP o il nome del server TACACS+.
- **Priorità**: immettere l'ordine in cui viene utilizzato questo server TACACS+. Zero è la priorità più alta del server TACACS+, il primo server utilizzato. Se non è possibile stabilire una sessione con il server ad alta priorità, il dispositivo cercherà il server con la priorità più alta successiva.
- **Indirizzo IP di origine**: (per i dispositivi SG500X e altri dispositivi in modalità di sistema Livello 3) selezionare questa opzione per utilizzare l'indirizzo di origine predefinito del dispositivo o uno degli indirizzi IP disponibili per la comunicazione con il server TACACS+.
- **Stringa di chiavi**: immettere la stringa di chiavi predefinita utilizzata per l'autenticazione e la crittografia tra il dispositivo e il server TACACS+. Questa chiave deve corrispondere alla chiave configurata nel server TACACS+.

  Una stringa di chiavi viene utilizzata per crittografare le comunicazioni utilizzando MD5. È possibile selezionare la chiave predefinita sul dispositivo oppure immettere la chiave in modalità **Con crittografia** o **Testo normale**. Se non si dispone di una stringa di chiavi crittografata (da un altro dispositivo), immettere la stringa di chiavi in modalità testo normale e scegliere **Applica**. La stringa di chiavi con crittografia viene creata e visualizzata.

  La chiave immessa qui sostituisce la stringa di chiavi predefinita per il dispositivo, se specificata nella pagina principale.
- **Timeout per risposta**: immettere l'intervallo di tempo che deve trascorrere prima che si verifichi il timeout della connessione tra il dispositivo e il server TACACS+. Selezionare **Usa predefinito** per utilizzare il valore predefinito visualizzato nella pagina.
- **Porta IP**: immettere il numero della porta utilizzata per la sessione TACACS+.
- **Connessione singola**: selezionare l'opzione per ricevere tutte le informazioni in una connessione singola. Se il server TACACS+ non la supporta, il dispositivo torna a più connessioni.

PASSAGGIO 7 Per visualizzare i dati sensibili sempre in formato testo normale nel file di configurazione, fare clic su **Visualizza dati sensibili in testo normale**.

PASSAGGIO 8 Fare clic su **Applica**. Il server TACACS+ viene aggiunto al file di configurazione esecuzione del dispositivo.

Configurazione del RADIUS

I server RADIUS (Remote Authorization Dial-In User Service) offrono un controllo di accesso di rete centralizzato 802.1X o basato su MAC. Il dispositivo è un client RADIUS in grado di utilizzare un server RADIUS per fornire protezione centralizzata.

Un'azienda può configurare un server RADIUS (Remote Authorization Dial-In User Service) per fornire un controllo degli accessi di rete centralizzato 802.1X o basato su MAC per tutti i suoi dispositivi. In questo modo, è possibile gestire l'autenticazione e l'autorizzazione su un singolo server per tutti i dispositivi dell'azienda.

Il dispositivo può agire come client RADIUS che utilizza il server RADIUS per i seguenti servizi:

- **Autenticazione**: fornisce l'autenticazione degli utenti normali e 802.1X che accedono al dispositivo utilizzando nomi utente e password definiti dagli utenti.
- **Autorizzazione**: eseguita al momento dell'accesso. Terminata la sessione di autenticazione, viene avviata una sessione di autorizzazione utilizzando il nome utente autenticato. Il server RADIUS verifica quindi i privilegi utente.
- **Accounting**: attivare l'accounting delle sessioni di accesso tramite il server RADIUS. Ciò consente a un amministratore di sistema di generare report di accounting dal server RADIUS.

Accounting tramite un server RADIUS

L'utente può attivare l'accounting delle sessioni di accesso utilizzando un server RADIUS.

La porta TCP configurabile dall'utente e utilizzata per l'accounting del server RADIUS è la stessa porta TCP utilizzata per l'autenticazione e l'autorizzazione del server RADIUS.

Impostazioni predefinite

Di seguito vengono descritti i valori predefiniti per questa funzionalità:

- Per impostazione predefinita non è definito alcun server RADIUS.
- Se si configura un server RADIUS, la funzionalità di accounting sarà disattivata per impostazione predefinita.

Interazioni con altre funzioni

Non è possibile attivare l'accounting sia su un server RADIUS che su un server TACACS+.

Flusso di lavoro RADIUS

Per utilizzare un server RADIUS, attenersi alla seguente procedura:

PASSAGGIO 1 Creare un account per il dispositivo sul server RADIUS.

PASSAGGIO 2 Configurare il server con gli altri parametri nelle pagine RADIUS e Aggiungi server RADIUS.

NOTA Se sono stati configurati più server RADIUS, il dispositivo utilizza le priorità configurate dei server RADIUS disponibili per selezionare il server RADIUS che il dispositivo dovrà utilizzare.

Per impostare i parametri del server RADIUS, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **RADIUS**.

PASSAGGIO 2 Immettere l'opzione Accounting RADIUS. Sono disponibili le seguenti opzioni:

- **Controllo dell'accesso basato su porte (802.1X, basato su MAC, autenticazione Web)**: specifica che il server RADIUS viene utilizzato per la registrazione della porta 802.1x.
- **Accesso di gestione**: specifica che il server RADIUS viene utilizzato per la registrazione dell'accesso utente.
- **Controllo di accesso in base alla porta e accesso a gestione**: specifica che il server RADIUS viene utilizzato sia per la registrazione della porta 802.1x che per la registrazione dell'accesso utente.

- **Nessuna**: specifica che il server RADIUS non viene utilizzato per alcuna registrazione.

PASSAGGIO 3 Immettere i parametri RADIUS predefiniti, se necessario. I valori immessi nei parametri predefiniti vengono applicati a tutti i server. Se non viene immesso un valore di un server specifico (nella pagina Aggiungi server RADIUS), il dispositivo utilizza i valori di questi campi.

- **Tentativi**: immettere il numero di richieste che devono essere trasmesse al server RADIUS prima che si verifichi un errore.
- **Timeout per risposta**: immettere il tempo in secondi durante il quale il dispositivo deve attendere una risposta del server RADIUS prima di provare a inviare nuovamente la query o di passare al server successivo.
- **Tempo morto**: immettere il numero di minuti che possono trascorrere prima che un server RADIUS bloccato venga ignorato per le richieste di servizio. Se il valore è 0, il server non viene ignorato.
- **Stringa di chiavi**: immettere la stringa di chiavi predefinita utilizzata per l'autenticazione e la crittografia tra il dispositivo e il server RADIUS. Questa chiave deve corrispondere a quella configurata nel server RADIUS. Una stringa di chiavi viene utilizzata per crittografare le comunicazioni utilizzando MD5. È possibile immettere la chiave in modalità **Con crittografia** o **Testo normale**. Se non si dispone di una stringa di chiavi crittografata (da un altro dispositivo), immettere la stringa di chiavi in modalità testo normale e scegliere **Applica**. La stringa di chiavi con crittografia viene creata e visualizzata.

Ciò annulla la stringa di chiavi predefinita, se ne è stata definita una.

- **IPv4 di origine**: (solo in modalità di sistema Livello 3) selezionare l'interfaccia di origine IPv4 del dispositivo che verrà utilizzato nei messaggi inviati per la comunicazione con il server RADIUS.
- **IPv6 di origine**: (solo in modalità di sistema Livello 3) selezionare l'interfaccia di origine IPv6 del dispositivo che verrà utilizzato nei messaggi inviati per la comunicazione con il server RADIUS.

  NOTA Se viene selezionata l'opzione Automatica, il sistema prende l'indirizzo IP di origine dall'indirizzo IP definito nell'interfaccia di uscita.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni predefinite RADIUS per il dispositivo vengono aggiornate nel file di configurazione esecuzione.

Per aggiungere un server RADIUS fare clic su **Aggiungi**.

PASSAGGIO 5 Immettere i valori nei campi corrispondenti ad ogni server RADIUS. Per utilizzare i valori predefiniti immessi nella pagina RADIUS, selezionare **Usa predefinito**.

- **Definizione server**: selezionare se specificare il server RADIUS in base all'indirizzo IP o al nome.
- **Versione IP**: selezionare la versione dell'indirizzo IP del server RADIUS.
- **Tipo di indirizzo IPv6**: indica che il tipo di indirizzo IPv6 è Globale.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se IPv6 viene utilizzato). Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale collegamento presenta un prefisso **FE80** non reindirizzabile, che è possibile utilizzare solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questa voce sostituisce l'indirizzo nella configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento (se Collega locale - Tipo di indirizzo IPv6 è selezionato) dall'elenco.
- **Indirizzo IP/Nome server**: immettere l'indirizzo IP o il nome del server RADIUS.
- **Priorità**: immettere la priorità del server. La priorità determina l'ordine in cui il dispositivo tenta di contattare i server per autenticare un utente. Il dispositivo inizia con il server RADIUS con la priorità più alta. Zero è la priorità più alta.
- **Stringa di chiavi**: immettere la stringa di chiavi utilizzata per l'autenticazione e la crittografia della comunicazione tra il dispositivo e il server RADIUS. Questa chiave deve corrispondere a quella configurata nel server RADIUS. È possibile immettere la chiave in modalità **Con crittografia** o **Testo normale**. Se il campo **Usa predefinito** è selezionato, il dispositivo cercherà di autenticarsi al server RADIUS utilizzando la stringa di chiavi predefinita.
- **Timeout per risposta**: immettere il tempo in secondi durante il quale il dispositivo deve attendere di ricevere una risposta dal server RADIUS prima di provare a inviare di nuovo la query o passare al server successivo qualora il limite massimo dei tentativi a disposizione sia stato raggiunto. Se il campo **Usa predefinito** è selezionato, il dispositivo utilizza il valore di timeout predefinito.

- **Porta di autenticazione**: immettere il numero della porta UDP della porta del server RADIUS per le richieste di autenticazione.
- **Porta di accounting**: immettere il numero di porta UDP della porta del server RADIUS per le richieste di accounting.
- **Tentativi**: immettere il numero di richieste che devono essere trasmesse al server RADIUS prima che si verifichi un errore. Se il campo **Usa predefinito** è selezionato, il dispositivo utilizza il valore predefinito per il numero di tentativi.
- **Tempo morto**: immettere il numero di minuti che devono trascorrere prima che un server RADIUS bloccato venga ignorato per le richieste di servizio. Se il campo **Usa predefinito** è selezionato, il dispositivo utilizza il valore predefinito per il tempo morto. Se si immette 0 minuti, non c'è tempo morto.
- **Tipo di utilizzo**: immettere il tipo di autenticazione del server RADIUS. Sono disponibili le seguenti opzioni:
  - *Accesso*: il server RADIUS viene utilizzato per autenticare gli utenti che desiderano amministrare il dispositivo.
  - *802.1X*: il server RADIUS viene utilizzato per l'autenticazione 802.1X.
  - *Tutti*: il server RADIUS viene utilizzato per autenticare gli utenti che desiderano amministrare il dispositivo e per l'autenticazione 802.1X.

PASSAGGIO 6 Per visualizzare i dati sensibili sempre in formato testo normale nel file di configurazione, fare clic su **Visualizza dati sensibili in testo normale**.

PASSAGGIO 7 Fare clic su **Applica**. La definizione del server RADIUS viene aggiunta al file di configurazione esecuzione del dispositivo.

Gestione delle chiavi

Gestione delle chiavi

NOTA Questo capitolo riguarda soltanto i dispositivi SG500X/ESW2-550X.

In questa sezione viene descritto come configurare i keychain per le applicazioni e il protocolli, ad esempio il protocollo RIP. Per una descrizione del modo in cui il RIP utilizza il keychain per l'autenticazione, vedere **Autenticazione RIP**.

Per creare un keychain, attenersi alla seguente procedura:

PASSAGGIO 1 Creare un keychain con chiave univoca nella pagina Impostazioni keychain.

PASSAGGIO 2 Aggiungere ulteriori chiavi nella pagina Impostazioni chiavi.

Creazione di un keychain

Accedere alla pagina Impostazioni keychain per creare un nuovo keychain.

PASSAGGIO 1 Scegliere **Protezione** > **Gestione delle chiavi** > **Impostazioni keychain**.

PASSAGGIO 2 Per aggiungere un nuovo keychain, fare clic su **Aggiungi** per aprire la pagina Aggiungi keychain e compilare i seguenti campi:

- **Keychain**: il nome del keychain.
- **Identificatore di chiavi**: identificatore intero del keychain.
- **Stringa di chiavi**: valore della stringa del keychain. Selezionare una delle seguenti opzioni:
  - *Definito dall'utente (con crittografia)*: immettere una versione crittografata.
  - *Definito dall'utente (testo normale)*: immettere una versione testo normale.

  NOTA È possibile immettere entrambi i valori di **Accetta periodo di validità** e di **Invia periodo di validità**. Il valore Accetta periodo di validità indica il periodo di tempo in cui la ricezione dei pacchetti è valida per l'identificatore di chiavi. Il valore Invia periodo di validità indica il periodo di tempo in cui l'invio dei pacchetti è valido per l'identificatore di chiavi.

- **Accetta periodo di validità/Invia periodo di validità**: specifica i casi in cui i pacchetti con questa chiave vengono accettati. Selezionare una delle seguenti opzioni.
  - *Sempre valido*: indica che l'identificatore chiave ha validità infinita.
  - *Definito dall'utente*: indica che la durata del keychain è limitata. Se si seleziona questa opzione, è necessario immettere i valori nei campi seguenti.

NOTA Se si seleziona Definito dall'utente, è necessario impostare l'ora di sistema, manualmente o da SNTP. In caso contrario, i valori Accetta periodo di validità e Invia periodo di validità daranno sempre esito negativo.

I seguenti campi riguardano i campi Accetta periodo di validità e Invia periodo di validità:

- **Data di inizio**: inserire la prima data in assoluto in cui l'identificatore di chiavi è risultato valido.
- **Ora di inizio**: inserire la prima ora in assoluto in cui l'identificatore di chiavi è valido nella data di inizio.
- **Ora di fine**: inserire l'ultima data in cui l'identificatore di chiavi è valido. Selezionare una delle seguenti opzioni.
  - *Infinito*: indica che l'identificatore chiave ha validità infinita.
  - *Durata*: indica che la durata dell'identificatore di chiavi è limitata. Se si seleziona questa opzione, è necessario immettere i valori nei campi seguenti.
- **Durata**: il periodo di tempo in cui l'identificatore di chiavi è valido. Immettere informazioni nei seguenti campi:
  - *Giorni*: il numero di giorni in cui l'identificatore di chiavi è valido.
  - *Ore*: il numero di ore in cui l'identificatore di chiavi è valido.
  - *Minuti*: il numero di minuti in cui l'identificatore di chiavi è valido.
  - *Secondi*: il numero di secondi in cui l'identificatore di chiavi è valido.

PASSAGGIO 3 Fare clic su **Applica**. Le impostazioni vengono scritte nel file Configurazione di esecuzione.

Creazione delle impostazioni di un keychain

Accedere alla pagina Impostazioni keychain per aggiungere una chiave al keychain esistente.

PASSAGGIO 1 Scegliere **Protezione** > **Gestione delle chiavi** > **Impostazioni delle chiavi**.

PASSAGGIO 2 Per aggiungere una nuova stringa chiave, fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere informazioni nei seguenti campi:

- **Keychain**: il nome del keychain.
- **Identificatore di chiavi**: identificatore intero del keychain.
- **Stringa di chiavi**: valore della stringa del keychain. Selezionare una delle seguenti opzioni:
  - *Definito dall'utente (con crittografia)*: immettere una versione crittografata.
  - *Definita dall'utente (testo normale)*: immettere una versione testo normale.

  NOTA È possibile immettere entrambi i valori di **Accetta periodo di validità** e di **Invia periodo di validità**. Il valore **Accetta periodo di validità** indica il periodo di tempo in cui la ricezione dei pacchetti è valida per l'identificatore di chiavi. Il valore **Invia periodo di validità** indica il periodo di tempo in cui l'invio dei pacchetti è valido per il keychain. Sono stati descritti solo i campi per il valore **Accetta periodo di validità**, poiché sono identici a quelli del valore **Invia periodo di validità**.

- **Accetta periodo di validità**: specifica i casi in cui i pacchetti con questa chiave vengono accettati. Selezionare una delle seguenti opzioni.
  - *Sempre valido*: indica che l'identificatore chiave ha validità infinita.
  - *Definito dall'utente*: indica che la durata del keychain è limitata. Se si seleziona questa opzione, è necessario immettere i valori nei campi seguenti.
- **Data di inizio**: inserire la prima data in assoluto in cui l'identificatore di chiavi è risultato valido.
- **Ora di inizio**: inserire la prima ora in assoluto in cui l'identificatore di chiavi è valido nella data di inizio.
- **Ora di fine**: inserire l'ultima data in cui l'identificatore di chiavi è valido. Selezionare una delle seguenti opzioni.
  - *Infinito*: indica che l'identificatore chiave ha validità infinita.
  - *Durata*: indica che la durata dell'identificatore di chiavi è limitata. Se si seleziona questa opzione, è necessario immettere i valori nei campi seguenti.

- **Durata**: il periodo di tempo in cui l'identificatore di chiavi è valido. Immettere informazioni nei seguenti campi:
  - *Giorni*: il numero di giorni in cui l'identificatore di chiavi è valido.
  - *Ore*: il numero di ore in cui l'identificatore di chiavi è valido.
  - *Minuti*: il numero di minuti in cui l'identificatore di chiavi è valido.
  - *Secondi*: il numero di secondi in cui l'identificatore di chiavi è valido.

PASSAGGIO 4 Per visualizzare i dati sensibili sempre in formato testo normale (e non crittografato), fare clic su **Visualizza dati sensibili in testo normale**.

PASSAGGIO 5 Fare clic su **Applica**. Le impostazioni vengono scritte nel file Configurazione di esecuzione.

Metodo di accesso a gestione

I profili di accesso determinano come autenticare e autorizzare gli utenti che accedono al dispositivo mediante metodi di accesso diversi. I profili di accesso possono limitare l'accesso alla gestione da fonti specifiche.

L'accesso al dispositivo in modalità gestione viene concesso soltanto agli utenti che superano l'autenticazione del profilo di accesso attivo e l'autenticazione di accesso a gestione.

Sul dispositivo è consentito un solo profilo di accesso attivo per volta.

Ogni profilo di accesso è composta da una o più regole. Le regole vengono eseguite in ordine di priorità nel profilo di accesso (dall'alto al basso).

Le regole sono composte da filtri che includono i seguenti elementi:

- **Metodi di accesso**: metodi per accedere e gestire il dispositivo:
  - Telnet
  - Telnet protetto (SSH)
  - Protocollo di trasferimento Hypertext (HTTP)
  - HTTP protetto (HTTPS)
  - SNMP (Simple Network Management Protocol)
  - Tutti quelli indicati sopra

- **Azione**: consente o nega l'accesso a un'interfaccia o a un indirizzo di origine.
- **Interfaccia**: le porte, i LAG o le VLAN che possono accedere o che non possono accedere all'utilità di configurazione basata sul Web.
- **Indirizzo IP di origine**: indirizzi IP o subnet. I metodi di accesso alla gestione possono essere diversi tra i gruppi utenti. Ad esempio, un gruppo utenti può accedere al modulo dispositivo solo tramite una sessione HTTPS, mentre un altro gruppo può accedere sia tramite una sessione HTTPS che tramite una sessione Telnet.

Profilo di accesso attivo

Nella pagina Profili di accesso vengono visualizzati i profili di accesso definiti ed è possibile selezionare un profilo di accesso come profilo attivo.

Quando un utente tenta di accedere al dispositivo con un metodo di accesso, il dispositivo verifica se il profilo di accesso attivo consente esplicitamente l'accesso alla gestione del dispositivo tramite questo metodo. Se non viene trovata nessuna corrispondenza, l'accesso viene negato.

Se un tentativo di accesso al dispositivo viola il profilo di accesso attivo, il dispositivo genera un messaggio SYSLOG per avvisare l'amministratore di sistema del tentativo.

Se è stato attivato un profilo di accesso solo console, per poterlo disattivare è necessaria una connessione diretta dalla stazione di gestione alla porta console fisica sul dispositivo; non è possibile farlo in altri modi.

Per ulteriori informazioni, vedere la sezione **Definizione delle regole di profilo**.

Utilizzare la pagina Profili di accesso per creare un profilo di accesso e per aggiungere la sua prima regola. Se il profilo di accesso contiene solo una singola regola, il processo è terminato. Per aggiungere ulteriori regole al profilo, utilizzare la pagina Regole di profilo.

PASSAGGIO 1 Scegliere **Protezione** > **Metodo accesso Gestione** > **Profili di accesso**.

In questa pagina vengono visualizzati tutti i profili di accesso, attivi e inattivi.

PASSAGGIO 2 Per modificare il profilo di accesso attivo, selezionare un profilo dalla casella a discesa **Attiva profilo di accesso** e fare clic su **Applica**. In questo modo il profilo scelto diventa il profilo di accesso attivo.

NOTA Se è stata selezionata l'opzione Solo console viene visualizzato un messaggio di avviso. Se si continua, l'utente viene disconnesso immediatamente dall'utilità di configurazione basata sul Web ed è possibile accedere al dispositivo solo attraverso la porta console. Questo si applica solo ai tipi di dispositivi che presentano una porta della console.

Se si seleziona qualsiasi altro profilo di accesso, viene visualizzato un messaggio di avviso in cui si informa che, in base al profilo di accesso selezionato, l'utente potrebbe essere disconnesso dall'utilità di configurazione basata sul Web.

PASSAGGIO 3 Scegliere **OK** per selezionare il profilo di accesso attivo oppure su **Annulla** per interrompere l'azione.

PASSAGGIO 4 Fare clic su **Aggiungi** per aprire la pagina Aggiungi profilo di accesso. La pagina consente di configurare un nuovo profilo e una regola.

PASSAGGIO 5 Immettere il **nome del profilo di accesso**. Tale nome può contenere un massimo di 32 caratteri.

PASSAGGIO 6 Immettere i parametri.

- **Priorità regole**: immettere la priorità regole. Se il pacchetto corrisponde a una regola, ai gruppi utenti viene concesso o negato l'accesso al dispositivo. La priorità regole è fondamentale per il confronto dei pacchetti con le regole, dato che i pacchetti vengono confrontati su una base di prima corrispondenza. Uno è la priorità più alta.
- **Metodo di gestione**: selezionare il metodo di gestione secondo il quale viene definita la regola. Sono disponibili le seguenti opzioni:
  - *Tutti*: assegna tutti i metodi di gestione alla regola.
  - *Telnet*: agli utenti che richiedono l'accesso al dispositivo e che soddisfano i criteri del profilo di accesso Telnet viene consentito o negato l'accesso.
  - *Telnet protetto (SSH)*: agli utenti che richiedono l'accesso al dispositivo e che soddisfano i criteri del profilo di accesso SSH viene consentito o negato l'accesso.
  - *HTTP*: gli utenti che richiedono l'accesso al dispositivo e che soddisfano i criteri del profilo di accesso HTTP viene consentito o negato l'accesso.
  - *HTTP protetto (HTTPS)*: agli utenti che richiedono l'accesso al dispositivo e che soddisfano i criteri del profilo di accesso HTTPS viene consentito o negato l'accesso.

- *SNMP*: agli utenti che richiedono l'accesso al dispositivo e che soddisfano i criteri del profilo di accesso SNMP viene consentito o negato l'accesso.

- **Azione**: selezionare l'azione associata alla regola. Sono disponibili le seguenti opzioni:
  - *Consenti*: consente l'accesso al dispositivo se l'utente corrisponde alle impostazioni del profilo.
  - *Nega*: nega l'accesso al dispositivo se l'utente corrisponde alle impostazioni del profilo.
- **Si applica all'interfaccia**: selezionare l'interfaccia associata alla regola. Sono disponibili le seguenti opzioni:
  - *Tutte*: si applica a tutte le porte, le reti VLAN e i gruppi LAG.
  - *Definita dall'utente*: si applica all'interfaccia selezionata.
- **Interfaccia**: immettere il numero di interfaccia se è stato selezionato Definito dall'utente.
- **Si applica all'indirizzo IP di origine**: selezionare il tipo di indirizzo IP di origine al quale viene applicato il profilo di accesso. Il campo *Indirizzo IP di origine* è valido per una subnet. Selezionare uno dei seguenti valori:
  - *Tutti*: si applica a tutti i tipi di indirizzi IP.
  - *Definiti dall'utente* : si applica solo ai tipi di indirizzi IP definiti nei campi.
- **Indirizzo IP**: immettere l'indirizzo IP di origine.
- **Maschera**: selezionare il formato per la subnet mask dell'indirizzo IP di origine e immettere un valore in uno dei campi:
  - *Maschera di rete*: selezionare la sottorete a cui appartiene l'indirizzo IP di origine e immettere la subnet mask nel formato decimale separato da punti.
  - *Lunghezza prefisso*: selezionare la Lunghezza prefisso e immettere il numero di bit che formano il prefisso dell'indirizzo IP di origine.

PASSAGGIO 7 Fare clic su **Applica**. Il profilo di accesso viene scritto nel file Configurazione di esecuzione. Ora è possibile selezionare questo profilo di accesso come profilo di accesso attivo.

Definizione delle regole di profilo

I profili di accesso possono contenere fino a 128 regole per stabilire chi ha il permesso di gestire e accedere al dispositivo e i metodi di accesso che è possibile utilizzare.

Ogni regola in un profilo di accesso contiene un'azione e criteri (uno o più parametri) a cui corrispondere. Ogni regola ha una priorità le regole con la priorità più bassa vengono verificate per prime. Se il pacchetto in ingresso corrisponde a una regola, viene eseguita l'azione associata alla regola. Se non viene trovata nessuna regola corrispondente nel profilo di accesso attivo, il pacchetto viene eliminato.

Ad esempio, è possibile limitare l'accesso al dispositivo da tutti gli indirizzi IP, ad eccezione degli indirizzi IP allocati nel centro di gestione IT. In questo modo, il dispositivo può ancora essere gestito e ottenere un altro livello di protezione.

Per aggiungere regole di profilo a un profilo di accesso, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Metodo accesso Gestione** > **Regole di profilo**.

PASSAGGIO 2 Selezionare il campo Filtro e un profilo di accesso. Scegliere **Vai**.

Il profilo di accesso selezionato viene visualizzato nella tabella Regola profilo.

PASSAGGIO 3 Fare clic su **Aggiungi** per aggiungere una regola.

PASSAGGIO 4 Immettere i parametri.

- **Nome profilo di accesso**: selezionare un profilo di accesso.
- **Priorità regole**: immettere la priorità regole. Se il pacchetto corrisponde a una regola, ai gruppi utenti viene concesso o negato l'accesso al dispositivo. La priorità regole è fondamentale per il confronto dei pacchetti con le regole, dato che i pacchetti vengono confrontati su una base di first-fit.
- **Metodo di gestione**: selezionare il metodo di gestione secondo il quale viene definita la regola. Sono disponibili le seguenti opzioni:
  - *Tutti*: assegna tutti i metodi di gestione alla regola.
  - *Telnet*: agli utenti che richiedono l'accesso al dispositivo e che soddisfano i criteri del profilo di accesso Telnet viene consentito o negato l'accesso.

- *Telnet protetto (SSH)*: agli utenti che richiedono l'accesso al dispositivo e che soddisfano i criteri del profilo di accesso Telnet viene consentito o negato l'accesso.
- *HTTP*: assegna l'accesso HTTP alla regola. Agli utenti che richiedono l'accesso al dispositivo e che soddisfano i criteri del profilo di accesso HTTP viene consentito o negato l'accesso.
- *HTTP protetto (HTTPS)*: agli utenti che richiedono l'accesso al dispositivo e che soddisfano i criteri del profilo di accesso HTTPS viene consentito o negato l'accesso.
- *SNMP*: agli utenti che richiedono l'accesso al dispositivo e che soddisfano i criteri del profilo di accesso SNMP viene consentito o negato l'accesso.

- **Azione**: selezionare **Consenti** per accettare gli utenti che cercano di accedere al dispositivo utilizzando il metodo di accesso configurato dall'interfaccia e dall'origine IP definite in questa regola. Oppure selezionare **Nega** per negare l'accesso.
- **Si applica all'interfaccia**: selezionare l'interfaccia associata alla regola. Sono disponibili le seguenti opzioni:
  - *Tutte*: si applica a tutte le porte, le reti VLAN e i gruppi LAG.
  - *Definiti dall'utente*: si applica solo alla porta, alla VLAN o al gruppo LAG selezionati.
- **Interfaccia**: immettere il numero di interfaccia.
- **Si applica all'indirizzo IP di origine**: selezionare il tipo di indirizzo IP di origine al quale viene applicato il profilo di accesso. Il campo *Indirizzo IP di origine* è valido per una subnet. Selezionare uno dei seguenti valori:
  - *Tutti*: si applica a tutti i tipi di indirizzi IP.
  - *Definiti dall'utente*: si applica solo ai tipi di indirizzi IP definiti nei campi.
- **Versione IP**: selezionare la versione IP supportata dell'indirizzo di origine: IPv6 o IPv4.
- **Indirizzo IP**: immettere l'indirizzo IP di origine.

- **Maschera**: selezionare il formato per la subnet mask dell'indirizzo IP di origine e immettere un valore in uno dei campi:
  - *Maschera di rete*: selezionare la sottorete a cui appartiene l'indirizzo IP di origine e immettere la subnet mask nel formato decimale separato da punti.
  - *Lunghezza prefisso*: selezionare la Lunghezza prefisso e immettere il numero di bit che formano il prefisso dell'indirizzo IP di origine.

PASSAGGIO 5 Facendo clic su **Applica** la regola viene aggiunta al profilo di accesso.

Autenticazione di accesso a gestione

È possibile assegnare metodi di autenticazione ai vari metodi di accesso a gestione, come SSH, console, Telnet, HTTP e HTTPS. L'autenticazione può essere eseguita localmente o su un server TACACS+ o RADIUS.

Per concedere l'accesso all'utilità di configurazione basata sul Web, il server RADIUS deve restituire cisco-avpair = shell:priv-lvl=15.

L'autenticazione degli utenti avviene nell'ordine di selezione dei metodi di autenticazione. Se il primo metodo di autenticazione non è disponibile, viene utilizzato quello selezionato successivamente. Ad esempio, se i metodi di autenticazione selezionati sono RADIUS e Locale e tutti i server RADIUS configurati vengono cercati in ordine di priorità e non rispondono, l'utente viene autenticato localmente.

Se un metodo di autenticazione ha esito negativo o l'utente non dispone del livello di privilegi necessario, l'accesso al dispositivo non sarà consentito. In altre parole, se un metodo di autenticazione fallisce, il dispositivo arresta il tentativo di autenticazione; il dispositivo non continua provando con il metodo successivo.

Per definire i metodi di autenticazione per un metodo di accesso, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Autenticazione di accesso a gestione**.

PASSAGGIO 2 Selezionare un metodo di accesso dall'elenco **Applicazione**.

PASSAGGIO 3 Utilizzare le frecce per spostare il metodo di autenticazione tra la colonna Metodi facoltativi e la colonna Metodi selezionati. Il primo metodo selezionato è il primo metodo utilizzato.

- *RADIUS*: l'utente viene autenticato in un server RADIUS. È necessario aver configurato uno o più server RADIUS.
- *TACACS+*: l'utente autenticato sul server TACACS+. È necessario aver configurato uno o più server TACACS+.
- *Nessuno*: l'utente può accedere al dispositivo senza autenticazione.
- *Locale*: il nome utente e la password vengono confrontati con i dati memorizzati nel dispositivo locale. Le coppie nome utente e password vengono definite nella pagina Account utente.

  NOTA Il metodo di autenticazione **Locale** o **Nessuno** deve essere sempre selezionato per ultimo. Tutti i metodi di autenticazione selezionati dopo **Locale** o **Nessuno** vengono ignorati.

PASSAGGIO 4 Fare clic su **Applica**. I metodi di autenticazione selezionati vengono associati al metodo di accesso.

Gestione sicura dei dati sensibili

Vedere **Protezione: gestione sicura dei dati sensibili**.

Server SSL

In questa sezione viene descritta la funzione SSL (Secure Socket Layer)

Panoramica di SSL

La funzione SSL viene utilizzata per aprire una sessione HTTPS sul dispositivo.

Una sessione HTTPS può essere aperta con il certificato predefinito presente sul dispositivo.

Quando si utilizza un certificato predefinito, alcuni browser generano degli avvisi poiché questo non presenta la firma dell'autorità di certificazione (CA). È consigliabile avere un certificato firmato da un'autorità di certificazione attendibile.

Per aprire una sessione HTTPS con un certificato creato dall'utente, attenersi alla seguente procedura:

1. Generare un certificato.
2. Richiedere che l'attestato venga certificato da una CA.
3. Importare il certificato firmato nel dispositivo.

Impostazioni predefinite e configurazione

Il dispositivo contiene un certificato modificabile per impostazione predefinita.

HTTPS è attivo per impostazione predefinita.

Impostazioni autenticazione del server SSL

Potrebbe essere necessario generare un nuovo certificato che sostituisca il certificato predefinito rilevato nel dispositivo.

Per creare un nuovo certificato, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione > Server SSL > Impostazioni autenticazione del server SSL**.

Vengono visualizzate le informazioni per i certificati 1 e 2 nella tabella chiave del server SSL. Questi campi sono definiti nella pagina **Modifica** ad eccezione dei seguenti:

- **Valido da**: indica la data di inizio validità del certificato.
- **Valido fino a**: indica la data di fine validità del certificato.
- **Origine certificato**: indica se il certificato è stato generato dal sistema (Generato automaticamente) o dall'utente (Definito dall'utente).

PASSAGGIO 2 Selezionare un certificato valido.

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

PASSAGGIO 4 Immettere informazioni nei seguenti campi:

- **Rigenera chiave RSA**: selezionare l'opzione per rigenerare la chiave RSA.
- **Lunghezza chiave**: immettere la lunghezza della chiave RSA da generare.
- **Nome comune**: indica l'URL o l'indirizzo IP completo del dispositivo. Se non specificato, viene inserito l'indirizzo IP più basso del dispositivo per impostazione predefinita (quando il certificato viene generato).
- **Unità organizzazione**: specifica l'unità organizzazione o il nome del reparto.
- **Nome organizzazione**: indica il nome dell'organizzazione.
- **Località**: specifica il nome della località o della città.
- **Stato**: specifica il nome dello stato o della provincia.
- **Paese**: specifica il nome del Paese.
- **Durata**: specifica il numero di giorni di validità del certificato.

PASSAGGIO 5 Fare clic su **Genera richiesta di certificato**. Viene creata una chiave da immettere nella CA (Certification Authority).

Per importare un certificato, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione > Server SSL > Impostazioni autenticazione del server SSL**.

PASSAGGIO 2 Fare clic su **Importa certificato**.

PASSAGGIO 3 Immettere informazioni nei seguenti campi:

- **ID certificato**: selezionare il certificato valido.
- **Certificato**: copiare nel certificato ricevuto.
- **Importa coppia di chiavi RSA**: selezionare l'opzione per copiare nella nuova coppia di chiavi RSA.
- **Chiave pubblica**: copia nella chiave pubblica RSA.
- **Chiave privata (con crittografia)**: selezionare e copiare nella chiave privata RSA in formato crittografato.
- **Chiave privata (testo normale)**: selezionare e copiare nella chiave privata RSA in formato testo normale.

PASSAGGIO 4 Fai clic su **Visualizza dati sensibili con crittografia** per visualizzare la chiave con crittografia. In questo caso, le chiavi private vengono scritte nel file di configurazione in formato crittografato (quando si seleziona Applica).

PASSAGGIO 5 Scegliere **Applica** per applicare le modifiche alla Configurazione di esecuzione.

Il pulsante **Dettagli** mostra il certificato e la coppia di chiavi RSA. Questa opzione viene utilizzata per copiare il certificato e la coppia di chiavi RSA su un altro dispositivo (utilizzando copia/incolla). Quando si fa clic su **Visualizza dati sensibili con crittografia**, le chiavi private vengono visualizzate in formato crittografato.

Server SSH

Vedere **Protezione: server SSH**.

Client SSH

Vedere **Protezione: client SSH**.

Configurazione dei servizi TCP/UDP

Nella pagina Servizi TCP/UDP è possibile attivare i servizi basati su TCP o UDP nel dispositivo, di solito per motivi di sicurezza.

Il dispositivo offre i seguenti servizi TCP/UDP:

- **HTTP**: attivato per impostazioni predefinite di fabbrica
- **HTTPS**: attivato per impostazioni predefinite di fabbrica
- **SNMP**: disattivato per impostazioni predefinite di fabbrica
- **Telnet**: disattivato per impostazioni predefinite di fabbrica
- **SSH**: disattivato per impostazioni predefinite di fabbrica

Le connessioni TCP attive vengono visualizzate anche in questa finestra.

Per configurare i servizi TCP/UDP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Servizi TCP/UDP**.

PASSAGGIO 2 Attivare o disattivare i seguenti servizi TCP/UDP nei servizi visualizzati.

- **Servizio HTTP**: indica se il servizio HTTP è attivato o disattivato.
- **Servizio HTTPS**: indica se il servizio HTTPS è attivato o disattivato.
- **Servizio SNMP**: indica se il servizio SNMP è attivato o disattivato.
- **Servizio Telnet**: indica se il servizio Telnet è attivato o disattivato.
- **Servizio SSH**: indica se il servizio SSH è attivato o disattivato.

Nella tabella Servizio TCP vengono visualizzati i seguenti campi per ogni servizio:

- **Nome servizio**: metodo di accesso attraverso il quale il dispositivo offre il servizio TCP.
- **Tipo**: protocollo IP utilizzato dal servizio.
- **Indirizzo IP locale**: indirizzo IP locale attraverso il quale il dispositivo offre il servizio.
- **Porta locale**: porta TCP locale attraverso la quale il dispositivo offre il servizio.
- **Indirizzo IP remoto**: indirizzo IP del dispositivo remoto che richiede il servizio.
- **Porta remota**: porta TCP del dispositivo remoto che richiede il servizio.
- **Stato**: stato del servizio.

Nella tabella Servizi UDP vengono visualizzate le seguenti informazioni:

- **Nome servizio**: metodo di accesso attraverso il quale il dispositivo offre il servizio UDP.
- **Tipo**: protocollo IP utilizzato dal servizio.
- **Indirizzo IP locale**: indirizzo IP locale attraverso il quale il dispositivo offre il servizio.
- **Porta locale**: porta UDP locale attraverso la quale il dispositivo offre il servizio.

- **Istanza dell'applicazione**: l'istanza dell'applicazione del servizio UDP (ad esempio, quando due mittenti inviano dati alla stessa destinazione).

PASSAGGIO 3 Fare clic su **Applica**. I servizi vengono scritti nel file Configurazione di esecuzione.

Definizione del controllo storm

Quando i frame broadcast, multicast o unicast sconosciuti vengono ricevuti, vengono duplicati e viene inviata una copia a tutte le possibili porte in uscita. Ciò significa che vengono in pratica inviati a tutte le porte appartenenti alla VLAN pertinente. In questo modo, un unico frame in ingresso viene trasformato in molti frame, creando il potenziale per uno storm del traffico.

La protezione storm consente di limitare il numero di frame in ingresso sul dispositivo e di definire i tipi di frame inclusi entro tale limite.

Se la velocità dei frame Broadcast, Multicast o Unicast sconosciuto è maggiore della soglia definita dall'utente, i frame ricevuti oltre la soglia vengono eliminati.

Per definire il controllo storm, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Controllo storm**.

Tutti i campi di questa pagina sono descritti nella pagina Modifica controllo storm, ad eccezione di **Soglia di velocità controllo storm (%)**. Viene visualizzata la percentuale della larghezza di banda totale disponibile per i pacchetti Unicast, Multicast e Broadcast sconosciuti prima che il controllo storm venga applicato alla porta. Il valore predefinito è 10% della velocità massima della porta e viene impostato nella pagina Modifica controllo storm.

PASSAGGIO 2 Selezionare una porta e fare clic su **Modifica**.

PASSAGGIO 3 Immettere i parametri.

- **Interfaccia**: selezionare la porta per cui attivare la funzione di controllo storm.
- **Controllo storm**: selezionare per attivare il controllo storm.
- **Soglia di velocità controllo storm**: immettere la velocità massima alla quale possono essere inoltrati i pacchetti sconosciuti. Il valore predefinito per questa soglia è pari a 10.000 per i dispositivi FE e a 100.000 per i dispositivi GE.

- **Modalità Controllo storm**: selezionare una delle modalità seguenti.
  - *Unicast sconosciuto, Multicast e Broadcast*: include il traffico unicast, broadcast e multicast sconosciuto nella soglia della larghezza di banda.
  - *Multicast e Broadcast*: include il traffico broadcast e multicast nella soglia della larghezza di banda.
  - *Solo broadcast*: include solo il traffico broadcast nella soglia della larghezza di banda.

PASSAGGIO 4 Fare clic su **Applica**. Il controllo storm viene modificato e la Configurazione di esecuzione viene aggiornata.

Configurazione della sicurezza della porta

La sicurezza della rete può essere migliorata limitando l'accesso a una porta agli utenti con determinati indirizzi MAC. Gli indirizzi MAC possono essere rilevati dinamicamente o configurati staticamente.

La funzione di sicurezza della porta monitora i pacchetti ricevuti e rilevati. L'accesso alle porte bloccate è consentito solo agli utenti con indirizzi MAC specifici.

La funzione di sicurezza della porta presenta quattro modalità:

- **Blocco tradizionale**: tutti gli indirizzi MAC rilevati nella porta sono bloccati e la porta non rileva nessun nuovo indirizzo MAC. Gli indirizzi rilevati non sono soggetti a validità temporale o a ulteriore rilevamento.
- **Blocco dinamico limitato**: il dispositivo rileva indirizzi MAC fino al limite di indirizzi consentiti configurato. Raggiunto il limite, il dispositivo non rileva altri indirizzi. In questa modalità gli indirizzi sono soggetti a validità temporale e a ulteriore rilevamento.
- **Protezione perenne**: mantiene gli attuali indirizzi MAC dinamici associati alla porta e li rileva fino a raggiungere il numero massimo configurato per la porta (N. max di indirizzi consentito). Il rilevamento e la validità temporale vengono disattivati.
- **Eliminazione sicura durante ripristino**: elimina gli attuali indirizzi MAC dinamici associati alla porta dopo il ripristino. I nuovi indirizzi MAC possono essere rilevati come quelli eliminati durante il ripristino fino a raggiungere il numero massimo di indirizzi configurato per la porta. Il rilevamento e la validità temporale vengono disattivati.

Quando viene rilevato un frame di un nuovo indirizzo MAC in una porta in cui non ha l'autorizzazione (la porta è bloccata in modo tradizionale e c'è un nuovo indirizzo MAC oppure la porta è bloccata dinamicamente e il numero massimo di indirizzi consentiti è stato superato), viene invocato il meccanismo di protezione e può verificarsi una delle azioni seguenti:

- Il frame viene eliminato
- Il frame viene reindirizzato
- La porta viene arrestata

Quando l'indirizzo MAC sicuro viene visualizzato in un'altra porta, il frame viene reindirizzato ma l'indirizzo MAC non viene rilevato in quella porta.

Oltre a una di queste azioni è inoltre possibile generare trap e limitare la loro frequenza e numero per evitare il sovraccarico dei dispositivi.

NOTA Se si desidera utilizzare 802.1X su una porta, è necessario che la porta sia in modalità host multipli o multisessione. Se la porta è in modalità singola non è possibile impostare la protezione (vedere la pagina 802.1x, Autenticazione host e sessione*)*.

Per configurare la sicurezza della porta, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Sicurezza porta**.

PASSAGGIO 2 Selezionare un'interfaccia da modificare e fare clic su **Modifica.**

PASSAGGIO 3 Immettere i parametri.

- **Interfaccia**: selezionare il nome dell'interfaccia.
- **Stato dell'interfaccia**: selezionare per bloccare la porta.
- **Modalità di rilevamento**: selezionare il tipo di blocco della porta. Per configurare questo campo, Stato dell'interfaccia deve essere sbloccato. Il campo Modalità di rilevamento è attivato solo se il campo *Stato dell'interfaccia* è bloccato. Per modificare la Modalità di rilevamento, è necessario cancellare Stato dell'interfaccia. Dopo avere modificato la modalità è possibile selezionare nuovamente Stato dell'interfaccia. Sono disponibili le seguenti opzioni:
  - *Blocco tradizionale*: la porta viene bloccata immediatamente, indipendentemente dal numero di indirizzi già rilevati.
  - *Blocco dinamico limitato*: la porta viene bloccata eliminando gli indirizzi MAC dinamici correnti associati alla porta. La porta rileva quindi gli indirizzi fino a raggiungere il numero massimo configurato per la porta. Sono attivati sia l'ulteriore rilevamento che la validità temporale degli indirizzi MAC.

- *Protezione perenne*: mantiene gli attuali indirizzi MAC dinamici associati alla porta e li rileva fino a raggiungere il numero massimo configurato per la porta (**N. max di indirizzi consentito**). Il rilevamento e la validità temporale sono attivati.
- *Eliminazione sicura durante ripristino*: elimina gli attuali indirizzi MAC dinamici associati alla porta dopo il ripristino. I nuovi indirizzi MAC possono essere rilevati come quelli eliminati durante il ripristino fino a raggiungere il numero massimo di indirizzi configurato per la porta. Il rilevamento e la validità temporale vengono disattivati.

- **N. max di indirizzi consentito**: inserire il numero massimo di indirizzi MAC che è possibile rilevare nella porta se la modalità di rilevamento *Blocco dinamico limitato* è selezionata. Il numero 0 indica che solo gli indirizzi statici sono supportati sull'interfaccia.
- **Intervento per violazione**: selezionare un'azione da applicare ai pacchetti che arrivano sulla porta bloccata Sono disponibili le seguenti opzioni:
  - *Elimina*: i pacchetti provenienti da origini non rilevate vengono eliminati.
  - *Inoltra*: i pacchetti provenienti da un'origine sconosciuta vengono inoltrati senza rilevare l'indirizzo MAC.
  - *Arresta*: i pacchetti provenienti da origini non rilevate vengono eliminati e la porta viene arrestata. La porta rimane in questo stato finché non viene riattivata o finché il dispositivo non viene riavviato.
- **Trap**: selezionare per attivare trap quando si riceve un pacchetto su una porta bloccata. È importante per le violazioni dei blocchi. Per il blocco tradizionale, si tratta di qualsiasi indirizzo nuovo ricevuto. Per il blocco dinamico limitato, si tratta di un nuovo indirizzo che supera il numero di indirizzi consentiti.
- **Frequenza trap**: immettere il tempo minimo (in secondi) che deve trascorrere tra le trap.

PASSAGGIO 4 Fare clic su **Applica**. Viene modificata la sicurezza della porta e il file di Configurazione di esecuzione viene aggiornato.

802.1X

Per informazioni sull'autenticazione 802.1X, consultare il capitolo **Protezione: autenticazione 802.1x**. Questa opzione include l'autenticazione basata sul Web e su MAC.

Blocco da attacchi DoS

Un attacco DoS (Denial of Service) è il tentativo da parte di un pirata informatico di rendere un dispositivo non disponibile ai suoi utenti.

Gli attacchi DoS saturano il dispositivo con richieste di comunicazione esterne in modo che non possa rispondere al traffico legittimo. Tali attacchi portano in genere al sovraccarico della CPU di un dispositivo.

SCT (Secure Core Technology)

Un metodo per resistere agli attacchi DoS utilizzati dal dispositivo consiste nell'uso della tecnologia SCT. SCT viene attivata per impostazione predefinita e non può essere disattivata.

Il dispositivo Cisco è un dispositivo avanzato che gestisce il traffico di gestione, il traffico di protocollo e il traffico di snooping, oltre al traffico dell'utente finale (TCP).

SCT assicura che il dispositivo riceva ed elabori il traffico di gestione e di protocollo, indipendentemente dal volume di traffico totale ricevuto. Questa operazione viene eseguita limitando la velocità del traffico TCP alla CPU.

Non vi sono interazioni con altre funzioni.

Le opzioni SCT possono essere monitorate nella pagina Denial of Service > Blocco degli attacchi DoS > Impostazioni suite di sicurezza (pulsante **Dettagli**).

Tipi di attacchi DoS

Un attacco Denial of Service può essere rivolto ai seguenti tipi di pacchetti o altre strategie:

- **Pacchetti SYN TCP**: questi pacchetti hanno spesso un falso indirizzo del mittente. Ogni pacchetto viene gestito come una richiesta di connessione che induce il server a generare una connessione half-open rinviando un

pacchetto TCP/SYN-ACK (Acknowledge) e attendendo un pacchetto in risposta dall'indirizzo del mittente (risposta al pacchetto ACK). Tuttavia, dal momento che l'indirizzo del mittente è falso, la risposta non giunge mai. Queste connessioni half-open saturano il numero di connessioni disponibili che il dispositivo è in grado di effettuare, impedendogli di rispondere a richieste legittime.

- **Pacchetti SYN-FIN TCP**: i pacchetti SYN vengono inviati per creare una nuova connessione TCP. I pacchetti FIN TCP vengono inviati per chiudere una connessione. Non deve mai esistere un pacchetto in cui siano impostati il flag SYN e FIN contemporaneamente. Di conseguenza, questi pacchetti possono indicare un attacco sul dispositivo e devono essere bloccati.
- **Martian Address**: i Martian Address non sono validi dal punto di vista del protocollo IP. Per ulteriori dettagli, vedere la sezione **Martian Address**.
- **Attacco ICMP**: l'invio di pacchetti ICMP in formato non corretto o di un numero eccessivo di pacchetti ICMP alla vittima che potrebbe portare a un arresto imprevisto del sistema.
- **Frammentazione IP**: frammenti IP danneggiati con carichi eccessivi e sovrapposti vengono inviati al dispositivo. Ciò può causare un arresto di vari sistemi operativi a causa di un bug nel codice di riassemblaggio della frammentazione TCP/IP. I sistemi operativi Windows 3.1x, Windows 95 e Windows NT, oltre alle versioni di Linux precedenti alle versioni 2.0.32 e 2.1.63, sono vulnerabili a questo attacco.
- **Distribuzione Stacheldraht**: il pirata informatico utilizza un programma client per connettersi a gestori che sono sistemi compromessi che emettono comandi ad agenti zombie, che a loro volta facilitano l'attacco DoS. Gli agenti sono compromessi tramite i gestori dall'autore di un attacco.

  Utilizzando routine automatizzate che sfruttano le vulnerabilità dei programmi che accettano più connessioni remote sugli host remoti bersaglio, ogni gestore può controllare fino a un migliaio di agenti.
- **Trojan Invasor**: un trojan consente all'autore di un attacco di scaricare un agente zombie (o il trojan può contenerne uno). Gli autori degli attacchi possono inoltre irrompere nei sistemi utilizzando strumenti automatizzati che sfruttano le falle nei programmi che ascoltano le connessioni da host remoti. Questo scenario interessa in primo luogo i dispositivi che fungono da server sul Web.
- **Trojan Back Oriface**: si tratta di una variazione di un trojan che utilizza il software Back Oriface per impiantare il trojan.

Difesa dagli attacchi DoS

La funzione Blocco degli attacchi DoS assiste l'amministratore del sistema nel resistere a tali attacchi nei seguenti modi:

- Attivare la protezione SYN TCP. Se questa funzionalità è attivata, quando viene identificato un attacco SYN viene generato un rapporto e la porta attaccata può essere arrestata temporaneamente. Un attacco SYN viene identificato se il numero di pacchetti SYN al secondo supera una soglia configurata dall'utente.
- Bloccare i pacchetti SYN-FIN.
- Bloccare i pacchetti contenenti Martian Address riservati (pagina Martian Address).
- Impedire le connessioni TCP da un'interfaccia specifica (pagina Filtro SYN) e stabilire un limite di velocità dei pacchetti (pagina Protezione velocità SYN).
- Configurare il blocco di determinati pacchetti ICMP (pagina Filtro ICMP).
- Eliminare i pacchetti IP frammentati da una specifica interfaccia (pagina Filtro frammenti IP).
- Respingere gli attacchi da parte di Distribuzione Stacheldraht, Trojan Invasor e Trojan Back Orifice (pagina Impostazioni suite di sicurezza).

Dipendenze tra funzioni

L'ACL e i criteri QoS avanzati non sono attivi se per una porta è attiva l'opzione Protezione dagli attacchi DoS. Se si tenta di attivare l'opzione Protezione da attacchi DoS quando si definisce un ACL sull'interfaccia o si tenta di definire un ACL su un'interfaccia sulla quale è attivata l'opzione Protezione da attacchi DoS viene visualizzato un messaggio.

Non è possibile bloccare un attacco SYN se è presente un ACL attivo su un'interfaccia.

Configurazione predefinita

La funzionalità Protezione da attacchi DoS presenta le seguenti caratteristiche predefinite:

- Questa funzione è disattivata per impostazione predefinita.
- La protezione SYN-FIN è attiva per impostazione predefinita (anche se l'opzione Protezione da attacchi DoS è disattivata).
- Se la protezione SYN è attivata, la modalità di protezione predefinita è **Blocca e segnala**. La soglia predefinita è 30 pacchetti SYN al secondo.
- Tutte le altre funzioni di prevenzione DoS sono disattivate per impostazione predefinita.

Configurazione della prevenzione DoS

Le pagine seguenti sono utilizzate per configurare questa funzionalità.

Impostazioni suite di sicurezza

NOTA Prima di attivare l'opzione Protezione da attacchi DoS, è necessario annullare l'associazione di tutti gli elenchi di controllo degli accessi (ACL) o dei criteri QoS avanzati associati a una porta. L'ACL e i criteri QoS avanzati non sono attivi quando una porta ha l'opzione Protezione dagli attacchi DoS attivata.

Per configurare le impostazioni globali dell'opzione Protezione da attacchi DoS e per monitorare SCT, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Blocco da attacchi DoS** > **Impostazioni suite di sicurezza**. Vengono visualizzate le *Impostazioni suite di sicurezza*.

Meccanismo di protezione CPU: Attivato indica che la SCT è abilitata.

PASSAGGIO 2 Fare clic su **Dettagli** accanto a **Utilizzo della CPU** per accedere alla pagina omonima e visualizzare le informazioni sull'utilizzo delle risorse CPU.

PASSAGGIO 3 Fare clic su **Modifica** accanto a **Protezione SYN TCP** per accedere alla pagina Protezione SYN e attivare questa funzionalità.

PASSAGGIO 4 Selezionare **Protezione da attacchi DoS** per attivare la funzione.

- **Disattiva**: disattivare la funzione.
- **Prevenzione a livello di sistema**: attiva quella parte della funzione che blocca gli attacchi da parte di Distribuzione Stacheldraht, Trojan Invasor e Trojan Back Orifice.

PASSAGGIO 5 Se viene selezionata l'opzione **Prevenzione a livello di sistema** o **Prevenzione a livello di sistema e a livello di interfaccia**, attivare una o più delle seguenti opzioni di Blocco da attacchi DoS:

- **Distribuzione Stacheldraht**: elimina i pacchetti TCP con porta TCP di origine uguale a 16660.
- **Trojan Invasor**: elimina i pacchetti TCP con porta TCP di destinazione uguale a 2140 e porta TCP di origine uguale a 1024.
- **Trojan Back Orifice**: elimina i pacchetti UDP con porta UDP di destinazione uguale a 31337 e porta UDP di origine uguale a 1024.

PASSAGGIO 6 Fare clic su **Applica**. Le impostazioni della suite di sicurezza di Blocco da attacchi DoS vengono scritte nel file Configurazione di esecuzione.

- Se la Prevenzione a livello di interfaccia è selezionata, fare clic sul pulsante **Modifica** appropriato per configurare la prevenzione desiderata.

Protezione SYN

Le porte di rete possono essere utilizzate dai pirati informatici per attaccare un dispositivo in un attacco SYN, che consuma risorse TCP (buffer) e potenza della CPU.

Dal momento che la CPU è protetta utilizzando la tecnologia SCT, il traffico TCP alla CPU è limitato. Tuttavia, se una o più porte di rete vengono attaccate con un alto livello di pacchetti SYN, la CPU riceve soltanto i pacchetti dell'autore dell'attacco creando così un Denial-Of-Service.

Quando si utilizza la funzionalità di protezione SYN, la CPU conteggia i pacchetti SYN in ingresso al secondo da ogni porta di rete alla CPU.

Se il numero è superiore alla soglia specifica definita dall'utente, alla porta si applica una regola di negazione SYN con MAC-to-me. Questa regola non è legata all'intervallo definito dall'utente (Periodo protezione SYN) della porta.

Per configurare la protezione SYN, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Blocco da attacchi DoS** > **Protezione SYN**.

PASSAGGIO 2 Immettere i parametri.

- **Blocca pacchetti SYN-FIN**: selezionare questa opzione per attivare la relativa funzione. Tutti i pacchetti TCP con flag sia SYN che FIN vengono eliminati su tutte le porte.
- **Modalità di protezione SYN**: selezionare una delle tre modalità:
  - *Disattiva*: la funzionalità viene disattivata su un dispositivo specifico.
  - *Segnala*: genera un messaggio SYSLOG. Se viene superato il valore di soglia, lo stato della porta diventa **Attaccato**.
  - *Blocca e segnala*: quando viene identificato un attacco SYN TCP, i pacchetti SYN TCP destinati al sistema vengono eliminati e lo stato della porta diventa **Bloccato**.
- **Soglia protezione SYN**: numero di pacchetti SYN al secondo prima che i pacchetti SYN vengano bloccati (sulla porta sarà applicata la regola di negazione SYN con MAC-to-me).
- **Periodo protezione SYN**: intervallo di tempo (in secondi) prima dello sblocco di pacchetti SYN (la regola di negazione SYN con MAC-to-me è scollegata dalla porta).

PASSAGGIO 3 Fare clic su **Applica**. La protezione SYN viene definita e il file di configurazione esecuzione viene aggiornato.

Nella tabella Interfaccia protezione SYN vengono visualizzati i seguenti campi per ogni porta o LAG (come richiesto dall'utente).

- **Stato corrente**: lo stato dell'interfaccia. I valori selezionabili sono:
  - *Normale*: nessun attacco identificato su questa interfaccia.
  - *Bloccato*: il traffico non viene inoltrato a questa interfaccia.
  - *Attaccato*: è stato identificato un attacco su questa interfaccia.
- **Ultimo attacco**: data dell'ultimo attacco SYN-FIN identificato dal sistema e azione del sistema (**Segnalato** o **Bloccato e segnalato**).

Martian Address

La pagina Martian Address consente l'inserimento degli indirizzi IP che indicano un attacco se visualizzati nella rete. I pacchetti provenienti da questi indirizzi vengono eliminati.

Il dispositivo supporta un insieme di Martian Address riservati non validi dal punto di vista del protocollo IP. I Martian address riservati supportati sono:

- Indirizzi definiti non validi nella pagina Martian Address.
- Indirizzi definiti non validi dal punto di vista del protocollo, ad esempio gli indirizzi di loopback, inclusi quelli nei seguenti intervalli:
  - **0.0.0.0/8 (tranne 0.0.0.0/32 in quanto un indirizzo di origine)**: gli indirizzi in questo blocco fanno riferimento agli host di origine di questa rete.
  - **127.0.0.0/8**: utilizzato come indirizzo loopback host Internet.
  - **192.0.2.0/24**: utilizzato come TEST-NET nella documentazione e nei codici di esempio.
  - **224.0.0.0/4 (come un indirizzo IP di origine)**: utilizzato nelle assegnazioni dell'indirizzo multicast IPv4 e conosciuto in precedenza come spazio degli indirizzi di classe D.
  - **224.0.0.0/4 (tranne 255.255.255.255/32 come un indirizzo di destinazione)**: intervallo di indirizzi riservato e conosciuto in precedenza come spazio degli indirizzi di classe D.

È inoltre possibile aggiungere nuovi Martian Address per Blocco da attacchi DoS. I pacchetti con Martian Address vengono eliminati.

Per definire gli Martian Address, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Blocco da attacchi DoS** > **Martian Address**.

PASSAGGIO 2 Selezionare Indirizzi Martian riservati e fare clic su **Applica** per includere i Martian Address riservati nell'elenco Prevenzione a livello di sistema.

PASSAGGIO 3 Per aggiungere un Indirizzo fittizio fare clic su **Aggiungi**.

PASSAGGIO 4 Immettere i parametri.

- **Versione IP**: indica la versione IP supportata. Al momento, il supporto è offerto solo per IPv4.

- **Indirizzo IP**: immettere un indirizzo IP da rifiutare. I valori selezionabili sono:
  - *Da elenco riservato*: selezionare un indirizzo IP noto dall'elenco riservato.
  - *Nuovo indirizzo IP*: immettere un indirizzo IP.
- **Maschera**: immettere la maschera dell'indirizzo IP per definire un intervallo di indirizzi IP da rifiutare. I valori sono:
  - *Maschera di rete*: la maschera di rete nel formato decimale separato da punti.
  - *Lunghezza prefisso*: immettere il prefisso dell'indirizzo IP per definire l'intervallo degli indirizzi IP per cui è attivato il Blocco da attacchi DoS.

PASSAGGIO 5 Fare clic su **Applica**. I Martian Address vengono scritti nel file Configurazione di esecuzione.

Filtro SYN

La pagina Filtro SYN consente di filtrare pacchetti TCP contenenti un flag SYN e destinati a una o più porte.

Per definire un filtro SYN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Blocco da attacchi DoS** > **Filtro SYN**.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **Interfaccia**: selezionare l'interfaccia su cui è definito il filtro.
- **Indirizzo IPv4**: immettere l'indirizzo IP per cui è definito il filtro oppure selezionare *Tutti gli indirizzi*.
- **Maschera di rete**: immettere la maschera di rete per cui è attivato il filtro nel formato dell'indirizzo IP.
- **Porta TCP**: selezionare la porta TCP di destinazione che verrà filtrata.
  - *Porte note*: selezionare una porta dall'elenco.
  - *Definita dall'utente*: immettere un numero della porta.
  - *Tutte le porte*: selezionare per indicare che tutte le porte sono filtrate.

PASSAGGIO 4 Fare clic su **Applica**. Il filtro SYN viene definito e il file di Configurazione di esecuzione viene aggiornato.

Protezione velocità SYN

Nella pagina Protezione velocità SYN è possibile limitare il numero di pacchetti SYN ricevuti nella porta in ingresso. Questo può mitigare l'effetto di un flusso SYN sui server, limitando la velocità del numero di nuove connessioni aperte per gestire pacchetti.

Questa funzione è disponibile solo quando il dispositivo è in modalità di sistema Livello 2.

Per definire la protezione velocità SYN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Blocco da attacchi DoS** > **Protezione velocità SYN**.

In questa pagina viene visualizzata la protezione velocità SYN attualmente definita per interfaccia.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **Interfaccia**: selezionare l'interfaccia su cui è definita la protezione velocità.
- **Indirizzo IP**: immettere l'indirizzo IP per cui è definita la protezione velocità SYN oppure selezionare *Tutti gli indirizzi*. Se si immette l'indirizzo IP, immettere la maschera o la lunghezza del prefisso.
- **Maschera di rete**: selezionare il formato per la maschera di rete dell'indirizzo IP di origine e immettere un valore in uno dei campi.
  - *Maschera*: selezionare la sottorete a cui appartiene l'indirizzo IP di origine e immettere la subnet mask nel formato decimale separato da punti.
  - *Lunghezza prefisso*: selezionare la Lunghezza prefisso e immettere il numero di bit che formano il prefisso dell'indirizzo IP di origine.
- **Limite di velocità SYN**: immettere il numero di pacchetti SYN che verranno ricevuti.

PASSAGGIO 4 Fare clic su **Applica**. La protezione velocità SYN viene definita e la Configurazione di esecuzione viene aggiornata.

Filtro ICMP

La pagina Filtro ICMP consente il blocco dei pacchetti ICMP provenienti da determinate fonti. In questo modo è possibile ridurre il carico sulla rete in caso di un attacco ICMP.

Per definire il filtro ICMP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Blocco da attacchi DoS** > **Filtro ICMP**.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **Interfaccia**: selezionare l'interfaccia su cui sono definiti i filtri ICMP.
- **Indirizzo IP**: immettere l'indirizzo IPv4 per cui sono attivati i filtri del pacchetto ICMP oppure selezionare *Tutti gli indirizzi* per bloccare i pacchetti ICMP provenienti da tutti gli indirizzi di origine. Se si immette l'indirizzo IP, immettere la maschera o la lunghezza del prefisso.
- **Maschera di rete**: selezionare il formato per la maschera di rete dell'indirizzo IP di origine e immettere un valore in uno dei campi.
  - *Maschera*: selezionare la sottorete a cui appartiene l'indirizzo IP di origine e immettere la subnet mask nel formato decimale separato da punti.
  - *Lunghezza prefisso*: selezionare la Lunghezza prefisso e immettere il numero di bit che formano il prefisso dell'indirizzo IP di origine.

PASSAGGIO 4 Fare clic su **Applica**. I filtri ICMP vengono definiti e la Configurazione di esecuzione viene aggiornata.

Filtro frammenti IP

Nella pagina IP suddiviso viene consentito il blocco dei pacchetti IP frammentati.

Per configurare il blocco dell'IP frammentato, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Blocco da attacchi DoS** > **Filtro frammenti IP**.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **Interfaccia**: selezionare l'interfaccia su cui è definita la frammentazione IP.
- **Indirizzo IP**: immettere una rete IP da cui vengono filtrati i pacchetti IP frammentati oppure selezionare *Tutti gli indirizzi* per bloccare i pacchetti frammentati IP provenienti da tutti gli indirizzi. Se si immette l'indirizzo IP, immettere la maschera o la lunghezza del prefisso.
- **Maschera di rete**: selezionare il formato per la maschera di rete dell'indirizzo IP di origine e immettere un valore in uno dei campi.
  - *Maschera*: selezionare la sottorete a cui appartiene l'indirizzo IP di origine e immettere la subnet mask nel formato decimale separato da punti.
  - *Lunghezza prefisso*: selezionare la Lunghezza prefisso e immettere il numero di bit che formano il prefisso dell'indirizzo IP di origine.

PASSAGGIO 4 Fare clic su **Applica**. La frammentazione IP viene definita e il file di Configurazione di esecuzione viene aggiornato.

Snooping DHCP

Vedere **Snooping/inoltro DHCPv4**.

Guardia origine IP

La guardia origine IP è una funzione di protezione utilizzabile per bloccare eventuali attacchi al traffico che si possono verificare quando un host prova a utilizzare l'indirizzo IP di un host contiguo.

Se l'opzione Guardia origine IP è attivata, il dispositivo trasmette soltanto il traffico IP client agli indirizzi IP presenti nel database di binding per snooping DHCP. Ciò include sia gli indirizzi aggiunti dallo snooping DHCP sia le voci aggiunte manualmente.

Se il pacchetto trova corrispondenza in una voce del database, viene inoltrato dal dispositivo. In caso contrario, viene eliminato.

Interazioni con altre funzioni

I seguenti punti trattati sono rilevanti per la guardia origine IP:

- Lo snooping DHCP deve essere attivato a livello globale per consentire l'avvio della guardia origine IP su un'interfaccia.
- È possibile attivare la guardia origine IP su un'interfaccia solo se:
  - lo snooping DHCP viene attivato su almeno una delle VLAN della porta.
  - l'interfaccia non è attendibile per DHCP. Tutti i pacchetti sulle porte attendibili vengono inoltrati.
- Se una porta è attendibile per DHCP, è possibile configurare il filtro degli indirizzi IP statici abilitando sulla porta la guardia origine IP, anche se quest'ultima non è attiva in tale condizione.
- Se lo stato della porta cambia da Non attendibile per DHCP ad Attendibile per DHCP, le voci filtro dell'indirizzo IP statico rimangono nel database di binding, ma non sono più attive.
- La sicurezza della porta non può essere attivata se il filtro dell'IP di origine e dell'indirizzo MAC viene configurato su una porta.
- La guardia origine IP sfrutta le risorse TCAM e richiede una regola TCAM singola per la voce relativa all'indirizzo di guardia origine IP. Se il numero delle voci guardia origine IP supera il numero delle regole TCAM disponibili, gli indirizzi supplementari sono inattivi.

Filtro

Se l'opzione Guardia origine IP è attivata su una porta:

- i pacchetti DHCP concessi dallo snooping DHCP vengono consentiti.
- Se il filtro di indirizzo IP di origine viene attivato:
  - Traffico IPv4: è consentito solo il traffico con indirizzo IP di origine associato alla porta.
  - Traffico non IPv4: consentito (inclusi i pacchetti ARP).

Configurazione del flusso di lavoro della guardia origine IP

Per configurare l'opzione Guardia origine IP, attenersi alla seguente procedura:

PASSAGGIO 1 Attivare lo snooping DHCP nella pagina Configurazione IP > DHCP >Proprietà o nella pagina Protezione > Snooping DHCP > Proprietà.

PASSAGGIO 2 Specificare le VLAN su cui attivare lo Snooping DHCP nella pagina Configurazione IP > DHCP > Impostazioni interfaccia.

PASSAGGIO 3 Configurare le interfacce come attendibili o non attendibili nella pagina Configurazione IP > DHCP > Impostazioni delle interfacce per snooping DHCP.

PASSAGGIO 4 Attivare l'opzione Guardia origine IP nella pagina Protezione > Guardia origine IP > Proprietà.

PASSAGGIO 5 Attivare l'opzione Guardia origine IP nelle interfacce non attendibili come richiesto nella pagina Proprietà > Guardia origine IP > Impostazioni interfaccia.

PASSAGGIO 6 Visualizzare le voci del database di binding nella pagina Protezione > Guardia origine IP > Database di binding.

Attivazione della guardia origine IP

Per attivare la guardia origine IP a livello globale, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Guardia origine IP** > **Proprietà**.

PASSAGGIO 2 Per attivare la guardia origine IP a livello globale, scegliere **Attiva**.

Configurazione dell'opzione Guardia origine IP sulle interfacce

Se la guardia origine IP viene attivata su una porta/LAG non attendibile, i pacchetti DHCP consentiti dallo snooping DHCP vengono trasmessi. Se si attiva il filtro dell'indirizzo IP di origine, la trasmissione dei pacchetti viene consentita nel seguente modo:

- **Traffico IPv4**: è consentito solo il traffico IPv4 con indirizzo IP di origine associato alla porta specifica.
- **Traffico non IPv4**: è consentito tutto il traffico non IPv4.

Vedere **Interazioni con altre funzioni** per ulteriori informazioni sull'attivazione della guardia origine IP sulle interfacce.

Per configurare la guardia origine IP sulle interfacce, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Guardia origine IP** > **Impostazioni interfaccia**.

PASSAGGIO 2 Selezionare la porta o il LAG dal campo **Filtro** e fare clic su **Vai**. Le porte o i LAG su questa unità vengono visualizzati insieme a:

- **Guardia origine IP**: indica se la guardia origine IP sulla porta è attiva.
- **Interfaccia Snooping DHCP attendibile**: indica se si tratta di un'interfaccia DHCP attendibile.

PASSAGGIO 3 Selezionare la porta o il LAG e fare clic su **Modifica**. Scegliere **Attiva** nel campo **Guardia origine IP** per attivare la guardia origine IP sull'interfaccia.

PASSAGGIO 4 Fare clic su **Applica** per copiare le impostazione sul file Configurazione di esecuzione.

Database di binding

La guardia origine IP utilizza il database di binding per snooping DHCP con lo scopo di controllare i pacchetti dalle porte non attendibili. Se il dispositivo prova a scrivere troppe voci nel database di binding per snooping DHCP, le voci in eccesso vengono mantenute in stato di inattività. Le voci vengono eliminate alla scadenza della durata lease, in modo da poter attivare le voci inattive.

Vedere **Snooping/inoltro DHCPv4**.

NOTA Nella pagina Database di binding vengono visualizzate **solo** le voci del database di binding per snooping DHCP definite sulle porte abilitate per la guardia origine IP.

Per visualizzare il database di binding per lo snooping DHCP e conoscere l'utilizzo di TCAM , scegliere **Inserisci non attivo**:

PASSAGGIO 1 Scegliere **Protezione** > **Guardia origine IP** > **Database di binding.**

PASSAGGIO 2 Il database di binding per snooping DHCP sfrutta le risorse TCAM per la gestione del database. Selezionare il campo **Inserisci non attivo** per definire la frequenza con cui il dispositivo deve provare ad attivare le voci non attive. È possibile scegliere tra le seguenti opzioni:

- **Frequenza nuovo tentativo**: indica la frequenza con cui le risorse TCAM vengono controllate.
- **Mai**: non provare mai a riattivare gli indirizzi non attivi.

PASSAGGIO 3 Fare clic su **Applica** per salvare le modifiche apportate alla configurazione di esecuzione e/o su **Riprova ora** per controllare le risorse TCAM.

Vengono visualizzate le voci nel database di binding:

- **ID VLAN:** VLAN sulla quale è atteso il pacchetto.
- **Indirizzo MAC**: indirizzo MAC da associare.
- **Indirizzo IP**: indirizzo IP da associare.
- **Interfaccia**: interfaccia sulla quale è atteso il pacchetto.
- **Stato**: indica se l'interfaccia è attiva.
- **Tipo**: indica se la voce è dinamica o statica.
- **Motivo**: indica il motivo per cui l'interfaccia non è attiva. I motivi possibili sono:
  - *Nessun problema*: l'interfaccia è attiva.
  - *VLAN senza snoop*: lo snooping DHCP non è attivo sulla VLAN.
  - *Porta attendibile*: indica che la porta è diventata attendibile.
  - *Problema di risorse*: comunica l'esaurimento delle risorse TCAM.

Per vedere un sottoinsieme di voci, immettere i criteri di ricerca pertinenti e fare clic su **Vai**.

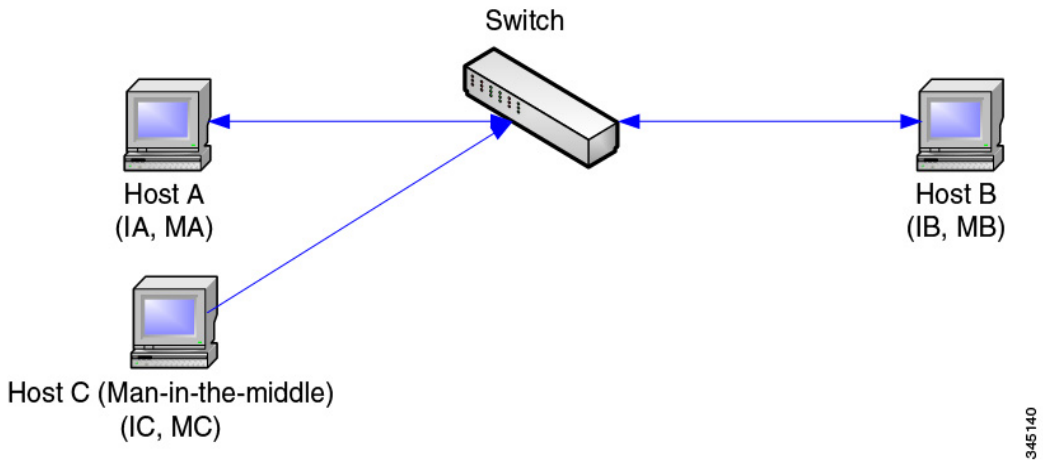
Esame di ARP

ARP attiva la comunicazione IP nel dominio di broadcast di Livello 2 tramite l'associazione degli indirizzi IP con gli indirizzi MAC.

Un utente malintenzionato può attaccare host, switch e router connessi a una rete di Livello 2 contaminando le cache ARP dei sistemi connessi alla sottorete e intercettando il traffico destinato ad altri host sulla sottorete. Ciò può verificarsi perché l'ARP consente all'host di inviare una risposta gratuita nel caso in cui la richiesta ARP non venga ricevuta. Dopo l'attacco, tutto il traffico del dispositivo preso di mira passa attraverso il computer del malintenzionato, poi attraverso il router, lo switch e l'host.

Di seguito viene riportato un esempio di contaminazione della cache ARP.

Contaminazione della cache ARP



Gli host A, B e C sono collegati allo switch sulle interfacce A, B e C e si trovano tutte sulla stessa sottorete. I loro indirizzi MAC e IP vengono indicati tra parentesi, ad esempio l'host A utilizza l'indirizzo IP IA e l'indirizzo MAC MA. Quando l'host A deve comunicare con l'host B al livello IP, trasmette una richiesta ARP per l'indirizzo MAC associato con l'indirizzo IP IB. L'host B risponde con una risposta ARP. Lo switch e l'host A aggiornano la propria cache ARP con il MAC e l'IP dell'host B.

L'host C può contaminare le cache ARP dello switch, dell'host A e dell'host B tramite la trasmissione di risposte ARP contraffatte con binding per un host con un indirizzo IP di IA (o IB) e un indirizzo MAC di MC. Gli host con cache ARP contaminate utilizzano l'indirizzo MAC MC come indirizzo MAC di destinazione per il traffico destinato a IA o IB, permettendo all'host C di intercettare quel traffico.

Dato che l'host C conosce il vero indirizzo MAC associato a IA e IB, è in grado di inoltrare agli host il traffico intercettato, utilizzando come destinatario l'indirizzo MAC corretto. L'host C si inserisce nel flusso del traffico che dall'host A arriva all'host B, attuando il tradizionale attacco "man in the middle".

Il modo in cui ARP previene la contaminazione delle cache

La funzione Esame di ARP viene applicata alle interfacce attendibili o non attendibili (vedere la pagina Protezione > Esame di ARP >Impostazione interfaccia).

Le interfacce vengono classificate dall'utente come descritto di seguito:

- **Attendibile**: i pacchetti non vengono controllati.
- **Non attendibile**: i pacchetti vengono controllati secondo la modalità descritta sopra.

L'esame di ARP viene eseguito solo sulle interfacce non attendibili. I pacchetti ARP ricevuti su interfacce attendibili vengono semplicemente inoltrati.

Quando i pacchetti arrivano su interfacce non attendibili viene implementata la procedura logica seguente:

- Cercare le regole del controllo di accesso ARP per gli indirizzi IP/MAC del pacchetto. Se l'indirizzo IP viene trovato e l'indirizzo MAC nell'elenco corrisponde all'indirizzo MAC del pacchetto, il pacchetto è valido; in caso contrario risulta non valido.
- Se l'indirizzo IP del pacchetto non viene trovato e lo snooping DHCP viene attivato per la VLAN del pacchetto, cercare il database di binding per snooping DHCP per la coppia <indirizzo IP e VLAN > del pacchetto. Se la coppia <VLAN e indirizzo IP> è stata trovata e l'indirizzo MAC e l'interfaccia nel database corrispondono all'indirizzo MAC e all'interfaccia iniziale del pacchetto, il pacchetto è valido.
- Se l'indirizzo IP del pacchetto non è stato trovato nelle regole del controllo di accesso ARP o nel database di binding per snooping DHCP, il pacchetto non è valido e viene eliminato. Viene generato un messaggio SYSLOG.
- Se un pacchetto è valido viene inoltrato e la cache ARP aggiornata.

Se si seleziona l'opzione Convalida pacchetto ARP (pagina Proprietà), vengono eseguiti ulteriori controlli di convalida:

- **MAC di origine**: confronta l'indirizzo MAC di origine del pacchetto nell'intestazione Ethernet con l'indirizzo MAC del mittente nella richiesta ARP. Questo controllo viene eseguito sia sulle richieste sia sulle risposte ARP.
- **MAC di destinazione**: confronta l'indirizzo MAC di destinazione del pacchetto nell'intestazione Ethernet con l'indirizzo MAC dell'interfaccia di destinazione. Questo controllo viene eseguito per le risposte ARP.
- **Indirizzi IP**: confronta il corpo ARP per indirizzi IP sconosciuti o non validi. Gli indirizzi includono 0.0.0.0, 255.255.255.255 e tutti gli indirizzi IP multicast.

I pacchetti con binding dell'esame di ARP non validi vengono registrati ed eliminati.

Nella tabella di controllo dell'accesso ARP è possibile indicare un massimo di 1024 voci.

Interazione tra l'esame di ARP e lo snooping DHCP

Se lo snooping DHCP viene attivato, l'esame di ARP utilizza il database di binding per snooping DHCP insieme alle regole di controllo di accesso ARP. Se lo snooping DHCP non viene attivato, vengono utilizzate soltanto le regole di controllo di accesso ARP.

Impostazioni predefinite di ARP

Nella tabella seguente sono descritti i valori predefiniti di ARP:

Opzione	Stato predefinito
Esame di ARP dinamico	Non attivato
Convalida pacchetto ARP	Non attivato
Esame di ARP abilitato su VLAN	Non attivato
Intervallo di buffer log	Viene attivata la creazione del messaggio SYSLOG per i pacchetti eliminati a intervalli di 5 secondi.

Flusso di lavoro dell'esame di ARP

Per configurare l'esame di ARP, attenersi alla seguente procedura:

PASSAGGIO 1 Attivare l'esame di ARP e configurare le varie opzioni presenti nella pagina Protezione > Esame di ARP > Proprietà.

PASSAGGIO 2 Configurare le interfacce come attendibili o non attendibili per ARP nella pagina Protezione > Esame di ARP > Impostazione interfaccia.

PASSAGGIO 3 Aggiungere le regole nelle pagine Protezione > Esame di ARP > Controllo di accesso ARP e Regole controllo di accesso ARP.

PASSAGGIO 4 Definire le VLAN su cui attivare l'esame di ARP e le regole del controllo di accesso per ciascuna VLAN nella pagina Protezione > Esame di ARP > Impostazioni VLAN.

Definizione delle proprietà dell'esame di ARP

Per configurare l'esame di ARP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Esame di ARP > Proprietà**.

Immettere informazioni nei seguenti campi:

- **Stato esame di ARP:** selezionare questa opzione per attivare l'esame di ARP.
- **Convalida pacchetto ARP**: selezionare questa opzione per attivare i seguenti controlli di convalida:
  - **Indirizzo MAC di origine**: confronta l'indirizzo MAC di origine del pacchetto nell'intestazione Ethernet con l'indirizzo MAC del mittente nella richiesta ARP. Questo controllo viene eseguito sia sulle richieste sia sulle risposte ARP.
  - **Indirizzo MAC di destinazione**: confronta l'indirizzo MAC di destinazione del pacchetto nell'intestazione Ethernet con l'indirizzo MAC dell'interfaccia di destinazione. Questo controllo viene eseguito per le risposte ARP.
  - **Indirizzi IP**: confronta il corpo ARP per indirizzi IP sconosciuti o non validi. Gli indirizzi includono 0.0.0.0, 255.255.255.255 e tutti gli indirizzi IP multicast.

- **Intervallo di buffer log**: selezionare una delle opzioni riportate di seguito.
  - **Frequenza nuovo tentativo:** attivare l'invio di messaggi SYSLOG per i pacchetti eliminati. Immettere il valore relativo alla frequenza di invio dei messaggi.
  - **Mai:** disattiva i messaggi SYSLOG per i pacchetti eliminati.

PASSAGGIO 2 Fare clic su **Applica**. Le impostazioni vengono definite e il file di Configurazione di esecuzione viene aggiornato.

Definizione delle impostazioni di interfaccia dell'esame di ARP dinamico

I pacchetti provenienti da porte o LAG non attendibili vengono confrontati con la tabella delle regole di accesso ARP e con il database di binding per snooping DHCP se lo snooping DHCP è attivato (consultare la pagina Database di binding per snooping DHCP).

Per impostazione predefinita, le porte o i LAG non sono attendibili per l'esame di ARP.

Per modificare lo stato di attendibilità per ARP di una porta o di un LAG, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Esame di ARP** > **Impostazioni interfaccia**.

Vengono visualizzate le porte o i LAG e il relativo stato attendibile/non attendibile per ARP.

PASSAGGIO 2 Per impostare lo stato di una porta o di un LAG su non attendibile, selezionare la porta o il LAG e fare clic su **Modifica**.

PASSAGGIO 3 Scegliere **Attendibile** o **Non attendibile** e fare clic su **Applica** per salvare le impostazioni nel file Configurazione di esecuzione.

Definizione del controllo di accesso dell'esame di ARP

Per aggiungere voci alla tabella dell'esame di ARP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Esame di ARP > Controllo di accesso ARP**.

PASSAGGIO 2 Per aggiungere una voce, fare clic su **Aggiungi**.

PASSAGGIO 3 Completare i seguenti campi:

- **Nome del controllo di accesso ARP**: immettere un nome creato dall'utente.
- **Indirizzo MAC**: indirizzo MAC del pacchetto.
- **Indirizzo IP**: indirizzo IP del pacchetto.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni vengono definite e il file di Configurazione di esecuzione viene aggiornato.

Definizione delle regole del controllo di accesso dell'esame di ARP

Per aggiungere altre regole al gruppo di controllo di accesso ARP creato in precedenza, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Esame di ARP > Regole controllo di accesso ARP**.

Vengono visualizzate le regole di accesso definite attualmente.

PASSAGGIO 2 Per aggiungere altre regole a un gruppo, fare clic su **Aggiungi**.

PASSAGGIO 3 Selezionare un gruppo di controllo di accesso e compilare i campi:

- **Indirizzo MAC**: indirizzo MAC del pacchetto.
- **Indirizzo IP**: indirizzo IP del pacchetto.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni vengono definite e il file di Configurazione di esecuzione viene aggiornato.

Definizione delle impostazioni VLAN dell'esame di ARP

Per attivare l'esame di ARP sulle VLAN e associare i gruppi di controllo di accesso a una VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Esame di ARP > Impostazioni VLAN.**

PASSAGGIO 2 Per attivare l'esame di ARP su una VLAN, spostare la VLAN dall'elenco **VLAN disponibili** all'elenco **VLAN attive**.

PASSAGGIO 3 Per associare una VLAN a un gruppo di controllo di accesso ARP, fare clic su **Aggiungi**. Selezionare il numero di VLAN e scegliere un gruppo di **Controllo di accesso ARP** definito in precedenza.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni vengono definite e il file di Configurazione di esecuzione viene aggiornato.

Protezione primo hop

Protezione: protezione primo hop IPV6

22

Protezione: autenticazione 802.1x

In questa sezione viene descritta l'autenticazione 802.1X.

Vengono trattati i seguenti argomenti:

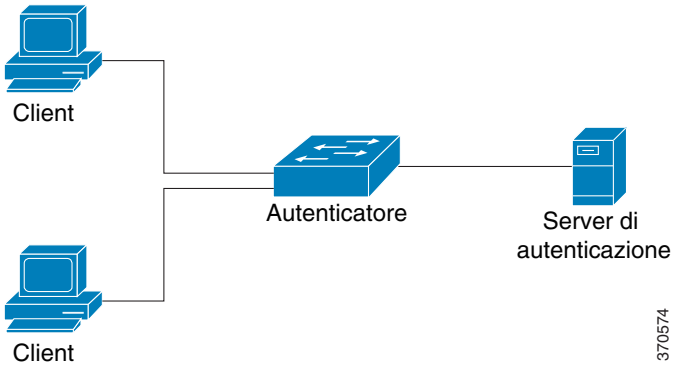
- **Panoramica di 802.1X**
- **Panoramica sull'autenticatore**
- **Attività comuni**
- **Configurazione 802.1X mediante l'interfaccia utente**
- **Definizione degli intervalli di tempo**
- **Supporto modalità porta e metodo di autenticazione**

Panoramica di 802.1X

L'autenticazione 802.1x impedisce ai client non autorizzati di connettersi a una LAN tramite porte con accesso pubblico. L'autenticazione 802.1x è un modello client-server. In questo modello, ai dispositivi di rete vengono assegnati ruoli specifici.

- Client o richiedente
- Autenticatore
- Server di autenticazione

Tutto questo è descritto nella figura di seguito:



Per ogni porta, un dispositivo di rete può essere un client/richiedente, un autenticatore o entrambe le cose.

Client o richiedente

Un client o richiedente è un dispositivo di rete che richiede l'accesso alla LAN. Il client è collegato a un autenticatore.

Se il client utilizza il protocollo 802.1x per l'autenticazione, svolge la parte del richiedente del protocollo 802.1x e la parte del client del protocollo EAP.

Il client non richiede alcun software speciale per utilizzare un'autenticazione basata su Web o su MAC.

Autenticatore

Un autenticatore è un dispositivo di rete che fornisce servizi di rete e a cui vengono collegate le porte del richiedente.

Le modalità di autenticazione impostate su porte (in Protezione > Autenticazione 802.1X Web/MAC > Host e autenticazione) supportate sono le seguenti:

- **Host singolo**: supporta l'autenticazione basata sulla porta con un client singolo per porta.
- **Host multipli**: supporta l'autenticazione basata sulla porta con più client per porta.
- **Multisessione**: supporta l'autenticazione basata sul client con più client per porta.

Per ulteriori informazioni, vedere la sezione **Modalità host della porta**.

Sono supportati i seguenti metodi di autenticazione:

- **Basato su 802.1x**: supportato in tutte le modalità di autenticazione.
- **Basato su MAC**: supportato in tutte le modalità di autenticazione.
- **Basato su WEB**: supportato in tutte le modalità multisessione.

Nell'autenticazione basata su 802.1, l'autenticatore estrae i messaggi EAP dai messaggi 802.1x (frame EAPOL) e li passa al server di autenticazione, utilizzando il protocollo RADIUS.

Con l'autenticazione basata su Web o su MAC, è l'autenticatore stesso a eseguire la parte del client EAP del software.

Server di autenticazione

Il server di autenticazione esegue l'effettiva autenticazione del client. Il server di autenticazione per il dispositivo è un server di autenticazione RADIUS con estensioni EAP.

Panoramica sull'autenticatore

Stati di autenticazione della porta amministrativa

Lo stato della porta amministrativa determina se il client è autorizzato ad accedere alla rete.

È possibile configurare lo stato della porta amministrativa dalla pagina Protezione > Autenticazione 802.1X Web/MAC > Autenticazione porta.

Sono disponibili i seguenti valori:

- **imposizione autorizzata**

  L'autenticazione della porta viene disattivata e la porta trasmette tutto il traffico nel pieno rispetto della sua configurazione statica, senza richiedere alcuna autenticazione. Quando riceve il messaggio iniziale di EAPOL 802.1x, lo switch invia il pacchetto 802.1x EAP, compreso il messaggio EAP di operazione riuscita.

  Questo è lo stato predefinito.

- **imposizione non autorizzata**

  L'autenticazione della porta viene disattivata e la porta trasmette tutto il traffico tramite la VLAN ospite e le VLAN non autenticate. Per ulteriori informazioni, vedere la sezione **Definizione autenticazione host e sessione**. Quando riceve i messaggi iniziali di EAPOL 802.1x, lo switch invia i pacchetti 802.1x EAP, compresi i messaggi di errore EAP.

- **automatico**

  Attiva le autenticazioni 802.1 x secondo la modalità host della porta configurata e i metodi di autenticazione configurati sulla porta.

Modalità host della porta

Le porte possono essere configurate (in Protezione > Autenticazione 802.1X Web/MAC > Host e autenticazione) nelle seguenti modalità host:

- **Modalità host singolo**

  Una porta viene autorizzata se è presente un client autorizzato. È possibile autorizzare un solo host per porta.

  Quando una porta non è autorizzata e la VLAN ospite è attiva, il traffico senza tag viene associato nuovamente alla VLAN ospite. Il traffico con tag viene eliminato a meno che non appartenga alla VLAN ospite o a una VLAN non autenticata. Se una VLAN ospite non è attiva sulla porta, verrà collegato solo il traffico con tag appartenente alle VLAN non autenticate.

  Se una porta è autorizzata, il traffico con e senza tag proveniente dall'host autorizzato viene collegato in base alla configurazione della porta di appartenenza della VLAN statica. Il traffico proveniente da altri host viene eliminato.

  L'utente può specificare che il traffico senza tag proveniente dall'host autorizzato venga nuovamente associato a una VLAN assegnata da un server RADIUS durante il processo di autenticazione. Il traffico con tag viene eliminato a meno che non appartenga alla VLAN assegnata da RADIUS o alle VLAN non autenticate. L'assegnazione della VLAN RADIUS a una porta viene impostata nella pagina Protezione > Autenticazione 802.1X Web/MAC > Autenticazione porta.

- **Modalità host multipli**

  Una porta viene autorizzata se è presente almeno un client autorizzato.

Quando una porta non è autorizzata e la VLAN ospite è attiva, il traffico senza tag viene associato nuovamente alla VLAN ospite. Il traffico con tag viene eliminato a meno che non appartenga alla VLAN ospite o a una VLAN non autenticata. Se una VLAN ospite non è attiva sulla porta, verrà collegato solo il traffico con tag appartenente alle VLAN non autenticate.

Se una porta è autorizzata, il traffico con e senza tag proveniente da tutti gli host connessi alla porta viene collegato in base alla configurazione della porta di appartenenza della VLAN statica.

È possibile specificare che il traffico senza tag proveniente dalla porta autorizzata venga nuovamente associato a una VLAN assegnata da un server RADIUS durante il processo di autenticazione. Il traffico con tag viene eliminato a meno che non appartenga alla VLAN assegnata da RADIUS o alle VLAN non autenticate. L'assegnazione della VLAN RADIUS a una porta viene impostata nella pagina Autenticazione porta.

- **Modalità multisessione**

  A differenza delle modalità host singolo o host multipli, una porta in modalità multisessione non ha uno stato di autenticazione. Tale stato viene assegnato a tutti i client collegati alla porta. Questa modalità richiede una ricerca TCAM. Dal momento che agli switch in modalità Livello 3 (vedi **Supporto alla modalità multisessione**) non viene assegnata una ricerca TCAM per la modalità multisessione, per questi è prevista una forma limitata di modalità multisessione, che non supporta gli attributi VLAN RADIUS e VLAN ospite. Il numero massimo di host autorizzati consentito sulla porta viene configurato nella pagina Autenticazione porta.

  Il traffico con tag appartenente a una VLAN non autenticata viene sempre collegato, indipendentemente dal fatto che l'host sia autorizzato o meno.

  Il traffico con e senza tag proveniente da host non autorizzati non appartenente a una VLAN non autenticata viene associato nuovamente alla VLAN ospite se definito e attivo sulla VLAN, oppure viene eliminato se la VLAN ospite non è attiva sulla porta.

  Se un server RADIUS assegna una VLAN a un host autorizzato, tutto il traffico, con e senza tag, non appartenente alle VLAN non autenticate viene collegato mediante la VLAN; se la VLAN non viene assegnata, tutto il suo traffico viene collegato in base alla configurazione della porta di appartenenza della VLAN statica.

  I seguenti dispositivi supportano la modalità multisessione senza l'assegnazione della VLAN RADIUS e della VLAN ospite:

  - Sx500/ESW2-550X in modalità router Livello 3

- SG500X in modalità stack ibrido di base e avanzata
- SG500XG

Più metodi di autenticazione

Se sullo switch viene attivato più di un metodo di autenticazione, viene applicata la seguente gerarchia di metodi di autenticazione:

- Autenticazione 802.1x: massima
- Autenticazione basata su WEB
- Autenticazione basata su MAC: minima

È possibile eseguire più metodi contemporaneamente. Quando un metodo viene completato correttamente, il client diventa autorizzato, i metodi con priorità più bassa vengono interrotti, mentre quelli con priorità più alta continuano.

Quando un metodo di autenticazione che viene eseguito contemporaneamente ha esito negativo, gli altri metodi continuano.

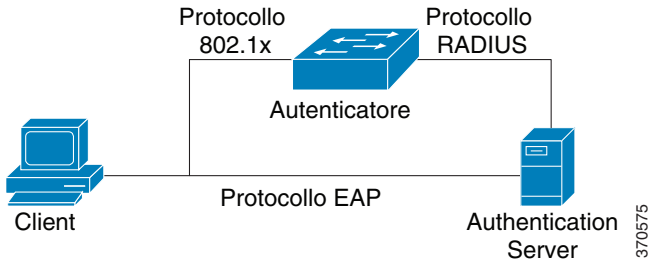
Quando un metodo di autenticazione viene eseguito correttamente per un client autenticato da un metodo di autenticazione con priorità bassa, vengono applicati gli attributi del nuovo metodo di autenticazione. Se il nuovo metodo ha esito negativo, il client rimane autorizzato con il metodo precedente.

Autenticazione basata su 802.1x

L'autenticatore basato su 802.1x trasmette messaggi EAP trasparenti tra i richiedenti 802.1x e i server di autenticazione. I messaggi EAP tra i richiedenti e l'autenticatore vengono incapsulati nei messaggi 802.1x, mentre i messaggi EAP tra l'autenticatore e i server di autenticazione vengono incapsulati nei messaggi RADIUS.

Questa procedura è descritta di seguito:

Figura 1 Autenticazione basata su 802.1x

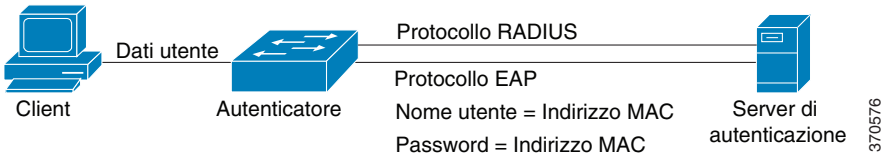


Autenticazione basata su MAC

L'autenticazione basata su MAC costituisce un'alternativa all'autenticazione 802.1X che consente alla rete di accedere ai dispositivi (quali stampanti e telefoni IP) che non dispongono della funzionalità di richiedente 802.1X. L'autenticazione basata su MAC utilizza l'indirizzo MAC del dispositivo di connessione per concedere o negare l'accesso alla rete.

In questo caso, lo switch supporta la funzionalità EAP-MD5 con lo stesso nome utente e la stessa password dell'indirizzo MAC del cliente, come mostrato di seguito.

Figura 2 Autenticazione basata su MAC



Il metodo non prevede alcuna configurazione specifica.

Autenticazione basata su WEB

L'autenticazione basata su WEB viene utilizzata per autenticare gli utenti finali che richiedono di accedere a una rete tramite uno switch. Permette ai client di connettersi direttamente allo switch per essere autenticati tramite un sistema Captive Portal prima che al client venga concesso l'accesso alla rete. L'autenticazione basata su Web è un'autenticazione basata sul client ed è supportata nella modalità multisessione sia a Livello 2 che a Livello 3.

Questo metodo di autenticazione viene attivato su ciascuna porta e, quando una porta è attiva, ogni singolo host deve autenticarsi per poter accedere alla rete. Pertanto, è possibile che su una porta attiva ci siano host autenticati e host non autenticati.

Quando su una porta viene attivata un'autenticazione basata su Web, lo switch elimina tutto il traffico sulla porta proveniente da client non autorizzati, a eccezione dei pacchetti ARP, DHCP, DNS e NETBIOS, che possono essere inoltrati dallo switch in modo tale che anche i client non autorizzati possano utilizzare un indirizzo IP e risolvere i nomi host o di dominio.

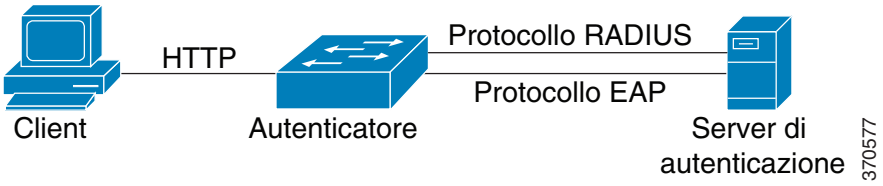
Su tutti i pacchetti HTTP/HTTPS su IPv4 provenienti da client non autorizzati viene eseguito il trap nella CPU dello switch. Quando un utente finale richiede l'accesso alla rete, se l'autenticazione basata su Web è attiva sulla porta, prima di accedere alla pagina richiesta viene visualizzata una pagina di accesso. L'utente deve immettere nome utente/password, autenticati da un server RADIUS mediante protocollo EAP. Se l'autenticazione ha esito positivo, l'utente verrà informato.

L'utente ha ora una sessione autenticata. La sessione rimane aperta mentre è in uso. Se non viene utilizzata per un determinato intervallo di tempo, la sessione viene chiusa. L'intervallo di tempo viene configurato dall'amministratore di sistema ed è detto Periodo di inattività. Quando la sessione scade, il nome utente/la password vengono eliminati, pertanto, se l'ospite desidera aprire una nuova sessione, dovrà inserirli nuovamente.

Vedere la sezione **Tabella 1. Modalità porta e metodi di autenticazione**.

Al termine dell'autenticazione, lo switch inoltra tutto il traffico proveniente dal client sulla porta, come mostrato nella figura di seguito.

Figura 3 Autenticazione basata su WEB



L'autenticazione basata su Web non può essere configurata su una porta con funzione VLAN assegnata da RADIUS o VLAN ospite attiva.

L'autenticazione basata su Web supporta le seguenti pagine:

- Pagina di accesso
- Pagina di accesso riuscito

Esiste una serie predefinita e integrata di pagine di questo genere.

Queste pagine possono essere modificate in Protezione > Autenticazione 802.1X/MAC/Web > Personalizzazione dell'autenticazione Web.

Ciascuna di queste pagine personalizzate può essere visualizzata in anteprima. La configurazione viene salvata nel file Configurazione di esecuzione.

Nella tabella di seguito sono riportati gli SKU che supportano l'autenticazione basata su Web e le relative modalità di sistema:

SKU	Modalità di sistema	Supporto WBA
Sx300	**Livello 2**	Sì
	Livello 3	No
Sx500, Sx500ESW2-550X	**Livello 2**	Sì
	Livello 3	No
SG500X	**Nativa**	Sì
	Ibrido di base - Livello 2	Sì
	Ibrido di base - Livello 3	No
SG500XG	**Come Sx500**	Sì

NOTA

- Quando l'autenticazione basata su Web non è supportata, DVA e VLAN ospite non possono essere configurate in modalità multisessione.
- Quando l'autenticazione basata su Web è supportata, DVA e VLAN ospite possono essere configurate in modalità multisessione.

VLAN non autenticate e VLAN ospite

La VLAN ospite e le VLAN non autenticate forniscono accesso ai servizi che non richiedono che i dispositivi o le porte di sottoscrizione siano 802.1x o autenticate e autorizzate basate su MAC.

La VLAN ospite è la VLAN che viene assegnata a un client non autorizzato. È possibile configurare la VLAN ospite e una o più VLAN in modo che non siano autenticate nella pagina Protezione > Autenticazione 802.1X/MAC/Web > Proprietà.

Una VLAN non autenticata è una VLAN che consente l'accesso dai dispositivi o dalle porte autorizzati e non autorizzati.

Una VLAN non autenticata presenta le seguenti caratteristiche:

- Deve essere una VLAN statica e non può essere la VLAN ospite o la VLAN predefinita.
- Le porte membro devono essere configurate manualmente come membri assegnati.
- Le porte membro devono essere porte trunk e/o porte generali. Una porta di accesso non può essere membro di una VLAN non autenticata.

La VLAN ospite, se configurata, è una VLAN statica con le seguenti caratteristiche:

- deve essere definita manualmente da una VLAN statica esistente;
- la VLAN ospite non può essere utilizzata come VLAN voce o VLAN non autenticata.

Per visualizzare un riepilogo delle modalità in cui la VLAN ospite viene supportata, fare riferimento a **Tabella 3. Supporto alla VLAN opsite e all'assegnazione della VLAN RADIUS**.

Modalità host con VLAN ospite

Le modalità host sono compatibili con la VLAN nel seguente modo:

- **Modalità host singolo e host multipli**

  Il traffico con e senza tag appartenente alla VLAN ospite in arrivo su una porta autorizzata viene collegato mediante la VLAN ospite. Tutto il traffico rimanente viene eliminato. Tutto il traffico appartenente a una VLAN non autenticata viene collegato mediante la VLAN.

- **Modalità multisessione in Livello 2**

  Il traffico con e senza tag non appartenente alle VLAN non autenticate e proveniente da client non autorizzati viene assegnato alla VLAN ospite utilizzando la regola TCAM e viene collegato mediante la VLAN ospite. Tutto il traffico con tag appartenente a una VLAN non autenticata viene collegato mediante la VLAN.

  Questa modalità non può essere configurata sulla stessa interfaccia di VLAN basate su criteri.

- **Modalità multisessione in Livello 3**

  La modalità non supporta la VLAN ospite.

Assegnazione VLAN RADIUS o VLAN dinamica

Un server RADIUS può assegnare una VLAN a un client autorizzato se questa opzione è attiva nella pagina Autenticazione porta. Tale opzione prende il nome di Assegnazione VLAN dinamica o VLAN assegnata da RADIUS. In questa guida si utilizza il termine VLAN assegnata da RADIUS.

Se una porta è in modalità multisessione e la VLAN assegnata da RADIUS è attiva, il dispositivo aggiunge automaticamente la porta come membro senza tag della VLAN assegnata dal server RADIUS durante il processo di autenticazione. Il dispositivo classifica i pacchetti senza tag per la VLAN assegnata se i pacchetti hanno origine dai dispositivi o dalle porte autenticati e autorizzati.

Per ulteriori informazioni sul funzionamento delle varie modalità quando sul dispositivo viene attivata una VLAN assegnata da RADIUS, fare riferimento a **Tabella 3. Supporto alla VLAN opsite e all'assegnazione della VLAN RADIUS** e **Nella tabella di seguito è mostrato come viene gestito il traffico, autenticato e non, in varie situazioni.**

NOTA L'assegnazione della VLAN RADIUS è supportata solo su dispositivi Sx500 quando il dispositivo si trova in modalità di sistema Livello 2. Quando si trovano in modalità stack ibrido e avanzata, i dispositivi SG500X e SG500XG funzionano come i dispositivi Sx500.

Affinché un dispositivo venga autenticato e autorizzato su una porta con funzione DVA attivata:

- Il server RADIUS deve autenticare il dispositivo e assegnare in modo dinamico una VLAN al dispositivo. È possibile impostare il campo Assegnazione VLAN RADIUS su statico nella pagina Autenticazione porta. In questo modo, l'host potrà essere collegato secondo la configurazione statica.
- Un server RADIUS deve supportare DVA con il tipo di tunnel degli attributi RADIUS (64) = VLAN (13), tipo di supporto tunnel (65) = 802 (6) e ID gruppo privato tunnel = un ID VLAN.

Quando la funzione VLAN assegnata da RADIUS è attiva, le modalità host funzionano nel seguente modo:

- **Modalità host singolo e host multipli**

  Il traffico con e senza tag appartenente alla VLAN assegnata da RADIUS viene collegato mediante questa VLAN. Tutto il traffico rimanente che non appartiene alle VLAN non autenticate viene eliminato.

- **Modalità multisessione completa**

  Il traffico con e senza tag non appartenente alle VLAN non autenticate proveniente dal client viene assegnato alla VLAN assegnata da RADIUS utilizzando le regole TCAM e viene collegato mediante la VLAN.

- **Modalità multisessione in modalità di sistema Livello 3**

  Questa modalità non supporta la VLAN assegnata da RADIUS, tranne per i dispositivi SG500X e SG500XG in modalità stack nativo

Nella tabella di seguito viene descritto il supporto dell'assegnazione della VLAN RADIUS e della VLAN ospite a seconda del metodo di autenticazione e della modalità della porta.

Metodo di autenticazione	Host singolo	Host multipli	Multisessione	
			Dispositivo in Livello 3	Dispositivo in Livello 2
802.1x	†	†	N/S	†
MAC	†	†	N/S	†
WEB	N/S	N/S	N/S	N/S

Legenda:

†: la modalità della porta supporta l'assegnazione della VLAN RADIUS e della VLAN ospite.

N/S: la modalità della porta non supporta il metodo di autenticazione.

Modalità di violazione

In modalità host singolo, è possibile configurare l'azione da intraprendere quando un host non autorizzato sulla porta autorizzata tenta di accedere all'interfaccia. Questa operazione viene eseguita nella pagina Autenticazione host e sessione.

Sono disponibili le seguenti opzioni:

- **Limita**: genera un trap quando una stazione, il cui indirizzo MAC non corrisponde all'indirizzo MAC del richiedente, tenta di accedere all'interfaccia. L'intervallo di tempo minimo che intercorre tra un trap e l'altro è 1 secondo. Questi frame vengono reindirizzati, tuttavia i relativi indirizzi di origine non vengono rilevati.
- **Proteggi**: consente di eliminare i frame con gli indirizzi di origine che non corrispondono all'indirizzo del richiedente.
- **Blocca**: consente di eliminare i frame con gli indirizzi di origine che non corrispondono all'indirizzo del richiedente e di bloccare la porta.

È inoltre possibile configurare il dispositivo in modo da inviare trap SNMP con un intervallo di tempo minimo configurabile tra i trap consecutivi. Se i secondi sono pari a 0, i trap vengono disattivati. Se non è specificato alcun intervallo di tempo minimo, per impostazione predefinita viene inserito il valore 1 secondo per la modalità Limita e 0 per le altre modalità.

Periodo di inattività

Il periodo di inattività corrisponde al periodo di tempo in cui la porta (modalità host singolo o host multipli) o il client (modalità multisessione) non può tentare l'autenticazione dopo uno scambio di autenticazione non riuscito. In modalità host singolo o host multipli, il periodo viene definito per porta, mentre in modalità multisessione viene definito per client. Durante il periodo di inattività, lo switch non accetta né avvia richieste di autenticazione.

Il periodo viene applicato solo alle autenticazioni basate su Web e su 802.1x.

Inoltre, è possibile indicare un numero massimo di tentativi di accesso prima che cominci il periodo di inattività. Il valore 0 specifica un numero illimitato di tentativi di accesso.

La durata del periodo di inattività e il numero massimo di tentativi di accesso possono essere impostati nella pagina Autenticazione porta.

Attività comuni

Flusso di lavoro 1: per configurare l'autenticazione 802.1x su una porta:

PASSAGGIO 1 Fare clic su **Protezione > Autenticazione 802.1X/MAC/Web > Proprietà**.

PASSAGGIO 2 Consentire l'autenticazione basata su porte

PASSAGGIO 3 Selezionare il **Metodo di autenticazione**.

PASSAGGIO 4 Scegliere **Applica** e il file con la Configurazione di esecuzione viene aggiornato.

PASSAGGIO 5 Fare clic su Protezione > Autenticazione 802.1X/MAC/Web> Host e sessione.

PASSAGGIO 6 Selezionare la porta richiesta e fare clic su **Modifica**.

PASSAGGIO 7 Impostare la modalità di autenticazione host.

PASSAGGIO 8 Scegliere **Applica** e il file con la Configurazione di esecuzione viene aggiornato.

PASSAGGIO 9 Fare clic su **Protezione > Autenticazione 802.1X/MAC/Web > Autenticazione porta**.

PASSAGGIO 10 Selezionare una porta e fare clic su **Modifica**.

PASSAGGIO 11 Impostare il campo Controllo porta amministrativa su **Auto**.

PASSAGGIO 12 Definire i metodi di autenticazione.

PASSAGGIO 13 Scegliere **Applica** e il file con la Configurazione di esecuzione viene aggiornato.

Flusso di lavoro 2: per configurare i trap, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Autenticazione 802.1X/MAC/Web** > **Proprietà**.

PASSAGGIO 2 Selezionare i trap richiesti.

PASSAGGIO 3 Scegliere **Applica** e il file con la Configurazione di esecuzione viene aggiornato.

Flusso di lavoro 3: per configurare l'autenticazione basata su 802.1x o su Web

PASSAGGIO 1 Fare clic su **Protezione > Autenticazione 802.1X/MAC/Web > Autenticazione porta**.

PASSAGGIO 2 Selezionare la porta richiesta e fare clic su **Modifica**.

PASSAGGIO 3 Immettere i campi richiesti per la porta.

I campi di questa pagina sono descritti in **Definizione dell'autenticazione delle porte 802.1X**.

PASSAGGIO 4 Scegliere **Applica** e il file con la Configurazione di esecuzione viene aggiornato.

Utilizzare il pulsante **Copia impostazioni** per copiare le impostazioni da una porta all'altra.

Flusso di lavoro 4: per configurare il periodo di inattività, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione > Autenticazione 802.1X/MAC/Web > Autenticazione porta**.

PASSAGGIO 2 Selezionare una porta e fare clic su **Modifica**.

PASSAGGIO 3 Immettere il periodo di inattività nel campo Periodo di inattività.

PASSAGGIO 4 Scegliere **Applica** e il file con la Configurazione di esecuzione viene aggiornato.

Flusso di lavoro 5: Per configurare la VLAN ospite, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Autenticazione 802.1X/MAC/Web**> **Proprietà**.

PASSAGGIO 2 Selezionare **Attiva** nel campo VLAN ospite.

PASSAGGIO 3 Selezionare la VLAN ospite nel campo ID VLAN ospite.

PASSAGGIO 4 Configurare il timeout VLAN ospite in modo che sia immediato oppure immettere un valore nel campo Definito dall'utente.

PASSAGGIO 5 Scegliere **Applica** e il file con la Configurazione di esecuzione viene aggiornato.

Flusso di lavoro 6: per configurare le VLAN non autenticate, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Autenticazione 802.1X/MAC/Web** > **Proprietà**.

PASSAGGIO 2 Selezionare una VLAN e fare clic su **Modifica**.

PASSAGGIO 3 Selezionare una VLAN.

PASSAGGIO 4 Se si desidera, deselezionare **Autenticazione** per rendere la VLAN una VLAN non autenticata.

PASSAGGIO 5 Scegliere **Applica** e il file con la Configurazione di esecuzione viene aggiornato.

Configurazione 802.1X mediante l'interfaccia utente

Definizione delle proprietà 802.1X

La pagina Proprietà 802.1X viene utilizzata per attivare 802.1X a livello globale e definire l'autenticazione delle porte. Affinché 802.1X funzioni, deve essere attivato sia a livello globale che singolarmente in ogni porta.

Per definire l'autenticazione basata su porte, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Autenticazione 802.1X/MAC/Web** > **Proprietà**.

PASSAGGIO 2 Immettere i parametri.

- **Autenticazione basata sulla porta**: attivare o disattivare l'autenticazione basata sulla porta.

  Se questa opzione non è attiva, l'autenticazione basata su Web, su MAC e su 802.1X non è attiva.

- **Metodo di autenticazione**: selezionare i metodi di autenticazione degli utenti. Sono disponibili le seguenti opzioni:

  - *RADIUS, Nessuno*: eseguire l'autenticazione della porta utilizzando per primo il server RADIUS. Se non viene ricevuta nessuna risposta da RADIUS (ad esempio, se il server è inattivo), non viene eseguita nessuna autenticazione e la sessione viene consentita. Se il server è disponibile, ma le credenziali utente non sono corrette, l'accesso verrà negato e la sessione chiusa.

  - *RADIUS*: autenticare l'utente nel server RADIUS. Se non viene eseguita nessuna autenticazione, la sessione non è consentita.

  - *Nessuno*: non autenticare l'utente. Consentire la sessione.

- **VLAN ospite**: selezionare questa opzione per attivare l'utilizzo di una VLAN ospite per le porte non autorizzate. Se viene attivata una VLAN ospite, tutte le porte non autorizzate si connettono automaticamente alla VLAN selezionata nel campo *ID VLAN ospite*. Se una porta viene autorizzata in seguito, viene rimossa dalla VLAN ospite.
- **ID VLAN ospite**: selezionare la VLAN ospite dall'elenco di VLAN.
- **Timeout VLAN ospite**: definire un periodo di tempo:
  - Dopo il collegamento, se il software non rileva il richiedente 802.1X o l'autenticazione non è riuscita, la porta viene aggiunta alla VLAN ospite solo dopo che l'intervallo *Timeout VLAN ospite* è scaduto.
  - Se lo stato della porta cambia da *Autorizzato* a *Non autorizzato*, la porta viene aggiunta alla VLAN ospite solo dopo che il timeout della *VLAN ospite* è scaduto.
- **Trap**: per attivare i trap, scegliere una o più delle seguenti opzioni:
  - *Trap di autenticazione 802.1x non riuscita*: selezionare questa opzione per generare un trap se l'autenticazione 802.1x ha esito negativo.
  - *Trap di autenticazione 802.1x riuscita*: selezionare questa opzione per generare un trap se l'autenticazione 802.1x ha esito positivo.
  - *Trap di autenticazione MAC non riuscita*: selezionare questa opzione per generare un trap se l'autenticazione MAC ha esito negativo.
  - *Trap di autenticazione MAC riuscita*: selezionare questa opzione per generare un trap se l'autenticazione MAC ha esito positivo.
- Quando lo switch è in modalità switch Livello 2:
  - *Trap di autenticazione Web non riuscita*: selezionare questa opzione per generare un trap se l'autenticazione Web ha esito negativo.
  - *Trap di autenticazione Web riuscita*: selezionare questa opzione per generare un trap se l'autenticazione Web ha esito positivo.
  - *Trap di autenticazione Web inattiva*: selezionare questa opzione per generare un trap se comincia un periodo di inattività.

Quando il dispositivo si trova in modalità router Livello 3, la tabella Autenticazione VLAN mostra tutte le VLAN e indica se su di esse è stata attivata l'autenticazione.

PASSAGGIO 3 Fare clic su **Applica**. Le proprietà 802.1X vengono aggiunte al file Configurazione di esecuzione.

Definizione dell'autenticazione delle porte 802.1X

Nella pagina Autenticazione porta è possibile configurare i parametri 802.1X per ogni porta. Dato che alcune delle modifiche alla configurazione possono essere eseguite soltanto quando la porta si trova in stato Imponi autorizzato, come nel caso dell'autenticazione host, si consiglia di modificare il controllo della porta in Imponi autorizzato prima di apportare modifiche. Completata la configurazione, ripristinare il controllo della porta nello stato precedente.

NOTA Una porta con 802.1x definito in essa non può diventare un membro di un LAG.

Per definire l'autenticazione 802.1X, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Autenticazione 802.1X/MAC/Web** > **Autenticazione porta**.

In questa pagina vengono visualizzate le impostazioni di autenticazione di tutte le porte.

PASSAGGIO 2 Selezionare una porta e fare clic su **Modifica.**

PASSAGGIO 3 Immettere i parametri.

- **Interfaccia**: selezionare una porta.
- **Controllo porta corrente**: viene visualizzato lo stato di autorizzazione della porta corrente. Se lo stato è *Autorizzato*, la porta è autenticata o il *Controllo porta amministrativa* è *Imposizione autorizzata*. Viceversa, se lo stato è *Non autorizzato*, la porta non è autenticata o il *Controllo porta amministrativa* è *Imposizione non autorizzata*.
- **Controllo porta amministrativa**: selezionare lo stato di autorizzazione della porta amministrativa. Sono disponibili le seguenti opzioni:
  - *Imposizione non autorizzata*: nega l'accesso all'interfaccia modificando l'interfaccia nello stato non autorizzato. Il dispositivo non fornisce i servizi di autenticazione al client attraverso l'interfaccia.
  - *Automatico*: attiva l'autenticazione basata su porte e l'autorizzazione sul dispositivo. L'interfaccia passa dallo stato autorizzato allo stato non autorizzato (e viceversa) in base allo scambio di autenticazione tra il dispositivo e il client.

- *Imposizione autorizzata*: autorizza l'interfaccia senza autenticazione.

- **Assegnazione VLAN RADIUS**: selezionare questa opzione per attivare l'assegnazione dinamica della VLAN sulla porta selezionata.
  - ***Disattiva***: la funzione non è attiva.
  - ***Rifiuta***: se il server RADIUS ha autorizzato il richiedente, ma non ha fornito una VLAN richiedente, il richiedente viene rifiutato.
  - ***Statico***: se il server RADIUS ha autorizzato il richiedente, ma non ha fornito una VLAN richiedente, il richiedente viene accettato.
- **VLAN ospite**: selezionare questa opzione per indicare che per il dispositivo è stato attivato l'utilizzo di una VLAN ospite definita in precedenza. Sono disponibili le seguenti opzioni:
  - *Selezionato*: consente l'utilizzo di una VLAN ospite per le porte non autorizzate. Se viene attivata una VLAN ospite, la porta non autorizzata si connette automaticamente alla VLAN selezionata nel campo ID VLAN ospite nella pagina Autenticazione porta 802.1X.
    In caso di errore di autenticazione e se la VLAN ospite viene attivata a livello globale su una determinata porta, la VLAN ospite viene assegnata automaticamente alle porte non autorizzate come VLAN senza tag.
  - *Cancellato*: disattiva la VLAN ospite nella porta.
- **Autenticazione basata su 802.1X**: l'autenticazione 802.1X è l'unico metodo di autenticazione eseguito sulla porta.
- **Autenticazione basata su MAC**: la porta viene autenticata in base all'indirizzo MAC del richiedente. Nella porta è possibile utilizzare le autenticazioni basate solo su MAC 8.

  NOTA Affinché l'autenticazione MAC riesca, il nome utente e la password del richiedente del server RADIUS devono essere l'indirizzo MAC del richiedente. L'indirizzo MAC deve essere in lettere minuscole e deve essere inserito senza i separatori ":" o "-". Ad esempio: 0020aa00bbcc.
- **Autenticazione basata su Web**: disponibile solo in modalità switch Livello 2. Selezionare questa opzione per attivare l'autenticazione basata su Web sullo switch.
- **Riautenticazione periodica**: selezionare per attivare i tentativi di riautenticazione della porta dopo il Periodo di riautenticazione specificato.
- **Periodo di riautenticazione**: immettere dopo quanti secondi la porta selezionata viene riautenticata.

- **Riautentica ora**: selezionare per attivare la riautenticazione immediata della porta.
- **Stato dell'autenticatore**: viene visualizzato lo stato di autorizzazione della porta definita. Sono disponibili le seguenti opzioni:
  - *Inizializza*: in corso di attivazione.
  - *Imposizione autorizzata*: lo stato delle porte controllate è impostato su Imposizione autorizzata (il traffico viene inoltrato).
  - *Imposizione non autorizzata*: lo stato delle porte controllate è impostato su Imposizione non autorizzata (il traffico viene respinto).

    NOTA Se la porta non è in stato Imposizione autorizzata o Imposizione non autorizzata, allora è in modalità Automatico e l'autenticatore visualizza lo stato di autenticazione in corso. Autenticata la porta, lo stato viene mostrato come Autenticato.
- **Intervallo di tempo**: attivare un limite di tempo per il quale la porta specifica è autorizzata all'utilizzo se è stato attivato 802.1x (opzione Autenticazione basata su porte selezionata).
- **Nome intervallo di tempo**: selezionare il profilo che specifica l'intervallo di tempo.
- **N. max di tentativi di accesso a WBA**: disponibile solo in modalità switch Livello 2. Immettere il numero massimo di tentativi di accesso consentito nell'interfaccia. Selezionare **Infinito** se non si desidera impostare alcun limite o **Definito dall'utente** per impostare un limite.
- **Periodo massimo di silenzio WBA**: disponibile solo in modalità switch Livello 2. Immettere la durata massima del periodo di silenzio consentito nell'interfaccia. Selezionare **Infinito** se non si desidera impostare alcun limite o **Definito dall'utente** per impostare un limite.
- **Numero massimo di host**: immettere il numero massimo di host autorizzati consentiti nell'interfaccia. Selezionare **Infinito** se non si desidera impostare alcun limite o **Definito dall'utente** per impostare un limite.

  NOTA Impostare questo valore su 1 per simulare la modalità host singolo per l'autenticazione basata su Web in modalità multisessione.
- **Periodo di inattività**: immettere l'intervallo (in secondi) durante il quale il dispositivo rimane in stato di inattività dopo uno scambio di autenticazione non riuscito.

- **Reinvio di EAP**: immettere l'intervallo (in secondi) durante il quale il dispositivo attende una risposta a un frame di richiesta/identità EAP (Extensible Authentication Protocol) dal richiedente (client) prima di inviare nuovamente la richiesta.
- **Richieste EAP max**: immettere il numero massimo di richieste EAP che è possibile inviare. Se non si riceve una risposta entro l'intervallo di tempo definito (timeout richiedente), il processo di autenticazione verrà riavviato.
- **Timeout richiedente**: immettere quanti secondi devono trascorrere prima che le richieste EAP vengano nuovamente inviate al richiedente.
- **Timeout server**: immettere l'intervallo (in secondi) che deve trascorrere prima che il dispositivo invii nuovamente la richiesta al server di autenticazione.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni della porta vengono scritte nel file Configurazione di esecuzione.

Definizione autenticazione host e sessione

La pagina Autenticazione host e sessione consente di definire la modalità di funzionamento di 802.1X sulla porta e l'azione da eseguire se viene rilevata una violazione.

Per la descrizione di queste modalità, consultare **Modalità host della porta**.

Per definire le impostazioni avanzate 802.1X delle porte, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Autenticazione 802.1X/MAC/Web** > **Autenticazione host e sessione**.

I parametri di autenticazione 802.1X vengono descritti per tutte le porte. Nella pagina Modifica autenticazione host e sessione vengono descritti tutti i campi tranne i seguenti.

- **Numero di violazioni di host singoli**: visualizza il numero di pacchetti che arrivano nell'interfaccia in modalità host singolo da un host il cui indirizzo MAC è diverso da quello del richiedente.

PASSAGGIO 2 Selezionare una porta e fare clic su **Modifica.**

PASSAGGIO 3 Immettere i parametri.

- **Interfaccia**: immettere un numero di porta per cui l'autenticazione host è attivata.
- **Autenticazione host**: selezionare una delle modalità. Queste modalità sono descritte precedentemente nella sezione **Modalità host della porta**.

  I campi seguenti sono rilevanti soltanto se si seleziona l'opzione Singolo nel campo Autenticazione host.

Impostazioni violazione host singolo:

- **Intervento per violazione**: selezionare l'azione da applicare ai pacchetti che arrivano in modalità Sessione singola/Host singolo da un host il cui indirizzo MAC è diverso da quello del richiedente. Sono disponibili le seguenti opzioni:
  - *Proteggi (elimina)*: i pacchetti vengono eliminati.
  - *Limita (inoltra)*: i pacchetti vengono inoltrati.
  - *Arresta*: i pacchetti vengono eliminati e la porta viene arrestata. La porta rimane in questo stato finché non viene riattivata o finché il dispositivo non viene riavviato.
- **Trap** (su violazione host singolo): selezionare per attivare le trap.
- **Frequenza trap (su violazione host singolo)**: specifica la frequenza di invio delle trap all'host. Questo campo è disponibile solo se sono stati attivati più host.
- **Numero di violazioni**: mostra gli errori di numero (numero di pacchetti in modalità Sessione singola/Host singolo, da un host il cui indirizzo MAC è diverso da quello del richiedente).

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni vengono scritte nel file Configurazione di esecuzione.

Visualizzazione di host autenticati

Per visualizzare i dettagli sugli utenti autenticati, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Autenticazione 802.1X/MAC/Web** > **Host autenticati**.

In questa pagina vengono visualizzati i seguenti campi:

- **Nome utente**: i nomi dei richiedenti che sono stati autenticati su ogni porta.
- **Porta**: numero della porta.
- **Ora della sessione (GG:HH:MM:SS)**: durata della connessione del richiedente alla porta.
- **Metodo di autenticazione**: metodo di autenticazione dell'ultima sessione.
- **Server di autenticazione**: server RADIUS.
- **Indirizzo MAC**: visualizza l'indirizzo MAC del richiedente.
- **ID VLAN**: VLAN della porta.

Client bloccati

Per visualizzare i client che sono stati bloccati a causa di tentativi di accesso non riusciti e per sbloccare un client bloccato:

PASSAGGIO 1 Fare clic su **Protezione** > **Autenticazione 802.1X/MAC/Web**> **Client bloccato**.

Vengono visualizzati i seguenti campi:

- **Interfaccia**: la porta bloccata.
- **Indirizzo MAC**: viene visualizzato lo stato di autorizzazione della porta corrente. Se lo stato è *Autorizzato*, la porta è autenticata o il *Controllo porta amministrativa* è *Imposizione autorizzata*. Viceversa, se lo stato è *Non autorizzato*, la porta non è autenticata o il *Controllo porta amministrativa* è *Imposizione non autorizzata*.
- **Tempo rimanente (sec)**: il tempo rimanente prima che la porta venga bloccata.

PASSAGGIO 2 Selezionare una porta.

PASSAGGIO 3 Fare clic su **Sblocca**.

Personalizzazione dell'autenticazione Web

Da questa pagina è possibile realizzare le pagine di autenticazione basata sul Web in varie lingue.

È possibile aggiungere fino a 4 lingue.

NOTA L'autenticazione basata su Web può essere richiesta contemporaneamente da un massimo di cinque utenti HTTP e un utente HTTPS. Una volta autenticati questi utenti, anche altri utenti possono richiedere l'autenticazione.

Per aggiungere una lingua per l'autenticazione basata su Web, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Autenticazione 802.1X/MAC/Web**> **Personalizzazione dell'autenticazione Web**.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Selezionare la lingua dall'elenco a discesa **Lingua**.

PASSAGGIO 4 Se la lingua scelta è la lingua predefinita, selezionare **Imposta come lingua display predefinita**. Se l'utente finale non seleziona una lingua, le pagine vengono visualizzate nella lingua predefinita.

PASSAGGIO 5 Facendo clic su **Applica**, le impostazioni vengono salvate nel file Configurazione di esecuzione.

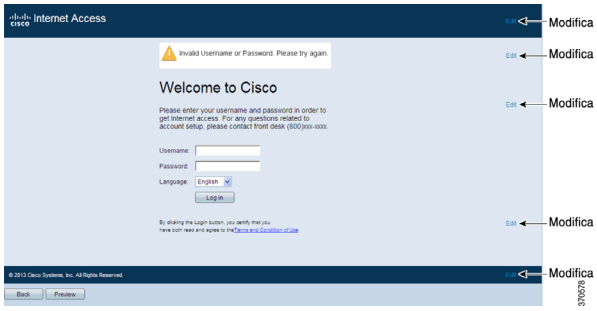
Per personalizzare le pagine di autenticazione Web, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Autenticazione 802.1X/MAC/Web**> **Personalizzazione dell'autenticazione Web.**

In questa pagina vengono visualizzate le lingue che possono essere personalizzate.

PASSAGGIO 2 Fare clic su **Modifica pagina di accesso**.

Figura 4 Viene visualizzata la seguente pagina:



PASSAGGIO 3 Fare clic su **Modifica1**. Vengono visualizzati i seguenti campi:

- **Lingua**: viene visualizzata la lingua della pagina.
- **Schema colori**: consente di selezionare una delle opzioni di contrasto.

  Se si seleziona lo schema di colori **personalizzato**, sono disponibili le seguenti opzioni:

  - *Colore sfondo pagina*: immettere il codice ASCII del colore di sfondo. Il colore selezionato viene visualizzato nel campo Testo.
  - *Colore sfondo intestazione e piè di pagina*: immettere il codice ASCII del colore di sfondo dell'intestazione e del piè di pagina. Il colore selezionato viene visualizzato nel campo Testo.
  - *Colore testo intestazione e piè di pagina*: immettere il codice ASCII del colore del testo dell'intestazione e del piè di pagina. Il colore selezionato viene visualizzato nel campo Testo.
  - *Colore colleg. ipertestuale*: immettere il codice ASCII del colore del collegamento ipertestuale. Il colore selezionato viene visualizzato nel campo Testo.
- **Immagine logo attuale**: consente di selezionare una delle seguenti opzioni:
  - *Nessuno*: nessun logo.
  - *Predefinito*: utilizzare il logo predefinito.
  - *Altro*: selezionare questa opzione per inserire un logo personalizzato.

  Se si seleziona l'opzione logo **Altro**, sono disponibili le seguenti opzioni:

  - *Nome del file di immagine logo*: immettere il nome del file del logo oppure **sfogliare** per recuperare l'immagine.
  - *Testo dell'applicazione*: immettere il testo da allegare al logo.

- *Testo titolo della finestra*: immettere un titolo per la pagina di accesso.

PASSAGGIO 4 Facendo clic su **Applica**, le impostazioni vengono salvate nel file Configurazione di esecuzione.

PASSAGGIO 5 Fare clic su **Modifica2**. Vengono visualizzati i seguenti campi:

- **Credenziali utente non valide**: consente di immettere il testo del messaggio da visualizzare quando l'utente finale immette un nome utente o una password non validi.
- **Servizio non disponibile**: consente di immettere il testo del messaggio da visualizzare quando il servizio di autenticazione non è disponibile.

PASSAGGIO 6 Facendo clic su **Applica**, le impostazioni vengono salvate nel file Configurazione di esecuzione.

PASSAGGIO 7 Fare clic su **Modifica3**. Vengono visualizzati i seguenti campi:

- **Messaggio di benvenuto**: consente di immettere il testo del messaggio da visualizzare quando l'utente finale esegue l'accesso.
- **Messaggio informativo**: consente di immettere le istruzioni che devono essere visualizzate dall'utente finale.
- **Autenticazione RADIUS**: indica se l'autenticazione RADIUS è attiva. In caso affermativo, il nome utente e la password devono essere inclusi nella pagina di accesso.
- **Casella di testo Nome utente**: consente di selezionare la casella di testo corrispondente al nome utente da visualizzare.
- **Etichetta casella di testo Nome utente**: consente di selezionare l'etichetta da visualizzare prima della casella di testo corrispondente al nome utente.
- **Casella di testo Password**: consente di selezionare la casella di testo corrispondente alla password da visualizzare.
- **Etichetta casella di testo Password**: consente di selezionare l'etichetta da visualizzare prima della casella di testo corrispondente alla password.
- **Selezione della lingua**: selezionare questa opzione per consentire all'utente finale di scegliere una lingua.
- **Etichetta elenco a discesa Lingua**: consente di immettere l'etichetta dell'elenco a discesa di selezione della lingua.
- **Etichetta pulsante Accedi**: consente di immettere l'etichetta del pulsante di accesso.

- **Etichetta avanzamento accesso**: consente di immettere il testo che verrà visualizzato durante la procedura di accesso.

PASSAGGIO 8 Facendo clic su **Applica**, le impostazioni vengono salvate nel file Configurazione di esecuzione.

PASSAGGIO 9 Fare clic su **Modifica4**. Vengono visualizzati i seguenti campi:

- **Termini e condizioni**: selezionare questa opzione per abilitare la casella di testo con termini e condizioni.
- **Avviso termini e condizioni**: consente di immettere il testo del messaggio da visualizzare per fornire indicazioni su come immettere i termini e le condizioni.
- **Contenuto Termini e condizioni**: consente di immettere il testo del messaggio da visualizzare come termini e condizioni.

PASSAGGIO 10 Facendo clic su **Applica**, le impostazioni vengono salvate nel file Configurazione di esecuzione.

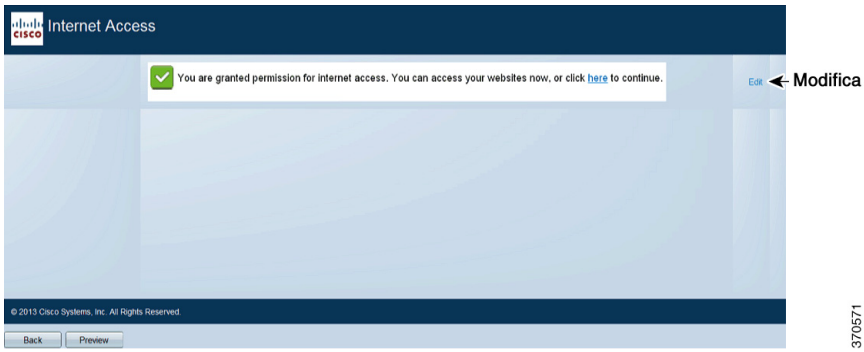
PASSAGGIO 11 **Modifica5**. Vengono visualizzati i seguenti campi:

- **Copyright**: selezionare questa opzione per attivare la visualizzazione del testo del copyright.
- **Testo copyright**: consente di immettere il testo del copyright.

PASSAGGIO 12 Facendo clic su **Applica**, le impostazioni vengono salvate nel file Configurazione di esecuzione.

PASSAGGIO 13 Fare clic su **Modifica pagina oper. riuscita**.

Figura 5 Viene visualizzata la seguente pagina:



PASSAGGIO 14 Fare clic sul pulsante **Modifica** sul lato destro della pagina.

PASSAGGIO 15 Immettere il **messaggio di operazione riuscita**, cioè il testo visualizzato dall'utente una volta eseguito l'accesso.

PASSAGGIO 16 Facendo clic su **Applica**, le impostazioni vengono salvate nel file Configurazione di esecuzione.

Per visualizzare in anteprima il messaggio di operazione riuscita o di accesso, fare clic su **Anteprima**.

Per impostare una delle lingue come lingua predefinita, fare clic su **Imposta lingua display predefinita**.

Definizione degli intervalli di tempo

Per la descrizione di questa funzionalità vedere **Intervallo di tempo**.

Supporto modalità porta e metodo di autenticazione

Nella tabella di seguito vengono riportate le combinazioni di modalità della porta e metodo di autenticazione supportate.

Metodo di autenticazione	Host singolo	Host multipli	Multisessione	
			Dispositivo in Livello 3	Dispositivo in Livello 2
802.1x	†	†	†	†
MAC	†	†	†	†
WEB	N/S	N/S	N/S	†

Legenda:

†: la modalità della porta supporta anche l'assegnazione della VLAN RADIUS e della VLAN ospite.

N/S: il metodo di autenticazione non supporta la modalità della porta.

NOTA L'autenticazione basata su Web richiede un supporto TCAM per la classificazione del traffico di input ed è supportata solo dalla modalità multisessione completa. È possibile simulare la modalità host singolo impostando il parametro Numero massimo di host su 1 nella pagina Autenticazione porta.

Funzionamento modalità

Nella tabella di seguito è mostrato come viene gestito il traffico, autenticato e non, in varie situazioni.

	Traffico non autenticato				Traffico autenticato			
	Con VLAN ospite		Senza VLAN ospite		Con VLAN RADIUS		Senza VLAN RADIUS	
	Senza tag	Con tag	Senza tag	Con tag	Senza tag	Con tag	Senza tag	Con tag
Host singolo	I frame vengono riassociati alla VLAN ospite	I frame vengono eliminati a meno che non appartengano alla VLAN ospite o alle VLAN non autenticate	I frame vengono eliminati	I frame vengono eliminati a meno che non appartengano alle VLAN non autenticate	I frame vengono riassociati alla VLAN assegnata da RADIUS	I frame vengono eliminati a meno che non appartengano alla VLAN RADIUS o alle VLAN non autenticate	I frame vengono collegati in base alla configurazione VLAN statica	I frame vengono collegati in base alla configurazione VLAN statica
Host multipli	I frame vengono riassociati alla VLAN ospite	I frame vengono eliminati a meno che non appartengano alla VLAN ospite o alle VLAN non autenticate	I frame vengono eliminati	I frame vengono eliminati a meno che non appartengano alle VLAN non autenticate	I frame vengono riassociati alla VLAN assegnata da RADIUS	I frame vengono eliminati a meno che non appartengano alla VLAN RADIUS o alle VLAN non autenticate	I frame vengono collegati in base alla configurazione VLAN statica	I frame vengono collegati in base alla configurazione VLAN statica

	Traffico non autenticato				Traffico autenticato			
	Con VLAN ospite		Senza VLAN ospite		Con VLAN RADIUS		Senza VLAN RADIUS	
	Senza tag	Con tag	Senza tag	Con tag	Senza tag	Con tag	Senza tag	Con tag
Multisessioni parziali	N/S	N/S	I frame vengono eliminati	I frame vengono eliminati a meno che non appartengano alle VLAN non autenticate	N/S	N/S	I frame vengono collegati in base alla configurazione VLAN statica	I frame vengono collegati in base alla configurazione VLAN statica
Multisessioni complete	I frame vengono riassociati alla VLAN ospite	I frame vengono riassociati alla VLAN ospite a meno che non appartengano alle VLAN non autenticate	I frame vengono eliminati	I frame vengono eliminati a meno che non appartengano alle VLAN non autenticate	I frame vengono riassociati alla VLAN assegnata da RADIUS	I frame vengono riassociati alla VLAN RADIUS a meno che non appartengano alle VLAN non autenticate	I frame vengono collegati in base alla configurazione VLAN statica	I frame vengono collegati in base alla configurazione VLAN statica

23

Protezione: protezione primo hop IPV6

In questa sezione viene illustrato il funzionamento di Protezione primo hop (FHS) e come effettuare la configurazione nell'interfaccia utente.

Vengono trattati i seguenti argomenti:

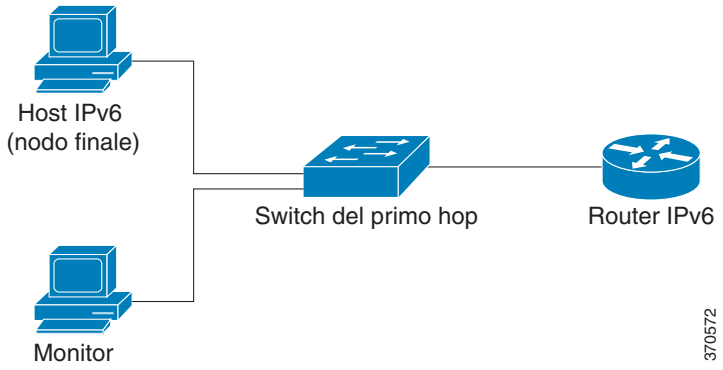
- **Panoramica su Protezione primo hop**
- **Guardia annuncio router**
- **Esame di rilevamento router adiacente**
- **Guardia DHCPv6**
- **Integrità binding dei router adiacenti**
- **Protezione da attacchi**
- **Criteri, parametri globali e impostazioni predefinite del sistema**
- **Attività comuni**
- **Impostazioni predefinite e configurazione**
- **Operazioni preliminari**
- **Configurazione di Protezione primo hop tramite interfaccia utente Web**

Panoramica su Protezione primo hop

FHS IPv6 è una suite di funzioni ideate per proteggere le operazioni dei collegamenti in una rete con IPv6 attivato. Si basa su protocollo NDP (Neighbor Discovery Protocol) e messaggi DHCPv6.

In questa funzione, uno switch di Livello 2 (come illustrato nella **Figura 6**) filtra i messaggi NDP, i messaggi DHCPv6 e i messaggi dei dati utente secondo un numero di regole diverse.

Figura 6 Configurazione di Protezione primo hop



Un'istanza separata e indipendente di Protezione primo hop IPv6 viene eseguita su ogni VLAN su cui è attivata la funzione.

Abbreviazioni

Nome	Descrizione
Messaggio CPA	Messaggio di annuncio percorso certificazione (Certification Path Advertisement)
Messaggio CPS	Messaggio di richiesta percorso certificazione (Certification Path Solicitation)
Messaggio DAD-NS	Messaggio di rilevamento indirizzo duplicato (Duplicate Address Detection) - richiesta router adiacente (Neighbor Solicitation)
FCFS-SAVI	Criterio di evasione in ordine cronologico (First Come First Served) - miglioramento convalida indirizzo origine (Source Address Validation Improvement)

Nome	Descrizione
Messaggio NA	Messaggio di annuncio router adiacente (Neighbor Advertisement)
NDP	Protocollo rilevamento router adiacente (Neighbor Discovery Protocol)
Messaggio NS	Messaggio di richiesta router adiacente (Neighbor Solicitation)
Messaggio RA	Messaggio di annuncio router (Router Advertisement)
Messaggio RS	Messaggio di richiesta router (Router Solicitation)
SAVI	Miglioramento convalida indirizzo origine (Source Address Validation Improvement)

Componenti di Protezione primo hop IPv6

Protezione primo hop IPv6 include le seguenti funzioni:

- Common Protezione primo hop IPv6
- Guardia RA
- Esame di ND
- Integrità binding dei router adiacenti
- Guardia DHCPv6

Questi componenti possono essere attivati o disattivati sulle VLAN.

Esistono due criteri vuoti e predefiniti per ciascuna funzione con i seguenti nomi: vlan_default e port_default. Il primo è associato a ciascuna VLAN non collegata a un criterio definito dall'utente, mentre il secondo è associato a ciascuna interfaccia e VLAN non collegata a un a criterio definito dall'utente. Questi criteri non possono essere associati esplicitamente dall'utente. Vedere **Criteri, parametri globali e impostazioni predefinite del sistema**.

Pipe Protezione primo hop IPv6

Se Protezione primo hop IPv6 è attivato su una VLAN, lo switch esegue il trapping dei seguenti messaggi:

- Messaggi RA (Router Advertisement)
- Messaggi RS (Router Solicitation)
- Messaggi NA (Neighbor Advertisement)
- Messaggi NS (Neighbor Solicitation)
- Messaggi di reindirizzamento ICMPv6
- Messaggi CPA (Certification Path Advertisement)
- Messaggi CPS (Certification Path Solicitation)
- Messaggi DHCPv6

I messaggi sottoposti a trap RA, CPA e reindirizzamento ICMPv6 vengono trasmessi alla funzione Guardia RA. Guardia RA convalida questi messaggi, elimina i messaggi non validi e trasmette i messaggi validi alla funzione Esame di ND.

Esame di ND convalida questi messaggi, elimina i messaggi non validi e trasmette i messaggi validi alla funzione Guardia origine IPv6.

I messaggi DHCPv6 sottoposti a trap vengono trasmessi alla funzione Guardia DHCPv6. Guardia DHCPv6 convalida questi messaggi, elimina i messaggi non validi e trasmette i messaggi validi alla funzione Guardia origine IPv6.

I messaggi dei dati sottoposti a trap vengono trasmessi alla funzione Guardia origine DHCPv6. Guardia origine DHCPv6 convalida i messaggi ricevuti (messaggi dei dati sottoposti a trap, messaggi NDP da Esame di ND e messaggi DHCPv6 da Guardia DHCPv6) tramite l'utilizzo della tabella di binding dei router adiacenti, elimina i messaggi non validi e trasmette quelli validi per l'inoltro.

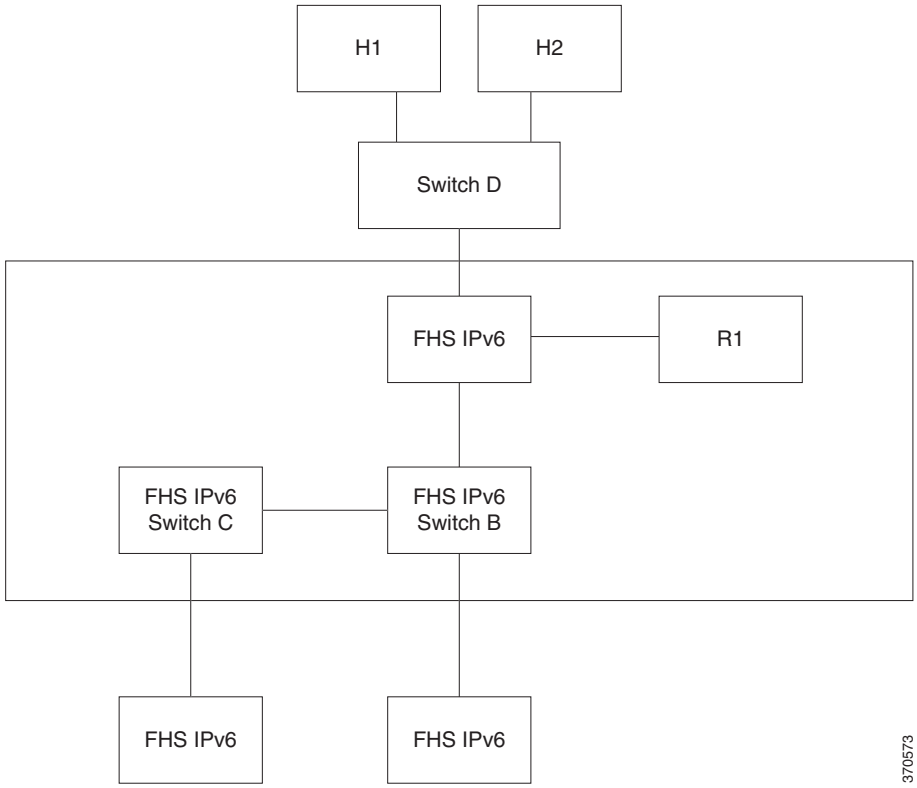
Integrità binding dei router adiacenti scopre i router adiacenti dai messaggi ricevuti (messaggi NDP e DHCPv6) e li memorizza nella tabella di binding dei router adiacenti. Inoltre, le voci statiche possono essere aggiunte manualmente. Dopo aver rilevato gli indirizzi, la funzione NBI trasmette i frame per l'inoltro.

Anche i messaggi sottoposti a trap RS, CPS e NA vengono trasmessi alla funzione Esame di ND. Esame di ND convalida questi messaggi, elimina i messaggi non validi e trasmette i messaggi validi alla funzione Guardia origine IPv6.

Perimetro di Protezione primo hop IPv6

Gli switch di Protezione primo hop IPv6 possono formare un perimetro separando un'area non attendibile da una attendibile. Tutti gli switch all'interno del perimetro supportano Protezione primo hop IPv6, mentre gli host e i router all'interno di questo perimetro sono dispositivi attendibili. Ad esempio, i collegamenti SwitchC-H3, SwitchB-H4 e SwitchA-SwitchD nella **Figura 7** formano il perimetro, mentre i collegamenti SwitchA-SwitchB, SwitchB-SwitchC e SwitchA-R1 sono collegamenti interni, all'interno dell'area protetta.

Figura 7 Perimetro di Protezione primo hop IPv6



Il comando **ruolo-dispositivo** nella schermata di configurazione dei criteri binding dei router adiacenti specifica il perimetro.

Ogni switch di Protezione primo hop IPv6 stabilisce il binding dei router adiacenti ripartiti dall'edge. In questo modo, le voci di binding vengono distribuite sui dispositivi di Protezione primo hop IPv6 che formano il perimetro. I dispositivi di Protezione primo hop IPv6 possono quindi fornire l'integrità binding all'interno del perimetro, senza impostare binding per tutti gli indirizzi su ogni dispositivo.

Guardia annuncio router

Guardia RA (Router Advertisement, annuncio router) è la prima funzione di FHS che tratta i messaggi RA sottoposti a trap. Guardia RA supporta le seguenti funzioni:

- Filtro dei messaggi di reindirizzamento ICMPv6, CPA e RA ricevuti.
- Convalida dei messaggi RA ricevuti.

Filtro dei messaggi di reindirizzamento IPCMv6, CPA e RA ricevuti.

Guardia RA elimina i messaggi RA e CPA ricevuti sulle interfacce i cui ruoli non sono router. Il ruolo interfaccia è configurato in Protezione > Protezione primo hop IPv6 > Impostazioni Guardia RA.

Convalida dei messaggi RA

Guardia RA convalida i messaggi RA utilizzando i filtri basati sui criteri di Guardia RA associati all'interfaccia. Tali criteri possono essere configurati nella pagina Impostazioni Guardia RA.

Se un messaggio non supera la verifica, viene eliminato. Se la configurazione per l'eliminazione dei pacchetti di accesso sul componente comune FHS è attiva, viene inviato un messaggio SYSLOG con limite di velocità.

Esame di rilevamento router adiacente

Esame di ND (Neighbor Discovery, rilevamento router adiacente) supporta le seguenti funzioni:

- Convalida dei messaggi NDP ricevuti.
- Filtri in uscita

Convalida messaggio

Esame di ND convalida i messaggi NDP, in base a un criterio Esame di ND associato all'interfaccia. Tale criterio può essere definito nella pagina Impostazioni Esame di ND.

Se un messaggio non supera la verifica definita nel criterio, viene eliminato e viene inviato un messaggio SYSLOG con limite di velocità.

Filtri in uscita

Esame di ND blocca l'inoltro dei messaggi RS e CPS sulle interfacce configurate come interfacce host.

Guardia DHCPv6

Guardia DHCPv6 tratta i messaggi DHCPv6 sottoposti a trap. Guardia DHCPv6 supporta le seguenti funzioni:

- Filtro dei messaggi DHCPv6 ricevuti.

  Guardia DHCP elimina i messaggi di risposta DHCPv6 ricevuti sull'interfaccia il cui ruolo è client. Il ruolo interfaccia è configurato nella pagina Impostazioni Guardia DHCP.

- Convalida dei messaggi DHCPv6 ricevuti.

  Guardia DHCPv6 convalida i messaggi DHCPv6 che corrispondono ai filtri basati sui criteri di Guardia DHCPv6 associati all'interfaccia.

Se un messaggio non supera la verifica, viene eliminato. Se la configurazione per l'eliminazione dei pacchetti di accesso sul componente comune FHS è attiva, viene inviato un messaggio SYSLOG con limite di velocità.

Integrità binding dei router adiacenti

Integrità NB (Neighbor Binding, binding dei router adiacenti) determina il binding dei router adiacenti.

Un'istanza separata e indipendente di Integrità NB viene eseguita su ogni VLAN su cui è attivata la funzione.

Rilevamento dei prefissi IPv6 dichiarati

Integrità NB rileva i prefissi IPv6 dichiarati nei messaggi RA e li salva nella tabella Prefissi router adiacenti. I prefissi vengono utilizzati per verificare gli indirizzi IPv6 globali assegnati.

Per impostazione predefinita, questa convalida è disattivata. Quando è disattivata, gli indirizzi vengono confrontati con i prefissi nella pagina Impostazioni binding router adiacenti.

I prefissi statici utilizzati per la convalida degli indirizzi possono essere aggiunti alla pagina della tabella di binding dei router adiacenti.

Overflow tabella di binding dei router adiacenti

Quando non c'è spazio libero a disposizione per creare una nuova voce, la nuova voce annulla quella con l'ora di creazione più recente.

Creazione di binding dei router adiacenti

Uno switch Protezione primo hop IPv6 può rilevare e registrare informazioni di binding utilizzando i seguenti metodi:

- **Metodo NBI-NDP**: rilevamento degli indirizzi IPv6 dai messaggi NDP sottoposti a snooping
- **Metodo NBI-manuale:** tramite configurazione manuale

Un indirizzo IPv6 è associato a una proprietà di livello di collegamento dell'allegato di rete dell'host. Questa proprietà, denominata "ancoraggio binding", è costituita dall'identificatore di interfaccia (ifIndex) tramite il quale l'host è connesso e dall'indirizzo MAC dell'host.

Lo switch Protezione primo hop IPv6 stabilisce il binding solo su interfacce perimetrali (vedere **Perimetro di Protezione primo hop IPv6**).

Le informazioni di binding vengono salvate nella tabella di binding dei router adiacenti.

Metodo NBI-NDP

Il metodo NBI-NDP utilizzato si basa sul metodo FCFS- SAVI specificato in RFC6620, con le seguenti differenze:

- A differenza di FCFS-SAVI, che supporta soltanto il binding degli indirizzi IPv6 locale collegamento, NBI-NDP supporta anche il binding degli indirizzi IPv6 globali.
- NBI-NDP supporta il binding degli indirizzi IPv6 solo per gli indirizzi IPv6 acquisiti dai messaggi NDP. La convalida degli indirizzi di origine per i messaggi di dati viene fornita da Guardia indirizzo di origine IPv6.
- In NBI-NDP, la prova della proprietà dell'indirizzo si basa sul principio di evasione in ordine cronologico. Il primo host che reclama un certo indirizzo origine ne sarà il titolare fino a ulteriore notifica. Poiché non sono accettabili modifiche dell'host, è necessario trovare un modo per confermare la titolarità dell'indirizzo senza richiedere un nuovo protocollo. Per questo motivo, ogni volta che un indirizzo IPv6 viene acquisito per la prima volta da un messaggio NDP, lo switch lo associa all'interfaccia. Perciò i messaggi NDP contenenti questo indirizzo IPv6 possono essere confrontati con lo stesso ancoraggio binding per verificare che l'indirizzo IP di origine appartenga alla stessa origine.

  L'eccezione a questa regola ha luogo quando un host IPv6 esegue il roaming nel dominio L2 o modifica il suo indirizzo MAC. In questo caso, l'host continua a essere il titolare dell'indirizzo IP, ma l'ancoraggio binding associato potrebbe essere cambiato. Per affrontare tale situazione, il comportamento NBI-NDP definito implica l'invio di messaggi DAD-NS alla interfaccia binding precedente per verificare se l'host è ancora raggiungibile. Se l'host non è più raggiungibile presso l'ancoraggio binding precedentemente registrato, NBI-NDP suppone che il nuovo ancoraggio sia valido e modifica l'ancoraggio binding. Se l'host è ancora raggiungibile con il precedente ancoraggio binding registrato, l'interfaccia binding non viene modificata.

Per ridurre le dimensioni della tabella di binding dei router adiacenti, NBI-NDP stabilisce il binding solo sulle interfacce perimetrali (vedere Perimetro di Protezione primo hop IPv6) e distribuisce le informazioni di binding attraverso le interfacce interne utilizzando i messaggi NS e NA. Prima di creare un binding locale NBI-NDP, il dispositivo invia un messaggio DAD-NS per richiedere l'indirizzo in questione. Se un host risponde al messaggio con un messaggio NA, il dispositivo che ha inviato il messaggio DAD-NS desume che esista un binding per quell'indirizzo in un altro dispositivo e, quindi, non crea un binding locale. Se non vengono ricevuti messaggi NA come riposta al messaggio DAD-NS, il dispositivo locale desume che non esista binding per quell'indirizzo in altri dispositivi e, quindi, crea il binding locale.

NBI-NDP supporta a timer a vita. Un valore del timer può essere configurato nella pagina Impostazioni binding router adiacenti. Il timer viene riavviato ogni volta che l'indirizzo IPv6 associato viene confermato. Se il timer scade, il dispositivo invia fino a due messaggi DAD-NS con brevi intervalli per verificare il router adiacente.

Criterio di integrità NB

Così come per le altre funzioni di Protezione primo hop IPv6, il comportamento di Integrità NB su un'interfaccia viene specificato da un criterio di Integrità NB associato a un'interfaccia. Tali criteri vengono configurati nella pagina Impostazioni binding router adiacenti.

Protezione da attacchi

In questa sezione viene descritta la protezione da attacchi fornita da Protezione primo hop IPv6.

Protezione contro lo spoofing del router IPv6

Un host IPv6 può utilizzare i messaggi RA ricevuti per:

- Rilevare router IPv6
- Configurare automaticamente l'indirizzo stateless

Un host dannoso potrebbe inviare messaggi RA annunciandosi come router IPv6 e fornendo prefissi contraffatti per la configurazione di indirizzi stateless.

Guardia RA fornisce protezione contro tali attacchi configurando il ruolo interfaccia come interfaccia host per tutte le interfacce in cui i router IPv6 non possono connettersi.

Protezione contro lo spoofing della risoluzione dell'indirizzo IPv6

Un host dannoso potrebbe inviare messaggi NA annunciandosi come host IPv6 dotato dell'indirizzo IPv6 fornito.

Integrità NB fornisce protezione contro tali attacchi nei seguenti modi:

- Se l'indirizzo IPv6 fornito è sconosciuto, il messaggio NS viene inoltrato esclusivamente sulle interfacce interne.
- Se l'indirizzo IPv6 fornito è noto, il messaggio NS viene inoltrato esclusivamente sull'interfaccia alla quale è associato l'indirizzo IPv6.
- Un messaggio NA viene eliminato se l'indirizzo IPv6 di destinazione è associato a un'altra interfaccia.

Protezione contro lo spoofing del rilevamento indirizzo duplicato IPv6

Un host IPv6 deve eseguire il rilevamento indirizzo duplicato per ogni indirizzo IPv6 assegnato inviando uno messaggio NS speciale: messaggio di rilevamento indirizzo duplicato - richiesta router adiacente (DAD_NS).

Un host dannoso potrebbe inviare una risposta a un messaggio DAD_RS annunciandosi come host IPv6 dotato dell'indirizzo IPv6 fornito.

Integrità NB fornisce protezione contro tali attacchi nei seguenti modi:

- Se l'indirizzo IPv6 fornito è sconosciuto, il messaggio DAD_NS viene inoltrato esclusivamente sulle interfacce interne.
- Se l'indirizzo IPv6 fornito è noto, il messaggio DAD_NS viene inoltrato esclusivamente sull'interfaccia alla quale è associato l'indirizzo IPv6.
- Un messaggio NA viene eliminato se l'indirizzo IPv6 di destinazione è associato a un'altra interfaccia.

Protezione contro lo spoofing del server DHCPv6

Un host IPv6 può utilizzare il protocollo DHCPv6 per:

- Configurare informazioni stateless
- Configurare indirizzi stateful

Un host dannoso potrebbe inviare messaggi di risposta DHCPv6 annunciandosi come server DHCPv6 e fornendo informazioni stateless e indirizzi IPv6 contraffatti. Guardia DHCPv6 fornisce protezione contro tali attacchi configurando il ruolo interfaccia come porta client per tutte le porte a cui i server DHCPv6 non possono connettersi.

Protezione contro lo spoofing della cache NBD

Un router IPv6 supporta la cache del protocollo NDP che associa l'indirizzo IPv6 all'indirizzo MAC per il routing dell'ultimo hop.

Un host dannoso potrebbe inviare messaggi IPv6 con un indirizzo IPv6 di destinazione diverso per l'inoltro dell'ultimo hop, causando l'overflow della cache NBD.

Un meccanismo incorporato nell'implementazione NDP, che limita il numero di voci consentite nello stato INCOMPLETO nella cache di rilevamento dei router adiacenti, fornisce protezione.

Criteri, parametri globali e impostazioni predefinite del sistema

Ogni funzione di FHS può essere attivata o disattivata singolarmente. Nessuna funzione è attiva per impostazione predefinita.

Le funzioni devono essere attivate inizialmente su VLAN specifiche. Quando si attiva una funzione, è possibile definire valori di configurazione globali per le regole di verifica di quella funzione. Se non si definisce un criterio contenente valori diversi per tali regole di verifica, i valori globali vengono utilizzati per applicare la funzione ai pacchetti.

Criteri

I criteri contengono le regole di verifica che vengono eseguite sui pacchetti di ingresso. Possono essere associati alle VLAN, ma anche a porte e LAG. Se la funzione non viene attivata su una VLAN, i criteri non hanno validità.

I criteri possono essere definiti dall'utente o predefiniti (vedere di seguito).

Criteri predefiniti

Per ogni funzione FHS esistono criteri predefiniti vuoti che, per impostazione predefinita, vengono associati a tutte le VLAN e le interfacce. I criteri predefiniti vengono denominati "vlan_default" e "port_default" (per ciascuna funzione):

- È possibile aggiungere regole ai criteri predefiniti, tuttavia non è possibile associare manualmente i criteri predefiniti alle interfacce, perché sono associati per impostazione predefinita.

- I criteri predefiniti non possono mai essere eliminati. È possibile eliminare soltanto la configurazione aggiunta dall'utente.

Criteri definiti dall'utente

È possibile definire criteri diversi da quelli predefiniti.

Quando un criterio definito dall'utente è associato a un'interfaccia, il criterio predefinito per quell'interfaccia viene separato. Se il criterio definito dall'utente viene separato dall'interfaccia, viene associato nuovamente il criterio predefinito.

I criteri non hanno effetto finché:

- La funzione nel criterio non viene attivata sulla VLAN contenente l'interfaccia.
- Il criterio non viene associato all'interfaccia (VLAN, porta o LAG).

Quando viene associato un criterio, il criterio predefinito per l'interfaccia in questione viene separato. Quando si rimuove un criterio dall'interfaccia, viene associato nuovamente il criterio predefinito.

È possibile associare un solo criterio (per una funzione specifica) a una VLAN.

Se specificano VLAN diverse, è possibile associare più criteri (per una funzione specifica) a un'interfaccia.

Livelli delle regole di verifica.

L'insieme finale di regole che si applicano a un pacchetto di ingresso su un'interfaccia è il seguente:

- Le regole configurate nei criteri associati all'interfaccia (porta o LAG) su cui è arrivato il pacchetto vengono aggiunte all'insieme.
- Le regole configurate nel criterio associato alla VLAN vengono aggiunte all'insieme se non sono state aggiunte a livello di porta.
- Le regole globali vengono aggiunte all'insieme se non sono state aggiunte a livello di VLAN o porta.

Le regole definite a livello di porta annullano l'insieme di regole a livello di VLAN. Le regole definite a livello di VLAN annullano le regole configurate globalmente. Le regole configurate globalmente annullano le impostazioni predefinite del sistema.

Attività comuni

Flusso di lavoro comune Protezione primo hop

PASSAGGIO 1 Nella pagina Impostazioni FHS, inserire l'elenco di VLAN su cui è attivata la funzione.

PASSAGGIO 2 Nella stessa pagina, impostare la funzione Accesso eliminazione pacchetti globale.

PASSAGGIO 3 Se richiesto, configurare un criterio definito dall'utente oppure aggiungere regole ai criteri predefiniti per la funzione.

PASSAGGIO 4 Associare il criterio a una VLAN, una porta o un LAG utilizzando la pagina Associazione criteri (VLAN) o Associazione criteri (porta).

Flusso di lavoro Guardia annuncio router

PASSAGGIO 1 Nella pagina Impostazioni Guardia RA, inserire l'elenco di VLAN su cui è attivata la funzione.

PASSAGGIO 2 Nella stessa pagina, impostare i valori di configurazione globali che vengono utilizzati se in un criterio non sono impostati valori.

PASSAGGIO 3 Se richiesto, configurare un criterio definito dall'utente oppure aggiungere regole ai criteri predefiniti per la funzione.

PASSAGGIO 4 Associare il criterio a una VLAN, una porta o un LAG utilizzando la pagina Associazione criteri (VLAN) o Associazione criteri (porta).

Flusso di lavoro Guardia DHCPv6

PASSAGGIO 1 Nella pagina Impostazioni Guardia DHCPv6, inserire l'elenco di VLAN su cui è attivata la funzione.

PASSAGGIO 2 Nella stessa pagina, impostare i valori di configurazione globali che vengono utilizzati se in un criterio non sono impostati valori.

PASSAGGIO 3 Se richiesto, configurare un criterio definito dall'utente oppure aggiungere regole ai criteri predefiniti per la funzione.

PASSAGGIO 4 Associare il criterio a una VLAN, una porta o un LAG utilizzando la pagina Associazione criteri (VLAN) o Associazione criteri (porta).

Flusso di lavoro Esame di rilevamento router adiacente

PASSAGGIO 1 Nella pagina Impostazioni Esame di ND, inserire l'elenco di VLAN su cui è attivata la funzione.

PASSAGGIO 2 Nella stessa pagina, impostare i valori di configurazione globali che vengono utilizzati se in un criterio non sono impostati valori.

PASSAGGIO 3 Se richiesto, configurare un criterio definito dall'utente oppure aggiungere regole ai criteri predefiniti per la funzione.

PASSAGGIO 4 Associare il criterio a una VLAN, una porta o un LAG utilizzando la pagina Associazione criteri (VLAN) o Associazione criteri (porta).

Flusso di lavoro del binding dei router adiacenti

PASSAGGIO 1 Nella pagina Impostazioni binding router adiacenti, inserire l'elenco di VLAN su cui è attivata la funzione.

PASSAGGIO 2 Nella stessa pagina, impostare i valori di configurazione globali che vengono utilizzati se in un criterio non sono impostati valori.

PASSAGGIO 3 Se richiesto, configurare un criterio definito dall'utente oppure aggiungere regole ai criteri predefiniti per la funzione.

PASSAGGIO 4 Aggiungere le eventuali voci manuali richieste nella pagina della tabella di binding dei router adiacenti.

PASSAGGIO 5 Associare il criterio a una VLAN, una porta o un LAG utilizzando la pagina Associazione criteri (VLAN) o Associazione criteri (porta).

Impostazioni predefinite e configurazione

Se Protezione primo hop IPv6 è attivato su una VLAN, lo switch esegue per impostazione predefinita il trapping dei seguenti messaggi:

- Messaggi RA (Router Advertisement)
- Messaggi RS (Router Solicitation)

- Messaggi NA (Neighbor Advertisement)
- Messaggi NS (Neighbor Solicitation)
- Messaggi di reindirizzamento ICMPv6
- Messaggi CPA (Certification Path Advertisement)
- Messaggi CPS (Certification Path Solicitation)
- Messaggi DHCPv6

Le funzioni di FHS sono disattivate per impostazione predefinita.

Operazioni preliminari

Nessuna attività preliminare richiesta.

Configurazione di Protezione primo hop tramite interfaccia utente Web

Impostazioni Common FHS

Utilizzare la pagina Impostazioni FHS per attivare la funzione Common FHS su un gruppo specifico di VLAN e per impostare il valore di configurazione globale per accedere all'eliminazione dei pacchetti. Se necessario, è possibile aggiungere un criterio oppure aggiungere l'accesso per l'eliminazione dei pacchetti al criterio predefinito stabilito dal sistema.

Per configurare Common Protezione primo hop su porte o LAG:

PASSAGGIO 1 Fare clic su **Protezione** > **Protezione primo hop** > **Impostazioni FHS**.

PASSAGGIO 2 Compilare i seguenti campi di configurazione globale:

- **Elenco VLAN FHS**: inserire una o più VLAN su cui è attiva Protezione primo hop.
- **Accesso pacchetti eliminati** : selezionare questa opzione per creare un SYSLOG quando un pacchetto viene eliminato da una funzione Protezione primo hop. Se non è definito alcun criterio, questo è il valore predefinito globale.

PASSAGGIO 3 Se necessario, creare un criterio FHS facendo clic su **Aggiungi**.

Immettere informazioni nei seguenti campi:

- **Nome criterio**: immettere un nome per il criterio definito dall'utente.
- **Accesso eliminazione pacchetti**: selezionare questa opzione per creare un SYSLOG quando un pacchetto viene eliminato in seguito a una funzione Protezione primo hop all'interno di questo criterio.
  - *Eredita*: utilizzare questo valore dalla VLAN o dalla configurazione globale.
  - *Attiva*: consente di creare un SYSLOG quando un pacchetto viene eliminato in seguito a Protezione primo hop.
  - *Disattiva*: consente di non creare un SYSLOG quando un pacchetto viene eliminato in seguito a Protezione primo hop.

Impostazioni guardia RA

Utilizzare la pagina Impostazioni Guardia RA per attivare la funzione Guardia RA su un gruppo specifico di VLAN e per impostare i valori di configurazione globali per questa funzione. Se necessario, è possibile aggiungere un criterio oppure è possibile configurare in questa pagina i criteri Guardia RA definiti dal sistema.

Per configurare Guardia RA su porte o LAG:

PASSAGGIO 1 Fare clic su **Protezione** > **Protezione primo hop** > **Impostazioni Guardia RA**.

PASSAGGIO 2 Compilare i seguenti campi di configurazione globale:

- **Elenco VLAN Guardia RA**: inserire una o più VLAN su cui è attiva la funzione Guardia RA.
- **Limite hop minimo**: questo campo indica se il criterio Guardia RA verificherà il limite hop minimo del pacchetto ricevuto.
  - *Limite hop minimo*: verifica che il limite del numero di hop sia maggiore o uguale a questo valore.
  - *Nessuna verifica*: disattiva la verifica del limite minimo di conteggio degli hop.

- **Limite hop massimo**: questo campo indica se il criterio Guardia RA verificherà il limite hop massimo del pacchetto ricevuto.
  - *Limite hop massimo*: verifica che il limite del numero di hop sia minore o uguale a questo valore. Il valore del limite massimo deve essere maggiore o uguale al valore del limite minimo.
  - *Nessuna verifica*: disattiva la verifica del limite massimo di conteggio degli hop.
- **Flag configurazione gestita**: questo campo specifica la verifica del flag configurazione indirizzo gestito annunciato all'interno di un criterio Guardia RA IPv6.
  - *Nessuna verifica*: disattiva la verifica del flag configurazione indirizzo gestito annunciato.
  - *Attivo*: attiva la verifica del flag configurazione indirizzo gestito annunciato.
  - *Non attivo*: il valore del flag deve corrispondere a zero.
- **Altro flag di configurazione**: questo campo specifica la verifica dell'altro flag di configurazione annunciato all'interno di un criterio Guardia RA IPv6.
  - *Nessuna verifica*: disattiva la verifica dell'altro flag di configurazione annunciato.
  - *Attivo*: attiva la verifica dell'altro flag di configurazione annunciato.
  - *Non attivo*: il valore del flag deve corrispondere a zero.
- **Preferenza minima routing**: questo campo indica se il criterio Guardia RA verificherà il valore minimo di preferenza di routing predefinita annunciata nei messaggi RA all'interno del criterio Guardia RA.
  - *Nessuna verifica*: disattiva la verifica del limite minimo della preferenza routing predefinita annunciata.
  - *Basso*: specifica il valore minimo consentito della preferenza di routing predefinita annunciata. Sono validi i seguenti valori: basso, medio e alto (vedere RFC4191).
  - *Medio*: specifica il valore minimo consentito della preferenza di routing predefinita annunciata. Sono validi i seguenti valori: basso, medio e alto (vedere RFC4191).

- *Alto*: specifica il valore minimo consentito della preferenza di routing predefinita annunciata. Sono validi i seguenti valori: basso, medio e alto (vedere RFC4191).

- **Preferenza massima routing**: questo campo indica se il criterio Guardia RA verificherà il valore massimo di preferenza di routing predefinita annunciata nei messaggi RA all'interno del criterio Guardia RA.
  - *Nessuna verifica*: disattiva la verifica del limite massimo della preferenza routing predefinita annunciata.
  - *Basso*: specifica il valore massimo consentito della preferenza di routing predefinita annunciata. Sono validi i seguenti valori: basso, medio e alto (vedere RFC4191).
  - *Medio*: specifica il valore massimo consentito della preferenza di routing predefinita annunciata. Sono validi i seguenti valori: basso, medio e alto (vedere RFC4191).
  - *Alto*: specifica il valore massimo consentito della preferenza di routing predefinita annunciata. Sono validi i seguenti valori: basso, medio e alto (vedere RFC4191).

Per creare un criterio Guardia RA o per configurare i criteri definiti dal sistema, fare clic su **Aggiungi** e inserire i parametri elencati sopra.

Se richiesto, fare clic su **Associa criterio alla VLAN** o su **Associa criterio all'interfaccia**.

Impostazioni guardia DHCPv6

Utilizzare la pagina Impostazioni Guardia DHCPv6 per attivare la funzione Guardia DHCPv6 su un gruppo specifico di VLAN e per impostare i valori di configurazione globali per questa funzione. Se necessario, è possibile aggiungere un criterio oppure è possibile configurare in questa pagina i criteri Guardia DHCPv6 definiti dal sistema.

Per configurare Guardia DHCPv6 su porte o LAG:

PASSAGGIO 1 Fare clic su **Protezione** > **Protezione primo hop** > **Impostazioni Guardia DHCPv6**.

PASSAGGIO 2 Compilare i seguenti campi di configurazione globale:

- **Elenco VLAN Guardia DHCPv6**: inserire una o più VLAN su cui è attiva la funzione Guardia DHCPv6.

- **Preferenza minima**: questo campo indica se il criterio Guardia DHCPv6 verificherà il valore di preferenza minima annunciato del pacchetto ricevuto.
  - *Nessuna verifica*: disattiva la verifica del valore di preferenza minima annunciato del pacchetto ricevuto.
  - *Definito dall'utente*: verifica che il valore di preferenza annunciato sia maggiore o uguale a questo valore. Tale valore deve essere minore del valore Preferenza massima.
- **Preferenza massima**: questo campo indica se il criterio Guardia DHCPv6 verificherà il valore di preferenza massima annunciato del pacchetto ricevuto. Tale valore deve essere maggiore del valore Preferenza minima.
  - *Nessuna verifica*: disattiva la verifica del limite minimo di conteggio degli hop.
  - *Definito dall'utente*: verifica che il valore di preferenza annunciato sia minore o uguale a questo valore.

PASSAGGIO 3 Se necessario, fare clic su **Aggiungi** per creare un criterio DHCPv6.

PASSAGGIO 4 Immettere informazioni nei seguenti campi:

- **Nome criterio**: immettere un nome per il criterio definito dall'utente.
- **Ruolo dispositivo**: selezionare **Server** o **Client** per specificare il ruolo del dispositivo associato alla porta per Guardia DHCPv6.
  - *Ereditato*: il ruolo del dispositivo è ereditato dalla VLAN o è predefinito del sistema (client).
  - *Client*: il ruolo del dispositivo è client.
  - *Host*: il ruolo del dispositivo è host.
- **Associa prefissi di risposta**: selezionare questa opzione per attivare la verifica dei prefissi annunciati nei messaggi di risposta DHCP all'interno del criterio Guardia DHCPv6.
  - *Ereditato*: il valore è ereditato dalla VLAN o è predefinito del sistema (nessuna verifica).
  - *Nessuna verifica*: i prefissi annunciati non sono verificati.
  - *Elenco corrispondenze*: elenco dei prefissi IPv6 da associare.

- **Associa indirizzo server**: selezionare questa opzione per attivare la verifica del server DHCP e dell'indirizzo IPv6 di inoltro nei messaggi di risposta DHCP ricevuti all'interno del criterio Guardia DHCPv6.
  - *Ereditato*: il valore è ereditato dalla VLAN o è predefinito del sistema (nessuna verifica).
  - *Nessuna verifica*: disattiva la verifica dell'indirizzo IPv6 di inoltro e del server DHCP.
  - *Elenco corrispondenze*: elenco dei prefissi IPv6 da associare.
- **Preferenza minima**: vedere sopra.
- **Preferenza massima**: vedere sopra.

PASSAGGIO 5 Se richiesto, fare clic su **Associa criterio alla VLAN** o su **Associa criterio all'interfaccia**.

Impostazioni Esame di rilevamento router adiacente

Utilizzare la pagina Impostazioni Esame di ND per attivare la funzione Esame di ND su un gruppo specifico di VLAN e per impostare i valori di configurazione globali per questa funzione. Se necessario, è possibile aggiungere un criterio oppure è possibile configurare in questa pagina i criteri Esame di ND definiti dal sistema.

Per configurare Esame di ND su porte o LAG:

PASSAGGIO 1 Fare clic su **Protezione** > **Protezione primo hop** > **Impostazioni Esame di ND**.

PASSAGGIO 2 Compilare i seguenti campi di configurazione globale:

- **Elenco VLAN Esame di ND**: inserire una o più VLAN su cui è attiva la funzione Esame di ND.
- **Elimina non protetti**: selezionare questa opzione per attivare l'eliminazione dei messaggi senza firma RSA o CGA o all'interno di un criterio Esame di ND IPv6.
- **Livello protezione minimo**: se i messaggi non protetti non vengono eliminati, selezionare il livello di protezione al di sotto del quale i messaggi non vengono inoltrati.
  - *Nessuna verifica*: disattiva la verifica del livello di protezione.
  - *Definito dall'utente*: specifica il livello di protezione del messaggio da inoltrare.

PASSAGGIO 3 Se necessario, fare clic su **Aggiungi** per creare un criterio Esame di ND.

PASSAGGIO 4 Immettere informazioni nei seguenti campi:

- **Nome criterio**: immettere un nome per il criterio definito dall'utente.
- **Ruolo dispositivo**: selezionare **Server** o **Client** per specificare il ruolo del dispositivo associato alla porta per Esame di ND.
  - *Ereditato*: il ruolo del dispositivo è ereditato dalla VLAN o è predefinito del sistema (client).
  - *Client*: il ruolo del dispositivo è client.
  - *Host*: il ruolo del dispositivo è host.
- **Elimina non protetti**: vedere sopra.
- **Livello protezione minimo**: vedere sopra.
- **Convalida MAC di origine**: consente di specificare se attivare globalmente il confronto dell'indirizzo MAC di origine con l'indirizzo a livello di collegamento:
  - *Ereditato*: valore ereditato dalla VLAN o predefinito del sistema (disattivato).
  - *Attiva*: attiva il confronto dell'indirizzo MAC di origine con l'indirizzo a livello di collegamento.
  - *Disattiva*: disattiva il confronto dell'indirizzo MAC di origine con l'indirizzo a livello di collegamento.

PASSAGGIO 5 Se richiesto, fare clic su **Associa criterio alla VLAN** o su **Associa criterio all'interfaccia**.

Impostazioni binding router adiacenti

La tabella di binding dei router adiacenti è una tabella di database di router adiacenti IPv6 connessa a un dispositivo e viene creata dalle fonti di informazioni, ad esempio lo snooping del protocollo NDP. Questa tabella di database, o binding, viene utilizzata da varie funzioni di guardia IPv6 per impedire lo spoofing e reindirizzare gli attacchi.

Utilizzare la pagina Impostazioni binding router adiacenti per attivare la funzione Binding dei router adiacenti su un gruppo specifico di VLAN e per impostare i valori di configurazione globali per questa funzione. Se necessario, è possibile aggiungere un criterio oppure è possibile configurare in questa pagina i criteri Binding dei router adiacenti definiti dal sistema.

Per configurare Binding dei router adiacenti su porte o LAG:

PASSAGGIO 1 Fare clic su **Protezione** > **Protezione primo hop** > **Impostazioni binding router adiacenti**.

PASSAGGIO 2 Compilare i seguenti campi di configurazione globale:

- **Elenco VLAN binding dei router adiacenti**: inserire una o più VLAN su cui è attiva la funzione Binding dei router adiacenti.
- **Binding dei router adiacenti manuale**: selezionare questa opzione per indicare che è possibile aggiungere manualmente le voci alla tabella di binding dei router adiacenti.
- **Durata binding dei router adiacenti**: consente di indicare per quanto tempo gli indirizzi rimangono nella tabella di binding dei router adiacenti.
- **Accesso binding dei router adiacenti**: questo campo indica se attivare il confronto di un indirizzo IPv6 associato con la tabella Prefissi dei router adiacenti e l'accesso agli eventi principali della tabella di binding.
- **Limiti voci binding dei router adiacenti**: specifica il numero massimo di voci Binding dei router adiacenti per tipo di interfaccia o indirizzo:
  - *Voci per VLAN*: specifica il limite di binding dei router adiacenti per numero di VLAN.
  - *Voci per interfaccia*: specifica il limite di binding dei router adiacenti per interfaccia.
  - *Voci per indirizzo MAC*: specifica il limite di binding dei router adiacenti per indirizzo MAC.

PASSAGGIO 3 Se necessario, fare clic su **Aggiungi** per creare un criterio binding dei router adiacenti.

PASSAGGIO 4 Immettere informazioni nei seguenti campi:

- **Nome criterio**: immettere un nome per il criterio definito dall'utente.
- **Ruolo dispositivo**: selezionare **Server** o **Client** per specificare il ruolo del dispositivo associato alla porta per il criterio binding dei router adiacenti.
  - *Ereditato*: il ruolo del dispositivo è ereditato dalla VLAN o è predefinito del sistema (client).
  - *Client*: il ruolo del dispositivo è client.
  - *Host*: il ruolo del dispositivo è host.

- **Accesso binding dei router adiacenti**: vedere sopra.
- **Limiti voci binding dei router adiacenti**: vedere sopra.

PASSAGGIO 5 Se richiesto, fare clic su **Associa criterio alla VLAN** o su **Associa criterio all'interfaccia**.

Associazione criteri (VLAN)

Per associare un criterio a una o più LAN, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Protezione primo hop** > **Associazione criteri (VLAN)**.

L'elenco dei criteri già associati viene visualizzato insieme a **Tipo di criterio**, **Nome criterio** ed **Elenco VLAN**.

PASSAGGIO 2 Per associare un criterio a una VLAN, fare clic su **Aggiungi** e compilare i seguenti campi:

- **Tipo di criterio**: selezionare il tipo di criterio da associare all'interfaccia.
- **Nome criterio**: selezionare il nome del criterio da associare all'interfaccia.
- **Elenco VLAN**: selezionare le VLAN alle quali è associato il criterio. Selezionare **Tutte le VLAN** oppure inserire un intervallo di VLAN.

PASSAGGIO 3 Fare clic su **Applica** per aggiungere le impostazioni al file Configurazione di esecuzione.

Associazione criteri (porta)

Per associare un criterio a una o più porte o LAG, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Protezione primo hop** > **Associazione criteri (porta)**.

L'elenco dei criteri già associati viene visualizzato insieme a **Numero interfaccia**, **Tipo di criterio**, **Nome criterio** e **Elenco VLAN**.

PASSAGGIO 2 Per associare un criterio a una porta o un LAG, fare clic su **Aggiungi** e compilare i seguenti campi:

- **Interfaccia**: selezionare l'interfaccia alla quale verrà associato il criterio.
- **Tipo di criterio**: selezionare il tipo di criterio da associare all'interfaccia.

- **Nome criterio**: selezionare il nome del criterio da associare all'interfaccia.
- **Elenco VLAN**: selezionare le VLAN alle quali è associato il criterio. Selezionare **Tutte le VLAN** oppure inserire un intervallo di VLAN.

PASSAGGIO 3 Fare clic su **Applica** per aggiungere le impostazioni al file Configurazione di esecuzione.

Tabella di binding dei router adiacenti

Per aggiungere o modificare le voci nella tabella di binding dei router adiacenti:

PASSAGGIO 1 Fare clic su **Protezione** > **Protezione primo hop** > **Tabella di binding dei router adiacenti**.

PASSAGGIO 2 Selezionare una delle seguenti opzioni di Cancella tabella:

- **Solo statico**: consente di cancellare tutte le voci statiche della tabella.
- **Solo dinamico**: consente di cancellare tutte le voci dinamiche della tabella.
- **Tutti dinamici e statici**: consente di cancellare tutte le voci dinamiche e statiche della tabella.

PASSAGGIO 3 Fare clic su **Aggiungi** per aggiungere una nuova voce alla tabella.

PASSAGGIO 4 Immettere informazioni nei seguenti campi:

- **ID VLAN**: l'ID VLAN della voce.
- **Indirizzo IPv6**: l'indirizzo IPv6 origine della voce.
- **Nome interfaccia**: la porta su cui viene ricevuto il pacchetto.
- **Indirizzo MAC**: l'indirizzo MAC del router adiacente del pacchetto.

Stato FHS

Per visualizzare la configurazione globale delle funzioni FHS, eseguire i passaggi riportati di seguito:

PASSAGGIO 1 Fare clic su **Protezione** > **Protezione primo hop** > **Stato FHS**.

PASSAGGIO 2 Selezionare una porta, un LAG o una VLAN per cui è segnalato lo stato FHS.

PASSAGGIO 3 Vengono visualizzati i seguenti campi delle interfacce selezionate:

- **Stato FHS**
  - *Stato FHS su VLAN corrente*: indica se FHS è attivo sulla VLAN corrente.
  - *Accesso eliminazione pacchetti*: indica se questa funzione è attivata per l'interfaccia corrente (a livello di configurazione globale o in un criterio associato all'interfaccia).
- **Stato guardia RA**
  - *Stato Guardia RA su VLAN corrente*: indica se Guardia RA è attiva sulla VLAN corrente.
  - *Ruolo dispositivo:* il ruolo del dispositivo RA.
  - *Flag configurazione gestita*: indica se la verifica del flag di configurazione gestito è attiva.
  - *Altro flag di configurazione*: indica se la verifica dell'altro flag di configurazione è attiva.
  - *Elenco indirizzi RA*: l'elenco di indirizzi RA da associare.
  - *Elenco prefissi RA*: l'elenco di prefissi RA da associare.
  - *Limite hop minimo*: indica se la verifica del limite di hop RA minimo è attiva.
  - *Limite hop massimo*: indica se la verifica del limite di hop RA massimo è attiva.
  - *Preferenza router minima*: indica se la verifica della preferenza router minima è attiva.
  - *Preferenza router massima*: indica se la verifica della preferenza router massima è attiva.
- **Stato Esame di ND**
  - *Stato Esame di ND su VLAN corrente*: indica se Esame di ND è attivo sulla VLAN corrente.
  - *Ruolo dispositivo*: ruolo del dispositivo Esame di ND.
  - *Elimina non protetti*: indica se i messaggi non protetti vengono eliminati.
  - *Livello protezione minimo*: se i messaggi non protetti non vengono eliminati, indica il livello di protezione minimo per i pacchetti da inoltrare.

- *Convalida MAC di origine*: indica se la verifica dell'indirizzo MAC è attiva.

- **Stato Guardia DHCP**
  - *Stato Guardia DHCPv6 su VLAN corrente*: indica se Guardia DHCPv6 è attiva sulla VLAN corrente.
  - *Ruolo dispositivo:* il ruolo del dispositivo DHCP.
  - *Associa prefissi di risposta*: indica se la verifica dei prefissi di risposta DHCP è attiva.
  - *Associa indirizzo server*: indica se la verifica degli indirizzi server DHCP è attiva.
  - *Preferenza minima*: indica se la verifica della preferenza minima è attiva.
  - *Preferenza massima*: indica se la verifica della preferenza massima è attiva.

- **Stato binding dei router adiacenti**
  - *Stato binding dei router adiacenti su VLAN corrente*: indica se il binding dei router adiacenti è attivo sulla VLAN corrente.
  - *Ruolo dispositivo*: il ruolo dispositivo binding dei router adiacenti.
  - *Accesso binding*: indica se l'accesso eventi della tabella di binding dei router adiacenti è attivo.
  - *Numero massimo di voci per VLAN*: indica il numero massimo di voci dinamiche della tabella di binding dei router adiacenti per VLAN consentito.
  - *Numero massimo di voci per interfaccia*: indica il numero massimo di voci della tabella di binding dei router adiacenti per interfaccia consentito.
  - *Numero massimo di voci per indirizzo MAC*: indica il numero massimo di voci della tabella di binding dei router adiacenti per indirizzo MAC consentito.

Statistiche FHS

Per visualizzare le statistiche FHS, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Protezione primo hop** > **Statistiche FHS**.

PASSAGGIO 2 Vengono visualizzati i seguenti campi:

- **Messaggi NDP (Neighbor Discovery Protocol)**: il numero di messaggi ricevuti e sottoposto a bridging viene visualizzato per i seguenti tipi di messaggi:
  - *RA*: messaggi di annuncio router.
  - *CPA*: messaggi di annuncio percorso certificazione.
  - *ICMPv6*: messaggi di Internet Control Message IPv6 Protocol.
  - *NS*: messaggi di richiesta router adiacente.
  - *RS*: messaggi di richiesta router.
  - *CPS*: messaggi di richiesta percorso certificazione.
- **Messaggi DHCPv6**: il numero di messaggi ricevuti e sottoposto a bridging viene visualizzato per i differenti tipi di messaggi DHCPv6

In Tabella messaggi eliminati FHS vengono visualizzati i campi seguenti.

- **Protocollo**: il protocollo del messaggio eliminato.
- **Tipo di messaggio**: il tipo di messaggio eliminato.
- **Conteggio**: il numero di messaggi eliminati.
- **Motivo**: il motivo per cui i messaggi sono stati eliminati.

24

Protezione: client SSH

In questa sezione viene descritto il dispositivo quando funziona come client SSH.

Vengono trattati i seguenti argomenti:

- **SCP (Secure Copy, copia sicura) e SSH**
- **Metodi di protezione**
- **Autenticazione del server SSH**
- **Autenticazione del client SSH**
- **Operazioni preliminari**
- **Attività comuni**
- **Configurazione del client SSH mediante l'interfaccia utente**

SCP (Secure Copy, copia sicura) e SSH

Secure Shell o SSH è un protocollo di rete che consente lo scambio di dati su un canale protetto tra client SSH (in questo caso il dispositivo) e un server SSH.

Il protocollo SSH facilita la gestione di una rete composta da uno o più switch, nella quale sono memorizzati diversi file di sistema su un server SSH centralizzato. Quando i file di configurazione vengono trasferiti su una rete, Secure Copy (SCP), applicazione che utilizza il protocollo SSH, garantisce che i dati sensibili, come nome utente o password, non possano essere intercettati.

SCP serve per trasferire in sicurezza firmware, immagine di avvio, file di configurazione, file della lingua e file di log da un server SCP centrale al dispositivo.

Rispetto a SSH, l'applicazione SCP in esecuzione sul dispositivo un'applicazione client SSH e il server SCP è un'applicazione server SSH.

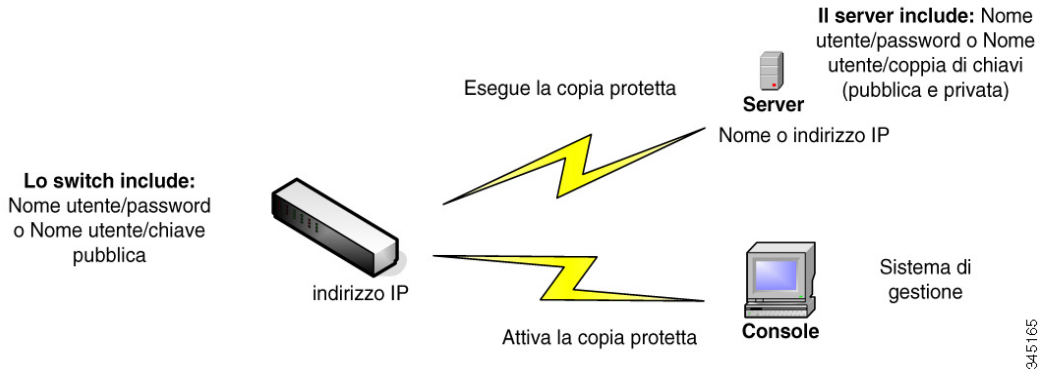
Quando i file vengono scaricati mediante TFTP o HTTP, il trasferimento dati non è protetto.

Se i file sono scaricati tramite SCP, le informazioni vengono scaricate dal server SCP sul dispositivo da un canale protetto. La creazione di questo canale protetto è preceduta da autenticazione, come garanzia del fatto che l'utente disponga delle autorizzazioni necessarie per l'operazione.

L'utente deve inserire le informazioni di autenticazione sia sul dispositivo che sul server SSH, sebbene questa guida non descriva le operazioni sul server.

Nella figura viene mostrata una configurazione di rete tipica nella quale è possibile utilizzare la funzione SCP.

Configurazione di rete tipica



Metodi di protezione

Quando i dati vengono trasferiti da un server SSH a un dispositivo (client), il server SSH utilizza i metodi seguenti per l'autenticazione del client.

Password

Per sfruttare il metodo con password, per prima cosa verificare che sul server SSH siano definiti nome utente e password. Questa operazione non avviene mediante il sistema di gestione del dispositivo; tuttavia, dopo aver definito un nome utente sul server, è possibile modificare la password del server nel sistema di gestione del dispositivo.

È necessario poi creare il nome utente/la password sul dispositivo. Quando i dati vengono trasferiti dal server al dispositivo, il nome utente e la password forniti dal dispositivo devono corrispondere al nome utente e alla password sul server.

I dati possono essere crittografati utilizzando una chiave simmetrica monouso negoziata durante la sessione.

Ogni dispositivo gestito deve possedere nome utente e password propri, sebbene sia possibile utilizzare la stessa combinazione di nome utente e password per più dispositivi.

L'autenticazione tramite password rappresenta il metodo predefinito del dispositivo.

Chiavi pubbliche/private

Per sfruttare il metodo con chiave pubblica/privata, creare un nome utente e una chiave pubblica sul server SSH. La chiave pubblica viene generata sul dispositivo, come descritto di seguito e viene copiata sul server. Le operazioni di creazione di un nome utente e di copia della chiave pubblica sul server non sono trattate in questa guida.

Le coppie di chiavi RSA e DSA predefinite vengono generate per il dispositivo all'avvio. Una di queste chiavi serve per crittografare i dati scaricati dal server SSH. La chiave RSA è quella predefinita.

Se l'utente elimina una o entrambe le chiavi, queste vengono rigenerate.

Le chiavi pubbliche/private sono crittografate e memorizzate nella memoria del dispositivo. Le chiavi fanno parte del file di configurazione del dispositivo e la chiave privata è visualizzabile dall'utente in formato crittografato e in testo normale.

Poiché la chiave privata non può essere copiata direttamente come chiave privata di un altro dispositivo, esiste un metodo di importazione per la copia di chiavi private da un dispositivo all'altro (descritto nella sezione **Importazione di chiavi**).

Importazione di chiavi

Nel metodo con chiave, è necessario creare le singole chiavi pubbliche/private per ogni dispositivo; queste chiavi private non possono essere copiate direttamente da un dispositivo all'altro per motivi di sicurezza.

In caso di più switch su una rete, il processo di creazione di chiavi pubbliche/private per tutti gli switch potrebbe essere molto lungo, poiché ogni chiave pubblica/privata deve essere creata e successivamente caricata sul server SSH.

Per facilitare questa procedura, una funzione aggiuntiva consente il trasferimento sicuro della chiave privata crittografata su tutti gli switch del sistema.

Quando viene creata una chiave privata su un dispositivo, è anche possibile creare una *frase chiave* associata. La frase chiave serve per crittografare la chiave privata e importarla negli switch rimanenti. In questo modo, tutti gli switch utilizzeranno la stessa chiave pubblica/privata.

Autenticazione del server SSH

Un dispositivo che funge da client SSH comunica solo con un server SSH attendibile. Quando l'Autenticazione del server SSH è disattivata (impostazione predefinita), ogni server SSH è considerato attendibile. Se l'Autenticazione del server SSH è attiva, l'utente deve aggiungere una voce per i server attendibili alla Tabella server SSH affidabili. La tabella memorizza le seguenti informazioni per ogni server SSH attendibile, fino a un massimo di 16 server:

- Nome host/Indirizzo IP del server
- Impronta digitale chiave pubblica del server

Se la funzione di autenticazione del server SSH è attiva, il client SSH in esecuzione sul dispositivo autentica il server SSH mediante la seguente procedura:

- Il dispositivo calcola l'impronta digitale della chiave pubblica del server SSH ricevuta.
- Il dispositivo cerca nella tabella dei server SSH attendibili l'indirizzo IP o il nome host del server SSH. Viene eseguita una delle seguenti operazioni:
  - In caso di corrispondenza, sia per indirizzo IP/nome host che per l'impronta digitale del server, il server viene autenticato.
  - In caso di corrispondenza di indirizzo IP/nome host, ma non dell'impronta digitale, la ricerca continua. Se non viene trovata corrispondenza per l'impronta digitale, la ricerca termina e l'autenticazione non riesce.
  - Se non viene trovata corrispondenza per indirizzo IP/nome host, la ricerca termina e l'autenticazione non riesce.
- Se nell'elenco di server attendibili non viene trovata la voce per il server SSH, il processo non viene completato.

Autenticazione del client SSH

L'Autenticazione del client SSH tramite password è attiva per impostazione predefinita con nome utente e password "anonymous" (anonimi).

L'utente deve configurare le seguenti informazioni per l'autenticazione:

- Metodo di autenticazione da utilizzare.
- Coppia nome utente/password o chiave pubblica/privata.

Per rendere possibile la configurazione automatica di un dispositivo nuovo (dispositivo con la configurazione predefinita), l'Autenticazione del server SSH è disattivata per impostazione predefinita.

Algoritmi supportati

Una volta stabilita la connessione tra un dispositivo (come un client SSH) e un server SSH, client e server SSH si scambiano dati per determinare gli algoritmi da utilizzare a livello di trasporto SSH.

Sul lato client sono supportati i seguenti algoritmi:

- Algoritmo scambio di chiavi Diffie-Hellman
- Algoritmi di crittografia
  - aes128-cbc
  - 3des-cbc
  - arcfour
  - aes192-cbc
  - aes256-cbc
- Algoritmi con codice di autenticazione dei messaggi
  - hmac-sha1
  - hmac-md5

NOTA Gli algoritmi di compressione non sono supportati.

Operazioni preliminari

Prima di utilizzare la funzione SCP, è necessario svolgere le seguenti operazioni:

- Quando si utilizza il metodo di autenticazione con password, nome utente e password devono essere configurati sul server SSH.
- Quando si utilizza il metodo di autenticazione con chiavi pubbliche/private, la chiave pubblica deve essere memorizzata sul server SSH.

Attività comuni

In questa sezione vengono descritte alcune attività comuni eseguite con il client SSH. Tutte le pagine indicate sono presenti nel menu Client SSH.

Flusso di lavoro 1: per configurare il client SSH e il trasferimento dei dati verso/da un server SSH, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere il metodo da utilizzare: password o chiave pubblica/privata. Utilizzare la pagina Autenticazione degli utenti SSH.

PASSAGGIO 2 Nel caso di metodo con password, attenersi alla seguente procedura:

a. Creare una password globale nella pagina Autenticazione degli utenti SSH oppure crearne una temporanea nelle pagine Aggiornamento/Backup del firmware/Lingua o Configurazione di backup/Log, durante l'attivazione effettiva del trasferimento di dati protetti.

b. Utilizzare SCP per aggiornare il firmware, l'immagine di avvio o il file della lingua mediante; a tal fine, selezionare l'opzione **via SCP (tramite SSH)** nella pagina Aggiornamento/Backup del firmware/Lingua. È possibile immettere direttamente la password in questa pagina oppure è possibile utilizzare la password specificata nella pagina Autenticazione degli utenti SSH.

c. Utilizzare SCP per scaricare o eseguire il backup del file di configurazione; a tal fine, selezionare l'opzione **via SCP (tramite SSH)** della pagina Download/Configurazione backup/Log. È possibile immettere direttamente la password in questa pagina oppure è possibile utilizzare la password specificata nella pagina Autenticazione degli utenti SSH.

PASSAGGIO 3 Impostare nome utente e password sul server SSH oppure modificare la password sul server SSH. Questa operazione dipende dal server e non viene descritta qui.

PASSAGGIO 4 Nel caso di metodo con chiave pubblica/privata, attenersi alla seguente procedura:

a. Selezionare se si utilizza una chiave RSA o DSA, creare un nome utente, quindi generare le chiavi pubbliche/private.

b. Visualizzare la chiave generata premendo **Dettagli** e trasferire nome utente e chiave pubblica sul server SSH. Questa operazione dipende dal server e non viene descritta in questa guida.

c. Utilizzare SCP per aggiornare ed eseguire il backup del firmware o del file della lingua; a tal fine, selezionare l'opzione **via SCP (tramite SSH)** nella pagina Aggiornamento/Backup del firmware/Lingua.

d. Utilizzare SCP per scaricare o eseguire il backup del file di configurazione; a tal fine, selezionare l'opzione **via SCP (tramite SSH)** della pagina Download/ Configurazione backup/Log.

Flusso di lavoro 2: per importare le chiavi pubbliche/private da un dispositivo all'altro, attenersi alla seguente procedura.

PASSAGGIO 1 Generare una chiave pubblica/privata nella pagina Autenticazione degli utenti SSH.

PASSAGGIO 2 Impostare le proprietà SSD e creare una nuova frase chiave locale nella pagina Gestione sicura dei dati sensibili > Proprietà.

PASSAGGIO 3 Fare clic su **Dettagli** per visualizzare le chiavi crittografate generate e copiarle (inclusi i piè di pagina Inizio e Fine) dalla pagina Dettagli su un dispositivo esterno. Copiare separatamente le chiavi pubbliche e private.

PASSAGGIO 4 Accedere a un altro dispositivo e aprire la pagina Autenticazione degli utenti SSH. Selezionare il tipo di chiave richiesto e fare clic su **Modifica**. Incollare le chiavi pubbliche/private.

PASSAGGIO 5 Fare clic su **Applica** per copiare le chiavi pubbliche/private sul secondo dispositivo.

Flusso di lavoro 3: per modificare la password su un server SSH, attenersi alla seguente procedura:

PASSAGGIO 1 Identificare il server nella pagina Modifica password sul server SSH.

PASSAGGIO 2 Immettere la nuova password.

PASSAGGIO 3 Fare clic su **Applica**.

Configurazione del client SSH mediante l'interfaccia utente

In questa sezione vengono descritte le pagine da cui configurare la funzione del client SSH.

Autenticazione degli utenti SSH

Utilizzare questa pagina per selezionare un metodo di autenticazione utente SSH e per impostare nome utente e password sul dispositivo, se è stato selezionato il metodo con password, oppure generare una chiave RSA o DSA se è stato selezionato il metodo con chiave pubblica/privata.

Per selezionare un metodo di autenticazione e impostare nome utente/password/chiavi, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Client SSH** > **Autenticazione degli utenti SSH**.

PASSAGGIO 2 Selezionare un **Metodo di autenticazione degli utenti SSH**. Questo è il metodo globale definito per la copia protetta (SCP). Selezionare una delle seguenti opzioni:

- **Tramite password**: impostazione predefinita. Se selezionata, immettere una password o lasciare quella predefinita.
- **Tramite chiave pubblica RSA**: se si seleziona questa opzione viene creata una chiave pubblica/privata RSA nel blocco **Tabella chiavi utenti SSH**.
- **Tramite chiave pubblica DSA**: se si seleziona questa opzione viene creata una chiave pubblica/privata DSA nel blocco **Tabella chiavi utenti SSH**.

PASSAGGIO 3 Immettere il **Nome utente** (indipendentemente dal metodo selezionato) o utilizzare quello predefinito. Deve corrispondere al nome utente definito sul server SSH.

PASSAGGIO 4 Se è stato selezionato il metodo *Tramite password*, immettere la password (**Con crittografia** o **Testo normale**) oppure lasciare la password crittografata predefinita.

PASSAGGIO 5 Eseguire una delle seguenti operazioni:

- **Applica**: i metodi di autenticazione selezionati vengono associati al metodo di accesso.
- **Ripristina credenziali predefinite**: vengono ripristinati il nome utente e la password (anonimi) predefiniti.

- **Visualizza dati sensibili in testo normale**: i dati sensibili della pagina corrente sono visualizzati come testo normale.

Nella **Tabella chiavi utenti SSH** vengono visualizzati i seguenti campi per ogni chiave:

- **Tipo di chiave**: RSA o DSA.
- **Origine chiave**: generata automaticamente o definita dall'utente.
- **Impronta digitale**: impronta digitale generata dalla chiave.

PASSAGGIO 6 Per gestire una chiave RSA o DSA, selezionare RSA o DSA ed eseguire una delle seguenti operazioni:

- **Genera**: genera una nuova chiave.
- **Modifica**: visualizza le chiavi per le operazioni di copia o incolla su un altro dispositivo.
- **Elimina**: elimina la chiave.
- **Dettagli**: visualizza le chiavi.

Autenticazione del server SSH

Per attivare l'Autenticazione del server SSH e definire i server attendibili, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Client SSH** > **Autenticazione del server SSH**.

PASSAGGIO 2 Selezionare **Attiva** per attivare l'Autenticazione del server SSH.

- **Interfaccia di origine IPv4**: selezionare l'interfaccia di origine il cui indirizzo IPv4 sarà utilizzato come indirizzo IPv4 di origine dei messaggi utilizzati nelle comunicazioni con i server SSH IPv4.
- **Interfaccia di origine IPv6**: selezionare l'interfaccia di origine il cui indirizzo IPv6 sarà utilizzato come indirizzo IPv6 di origine dei messaggi utilizzati nelle comunicazioni con i server SSH IPv6.

  NOTA Se è selezionata l'opzione Auto, il sistema utilizza l'indirizzo IP definito nell'interfaccia in uscita come indirizzo IP di origine.

PASSAGGIO 3 Fare clic su **Aggiungi** e completare i seguenti campi per il server SSH attendibile:

- **Definizione server**: selezionare uno dei seguenti metodi per identificare il server SSH:
  - *Per indirizzo IP*: se questa opzione è selezionata, immettere l'indirizzo IP del server nei campi sottostanti.
  - *Per nome*: se questa opzione è selezionata, inserire il nome del server nel campo **Indirizzo IP/Nome server**.
- **Versione IP**: se il server SSH viene specificato per indirizzo IP, selezionare se si tratta di un indirizzo IPv4 o IPv6.
- **Tipo di indirizzo IP**: se l'indirizzo IP del server SSH è IPv6, selezionare il tipo di indirizzo IPv6. Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale di collegamento presenta un prefisso FE80, non è instradabile e può essere utilizzato solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento dal rispettivo elenco.
- **Indirizzo IP/Nome server**: immettere l'indirizzo IP o il nome del server SSH, a seconda dell'opzione selezionata per **Definizione server**.
- **Impronta digitale**: immettere l'impronta digitale del server SSH (copiata da quel server).

PASSAGGIO 4 Fare clic su **Applica**. La definizione del server attendibile viene memorizzata nel file Configurazione di esecuzione.

Modifica della password dell'utente sul server SSH

Per modificare la password su un server SSH, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Protezione** > **Client SSH** > **Modifica password sul server SSH**.

PASSAGGIO 2 Immettere informazioni nei seguenti campi:

- **Definizione del server**: selezionare **Per indirizzo IP** o **Per nome** per definire il server SSH. Immettere il nome del server o l'indirizzo IP del server nel campo **Indirizzo IP/Nome server**.
- **Versione IP**: se il server SSH viene specificato per indirizzo IP, selezionare se si tratta di un indirizzo IPv4 o IPv6.
- **Tipo di indirizzo IP**: se l'indirizzo IP del server SSH è IPv6, selezionare il tipo di indirizzo IPv6. Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale di collegamento presenta un prefisso FE80, non è instradabile e può essere utilizzato solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questo sostituisce l'indirizzo della configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento dal rispettivo elenco.
- **Indirizzo IP/Nome server**: immettere l'indirizzo IP o il nome del server SSH, a seconda dell'opzione selezionata per **Definizione server**.
- **Nome utente**: deve corrispondere al nome utente definito sul server.
- **Vecchia password**: deve corrispondere alla password sul server.
- **Nuova password**: immettere la nuova password e confermarla nel campo **Conferma password**.

PASSAGGIO 3 Fare clic su **Applica**. La password nel server SSH viene modificata.

25

Protezione: server SSH

In questa sezione viene descritto come stabilire una sessione SSH sul dispositivo.

Vengono trattati i seguenti argomenti:

- **Panoramica**
- **Attività comuni**
- **Pagine di configurazione del server SSH**

Panoramica

La funzione del server SSH consente agli utenti di avviare una sessione SSH sul dispositivo. Questa operazione è analoga alla creazione di una sessione Telnet, con la differenza che si tratta di una sessione protetta.

Le chiavi pubbliche e private vengono generate automaticamente sul dispositivo e possono essere modificate dall'utente.

La sessione SSH viene aperta con una particolare applicazione client SSH, come PuTTY.

Il server SSH può funzionare nei seguenti modi:

- **Tramite chiavi RSA/DSA generate internamente (impostazione predefinita)**: una chiave RSA e una chiave DSA vengono generate. Gli utenti accedono all'applicazione del server SSH e vengono automaticamente autenticati per aprire una sessione sul dispositivo non appena forniscono l'indirizzo IP del dispositivo.
- **Modalità chiave pubblica**: gli utenti vengono definiti sul dispositivo. Le chiavi RSA/DSA vengono generate nell'applicazione di un server SSH esterno, come PuTTY. Le chiavi pubbliche vengono immesse nel dispositivo. Successivamente, gli utenti possono avviare una sessione SSH sul dispositivo tramite l'applicazione del server SSH esterno.

Attività comuni

In questa sezione vengono descritte alcune attività comuni eseguite mediante la funzione del server SSH.

Flusso di lavoro 1: per accedere al dispositivo su SSH tramite la chiave del dispositivo creata automaticamente (impostazione predefinita), attenersi alla seguente procedura:

PASSAGGIO 1 Attivare il server SSH nella pagina Servizi TCP/UDP e verificare che l'autenticazione utente SSH tramite chiave pubblica sia disattivata nella pagina Autenticazione degli utenti SSH.

PASSAGGIO 2 Accedere a un'applicazione client SSH esterna, come PuTTY, utilizzando l'indirizzo IP del dispositivo (non è necessario inserire il nome utente o la chiave che viene riconosciuta dal dispositivo).

Flusso di lavoro 2: per creare un utente SSH e accedere al dispositivo su SSH con questo utente, attenersi alla seguente procedura:

PASSAGGIO 1 Generare una chiave RSA o DSA in un'applicazione client SSH esterna, come PuTTY.

PASSAGGIO 2 Attivare l'autenticazione utente SSH tramite chiave pubblica o password nella pagina Autenticazione degli utenti SSH.

PASSAGGIO 3 Se necessario, attivare l'accesso automatico (vedere **Accesso automatico** sotto).

PASSAGGIO 4 Aggiungere un utente nella pagina Autenticazione degli utenti SSH e copiarlo nella chiave pubblica generata esternamente.

PASSAGGIO 5 Accedere all'applicazione client SSH esterna, ad esempio PuTTY, utilizzando l'indirizzo IP del dispositivo e il nome utente.

Flusso di lavoro 3: per importare una chiave RSA o DSA dal dispositivo A al dispositivo B, attenersi alla seguente procedura:

PASSAGGIO 1 Sul dispositivo A, selezionare una chiave RSA o DSA nella pagina Autenticazione del server SSH.

PASSAGGIO 2 Fare clic su **Dettagli** e copiare la chiave pubblica del tipo di chiave selezionata nel Blocco note o in un altro editor di testo.

PASSAGGIO 3 Accedere al dispositivo B e aprire la pagina Autenticazione del server SSH. Selezionare la chiave RSA o DSA, fare clic su **Modifica** e incollare la chiave del dispositivo A.

Pagine di configurazione del server SSH

In questa sezione vengono descritte le pagine in cui è possibile configurare la funzione **Server SSH**.

Autenticazione degli utenti SSH

Utilizzare questa pagina per attivare l'autenticazione utente SSH tramite la chiave pubblica e/o la password, e (quando si usa l'autenticazione tramite chiave pubblica) per aggiungere un utente client SSH che verrà utilizzato per creare una sessione SSH in un'applicazione SSH esterna (come PuTTY).

Per poter aggiungere un utente, è necessario generare prima una chiave RSA o DSA per l'utente nell'applicazione client/di generazione della chiave SSH esterna (come PuTTY).

Accesso automatico

Se si utilizza la pagina Autenticazione degli utenti SSH per creare un nome utente SSH per un utente che è già configurato nel database utente locale. È possibile configurare la funzione **Accesso automatico** per impedire ulteriori autenticazioni; questa opzione funziona nel modo seguente:

- **Attivata**: se un utente è definito nel database locale e ha superato l'autenticazione SSH usando una chiave pubblica, l'autenticazione con il nome utente e la password del database locale viene saltata.

  NOTA Il metodo di autenticazione configurato per questo specifico metodo di gestione (console, Telnet, SSH e così via) deve essere *Locale* (ovvero non *RADIUS* o *TACACS+*). Per maggiori dettagli, vedere la sezione **Metodo di accesso a gestione**).

- **Disattivata**: una volta effettuata l'autenticazione con la chiave pubblica SSH, anche se il nome utente è configurato nel database utente locale, l'utente viene autenticato di nuovo, in base ai metodi di autenticazione configurati nella pagina Autenticazione di accesso a gestione.

È una pagina facoltativa. Non è necessario eseguire l'autenticazione utente in SSH.

Per attivare l'autenticazione e aggiungere un utente, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Server SSH** > **Autenticazione utente SSH**.

PASSAGGIO 2 Selezionare i seguenti campi:

- **Autenticazione utente SSH in base alla password**: selezionare questa opzione per eseguire l'autenticazione dell'utente client SSH tramite il nome utente e la password configurati nel database locale (vedere **Definizione degli utenti**).
- **Autenticazione degli utenti SSH tramite chiave pubblica**: selezionare questa opzione per eseguire l'autenticazione degli utenti client SSH tramite chiave pubblica.
- **Accesso automatico**: questo campo può essere attivato se è stata selezionata la funzione **Autenticazione degli utenti SSH tramite chiave pubblica**. Vedere la sezione **Accesso automatico**.

Per gli utenti configurati vengono visualizzati i campi seguenti:

- **Nome utente SSH**: il nome utente dell'utente.
- **Tipo di chiave**: indica se si tratta di una chiave RSA o DSA.
- **Impronta digitale**: impronta digitale generata dalle chiavi pubbliche.

PASSAGGIO 3 Fare clic su **Aggiungi** per aggiungere un nuovo utente e compilare i campi:

- **Nome utente SSH**: immettere un nome utente.
- **Tipo di chiave**: scegliere **RSA** o **DSA**.
- **Chiave pubblica**: copiare la chiave pubblica generata tramite un'applicazione client SSH esterna (come PuTTY) in questa casella di testo.

Autenticazione del server SSH

Le chiavi RSA e DSA pubbliche e private vengono generate automaticamente all'avvio del dispositivo con impostazioni predefinite. Ogni chiave viene anche creata automaticamente quando la rispettiva chiave configurata dall'utente viene eliminata dall'utente.

Per rigenerare una chiave RSA o DSA o per copiarla in una chiave RSA/DSA generata su un altro dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Server SSH** > **Autenticazione server SSH**.

Per ogni chiave vengono visualizzati i campi seguenti:

- **Tipo di chiave**: RSA o DSA.
- **Origine chiave**: generata automaticamente o definita dall'utente.
- **Impronta digitale**: impronta digitale generata dalla chiave.

PASSAGGIO 2 Selezionare una chiave RSA o DSA.

PASSAGGIO 3 È possibile eseguire una delle seguenti operazioni:

- **Genera**: consente di generare una chiave del tipo specificato.
- **Modifica**: consente di eseguire l'operazione di copia in una chiave da un altro dispositivo.
- **Elimina**: consente di eliminare una chiave.
- **Dettagli**: consente di visualizzare la chiave generata. Dalla finestra Dettagli è anche possibile fare clic su **Visualizza dati sensibili in testo normale**. Se questa opzione è stata selezionata, le chiavi vengono visualizzate in testo normale e non in formato crittografato. Se la chiave è già visualizzata in testo normale, è possibile fare clic su **Visualizza dati sensibili con crittografia** per visualizzare il testo in formato crittografato.

PASSAGGIO 4 Se vengono copiate nuove chiavi, fare clic su **Applica**. Le chiavi vengono memorizzate nel file Configurazione di esecuzione.

26

Protezione: gestione sicura dei dati sensibili

SSD (Secure Sensitive Data, dati sensibili protetti) è un'architettura che agevola la protezione dei dati sensibili su un dispositivo, come password e chiavi. L'infrastruttura sfrutta le frasi chiave, la crittografia, il controllo degli accessi e l'autenticazione degli utenti per offrire una soluzione di protezione nella gestione dei dati sensibili.

L'infrastruttura è stata estesa per proteggere l'integrità dei file di configurazione, la procedura di configurazione e per supportare la configurazione automatica immediata SSD.

Introduzione

L'SSD protegge i dati sensibili su un dispositivo, come password e chiavi, consente e nega l'accesso ai dati sensibili crittografati e in testo normale in base alle credenziali utente e alle regole SSD, oltre a proteggere dalla manomissione i file di configurazione che contengono dati sensibili.

Inoltre, l'SSD consente di eseguire il backup protetto e la condivisione dei file di configurazione contenenti dati sensibili.

L'SSD offre agli utenti la flessibilità per configurare il livello di protezione desiderato sui dati sensibili; da nessuna protezione con i dati sensibili in testo normale, passando per una protezione minima con la crittografia basata su una frase chiave predefinita, per arrivare alla protezione massima con crittografia basata su una frase chiave definita dall'utente.

L'SSD concede l'autorizzazione di lettura dei dati sensibili solo agli utenti autenticati e autorizzati, conformemente alle regole SSD. Un dispositivo autentica e autorizza l'accesso alla gestione per gli utenti tramite il processo di autenticazione utente.

Che si utilizzi l'SSD o meno, è consigliabile che un amministratore protegga il processo di autenticazione mediante il database di autenticazione locale, e/o protegga la comunicazione verso i server di autenticazione esterni utilizzati nel processo di autenticazione utente.

Per riassumere, l'SSD protegge i dati sensibili su un dispositivo con regole SSD, proprietà SSD e autenticazione utente. Le stesse configurazioni di regole SSD, proprietà SSD e autenticazione utente del dispositivo rappresentano dati sensibili protetti a loro volta da SSD.

Gestione SSD

La gestione SSD include una raccolta di parametri di configurazione che definiscono la gestione e la protezione dei dati sensibili. Gli stessi parametri di configurazione SSD rappresentano dati sensibili protetti da SSD.

Tutte le configurazioni dell'SSD vengono eseguite nelle pagine SSD a cui possono accedere solo gli utenti autorizzati (vedere **Regole SSD**).

Regole SSD

Le regole SSD definiscono le autorizzazioni di lettura e la modalità di lettura predefinita assegnata a una sessione utente su un canale di gestione.

Una regola SSD è identificata unicamente dal suo utente e dal canale di gestione SSD. Potrebbero esistere diverse regole SSD per lo stesso utente ma per canali diversi e, al contrario, potrebbero esistere diverse regole per lo stesso canale, ma per utenti diversi.

Le autorizzazioni di lettura determinano la visualizzazione dei dati sensibili: solo in forma crittografata, solo in testo normale, sia crittografati che in testo normale o senza autorizzazione per la visualizzazione dei dati sensibili. Anche le regole SSD sono protette come dati sensibili.

Un dispositivo è in grado di supportare un totale di 32 regole SSD.

Un dispositivo concede all'utente le autorizzazioni SSD di lettura della regola SSD che corrisponde maggiormente a identità/credenziali dell'utente e in base al tipo di canale di gestione dal quale l'utente accede o accederà ai dati sensibili.

Un dispositivo è dotato di una serie di regole SSD predefinite. Un amministratore è in grado di aggiungere, eliminare e modificare le regole SSD in base alle specifiche esigenze.

NOTA Un dispositivo potrebbe non supportare tutti i canali definiti dall'SSD.

Elementi di una regola SSD

Una regola SSD include i seguenti elementi:

- **Tipo di utente**: i tipi di utente supportati in ordine di preferenza (dalla preferenza maggiore a quella minore) sono i seguenti (se un utente corrisponde a più regole SSD, verrà applicata la regola con la preferenza maggiore):
  - **Specifico**: la regola viene applicata a un utente specifico.
  - **Utente predefinito (cisco)**: la regola viene applicata a un utente predefinito (cisco).
  - **Livello 15**: la regola viene applicata agli utenti con livello 15 di privilegio.
  - **Tutti**: la regola viene applicata a tutti gli utenti.
- **Nome utente**: se si selezione l'opzione Specifico è necessario immettere un nome utente.
- **Canale**: il tipo di canale di gestione SSD a cui viene applicata la regola. I tipi di canale supportati sono:
  - **Protetto**: la regola viene applicata solo ai canali protetti. A seconda del dispositivo, potrebbero essere supportati alcuni o tutti i seguenti canali protetti: interfaccia porta console, SCP, SSH e HTTPS.
  - **Non protetto**: la regola viene applicata solo ai canali non protetti. A seconda del dispositivo, potrebbero essere supportati alcuni o tutti i seguenti canali non protetti: Telnet, TFTP e HTTP.
  - **SNMP XML protetto**: la regola viene applicata solo a XML tramite HTTPS o SNMPv3 con privacy. Un dispositivo potrebbe supportare o meno tutti i canali XML e SNMP protetti.

- **SNMP XML non protetto**: la regola viene applicata solo a XML tramite HTTP o SNMPv1/v2 e SNMPv3 senza privacy. Un dispositivo potrebbe supportare o meno tutti i canali XML e SNMP protetti.

- **Autorizzazione di lettura**: le autorizzazioni di lettura sono associate alle regole e possono essere:
  - (Minima) **Escludi**: gli utenti non sono autorizzati ad accedere ai dati sensibili in nessun caso.
  - (Intermedia) **Solo con crittografia**: gli utenti sono autorizzati ad accedere solo ai dati sensibili con crittografia.
  - (Superiore) **Solo testo normale**: gli utenti sono autorizzati ad accedere solo ai dati sensibili in testo normale. Gli utenti hanno autorizzazioni di lettura e di scrittura anche per i parametri SSD.
  - (Massima) **Entrambi**: gli utenti hanno autorizzazioni sia con crittografia che in testo normale e sono autorizzati ad accedere ai dati sensibili con crittografia e in testo normale. Gli utenti hanno autorizzazioni di lettura e di scrittura anche per i parametri SSD.

  Ogni canale di gestione fornisce specifiche autorizzazioni di lettura, riassunte nella seguente tabella.

Canale di gestione	Opzioni consentite per l'autorizzazione di lettura
Protetto	Entrambi, Solo con crittografia
Non protetto	Entrambi, Solo con crittografia
SNMP XML protetto	Escludi, Solo testo normale
SNMP XML non protetto	Escludi, Solo testo normale

- **Modalità lettura predefinita**: tutte le modalità di lettura predefinite sono soggette all'autorizzazione di lettura della regola. Esistono le seguenti opzioni, ma alcune potrebbero essere rifiutate, a seconda dell'autorizzazione di lettura applicata. Se l'autorizzazione di lettura definita da un utente è Escludi (ad esempio) e la modalità di lettura predefinita è Con crittografia, prevale l'autorizzazione di lettura definita dall'utente.
  - **Escludi**: non consente la lettura dei dati sensibili.
  - **Con crittografia**: i dati sensibili sono crittografati.
  - **Testo normale**: i dati sensibili sono visualizzati in formato testo normale.

Ogni canale di gestione fornisce specifiche autorizzazioni di lettura, riassunte nella seguente tabella.

Autorizzazione di lettura	Modalità lettura predefinita consentita
Escludi	Escludi
Solo con crittografia	*Con crittografia
Solo testo normale	*Testo normale
Entrambi	*Testo normale, Con crittografia

* La modalità Lettura di una sessione può essere modificata temporaneamente nella pagina Proprietà dell'SSD se la nuova modalità di lettura non viola l'autorizzazione di lettura.

NOTA Tenere presente quanto segue:

- La Modalità lettura predefinita per i canali di gestione SNMP XML protetto e SNMP XML non protetto deve essere identica alla rispettiva autorizzazione di lettura.
- L'autorizzazione di lettura Escludi è ammessa solo per i canali di gestione SNMP XML protetto e SNMP XML non protetto, mentre non è consentita per i normali canali protetti e non protetti.
- L'esclusione dei dati sensibili nei canali di gestione SNMP XML protetto e non protetto comporta la presentazione dei dati sensibili come 0 (ovvero stringa nulla o numero 0). Se l'utente vuole visualizzare i dati sensibili, la regola deve essere cambiata in testo normale.
- Per impostazione predefinita, un utente SNMPv3 con privacy e autorizzazioni per XML su canali sicuri è considerato un utente di livello 15.
- Gli utenti SNMP su canali XML E SNMP non protetto SNMP (SNMPv1,v2 e v3 senza privacy) vengono considerati come tutti gli utenti.
- I nomi della comunità SNMP non sono usati come nomi utente da associare alle regole SSD.
- È possibile controllare l'accesso da parte di uno specifico utente SNMPv3 configurando una regola SSD con nome utente che corrisponde al nome utente SNMPv3.
- Deve sempre essere presente almeno una regola con autorizzazione di lettura: Solo testo normale o Entrambi, poiché solo gli utenti con queste autorizzazioni possono accedere alle pagine SSD.

- Le modifiche alla Modalità lettura predefinita e alle autorizzazioni di lettura di una regola entrano in vigore e vengono applicate agli utenti interessati e al canale di tutte le sessioni di gestione attive immediatamente, ad eccezione della sessione che apporta le modifiche, anche se la regola risulta applicabile. Quando una regola è modificata (aggiungi, elimina, modifica), il sistema aggiorna tutte le sessioni CLI/interfaccia grafica utente interessate.

  NOTA Quando la regola SSD applicata all'accesso della sessione viene cambiata dall'interno di quella sessione, l'utente deve disconnettersi e accedere di nuovo per vedere la modifica.

  NOTA Durante il trasferimento di un file avviato da un comando XML o SNMP, il protocollo sottostante utilizzato è TFTP. Pertanto, viene applicata la regola SSD per un canale non protetto.

Regole SSD e autenticazione utente

L'SSD concede l'autorizzazione SSD solo agli utenti autenticati e autorizzati, conformemente alle regole SSD. Un dispositivo dipende dal proprio processo di autenticazione utente per autenticare e autorizzare l'accesso alla gestione. Per proteggere un dispositivo e i relativi dati (tra cui i dati sensibili e le configurazioni SSD) dall'accesso non autorizzato, si consiglia di proteggere il processo di autenticazione utente sul dispositivo. Per proteggere il processo di autenticazione utente, è possibile utilizzare il database locale di autenticazione, oltre a proteggere la comunicazione tramite server di autenticazione esterna, come un server RADIUS. La configurazione della comunicazione protetta su server di autenticazione esterni è un dato sensibile ed è protetta da SSD.

NOTA Le credenziali utente nel database locale autenticato sono già protette da un meccanismo correlato non SSD.

Se un utente da un canale esegue un'azione che sfrutta un canale alternativo, il dispositivo applica l'autorizzazione di lettura e la modalità lettura predefinita dalla regola SSD che corrisponde alle credenziali utente e al canale alternativo. Ad esempio, se un utente accede tramite canale protetto e avvia una sessione di caricamento TFTP, viene applicata l'autorizzazione di lettura SSD dell'utente sul canale non protetto (TFTP).

Regole SSD predefinite

Il dispositivo dispone delle seguenti regole predefinite:

Tabella 3

Chiave regola		Azione regola	
Utente	**Canale**	**Autorizzazione di lettura**	**Modalità lettura predefinita**
Livello 15	SNMP XML protetto	Solo testo normale	Testo normale
Livello 15	Protetto	Entrambi	Con crittografia
Livello 15	Non protetto	Entrambi	Con crittografia
Tutte	SNMP XML non protetto	Escludi	Escludi
Tutte	Protetto	Solo con crittografia	Con crittografia
Tutte	Non protetto	Solo con crittografia	Con crittografia

Le regole predefinite sono modificabili, ma non eliminabili. Se le regole SSD predefinite vengono modificate, è comunque possibile ripristinarle.

Sostituzione sessione Modalità lettura predefinita SSD

Il sistema visualizza i dati sensibili in una sessione, sia in forma crittografata che come testo normale, in base all'autorizzazione di lettura e alla modalità di lettura predefinita dell'utente.

La modalità di lettura predefinita può essere temporaneamente sostituita, finché non entra in conflitto con l'autorizzazione di lettura SSD della sessione. Questa modifica entra immediatamente in vigore nella sessione corrente, finché non si verifica uno dei seguenti eventi:

- L'utente la modifica di nuovo.
- La sessione viene terminata.
- L'autorizzazione di lettura della regola SSD applicata all'utente della sessione è stata modificata e non è più compatibile con la modalità di lettura corrente della sessione. In questo caso, la modalità di lettura torna alla modalità di lettura predefinita della regola SSD.

Proprietà SSD

Le proprietà SSD sono una serie di parametri che, insieme alle regole SSD, definiscono e controllano l'ambiente SSD di un dispositivo. L'ambiente SSD è costituito dalle seguenti proprietà:

- Controllo delle modalità di crittografia dei dati sensibili.
- Controllo della complessità di protezione esercitata sui file di configurazione.
- Controllo della modalità di visualizzazione dei dati sensibili all'interno della sessione corrente.

Frase chiave

La frase chiave è la base del meccanismo di protezione in una funzione SSD ed è utilizzata per generare la chiave per la crittografia e la decrittografia dei dati sensibili. Gli switch serie Sx200, Sx300, Sx500 e SG500x/SG500XG/ESW2-550X dotati della stessa frase chiave sono in grado di decodificare i dati sensibili di ogni switch crittografati con la chiave generata dalla frase chiave.

La frase chiave deve essere conforme alle seguenti regole:

- **Lunghezza**: tra 8 e 16 caratteri.
- **Classi di caratteri**: la frase chiave deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero e un carattere speciale, ad esempio #,$.

Frasi chiave predefinite e definite dall'utente

Tutti i dispositivi sono dotati di una frase chiave predefinita pronta all'uso, trasparente agli utenti. La frase chiave predefinita non viene mai visualizzata nel file di configurazione o nell'interfaccia grafica utente/CLI.

Per avere un maggior livello di sicurezza e protezione, un amministratore deve configurare l'SSD su un dispositivo in modo che utilizzi una frase chiave definita dall'utente, anziché la frase chiave predefinita. Una frase chiave definita da un utente deve essere considerata come un segreto da proteggere, al fine di non compromettere la sicurezza dei dati sensibili sul dispositivo.

La frase chiave definita dall'utente è configurabile manualmente in testo normale, ma può anche essere ricavata da un file di configurazione (vedere la sezione **Configurazione automatica immediata dei dati sensibili**). Un dispositivo visualizza sempre le frasi chiave definite dall'utente crittografate.

Frase chiave locale

Un dispositivo mantiene una frase chiave locale, ossia la frase chiave della propria Configurazione di esecuzione. Di norma, l'SSD esegue la crittografia e la decrittografia dei dati sensibili con la chiave generata dalla frase chiave locale.

La frase chiave locale è configurabile sia come frase chiave predefinita sia come frase chiave definita dall'utente. Per impostazione predefinita, frase chiave locale e frase chiave predefinita sono identiche, ma possono essere modificate da un amministratore sia tramite interfaccia da linea di comando (se disponibile), che da interfaccia basata sul Web. La frase chiave locale viene automaticamente modificata nella frase chiave nel file di configurazione di avvio quando la configurazione di avvio diventa la configurazione di esecuzione del dispositivo. Quando in un dispositivo si ripristinano le impostazioni predefinite, la frase chiave locale è reimpostata alla frase chiave predefinita.

Controllo frase chiave del file di configurazione

Il controllo della frase chiave garantisce una maggiore protezione per una frase chiave definita dall'utente e per i dati sensibili crittografati con la chiave generata dalla frase chiave definita dall'utente, all'intero file di configurazione di testo.

Di seguito sono indicate le modalità di controllo della frase chiave esistente:

- **Illimitato** (opzione predefinita): il dispositivo include la propria frase chiave durante la creazione del file di configurazione. Ciò consente a ogni dispositivo che accetta il file di configurazione di apprendere la frase chiave dal file.
- **Limitato**: il dispositivo limita l'esportazione della frase chiave nel file di configurazione. La modalità limitata protegge i dati sensibili crittografati in un file di configurazione dai dispositivi privi di frase chiave. Questa modalità deve essere utilizzata quando un utente non vuole rendere nota la frase chiave in un file di configurazione.

Dopo aver ripristinato le impostazioni predefinite di un dispositivo, la relativa frase chiave locale viene reimpostata alla frase chiave predefinita. Di conseguenza, il dispositivo non sarà in grado di effettuare la decrittografia di eventuali dati sensibili in base a una frase chiave definita dall'utente inserita dalla sessione di

gestione (interfaccia utente/linea di comando) o in qualsiasi file di configurazione con modalità limitata, inclusi i file creati dal dispositivo stesso prima che venissero ripristinate le impostazioni predefinite. Tale impostazione rimane in uso finché il dispositivo non viene riconfigurato manualmente con la frase chiave definita dall'utente o apprende la frase chiave definita dall'utente da un file di configurazione.

Controllo dell'integrità del file di configurazione

L'utente può proteggere il file di configurazione dalla manomissione o dalla modifica, creandolo con il Controllo integrità del file di configurazione. Si consiglia di attivare il Controllo integrità del file di configurazione quando un dispositivo utilizza una frase chiave definita dall'utente con Controllo frase chiave del file di configurazione Illimitato.

ATTENZIONE Qualsiasi modifica apportata al file di configurazione protetto in termini di integrità viene considerata come una manomissione.

Un dispositivo determina se l'integrità di un file di configurazione è protetta esaminando il comando Controllo integrità del file di configurazione nel blocco di controllo SSD del file. Se un file è protetto in termini di integrità, ma il dispositivo scopre che il file non è intatto, tale file viene rifiutato. In caso contrario, il file viene accettato per ulteriori elaborazioni.

Un dispositivo verifica l'integrità di un file di configurazione di testo quando il file viene scaricato o copiato nel file di Configurazione di avvio.

Modalità lettura

Ogni sessione dispone di una Modalità lettura. Questa modalità determina il modo in cui vengono visualizzati i dati sensibili. La modalità di lettura può essere Testo normale, in cui i dati sensibili sono visualizzati come testo normale, o Con crittografia, con i dati sensibili crittografati.

File di configurazione

Il file di configurazione contiene la configurazione di un dispositivo. Un dispositivo è dotato di file di Configurazione di esecuzione, file di Configurazione di avvio, file di Configurazione mirror (opzionale) e file di Configurazione backup. L'utente può caricare e scaricare manualmente un file di configurazione su e da un file server remoto. Un dispositivo può scaricare automaticamente la propria Configurazione di avvio da un file server remoto durante la fase di configurazione automatica utilizzando il DHCP. I file di configurazione memorizzati su file server remoti sono detti file di configurazione remoti.

Il file Configurazione di esecuzione contiene la configurazione attualmente utilizzata da un dispositivo. La configurazione di un file di Configurazione di avvio diventa la Configurazione di esecuzione dopo il riavvio. I file di Configurazione di esecuzione e Configurazione di avvio sono formattati nel formato interno. I file di configurazione mirror, backup e remoti sono file di testo solitamente conservati per scopi di archiviazione, registrazione o ripristino. Durante la copia, il caricamento e il download di un file di configurazione di origine, il dispositivo trasforma automaticamente il contenuto di origine nel formato del file di destinazione, se i due file sono di formati diversi.

Indicatore SSD del file

Durante la copia del file di Configurazione di esecuzione o Configurazione di avvio in un file di configurazione di testo, il dispositivo genera e posiziona l'indicatore SSD del file nel file di configurazione di testo, indicando se il file contiene dati sensibili crittografati, dati sensibili in testo normale o esclude i dati sensibili.

- L'indicatore SSD, se esiste, deve essere contenuto nell'intestazione del file di configurazione.
- Un file di configurazione di testo che non include l'indicatore SSD è considerato privo di dati sensibili.
- L'indicatore SSD serve per applicare le autorizzazioni di lettura SSD ai file di configurazione di testo, ma viene ignorato durante la copia dei file di configurazione sul file di Configurazione di esecuzione o Configurazione di avvio.

L'indicatore SSD in un file viene impostato in base alle istruzioni dell'utente durante la copia, per includere dati sensibili crittografati, in testo normale o per escludere i dati sensibili dal file.

Blocco di controllo SSD

Quando un dispositivo crea un file di configurazione di testo dal file Configurazione di avvio o Configurazione di esecuzione, inserisce un blocco di controllo SSD nel file, se l'utente richiede il file per includere dati sensibili. Il blocco di controllo SSD, protetto da manomissione, contiene regole e proprietà SSD del dispositivo che crea il file. Un blocco di controllo SSD inizia e finisce rispettivamente con "ssd-control-start" e "ssd-control-end".

File di configurazione avvio

Attualmente il dispositivo supporta la copia dal file di Configurazione backup, Configurazione mirror e Configurazione remota su un file di Configurazione di avvio. Le configurazioni nella Configurazione di avvio entrano in vigore e diventano la Configurazione di esecuzione dopo il riavvio. Un utente può recuperare i dati sensibili crittografati o in testo normale da un file di configurazione di avvio in base alle autorizzazioni di lettura SSD e alla modalità di lettura SSD corrente della sessione di gestione.

L'accesso di lettura ai dati sensibili nella configurazione di avvio di ogni tipo è escluso se la frase chiave nel file Configurazione di avvio e la frase chiave locale sono diversi.

L'SSD aggiunge le seguenti regole durante la copia dei file di Configurazione backup, Configurazione mirror e Configurazione remota nel file di Configurazione di avvio:

- In seguito al ripristino delle impostazioni predefinite in un dispositivo, tutte le sue configurazioni, regole e proprietà SSD comprese, vengono riportate ai valori predefiniti.
- Se un file di configurazione di origine contiene dati sensibili crittografati, ma non presenta il blocco di controllo SSD, il dispositivo rifiuta il file di origine e la copia non viene eseguita.
- Se non è presente il blocco di controllo SSD nel file di configurazione di origine, la configurazione SSD nel file Configurazione di avvio viene riportata ai valori predefiniti.
- Qualora nel blocco di controllo SSD del file di configurazione di origine sia presente una frase chiave, il dispositivo rifiuta il file di origine e la copia non viene eseguita se nel file sono presenti dati sensibili crittografati, ma non dalla chiave generata dalla frase chiave del blocco di controllo SSD.

- Se nel file di configurazione di origine è presente un blocco di controllo SSD e il file non supera il controllo di integrità SSD e/o il controllo di integrità del file, il dispositivo rifiuta il file di origine e la copia non viene eseguita.
- In assenza di una frase chiave nel blocco di controllo SSD del file di configurazione di origine, tutti i dati sensibili crittografati presenti nel file devono essere crittografati dalla chiave generata dalla frase chiave locale o da quella generata dalla frase chiave predefinita, ma non da entrambe. In caso contrario, il file di origine viene rifiutato e la copia non viene eseguita.
- Il dispositivo configura la frase chiave, il controllo della frase chiave e l'integrità del file, se presente, dal blocco di controllo SSD del file di configurazione di origine sul file Configurazione di avvio. Configura il file Configurazione di avvio con la frase chiave utilizzata per generare la chiave utile a decrittografare i dati sensibili nel file di configurazione di origine. Qualsiasi configurazione SSD non trovata viene riportata alle impostazioni predefinite.
- In caso di blocco di controllo SSD nel file di configurazione di origine e se il file contiene dati sensibili in testo normale che escludono configurazioni SSD nel blocco di controllo SSD, il file viene accettato.

File di configurazione esecuzione

Il file Configurazione di esecuzione contiene la configurazione attualmente utilizzata da un dispositivo. Un utente può recuperare i dati sensibili crittografati o in testo normale da un file di configurazione di esecuzione in base alle autorizzazioni di lettura SSD e alla modalità di lettura SSD corrente della sessione di gestione. Per modificare la configurazione di esecuzione è possibile copiare i file di configurazione backup e configurazione mirror tramite altre operazioni di gestione mediante CLI, XML, SNMP e così via.

Un dispositivo applica le seguenti regole quando un utente modifica direttamente la configurazione SSD nella Configurazione di esecuzione:

- Se l'utente che ha aperto la sessione di gestione non dispone delle autorizzazioni SSD (ovvero autorizzazioni di lettura Entrambi o Solo testo normale), il dispositivo rifiuta tutti i comandi SSD.
- Se copiati da un file di origine, l'indicatore SSD del file, l'integrità del blocco di controllo SSD e l'integrità del file SSD non vengono né verificati, né applicati.

- Se copiati da un file di origine, la copia non viene eseguita quando la frase chiave del file di origine è in testo normale. Se la frase chiave è crittografata, viene ignorata.
- Durante la configurazione diretta della frase chiave (non la copia del file) nella Configurazione di esecuzione, la frase chiave nel comando deve essere inserita in testo normale. In caso contrario, il comando viene respinto.
- I comandi di configurazione con dati sensibili crittografati mediante la chiave generata dalla frase chiave locale sono configurati nella Configurazione di esecuzione. In caso contrario, il comando di configurazione genera un errore e non viene incluso nel file Configurazione di esecuzione.

File di Configurazione backup e Configurazione mirror

Un dispositivo genera periodicamente il proprio file di Configurazione mirror dal file di Configurazione di avvio se il servizio Configurazione mirror automatica è attivo. Un dispositivo genera sempre un file Configurazione mirror con dati sensibili crittografati. Pertanto, l'indicatore SSD del file in un file Configurazione mirror indica sempre che il file contiene dati sensibili crittografati.

Per impostazione predefinita, il servizio di Configurazione mirror automatica è attivo. Per configurare la Configurazione mirror automatica da attivare o disattivare, scegliere **Amministrazione > Gestione di file > Proprietà file di configurazione**.

L'utente può visualizzare, copiare e caricare file di configurazione backup e mirror completi, attenendosi alle autorizzazioni di lettura SSD, alla modalità di lettura corrente nella sessione e all'indicatore SSD del file nel file di origine, secondo le seguenti modalità:

- In assenza di indicatore SSD del file in un file di configurazione mirror o backup, tutti gli utenti possono accedere al file.
- Un utente dotato di autorizzazione di lettura Entrambi può accedere a tutti i file di configurazione mirror e backup. Tuttavia, se la modalità di lettura corrente della sessione è diversa dall'indicatore SSD del file, un messaggio all'utente indica che l'operazione non è consentita.
- Un utente con autorizzazione Solo testo normale può accedere ai file di configurazione mirror e backup se l'indicatore SSD del file mostra dati sensibili con autorizzazioni Escludi o Solo testo normale.

- Un utente con autorizzazione Solo con crittografia può accedere ai file di configurazione mirror e backup con il proprio indicatore SSD del file che mostra dati sensibili con autorizzazioni Escludi o Solo testo normale.
- Un utente con autorizzazione Escludi non può accedere ai file di configurazione mirror e backup con il proprio indicatore SSD del file che mostra dati sensibili con autorizzazioni Con crittografia o Testo normale.

L'utente deve modificare manualmente l'indicatore SSD del file in conflitto con i dati sensibili, se presente nel file. In caso contrario, i dati sensibili in testo normale potrebbero rimanere inaspettatamente visibili.

Configurazione automatica immediata dei dati sensibili

Configurazione automatica immediata dei dati sensibili è la configurazione automatica dei dispositivi di destinazione con dati sensibili crittografati, senza la necessità di preconfigurare manualmente i dispositivi di destinazione con la frase chiave relativa alla chiave utilizzata per crittografare i dati sensibili.

Il dispositivo attualmente supporta la Configurazione automatica, attiva per impostazione predefinita. Quando la Configurazione automatica è attiva su un dispositivo e il dispositivo riceve le opzioni DHCP che specificano un file server e un file di avvio, il dispositivo scarica il file di avvio (file di configurazione remota) nel file di Configurazione di avvio da un file server, quindi si riavvia.

NOTA Il file server è specificato dai campi bootp siaddr e sname, oltre all'opzione DHCP 150 ed è configurato staticamente sul dispositivo.

L'utente può configurare automaticamente e in sicurezza i dispositivi destinazione con dati sensibili crittografati, creando prima il file di configurazione da utilizzare nella configurazione automatica da un dispositivo che contiene le configurazioni. Il dispositivo deve essere configurato e comandato per:

- Crittografare i dati sensibili nel file
- Applicare l'integrità dei contenuti del file
- Includere i comandi di configurazione di autenticazione protetta e le regole SSD in grado di controllare e proteggere adeguatamente l'accesso a dispositivi e dati sensibili

Se il file di configurazione è stato generato con una frase chiave definita dall'utente e il controllo della frase chiave del file SSD è Limitato, il file di configurazione risultante è configurabile automaticamente sui dispositivi di destinazione richiesti. Tuttavia, per il completamento della configurazione automatica con una frase chiave definita dall'utente, i dispositivi di destinazione devono essere preconfigurati manualmente con la stessa frase chiave come dispositivo che genera i file, senza funzionalità immediate.

Se il dispositivo che crea il file di configurazione presenta un controllo frase chiave Illimitato, la frase chiave viene inclusa nel file. Di conseguenza, l'utente può configurare automaticamente i dispositivi di destinazione, inclusi quelli con impostazioni predefinite, per mezzo del file di configurazione senza dover preconfigurare manualmente i dispositivi di destinazione con la frase chiave. Si tratta quindi di una configurazione immediata, dato che i dispositivi di destinazione apprendono la frase chiave direttamente dal file di configurazione.

NOTA I dispositivi con le impostazioni predefinite utilizzano l'utente anonimo predefinito per accedere al server SCP.

Canali di gestione SSD

I dispositivi possono essere gestiti su canali di gestione come Telnet, SSH e Web. L'SSD categorizza i canali nei seguenti tipi, in base alla protezione e/o ai protocolli: Protetto, Non protetto, SNMP XML protetto e SNMP XML non protetto.

La seguente tabella descrive i criteri secondo i quali l'SSD considera un canale di gestione protetto o non protetto. Se non è protetto, la tabella indica il canale protetto parallelo.

Canale di gestione	Tipo canale di gestione SSD	Canale di gestione protetto parallelo
Console	Protetto	
Telnet	Non protetto	SSH
SSH	Protetto	
Interfaccia grafica utente/ HTTP	Non protetto	Interfaccia grafica utente/HTTPS
Interfaccia grafica utente/ HTTPS	Protetto	

Canale di gestione	Tipo canale di gestione SSD	Canale di gestione protetto parallelo
XML/HTTP	SNMP XML non protetto	XML/HTTPS
XML/HTTPS	SNMP XML protetto	
SNMPv1/v2/v3 senza privacy	SNMP XML non protetto	SNMP XML protetto
SNMPv3 con privacy	SNMP XML protetto (utenti di livello 15)	
TFTP	Non protetto	SCP
SCP (copia protetta)	Protetto	
Trasferimento di file basato su HTTP	Non protetto	Trasferimento di file basato su HTTPS
Trasferimento di file basato su HTTPS	Protetto	

CLI del menu e ripristino password

L'interfaccia CLI del menu è disponibile per gli utenti solo se le autorizzazioni di lettura sono Entrambi o Solo testo normale. Gli altri utenti vengono respinti. I dati sensibili nella CLI del menu sono sempre visualizzati come testo normale.

Il ripristino della password attualmente viene attivato dal menu di avvio e permette all'utente di accedere al terminale senza autenticazione. Se l'SSD è supportato, questa opzione è consentita solo nel caso in cui la frase chiave locale sia identica alla frase chiave predefinita. Se un dispositivo è configurato con una frase chiave definita dall'utente, l'utente non può attivare il ripristino della password.

Configurazione dell'SSD

La funzione SSD è configurata nelle seguenti pagine:

- Le proprietà dell'SSD vengono impostate nella pagina Proprietà.
- Le regole SSD sono definite nella pagina Regole SSD.

Proprietà SSD

Le proprietà SSD possono essere impostate solo dagli utenti con autorizzazioni di lettura SSD Solo testo normale o Entrambi.

Per configurare le proprietà SSD globali, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Gestione sicura dei dati sensibili** > **Proprietà**. Vengono visualizzati i seguenti campi:

- **Tipo di frase chiave locale corrente**: indica il tipo di frase chiave in uso: predefinita o definita dall'utente.

PASSAGGIO 2 Compilare i seguenti campi **Impostazioni permanenti**:

- **Controllo frase chiave del file di configurazione**: consente di selezionare un'opzione come descritto in **Controllo frase chiave del file di configurazione**.
- **Controllo integrità del file di configurazione**: selezionare questa opzione per attivare la funzione corrispondente. Vedere la sezione **Controllo dell'integrità del file di configurazione**.

PASSAGGIO 3 Selezionare la Modalità lettura per la sessione corrente (vedere **Elementi di una regola SSD**).

Per modificare la frase chiave locale, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Modifica frase chiave locale**, quindi immettere una nuova **frase chiave locale**:

- **Predefinito**: utilizza la frase chiave predefinita del dispositivo.
- **Definita dall'utente (testo normale)**: immettere una nuova frase chiave.
- **Conferma frase chiave**: confermare la nuova frase chiave.

Regole SSD

Le regole SSD possono essere impostate solo dagli utenti con autorizzazioni di lettura SSD Solo testo normale o Entrambi.

Per configurare le regole SSD, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Protezione** > **Gestione sicura dei dati sensibili** > **Regole SSD**.

Vengono visualizzate le regole definite attualmente.

PASSAGGIO 2 Per aggiungere una nuova regola, fare clic su **Aggiungi**. Immettere informazioni nei seguenti campi:

- **Utente**: consente di definire gli utenti a cui applicare la regola. Selezionare una delle seguenti opzioni:
  - *Utente specifico*: selezionare questa opzione e immettere il nome utente specifico a cui applicare la regola; non è obbligatorio definire l'utente.
  - *Utente predefinito (cisco)*: la regola viene applicata all'utente predefinito.
  - *Livello 15*: la regola viene applicata agli utenti con livello 15 di privilegio.
  - *Tutti*: la regola viene applicata a tutti gli utenti.
- **Canale**: consente di definire il livello di sicurezza del canale di ingresso a cui viene applicata la regola. Selezionare una delle seguenti opzioni:
  - *Protetto*: la regola viene applicata solo ai canali protetti (console, SCP, SSH e HTTPS), escludendo i canaliSNMP e XML.
  - *Non protetto*: la regola viene applicata solo ai canali non protetti (Telnet, TFTP e HTTP), escludendo i canaliSNMP e XML.
  - *SNMP XML protetto*: la regola viene applicata solo a XML su HTTPS o SNMPv3 con privacy.
  - *SNMP XML non protetto*: la regola viene applicata solo a XML su HTTP e/o SNMPv1/v2 e SNMPv3 senza privacy.
- **Autorizzazione di lettura**: le autorizzazioni di lettura sono associate alla regola e possono essere:
  - *Escludi*: autorizzazione di lettura minima. Gli utenti non sono autorizzati ad accedere ai dati sensibili in nessun caso.
  - *Solo testo normale*: autorizzazione di lettura maggiore rispetto a quelle precedenti. Gli utenti sono autorizzati ad accedere ai dati sensibili solo in testo normale.
  - *Solo con crittografia*: autorizzazione di lettura intermedia. Gli utenti sono autorizzati ad accedere ai dati sensibili solo con crittografia.

- *Entrambi (testo normale e con crittografia)*: autorizzazione di lettura massima. Gli utenti hanno sia le autorizzazioni con crittografia che in testo normale e sono autorizzati ad accedere ai dati sensibili con crittografia e in testo normale.

- **Modalità lettura predefinita**: tutte le modalità di lettura predefinite sono soggette all'autorizzazione di lettura della regola. Esistono le seguenti opzioni, ma alcune potrebbero essere rifiutate, a seconda dell'autorizzazione di lettura della regola applicata.
  - *Escludi*: non consente la lettura dei dati sensibili.
  - *Con crittografia*: i dati sensibili sono crittografati.
  - *Testo normale*: i dati sensibili sono visualizzati come testo normale.

PASSAGGIO 3 È possibile eseguire le seguenti operazioni:

- **Ripristina impostazioni predefinite**: sostituisce una regola predefinita modificata dall'utente con la regola predefinita originale.
- **Ripristina impostaz. predef. di tutte le regole**: sostituisce tutte le regole predefinite modificate dall'utente con le regole predefinite originali e rimuove le regole definite dall'utente.

27

Controllo di accesso

La funzione ACL (Access Control List) fa parte del meccanismo di protezione. Le definizioni ACL fungono da meccanismo per definire i flussi di traffico assegnati a una funzione QoS (Quality of Service) specifica. Per ulteriori informazioni, vedere la sezione **QoS**.

Gli ACL consentono ai responsabili di rete di definire modelli (filtro e azioni) per il traffico in ingresso. Ai pacchetti in ingresso su un dispositivo tramite una porta o gruppo LAG con un ACL attivo può essere negato o consentito l'accesso.

In questa sezione vengono illustrati i seguenti argomenti:

- **Elenco di controllo di accesso**
- **Definizione di ACL basati su MAC**
- **ACL basati su IPv4**
- **ACL basati su IPv6**
- **Definizione di un binding di ACL**

Elenco di controllo di accesso

Un ACL (Access Control List) è un elenco ordinato di filtri e azioni di classificazione. Ogni singola regola di classificazione, insieme alla sua azione, viene chiamata ACE (Access Control Element).

Ogni ACE è composto da filtri che distinguono i gruppi di traffico e le azioni associate. Un singolo ACL può contenere uno o più ACE, che vengono confrontati con i contenuti dei frame in ingresso. Ai frame i cui contenuti corrispondono al filtro viene applicata un'azione NEGA o CONSENTI.

Il dispositivo supporta massimo 512 ACL e 512 ACE.

Quando si riscontra corrispondenza fra un pacchetto e un filtro ACE, viene eseguita l'azione ACE e il processo di elaborazione di ACL viene interrotto. Se non si riscontra corrispondenza fra il pacchetto e il filtro ACE, viene elaborato l'ACE successivo. Se tutti gli ACE di un ACL sono stati elaborati senza trovare una corrispondenza ed esiste un altro ACL, questo viene elaborato in modo simile.

NOTA Se non viene trovata nessuna corrispondenza con nessun ACE in tutti gli ACL rilevanti, il pacchetto viene eliminato (come azione predefinita). A causa di questa azione di eliminazione predefinita, è necessario aggiungere esplicitamente ACE all'ACL per consentire il traffico desiderato, incluso il traffico di gestione come Telnet, HTTP o SNMP, indirizzato al dispositivo stesso. Per esempio, se non si desidera eliminare tutti i pacchetti che non corrispondono alle condizioni in un ACL, è necessario aggiungere esplicitamente una voce ACE di priorità più bassa nell'ACL che permette tutto il traffico.

Se lo snooping IGMP/MLD è attivato su una porta associata a un ACL, aggiungere filtri ACE nell'ACL per reindirizzare i pacchetti IGMP/MLD al dispositivo. Altrimenti, lo snooping IGMP/MLD non viene eseguito correttamente sulla porta.

L'ordine degli ACE nell'ACL è importante, dato che vengono applicati in base a una modalità first-fit. Gli ACE vengono elaborati in sequenza, a partire dal primo ACE.

Gli ACL possono essere utilizzati per motivi di sicurezza, per esempio consentendo o negando determinati flussi di traffico, oltre che per la classificazione e l'assegnazione delle priorità nella modalità QoS avanzata.

NOTA Una porta può essere protetta con gli ACL oppure configurata con criteri QoS avanzati, ma non entrambe le cose.

È consentito un solo ACL per porta, tuttavia è possibile associare un ACL basato su IP e a un ACL basato su IPv6 entrambi a una singola porta.

Per associare più ACL a una porta, è necessario utilizzare un criterio con una o più mappe delle classi.

È possibile definire i seguenti tipi di ACL (in base a quale parte dell'intestazione del frame viene esaminata):

- ACL MAC: esamina solo i campi Livello 2, come descritto in *Definizione di ACL basati su MAC*
- ACL IP: esamina il livello 3 dei frame IP, come descritto in *ACL basati su IPv4*
- ACL IPv6: esamina il livello 3 dei frame IPv4, come descritto in *Definizione di ACL basati su IPv6*

Se un frame corrisponde al filtro di un ACL, viene definito come flusso con il nome di tale ACL. Nella modalità QoS avanzata, è possibile fare riferimento a questi frame utilizzando questo Nome flusso e la QoS può essere applicata a tali frame (vedere **Modalità avanzata QoS**).

Creazione del flusso di lavoro degli ACL

Per creare ACL e associarli a un'interfaccia, attenersi alla seguente procedura:

1. Creare uno o più dei seguenti tipi di ACL:
   a. ACL basato su MAC utilizzando la pagina ACL basato su MAC e la pagina ACE basato su MAC
   b. ACL basato su IP utilizzando la pagina ACL basato su IPV4 e la pagina ACE basato su IPV4
   c. ACL basato su IPv6 utilizzando la pagina ACL basato su IPV6 e la pagina ACE basato su IPV6
2. Associare l'ACL alle interfacce utilizzando la pagina Binding di ACL.

Modifica del flusso di lavoro degli ACL

È possibile modificare un ACL solo se non è in uso. Di seguito viene descritto il processo di annullamento dell'associazione di un ACL per consentirne la modifica:

1. Se l'ACL non appartiene a una mappa delle classi in modalità QoS avanzata, ma è stato associato a un'interfaccia, annullare l'associazione dall'interfaccia utilizzando la pagina Binding di ACL.
2. Se l'ACL fa parte della mappa delle classi e non è associato a un'interfaccia, può essere modificato.
3. Se l'ACL fa parte di una mappa delle classi contenuta in un criterio associato a un'interfaccia, è necessario eseguire la catena di annullamento dell'associazione come indicato di seguito:
   - Annullare l'associazione del criterio contenente la mappa delle classi dall'interfaccia utilizzando la pagina *Binding del criterio*.
   - Eliminare la mappa delle classi contenente l'ACL dal criterio utilizzando *Configurazione di un Criterio* (**Modifica**).
   - Eliminare la mappa delle classi contenente l'ACL utilizzando *Definizione dell'Associazione classi*.

Solo dopo aver eseguito queste operazioni è possibile modificare l'ACL, come descritto in questa sezione.

Definizione di ACL basati su MAC

Gli ACL basati su MAC vengono utilizzati per filtrare il traffico in base ai campi Livello 2. Gli ACL basati su MAC verificano la disponibilità di una corrispondenza per tutti i frame.

Gli ACL basati su MAC sono definiti nella pagina ACL basato su MAC. Le regole vengono definite nella pagina ACE basato su MAC.

Per definire un ACL basato su MAC, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Controllo di accesso** > **ACL basato su MAC**.

Nella pagina viene visualizzato un elenco di tutti gli ACL basati su MAC attualmente definiti.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere il nome del nuovo ACL nel campo **Nome ACL**. I nomi degli ACL fanno distinzione tra maiuscole e minuscole.

PASSAGGIO 4 Fare clic su **Applica**. L'ACL basato su MAC viene salvato nel file di configurazione esecuzione.

Aggiunta di regole a un ACL basato su MAC

NOTA Ogni regola basata su MAC consuma una regola TCAM. L'allocazione TCAM viene eseguita a coppie, di modo che per il primo ACE vengono allocate 2 regole TCAM e la seconda regola TCAM viene allocata all'ACE successivo e così via.

Per aggiungere regole (ACE) a un ACL, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Controllo di accesso** > **ACE basato su MAC**.

PASSAGGIO 2 Selezionare un ACL e fare clic su **Vai**. Gli ACE nell'ACL vengono elencati.

PASSAGGIO 3 Fare clic su **Aggiungi**.

PASSAGGIO 4 Immettere i parametri.

- **Nome ACL**: viene indicato il nome dell'ACL a cui è stato aggiunto un ACE.
- **Priorità**: immettere la priorità dell'ACE. Gli ACE con priorità maggiore vengono elaborati per primi. Uno è la priorità più alta.

- **Azione**: selezionare l'azione eseguita al verificarsi di una corrispondenza. Sono disponibili le seguenti opzioni:
  - *Consenti*: reindirizzare i pacchetti che soddisfano i criteri ACE.
  - *Nega*: eliminare i pacchetti che soddisfano i criteri ACE.
  - *Arresta*: eliminare i pacchetti che soddisfano i criteri ACE e disattivare la porta da cui sono stati ricevuti i pacchetti. Queste porte possono essere riattivate nella pagina Impostazioni porta.
- **Intervallo di tempo**: seleziona questa opzione per limitare l'utilizzo dell'ACL per un determinato intervallo di tempo.
- **Nome intervallo di tempo**: se l'opzione **Intervallo di tempo** è selezionata, scegliere l'intervallo di tempo desiderato. Gli intervalli di tempo vengono definiti nella sezione **Intervallo di tempo**.
- **Indirizzo MAC di destinazione**: selezionare *Qualsiasi* se tutti gli indirizzi di destinazione sono accettabili o *Definito dall'utente* per immettere un indirizzo di destinazione o un intervallo di indirizzi di destinazione.
- **Valore indirizzo MAC di destinazione**: immettere l'indirizzo MAC a cui viene fatto corrispondere l'indirizzo MAC di destinazione e la relativa maschera (se presente).
- **Maschera controllo accesso MAC di destinazione**: immettere la maschera per definire un intervallo di indirizzi MAC. Si noti che questa maschera è diversa da quella utilizzata per altri usi, ad esempio la subnet mask. Qui l'impostazione di un bit come **1** indica "non importa" e **0** indica di mascherare quel valore.

  NOTA Data una maschera 0000 0000 0000 0000 0000 0000 1111 1111, si ottiene una corrispondenza sui bit in presenza dello zero, mentre non la si ottiene in presenza dei valori pari a 1. È necessario tradurre i valori pari a 1 in numeri interi decimali e scrivere 0 ogni quattro zeri. Nell'esempio 1111 1111 = 255, la maschera verrà scritta nel modo seguente: 0.0.0.255.
- **Indirizzo MAC di origine**: selezionare *Qualsiasi* se tutti gli indirizzi di origine sono accettabili o *Definiti dall'utente* per immettere un indirizzo di origine o un intervallo di indirizzi di origine.
- **Valore indirizzo MAC di origine**: immettere l'indirizzo MAC a cui viene fatto corrispondere l'indirizzo MAC di origine e la relativa maschera (se presente).
- **Maschera controllo accesso MAC di origine**: immettere la maschera per definire un intervallo di indirizzi MAC.

- **ID VLAN**: immettere la sezione ID VLAN del tag VLAN per corrispondenza.
- **802.1p**: selezionare **Includi** per utilizzare 802.1p.
- **Valore 802.1p**: immettere il valore 802.1p da aggiungere al tag VPT.
- **Maschera 802.1p**: immettere la maschera di controllo di accesso da applicare al tag VPT.
- **Tipo connessione Ethernet**: immettere il tipo connessione Ethernet del frame da soddisfare.

PASSAGGIO 5 Fare clic su **Applica**. L'ACE basato su MAC viene salvato nel file di configurazione esecuzione.

ACL basati su IPv4

Gli ACL basati su IPv4 vengono utilizzati per verificare i pacchetti IPv4, mentre gli altri tipi di frame, ad esempio gli ARP, non vengono verificati.

È possibile soddisfare i seguenti campi:

- Protocollo IP (per nome per i protocolli noti oppure direttamente per valore)
- Porte di origine/di destinazione per il traffico TCP/UDP
- Valori flag per i frame TCP
- Tipo e codice ICMP e IGMP
- Indirizzi IP di origine/di destinazione (inclusi controlli di accesso)
- Valore precedenza DSCP/IP

NOTA Gli ACL vengono utilizzati anche come elementi di creazione delle definizioni di flussi per la gestione di QoS basata sul flusso (vedere **Modalità avanzata QoS**).

La pagina ACL basato su IPv4 consente di aggiungere ACL al sistema. Le regole vengono definite nella pagina ACE basato su IPv4.

Gli ACL IPv6 sono definiti nella pagina ACL basato su IPv6.

Definizione di ACL basati su IPv4

Per definire un ACL basato su IPv4, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Controllo di accesso** > **ACL basato su IPv4**.

Nella pagina vengono visualizzati tutti gli ACL basati su IPv4 attualmente definiti.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere il nome del nuovo ACL nel campo **Nome ACL**. I nomi fanno distinzione tra maiuscole e minuscole.

PASSAGGIO 4 Fare clic su **Applica**. L'ACL basato su IPv4 viene salvato nel file di configurazione esecuzione.

Aggiunta di regole (ACE) a un ACL basato su IPv4

NOTA Ogni regola basata su IPv4 consuma una regola TCAM. L'allocazione TCAM viene eseguita a coppie, di modo che per il primo ACE vengono allocate 2 regole TCAM e la seconda regola TCAM viene allocata all'ACE successivo e così via.

Per aggiungere regole (ACE) a un ACL basato su IPv4, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Controllo di accesso** > **ACE basato su IPv4**.

PASSAGGIO 2 Selezionare un ACL e fare clic su **Vai**. Vengono visualizzati tutti gli ACE IP attualmente definiti per l'ACL selezionato.

PASSAGGIO 3 Fare clic su **Aggiungi**.

PASSAGGIO 4 Immettere i parametri.

- **Nome ACL**: viene visualizzato il nome dell'ACL.
- **Priorità**: immettere la priorità. Gli ACE con priorità maggiore vengono elaborati per primi.
- **Azione**: selezionare l'azione assegnata al pacchetto che corrisponde all'ACE. Le opzioni disponibili sono:
  - *Consenti*: reindirizzare i pacchetti che soddisfano i criteri ACE.
  - *Nega*: eliminare i pacchetti che soddisfano i criteri ACE.

- *Arresta*: eliminare i pacchetti che soddisfano i criteri ACE e disattivare la porta a cui il pacchetto era indirizzato. Le porte vengono riattivate nella pagina Gestione porte.

- **Intervallo di tempo**: seleziona questa opzione per limitare l'utilizzo dell'ACL per un determinato intervallo di tempo.
- **Nome intervallo di tempo**: se l'opzione **Intervallo di tempo** è selezionata, scegliere l'intervallo di tempo desiderato. Gli intervalli di tempo vengono definiti nella sezione **Intervallo di tempo**.
- **Protocollo**: selezionare per creare un ACE basato su un protocollo specifico o un ID protocollo. Selezionare *Qualsiasi (IP)* per accettare tutti i protocolli IP. Altrimenti, selezionare uno dei seguenti protocolli dall'elenco a discesa:
  - *ICMP*: Internet Control Message Protocol
  - *IGMP*: Internet Group Management Protocol
  - *IP in IP*: incapsulamento di IP in IP
  - *TCP*: Transmission Control Protocol
  - *EGP*: Exterior Gateway Protocol
  - *IGP*: Interior Gateway Protocol
  - *UDP*: User Datagram Protocol
  - *HMP*: Host Mapping Protocol
  - *RDP*: Reliable Datagram Protocol
  - *IDPR*: Inter-Domain Policy Routing Protocol
  - *IPV6*: IPv6 su tunnel IPv4
  - *IPV6:ROUT*: confronta i pacchetti appartenenti al percorso IPv6 over IPv4 tramite un gateway
  - *IPV6:FRAG*: confronta i pacchetti appartenenti all'intestazione di frammenti IPv6 over IPv4
  - *IDRP*: Inter-Domain Routing Protocol
  - *RSVP*: ReSerVation Protocol
  - *AH*: Authentication Header
  - *IPV6:ICMP*: Internet Control Message Protocol

- *EIGRP*: Enhanced Interior Gateway Routing Protocol
- *OSPF*: Open Shortest Path First
- *IPIP*: IP in IP
- *PIM*: Protocol Independent Multicast
- *L2TP*: Layer 2 Tunneling Protocol
- *ISIS*: protocollo specifico di IGP

- **ID protocollo per corrispondenza**: invece di selezionare il nome, immettere l'ID protocollo.
- **Indirizzo IP di origine**: selezionare *Qualsiasi* se tutti gli indirizzi di origine sono accettabili o *Definiti dall'utente* per immettere un indirizzo di origine o un intervallo di indirizzi di origine.
- **Valore indirizzo IP di origine**: immettere l'indirizzo IP a cui viene fatto corrispondere l'indirizzo IP di origine.
- **Maschera controllo accesso IP di origine**: immettere la maschera per definire un intervallo di indirizzi IP. Si noti che questa maschera è diversa da quella utilizzata per altri usi, ad esempio la subnet mask. Qui l'impostazione di un bit come 1 indica "non importa" e 0 indica di mascherare quel valore.

  NOTA Data una maschera 0000 0000 0000 0000 0000 0000 1111 1111, si ottiene una corrispondenza sui bit in presenza dello zero, mentre non la si ottiene in presenza dei valori pari a 1. È necessario tradurre i valori pari a 1 in numeri interi decimali e scrivere 0 ogni quattro zeri. Nell'esempio 1111 1111 = 255, la maschera verrà scritta nel modo seguente: 0.0.0.255.
- **Indirizzo IP di destinazione**: selezionare *Qualsiasi* se tutti gli indirizzi di destinazione sono accettabili o *Definiti dall'utente* per immettere un indirizzo di destinazione o un intervallo di indirizzi di destinazione.
- **Valore indirizzo IP di destinazione**: immettere l'indirizzo IP a cui viene fatto corrispondere l'indirizzo IP di destinazione.
- **Maschera controllo accesso IP di destinazione**: immettere la maschera per definire un intervallo di indirizzi IP.
- **Porta di origine**: selezionare una delle seguenti opzioni.
  - *Qualsiasi*: far corrispondere a tutte le porte di origine.

- *Singola*: immettere una singola porta TCP/UDP di origine a cui vengono fatti corrispondere i pacchetti. Questo campo è attivo solo se nella casella a discesa Seleziona da elenco è stato selezionato 800/6-TCP o 800/17-UDP.
- *Intervallo*: selezionare un intervallo di porte TCP/UDP di origine a cui viene fatto corrispondere il pacchetto. Esistono otto diversi intervalli di porte che è possibile configurare (tra porte di origine e di destinazione). Ogni protocollo TCP e UDP ha otto intervalli di porte.

- **Porta di destinazione**: selezionare uno dei valori disponibili, che sono uguali a quelli del campo Porta di origine descritto sopra.

  NOTA È necessario specificare il protocollo IP per l'ACE prima di poter immettere la porta di origine e/o di destinazione.

- **Flag TCP**: selezionare uno o più flag TCP con cui filtrare i pacchetti. I pacchetti filtrati vengono reindirizzati o eliminati. Il filtraggio di pacchetti basato su flag TCP consente di migliorare il controllo dei pacchetti e quindi la sicurezza della rete.
- **Tipo di servizio**: **il tipo di servizio del pacchetto IP.**
  - *Qualsiasi*: qualsiasi tipo di servizio.
  - *DSCP per corrispondenza*: DSCP (Differentiated Serves Code Point) per corrispondenza.
  - *Precedenza IP per* **corrispondenza**: la precedenza IP è un modello di TOS (Type Of Service, tipo di servizio) che la rete utilizza per aiutare ad assumere gli impegni QoS appropriati. Questo modello utilizza i 3 bit più significativi del byte del tipo di servizio nell'intestazione IP, come descritto in RFC 791 e RFC 1349.
- **ICMP**: se il protocollo IP dell'ACL è ICMP, selezionare il tipo di messaggio ICMP utilizzato per operazioni di filtro. Selezionare il tipo di messaggio per nome oppure immettere il numero del tipo di messaggio:
  - *Qualsiasi*: vengono accettati tutti i tipi di messaggio.
  - *Seleziona da elenco*: selezionare il tipo di messaggio per nome.
  - *Tipo ICMP per corrispondenza*: numero del tipo di messaggio da utilizzare per operazioni di filtro.

- **Codice ICMP**: i messaggi ICMP possono avere un campo codice che indica come gestire il messaggio. Selezionare una delle seguenti opzioni per decidere se applicare il filtro su questo codice.
  - *Qualsiasi*: accettare tutti i codici.
  - *Definito dall'utente*: immettere un codice ICMP per operazioni di filtro.
- **IGMP**: se l'ACL è basato su IGMP, selezionare il tipo di messaggio IGMP da utilizzare per operazioni di filtro. Selezionare il tipo di messaggio per nome oppure immettere il numero del tipo di messaggio:
  - *Qualsiasi*: vengono accettati tutti i tipi di messaggio.
  - *Seleziona da elenco*: selezionare il tipo di messaggio per nome.
  - *Tipo IGMP per corrispondenza*: numero del tipo di messaggio che viene utilizzato per operazioni di filtro.

PASSAGGIO 5 Fare clic su **Applica**. L'ACE basato su IPv4 viene salvato nel file di configurazione esecuzione.

ACL basati su IPv6

Nella pagina ACL basato su IPv6 viene visualizzata e attivata la creazione di ACL IPv6 che controllano il traffico puro basato su IPv6. Gli ACL IPv6 non controllano i pacchetti IPv6 su IPv4 o ARP.

NOTA Gli ACL vengono utilizzati anche come elementi di creazione delle definizioni di flussi per la gestione di QoS basata sul flusso (vedere **Modalità avanzata QoS**).

Definizione di un ACL basato su IPv6

Per definire un ACL basato su IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Controllo di accesso** > **ACL basato su IPv6**.

Nella finestra viene visualizzato l'elenco di ACL definiti e i relativi contenuti.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere il nome di un nuovo ACL nel campo **Nome ACL**. I nomi fanno distinzione tra maiuscole e minuscole.

PASSAGGIO 4 Fare clic su **Applica**. L'ACL basato su IPv6 viene salvato nel file di configurazione esecuzione.

Aggiunta di regole (ACE) a un ACL basato su IPv6

NOTA Ogni regola basata su IPv6 consuma due regole TCAM.

PASSAGGIO 1 Scegliere **Controllo di accesso** > **ACE basato su IPv6**.

In questa finestra viene visualizzato l'ACE (regole) per un ACL specifico (gruppo di regole).

PASSAGGIO 2 Selezionare un ACL e fare clic su **Vai**. Vengono visualizzati tutti gli ACE IP attualmente definiti per l'ACL selezionato.

PASSAGGIO 3 Fare clic su **Aggiungi**.

PASSAGGIO 4 Immettere i parametri.

- **Nome ACL**: viene indicato il nome dell'ACL a cui è stato aggiunto un ACE.
- **Priorità**: immettere la priorità. Gli ACE con priorità maggiore vengono elaborati per primi.
- **Azione**: selezionare l'azione assegnata al pacchetto che corrisponde all'ACE. Le opzioni disponibili sono:
  - *Consenti*: reindirizzare i pacchetti che soddisfano i criteri ACE.
  - *Nega*: eliminare i pacchetti che soddisfano i criteri ACE.
  - *Arresta*: eliminare i pacchetti che soddisfano i criteri ACE e disattivare la porta a cui i pacchetti erano indirizzati. Le porte vengono riattivate nella pagina Gestione porte.
- **Intervallo di tempo**: seleziona questa opzione per limitare l'utilizzo dell'ACL per un determinato intervallo di tempo.
- **Nome intervallo di tempo**: se l'opzione **Intervallo di tempo** è selezionata, scegliere l'intervallo di tempo desiderato. Gli intervalli di tempo vengono descritti nella sezione **Intervallo di tempo**.

- **Protocollo**: selezionare per creare un ACE basato su un protocollo specifico. Selezionare *Qualsiasi (IPv6)* per accettare tutti i protocolli IP. Altrimenti, selezionare uno dei seguenti protocolli:
  - *TCP*: Transmission Control Protocol. Attiva due host per la comunicazione e lo scambio di flussi di dati. TCP garantisce la consegna dei pacchetti e che i pacchetti vengano trasmessi e ricevuti nell'ordine in cui sono stati inviati.
  - *UDP*: User Datagram Protocol. Trasmette i pacchetti ma non ne garantisce la consegna.
  - *ICMP*: confronta i pacchetti con l'Internet Control Message Protocol (ICMP).
- **ID protocollo per corrispondenza**: immettere l'ID del protocollo da soddisfare.
- **Indirizzo IP di origine**: selezionare *Qualsiasi* se tutti gli indirizzi di origine sono accettabili o *Definiti dall'utente* per immettere un indirizzo di origine o un intervallo di indirizzi di origine.
- **Valore indirizzo IP di origine**: immettere l'indirizzo IP a cui viene fatto corrispondere l'indirizzo IP di origine e la relativa maschera (se presente).
- **Lunghezza prefisso IP di origine**: immettere la lunghezza del prefisso dell'indirizzo IP di origine.
- **Indirizzo IP di destinazione**: selezionare *Qualsiasi* se tutti gli indirizzi di destinazione sono accettabili o *Definiti dall'utente* per immettere un indirizzo di destinazione o un intervallo di indirizzi di destinazione.
- **Valore indirizzo IP di destinazione**: immettere l'indirizzo IP a cui viene fatto corrispondere l'indirizzo MAC di destinazione e la relativa maschera (se presente).
- **Lunghezza prefisso IP di destinazione**: immettere la lunghezza del prefisso dell'indirizzo IP.
- **Porta di origine**: selezionare una delle seguenti opzioni.
  - *Qualsiasi*: far corrispondere a tutte le porte di origine.
  - *Singola*: immettere una singola porta TCP/UDP di origine a cui vengono fatti corrispondere i pacchetti. Questo campo è attivo solo se nella casella a discesa Seleziona da elenco è stato selezionato 800/6-TCP o 800/17-UDP.

- *Intervallo*: selezionare un intervallo di porte TCP/UDP di origine a cui viene fatto corrispondere il pacchetto.

- **Porta di destinazione**: selezionare uno dei valori disponibili (sono uguali a quelli del campo Porta di origine descritto sopra).

  NOTA È necessario specificare il protocollo IPv6 per l'ACL prima di poter configurare la porta di origine e/o di destinazione.

- **Flag TCP**: selezionare uno o più flag TCP con cui filtrare i pacchetti. I pacchetti filtrati vengono reindirizzati o eliminati. Il filtraggio di pacchetti basato su flag TCP consente di migliorare il controllo dei pacchetti e quindi la sicurezza della rete.
  - Imposta: corrispondenza se il flag è IMPOSTATO.
  - Annulla impost.: corrispondenza se il flag è NON IMPOSTATO.
  - Non importa: ignorare il flag TCP.
- **Tipo di servizio**: il tipo di servizio del pacchetto IP.
- **ICMP**: se l'ACL è basato su ICMP, selezionare il tipo di messaggio ICMP da utilizzare per operazioni di filtro. Selezionare il tipo di messaggio per nome oppure immettere il numero del tipo di messaggio. Se vengono accettati tutti i tipi di messaggio, selezionare *Qualsiasi*.
  - *Qualsiasi*: vengono accettati tutti i tipi di messaggio.
  - *Seleziona da elenco*: selezionare il tipo di messaggio per nome dall'elenco a discesa.
  - *Tipo ICMP per corrispondenza*: numero del tipo di messaggio che viene utilizzato per operazioni di filtro.
- **Codice ICMP**: i messaggi ICMP possono avere un campo codice che indica come gestire il messaggio. Selezionare una delle seguenti opzioni per decidere se applicare il filtro su questo codice.
  - *Qualsiasi*: accettare tutti i codici.
  - *Definito dall'utente*: immettere un codice ICMP per operazioni di filtro.

PASSAGGIO 5 Fare clic su **Applica**.

Definizione di un binding di ACL

Quando un ACL viene associato a un'interfaccia (porta, LAg o VLAN), le regole ACE corrispondenti vengono applicate ai pacchetti in arrivo sull'interfaccia. I pacchetti che non corrispondono a nessun ACE nell'ACL vengono confrontati con una regola predefinita, la cui azione è eliminare i pacchetti privi di corrispondenza.

Sebbene ogni interfaccia possa essere associata a un solo ACL, più interfacce possono essere associate allo stesso ACL, raggruppandole in una mappa di criteri e associando quella mappa di criteri all'interfaccia.

Dopo che un ACL viene associato a un'interfaccia, non è possibile eliminarlo o modificarlo fino a quando non viene rimosso da tutte le porte a cui è associato o su cui è in uso.

NOTA È possibile associare un'interfaccia (porta, LAG o VLAN) a un criterio o a un ACL ma non è possibile associarli entrambi sia a un criterio che a un ACL.

Per associare un ACL a una porta o LAG, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Controllo di accesso** > **Binding di ACL (porta)**.

PASSAGGIO 2 Selezionare un tipo di interfaccia **Porte/LAG** (porta o LAG).

PASSAGGIO 3 Scegliere **Vai**. Per ogni tipo di interfaccia selezionata, tutte le interfacce di quel tipo vengono visualizzate con un elenco dei relativi ACL correnti.

- **Interfaccia**: identificatore dell'interfaccia.
- **ACL MAC**: ACL di tipo MAC associati all'interfaccia (se presenti).
- **ACL IPv4**: ACL di tipo IPV4 associati all'interfaccia (se presenti).
- **ACL IPv6**: ACL di tipo IPV6 associati all'interfaccia (se presenti).

NOTA Per annullare l'associazione di ACL da un'interfaccia, selezionare l'interfaccia e fare clic su **Cancella**.

PASSAGGIO 4 Selezionare un'interfaccia e fare clic su **Modifica**.

PASSAGGIO 5 Selezionare una delle seguenti opzioni:

- **Seleziona ACL basato su MAC**: selezionare un ACL basato su MAC da associare all'interfaccia.
- **Seleziona ACL basato su IPv4**: selezionare un ACL basato su IPv4 da associare all'interfaccia.

- **Seleziona ACL basato su IPv6**: selezionare un ACL basato su IPv6 da associare all'interfaccia.
- **Azione predefinita**: selezionare una delle seguenti opzioni:
  - *Nega tutti*: se il pacchetto non corrisponde a un ACL, viene negato (eliminato).
  - *Consenti tutti*: se il pacchetto non corrisponde a un ACL, viene consentito (inoltrato).

  NOTA È possibile selezionare Azione predefinita solo se la Guardia origine IP non è attiva sull'interfaccia.

PASSAGGIO 6 Fare clic su **Applica**. Il binding ACL viene modificato e il file Configurazione di esecuzione viene aggiornato.

NOTA Se non viene selezionato alcun ACL, l'associazione degli ACL precedentemente associati all'interfaccia viene annullata.

Per associare un ACL a una VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Controllo di accesso** > **Binding di ACL (VLAN)**.

PASSAGGIO 2 Selezionare una VLAN e fare clic su **Modifica**.

Se la VLAN richiesta non è visualizzata, aggiungerne una nuova.

PASSAGGIO 3 Selezionare una delle seguenti opzioni:

- **Seleziona ACL basato su MAC**: selezionare un ACL basato su MAC da associare all'interfaccia.
- **Seleziona ACL basato su IPv4**: selezionare un ACL basato su IPv4 da associare all'interfaccia.
- **Seleziona ACL basato su IPv6**: selezionare un ACL basato su IPv6 da associare all'interfaccia.
- **Azione predefinita**: selezionare una delle seguenti opzioni:
  - *Nega tutti*: se il pacchetto non corrisponde a un ACL, viene negato (eliminato).
  - *Consenti tutti*: se il pacchetto non corrisponde a un ACL, viene consentito (inoltrato).

  NOTA È possibile selezionare Azione predefinita solo se la Guardia origine IP non è attiva sull'interfaccia.

PASSAGGIO 4 Fare clic su **Applica**. Il binding ACL viene modificato e il file Configurazione di esecuzione viene aggiornato.

NOTA Se non viene selezionato alcun ACL, l'associazione degli ACL precedentemente associati alla VLAN viene annullata.

28

QoS

La funzione Qualità del servizio viene applicata su tutta la rete al fine di garantire che la priorità del traffico di rete venga assegnata in base ai criteri indicati e che il traffico desiderato venga elaborato con modalità preferenziali.

In questa sezione vengono illustrati i seguenti argomenti:

- **Funzioni e componenti di QoS**
- **Configurazione QoS - Generale**
- **Modalità QoS di base**
- **Modalità avanzata QoS**
- **Gestione delle statistiche QoS**

Funzioni e componenti di QoS

La funzione QoS viene utilizzata per ottimizzare le prestazioni della rete.

QoS consente di eseguire la seguente operazione:

- Classificazione del traffico in ingresso in classi di traffico, in base agli attributi, inclusi:
  - Configurazione dispositivo
  - Interfaccia di ingresso
  - Contenuto dei pacchetti
  - Combinazione degli attributi

QoS include le funzioni seguenti:

- **Classificazione del traffico**: consente di classificare ciascun pacchetto in ingresso come parte di un flusso del traffico specifico, in base ai contenuti dei pacchetti e/o alla porta. La classificazione viene effettuata tramite ACL (Access Control List, elenco di controllo degli accessi) e solo il traffico che soddisfa i criteri ACL è soggetto alla classificazione CoS o QoS.
- **Assegnazione a code hardware**: consente di assegnare pacchetti in ingresso a code di reindirizzamento. I pacchetti vengono inviati a una determinata coda e gestiti come una funzione della classe di traffico a cui appartengono. Vedere **Configurazione delle code QoS**.
- **Attributi per la gestione di altre classi di traffico**: applica il meccanismo QoS a classi diverse, inclusa la gestione della larghezza di banda.

Funzionamento di QoS

Il tipo di campo dell'intestazione da associare viene inserito nella pagina Impostazioni generali. Per ciascun valore di quel campo, nella pagina CoS/802.1p a Coda o nella pagina DSCP alla Coda (a seconda che la modalità trust sia CoS/802.1p o DSCP, rispettivamente) viene assegnata una coda di uscita, indicante il punto in cui viene inviato il frame.

Modalità QoS

La modalità QoS selezionata viene applicata a tutte le interfacce del sistema.

- **Modalità di base**: CoS (Class of Service, Classe di servizio).

  Tutto il traffico della stessa classe viene elaborato secondo la medesima modalità, ovvero l'unica operazione QoS che determina la coda di uscita sulla porta di uscita, in base al valore QoS indicato nel frame in ingresso. Questo corrisponde al valore 802.1p del tag di priorità VLAN (VPT, VLAN Priority Tag) nel Livello 2 e al valore DSCP (Differentiated Service Code Point) per IPv4 o il valore TC (Traffic Class) per IPv6 nel Livello 3. In modalità di base, il dispositivo viene associato al valore QoS esterno assegnato. Tale valore determina la classe di traffico e il QoS.

  Il campo dell'intestazione da associare viene inserito nella pagina Impostazioni generali. Per ciascun valore di quel campo, nella pagina CoS/802.1p a coda o nella pagina DSCP alla coda (a seconda che la modalità trust sia CoS/802.1p o DSCP, rispettivamente) viene assegnata una coda di uscita in cui viene inviato il frame.

- **Modalità avanzata**: Qualità del servizio (QoS) basata sul flusso.

  In modalità avanzata, un QoS per flusso include una mappa delle classi e/o una funzionalità di monitoraggio:

  - Una mappa delle classi definisce il tipo di traffico in un flusso, e include uno o più ACL. I pacchetti che corrispondono agli elenchi ACL appartengono al flusso.
  - Una funzionalità di monitoraggio viene applicata al QoS configurato in un flusso. La configurazione del QoS di un flusso può essere costituito da una coda di uscita, dal valore DSCP o COS/802.1 e dalle azioni eseguite sul traffico (in eccesso) fuori dal profilo.

- **Modalità di disattivazione**: in questa modalità, tutto il traffico viene associato a una singola coda best-effort, in modo che nessun tipo di traffico abbia la priorità sugli altri.

È possibile attivare una sola modalità alla volta. Quando il sistema viene configurato per operare in modalità avanzata QoS, le impostazioni della modalità QoS di base non sono attive, e viceversa.

Quando si modifica la modalità, si verificano le azioni seguenti:

- Quando si passa dalla modalità avanzata QoS a un altro tipo di modalità, le definizioni del profilo del criterio e le mappe delle classi vengono eliminate. Gli ACL collegati direttamente alle interfacce rimangono invariati.
- Quando si passa dalla modalità QoS di base alla modalità avanzata, la configurazione della modalità trust QoS in Modalità di base non viene mantenuta.
- Quando si disattiva il QoS, le impostazioni del normalizzatore e della coda (impostazione della larghezza di banda WRR/SP) tornano ai valori predefiniti.

Tutte le altre configurazioni effettuate dall'utente rimangono invariate.

Flusso di lavoro del QoS

Per configurare i parametri generali QoS, eseguire le seguenti operazioni:

PASSAGGIO 1 Utilizzare la pagina Proprietà QoS per scegliere il tipo di modalità QoS per il sistema (base, avanzata o disattivata, come descritto nella sezione **"Modalità QoS"**). Le seguenti operazioni eseguite nel flusso di lavoro presumono che sia stato scelto di attivare il QoS.

PASSAGGIO 2 Utilizzare la pagina Proprietà QoS per assegnare a ogni interfaccia una priorità predefinita CoS.

PASSAGGIO 3 Utilizzare la pagina Coda per assegnare il metodo di pianificazione (Priorità stretta o WRR) e la larghezza di banda per WRR sulle code di uscita.

PASSAGGIO 4 Indicare una coda di uscita per ciascun valore IP DSCP/TC nella pagina DSCP alla coda. Se il dispositivo è in modalità trust DSCP, i pacchetti in ingresso vengono inseriti nelle code di uscita, sulla base del loro valore DSCP/TC.

PASSAGGIO 5 Indicare una coda di uscita per ciascuna priorità CoS/802.1p. Se il dispositivo è in modalità trust CoS/802.1, tutti i pacchetti in ingresso verranno inseriti nelle code di uscita indicate, in base alla priorità CoS/802.1p dei pacchetti. Questa operazione viene eseguita nella pagina CoS/802.1p a coda.

PASSAGGIO 6 Se necessario solo per il traffico di livello 3, utilizzare la pagina DSCP a coda per assegnare una coda a ciascun valore DSCP/TC.

PASSAGGIO 7 Inserire i limiti della larghezza di banda e di velocità nelle pagine seguenti:

a. Impostare la normalizzazione in uscita per coda tramite la pagina omonima.

b. Utilizzare la pagina Larghezza di banda per impostare il limite di velocità in ingresso e la velocità di normalizzazione in uscita per porta.

PASSAGGIO 8 Configurare la modalità selezionata tramite una delle operazioni seguenti:

a. Configurare la modalità di base, come descritto nella sezione *Flusso di lavoro per la configurazione della modalità QoS di base*.

b. Configurare la modalità avanzata, come descritto nella sezione *Flusso di lavoro per la configurazione della modalità avanzata QoS*.

Configurazione QoS - Generale

La pagina Proprietà QoS contiene i campi per l'impostazione della modalità QoS per il sistema (base, avanzata o disattivata, come descritto nella sezione **"Modalità QoS"**). Inoltre, è possibile definire la proprietà CoS predefinita di ciascuna interfaccia.

Impostazioni delle proprietà QoS

Per selezionare la modalità QoS, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Qualità del servizio** > **Generale** > **Proprietà QoS**.

PASSAGGIO 2 Impostare la modalità QoS. Sono disponibili le seguenti opzioni:

- **Disattiva**: QoS viene disattivato sul dispositivo.
- **Base**: QoS è attivo sul dispositivo in modalità di base.
- **Avanzato**: QoS è attivo sul dispositivo in modalità avanzata.

PASSAGGIO 3 Selezionare **Porta/LAG** e fare clic su **Vai** per visualizzare/modificare tutte le porte/LAG sul dispositivo e le informazioni sul CoS.

Per tutte le porte/LAG vengono visualizzati i campi seguenti:

- **Interfaccia**: tipo di interfaccia.
- **CoS predefinito**: valore VPT predefinito per i pacchetti in ingresso che non hanno un tag VLAN. Il CoS predefinito è 0. Tale valore è rilevante solo per i frame senza tag e solo se il sistema è in modalità di base e nella pagina Impostazioni generali è selezionato Trust CoS.

Selezionare **Ripristina impostazioni predefinite** per ripristinare l'impostazione CoS predefinita per questa interfaccia.

PASSAGGIO 4 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Per impostare QoS su un'interfaccia, selezionarlo e fare clic su **Modifica**.

PASSAGGIO 1 Immettere i parametri.

- **Interfaccia**: selezionare una porta o un LAG.
- **CoS predefinito**: selezionare il valore CoS (Class-of-Service) predefinito da assegnare ai pacchetti in ingresso (che non hanno un tag VLAN).

PASSAGGIO 2 Fare clic su **Applica**. Il valore CoS predefinito dell'interfaccia viene salvato nel file di configurazione esecuzione.

Configurazione delle code QoS

Il dispositivo supporta code con priorità 4 o 8 per ogni interfaccia selezionata nella pagina Modalità Sistema e Gestione stack. Il numero di coda quattro o otto rappresenta la coda con priorità più alta. Il numero uno rappresenta invece la coda con priorità più bassa.

È possibile determinare la modalità di gestione del traffico nelle code in due modi: Priorità stretta (Strict Priority) e WRR (Weighted Round Robin, round-robin pesato).

- **Priorità stretta**: il traffico in uscita della coda con priorità più alta viene trasmesso per primo. Il traffico proveniente dalle code con priorità più bassa viene elaborato solo dopo la trasmissione della coda con priorità più alta, quindi fornendo il livello più alto di priorità del traffico alla coda con numero più alto.
- **WRR (Weighted Round Robin, round-robin pesato)**: in modalità WRR il numero di pacchetti inviati dalla coda è proporzionale al peso della coda (maggiore è il peso maggiore sarà il numero di frame inviati). Ad esempio, se ci sono massimo quattro code, tutte di tipo WRR, e viene usato il peso predefinito, la coda 1 riceve 1/15 della larghezza di banda (supponendo che le code siano piene e che si verifichi una congestione), la coda 2 riceve 2/15, la coda 3 4/15 e la coda 4 riceve 8/15 della larghezza di banda. Il tipo di algoritmo WRR utilizzato nel dispositivo non è il Deficit WRR (DWRR) standard, ma lo Shaped Deficit WRR (SDWRR).

Le modalità di accodamento possono essere selezionate nella pagina Coda. Se la modalità di coda è Priorità stretta, la priorità imposta l'ordine in cui le code vengono servite, partendo dalla coda 4 o 8 (coda con priorità più alta) e passando a quella successiva al completamento di ogni coda.

Quando la modalità di accodamento è Weighted Round Robin, le code vengono servite fino al raggiungimento della soglia massima e successivamente viene servita un'altra coda.

È inoltre possibile assegnare al WRR alcune delle quattro code più basse, mantenendo allo stesso tempo la priorità stretta in alcune code con priorità più alta. In questo caso, il traffico delle code a stretta priorità viene sempre inviato prima del traffico delle code WRR. Il traffico delle code WRR viene inoltrato solo dopo che le code a stretta priorità sono state svuotate. La parte di ciascuna coda WRR dipende dal peso.

Per selezionare il metodo di priorità e inserire dati WRR, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Generale** > **Coda**.

PASSAGGIO 2 Immettere i parametri.

- **Coda**: viene indicato il numero della coda.
- **Metodo di programmazione:** Selezionare una delle seguenti opzioni:
  - *Priorità stretta*: la programmazione del traffico per la coda selezionata e per le code superiori si basa unicamente sulla priorità della coda.
  - *WRR*: la programmazione del traffico per la coda selezionata si basa sul WRR. Il periodo di elaborazione del traffico si divide tra le code WRR che non sono vuote, ovvero tra le code che hanno descrittori in uscita. Questo si verifica solo se le code a stretta priorità sono vuote.
  - *Peso WRR*: se WRR è selezionato, immettere il peso WRR assegnato alla coda.
  - *% di larghezza di banda WRR*: viene indicata la quantità di larghezza di banda assegnata alla coda. Tali valori indicano la percentuale del peso WRR.

PASSAGGIO 3 Fare clic su **Applica**. Le code sono configurate e il file Configurazione di esecuzione viene aggiornato.

Associazione di CoS/802.1p a una coda

La pagina CoS/802.1p a coda consente di associare le priorità 802.1p alle code di uscita. La tabella CoS/802.1p a Coda determina le code di uscita dei pacchetti in ingresso sulla base della priorità 802.1p nei tag VLAN. Per i pacchetti in ingresso senza tag, alle porte in ingresso viene assegnata la priorità CoS/802.1p predefinita.

Nella tabella seguente viene descritta l'associazione predefinita in presenza di 4 code:

Valori 802.1p (tra 0 e 7, in cui 7 è il valore più alto)	Coda (4 code tra 1 e 4, in cui 4 rappresenta la priorità più alta)	Note
0	1	Background
1	1	Best-effort

Valori 802.1p (tra 0 e 7, in cui 7 è il valore più alto)	Coda (4 code tra 1 e 4, in cui 4 rappresenta la priorità più alta)	Note
2	2	Excellent-effort
3	3	Applicazione critica - Telefoni LVS con SIP
4	3	Sorveglianza
5	4	Servizio vocale - Telefoni IP Cisco predefiniti
6	4	Controllo interworking - Telefoni LVS con RTP
7	4	Controllo della rete

Nella tabella seguente viene descritta l'associazione predefinita in presenza di 8 code:

Valori 802.1p (tra 0 e 7, in cui 7 è il valore più alto)	Coda (8 code da 1 a 8, in cui 8 rappresenta la priorità più alta) Indipendente	Code con priorità 7 (8 è la priorità massima utilizzata per il traffico di controllo dello stack) Stack	Note
0	1	1	Background
1	2	1	Best-effort
2	3	2	Excellent-effort
3	6	5	Applicazione critica - Telefoni LVS con SIP
4	5	4	Sorveglianza
5	8	7	Servizio vocale - Telefoni IP Cisco predefiniti
6	8	7	Controllo interworking su telefoni LVS con RTP
7	7	6	Controllo della rete

Se si modificano l'associazione CoS/802.1p a coda (pagina CoS/802.1p a coda), il metodo di pianificazione della coda e l'allocazione della larghezza di banda (pagina Coda), è possibile ottenere la qualità desiderata dei servizi di una rete.

L'associazione CoS/802.1p a coda può essere applicata solo se si riscontra una delle condizioni seguenti:

- Il dispositivo si trova in modalità QoS di base e in modalità trust CoS/802.1p
- Il dispositivo si trova in modalità QoS avanzata e i pacchetti appartengono ai flussi associati a CoS/802.1p

La coda 1 ha la priorità più bassa, la coda 4 o 8 ha la priorità più alta.

Per associare i valori CoS alle code di uscita, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Generale** > **CoS/802.1p a Coda**.

PASSAGGIO 2 Immettere i parametri.

- **802.1p**: vengono indicati i valori dei tag di priorità 802.1p da assegnare a una coda di uscita, dove 0 è la priorità più bassa e 7 quella più alta.
- **Coda in uscita**: selezionare la coda di uscita a cui è associata la priorità 802.1p. Sono supportate quattro o otto code di uscita, dove Coda 4 o Coda 8 è la coda di uscita con priorità più alta e Coda 1 è quella con priorità più bassa.

PASSAGGIO 3 Per ciascuna priorità 802.1p selezionare la coda in uscita a cui è associata.

PASSAGGIO 4 Fare clic su **Applica**. I valori di priorità 802.1p nelle code vengono associati e il file Configurazione di esecuzione viene aggiornato.

Associazione DSCP a una coda

La pagina DSCP (Differentiated Services Code Point dell'IP) a Coda consente di associare DSCP alle code di uscita. La tabella da DSCP a Coda determina le code di uscita di pacchetti IP in ingresso, sulla base dei valori DSCP. Il VTP (VLAN Priority Tag) originale del pacchetto rimane invariato.

Se si modificano semplicemente l'associazione DSCP a una coda, il metodo di pianificazione della coda e la larghezza di banda, è possibile ottenere la qualità desiderata dei servizi di una rete.

L'associazione di DSCP a Coda può essere applicata ai pacchetti IP se:

- Il dispositivo si trova in modalità QoS di base e in modalità trust DSCP, oppure
- Il dispositivo si trova in modalità QoS avanzata e i pacchetti appartengono ai flussi connessi tramite DSCP

I pacchetti non IP vengono sempre classificati in base alla coda best-effort.

Nelle tabelle seguenti viene descritta l'associazione predefinita DSCP a coda per sistemi a 4 code:

DSCP	63	55	47	39	31	23	15	7
Coda	3	3	4	3	3	2	1	1
DSCP	62	54	46	38	30	22	14	6
Coda	3	3	4	3	3	2	1	1
DSCP	61	53	45	37	29	21	13	5
Coda	3	3	4	3	3	2	1	1
DSCP	60	52	44	36	28	20	12	4
Coda	3	3	4	3	3	2	1	1
DSCP	59	51	43	35	27	19	11	3
Coda	3	3	4	3	3	2	1	1
DSCP	58	50	42	34	26	18	10	2
Coda	3	3	4	3	3	2	1	1
DSCP	57	49	41	33	25	17	9	1
Coda	3	3	4	3	3	2	1	1
DSCP	56	48	40	32	24	16	8	0
Coda	3	3	4	3	3	2	1	1

Le seguenti tabelle descrivono l'associazione predefinita DSCP a coda per un sistema a 8 code (7 è la priorità più alta; 8 viene usato per scopi di controllo dello stack).

DSCP	63	55	47	39	31	23	15	7
Coda	6	6	7	5	4	3	2	1
DSCP	62	54	46	38	30	22	14	6
Coda	6	6	7	5	4	3	2	1
DSCP	61	53	45	37	29	21	13	5
Coda	6	6	7	5	4	3	2	1
DSCP	60	52	44	36	28	20	12	4
Coda	6	6	7	5	4	3	2	1
DSCP	59	51	43	35	27	19	11	3
Coda	6	6	7	5	4	3	2	1
DSCP	58	50	42	34	26	18	10	2
Coda	6	6	7	5	4	3	2	1
DSCP	57	49	41	33	25	17	9	1
Coda	6	6	7	5	4	3	2	1
DSCP	56	48	40	32	24	16	8	0
Coda	6	6	6	7	6	6	1	1

Nelle tabelle seguenti viene descritta l'associazione predefinita DSCP a coda per sistemi a 8 code in cui 8 è la priorità più alta:

DSCP	63	55	47	39	31	23	15	7
Coda	7	7	8	6	5	4	3	1
DSCP	62	54	46	38	30	22	14	6
Coda	7	7	8	6	5	4	3	1

DSCP	61	53	45	37	29	21	13	5
Coda	7	7	8	6	5	4	3	1
DSCP	60	52	44	36	28	20	12	4
Coda	7	7	8	6	5	4	3	1
DSCP	59	51	43	35	27	19	11	3
Coda	7	7	8	6	5	4	3	1
DSCP	58	50	42	34	26	18	10	2
Coda	7	7	8	6	5	4	3	1
DSCP	57	49	41	33	25	17	9	1
Coda	7	7	8	6	5	4	3	1
DSCP	56	48	40	32	24	16	8	0
Coda	7	7	7	8	7	7	1	2

Per associare DSCP alle code, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Generale** > **DSCP a Coda**.

Nella pagina DSCP a Coda è disponibile il campo **DSCP in ingresso**, in cui viene indicato il valore DSCP del pacchetto in ingresso e delle classi associate.

PASSAGGIO 2 Selezionare la **Coda in uscita** (coda di inoltro del traffico) a cui è associato il valore DSCP.

PASSAGGIO 3 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Configurazione della larghezza di banda

Nella pagina Larghezza di banda gli utenti possono definire due valori (Limite velocità in ingresso e Velocità normalizzazione in uscita), che determinano la quantità di traffico che il sistema può ricevere e inviare.

Il limite di velocità in ingresso è il numero di bit per secondo che è possibile ricevere dall'interfaccia in ingresso. La larghezza di banda che supera tale limite viene eliminata.

Per la normalizzazione in uscita, vengono inseriti i valori seguenti:

- **Banda minima garantita (CIR)** consente di impostare una quantità massima di dati consentita, calcolata in bit al secondo, da inviare nell'interfaccia in uscita.
- **Committed Burst Size (CBS)** indica la quantità di dati da inviare consentita, anche se superiore al valore CIR. Tale quantità viene definita come numero di byte di dati.

Per inserire un limite della larghezza di banda, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Generale** > **Larghezza di banda**.

Nella pagina Larghezza di banda vengono visualizzate le informazioni sulla larghezza di banda relative a ciascuna interfaccia.

La colonna **%** indica il limite di velocità in ingresso della porta diviso per la larghezza di banda totale della porta.

PASSAGGIO 2 Selezionare un'interfaccia e fare clic su **Modifica**.

PASSAGGIO 3 Selezionare l'interfaccia **Porta o LAG**. Gli switch della serie 500 offrono anche la possibilità di scegliere tra Unità e Porta.

PASSAGGIO 4 Immettere i valori dei campi per l'interfaccia selezionata:

- **Limite velocità in ingresso**: consente di attivare il limite velocità in ingresso, definito nel campo sottostante.
- **Limite velocità in ingresso**: immettere la quantità massima di larghezza di banda consentita nell'interfaccia.

  NOTA I due campi **Limite velocità in ingresso** non vengono visualizzati quando il tipo dell'interfaccia è LAG.

- **Committed Burst Size (CBS) in ingresso**: immettere la dimensione massima in byte di dati inviati per l'interfaccia in uscita. È possibile inviare la quantità indicata anche se la larghezza di banda supera temporaneamente il limite consentito. Il campo è disponibile solo se l'interfaccia è una porta.
- **Velocità normalizzazione in uscita**: consente di attivare la normalizzazione in uscita nell'interfaccia.

NOTA Il valore CIR minimo che è possibile configurare nel campo Velocità normalizzazione in uscita è 2 Mbps anziché 64 Kbps, sui seguenti switch: SF500 porte GE1—GE4 e SG500 porte GE—49-GE52.

- **Committed Information Rate (CIR)**: immettere la larghezza di banda massima per l'interfaccia in uscita.
- **Committed Burst Size (CBS) in uscita**: immettere la dimensione massima in byte di dati inviati per l'interfaccia in uscita. È possibile inviare la quantità indicata anche se la larghezza di banda supera temporaneamente il limite consentito.

PASSAGGIO 5 Fare clic su **Applica**. Le impostazioni relative alla larghezza di banda vengono scritte nel file Configurazione di esecuzione.

Configurazione della normalizzazione in uscita per coda

Oltre a limitare la velocità di trasmissione per porta nella pagina Larghezza di banda, il dispositivo può limitare la velocità di trasmissione dei frame in uscita selezionati in base alla coda e alla porta. Il limite di velocità in uscita viene eseguito tramite la normalizzazione del carico in uscita.

Il dispositivo limita tutti i frame tranne quelli di gestione. I calcoli della velocità dei frame su cui non è stato impostato un limite vengono ignorati. Ciò significa che la loro dimensione non viene inclusa nel limite complessivo.

È possibile disattivare la normalizzazione della velocità in uscita per coda.

Per definire la normalizzazione in uscita per coda, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Generale** > **Normalizzazione in uscita per coda**.

Nella pagina Normalizzazione in uscita per coda viene visualizzato il limite di velocità e dimensioni burst per ogni coda.

PASSAGGIO 2 Selezionare un tipo di interfaccia (porta o LAG) e fare clic su **Vai**.

PASSAGGIO 3 Selezionare una porta/un LAG e fare clic su **Modifica**.

In questa pagina è possibile normalizzare l'uscita di massimo otto code su ciascuna interfaccia.

PASSAGGIO 4 Selezionare l'**interfaccia**.

PASSAGGIO 5 Per ciascuna coda richiesta, immettere i valori nei seguenti campi:

- **Attiva normalizzazione**: selezionare per consentire la normalizzazione in uscita su questa coda.
- **Committed Information Rate (CIR)**: immettere la velocità massima (CIR) in Kbit per secondo (Kbps). CIR rappresenta la quantità massima di dati che è possibile inviare.
- **Committed Burst Size (CBS)**: immettere la dimensione massima dei dati trasmessi (CBS) in byte. CBS rappresenta la quantità massima consentita di dati da inviare anche se eccedente il CIR.

PASSAGGIO 6 Fare clic su **Applica**. Le impostazioni relative alla larghezza di banda vengono scritte nel file Configurazione di esecuzione.

Limite velocità in ingresso VLAN

NOTA La funzione Limite di velocità VLAN non è disponibile se il dispositivo è in modalità Livello 3.

Il limite di velocità per VLAN, eseguito nella pagina Limite velocità in ingresso VLAN consente di attivare il limite del traffico sulle VLAN. Il limite di velocità in ingresso VLAN, se impostato, consente di limitare il traffico aggregato di tutte le porte del dispositivo.

Le seguenti restrizioni vengono applicate per limitare la velocità su ciascuna VLAN:

- Ha precedenza più bassa rispetto a qualsiasi altro monitoraggio di traffico definito nel sistema. Ad esempio, se un pacchetto viene sottoposto ai limiti di velocità QoS e a quelli VLAN e tali limiti sono in conflitto, avranno la precedenza i limiti di velocità QoS.
- Viene applicato a livello di dispositivo e all'interno del dispositivo a livello di processore del pacchetto. Se il dispositivo dispone di più processori di pacchetto, il limite di velocità della VLAN configurato viene applicato indipendentemente su ciascun processore del pacchetto. I dispositivi che hanno fino a 24 porte dispongono di un solo processore di pacchetto, mentre i dispositivi a 48 porte o più ne hanno due.

Il limite di velocità viene calcolato singolarmente per ciascun processore di pacchetto presente in un'unità e per ogni singola unità presente in uno stack.

Per definire il limite di velocità in ingresso VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Qualità del servizio** > **Generale** > **Limite velocità in ingresso VLAN**.

Nella pagina viene visualizzata la tabella Limite di velocità in ingresso VLAN.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **ID VLAN**: selezionare una VLAN.
- **Committed Information Rate (CIR)**: immettere la quantità massima di dati in Kilobyte accettabili nella VLAN.
- **Committed Burst Size (CBS)**: immettere la dimensione massima in byte di dati inviati per l'interfaccia in uscita. È possibile inviare la quantità indicata anche se la larghezza di banda supera temporaneamente il limite consentito. Tali inserimenti non sono consentiti per i LAG.

PASSAGGIO 4 Fare clic su **Applica**. Il limite di velocità VLAN viene aggiunto e il file Configurazione di esecuzione viene aggiornato.

Prevenzione congestione TCP

Nella pagina Prevenzione congestione TCP è possibile attivare un algoritmo di prevenzione della congestione TCP. L'algoritmo consente di interrompere o di impedire la sincronizzazione globale TCP in un nodo congestionato, la cui congestione è dovuta all'invio di pacchetti con lo stesso numero di byte da origini diverse.

Per configurare la prevenzione della congestione TCP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Generale** > **Prevenzione congestione TCP**.

PASSAGGIO 2 Fare clic su **Attiva** per attivare la prevenzione congestione TCP, quindi su **Applica**.

Modalità QoS di base

In modalità QoS di base, è possibile definire un dominio specifico della rete come attendibile. All'interno di quel dominio, i pacchetti vengono contrassegnati con priorità 802.1p e/o DSCP per segnalare il tipo di servizio necessario. I nodi dentro il dominio usano questi campi per assegnare il pacchetto a una specifica coda in uscita. La classificazione iniziale del pacchetto e la selezione di questi campi vengono eseguite nell'ingresso del dominio attendibile.

Flusso di lavoro per la configurazione della modalità QoS di base

Per configurare la modalità QoS di base, attenersi alla seguente procedura:

1. Utilizzare la pagina Proprietà QoS per selezionare la modalità di base per il sistema.
2. Utilizzare la pagina Impostazioni generali per selezionare la modalità trust. Il dispositivo supporta le modalità trust CoS/802.1p e DSCP. La prima utilizza la priorità 802.1p nel tag VLAN, mentre la seconda usa il valore DSCP nell'intestazione IP.

Se una porta, per eccezione, non deve essere associata alla selezione CoS in ingresso, disattivare lo stato QoS nella pagina Impostazioni interfaccia.

Attivare o disattivare la modalità Trust selezionata a livello globale per le porte nella pagina Impostazioni interfaccia. Se una porta viene disattivata senza impostare la modalità Trust, tutti i suoi pacchetti in ingresso vengono inoltrati nella coda best-effort. Si consiglia di disattivare la modalità Trust sulle porte in cui i valori CoS/802.1p e/o DSCP dei pacchetti in ingresso non sono attendibili. In caso contrario, si potrebbero compromettere le prestazioni della rete.

Configurazione delle impostazioni generali

La pagina Impostazioni generali contiene informazioni relative all'attivazione di Trust sul dispositivo (vedere il campo seguente Modalità Trust). La configurazione è attiva quando la modalità QoS è quella di base. I pacchetti che entrano in un dominio QoS vengono classificati sull'edge del dominio QoS.

Per definire la configurazione di Trust, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Modalità QoS di base** > **Impostazioni globali**.

PASSAGGIO 2 Selezionare un'opzione nel campo **Modalità Trust** con il dispositivo in modalità di base. Se il livello CoS e il tag DSCP di un pacchetto sono associati a code diverse, la modalità Trust determina a quale coda assegnare il pacchetto:

- **CoS/802.1p**: il traffico viene associato alle code sulla base del campo VTP del tag VLAN oppure in base al valore CoS/802.1p predefinito per porta (se il pacchetto in ingresso non ha tag VLAN). È possibile configurare l'effettiva associazione del VTP alla coda nella pagina CoS/802.1p a coda.
- **DSCP**: tutto il traffico IP viene associato alle code in base al campo DSCP dell'intestazione IP. L'effettiva associazione di DSCP alla coda può essere configurata nella pagina DSCP a Coda. Se il traffico non è traffico IP, viene associato alla coda best-effort.
- **CoS/802.1p-DSCP**: CoS/802.1p o DSCP, a seconda dell'impostazione.

PASSAGGIO 3 Selezionare **Annullamento DSCP in ingresso** per annullare i valori DSCP originari nei pacchetti in ingresso e inserire nuovi valori in base alla tabella Annullamento DSCP. Se l'opzione Annullamento DSCP in ingresso è attiva, il dispositivo utilizzerà i nuovi valori DSCP per la coda di uscita. Inoltre, sostituirà i valori DSCP originari dei pacchetti con valori DSCP nuovi.

NOTA Il frame viene associato alla coda di uscita tramite i nuovi valori attribuiti e non dal valore DSCP originario.

PASSAGGIO 4 Se l'opzione **Annullamento DSCP in ingresso** è stata attivata, fare clic su **Tabella Annullamento DSCP** per riconfigurare DSCP.

Il **DSCP di ingresso** visualizza il valore DSCP del traffico in entrata e in uscita dallo switch.

PASSAGGIO 5 Selezionare il valore **DSCP di uscita** per indicare il valore di uscita a cui è associato.

PASSAGGIO 6 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato con i nuovi valori DSCP.

Impostazioni interfaccia QoS

Nella pagina Impostazioni interfaccia è possibile configurare QoS su ciascuna porta del dispositivo come indicato di seguito:

Stato QoS disattivato in un'interfaccia: tutto il traffico in ingresso sulla porta viene associato alla coda best-effort e non viene eseguita alcuna classificazione/prioritizzazione.

Stato QoS della porta attivato: la prioritizzazione del traffico in ingresso su una porta si basa sulla modalità Trust CoS/802.1p o DSCP configurata nell'intero sistema.

Per eseguire le impostazioni QoS per interfaccia, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Modalità QoS di base** > **Impostazioni interfaccia**.

PASSAGGIO 2 Scegliere **Porta** o **LAG** per visualizzare l'elenco di porte o LAG.

Stato QoS: indica se QoS è attivato sull'interfaccia.

PASSAGGIO 3 Selezionare un'interfaccia e fare clic su **Modifica**.

PASSAGGIO 4 Selezionare l'interfaccia **Porta** o **LAG**.

PASSAGGIO 5 Fare clic per attivare o disattivare lo **Stato QoS** in questa interfaccia.

PASSAGGIO 6 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Modalità avanzata QoS

I frame che corrispondono e che possono accedere a un ACL vengono etichettati implicitamente con il nome dell'ACL che ne consente l'ingresso. Pertanto, in questi flussi è possibile eseguire le operazioni QoS in modalità avanzata.

In modalità QoS avanzata, il dispositivo utilizza i criteri per supportare il QoS per flusso. Un criterio e i suoi componenti presentano le seguenti caratteristiche e relazioni:

- Un criterio contiene una o più mappe di classi.

- Una mappa di classi definisce un flusso con uno o più ACL associati. I pacchetti che soddisfano solo le regole ACL (ACE) in una mappa delle classi con un'azione Consenti (reindirizza) vengono considerati parte dello stesso flusso e sono sottoposti alla stessa qualità dei servizi. Pertanto, un criterio contiene uno o più flussi, ognuno dei quali presenta un QoS definito dall'utente.
- Il QoS di una mappa delle classi (flusso) viene applicato tramite il relativo monitoraggio. Sono disponibili due tipi di monitoraggio, singolo e aggregato. Ognuno di essi viene configurato tramite una specifica QoS. Un monitoraggio singolo consente di applicare il QoS a una mappa di classi singola, e quindi a un singolo flusso, sulla base delle specifiche QoS della funzionalità di monitoraggio. Un monitoraggio aggregato applica il QoS a una o più mappe di classi e di conseguenza a uno o più flussi. Inoltre, può supportare mappe di classi di criteri diversi.
- Il QoS per flusso viene applicato ai flussi tramite il binding dei criteri sulle porte desiderate. Un criterio e le sue mappe di classi possono essere associate a una o più porte, ma ciascuna di esse deve presentare almeno un criterio.

Note:

- I monitoraggi singolo e aggregato sono disponibili quando il dispositivo si trova in modalità Livello 2.
- È possibile configurare un ACL su una o più mappe di classi, indipendentemente dai criteri.
- Una mappa delle classi può appartenere soltanto a un criterio.
- Quando la mappa delle classi che usa un monitoraggio singolo viene associata a più porte, ciascuna porta presenta un'istanza legata alla funzionalità di monitoraggio singola e viene applicato il QoS sulla mappa delle classi (flusso) di porte l'una indipendente dall'altra.
- Inoltre, applica il QoS su tutti i flussi aggregati, indipendentemente dai criteri e dalle porte.

Le impostazioni QoS avanzate sono costituite da tre fasi:

- Definizioni delle regole da soddisfare. Tutti i frame che soddisfano un singolo gruppo di regole sono considerati un *flusso*.
- Definizione delle azioni da eseguire sui frame in ciascun flusso che soddisfa le regole.
- Associazione delle combinazioni di regole e azioni in una o più interfacce.

Flusso di lavoro per la configurazione della modalità QoS avanzata

Per configurare la modalità QoS avanzata, attenersi alla seguente procedura:

1. Utilizzare la pagina Proprietà QoS per selezionare la modalità avanzata per il sistema. Utilizzare la pagina Impostazioni generali per selezionare la modalità Trust. Se il livello CoS e il tag DSCP di un pacchetto sono associati a code diverse, la modalità Trust determina a quale coda assegnare il pacchetto:
   - Se i valori DSCP interni differiscono da quelli utilizzati sui pacchetti in ingresso, utilizzare la pagina Associazione DSCP fuori dal profilo per associare i valori esterni a quelli interni. Viene visualizzata la pagina Contrassegnazione DSCP.
2. Creare gli elenchi ACL, come descritto in Crea flusso di lavoro ACL.
3. Se sono stati definiti gli ACL, utilizzare la pagina Associazione classi per creare mappe di classi e associarle agli ACL.
4. Creare un criterio nella pagina Tabella Criteri e associarlo a una o più mappe di classi nella pagina Mappa delle classi di criteri. Quando si associa la mappa della classe al criterio, è possibile anche specificare il QoS, se necessario, assegnando un criterio a una mappa delle classi.
   - **Singolo monitoraggio**: creare un criterio che associa una mappa delle classi con un singolo monitoraggio nella pagina Tabella criteri e nella pagina Associazione classi. Indicare nel criterio il monitoraggio singolo.
   - **Monitoraggio aggregato**: creare un'azione QoS per ciascun flusso che invia tutti i frame corrispondenti allo stesso monitoraggio (monitoraggio aggregato) nella pagina Monitoraggio aggregato. Creare un criterio che associ una mappa delle classi a un monitoraggio aggregato nella pagina Tabella Criteri.
5. Utilizzare la pagina Binding del criterio per associare il criterio a un'interfaccia.

Configurazione delle impostazioni globali

La pagina Impostazioni generali contiene i parametri per l'attivazione del Trust sul dispositivo. I pacchetti che entrano in un dominio QoS vengono classificati sull'edge del dominio QoS.

Per definire la configurazione di Trust, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Modalità avanzata QoS** > **Impostazioni globali**.

PASSAGGIO 2 Selezionare un'opzione nel campo **Modalità Trust** con il dispositivo in modalità avanzata. Se il livello CoS e il tag DSCP di un pacchetto sono associati a code diverse, la modalità Trust determina a quale coda assegnare il pacchetto:

- **CoS/802.1p**: il traffico viene associato alle code sulla base del campo VTP del tag VLAN oppure in base al valore CoS/802.1p predefinito per porta (se il pacchetto in ingresso non ha tag VLAN). È possibile configurare l'effettiva associazione del VTP alla coda nella pagina CoS/802.1p a coda.
- **DSCP**: tutto il traffico IP viene associato alle code in base al campo DSCP dell'intestazione IP. L'effettiva associazione di DSCP alla coda può essere configurata nella pagina DSCP a Coda. Se il traffico non è traffico IP, viene associato alla coda best-effort.
- **CoS/802.1p-DSCP**: selezionare questa opzione per utilizzare la modalità Trust CoS per traffico non IP e la modalità Trust DSCP per il traffico IP.

PASSAGGIO 3 Selezionare la modalità avanzata Trust QoS (attendibile o non attendibile) per le interfacce nel campo **Stato modalità predefinita**. Questo fornisce funzionalità di base QoS su QoS avanzato, in modo da poter impostare in modo predefinito il trust CoS/DSCP su QoS avanzato (senza dover creare un criterio).

Nella **modalità avanzata QoS**, quando lo stato modalità predefinita è impostato su Non attendibile, i valori predefiniti CoS configurati nell'interfaccia vengono ignorati e tutto il traffico viene indirizzato nella coda 1. Per i dettagli vedere la pagina Qualità del servizio > Modalità avanzata QoS > Impostazioni generali. Per i dettagli, vedere la pagina Qualità del servizio > Modalità avanzata QoS > Impostazioni generali.

Se si dispone di un criterio su un'interfaccia, la modalità predefinita è irrilevante; l'azione, infatti, viene eseguita in base alla configurazione del criterio e il traffico senza corrispondenza viene scartato.

PASSAGGIO 4 Selezionare **Annullamento DSCP in ingresso** per annullare i valori DSCP originari nei pacchetti in ingresso e inserire nuovi valori in base alla tabella Annullamento DSCP. Se l'opzione Annullamento DSCP in ingresso è attiva, il dispositivo utilizzerà i nuovi valori DSCP per la coda di uscita. Inoltre, sostituirà i valori DSCP originari dei pacchetti con valori DSCP nuovi.

> **NOTA** Il frame viene associato alla coda di uscita tramite i nuovi valori attribuiti e non dal valore DSCP originario.

PASSAGGIO 5 Se l'opzione **Annullamento DSCP in ingresso** è stata attivata, fare clic su **Tabella Annullamento DSCP** per riconfigurare DSCP. Per ulteriori dettagli, vedere la pagina Tabella annullamento DSCP.

Configurazione dell'Associazione DSCP fuori dal profilo

Quando si assegna una funzionalità di monitoraggio a una mappa delle classi (flussi), è possibile specificare l'azione da eseguire quando la quantità di traffico dei flussi supera i limiti indicati dal QoS-. La parte del traffico del flusso che supera il limite QoS viene indicata come *pacchetti fuori dal profilo*.

Se l'evento di superamento è DSCP fuori dal profilo, il dispositivo associa nuovamente il valore DSCP originale dei pacchetti IP fuori dal profilo a un nuovo valore, in base alla tabella Associazione DSCP fuori dal profilo. Il dispositivo utilizza i nuovi valori per assegnare risorse e code di uscita a questi pacchetti. Inoltre, sostituisce fisicamente il valore DSCP originale dei pacchetti fuori dal profilo con il nuovo valore DSCP.

Per usare l'evento di superamento di DSCP fuori dal profilo, associare nuovamente il valore DSCP nella tabella Associazione DSCP fuori dal profilo. In caso contrario, l'azione verrà annullata poiché, per impostazione predefinita, i pacchetti vengono di nuovo associati al valore DSCP riportato nella tabella.

Questa funzione consente di modificare i tag DSCP per il traffico in ingresso scambiato tra domini QoS attendibili. Se si modificano i valori in uso in un dominio, viene impostata la priorità di quel tipo di traffico al valore DSCP usato nell'altro dominio al fine di identificare lo stesso tipo di traffico.

Tali impostazioni sono attive quando il sistema è in modalità QoS di base, e, una volta attivate, saranno attive a livello globale.

Ad esempio: immaginiamo che ci siano tre livelli di servizio: Argento, Oro e Platino e che i valori in ingresso DSCP che indicano tali livelli siano rispettivamente 10, 20 e 30. Se il traffico viene inoltrato su un altro fornitore del servizio avente gli stessi tre livelli di servizio ma che usa i valori DSCP 16, 24 e 48, l'**Associazione DSCP fuori dal profilo** modifica i valori in ingresso non appena vengono associati ai valori in uscita.

Per associare valori DSCP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio > Modalità avanzata QoS > Associazione DSCP fuori dal profilo**. Questa pagina consente di impostare la modifica del valore DSCP del traffico in ingresso o uscita dallo switch.

In questa pagina è possibile impostare il valore DSCP del traffico in entrata e in uscita dallo switch.

PASSAGGIO 2 Selezionare il valore **DSCP di uscita** a cui viene associato il valore di ingresso.

PASSAGGIO 3 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato con la nuova tabella Associazione DSCP.

Definizione dell'Associazione classe

Una mappa delle classi definisce un flusso di traffico con ACL (elenchi di controllo degli accessi). In una mappa delle classi è possibile combinare MAC ACL, IP ACL e IPv6 ACL. Le mappe di classi sono configurate per soddisfare i criteri del pacchetto su una base Abbina tutti o Abbina qualsiasi. Queste vengono associate ai pacchetti su una base first-fit, ovvero il sistema eseguirà l'azione sulla mappa di classi "associata per prima". I pacchetti che presentano la stessa mappa di classi sono considerati parte dello stesso flusso.

NOTA La definizione delle mappe di classi non incide sul QoS. Essa costituisce una fase di transizione che consente di utilizzare le mappe di classi successivamente.

Se viene richiesto un insieme di regole più complesse, è possibile raggruppare diverse mappe di classi in un gruppo più grande denominato Criterio (vedere la sezione **Configurazione di un criterio**).

La pagina Associazione classi mostra l'elenco di mappe di classi definite e gli ACL inclusi e consente di aggiungere/eliminare mappe delle classi.

Per definire una mappa delle classi, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Modalità avanzata QoS** > **Associazione classi**.

La pagina visualizza le mappe di classi già definite.

PASSAGGIO 2 Fare clic su **Aggiungi**.

L'aggiunta di una nuova mappa di classi viene eseguita selezionando uno o più ACL e assegnando un nome alla mappa di classi. Se una mappa di classi include due ACL, è possibile specificare che un frame deve corrispondere a entrambi gli ACL o a uno o entrambi gli ACL selezionati.

PASSAGGIO 3 Immettere i parametri.

- **Nome mappa delle classi**: immettere il nome di una nuova mappa delle classi.
- **Tipo di ACL corrispondente**: i criteri a cui un pacchetto deve corrispondere per poter essere considerato parte del flusso definito nella mappa di classi. Sono disponibili le seguenti opzioni:
  - *IP*: un pacchetto deve corrispondere a tutti gli elenchi ACL della mappa di classi basati su IP.
  - *MAC*: un pacchetto deve corrispondere all'elenco ACL della mappa delle classi basato su MAC.

- *IP e MAC*: un pacchetto deve corrispondere all'elenco ACL della mappa di classi basato su MAC e a quello basato su IP.
- *IP o MAC*: un pacchetto deve corrispondere o all'elenco ACL basato su IP oppure a quello basato su MAC della mappa di classi.

- **IP**: selezionare l'elenco ACL basato su IPv4 oppure quello basato su IPv6 della mappa di classi.
- **MAC**: selezionare l'ACL basato su MAC della mappa di classi.
- **ACL preferito**: selezionare se i pacchetti vengono confrontati prima con un elenco ACL basato su IP o con uno basato su MAC.

PASSAGGIO 4 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Monitoraggi QoS

NOTA I monitoraggi QoS non sono supportati dai dispositivi Sx500 in modalità di sistema Livello 3. Sono supportanti sempre su dispositivi SG500X.

È possibile misurare la frequenza del traffico corrispondente a una serie di regole predefinita e applicare dei limiti, ad esempio è possibile limitare su una porta la velocità del traffico del trasferimento di file.

Questa operazione può essere eseguita facendo corrispondere gli ACL delle mappe di classi al traffico desiderato e tramite un monitoraggio da applicare al QoS sul traffico corrispondente.

Un monitoraggio viene configurato tramite una specifica QoS. Sono disponibili due tipi di monitoraggi:

- **Monitoraggio singolo (regolare)**: il QoS viene applicato su una singola mappa di classi e a un singolo flusso sulla base delle specifiche QoS del monitoraggio. Quando la mappa di classi che usa una funzionalità di monitoraggio singola viene associata a più porte, ciascuna porta presenta un'istanza legata al monitoraggio singolo e viene applicato il QoS sulla mappa di classi (flusso) di porte indipendenti l'una dall'altra. Nella pagina Tabella Criteri viene creato un singolo monitoraggio.
- **Monitoraggio aggregato**: applica il QoS a una o più mappe di classi e a uno o più flussi. Un monitoraggio aggregato può supportare mappe di classi di criteri diversi. Inoltre, applica il QoS su tutti i flussi aggregati, indipendentemente dai criteri e dalle porte. Per creare un monitoraggio aggregato, utilizzare la pagina Monitoraggio aggregato.

Il monitoraggio aggregato viene definito se è necessario condividere il monitoraggio fra più classi. I monitoraggi su una porta possono essere condivisi con altri monitoraggi su un altro dispositivo.

Ciascun monitoraggio viene indicato con la propria specifica QoS e una combinazione dei parametri seguenti:

- Una velocità massima consentita, definita Committed Information Rate (CIR) e calcolata in Kbps.
- Una quantità di traffico, misurata in byte, denominata Committed Burst Size (CBS). Questa indica il traffico consentito nella trasmissione di un burst temporaneo, anche se supera la velocità massima specificata.
- Tale azione va applicata sui frame che superano i limiti (definiti con il nome di traffico fuori dal profilo), in cui tali frame possono essere trasmessi tali e quali o eliminati, ma associati nuovamente a un nuovo valore DSCP che li contrassegna come frame a bassa priorità per gestirli successivamente nel dispositivo.

L'assegnazione di un monitoraggio a una mappa di classi viene eseguita quando si aggiunge una mappa di classi a un criterio. Se si utilizza il monitoraggio aggregato, è necessario utilizzare la pagina Monitoraggio aggregato per crearlo.

Definizione dei monitoraggi aggregati

Un monitoraggio aggregato applica il QoS a una o più mappe di classi, di conseguenza a uno o più flussi. Un monitoraggio aggregato può supportare mappe di classi di diversi criteri e applica il QoS a tutti i flussi aggregati, indipendentemente dai criteri e dalle porte.

NOTA Il dispositivo supporta monitoraggi aggregati e singoli solo quando è in modalità Livello 2 in dispositivi che prevedono una modalità di sistema distinta di livello 2.

Per definire un monitoraggio aggregato, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Qualità del servizio** > **Modalità QoS avanzata** > **Monitoraggio aggregato**.

In questa pagina vengono visualizzati i monitoraggi aggregati esistenti:

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **Nome monitoraggio aggregato**: immettere il nome del monitoraggio aggregato.
- **CIR (Committed Information Rate) in ingresso**: immettere la larghezza di banda massima consentita in bit per secondo. Vedere la descrizione nella pagina Larghezza di banda.
- **Committed Burst Size (CBS) in ingresso**: immettere la dimensione massima dei dati trasmessi (anche se eccedenti il CIR) in byte. Vedere la descrizione nella pagina Larghezza di banda.
- **Evento di superamento**: selezionare l'azione da eseguire sui pacchetti in ingresso che superano il CIR. I valori possibili sono:
  - *Inoltra*: vengono inoltrati i pacchetti che superano il valore CIR specificato.
  - *Elimina*: vengono eliminati i pacchetti che superano il valore CIR specificato.
  - *DSCP fuori dal profilo*: i valori DSCP dei pacchetti che superano il valore CIR specificato vengono associati nuovamente a un valore secondo la tabella Associazione DSCP fuori dal profilo.

PASSAGGIO 4 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Configurazione di un Criterio

Nella pagina Tabella Criteri viene visualizzato l'elenco dei criteri QoS avanzati definiti nel sistema. Inoltre, nella pagina è possibile creare ed eliminare criteri. Sono attivi solo i criteri associati a un'interfaccia (vedere la pagina Binding del criterio).

Ciascun criterio è costituito da:

- Una o più mappe di classi di ACL che definiscono i flussi di traffico del criterio.
- Uno o più aggregati che applicano il QoS ai flussi di traffico del criterio.

Dopo aver aggiunto un criterio, è possibile utilizzare la pagina Tabella Criteri per aggiungere mappe delle classi.

Per aggiungere un criterio QoS, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Modalità avanzata QoS** > **Tabella criteri**.

La pagina visualizza l'elenco dei criteri specificati.

PASSAGGIO 2 Fare clic su **Tabella Mappa delle classi di criteri** per visualizzare la pagina Mappe delle classi di criteri.
oppure
fare clic su **Aggiungi** per aprire la pagina Aggiungi tabella Criteri.

PASSAGGIO 3 Nel campo **Nuovo nome criterio** immettere il nome del nuovo criterio.

PASSAGGIO 4 Fare clic su **Applica**. Viene aggiunto il profilo criteri QoS e il file di Configurazione di esecuzione viene aggiornato.

Mappe delle classi di criteri

È possibile aggiungere a un criterio una o più mappe di classi. Una mappa di classi indica il tipo di pacchetti che vengono considerati parte dello stesso flusso di traffico.

NOTA Se il dispositivo è in modalità Livello 3, non è possibile configurare un monitoraggio su una mappa di classi. Il dispositivo supporta monitoraggi in modalità Livello 2.

Per aggiungere una mappa di classi a un criterio, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Modalità avanzata QoS** > **Mappe delle classi di criteri**.

PASSAGGIO 2 Selezionare un criterio nel Filtro e fare clic su **Vai**. Vengono visualizzate tutte le mappe di classi di quel criterio.

PASSAGGIO 3 Per aggiungere una nuova mappa di classi, fare clic su **Aggiungi**.

PASSAGGIO 4 Immettere i parametri.

- **Nome criterio**: viene indicato il criterio a cui è stata aggiunta la mappa di classi.
- **Nome mappa delle classi**: selezionare la mappa di classi esistenti da associare al criterio. Le mappe di classe vengono create nella pagina Associazione classi.

- **Tipo di azione**: selezionare l'azione relativa al valore Cos/802.1p in ingresso o DSCP di tutti i pacchetti corrispondenti.
  - *Usare la modalità trust predefinita*: ignorare il valore CoS/802.1p in ingresso o DSCP. I pacchetti corrispondenti vengono inviati come best-effort.
  - *Sempre attendibile*: se si seleziona questa opzione, il dispositivo viene associato al CoS/802.1p e DSCP del pacchetto corrispondente. Se si tratta di un pacchetto IP, il dispositivo lo inserisce nella coda di uscita, in base al valore DSCP e alla tabella Da DSCP a coda; altrimenti, la coda di uscita del pacchetto si baserà sul valore CoS/802.1p del pacchetto e sulla tabella CoS/802.1p a coda.
  - *Imposta*: se questa opzione è selezionata, usare il valore inserito nella casella **Nuovo valore** per determinare la coda di uscita dei pacchetti corrispondenti in base a quanto indicato:

    Se il nuovo valore (0..7) è una priorità CoS/802.1p, usare tale valore e la tabella CoS/802.1p a coda per determinare la coda di uscita di tutti i pacchetti corrispondenti.

    Se il nuovo valore (0..63) è un DSCP, usare il nuovo DSCP e la tabella da DSCP a Coda per determinare la coda di uscita dei pacchetti IP corrispondenti.

    Altrimenti, usare il nuovo valore (1..8) come numero della coda di uscita per tutti i pacchetti corrispondenti.
- **Tipo di monitoraggio**: disponibile solo in modalità di sistema Livello 2. Selezionare il tipo di monitoraggio del criterio. Sono disponibili le seguenti opzioni:
  - *Nessuno*: non viene usato alcun criterio.
  - *Singolo*: il tipo di monitoraggio del criterio è singolo.
  - *Aggregato*: il tipo di monitoraggio del criterio è aggregato.
- **Monitoraggio aggregato**: disponibile solo in modalità di sistema Livello 2. Se il campo **Tipo di monitoraggio** è impostato su *Aggregato*, selezionare un monitoraggio aggregato definito in precedenza (nella pagina Monitoraggio aggregato).

Se il **Tipo di monitoraggio** è *Singolo*, immettere i seguenti parametri QoS:

- **Committed Information Rate (CIR) in ingresso**: immettere il CIR in Kbps. Vedere la descrizione nella pagina Larghezza di banda.

- **Committed Burst Size (CBS) in ingresso**: immettere il CBS in byte. Vedere la descrizione nella pagina Larghezza di banda.
- **Evento di superamento**: selezionare l'azione assegnata ai pacchetti in ingresso che superano il CIR. Le opzioni sono:
  - *Nessuno*: non viene eseguita alcuna azione.
  - *Elimina*: vengono eliminati i pacchetti che superano il valore CIR specificato.
  - *DSCP fuori dal profilo*: l'inoltro eseguito dai pacchetti IP che superano il CIR specificato avviene tramite un nuovo DSCP scaturito dalla tabella associazione DSCP fuori dal profilo.

PASSAGGIO 5 Fare clic su **Applica**.

Binding del criterio

Nella pagina Binding del criterio viene visualizzato il profilo del criterio e la porta alla quale è associato. Quando un profilo del criterio viene associato a una porta specifica, esso risulta attivo su quella porta. È possibile configurare su una singola porta un solo profilo del criterio, ma è possibile associare un singolo criterio a più di una porta.

Quando si associa un criterio a una porta, esso filtra e applica il QoS al traffico in ingresso appartenente ai flussi definiti nel criterio. Il criterio non viene applicato al traffico in uscita sulla stessa porta.

Per modificare un criterio, è necessario prima rimuoverlo (disassociarlo) da tutte le porte a cui è associato.

NOTA È possibile collegare la porta a un criterio o a un ACL ma non è possibile associarli entrambi.

Per definire il binding di un criterio, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Modalità avanzata QoS** > **Binding del criterio**.

PASSAGGIO 2 Selezionare un **Nome criterio** e un **Tipo di interfaccia**, se necessario.

PASSAGGIO 3 Scegliere **Vai**. Il criterio è stato selezionato.

PASSAGGIO 4 Selezionare i seguenti parametri per il criterio/interfaccia:

- **Binding**: selezionare questa opzione per collegare il criterio all'interfaccia.

- **Consenti tutti**: selezionare questa opzione per inoltrare i pacchetti sull'interfaccia, se questi non corrispondono ad alcun criterio.

  NOTA È possibile selezionare Consenti tutti solo se la Guardia origine IP non è attiva sull'interfaccia.

PASSAGGIO 5 Fare clic su **Applica**. Il binding del criterio QoS viene definito e il file di Configurazione di esecuzione viene aggiornato.

Gestione delle statistiche QoS

In queste pagine è possibile gestire il monitoraggio singolo e il monitoraggio aggregato, nonchè visualizzare le statistiche della coda.

Statistiche del monitoraggio

Un monitoraggio singolo viene associato a una relativa mappa di classi. Un monitoraggio aggregato viene associato a una o più mappe di classi di uno o più criteri.

Visualizzazione delle statistiche singolo monitoraggio

Nella pagina Statistiche singolo monitoraggio viene indicato il numero di pacchetti dentro e fuori dal profilo ricevuti da un'interfaccia che soddisfa le condizioni specificate nella mappa delle classi di un criterio.

NOTA La pagina non viene visualizzata se il dispositivo è in modalità Livello 3.

Per visualizzare le statistiche monitoraggio, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Statistiche QoS** > **Singolo monitoraggio Statistiche**.

In questa pagina vengono visualizzati i seguenti campi:

- **Interfaccia**: vengono visualizzate le statistiche relative a questa interfaccia.
- **Criterio**: vengono visualizzate le statistiche relative a questo criterio.
- **Mappa delle classi**: vengono visualizzate le statistiche relative questa mappa di classi.

- **Byte nel profilo**: numero di byte nel profilo ricevuti.
- **Byte fuori dal profilo**: numero di byte fuori dal profilo ricevuti.

PASSAGGIO 2 Fare clic su **Aggiungi.**

PASSAGGIO 3 Immettere i parametri.

- **Interfaccia**: selezionare l'interfaccia di cui vengono accumulate le statistiche.
- **Nome criterio**: selezionare il nome del criterio.
- **Nome mappa delle classi**: selezionare il nome della classe.

PASSAGGIO 4 Fare clic su **Applica**. Un'ulteriore richiesta di statistiche viene creata e il file di Configurazione di esecuzione viene aggiornato.

Visualizzazione delle statistiche monitoraggio aggregato

Per visualizzare le statistiche monitoraggio aggregato, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Statistiche QoS** > **Statistiche monitoraggio aggregato**.

In questa pagina vengono visualizzati i seguenti campi:

- **Nome monitoraggio aggregato**: il monitoraggio su cui si basano le statistiche.
- **Byte nel profilo**: numero di pacchetti nel profilo ricevuti.
- **Byte fuori dal profilo**: numero di pacchetti fuori dal profilo ricevuti.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Selezionare un **Nome monitoraggio aggregato**, uno dei monitoraggi aggregati creati in precedenza di cui verranno visualizzate le statistiche.

PASSAGGIO 4 Fare clic su **Applica**. Un'ulteriore richiesta di statistiche viene creata e il file di Configurazione di esecuzione viene aggiornato.

Visualizzazione delle statistiche code

Nella pagina Statistiche code vengono visualizzate le statistiche relative alle code, incluse le statistiche di pacchetti inoltrati ed eliminati, in base alla precedenza dell'interfaccia, della coda e dell'eliminazione.

Per visualizzare le statistiche code, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Qualità del servizio** > **Statistiche QoS** > **Statistiche code**.

In questa pagina vengono visualizzati i seguenti campi:

- **Frequenza aggiornamento**: selezionare il periodo di tempo che trascorre prima che le statistiche dell'interfaccia Ethernet vengano aggiornate. Le opzioni disponibili sono:
  - *Nessun aggiornamento*: le statistiche non vengono aggiornate.
  - *15 sec.*: le statistiche vengono aggiornate ogni 15 secondi.
  - *30 sec.*: le statistiche vengono aggiornate ogni 30 secondi.
  - *60 sec.*: le statistiche vengono aggiornate ogni 60 secondi.
- **Insieme contatori**: le opzioni sono:
  - *Serie 1*: indica le statistiche relative alla Serie 1 contenente tutte le interfacce e le code con una DP alta (Drop Precedence, Precedenza eliminazione).
  - *Serie 2*: indica le statistiche relative alla Serie 2 contenente tutte le interfacce e le code con una DP bassa.
- **Interfaccia**: vengono visualizzate le statistiche code relative a questa interfaccia.
- **Coda**: i pacchetti sono stati inoltrati o eliminati da questa coda.
- **Precedenza eliminazione**: la precedenza eliminazione più bassa ha la probabilità minore di essere eliminata.
- **Pacchetti totali**: numero di pacchetti inoltrati o eliminati dalla coda.
- **Pacchetti di algoritmi Tail drop**: percentuale di pacchetti eliminati dalla coda.

PASSAGGIO 2 Fare clic su **Aggiungi.**

PASSAGGIO 3 Immettere i parametri.

- **Insieme contatori**: selezionare l'insieme di contatori:
  - *Serie 1*: indica le statistiche relative alla Serie 1 contenente tutte le interfacce e le code con una DP alta (Drop Precedence, Precedenza eliminazione).
  - *Serie 2*: indica le statistiche relative alla Serie 2 contenente tutte le interfacce e le code con una DP bassa.
- **Interfaccia**: selezionare le porte di cui vengono visualizzate le statistiche. Sono disponibili le seguenti opzioni:
  - *N. unità*: consente di selezionare il numero di unità.
  - *Porta*: consente di selezionare la porta sul numero dell'unità indicato di cui vengono visualizzate le statistiche.
  - *Tutte le porte*: indica le statistiche visualizzate per tutte le porte.
- **Coda**: selezionare la coda di cui vengono visualizzate le statistiche.
- **Precedenza eliminazione**: immettere la precedenza eliminazione che indica la probabilità di eliminazione.

PASSAGGIO 4 Fare clic su **Applica**. Le Statistiche code vengono aggiunte e il file di Configurazione di esecuzione viene aggiornato.

29

SNMP

In questa sezione viene descritta la funzione di SNMP (Simple Network Management Protocol) che fornisce un metodo di gestione dei dispositivi di rete.

Vengono trattati i seguenti argomenti:

- **Versioni e flusso di lavoro di SNMP**
- **OID del modello**
- **ID motore SNMP**
- **Configurazione Viste SNMP**
- **Creazione di gruppi SNMP**
- **Gestione degli utenti SNMP**
- **Definizione delle comunità SNMP**
- **Definizione delle impostazioni trap**
- **Destinatari delle notifiche**
- **Filtri per le notifiche SNMP**

Versioni e flusso di lavoro di SNMP

Il dispositivo funge da agente SNMP e supporta le versioni SNMPv1,v2 e v3. Inoltre riporta sui ricevitori trap gli eventi del sistema tramite i trap definiti nei MIB (Management Information Base) supportati.

SNMPv1 e v2

Per controllare gli accessi sul sistema, viene definito un elenco di voci della comunità. ciascuna delle quali è costituita da una *stringa della comunità* e i relativi privilegi di accesso. Il sistema risponde solo ai messaggi SNMP, specificando la comunità che dispone delle autorizzazioni corrette e del funzionamento appropriato.

Gli agenti SNMP conservano un elenco di variabili usate per gestire il dispositivo. Tali variabili vengono definite nel *Management Information Base* (MIB).

NOTA A causa delle vulnerabilità legate alla sicurezza di altre versioni, si consiglia di utilizzare SNMPv3.

SNMPv3

Oltre alle funzionalità fornite da SNMPv1 e v2, SNMPv3 applica il controllo di accesso e nuovi meccanismi trap alle PDU di SNMPv1 e SNMPv2. SNMPv3 inoltre definisce un modello di protezione utente (USM; User Security Model), che comprende:

- **Autenticazione**: fornisce l'integrità e l'autenticazione della provenienza dei dati.
- **Privacy**: offre protezione dalla rivelazione del contenuto dei messaggi. Per la crittografia viene utilizzata la *Cipher Block-Chaining* (CBC-DES). Su un messaggio SNMP può essere attiva solo l'autenticazione oppure possono essere attivate sia l'autenticazione che la privacy. Tuttavia, senza l'autenticazione non è possibile attivare la privacy.
- **Tempestività**: protegge dai ritardi o dalla riproduzione dei messaggi. L'agente SNMP confronta l'ora d'ingresso dei messaggi registrata con l'ora di arrivo.
- **Gestione delle chiavi**: indica la generazione, gli aggiornamenti e gli utilizzi delle chiavi. Il dispositivo supporta i filtri delle notifiche SNMP sulla base degli *ID oggetto* (OID) che vengono utilizzati dal sistema per gestire le funzioni del dispositivo.

Flusso di lavoro di SNMP

NOTA Per motivi di sicurezza, la modalità SNMP è disattivata per impostazione predefinita. Per poter gestire il dispositivo tramite SNMP, è necessario attivare prima la modalità SNMP nella pagina Protezione > Servizi TCP/UDP.

Per configurare l'SNMP, si consiglia di eseguire le seguenti operazioni:

Se si decide di utilizzare SNMPv1 o v2, attenersi alla seguente procedura:

PASSAGGIO 1 Passare alla pagina SNMP > Comunità e fare clic su **Aggiungi**. È possibile associare la comunità ai diritti di accesso o a un gruppo e visualizzarla rispettivamente in modalità di base o in modalità avanzata. È possibile definire i diritti di accesso di una comunità in due modi:

- **Modalità di base**: i diritti di accesso di una comunità possono essere configurati in sola lettura, lettura/scrittura o Amministrazione SNMP. Inoltre, è possibile selezionare una vista (definita nella pagina Viste) per limitare l'accesso alla comunità solo a determinati oggetti MIB.
- **Modalità avanzata**: i diritti di accesso di una comunità sono definiti da un gruppo (definito nella pagina Gruppi). Il gruppo può essere configurato attraverso un modello di protezione specifico. I diritti di accesso di un gruppo sono lettura, scrittura e notifica.

PASSAGGIO 2 Scegliere se limitare la stazione di gestione SNMP a un indirizzo o consentire la gestione SNMP da tutti gli indirizzi. Se si sceglie di limitare la gestione SNMP a un indirizzo, immettere l'indirizzo del PC di gestione SNMP nel campo Indirizzo IP.

PASSAGGIO 3 Inserire la stringa della comunità univoca nel campo Stringa della comunità.

PASSAGGIO 4 Se si desidera, attivare le trap tramite la pagina Impostazioni trap.

PASSAGGIO 5 Se si desidera, definire un filtro (i) di notifica utilizzando la pagina Filtro di notifica.

PASSAGGIO 6 Configurare il destinatari delle notifiche nella pagina Destinatari delle notifiche SNMPv1,2.

Se si decide di utilizzare SNMPv3, attenersi alla seguente procedura:

PASSAGGIO 1 Definire il motore SNMP nella pagina ID motore. Creare un ID motore univoco oppure usare l'ID motore predefinito. L'applicazione di una configurazione ID Motore comporta la cancellazione del database SNMP.

PASSAGGIO 2 Se si desidera, utilizzare la pagina Viste per definire le viste SNMP. Questa operazione limita l'intervallo di OID disponibili per una comunità o gruppo.

PASSAGGIO 3 Specificare i gruppi nella pagina Gruppi.

PASSAGGIO 4 Definire gli utenti nella pagina degli utenti SNMP, in cui è possibile associarli a un gruppo. Se l'ID motore SNMP non è impostato, allora gli utenti non possono essere creati.

PASSAGGIO 5 Se si desidera, attivare o disattivare le trap utilizzando la pagina Impostazioni di trap.

PASSAGGIO 6 Se si desidera, definire un filtro (i) di notifica utilizzando la pagina Filtro di notifica.

PASSAGGIO 7 Utilizzare la pagina Destinatari delle notifiche SNMPv3 per definire i destinatari delle notifiche.

MIB supportati

Per consultare l'elenco dei MIB supportati, visitare il seguente URL e accedere all'area di download **MIB di Cisco**:

www.cisco.com/cisco/software/navigator.html

OID del modello

Di seguito vengono riportati gli *ID oggetto* (OID) del modello di dispositivo:

Nome modello	Descrizione	ID oggetto
SF500-24	Switch gestito stackable 10/100 a 24 porte	9.6.1.80.24.1
SF500-24P	Switch gestito stackable PoE 10/100 a 24 porte	9.6.1.80.24.2
SF500-48	Switch gestito stackable 10/100 a 48 porte	9.6.1.80.48.1

Nome modello	Descrizione	ID oggetto
SF500-48P	Switch gestito stackable PoE 10/100 a 48 porte	9.6.1.80.48.2
SG500-28	Switch gestito stackable Gigabit a 28 porte	9.6.1.81.28.1
SG500-28P	Switch gestito stackable PoE Gigabit a 28 porte	9.6.1.81.28.2
SG500-52	Switch gestito stackable Gigabit a 52 porte	9.6.1.81.52.1
SG500-52P	Switch gestito stackable PoE Gigabit a 52 porte	9.6.1.81.52.2
SG500X-24	Gigabit a 24 porte con switch gestito stackable 10-Gigabit a 4 porte	9.6.1.85.24.1
SG500X 24P	Gigabit a 24 porte con switch gestito stackable PoE 10-Gigabit a 4 porte	9.6.1.85.24.2
SG500X-48	Gigabit a 48 porte con switch gestito stackable 10-Gigabit a 4 porte	9.6.1.85.48.1
SG500X-48P	Gigabit a 48 porte con switch gestito stackable PoE 10-Gigabit a 4 porte	9.6.1.85.48.2
ESW2-550X-48	Gigabit a 48 porte con switch gestito stackable 10 Gigabit a 4 porte	9.6.1.86.48.1
ESW2-550X-48DC	Gigabit a 48 porte con switch gestito stackable 10 Gigabit a 4 porte	9.6.1.86.48.6
SG500-52MP	Switch gestito Gigabit PoE max a 52 porte	9.6.1.81.5.3.0
ESW2-550X-48DC	Gigabit a 48 porte con switch gestito stackable 10-Gigabit a 4 porte	9.6.1.86.48.6

Gli ID oggetto privati vengono posizionati sotto: enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101).

ID motore SNMP

L'ID motore viene utilizzato per identificare in modo univoco le entità SNMPv3. Un agente SNMP viene considerato un motore SNMP autoritario. Ciò significa che l'agente risponde ai messaggi in ingresso (Get, GetNext, GetBulk, Set) e invia messaggi Trap a un responsabile. Le informazioni locali dell'agente vengono inserite nei campi del messaggio.

Ciascun agente SNMP conserva le informazioni locali che vengono poi utilizzate negli scambi di messaggi SNMPv3. L'ID motore SNMP predefinito è costituito dal codice aziendale e l'indirizzo MAC predefinito. Inoltre, deve essere univoco per il dominio amministrativo, in modo tale che due dispositivi di una rete non riportino lo stesso ID motore.

Le informazioni locali vengono memorizzate in quattro variabili MIB in sola lettura (snmpEngineId, snmpEngineBoots, snmpEngineTime e snmpEngineMaxMessageSize).

ATTENZIONE Quando si modifica l'ID motore, tutti gli utenti e i gruppi configurati vengono cancellati.

Per definire l'ID motore SNMP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **SNMP** > **ID motore**.

PASSAGGIO 2 Scegliere quale utilizzare per **ID motore locale**.

- **Usa predefinito**: selezionare questa casella di controllo per utilizzare l'ID motore generato dal dispositivo, che si basa sull'indirizzo MAC del dispositivo e corrisponde a:
  - *Primi quattro ottetti*: primo bit = 1 e il resto è il codice IANA Enterprise.
  - *Quinto ottetto*: impostare su 3 per indicare l'inizio dell'indirizzo MAC.
  - *Ultimi sei ottetti*: l'indirizzo MAC del dispositivo.
- **Nessuno**: non viene utilizzato alcun ID motore.
- **Definito dall'utente**: specificare l'ID del motore del dispositivo locale in una stringa esadecimale **(intervallo compreso tra 10 - 64)**. Ogni byte della stringa di caratteri esadecimali è indicato tramite due cifre esadecimali.

Tutti gli ID motore remoto e i relativi indirizzi IP vengono visualizzati nella tabella ID motore remoto.

PASSAGGIO 3 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

La tabella ID motore remoto mostra l'associazione tra gli indirizzi IP del motore e l'ID motore. Per aggiungere l'indirizzo IP di un ID motore, attenersi alla seguente procedura:

PASSAGGIO 4 Fare clic su **Aggiungi**. Immettere informazioni nei seguenti campi:

- **Definizione server**: selezionare se specificare il server ID motore in base all'indirizzo IP o al nome.
- **Versione IP**: selezionare il formato IP supportato.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se IPv6 viene utilizzato). Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale collegamento presenta un prefisso **FE80** non reindirizzabile, che è possibile utilizzare solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questa voce sostituisce l'indirizzo nella configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento (se Collega locale - Tipo di indirizzo IPv6 è selezionato) dall'elenco.
- **Indirizzo IP/Nome server**: immettere l'indirizzo IP o il nome di dominio del server dei log.
- **ID motore**: immettere l'ID motore.

PASSAGGIO 5 Fare clic su **Applica**. Il file Configurazione di esecuzione viene aggiornato.

Configurazione Viste SNMP

Una vista indica un'etichetta di una raccolta di sottostrutture MIB definita dall'utente. Ciascun ID sottostruttura viene definito dall'*ID oggetto* del root delle sottostrutture appropriate. Per specificare il root della sottostruttura desiderata, è possibile usare nomi conosciuti oppure inserire un OID (vedere **OID del modello**).

Ciascuna sottostruttura è inclusa o esclusa dalla vista specificata.

Nella pagina Viste è possibile creare e modificare viste SNMP. Non è possibile modificare le viste predefinite (Default, DefaultSuper).

Nella pagina Gruppi è possibile unire le viste ai gruppi o a una comunità che utilizza la modalità di accesso di base tramite la pagina Comunità.

Per definire le viste SNMP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **SNMP** > **Viste**.

PASSAGGIO 2 Scegliere **Aggiungi** per definire nuove viste.

PASSAGGIO 3 Immettere i parametri.

- **Nome vista**: immettere un nome vista di lunghezza compresa tra 0 e 30 caratteri.
- **Sottostruttura ID oggetto**: selezionare il nodo della struttura MIB inclusa o esclusa dal filtro di notifica. Le opzioni disponibili per la selezione degli oggetti sono:
  - *Seleziona dall'elenco*: consente di navigare la struttura MIB. Premere la freccia *Su* per andare al livello principale e pari livello del nodo; premere la freccia *Giù* per passare al livello secondario del nodo selezionato. Fare clic sui nodi della vista per passare da un nodo principale a quello di pari livello. Usare la barra di scorrimento per visualizzare i nodi di pari livello.
  - *Definito dall'utente*: immettere un OID che non è stato fornito nell'opzione *Seleziona dall'elenco*.

PASSAGGIO 4 Selezionare o deselezionare **Includi in vista.** Se questa opzione è stata selezionata, i MIB selezionati vengono inclusi nella vista. In caso contrario vengono esclusi.

PASSAGGIO 5 Fare clic su **Applica**.

PASSAGGIO 6 Per verificare la configurazione della vista, selezionare le viste definite da utente dall'elenco **Filtro: Nome vista**. Per impostazione predefinita, sono disponibili le viste seguenti:

- **Default**: mostra la vista SNMP predefinita per le viste di lettura e lettura/scrittura.
- **DefaultSuper**: mostra la vista SNMP predefinita per le viste degli amministratori.

È possibile aggiungere altre viste.

- **Sottostruttura ID oggetto**: indica la sottostruttura da includere o escludere dalla vista SNMP.
- **Vista sottostruttura ID oggetto**: indica se la sottostruttura specificata viene inclusa o esclusa dal filtro di notifica.

Creazione di gruppi SNMP

In SNMPv1 e SNMPv2, viene inviata una stringa della comunità con i frame SNMP. La stringa della comunità funge da password per ottenere l'accesso su un agente SNMP. Tuttavia, non vengono crittografati né i frame né la stringa della comunità. Pertanto, SNMPv1 e SNMPv2 non sono protetti.

In SNMPv3, possono essere configurati i seguenti meccanismi di sicurezza.

- **Autenticazione**: il dispositivo verifica che l'utente SNMP sia un amministratore di sistema autorizzato. Questa operazione viene eseguita per ciascun frame.
- **Privacy**: i frame SNMP possono riportare dati crittografati.

Quindi, in SNMPv3, sono disponibili tre livelli di protezione:

- Nessuna sicurezza (senza autenticazione e senza privacy)
- Autenticazione (autenticazione e senza privacy)
- Autenticazione e privacy

SNMPv3 fornisce un mezzo per controllare il contenuto che ogni utente può leggere o scrivere e le notifiche che riceve. Un gruppo definisce i privilegi di lettura / scrittura e un livello di sicurezza. Diventa operativo quando è associato a un utente SNMP o a una comunità.

NOTA Per associare una vista non predefinita a un gruppo, creare la vista nella pagina Viste.

Per creare un gruppo SNMP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **SNMP** > **Gruppi**.

In questa pagina vengono visualizzati i gruppi SNMP esistenti e i relativi livelli di protezione:

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **Nome gruppo:** immettere un nuovo nome del gruppo.
- **Modello di protezione**: selezionare la versione SNMP associata al gruppo SNMPv1, v2, o v3.

È possibile definire tre tipi di vista con vari livelli di protezione. Per ciascun livello di protezione, selezionare le viste per Leggi, Scrivi e Notifica compilando i seguenti campi:

- **Attiva**: selezionare questa opzione per attivare il livello di protezione.
- **Livello di protezione**: definire il livello di protezione associato al gruppo. SNMPv1 e SNMPv2 non supportano né autenticazione né privacy. Se SNMPv3 è selezionata, scegliere una delle seguenti opzioni:
  - *Senza autenticazione e senza privacy*: al gruppo non sono assegnati né il livello di protezione di autenticazione né quello della privacy.
  - *Autenticazione senza privacy*: consente di autenticare i messaggi SNMP e garantisce che l'origine del messaggio SNMP sia autenticata senza crittografarli.
  - *Autenticazione e privacy*: consente di autenticare i messaggi SNMP e di crittografarli.

- **Vista**: l'associazione della vista con i privilegi di lettura, scrittura e notifica del gruppo limita la portata della struttura MIB a cui il gruppo ha accesso di lettura, scrittura e notifica.
  - *Vista*: selezionare una vista per lettura, scrittura e notifica definita in precedenza.
  - *Lettura*: consente di gestire l'accesso di sola lettura per la vista selezionata. In caso contrario, un utente o una comunità associata a questo gruppo può accedere in lettura a tutti i MIB tranne a quelli che controllano lo stesso SNMP.
  - *Scrittura*: consente di gestire l'accesso in scrittura per la vista selezionata. In caso contrario, un utente o una comunità associata a questo gruppo può accedere in scrittura a tutti i MIB tranne a quelli che controllano l'SNMP.
  - *Notifica*: limita il contenuto a disposizione delle trap a quelli inclusi nella vista selezionata. In caso contrario, i contenuti dei trap non presentano alcuna restrizione. Questa opzione può essere selezionata solo per SNMPv3.

PASSAGGIO 4 Fare clic su **Applica**. Il gruppo SNMP viene salvato nel file di configurazione esecuzione.

Gestione degli utenti SNMP

Un utente SNMP viene definito dalle credenziali di accesso (nome utente, password e metodo di autenticazione) e tramite il contesto e l'analisi in cui opera in associazione a un gruppo o un ID motore.

L'utente configurato ha gli attributi del suo gruppo, avendo i privilegi di accesso configurato all'interno della vista associata.

I gruppi consentono ai responsabili di rete di assegnare i diritti di accesso a un gruppo di utenti anziché a un singolo utente.

Un utente può solo appartenere a un singolo gruppo.

Per creare un utente SNMPv3, è necessario che ci sia la condizione seguente:

- Un ID motore deve essere prima configurato sul dispositivo. Ciò avviene nella pagina ID motore.

- Deve essere disponibile un gruppo SNMPv3. Un gruppo SNMPv3 è definito nella pagina Gruppi.

Per visualizzare utenti SNMP e definirne nuovi, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **SNMP** > **Utenti**.

Nella pagina vengono visualizzati gli utenti esistenti.

PASSAGGIO 2 Fare clic su **Aggiungi.**

Questa pagina fornisce le informazioni per assegnare privilegi sul controllo di accesso SNMP agli utenti SNMP.

PASSAGGIO 3 Immettere i parametri.

- **Nome utente**: immettere un nome per l'utente.
- **ID motore**: selezionare l'entità SNMP locale o remota a cui è collegato l'utente. La modifica o la rimozione dell'ID motore SNMP comporta l'eliminazione del Database utenti SNMPv3. Per ricevere messaggi informazione e informazioni relative alla richiesta, è necessario definire sia un utente locale che remoto.
  - *Locale*: l'utente è collegato a un dispositivo locale.
  - *Indirizzo IP remoto*: l'utente è collegato a una entità SNMP diversa oltre al dispositivo locale. Se viene indicato l'ID motore remoto, i dispositivi remoti ricevono messaggi inform ma non possono richiedere informazioni.

    Inserire l'ID motore remoto.
- **Nome gruppo**: selezionare i gruppi SNMP a cui appartiene l'utente SNMP. I gruppi SNMP vengono definiti nella pagina Aggiungi gruppo.

  NOTA Gli utenti che appartengono a gruppi che sono stati cancellati rimarranno, ma sono inattivi.
- **Metodo di autenticazione**: selezionare il metodo di autenticazione che varia in base al Nome gruppo assegnato. Se il gruppo non richiede l'autenticazione, non può essere configurata alcuna autenticazione per l'utente. Sono disponibili le seguenti opzioni:
  - *Nessuno*: non viene usata alcuna autenticazione.
  - *Password MD5*: è la password utilizzata per generare una chiave tramite il metodo di autenticazione MD5.

- *Password SHA*: è la password utilizzata per generare una chiave tramite il metodo di autenticazione SHA (Secure Hash Algorithm).

- **Password di autenticazione**: se l'autenticazione viene realizzata tramite una password MD5 o SHA, immettere la password dell'utente locale **Con crittografia** o **Testo normale**. Le password dell'utente locale vengono confrontate con il database locale e possono contenere massimo 32 caratteri ASCII.
- **Metodo di privacy**: selezionare una delle seguenti opzioni:
  - *Nessuno*: la password per la privacy non viene crittografata.
  - *DES*: la password per la privacy viene crittografata secondo il DES (Data Encryption Standard).
- **Password per la Privacy**: se il metodo di privacy è selezionato, sono necessari 16 byte (chiave crittografica DES). Il campo deve contenere esattamente 32 caratteri esadecimali. È possibile selezionare la modalità **Con crittografia** o **Testo normale**.

PASSAGGIO 4 Scegliere **Applica** per salvare le impostazioni.

Definizione delle comunità SNMP

In SNMPv1 e SNMPv2, i diritti di accesso vengono gestiti tramite la definizione delle comunità nella pagina Comunità. Il nome della comunità rappresenta un tipo di password condivisa tra la stazione di gestione SNMP e il dispositivo e viene usato per autenticare la stazione di gestione SNMP.

Le comunità vengono specificate solo in SNMPv1 e SNMPv2 poiché SnMPv3 può essere utilizzato con utenti e non con comunità. Gli utenti appartengono ai gruppi a cui sono stati assegnati i diritti di accesso.

La pagina Comunità consente di associare comunità che dispongono di diritti di accesso, sia direttamente (modalità di base) che tramite gruppi (modalità avanzata):

- **Modalità di base**: i diritti di accesso di una comunità possono essere configurati in sola lettura, lettura/scrittura o Amministrazione SNMP. Inoltre, è possibile selezionare una vista (definita nella pagina Viste SNMP) per limitare l'accesso alla comunità solo a determinati oggetti MIB.

- **Modalità avanzata**: i diritti di accesso di una comunità sono definiti da un gruppo (definito nella pagina Gruppi). Il gruppo può essere configurato attraverso un modello di protezione specifico. I diritti di accesso di un gruppo sono lettura, scrittura e notifica.

Per definire le comunità SNMP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **SNMP** > **Comunità**.

In questa pagina viene visualizzata una tabella di comunità SNMP configurate e le loro proprietà.

PASSAGGIO 2 Fare clic su **Aggiungi.**

In questa pagina i responsabili di rete possono definire e configurare nuove comunità SNMP.

PASSAGGIO 3 **Stazione di gestione SNMP**: fare clic su **Definito dall'utente** per immettere nella stazione di gestione l'indirizzo IP che può accedere alla comunità SNMP, oppure su **Tutti** per indicare che la comunità SNMP è accessibile da qualsiasi indirizzo IP.

- **Versione IP**: selezionare IPv4 o IPv6.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 supportato utilizzato. Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale collegamento presenta un prefisso **FE80** non reindirizzabile, che è possibile utilizzare solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questa voce sostituisce l'indirizzo nella configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: se il tipo di indirizzo IPv6 è Collega locale, selezionare se riceverlo tramite VLAN o ISATAP.
- **Indirizzo IP**: immettere l'indirizzo IP stazione di gestione SNMP.
- **Stringa della comunità**: immettere il nome della comunità utilizzato per autenticare la stazione di gestione sul dispositivo.

- **Di base**: selezionare questa modalità per una comunità selezionata. In questa modalità, non esistono legami a gruppi. È possibile scegliere solo il livello di accesso della comunità (Sola lettura, Lettura/scrittura, Amministrazione) e, facoltativamente, specificarlo ulteriormente per una vista specifica. Per impostazione predefinita, questa modalità viene applicata a tutto il MIB. Se selezionata, immettere i valori nei campi seguenti:
  - *Modalità di accesso*: selezionare i diritti di accesso della comunità. Sono disponibili le seguenti opzioni:

    Sola lettura: l'accesso può essere gestito esclusivamente in sola lettura e non è possibile apportare modifiche alla comunità.

    Lettura/scrittura: l'accesso può essere gestito in lettura/scrittura ed è possibile modificare la configurazione del dispositivo ma non la comunità.

    Amministrazione SNMP: l'utente può accedere a tutte le opzioni di configurazione del dispositivo e dispone dei diritti per modificare la comunità. Ammin. SNMP Admin è l'equivalente a lettura e scrittura per tutti i MIB tranne che per i MIB SNMP. Ammin. SNMP è necessario per l'accesso ai MNB SNMP.
  - *Visualizza nome*: selezionare una vista SNMP (un insieme di sottostrutture MIB a cui è concesso l'accesso).
- **Impostazioni avanzate**: selezionare questa modalità per una comunità selezionata.
  - *Nome gruppo*: selezionare un gruppo SNMP che determina i diritti di accesso.

PASSAGGIO 4 Fare clic su **Applica**. La comunità SNMP è definita e il file Configurazione di esecuzione viene aggiornato.

Definizione delle impostazioni trap

Nella pagina Impostazioni di trap è possibile scegliere se inviare o meno notifiche SNMP dal dispositivo e in quali circostanze. I destinatari delle notifiche SNMP possono essere configurati nella pagina Destinatari delle notifiche SNMPv1,2 o nella pagina Destinatari delle notifiche SNMPv3.

Per definire le impostazioni trap, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **SNMP** > **Impostazioni trap**.

PASSAGGIO 2 Selezionare **Attiva** per **Notifiche SNMP** per specificare che il dispositivo può inviare notifiche SNMP.

PASSAGGIO 3 Selezionare **Attiva** nelle **Notifiche di autenticazione** per attivare l'invio di notifiche in caso di errore di autenticazione SNMP.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni trap SNMP vengono scritte nel file Configurazione di esecuzione.

Destinatari delle notifiche

Come descritto in RFC 1215, i messaggi trap vengono generati per riportare gli eventi del sistema. Il sistema può generare messaggi trap definiti nel MIB supportato.

I ricevitori di trap (o destinatari delle notifiche) sono nodi della rete che ricevono i messaggi di trap inviati dal dispositivo. Un elenco di destinatari di notifiche viene definito come target dei messaggi trap.

Una voce di un ricevitore trap contiene l'indirizzo IP del nodo e le credenziali SNMP corrispondenti alla versione inclusa nel messaggio trap. Quando si verifica un evento che richiede l'invio di un messaggio trap, questo viene inviato a ciascun nodo riportato nella Tabella Destinatario notifiche.

Le pagine Destinatari delle notifiche SNMPv1,2 Destinatari delle notifiche SNMPv3 consentono di configurare le destinazioni delle notifiche SNMP e i tipi di notifiche SNMP inviate a ciascuna destinazione (trap o messaggi inform). Le finestre a comparsa Aggiungi/Modifica consentono di configurare gli attributi delle notifiche.

Una notifica SNMP consiste in un messaggio inviato dal dispositivo alla stazione di gestione SNMP in cui viene riportato un evento che si è verificato, ad esempio un collegamento attivo/inattivo.

Inoltre, è possibile filtrare determinate notifiche. A tal fine è possibile creare un filtro nella pagina Filtro di notifica e associarlo al destinatario di una notifica SNMP. Il filtro della notifica consente di filtrare il tipo di notifiche SNMP inviate alla stazione di gestione in base all'OID della notifica che sta per essere inviata.

Definizione dei destinatari delle notifiche SNMPv1,2

Per definire un destinatario in SNMPv1,2, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **SNMP** > **Destinatari delle notifiche SNMPv1,2**.

In questa pagina vengono visualizzati i destinatari per SNMPv1,2.

PASSAGGIO 2 Immettere informazioni nei seguenti campi:

- **Interfaccia IPv4 di origine inform**: selezionare l'interfaccia di origine il cui indirizzo IPv4 verrà utilizzato come indirizzo IPv4 di origine nei messaggi inform per comunicare con i server SNMP IPv4.
- **Interfaccia IPv4 di origine trap**: selezionare l'interfaccia di origine il cui indirizzo IPv6 verrà utilizzato come indirizzo IPv6 di origine nei messaggi trap per comunicare con i server SNMP IPv6.
- **Interfaccia IPv6 di origine inform**: selezionare l'interfaccia di origine il cui indirizzo IPv4 verrà utilizzato come indirizzo IPv4 di origine nei messaggi inform per comunicare con i server SNMP IPv4.
- **Interfaccia IPv6 di origine trap**: selezionare l'interfaccia di origine il cui indirizzo IPv6 verrà utilizzato come indirizzo IPv6 di origine nei messaggi trap per comunicare con i server SNMP IPv6.

  NOTA Se viene selezionata l'opzione Automatica, il sistema prende l'indirizzo IP di origine dall'indirizzo IP definito nell'interfaccia di uscita.

PASSAGGIO 3 Fare clic su **Aggiungi.**

PASSAGGIO 4 Immettere i parametri.

- **Definizione server**: selezionare se specificare il server di log remoti in base all'indirizzo IP o al nome.
- **Versione IP**: selezionare IPv4 o IPv6.
- **Tipo di indirizzo IPv6**: selezionare *Collega locale* o *Globale*.
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale collegamento presenta un prefisso **FE80** non reindirizzabile, che è possibile utilizzare solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questa voce sostituisce l'indirizzo nella configurazione.

  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.

- **Interfaccia locale collegamento**: se il tipo di indirizzo IPv6 è Collega locale, selezionare se riceverlo tramite VLAN o ISATAP.
- **Indirizzo IP/Nome destinatario**: immettere l'indirizzo IP o il nome del server a cui vengono inviate le trap.
- **Porta UDP**: immettere la porta UDP utilizzata per le notifiche sul dispositivo del destinatario.
- **Tipo di notifica**: scegliere se inviare trap o messaggi inform. Se sono necessari entrambi, si dovranno creare due destinatari.
- **Timeout**: immettere il numero di secondi che il dispositivo deve attendere prima di reinviare i messaggi inform.
- **Tentativi**: specificare quante volte il dispositivo reinvia una richiesta messaggi inform.
- **Stringa della comunità**: selezionare dall'elenco a discesa la stringa della comunità del gestore delle trap. I nomi della Stringa della comunità sono generati da quelli elencati nella pagina Comunità.
- **Versione di notifica**: selezionare la versione SNMP della trap. Nelle trap è possibile utilizzare SNMPv1 o SNMPv2, attivando una singola versione alla volta.
- **Filtro di notifica**: selezionare questa opzione per attivare il filtro del tipo di notifiche SNMP inviate alla stazione di gestione. I filtri vengono creati nella pagina Filtro di notifica.
- **Nome filtro**: selezionare il filtro SNMP che definisce le informazioni contenute nelle trap; il filtro viene impostato nella pagina Filtro di notifica.

PASSAGGIO 5 Fare clic su **Applica**. Le impostazioni del Destinatario notifiche SNMP vengono scritte nel file Configurazione di esecuzione.

Definizione dei Destinatari delle notifiche SNMPv3

Per definire un destinatario in SNMPv3, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **SNMP** > **Destinatari delle notifiche SNMPv3**.

In questa pagina vengono visualizzati i destinatari per SNMPv3.

- **Interfaccia IPv4 di origine inform**: selezionare l'interfaccia di origine il cui indirizzo IPv4 verrà utilizzato come indirizzo IPv4 di origine nei messaggi inform per comunicare con i server SNMP IPv4.
- **Interfaccia IPv4 di origine trap**: selezionare l'interfaccia di origine il cui indirizzo IPv6 verrà utilizzato come indirizzo IPv6 di origine nei messaggi trap per comunicare con i server SNMP IPv6.
- **Interfaccia IPv6 di origine inform**: selezionare l'interfaccia di origine il cui indirizzo IPv4 verrà utilizzato come indirizzo IPv4 di origine nei messaggi inform per comunicare con i server SNMP IPv4.
- **Interfaccia IPv6 di origine trap**: selezionare l'interfaccia di origine il cui indirizzo IPv6 verrà utilizzato come indirizzo IPv6 di origine nei messaggi trap per comunicare con i server SNMP IPv6.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **Definizione server**: selezionare se specificare il server di log remoti in base all'indirizzo IP o al nome.
- **Versione IP**: selezionare IPv4 o IPv6.
- **Tipo di indirizzo IPv6**: selezionare il tipo di indirizzo IPv6 (se IPv6 viene utilizzato). Sono disponibili le seguenti opzioni:
  - *Collega locale*: l'indirizzo IPv6 identifica in modo univoco gli host in un singolo collegamento di rete. Un indirizzo locale collegamento presenta un prefisso **FE80** non reindirizzabile, che è possibile utilizzare solo per le comunicazioni sulla rete locale. È supportato soltanto un indirizzo locale collegamento. Se sull'interfaccia è presente un indirizzo locale collegamento, questa voce sostituisce l'indirizzo nella configurazione.
  - *Globale*: l'IPv6 è un tipo di indirizzo IPv6 unicast globale visibile e raggiungibile da altre reti.
- **Interfaccia locale collegamento**: selezionare l'interfaccia locale collegamento (se Collega locale - Tipo di indirizzo IPv6 è selezionato) dall'elenco.

- **Indirizzo IP/Nome destinatario**: immettere l'indirizzo IP o il nome del server a cui vengono inviate le trap.
- **Porta UDP**: immettere le porta UDP utilizzata per le notifiche inviate sul dispositivo del destinatario.
- **Tipo di notifica**: scegliere se inviare trap o messaggi inform. Se sono necessari entrambi, si dovranno creare due destinatari.
- **Timeout**: immettere la quantità di tempo (secondi) che il dispositivo deve attendere prima di reinviare messaggi inform/trap. Timeout: intervallo compreso tra 1 e 300, predefinito 15.
- **Tentativi**: specificare quante volte il dispositivo reinvia una richiesta messaggi inform. Tentativi: intervallo compreso tra 1 e 255, predefinito 3.
- **Nome utente**: selezionare da un elenco a discesa l'utente a cui inviare le notifiche SNMP. Al fine di ricevere le notifiche, questo utente deve essere definito sulla pagina utente SNMP e il suo ID motore deve essere remoto.
- **Livello di protezione**: selezionare la quantità di autenticazione da applicare al pacchetto.

  NOTA Il livello di protezione dipende dal nome utente selezionato. Se questo nome utente è stato configurato come Nessuna autenticazione, il livello di protezione sarà solo Nessuna autenticazione. Tuttavia, se a questo Nome utente sono state assegnate Autenticazione e Privacy nella pagina Utente, il livello di protezione in questa schermata può essere Nessuna autenticazione, Solo autenticazione o Autenticazione e privacy.

  Sono disponibili le seguenti opzioni:

  - *Nessuna autenticazione*: indica che il pacchetto non viene né autenticato né crittografato.
  - *Autenticazione*: indica che il pacchetto viene autenticato ma non crittografato.
  - *Privacy*: indica che il pacchetto viene autenticato e crittografato.
- **Filtro di notifica**: selezionare questa opzione per attivare il filtro del tipo di notifiche SNMP inviate alla stazione di gestione. I filtri vengono creati nella pagina Filtro di notifica.
- **Nome filtro**: selezionare il filtro SNMP che definisce le informazioni contenute nelle trap; il filtro viene impostato nella pagina Filtro di notifica.

PASSAGGIO 4 Fare clic su **Applica**. Le impostazioni del Destinatario notifiche SNMP vengono scritte nel file Configurazione di esecuzione.

Filtri per le notifiche SNMP

Nella pagina Filtro di notifica è possibile configurare i filtri di notifica SNMP e gli ID oggetto (OID) selezionati. Dopo aver creato un filtro di notifica, è possibile associarlo a un destinatario di notifica nelle pagine Destinatari delle notifiche SNMPv1,2 e Destinatari delle notifiche SNMPv3 .

Il filtro della notifica consente di filtrare il tipo di notifiche SNMP inviate alla stazione di gestione in base all'OID della notifica da inviare.

Per definire un filtro per le notifiche, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **SNMP** > **Filtro di notifica**.

La pagina Filtro di notifica consente di visualizzare le informazioni di notifica per ciascun filtro. La tabella consente di filtrare le voce in base a Nome filtro.

PASSAGGIO 2 Fare clic su **Aggiungi**.

PASSAGGIO 3 Immettere i parametri.

- **Nome filtro**: immettere un nome con lunghezza compresa tra 0 e 30 caratteri.
- **Sottostruttura ID oggetto**: selezionare il nodo della struttura MIB inclusa o esclusa dal filtro SNMP selezionato. Le opzioni disponibili per la selezione degli oggetti sono:
  - *Seleziona dall'elenco*: consente di navigare la struttura MIB. Premere la freccia *Su* per andare al livello principale e pari livello del nodo; premere la freccia *Giù* per passare al livello secondario del nodo selezionato. Fare clic sui nodi della vista per passare da un nodo principale a quello di pari livello. Usare la barra di scorrimento per visualizzare i nodi di pari livello.
  - Se si utilizza l'*ID oggetto*, l'**identificatore oggetto immesso** viene incluso nella vista se l'opzione **Includi in filtro** è selezionata.

PASSAGGIO 4 Selezionare o deselezionare **Includi in filtro.** Se questa opzione è selezionata, i MIB selezionati sono inclusi nel filtro, altrimenti sono esclusi.

PASSAGGIO 5 Fare clic su **Applica**. Le viste SNMP vengono definite e la configurazione di esecuzione viene aggiornata.

File carrier per la versione stampata della Guida all'amministrazione dei modelli Sx500 e SG500X

Tag di condizione

I seguenti tag di condizione sono definiti nei file:

Nome tag di condizione			Descrizione
Commento	Inattivo		Utilizzato per domande/ problemi/commenti editoriali interni
Interno	Inattivo		Informazioni interne per scopi di sviluppo, non mostrate al cliente
Guida in linea	Inattivo		Per tutti gli aspetti e per la versione della guida in linea
Documenti stampati	Attivo	■	Per tutti gli aspetti e per la versione stampata
Sx200	Inattivo		Per le versioni stampate e in linea del modello Sx200
Sx200_Help	Inattivo		Per la versione della guida in linea del modello Sx200
Sx200_Print	Inattivo		Per la versione stampata del modello Sx200
Sx300	Inattivo		Per le versioni stampate e in linea del modello Sx300
Sx300_Help	Inattivo		Per la versione della guida in linea del modello Sx300
Sx300_Print	Inattivo		Per la versione stampata del modello Sx300
Sx500	Attivo	■	Per le versioni stampate e in linea del modello Sx500
Sx500_Help	Inattivo		Per la versione della guida in linea del modello Sx500
Sx500_Print	Attivo	■	Per la versione stampata del modello Sx500

Elenco delle variabili definite nei file

Nome variabile	Descrizione
Titolo libro	Guida all'amministrazione degli switch gestiti stackable Cisco Small Business serie 500
Copyright	Copyright © 2012-2013
defaultusername	**cisco**
defaultpassword	**cisco**
Interfaccia	utilità di configurazione dello switch basata sul Web
Famiglia prodotto	Cisco Small Business
Versione	78-21349-01