Modicon

MCSESM, MCSESM-E, MCSESP Switch con Management
Manuale utente Configurazione

QGH59082.02

www.schneider-electric.com

Schneider Electric

Questa documentazione contiene la descrizione generale e/o le caratteristiche tecniche dei prodotti qui contenuti. Questa documentazione non è destinata e non deve essere utilizzata per determinare l'adeguatezza o l'affidabilità di questi prodotti relativamente alle specifiche applicazioni dell'utente. Ogni utente o specialista di integrazione deve condurre le proprie analisi complete e appropriate del rischio, effettuare la valutazione e il test dei prodotti in relazione all'uso o all'applicazione specifica. Né Schneider Electric né qualunque associata o filiale deve essere tenuta responsabile o perseguibile per il cattivo uso delle informazioni ivi contenute. Gli utenti possono inviarci commenti e suggerimenti per migliorare o correggere questa pubblicazione.

Durante l'installazione e l'uso di questo prodotto è necessario rispettare tutte le normative locali, nazionali o internazionali in materia di sicurezza. Per motivi di sicurezza e per assicurare la conformità ai dati di sistema documentati, la riparazione dei componenti deve essere effettuata solo dal costruttore.

Quando i dispositivi sono utilizzati per applicazioni con requisiti tecnici di sicurezza, occorre seguire le istruzioni più rilevanti.

Un utilizzo non corretto del software Schneider Electric (o di altro software approvato) con prodotti hardware Schneider Electric può costituire un rischio per l'incolumità del personale o provocare danni alle apparecchiature.

La mancata osservanza di queste indicazioni può costituire un rischio per l'incolumità del personale o provocare danni alle apparecchiature.

Facendo parte di un gruppo di aziende responsabili e inclusive, stiamo aggiornando I contenuti della nostra comunicazione che potrebbero contenere una terminologia non inclusiva. Tuttavia, fino a quando il processo non sarà completato, potrebbero ancora essere presenti termini standard di business che alcuni dei nostri clienti potrebbero ritenere inappropriati.

Contenuto

Avvertenze di sicurezza

Nota: Leggere attentamente le presenti istruzioni e familiarizzare con l'apparecchio prima di installarlo, metterlo in funzione o sottoporlo a manutenzione. Le avvertenze riportate qui di seguito possono essere contenute su diversi punti di questa documentazione o leggibili sull'apparecchio. Le avvertenze mettono in guardia su possibili rischi e pericoli o richiamano l'attenzione su informazioni che chiariscono o semplificano i processi.

L'aggiunta di questo simbolo a un'etichetta di “Pericolo” o “Avviso” indica che esiste un potenziale pericolo da shock elettrico che può causare lesioni personali se non vengono rispettate le istruzioni.

Questo è un simbolo di avvertimento generale. Fa riferimento a possibili pericoli di ferimento. Osservare tutti gli avvertimenti elencati sotto questo simbolo per evitare ferite o incidenti anche mortali.

⚠ PERICOLO

PERICOLO fa riferimento a una situazione di pericolo imminente e la mancata osservanza porta **inevitabilmente** a lesioni gravi o mortali.

⚠ AVVERTENZA

AVVERTENZA fa riferimento a un possibile pericolo che se non viene evitato **può causare** ferite gravi o mortali.

⚠ ATTENZIONE

ATTENZIONE fa riferimento a un possibile pericolo che se non viene evitato **può causare** ferite lievi.

AVVISO

Un **AVVISO** è utilizzato per affrontare delle prassi non connesse all'incolumità personale.

Nota: Manutenzione, riparazione, installazione e uso delle apparecchiature elettriche si devono affidare solo a personale qualificato. Schneider Electric non si assume alcuna responsabilità per qualsiasi conseguenza derivante dall’uso di questo materiale.

Il personale qualificato è in possesso di capacità e conoscenze specifiche sulla costruzione, il funzionamento e l'installazione di apparecchiature elettriche ed è addestrato sui criteri di sicurezza da rispettare per poter riconoscere ed evitare le condizioni a rischio.

Informazioni sul presente manuale

Ambito di validità

I dati e le illustrazioni contenuti nel presente manuale non sono vincolanti. Ci riserviamo il diritto di apportare modifiche ai nostri prodotti, nel quadro della strategia di sviluppo costante da noi perseguita. Le informazioni contenute nella documentazione possono essere modificate senza preavviso e non sono da considerarsi vincolanti per Schneider Electric.

Commento dell'utente

Accogliamo sempre con piacere ogni nota e indicazione da parte dell'utente. Esse potranno essere inviate al nostro indirizzo e-mail: techpub@schneider-electric.com

Documentazione di riferimento

Il manuale utente “Configurazione” contiene le informazioni necessarie per la messa in servizio del dispositivo. Costituisce una guida passo per passo a partire dalla prima messa in funzione fino alle impostazioni basilari, per un funzionamento adeguato al relativo ambiente.

Il manuale utente “Installazione” comprende una descrizione del dispositivo, le avvertenze di sicurezza, una descrizione delle indicazioni visualizzate sul display e ulteriori informazioni necessarie per l’installazione del dispositivo.

Il manuale di riferimento “Interfaccia grafica utente” contiene informazioni dettagliate sull’uso dell’interfaccia grafica utente per l’impiego delle singole funzioni del dispositivo.

Il manuale di riferimento “Interfaccia a riga di comando” contiene informazioni dettagliate sull’uso dell’interfaccia a riga di comando per l’impiego di singole funzioni del dispositivo.

ConneXium Network Manager software di gestione della rete offre ulteriori possibilità per una configurazione e un monitoraggio senza problemi:
- Riconoscimento topologico automatico
- Interfaccia browser
- Struttura client/server
- Gestione degli eventi
- Event log
- Configurazione simultanea di più dispositivi
- Interfaccia grafica utente con layout della rete
- Gateway SNMP/OPC

Key

Le definizioni utilizzate in questo manuale hanno i seguenti significati:

▶	Elenco
□	Passaggio di lavoro
Connessione (Connection)	Riferimento incrociato con link
Nota:	Una nota sottolinea un evento importante oppure evidenzia una dipendenza.
`Courier`	Rappresentazione di un comando CLI o di contenuti di campo nell'interfaccia grafica utente

Esecuzione nell'interfaccia grafica utente

Esecuzione nell'interfaccia a riga di comando.

Sostituire un dispositivo

Per sostituire un dispositivo con un altro dello stesso tipo, se ad esempio è stato rilevato un guasto o per manutenzione preventiva, il dispositivo fornisce le seguenti soluzioni plug-and-play:

- Il nuovo dispositivo carica il profilo di configurazione del dispositivo sostituito dalla memoria esterna.
  Vedi “Caricamento del profilo di configurazione dalla memoria esterna” a pagina 106.
- Il nuovo dispositivo ottiene l'indirizzo IP utilizzando la *Option 82* DHCP.
  Vedi “Relè L2 DHCP” a pagina 316.
  Vedi “Impostazione di un server DHCP con opzione 82” a pagina 361.

Al riavvio, con ogni soluzione il nuovo dispositivo ottiene le stesse impostazioni IP del dispositivo sostituito.

- Per accedere alla gestione del dispositivo utilizzando HTTPS, il dispositivo utilizza un certificato digitale. È possibile importare il certificato dell'utente sul dispositivo.
  Vedi “Gestione del certificato HTTPS” a pagina 367.
- Per accedere alla gestione del dispositivo con SSH, il dispositivo utilizza una chiave host RSA. È possibile importare nel dispositivo la chiave host dell'utente in formato PEM.
  Vedi “Caricamento della propria chiave sul dispositivo” a pagina 364.

1 Interfacce utente

Il dispositivo consente di specificare le impostazioni del dispositivo utilizzando le seguenti interfacce utente.

Tabella 1: Interfacce utente per accedere alla gestione del dispositivo

Interfaccia utente	Raggiungibile tramite …	Prerequisito
Interfaccia grafica utente	Ethernet (In-Band)	Browser web
Interfaccia a riga di comando	Ethernet (In-Band) Interfaccia seriale (Out-of-Band)	Software per emulazione di terminale
Monitor di sistema	Interfaccia seriale (Out-of-Band)	Software per emulazione di terminale

1.1 Interfaccia grafica utente

Requisiti di sistema

Per aprire l'interfaccia grafica utente, è necessaria la versione desktop di un browser web che supporti l'HTML5.

Nota: Il software di terzi quali i browser web validano i certificati sulla base di criteri quali la data di scadenza e le attuali raccomandazioni per parametri crittografici. I certificati obsoleti potrebbero causare problemi dovuti a informazioni non valide o non aggiornate. Esempio: un certificato scaduto oppure modifica delle raccomandazioni crittografiche. Per risolvere i conflitti di validazione con il software di terzi, trasferire il certificato aggiornato al dispositivo oppure rigenerare il certificato con il firmware più aggiornato.

Avvio dell'interfaccia grafica utente

Il prerequisito per l'avvio dell'interfaccia grafica utente è che i parametri IP siano configurati nel dispositivo. Vedi “Definizione dei parametri IP” a pagina 43.

Eseguire i seguenti passaggi:
- ☐ Avviare il rispettivo browser web.
- ☐ Digitare l'indirizzo IP del dispositivo nel campo indirizzi del browser web.
  Utilizzare la seguente forma: `https://xxx.xxx.xxx.xxx`
  Il browser web imposta la connessione al dispositivo e visualizza la finestra di dialogo di accesso.
- ☐ Se si desidera modificare la lingua dell'interfaccia grafica utente, fare clic sul link appropriato nell'angolo in alto a destra nella finestra di dialogo di accesso.
- ☐ Inserire il nome utente.
- ☐ Inserire la password.
- ☐ Fare clic sul pulsante *Login*.
  Il browser web visualizza l'interfaccia grafica utente.

1.2 Interfaccia a riga di comando

L'interfaccia a riga di comando consente di comandare le funzioni del dispositivo tramite una connessione locale o a distanza.

Gli specialisti IT riconoscono nella Command Line Interface l'ambiente consueto per la configurazione di dispositivi IT. Un utente o amministratore competente conosce gli elementi di base e come utilizzare i dispositivi Schneider Electric.

1.2.1 Preparazione della connessione dati

Per le informazioni di assemblaggio e avvio del dispositivo, consultare il manuale utente “Installazione”.

- ☐ Connettere il dispositivo alla rete. Il prerequisito per una corretta connessione dati è l'impostazione corretta dei parametri di rete.

È possibile accedere all'interfaccia utente della Command Line Interface ad esempio, tramite il programma freeware *PuTTY*.

- ☐ Installare il programma *PuTTY* sul computer.

1.2.2 Accesso alla Command Line Interface utilizzando Telnet

Connessione Telnet utilizzando Windows

Telnet è installato di default solamente nelle versioni Windows anteriori a Windows Vista.

Eseguire i seguenti passaggi:

- ☐ Avviare il programma *Command Prompt* sul computer.
- ☐ Inserire il comando `telnet <IP_address>`.

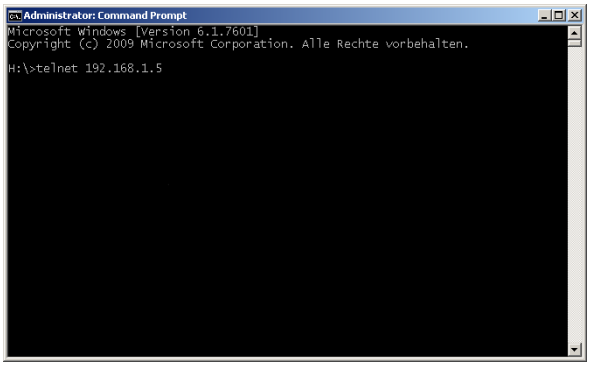


Figura 1: Command Prompt: impostazione della connessione Telnet al dispositivo

Connessione Telnet utilizzando PuTTY

Eseguire i seguenti passaggi:

- ☐ Avviare il programma *PuTTY* sul computer.

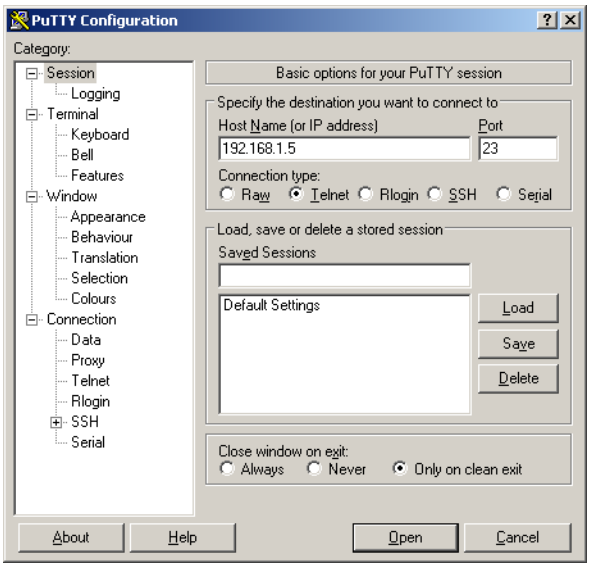


Figura 2: Schermata di immissione di PuTTY

- ☐ Nel campo *Host Name (or IP address)* si specifica l'indirizzo IP del dispositivo.
  L'indirizzo IP è costituito da 4 numeri decimali con valori da `0` a `255`. I 4 numeri decimali sono separati da punti.
- ☐ Per scegliere il tipo di connessione, selezionare il pulsante di opzione *Telnet* nell'elenco opzioni *Connection type*.
- ☐ Fare clic sul pulsante *Open* per impostare la connessione dati al dispositivo.
  Sullo schermo compare la Command Line Interface con una finestra per l'inserimento del nome utente. Il dispositivo consente a un massimo di 5 utenti di avere accesso alla Command Line Interface contemporaneamente.

Nota: Questo dispositivo è un prodotto importante dal punto di vista della sicurezza. Modificare la password durante la prima procedura di avvio.

Eseguire i seguenti passaggi:

- ☐ Inserire il nome utente.
  Il nome utente di default è `admin`.
- ☐ Premere il tasto <Enter>.

- ☐ Inserire la password.
  La password predefinita è `private`.
- ☐ Premere il tasto <Enter>.

```
                    Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                             MCSESM-E Release 08.7.00

                            (Build date 2022-07-11 16:30)


                  System Name   :  MCSESM-646038d5e846
                  Management IP :  192.168.1.5
                  Subnet Mask   :  255.255.255.0
                  Base MAC      :  64:60:38:01:02:03
                  USB IP        :  91.0.0.100
                  USB Mask      :  255.255.255.0
                  System Time   :  2022-07-13 19:41:31


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

Figura 3: Schermata di avvio della Command Line Interface

1.2.3 Accesso alla Command Line Interface utilizzando l'SSH (Secure shell)

Nel seguente esempio utilizziamo il programma *PuTTY*. Un'altra opzione è quella di accedere al dispositivo utilizzando SSH nella OpenSSH Suite.

Eseguire i seguenti passaggi:

- ☐ Avviare il programma *PuTTY* sul computer.

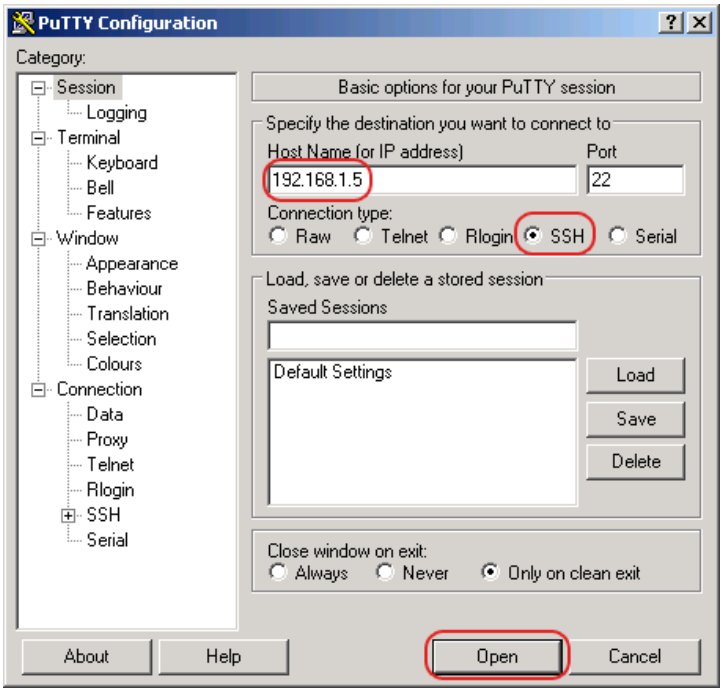


Figura 4: Schermata di immissione di PuTTY

- ☐ Nel campo *Host Name (or IP address)* si specifica l'indirizzo IP del dispositivo.
  L'indirizzo IP è costituito da 4 numeri decimali con valori da `0` a `255`. I 4 numeri decimali sono separati da punti.
- ☐ Per specificare il tipo di connessione, selezionare il pulsante di opzione *SSH* nell'elenco opzioni *Connection type*.
  Dopo aver selezionato e impostato i parametri richiesti, il dispositivo consente l'impostazione della connessione dati utilizzando SSH.

- Fare clic sul pulsante *Open* per impostare la connessione dati al dispositivo.
  Per impostare la connessione è richiesto fino a un minuto, in base al dispositivo e al momento in cui SSH è stato configurato.
  Quando si accede per la prima volta, verso la fine dell'impostazione della connessione, il programma *PuTTY* visualizza un avviso di protezione e consente di verificare l'impronta digitale della chiave.

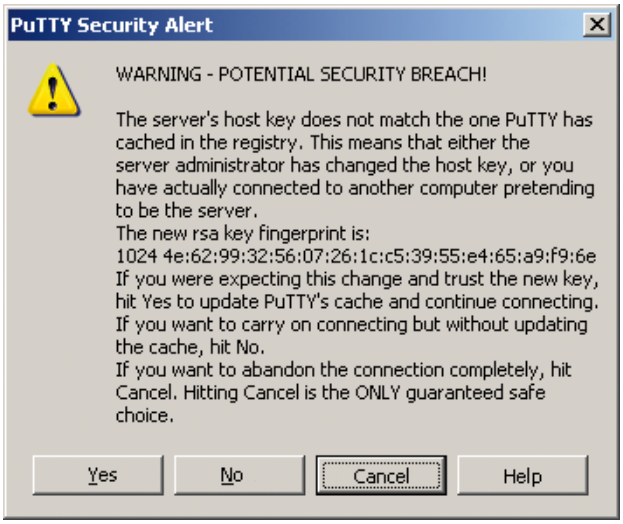


Figura 5: Richiesta di conferma per l'impronta digitale.

- Verificare l'impronta digitale.
  In questo modo si previene l'accesso di ospiti indesiderati.
- Quando l'impronta digitale corrisponde a quella della chiave dispositivo, fare clic sul pulsante *Yes*.
  Il dispositivo consente la visualizzazione delle impronte delle chiavi dispositivo con il comando `show ssh` o nella finestra di dialogo *Device Security > Management Access > Server*, scheda *SSH*.
  Sullo schermo compare la Command Line Interface con una finestra per l'inserimento del nome utente. Il dispositivo consente a un massimo di 5 utenti di avere accesso alla Command Line Interface contemporaneamente.
- Inserire il nome utente.
  Il nome utente di default è `admin`.
- Premere il tasto <Enter>.
- Inserire la password.
  La password predefinita è `private`.
- Premere il tasto <Enter>.

Nota: Questo dispositivo è un prodotto importante dal punto di vista della sicurezza. Modificare la password durante la prima procedura di avvio.

```
login as: admin
admin@192.168.1.5's password:


                        Copyright (c) 2011-2022 Schneider Electric

                                  All rights reserved

                               MCSESM-E Release 08.7.00

                              (Build date 2022-07-11 16:30)


                     System Name    :  MCSESM-646038d5e846
                     Management IP  :  192.168.1.5
                     Subnet Mask    :  255.255.255.0
                     Base MAC       :  64:60:38:01:02:03
                     USB IP         :  91.0.0.100
                     USB Mask       :  255.255.255.0
                     System Time    :  2022-07-13 19:41:31


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

Figura 6: Schermata di avvio della Command Line Interface

1.2.4 Accesso alla Command Line Interface utilizzando l'interfaccia seriale

L'interfaccia seriale è utilizzata per connettersi localmente ad una network management station esterna (terminale VT100 o PC con emulazione di terminale). L'interfaccia consente la configurazione di una connessione dati alla Command Line Interface e al monitor di sistema.

Eseguire i seguenti passaggi:

- ☐ Connettere il dispositivo a un terminale utilizzando l'interfaccia seriale. In alternativa, connettere il dispositivo a una porta COM del PC utilizzando l'emulazione di terminale sulla base di VT100 e premere qualsiasi tasto.
- ☐ In alternativa, configurare la connessione dati seriale al dispositivo con l'interfaccia seriale utilizzando il programma *PuTTY*. Premere il tasto <Enter>.

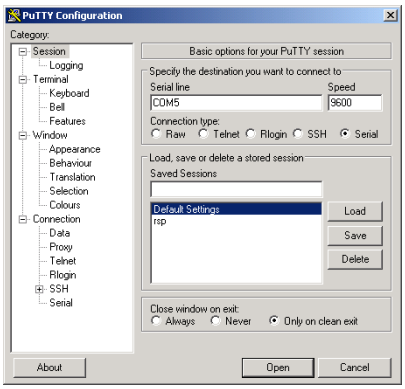


Figura 7: Connessione dati seriale con l'interfaccia seriale utilizzando il programma PuTTY

- ☐ Premere qualsiasi tasto sulla tastiera del terminale per diverse volte finché la schermata di accesso indica la modalità CLI.
- ☐ Inserire il nome utente.
  Il nome utente di default è `admin`.
- ☐ Premere il tasto <Enter>.
- ☐ Inserire la password.
  La password predefinita è `private`.
- ☐ Premere il tasto <Enter>.

Nota: Questo dispositivo è un prodotto importante dal punto di vista della sicurezza. Modificare la password durante la prima procedura di avvio.

```
                    Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                             MCSESM-E Release 08.7.00

                            (Build date 2022-07-11 16:30)


                  System Name   :  MCSESM-646038d5e846
                  Management IP :  192.168.1.5
                  Subnet Mask   :  255.255.255.0
                  Base MAC      :  64:60:38:01:02:03
                  USB IP        :  91.0.0.100
                  USB Mask      :  255.255.255.0
                  System Time   :  2022-07-13 19:41:31


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

Figura 8: Schermata di avvio della Command Line Interface

1.2.5 Gerarchia di comando basata sulla modalità

Nella Command Line Interface, i comandi sono raggruppati nelle relative modalità, in base al tipo di comando. Ogni modalità di comando supporta specifici comandi software Schneider Electric.

I comandi disponibili all'utente dipendono dal livello di privilegio (amministratore, operatore, ospite, auditor). Dipendono inoltre dalla modalità in qui si sta attualmente lavorando. Quando si passa ad una specifica modalità, i comandi della modalità sono disponibili.

I comandi della modalità User Exec sono un'eccezione. La Command Line Interface consente di eseguire questi comandi nella modalità Privileged Exec.

La seguente figura visualizza le modalità della Command Line Interface.

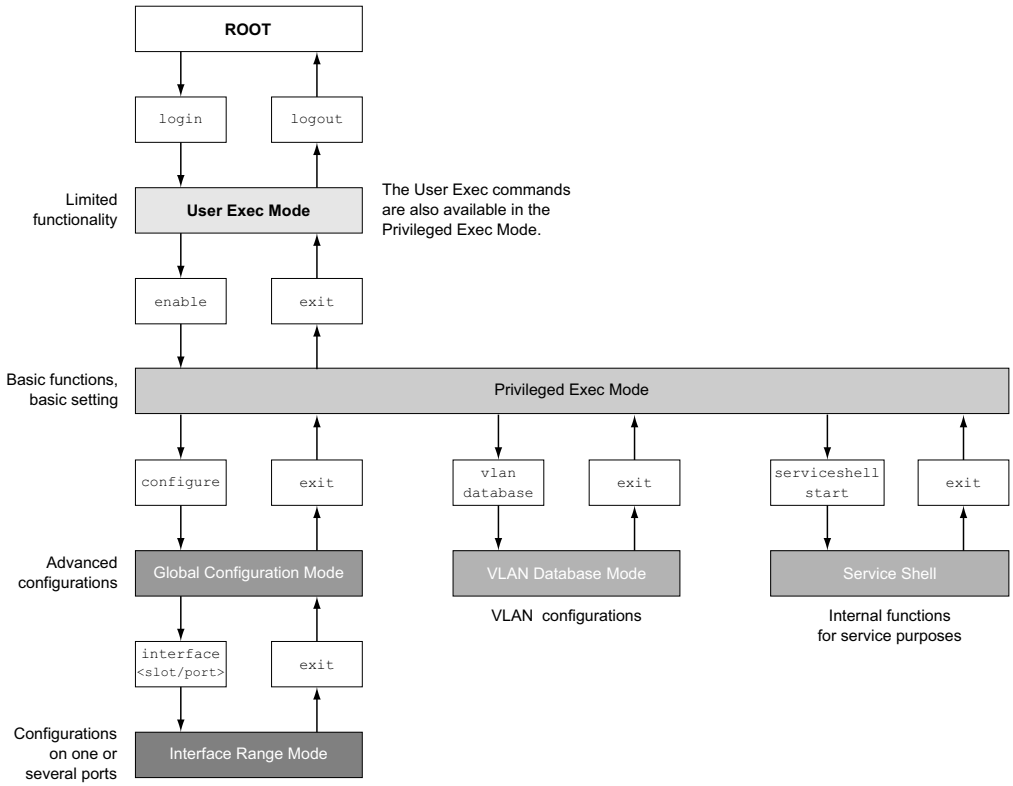


Figura 9: Struttura della Command Line Interface.

La Command Line Interface supporta, a seconda del livello dell'utente, le seguenti modalità:

- Modalità User Exec
  Quando si effettua l'accesso con la Command Line Interface si accede alla modalità User Exec. La modalità User Exec contiene una gamma limitata di comandi.
  Prompt dei comandi: `(MCSESM-E) >`
- Modalità Privileged Exec
  Per avere accesso all'intera gamma di comandi, accedere alla modalità Privileged Exec. Se si effettua un accesso come utente privilegiato, è possibile accedere alla modalità Privileged Exec. Nella modalità Privileged Exec, è possibile eseguire anche i comandi della modalità User Exec.
  Prompt dei comandi: `(MCSESM-E) #`
- Modalità VLAN
  La modalità VLAN contiene comandi correlati alla VLAN.
  Prompt dei comandi: `(MCSESM-E) (VLAN)#`
- Service Shell
  Service Shell è destinato solo a scopi di assistenza.
  Prompt dei comandi: `/mnt/fastpath #`

- Modalità Global Config
  La modalità Global Config consente di eseguire modifiche all'attuale configurazione. Questa modalità raggruppa comandi di configurazione generale.
  Prompt dei comandi: `(MCSESM-E) (config)#`
- Modalità Interface Range
  I comandi nella modalità Interface Range riguardano una specifica porta, un gruppo selezionato di porte multiple o tutte le porte di un dispositivo. I comandi modificano un valore o attivano/disattivano una funzione su una o più specifiche porte.
  - Tutte le porte fisiche nel dispositivo
    Prompt dei comandi: `(MCSESM-E) ((interface) all)#`
    Esempio: quando si passa dalla modalità Global Config alla modalità Interface Range, il prompt dei comandi cambia come di seguito esposto:
    ```
    (MCSESM-E) (config)#interface all
    (MCSESM-E) ((Interface)all)#
    ```
  - Una singola porta su una interfaccia
    Prompt dei comandi: `(MCSESM-E) (interface <slot/port>)#`
    Esempio: quando si passa dalla modalità Global Config alla modalità Interface Range, il prompt dei comandi cambia come di seguito esposto:
    ```
    (MCSESM-E) (config)#interface 2/1
    (MCSESM-E) (interface 2/1)#
    ```
  - Un intervallo di porte su una interfaccia
    Prompt dei comandi: `(MCSESM-E) (interface <interface range> )#`
    Esempio: quando si passa dalla modalità Global Config alla modalità Interface Range, il prompt dei comandi cambia come di seguito esposto:
    ```
    (MCSESM-E) (config)#interface 1/2-1/4
    (MCSESM-E) ((Interface)1/2-1/4)#
    ```
  - Una lista di singole porte
    Prompt dei comandi: `(MCSESM-E) (interface <interface list>)#`
    Esempio: quando si passa dalla modalità Global Config alla modalità Interface Range, il prompt dei comandi cambia come di seguito esposto:
    ```
    (MCSESM-E) (config)#interface 1/2,1/4,1/5
    (MCSESM-E) ((Interface)1/2,1/4,1/5)#
    ```
  - Un elenco di intervalli porte e singole porte
    Prompt dei comandi: `(MCSESM-E) (interface <complex range>)#`
    Esempio: quando si passa dalla modalità Global Config alla modalità Interface Range, il prompt dei comandi cambia come di seguito esposto:
    ```
    (MCSESM-E) (config)#interface 1/2-1/4,1/6-1/9
    (MCSESM-E) ((Interface)1/2-1/4,1/6-1/9)
    ```

La seguente tabella visualizza le modalità di comando, i prompt dei comandi (caratteri di richiesta di input) visibili nella modalità corrispondente e l'opzione con cui si esce da questa modalità.

Tabella 2: Modalità di comando

Modalità di comando	Metodo di acceso	Uscire o avviare la modalità successiva

Modalità User Exec	Livello di primo accesso. Effettuare attività base ed elencare le informazioni di sistema.	Per uscire, immettere `logout`:
		`(MCSESM-E) >logout`
		`Are you sure (Y/N) ?y`

Modalità Privileged Exec	Dalla modalità User Exec, immettere il comando `enable`:
	`(MCSESM-E) >enable`
	`(MCSESM-E) #`
		Per uscire dalla modalità Privileged Exec e ritornare alla modalità User Exec, immettere `exit`:
		`(MCSESM-E) #exit`
		`(MCSESM-E) >`

Modalità VLAN	Dalla modalità Privileged Exec, immettere il comando `vlan database`:
	`(MCSESM-E) #vlan database`
	`(MCSESM-E) (Vlan)#`
		Per chiudere la modalità VLAN e ritornare alla modalità Privileged Exec, immettere `exit` o premere Ctrl Z.
		`(MCSESM-E) (Vlan)#exit`
		`(MCSESM-E) #`

Modalità Global Config	Dalla modalità Privileged Exec, immettere il comando `configure`:
	`(MCSESM-E) #configure`
	`(MCSESM-E) (config)#`
	Dalla modalità User Exec, immettere il comando `enable`, e poi nella modalità Privileged Exec, immettere il comando `Configure`:
	`(MCSESM-E) >enable`
	`(MCSESM-E) #configure`
	`(MCSESM-E) (config)#`
		Per uscire dalla modalità Global Config e ritornare alla modalità Privileged Exec, immettere `exit`:
		`(MCSESM-E) (config)#exit`
		`(MCSESM-E) #`
		Per uscire poi dalla modalità Privileged Exec e ritornare alla modalità User Exec, immettere nuovamente `exit`:
		`(MCSESM-E) #exit`
		`(MCSESM-E) >`

Modalità Interface Range	Dalla modalità Global Config, immettere il comando `interface {all|<slot/port>|<interface range> |<interface list>|<complex range>}`.
	`(MCSESM-E) (config)#interface <slot/port>`
	`(MCSESM-E) (interface slot/port)#`
		Per uscire dalla modalità Interface Range e ritornare alla modalità Global Config, immettere `exit`. Per ritornare alla modalità Privileged Exec, premere Ctrl Z.
		`(MCSESM-E) (interface slot/port)#exit`
		`(MCSESM-E) #`

Inserendo un punto di domanda (?) dopo il prompt, la Command Line Interface visualizza un elenco dei comandi disponibili e una breve descrizione degli stessi.

```
(MCSESM-E)>
  cli              Set the CLI preferences.
  enable           Turn on privileged commands.
  help             Display help for various special keys.
  history          Show a list of previously run commands.
  logout           Exit this session.
  ping             Send ICMP echo packets to a specified IP address.
  show             Display device options and settings.
  telnet           Establish a telnet connection to a remote host.

(MCSESM-E)>
```

Figura 10: Comandi nella modalità User Exec

1.2.6 Esecuzione dei comandi

Analisi della sintassi

Quando si effettua l'accesso con la Command Line Interface si accede alla modalità User Exec. La Command Line Interface visualizza il prompt `(MCSESM-E)>` sullo schermo.

Quando si inserisce un comando e si preme il tasto <Enter>, la Command Line Interface avvia l'analisi della sintassi. La Command Line Interface ricerca l'albero dei comandi per il comando desiderato.

Quando il comando è al di fuori della gamma di Command Line Interface, un messaggio informa dell'errore rilevato.

Esempio:

Si desidera eseguire il comando `show system info`, ma si immette `info` senza `f` e si preme il tasto <Enter>.

La Command Line Interface successivamente visualizza il messaggio:

```
(MCSESM-E)>show system ino

Error: Invalid command 'ino'
```

Albero dei comandi

I comandi nella Command Line Interface sono organizzati in una struttura ad albero. I comandi e, ove applicabile, i relativi parametri, si diramano finché il comando è completamente definito e quindi eseguibile. La Command Line Interface verifica l'immissione. Quando si sono immessi correttamente il comando e i parametri, si esegue il comando con il tasto <Enter>.

Dopo avere immesso il comando e i parametri richiesti, gli altri parametri immessi sono trattati come parametri opzionali. Quando uno dei parametri è sconosciuto, la Command Line Interface visualizza un messaggio di sintassi.

L'albero dei comandi si dirama per i parametri richiesti finché i parametri richiesti hanno raggiunto l'ultimo ramo nella struttura.

Con parametri opzionali, l'albero dei comandi si ramifica finché i parametri richiesti e i parametri opzionali hanno raggiunto l'ultimo ramo nella struttura.

1.2.7 Struttura di un comando

Questa sezione descrive la sintassi, le convenzioni e la terminologia, e utilizza esempi per rappresentarli.

Formato dei comandi

La maggior parte dei comandi include parametri.

Quando manca il parametro di comando, la Command Line Interface informa del rilevamento di una sintassi del comando errata.

Questo manuale visualizza i comandi e i parametri nel font `Courier`.

Parametri

La sequenza dei parametri è rilevante per la sintassi corretta di un comando.

I parametri sono valori richiesti, valori opzionali, selezioni oppure una combinazione di questi elementi. La rappresentazione indica il tipo di parametro.

Tabella 3: Parametro e sintassi del comando

`<command>`	I comandi in parentesi angolate (`<>`) sono obbligatori.
`[command]`	I comandi in parentesi quadre (`[]`) sono opzionali.
`<parameter>`	I parametri in parentesi angolate (`<>`) sono obbligatori.
`[parameter]`	I parametri in parentesi quadre (`[]`) sono opzionali.
`...`	Puntini di sospensione (3 punti in sequenza senza spazi) dopo un elemento indicano che è possibile ripetere l'elemento.
`[Choice1 | Choice2]`	Una linea verticale in parentesi indica un'opzione di selezione. Selezionare un valore. Elementi separati da una linea verticale e compresi in parentesi quadre indicano una selezione opzionale (opzione1 oppure opzione2 o nessuna selezione).
`{list}`	Parentesi graffe (`{}`) indicano che un parametro va selezionato da un elenco di opzioni.
`{Choice1 | Choice2}`	Elementi separati da una linea verticale e compresi in parentesi graffe (`{}`) indicano un'opzione di selezione obbligatoria (opzione1 oppure opzione2).
`[param1 {Choice1 | Choice2}]`	Visualizza un parametro opzionale che contiene una selezione obbligatoria.
`<a.b.c.d>`	Le lettere minuscole sono caratteri jolly. Immettere i parametri con l'annotazione a.b.c.d con punti decimali (ad esempio indirizzi IP)
`<cr>`	Premere il tasto <Enter> per creare un'interruzione di riga (ritorno a capo).

Il seguente elenco visualizza i valori di parametro possibili all'interno della Command Line Interface:

Tabella 4: Valori di parametro nella Command Line Interface

Valore	Descrizione
Indirizzo IP	Questo parametro rappresenta un indirizzo IPv4 valido. L'indirizzo è costituito da 4 numeri decimali con valori da 0 a 255. I 4 numeri decimali sono separati da un punto decimale. L'indirizzo IP `0.0.0.0` è una voce valida.
Indirizzo MAC	Questo parametro rappresenta un indirizzo MAC valido. L'indirizzo è costituito da 6 numeri esadecimali con valori da 00 a FF. I numeri sono separati dai due punti, ad esempio: `00:F6:29:B2:81:40`.
Stringa	Testo definito dall'utente con una lunghezza nell'intervallo specificato, ad esempio un massimo di 32 caratteri.
Stringa di caratteri	Utilizzare le virgolette per indicare una stringa di caratteri, ad esempio `"System name with space character"`.
Numero	Integer intero nell'intervallo specificato, ad esempio `0..999999`.
Data	Data nel formato `YYYY-MM-DD`.
Ora	Ora nel formato `HH:MM:SS`.

Indirizzi di rete

Gli indirizzi di rete sono un requisito per stabilire una connessione dati ad una workstation remota, un server o un'altra rete. Distinguere tra gli indirizzi IP e gli indirizzi MAC.

L'indirizzo IP è un indirizzo allocato dall'amministratore di rete. L'indirizzo IP è univoco in un'area di rete.

Gli indirizzi MAC sono assegnati dal produttore hardware. Gli indirizzi MAC sono univoci in tutto il mondo.

La seguente tabella visualizza la rappresentazione e l'intervallo di tipi di indirizzo:

Tabella 5: Formato e intervallo di indirizzi di rete

Tipo di indirizzo	Formato	Intervallo	Esempio
Indirizzo IP	nnn.nnn.nnn.nnn	nnn: 0 - 255 (decimale)	192.168.11.110
Indirizzo MAC	mm:mm:mm:mm:mm:mm	mm: 00 - ff (coppie di numeri esadecimali)	A7:C9:89:DD:A9:B3

Stringhe

Una stringa è indicata con virgolette. Ad esempio, `"System name with space character"`. Gli spazi non sono stringhe definite dall'utente valide. Si immette uno spazio in un parametro tra virgolette.

Esempio:

```
*(MCSESM-E)#cli prompt Device name
Error: Invalid command 'name'

*(MCSESM-E)#cli prompt 'Device name'
```

```
*(Device name)#
```

1.2.8 Esempi di comandi

Esempio 1: cancella arp-tabella-switch

Comando per cancellare la tabella ARP dell'agente di gestione (cache).

`clear arp-table-switch` è il nome del comando. Il comando è eseguibile senza altri parametri, premendo il tasto <Enter>.

Esempio 2: timeout server radius

Comando per configurare il valore del timeout del server RADIUS.

```
(MCSESM-E) (config)#radius server timeout
 <1..30>              Timeout in seconds (default: 5).
```

`radius server timeout` è il nome del comando.

Il parametro è richiesto. L'intervallo di valori è `1..30`.

Esempio 3: radius server auth modify <1..8>

Comando per impostare i paramenti del server di autenticazione RADIUS 1.

```
(MCSESM-E) (config)#radius server auth modify 1
 [name]               RADIUS authentication server name.
 [port]               RADIUS authentication server port.
                      (default: 1812).
 [msgauth]            Enable or disable the message authenticator
                      attribute for this server.
 [primary]            Configure the primary RADIUS server.
 [status]             Enable or disable a RADIUS authentication
                      server entry.
 [secret]             Configure the shared secret for the RADIUS
                      authentication server.
 [encrypted]          Configure the encrypted shared secret.
  <cr>                Press Enter to execute the command.
```

`radius server auth modify` è il nome del comando.

È richiesto il parametro `<1..8>` (indice server RADIUS). L'intervallo di valori è `1..8` (integer).

I parametri `[name]`, `[port]`, `[msgauth]`, `[primary]`, `[status]`, `[secret]` e `[encrypted]` sono opzionali.

1.2.9 Richiesta di input

Modalità di comando

Con il prompt di immissione, la Command Line Interface visualizza in quale delle tre modalità ci si trova:

- `(MCSESM-E) >`
  Modalità User Exec
- `(MCSESM-E) #`
  Modalità Privileged Exec
- `(MCSESM-E) (config)#`
  Modalità Global Config
- `(MCSESM-E) (Vlan)#`
  VLAN Database mode
- `(MCSESM-E) ((Interface)all)#`
  Modalità Interface Range / Tutte le porte del dispositivo
- `(MCSESM-E) ((Interface)2/1)#`
  Modalità Interface Range / Una singola porta su una interfaccia
- `(MCSESM-E) ((Interface)1/2-1/4)#`
  Modalità Interface Range / Un intervallo di porte su una interfaccia
- `(MCSESM-E) ((Interface)1/2,1/4,1/5)#`
  Modalità Interface Range / Un elenco di singole porte
- `(MCSESM-E) ((Interface)1/1-1/2,1/4-1/6)#`
  Modalità Interface Range / Un elenco di intervalli porte e singole porte

Asterisco, segno del cancelletto e punto esclamativo

- Asterisco `*`
  Un asterisco `*` nella prima o nella seconda posizione della richiesta di input indica che le impostazioni nella memoria volatile e le impostazioni nella memoria non volatile sono differenti. Nella configurazione, il dispositivo ha rilevato modifiche che non sono state salvate.
  `*(MCSESM-E)>`
- Segno del cancelletto `#`
  Un segno del cancelletto `#` all'inizio della richiesta di input indica che i parametri di boot e i parametri durante la fase di boot sono differenti.
  `*#(MCSESM-E)>`
- Punto esclamativo `!`
  Un punto esclamativo `!` All'inizio della richiesta di input indica: la password per l'account utente `user` o `admin` corrisponde all'impostazione di default.
  `!(MCSESM-E)>`

Caratteri jolly

Il dispositivo consente di modificare il prompt della linea di comando.

La Command Line Interface supporta i seguenti caratteri jolly:

Tabella 6: Utilizzo dei caratteri jolly all'interno del prompt di immissione della Command Line Interface

Carattere jolly	Descrizione
`%d`	Data del sistema
`%t`	Ora del sistema

Tabella 6: Utilizzo dei caratteri jolly all'interno del prompt di immissione della Command Line Interface

Carattere jolly	Descrizione
`%i`	Indirizzo IP del dispositivo
`%m`	Indirizzo MAC del dispositivo
`%p`	Nome prodotto del dispositivo

```
!(MCSESM-E)>enable

!(MCSESM-E)#cli prompt %i

!192.168.1.5#cli prompt (MCSESM-E)%d

!*(MCSESM-E)2022-07-13#cli prompt (MCSESM-E)%d%t

!*(MCSESM-E)2022-07-13 19:41:31#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

1.2.10 Combinazioni di tasti

Le seguenti combinazioni di tasti facilitano il lavoro con la Command Line Interface:

Tabella 7: Combinazioni di tasti nella Command Line Interface

Combinazione di tasti	Descrizione
<CTRL> + <H>, <Back-space>	Per cancellare il carattere precedente
<CTRL> + <A>	Per spostarsi all'inizio della riga
<CTRL> + <E>	Per spostarsi alla fine della riga
<CTRL> + <F>	Per spostarsi in avanti idi un carattere
<CTRL> + <B>	Per spostarsi indietro di un carattere
<CTRL> + <D>	Per cancellare l'attuale carattere
<CTRL> + <U>, <X>	Per cancellare fino all'inizio della riga
<CTRL> + <K>	Per cancellare fino alla fine della riga
<CTRL> + <W>	Per cancellare la parola precedente
<CTRL> + <P>	Per raggiungere la riga precedente nel buffer storico
<CTRL> + <R>	Per riscrivere o incollare la riga
<CTRL> + <N>	Per raggiungere la riga successiva nel buffer storico
<CTRL> + <Z>	Per ritornare al prompt dei comandi root
<CTRL> + <G>	Interrompe la sessione tcpdump in corso
<Scheda>, <<SPACE>>	Completamento riga di comando
`Exit`	Per raggiungere il prompt dei comandi più bassi successivi
<?>	Scelte elenco

Il comando Guida visualizza le possibili combinazioni di tasti nella Command Line Interface sulla schermata:

```
(MCSESM-E) #help

HELP:
Special keys:

  Ctrl-H, BkSp delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
  Ctrl-D  .... delete current character
  Ctrl-U, X .. delete to beginning of line
  Ctrl-K  .... delete to end of line
  Ctrl-W  .... delete previous word
  Ctrl-P  .... go to previous line in history buffer
  Ctrl-R  .... rewrites or pastes the line
  Ctrl-N  .... go to next line in history buffer
  Ctrl-Z  .... return to root command prompt
  Ctrl-G  .... aborts running tcpdump session
  Tab, <SPACE> command-line completion
  Exit    .... go to next lower command prompt
  ?       .... list choices

(MCSESM-E) #
```

Figura 11: Elenco delle combinazioni di tasti con il comando Guida

1.2.11 Elementi di immissione dati

Completamento comando

Per semplificare la digitazione dei comandi, la Command Line Interface consente l'utilizzo del completamento comandi (scheda completamento). Pertanto, è possibile abbreviare le parole chiave.

- Digitare le prime lettere di una parola chiave. Quando con i caratteri immessi si identifica una parola chiave, la Command Line Interface completa la parola chiave dopo aver premuto il tasto tab o la barra spaziatrice. Quando è disponibile più di un'opzione per il completamento, immettere la lettera o le lettere per identificare in modo univoco la parola chiave. Premere nuovamente il tasto tab o barra spaziatrice. Dopo di che, il sistema completa il comando o il parametro.
- Quando si digita una voce non univoca e si preme <Tab> o <Space> due volte, la Command Line Interface fornisce un elenco di opzioni.
- Con una voce non univoca e premendo <Tab> o <Space>, la Command Line Interface completa il comando fino alla fine dell'univocità. Se esistono diversi comandi e si preme nuovamente <Tab> o <Space>, la Command Line Interface fornisce un elenco di opzioni.
  Esempio:
  ```
  (MCSESM-E) (Config)#lo
  (MCSESM-E) (Config)#log
  logging logout
  ```
  Immettendo `lo` e <Tab> o <Space>, la Command Line Interface completa il comando fino alla fine dell'univocità, cioè fino a `log`.
  Premendo nuovamente <Tab> o <Space>, la Command Line Interface fornisce un elenco di opzioni (`logging logout`).

Possibili comandi/parametri

Per visualizzare un elenco dei comandi oppure dei possibili parametri, immettere `help` o `?`, ad esempio `(MCSESM-E) >show ?`

Immettendo il comando visualizzato, si ottiene un elenco dei parametri disponibili per il comando `show`.

Quando si immette il comando senza spazio prima del punto di domanda, il dispositivo visualizza il testo della guida per il comando stesso:

```
!*#(MCSESM-E)(Config)#show?

   show          Display device options and settings.
```

1.2.12 Casi di utilizzo

Salvataggio della configurazione

Salvare la configurazione, per assicurarsi che le impostazioni della password e le altre modifiche di configurazione vengano conservate dopo il reset del dispositivo o in caso di interruzione dell'alimentazione di tensione. A tale scopo, eseguire i seguenti passaggi:

- ☐ Immettere `enable` per passare alla modalità Privileged Exec.
- ☐ Inserire il seguente comando:

  `save [profile]`
- ☐ Eseguire il comando premendo il tasto <Enter>.

Sintassi del comando “radius server auth add”

Utilizzare questo comando per aggiungere un server di autenticazione RADIUS.

- Modalità: `Global Config`
- Livello di privilegio: Administrator
- Formato: `radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - `[name]`: nome del server di autenticazione RADIUS.
  - `[port]`: porta del server di autenticazione RADIUS (valore predefinito: `1813`).

Parametro	Significato	Possibili valori
`<1..8>`	Indice del server RADIUS.	`1..8`
`<a.b.c.d>`	Indirizzo IP del server di accounting RADIUS.	Indirizzo IP
`<string>`	Immettere un testo definito dall'utente di max. 32 caratteri.	
`<1..65535>`	Immettere un numero porta compreso tra 1 e 65535.	`1..65535`

Modalità e livello di privilegio:

- Il prerequisito per l'esecuzione del comando: si è nella modalità Global Config. Vedi “Gerarchia di comando basata sulla modalità” a pagina 25.
- Il prerequisito per l'esecuzione del comando: si ha il ruolo di accesso Administrator.

Sintassi di comandi e parametri: Vedi “Struttura di un comando” a pagina 29.

Esempi di comandi eseguibili:

- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`

1.2.13 Service Shell

Service Shell è destinato solo a scopi di assistenza.

Service Shell consente agli utenti l'accesso a funzioni interne del dispositivo. Quando si necessita assistenza per il dispositivo, il personale di assistenza utilizza Service Shell per monitorare, ad esempio, le condizioni interne, lo switch o i registri CPU.

AVVISO
RISCHIO CHE IL DISPOSITIVO NON FUNZIONI Non eseguire funzioni interne come l'eliminazione della memoria non volatile (*NVM*) senza istruzioni tecniche di assistenza. **Il mancato rispetto di queste istruzioni potrebbe portare a un dispositivo non funzionante.**

Avviare Service Shell

Il prerequisito è che la modalità User Exec sia attiva. `(MCSESM-E) >`

Eseguire i seguenti passaggi:

- ☐ Inserire `enable` e premere il tasto <Enter>.
  Per ridurre lo sforzo durante la digitazione:
  - Inserire `e` e premere il tasto <Tab>.
- ☐ Inserire `serviceshell start` e premere il tasto <Enter>.
  Per ridurre lo sforzo durante la digitazione:
  - Inserire `ser` e premere il tasto <Tab>.
  - Inserire `s` e premere il tasto <Tab>.

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell start
 WARNING! The service shell offers advanced diagnostics and functions.
 Proceed only when instructed by a service technician.

 You can return to the previous mode using the 'exit' command.

 BusyBox v1.31.0 (2022-07-13 19:41:31 UTC) built-in shell (ash)
 Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

Lavorare con la Service Shell

Quando il Service Shell è attivo, il timeout dell'interfaccia a riga di comando non è attivo. Per contribuire a prevenire le incoerenze di configurazione, interrompere la Service Shell prima che un qualsiasi altro utente inizi a trasmettere una nuova configurazione al dispositivo.

Visualizzare i comandi Service Shell

Il prerequisito è che la Service Shell sia già stata avviata.

Eseguire i seguenti passaggi:
☐ Inserire `help` e premere il tasto <Enter>.

```
/mnt/fastpath # help
Built-in commands:
------------------
        . : [ [[ alias bg break cd chdir command continue echo eval exec
        exit export false fg getopts hash help history jobs kill let
        local pwd read readonly return set shift source test times trap
        true type ulimit umask unalias unset wait
/mnt/fastpath #
```

Interrompere la Service Shell

Eseguire i seguenti passaggi:
☐ Inserire `exit` e premere il tasto <Enter>.

Disattivare la Service Shell in modo permanente nel dispositivo

Quando si disattiva il Service Shell, è ancora possibile configurare il dispositivo. Tuttavia si limitano le possibilità del personale dell'assistenza di eseguire la diagnostica di sistema. Il tecnico dell'assistenza non potrà più accedere alle funzioni interne del dispositivo.

La disattivazione è irreversibile. Il Service Shell resta disattivato permanentemente. **Per riattivare il Service Shell, il dispositivo richiede lo smontaggio da parte del produttore.**

I prerequisiti sono:
- La Service Shell non è avviata.
- Modalità User Exec attiva. `(MCSESM-E) >`

Eseguire i seguenti passaggi:
☐ Inserire `enable` e premere il tasto <Enter>.
Per ridurre lo sforzo durante la digitazione:
– Inserire `e` e premere il tasto <Tab>.

- Inserire `serviceshell deactivate` e premere il tasto <Enter>.
  Per ridurre lo sforzo durante la digitazione:
  - Inserire `ser` e premere il tasto <Tab>.
  - Inserire `dea` e premere il tasto <Tab>.
- **Questo passaggio è irreversibile!**
  Premere il tasto <Y>.

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell deactivate
Notice: If you continue, then the Service Shell is permanently deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N) ?
```

1.3 Monitor di sistema

Il monitor di sistema consente l'impostazione di parametri di funzionamento base prima di avviare il sistema operativo.

1.3.1 Gamma funzionale

Nel monitor di sistema, si effettuano le seguenti operazioni, ad esempio:
- Gestione del sistema operativo e verifica dell'immagine software
- Aggiornamento del sistema operativo
- Avvio del sistema operativo
- Cancellazione dei profili di configurazione, reset del dispositivo allo stato di fornitura
- Verifica dell'informazione sul codice di avvio

1.3.2 Avvio del monitor di sistema

Stabilire una connessione seriale al dispositivo utilizzando l'interfaccia USB-C. Durante l'inizializzazione, l'interfaccia seriale del dispositivo non è disponibile. Per questo motivo, l'avvio del System Monitor funziona in modo diverso rispetto agli altri dispositivi Schneider Electric. Per avviare il System Monitor, impostare il dispositivo in Modalità recupero.

Impostare il dispositivo in Modalità recupero

Accessori richiesti:
- Memoria esterna (consigliata: ACA22-USB-C)
- Adattatore da USB-C a USB-A (soltanto se si utilizza una memoria esterna differente rispetto a quella consigliata)
- Cavo USB per connettersi alla porta USB-C del dispositivo con il computer
- Computer con emulazione di terminale VT100 (ad esempio PuTTY) oppure un terminale seriale

Eseguire i seguenti passaggi:
- ☐ Collegare la memoria esterna al computer.
- ☐ Nella directory principale della memoria esterna, creare un file vuoto rinominato `recovery.txt`.
- ☐ Collegare la memoria esterna al dispositivo.
- ☐ Riavviare il dispositivo.
- ☐ Osservare i LED durante il riavvio del dispositivo. Quando il LED *Status* lampeggia alternando il colore rosso e verde, il dispositivo si è riavviato correttamente nella Modalità recupero.

Nota: Per la descrizione degli elementi del display, consultare la sezione "Installazione" nel manuale utente.

Accesso al System Monitor

Eseguire i seguenti passaggi:
- ☐ Rimuovere la memoria esterna dal dispositivo.
- ☐ Collegare il computer al dispositivo utilizzando il cavo USB.
- ☐ Aprire l'emulazione di terminale VT100 sul computer per visualizzare il System Monitor.
- ☐ Selezionare la porta COM pertinente.

Quando il computer e il dispositivo sono connessi correttamente, apparirà una schermata di colore nero.

Eseguire i seguenti passaggi:

- ☐ Premere il tasto <Invio> per visualizzare il System Monitor.
  Apparirà la seguente schermata sul computer:

```
System Monitor 1
(Selected OS: ...-8.7 (2022-07-11 16:30))

1  Manage operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)




sysMon1>
```

Figura 12: Schermata System Monitor

- ☐ Per selezionare una voce del menu, inserire il numero corrispondente.
- ☐ Per uscire da un sottomenu e ritornare al menu principale, premere il tasto <ESC>.

Nota: Per avviare il dispositivo normalmente la volta successiva, aggiungere solo la memoria esterna senza il file `recovery.txt`.

2 Definizione dei parametri IP

Quando si installa il dispositivo per la prima volta, inserire i parametri IP.

Il dispositivo fornisce le seguenti opzioni per l'inserimento dei parametri IP durante la prima installazione:

- Immissione tramite l'interfaccia a riga di comando.
  Quando si preconfigura il proprio dispositivo esternamente al suo ambiente operativo, o si ripristina l'accesso di rete (“In-Band”) al dispositivo, scegliere questo metodo “Out-of-Band”.
- Immissione tramite il protocollo Ethernet Switch Configurator.
  Quando si dispone di un dispositivo di rete precedentemente installato o di un altro collegamento Ethernet tra il proprio PC e il dispositivo, si sceglie questo metodo “In-Band”.
- Configurazione tramite la memoria esterna.
  Quando si sostituisce un dispositivo con un dispositivo dello stesso tipo ed è già stata salvata la configurazione nella memoria esterna si sceglie questo metodo.
- Tramite BOOTP.
  Per configurare il dispositivo installato tramite BOOTP si sceglie questo metodo “In-Band”. Tale opzione presuppone un server BOOTP. Il server BOOTP assegna i dati di configurazione al dispositivo tramite il suo indirizzo MAC. La modalità DHCP è la modalità di default per il riferimento dei dati di configurazione.
- Configurazione tramite DHCP.
  Per configurare il dispositivo installato tramite DHCP si sceglie questo metodo “In-Band”. Tale opzione presuppone un server DHCP. Il server DHCP assegna i dati di configurazione al dispositivo tramite il suo indirizzo MAC o nome di sistema.
- Configurazione eseguita tramite l'interfaccia grafica utente.
  Quando il dispositivo dispone già di un indirizzo IP ed è raggiungibile tramite la rete, l'interfaccia grafica utente fornisce un'altra opzione di configurazione dei parametri IP.

2.1 Fondamenti dei parametri IP

2.1.1 IPv4

Indirizzo IP

Gli indirizzi IP sono costituiti da 4 byte. Scrivere questi 4 byte in valori decimali, separati da un punto decimale.

L'RFC 1340, scritto nel 1992, definisce 5 classi degli indirizzi IP.

Tabella 8: Classi degli indirizzi IP

Classe	Indirizzo di rete	Indirizzo host	Intervallo indirizzi
A	1 Byte	3 Bytes	Da 0.0.0.0 a 127.255.255.255
B	2 Bytes	2 Bytes	Da 128.0.0.0 a 191.255.255.255
C	3 Bytes	1 Byte	Da 192.0.0.0 a 223.255.255.255
D			Da 224.0.0.0 a 239.255.255.255
E			Da 240.0.0.0 a 255.255.255.255

Il primo byte di un indirizzo IP è l'indirizzo della rete. L'organismo mondiale che sovrintende all'assegnazione degli indirizzi di rete è la IANA ("Internet Assigned Numbers Authority"). In caso di necessità di un blocco dell'indirizzo IP, rivolgersi al proprio Internet Service Provider (ISP). L'ISP contatta l'organizzazione locale di livello superiore per prenotare un blocco dell'indirizzo IP:

- APNIC (Asia Pacific Network Information Center)
  Regione Asia/Pacifico
- ARIN (American Registry for Internet Numbers)
  Americhe e Africa subsahariana
- LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  America latina e alcune isole caraibiche
- RIPE NCC (Réseaux IP Européens)
  Europa e regioni limitrofe

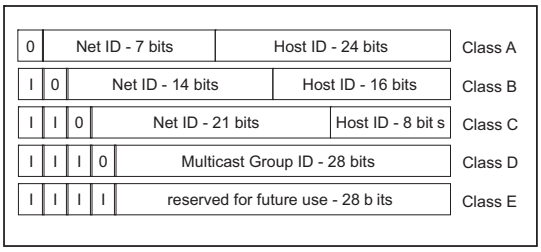


Figura 13: Rappresentazione in bit degli indirizzi IP

Quando il primo bit di un indirizzo IP è uno zero, appartiene alla classe A, ad esempio, il primo ottetto è inferiore a 128.

Quando il primo bit di un indirizzo IP è un uno e il secondo bit è uno zero, appartiene alla classe B, ad esempio, il primo ottetto è tra 128 e 191.

Quando i primi 2 bit di un indirizzo IP sono un uno, appartiene alla classe C, ad esempio, il primo ottetto è superiore a 191.

L'assegnazione dell'indirizzo host (host ID) è responsabilità dell'operatore di rete. Solo l'operatore di rete è responsabile per l'unicità degli indirizzi IP assegnati.

Subnet mask

I router e i Gateways suddividono in sottoreti le reti di grandi dimensioni. La subnet mask assegna gli indirizzi IP dei singoli dispositivi a una sottorete specificata.

Si esegue la divisione della sottorete utilizzando la subnet mask in modo analogo alla suddivisione degli indirizzi di rete (net id) in classi da A a C.

Impostare i bit dell'indirizzo host (host id) che rappresentano la maschera su uno. Impostare i bit restanti dell'indirizzo host su zero (vedere i seguenti esempi).

Esempio di una maschera di sottorete:

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000

Subnetwork mask bits
Class B

Esempio di applicazione della maschera di sottorete agli indirizzi IP per l'assegnazione della sottorete:

Decimal notation
129.218.65.17
└ 128 < 129 191 › Class B

Binary notation
10000001.11011010.01000001.00010001
Subnetwork 1
Network address

Decimal notation
129.218.129.17
└ 128 < 129 191 › Class B

Binary notation
10000001.11011010.10000001.00010001
Subnetwork 2
Network address

Esempio di utilizzo della subnet mask

In una rete di grandi dimensioni è possibile che i Gateways e i router separino l'agente di gestione dalla sua network management station. Come funziona in questo caso l'assegnazione di indirizzi?

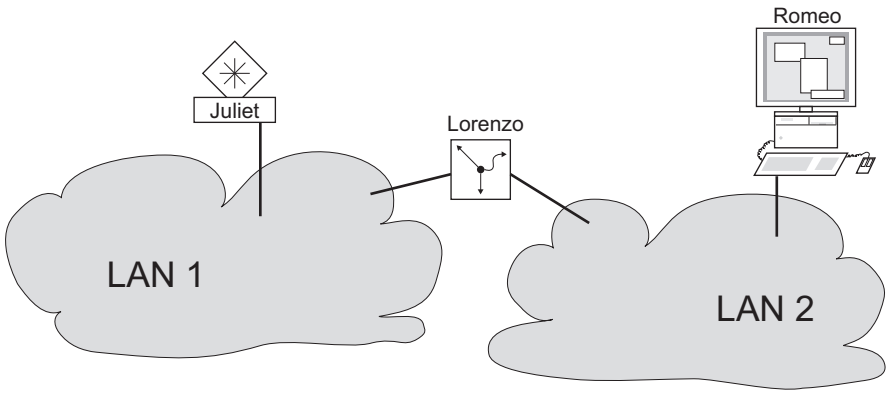


Figura 14: L'agente di gestione è separato dalla sua network management station da un router.

La network management station “Romeo” desidera inviare dati all'agente di gestione “Giulietta”. Romeo conosce l'indirizzo IP di Giulietta e sa anche che il router “Lorenzo” conosce la strada per raggiungere Giulietta.

Romeo infila quindi il suo messaggio in una busta, indicando come destinazione l'indirizzo IP di Giulietta e come indirizzo sorgente il proprio indirizzo IP.

Romeo infila poi questa busta in un'altra busta, con l'indirizzo MAC di Lorenzo come destinazione e il proprio indirizzo MAC come indirizzo sorgente. Questo processo è paragonabile al passaggio dal Layer 3 al Layer 2 del modello di riferimento di base ISO/OSI.

A questo punto, Romeo infila l'intero pacchetto dati nella cassetta delle lettere, il che è paragonabile al passaggio dal Layer 2 al Layer 1, vale a dire all'invio del pacchetto dati tramite Ethernet.

Lorenzo riceve la lettera, rimuove la busta esterna e, dalla busta interna, rileva che la lettera è destinata a Giulietta. Posiziona la busta interna in una nuova busta esterna e cerca nel suo elenco indirizzi (la tabella ARP) l'indirizzo MAC di Giulietta; scrive l'indirizzo MAC di Giulietta sulla busta esterna come indirizzo di destinazione e il proprio indirizzo MAC come indirizzo sorgente. Poi ripone l'intero pacchetto dati nella cassetta delle lettere.

Giulietta riceve la lettera e apre la busta eterna. Le rimane la busta interna con l'indirizzo IP di Romeo. L'apertura della busta interna e la lettura del suo contenuto corrispondono al trasferimento del messaggio a livelli di protocollo superiori del modello stratificato ISO/OSI.

Giulietta vorrebbe inviare una risposta a Romeo. Infila la risposta in una busta, indicando come indirizzo di destinazione l'indirizzo IP di Romeo e come indirizzo sorgente il proprio indirizzo IP. A chi deve inviare la risposta? Dato che non ha ricevuto l'indirizzo MAC di Romeo. È andato perso perché Lorenzo ha sostituito la busta esterna.

In MIB, Giulietta trova Lorenzo nell'elenco sotto la variabile `NetGatewayIPAddr` come mezzo di comunicazione con Romeo. Di conseguenza, infila la busta con gli indirizzi IP in un'altra busta con l'indirizzo MAC di destinazione di Lorenzo.

La lettera ritorna a Romeo attraverso Lorenzo, ripercorrendo lo stesso itinerario della lettera che Romeo ha inviato a Giulietta.

Classless Inter-Domain Routing

La classe C con un massimo di 254 indirizzi era troppo piccola, e la classe B con un massimo di 65534 indirizzi era troppo grande per la maggior parte degli utenti. Ne consegue un utilizzo inefficace degli indirizzi disponibili di classe B.

La classe D contiene indirizzi Multicast riservati. La classe E è per fini sperimentali. Un Gateway non partecipante ignora i datagrammi sperimentali con questi indirizzi di destinazione.

Dal 1993, l'RFC 1519 si è avvalso del Classless Inter-Domain Routing (CIDR) per fornire una soluzione. Il CIDR valica queste barriere di classe e supporta intervalli di indirizzi IP senza classi.

Con il CIDR si immette il numero di bit che designano l'intervallo di indirizzi IP. L'intervallo di indirizzi IP è così rappresentato sotto forma binaria e i bit della maschera sono conteggiati per designare la subnet mask. I bit della maschera sono uguali al numero di bit utilizzati per la sottorete in un dato intervallo di indirizzi IP.

Esempio:

IP address, decimal	Network mask, decimal	IP address, binary
192.168.112.1	255.255.255.128	11000000 10101000 01110000 00000001
192.168.112.127		11000000 10101000 01110000 01111111

25 mask bits

CIDR notation: 192.168.112.0/25

Mask bits

Il termine “supernetting” si riferisce alla combinazione di un numero di intervalli di indirizzi di classe C. Il supernetting consente di suddividere in maniera più precisa gli intervalli di indirizzi di classe B.

2.1.2 IPv6

Fondamenti dei parametri IP

L'Internet Protocol version 6 (IPv6) è la nuova versione dell'Internet Protocol version 4 (IPv4). La necessità di implementare l'IPv6 si deve al fatto che gli indirizzi IPv4 non sono sufficienti per l'attuale crescita del contesto Internet. Il protocollo IPv6 è descritto nell'RFC 8200.

Alcune differenze tra IPv6 e IPv4 sono:
- Rappresentazione e lunghezza dell'indirizzo
- Assenza del tipo di indirizzo broadcast
- Struttura semplificata dell'header
- Frammentazione svolta solo dall'host sorgente
- Aggiunta di capacità per l'identificazione del flusso di pacchetti nella rete

Sia il protocollo IPv4 sia il IPv6 possono operare contemporaneamente nel dispositivo. Ciò è possibile utilizzando la tecnica Dual IP Layer, detta anche Dual Stack.

Nota: Per far in modo che il dispositivo operi solamente utilizzando il protocollo IPv4, disattivare la funzione IPv6 nel dispositivo.

Nel dispositivo, il protocollo IPv6 ha le seguenti restrizioni:
- È possibile specificare un numero massimo di 8 indirizzi unicast IPv6.
  - 4 indirizzi IPv6 utilizzando la configurazione manuale
  - 2 indirizzi IPv6 quando è selezionato il pulsante di opzione *Auto*
  - 1 indirizzo IPv6 utilizzando il server DHCPv6
  - 1 indirizzo link-local
- La funzione IPv6 può essere abilitata solo sull'interfaccia di gestione. Il numero totale di indirizzi IPv6 configurabili può essere utilizzato contemporaneamente sull'interfaccia.
- Gli indirizzi IPv6 possono essere utilizzati per impostare l'indirizzo IP di gestione del dispositivo. Altri servizi in cui possono essere utilizzati gli indirizzi IPv6 includono, ad esempio, SNTP, SYSLOG, DNS e LDAP.

Rappresentazione dell'indirizzo

Gli indirizzi IPv6 sono costituiti da 128 bit. Sono rappresentati in 8 gruppi da 4 cifre esadecimali, dove ciascun gruppo rappresenta 16 bit, di seguito detti hextet. Gli hextet sono separati da due punti (:). Gli indirizzi IPv6 non fanno distinzione tra minuscole e maiuscole e possono essere scritti con entrambi i tipi di carattere.

Secondo RFC 4291, il formato preferito per un indirizzo IPv6 è x:x:x:x:x:x:x:x. Ogni "x" consiste di 4 valori esadecimali e rappresenta un hextet. Un esempio di un formato preferito di un indirizzo IPv6 è indicato nella tabella seguente.

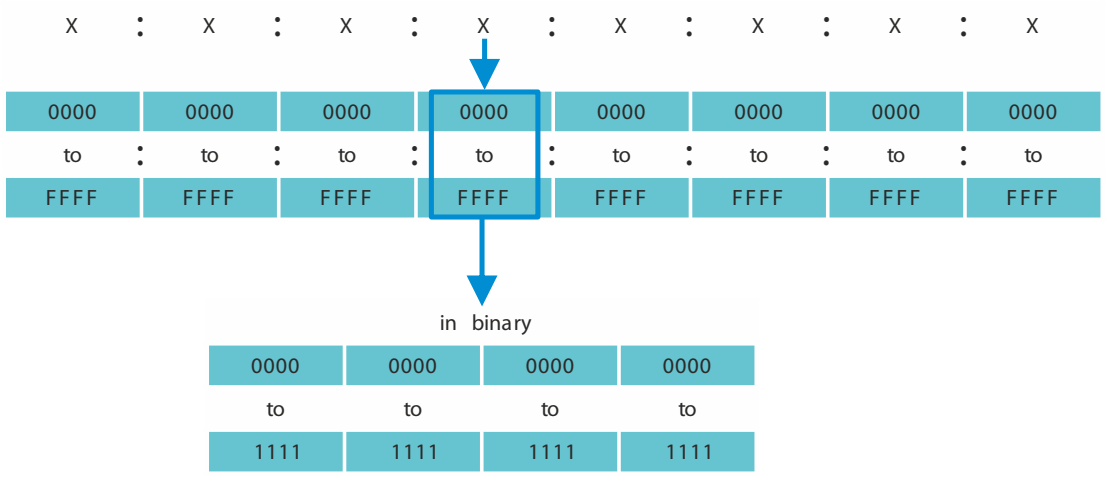


Figura 15: Rappresentazione dell'indirizzo IPv6

Come indica la figura sopra, solitamente un indirizzo IPv6 contiene molti zeri. Per abbreviare gli indirizzi IPv6 che contengono 0 bit è necessario seguire 2 regole di scrittura:

- La prima regola è di eliminare gli zeri iniziali in ogni hextet. Questa regola si applica solo agli zeri iniziali e non finali di un hextet. Se si eliminano anche gli zeri finali, l'indirizzo risultante è ambiguo.
- La seconda regola utilizza una sintassi speciale per comprimere gli zeri. È possibile utilizzare 2 due punti consecutivi "::" per sostituire una stringa di hextet adiacenti che contengono solo zeri. Il simbolo "::" può essere utilizzato solo una volta in un indirizzo. Se il simbolo "::" è utilizzato più di una volta in una rappresentazione di indirizzo, da quella annotazione può derivare più di un indirizzo.

Se si applicano le due regole, il risultato è generalmente detto formato compresso.

Nella tabella seguente si trovano 2 esempi di come applicare queste regole:

Tabella 9: Compressione dell'indirizzo IPv6

Preferito	CC03:0000:0000:0000:0001:AB30:0400:FF02
Nessuno zero iniziale	CC03: 0: 0: 0: 1:AB30: 400:FF02
Compresso	CC03::1:AB30:400:FF02

Preferito	2008:00B7:0000:DEF0:DDDD:0000:E604:0001
Nessuno zero iniziale	2008: B7: 0:DEF0:DDDD: 0:E604: 1
Compresso	2008:B7::DEF0:DDDD:0:E604:1

Lunghezza del prefisso

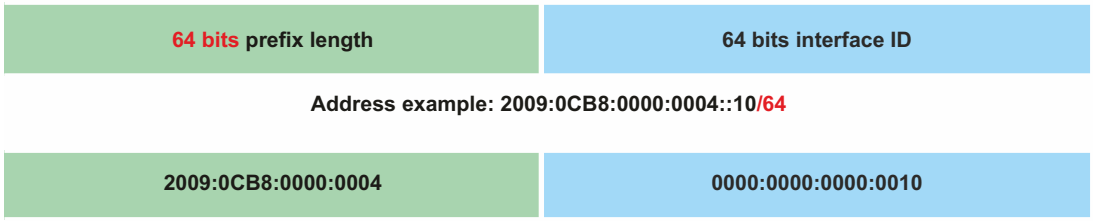
Diversamente da un indirizzo IPv4, l'indirizzo IPv6 non utilizza una maschera di sottorete per identificare la parte della rete di un'indirizzo. Il protocollo IPv6 utilizza invece la lunghezza del prefisso.

La rappresentazione del testo dell'indirizzo IPv6 è simile alla scrittura dell'indirizzo IPv4 in Classless Inter-Domain Routing (CIDR):

`<indirizzo-ipv6>/<lunghezza-prefisso>`

L'intervallo della lunghezza del prefisso è `0..128`. La lunghezza titpica del prefisso IPv6 per le LAN e per gli altri tipi di rete è /64. Ciò significa che la porzione di rete dell'indirizzo è lunga 64 bit. I restanti 64 bit rappresentano l'ID di interfaccia, similmente alla porzione di host dell'indirizzo IPv4.

Nella seguente figura è possibile trovare un esempio di assegnazione di bit nella lunghezza del prefisso.



Tipi di indirizzo

I tipi di indirizzo IPv6 sono descritti nell'RFC 4291.

I tipi di indirizzo IPv6 sono identificati dai bit con peso maggiore dell'indirizzo, come nella tabella seguente:

Tabella 10:Tipi di indirizzo IPv6

Tipo di indirizzo	Prefisso binario	Annotazione IPv6
Non specificato	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-local unicast	1111111010	FE80::/10
Unicast globale	(everything else)	

Indirizzo non specificato

L'indirizzo IPv4 con tutti i bit impostati su 0 è detto l'Indirizzo non specificato e corrisponde a 0.0.0.0 nell'IPv4. L'Indirizzo non specificato è utilizzato solo per indicare l'assenza di un indirizzo. Generalmente è utilizzato come indirizzo sorgente se non è ancora determinato un indirizzo univoco.

Nota: L'Indirizzo non specificato non può essere assgnato ad un'interfaccia o utilizzato come indirizzo di destinazione.

Indirizzo loopback

L'indirizzo unicast 0:0:0:0:0:0:0:1 è detto Indirizzo loopback. Può essere utilizzato da un dispositivo per inviare a se stesso un pacchetto IPv6. Non può essere assegnato a un'interfaccia fisica.

Indirizzo multicast

L'IPv6 non ha un indirizzo broadcast come l'IPv4. Tuttavia, vi è un indirizzo multicast IPv6 per tutti i nodi che di fatto offre lo stesso risultato.

Un indirizzo multicast IPv6 viene utilizzato per inviare un pacchetto IPv6 a destinazioni multiple. La struttura di un indirizzo multicast è la seguente: i successivi 4 bit indicano l'ambito dell'indirizzo multicast (fino a che punto viene trasmesso il pacchetto):
- I primi 8 bit sono inviati a `FF`.
- I successivi 4 bit sono la durata dell'indirizzo: 0 è permanente e 1 è temporaneo.
- I successivi 4 bit indicano l'ambito dell'indirizzo multicast, ovvero fino a che punto i pacchetti sono trasmessi nella rete.

Indirizzo link-local

L'indirizzo link-local viene utilizzato per comunicare con altri dispositivi sullo stesso link. Il termine "link" si riferisce a una sottorete. I router non inoltrano ad altri link i pacchetti con un indirizzo sorgente o di destinazione link-local.

Gli indirizzi link-local sono utilizzati per trasmettere i pacchetti a un link singolo per scopi come la configurazione automatica dell'indirizzo, rintracciare i vicini o quando non sono presenti router. Hanno il seguente formato:

Tabella 11:Formato Indirizzo link-local

10 bit	54 bit	64 bit
1111111010	0	ID di interfaccia

L'Indirizzo link-local è sempre configurato e non è modificabile.

Indirizzo unicast globale

Un indirizzo unicast globale è globalmente univoco e può essere indirizzato tramite Internet. Questo tipo di indirizzo è equivalente agli indirizzi IPv4 pubblici. Attualmente sono assegnati solo indirizzi unicast globali con i primi tre bit di 001 o 2000::/3.

Un Indirizzo unicast globale ha 3 parti:
- Prefisso di routing globale
- ID della sottorete
- ID di interfaccia

Il prefisso di routing globale è la parte di rete dell'indirizzo.

L'ID di sottorete è utilizzato da un'organizzazione per identificatore le sue sottoreti ed è lungo fino a 16 bit. La lunghezza di un ID della sottorete è determinata dalla lunghezza del Prefisso di routing globale.

L'ID d'interfaccia identifica un'interfaccia di un nodo specifico. Si utilizza il termine ID di interfaccia perché un host può avere più interfacce, ciascuna con uno o più indirizzi IPv6.

Il formato generale per gli indirizzi unicast globali IPv6 è rappresentato nella seguente figura.

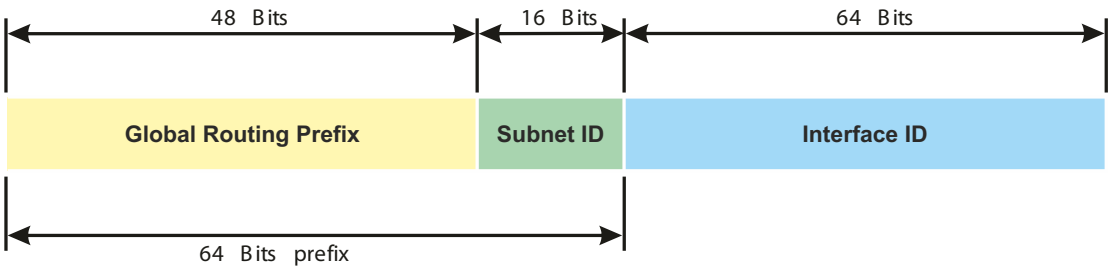


Figura 16: Formato generale dell'indirizzo unicast globale IPv6

2.2 Specificare i parametri IP utilizzando la Command Line Interface

2.2.1 IPv4

Per immettere i parametri IP sono disponibili i seguenti metodi:
- BOOTP/DHCP
- Protocollo Ethernet Switch Configurator
- Memoria esterna
- Command Line Interface utilizzando la connessione seriale

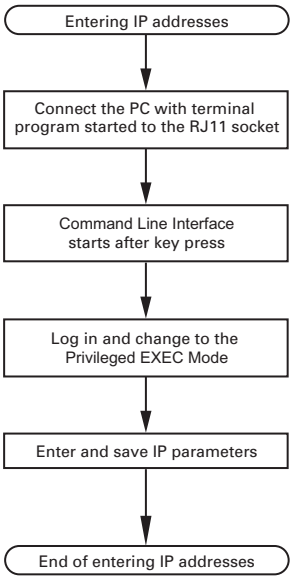
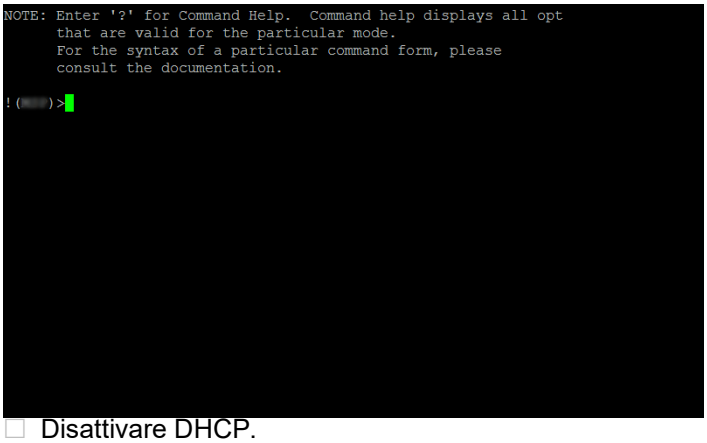


Figura 17: Organigramma per l'immissione degli indirizzi IP

Nota: Se un terminale o un PC con emulazione di terminale non è disponibile nei pressi della posizione di installazione, è possibile configurare il dispositivo presso la propria postazione di lavoro per poi portarlo alla sua posizione finale di installazione.

Eseguire i seguenti passaggi:
- ☐ Configurare una connessione al dispositivo.
  Compare la schermata iniziale.



- ☐ Disattivare DHCP.

- ☐ Immettere i parametri IP.
  - ▶ Indirizzo IP locale
    Nelle impostazioni di default, l'indirizzo IP locale è `0.0.0.0`.
  - ▶ Subnet mask
    Quando la rete è stata divisa in sottoreti, e queste sono identificate con una subnet mask, accedere alla subnet mask qui. Nelle impostazioni di default, la subnet mask locale è `0.0.0.0`.
  - ▶ Indirizzo IP del Gateway.
    Questa voce è richiesta solo nei casi in cui il dispositivo e la network management station o il TFTP server sono posizionati in sottoreti diverse (vedi pagina 45 “Esempio di utilizzo della subnet mask”).
    Specificare l'indirizzo IP del Gateway tra la sottorete con il dispositivo e il percorso verso la network management station.
    Nelle impostazioni di default, l'indirizzo IP è `0.0.0.0`.
- ☐ Salvare la configurazione specificata utilizzando `copy config running-config nvm`.

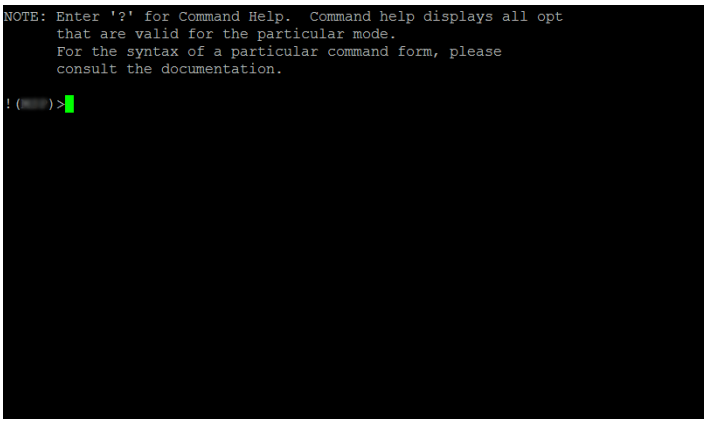
`enable`	Passare alla modalità Privileged EXEC.
`network protocol none`	Disattivazione del DHCP.
`network parms 10.0.1.23 255.255.255.0`	Assegnare al dispositivo l'indirizzo IP `10.0.1.23` e la subnet mask `255.255.255.0`. È inoltre possibile assegnare un indirizzo Gateway.
`copy config running-config nvm`	Salvare le impostazioni correnti nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

Dopo l'immissione dei parametri IP, il dispositivo si configura facilmente tramite l'interfaccia grafica utente.

2.2.2 IPv6

Il dispositivo consente di specificare i parametri IPv6 utilizzando la Command Line Interface tramite l'interfaccia seriale. Un'altra opzione per accedere alla Command Line Interface è utilizzare una connessione SSH con l''indirizzo di gestione IPv4.

Eseguire i seguenti passaggi:
- ☐ Configurare una connessione al dispositivo.
  Compare la schermata iniziale.



- ☐ Abilitare il protocollo IPv6 se il protocollo è disabilitato.
- ☐ Immettere i parametri IPv6.
  - ▶ Indirizzo IPv6
    Indirizzo IPv6 valido. L'indirizzo IPv6 è visualizzato in formato compresso.
  - ▶ Lunghezza del prefisso
    Diversamente da un indirizzo IPv4, l'indirizzo IPv6 non utilizza una maschera di sottorete per identificare la parte della rete di un'indirizzo. Nell'IPv6 questo ruolo è svolto dalla lunghezza del prefisso (vedi pagina 49 “Lunghezza del prefisso”).
  - ▶ Funzione *EUI option*
    È possibile utilizzare la funzione *EUI option* per configurare automaticamente l'ID di interfaccia dell'indirizzo IPv6. Il dispositivo utilizza l'indirizzo MAC della sua interfaccia con l'aggiunta dei valori `ff` e `fe` tra il byte 3 e il byte 4 per generare un'ID di interfaccia a 64 bit.
    È possibile selezionare questa opzione solo per gli indirizzi IPv6 che hanno una lunghezza di prefisso uguale a `64`.
  - ▶ Indirizzo IPv6 gateway
    L'indirizzo IPv6 gateway è l'indirizzo di un router attraverso il quale il dispositivo accede ad altri dispositivi al di fuori della sua rete.
    È possibile specificare qualsiasi indirizzo IPv6 ad eccezione degli indirizzi loopback e *Multicast*.
    Nell'impostazione di default, l'indirizzo IPv6 gateway è `::`.

`enable`	Passare alla modalità Privileged EXEC.
`network ipv6 operation`	Abilitare il protocollo IPv6 se il protocollo è disabilitato. Nell'impostazione di default, il protocollo IPv6 è abilitato.
`network ipv6 address add 2001::1 64 eui-64`	Assegnare l'indirizzo IPv6`2001::1` e la lunghezza di prefisso `64`. Il parametro `eui-64` è opzionale. È inoltre possibile assegnare un indirizzo gateway.
`copy config running-config nvm`	Salvare le impostazioni correnti nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

Dopo l'immissione dei parametri IPv6, il dispositivo si configura facilmente tramite l'interfaccia grafica utente. Per utilizzare un indirizzo IPv6 in un URL, utilizzare la seguente sintassi URL: `https://[<indirizzo_ipv6>]`.

2.3 Definizione dei parametri IP tramite Ethernet Switch Configurator

Il protocollo Ethernet Switch Configurator consente di assegnare parametri IP al dispositivo tramite l'Ethernet.

Tramite l'interfaccia grafica utente è possibile configurare facilmente altri parametri.

Installare il software Ethernet Switch Configurator sul proprio PC.

Eseguire i seguenti passaggi:
- ☐ Avviare il programma Ethernet Switch Configurator.

Quando Ethernet Switch Configurator è avviato, Ethernet Switch Configurator cerca automaticamente nella rete quei dispositivi che supportano il protocollo Ethernet Switch Configurator.

Ethernet Switch Configurator ricorre alla prima interfaccia di rete individuata per il PC. Quando il computer dispone di diverse schede di rete, è possibile selezionare quella desiderata nella barra degli strumenti Ethernet Switch Configurator.

Ethernet Switch Configurator mostra una riga per ciascun dispositivo che risponde a una richiesta del protocollo Ethernet Switch Configurator.

Ethernet Switch Configurator consente l'identificazione dei dispositivi visualizzati.
- ☐ Selezionare una riga del dispositivo.
- ☐ Per impostare i LED di modo che lampeggino per il dispositivo selezionato, fare clic sul pulsante *Signal* sulla barra degli strumenti. Per interrompere il lampeggio, fare clic nuovamente sul pulsante *Signal*.
- ☐ Con un doppio clic su una riga si apre una finestra nella quale si specifica il nome del dispositivo e il parametro IP.

Nota: Disabilitare la funzione Ethernet Switch Configurator nel dispositivo, dopo aver assegnato i parametri IP al dispositivo.

Nota: Salvare le impostazioni in modo da avere ancora le voci dopo il riavvio.

2.4 Definizione dei parametri IP tramite l'interfaccia grafica utente

2.4.1 IPv4

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Network > Global*.

In questa finestra di dialogo si specifica la VLAN in cui è possibile accedere alla gestione del dispositivo e configurare l'accesso Ethernet Switch Configurator.

- ☐ Nella colonna *VLAN ID* si specifica la VLAN in cui è possibile accedere alla gestione del dispositivo attraverso la rete.

Si noti che è possibile accedere alla gestione dei dispositivi solo utilizzando le porte che fanno parte della relativa VLAN.

Il campo *MAC address* mostra l'indirizzo MAC del dispositivo con cui si accede al dispositivo attraverso la rete.

- ☐ Nel riquadro *Ethernet Switch Configurator protocol v1/v2* si specificano le impostazioni per accedere al dispositivo utilizzando il software Ethernet Switch Configurator.
- ☐ Il protocollo Ethernet Switch Configurator consente di assegnare un indirizzo IP al dispositivo sulla base del suo indirizzo MAC. Attivare il protocollo Ethernet Switch Configurator se si desidera assegnare un indirizzo IP al dispositivo dal proprio PC con il software Ethernet Switch Configurator.
- ☐ Aprire la finestra di dialogo *Basic Settings > Network > IPv4*.

In questa finestra di dialogo si specifica l'origine dalla quale il dispositivo ottiene i propri parametri IP dopo l'avvio.

- ☐ Nel riquadro *Management interface* si specifica innanzitutto da dove il dispositivo ottiene i propri parametri IP.
- ▶ Nella modalità `BOOTP`, la configurazione sta utilizzando un server BOOTP o DHCP sulla base dell'indirizzo MAC del dispositivo.
- ▶ Nella modalità `DHCP`, la configurazione sta utilizzando un server DHCP sulla base dell'indirizzo MAC o del nome del dispositivo.
- ▶ Nella modalità `Local`, il dispositivo utilizza i parametri di rete dalla memoria interna del dispositivo.

Nota: Quando si modifica la modalità di assegnazione dell'indirizzo IP, il dispositivo attiva la nuova modalità subito dopo aver cliccato sul pulsante ✓.

- ☐ Se necessario, si inserisce l'indirizzo IP, la subnet mask e il Gateway nel riquadro *IP parameter*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

2.4.2 IPv6

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Network > IPv6*.
- ☐ Il protocollo IPv6 è abilitato di default. Verificare che il pulsante di opzione `On` sia selezionato nel riquadro *Operation*.
- ☐ Nel riquadro *Configuration* specificare da dove il dispositivo ottiene i suoi parametri IPv6:
  - ▶ Se il pulsante di opzione *None* è selezionato, il dispositivo riceve i parametri IPv6 manualmente.
    È possibile specificare manualmente un numero massimo di 4 indirizzi IPv6. Non è possibile specificare indirizzi loopback, link-local e *Multicast* come indirizzi IPv6 statici.
  - ▶ Se il pulsante di opzione *Auto* è selezionato, il dispositivo riceve i parametri IPv6 dinamicamente, ad esempio utilizzando un Router Advertisement Daemon.
    Il dispositivo riceve un massimo di 2 indirizzi IPv6.
  - ▶ Se il pulsante di opzione *DHCPv6* è selezionato, il dispositivo riceve i parametri IPv6 da un server DHCPv6.
    Il dispositivo può ricevere solamente un indirizzo IPv6 dal server DHCPv6.
  - ▶ Selezionando il pulsante di opzione *All*, il dispositivo riceve i suoi parametri IPv6 utilizzando tutte le alternative per le assegnazioni dinamiche e manuali.

Nota: Quando si modifica la modalità di assegnazione dell'indirizzo IPv6, il dispositivo attiva la nuova modalità subito dopo aver cliccato sul pulsante ✓.

- ☐ Se necessario, immettere il *Gateway address* nel riquadro *IP parameter*.

Nota: Selezionando il pulsante di opzione *Auto* e utilizzando un Router Advertisement Daemon (radvd), il dispositivo riceve automaticamente un *Gateway address* di tipo link-local con metrica superiore al *Gateway address* impostato manualmente.

- ☐ Nel riquadro *Duplicate Address Detection* è possibile specificare il numero di messaggi *Neighbor Solicitation* consecutivi che il dispositivo invia per la funzione *Duplicate Address Detection*(vedi pagina 63 “Duplicate Address Detection”).

Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Specificare manualmente un indirizzo IPv6. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Network > IPv6*.
- ☐ Fare clic sul pulsante ⊞.
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Immettere l'indirizzo IPv6 nel campo *IP address*.
- ☐ Immettere la lunghezza del prefisso dell'indirizzo IPv6 nel campo *PrefixLength*.
- ☐ Fare clic sul pulsante *Ok*.
  Il dispositivo aggiunge una nuova voce tabella.

2.5 Definizione dei parametri IP tramite BOOTP

Con la funzione *BOOTP* attivata, il dispositivo invia un messaggio di richiesta di boot al server BOOTP. Il messaggio di richiesta di boot contiene il Client ID configurato nella finestra di dialogo *Basic Settings > Network > IPv4*. Il server BOOTP immette il Client ID nel database e assegna un indirizzo IP. Il server risponde con un messaggio di risposta di boot. Il messaggio di risposta di boot contiene l'indirizzo IP assegnato.

2.6 Definizione dei parametri IP tramite DHCP

2.6.1 IPv4

Il DHCP (protocollo di configurazione IP dinamica) rappresenta l'evoluzione ulteriore subentrata al BOOTP. Il DHCP consente inoltre la configurazione di un client DHCP utilizzando un nome invece di un indirizzo MAC.

Per il DHCP, questo nome è conosciuto come “Client Identifier” in conformità alla RFC 2131.

Il dispositivo utilizza il nome immesso sotto il sysName nel gruppo di sistema del MIB II come Client Identifier. È possibile modificare il nome di sistema utilizzando l'interfaccia grafica utente (vedere la finestra di dialogo *Basic Settings > System*), la Command Line Interface o SNMP.

Il dispositivo invia il rispettivo nome di sistema al server DHCP. Il server DHCP utilizza poi il nome di sistema per assegnare un indirizzo IP come alternativa all'indirizzo MAC.

Oltre all'indirizzo IP il server DHCP invia
- la subnet mask
- il Gateway di default (se disponibile)
- l'URL TFTP del file di configurazione (se disponibile).

Il dispositivo applica i dati di configurazione ai parametri appropriati. Quando il server DHCP assegna l'indirizzo IP, il dispositivo salva in maniera permanente i dati di configurazione nella memoria non volatile.

Tabella 12:Opzioni DHCP richieste dal dispositivo

Opzioni	Significato
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

Il vantaggio offerto dal DHCP rispetto al BOOTP è costituito dal fatto che il server DHCP è in grado di vincolare la validità dei parametri di configurazione (“Lease”) a un intervallo di tempo definito (la cosiddetta assegnazione dinamica degli indirizzi). Prima che questo periodo (“Lease Duration”) scada, il client DHCP può tentare di rinnovare questo lease. In alternativa, il client può negoziare un nuovo lease. Il server DHCP assegna poi un indirizzo libero casuale.

Per contribuire a evitare ciò, i server DHCP offrono l'opzione di configurazione esplicita di assegnare a un determinato client, sulla base di un ID hardware univoco, lo stesso indirizzo IP (la cosiddetta assegnazione statica di indirizzi).

Nelle impostazioni di default, il DHCP è attivato. Finché il DHCP è attivato, il dispositivo tenta di ottenere un indirizzo IP. Se dopo il riavvio il dispositivo non sarà in grado di trovare un server DHCP, non disporrà di un indirizzo IP. La finestra di dialogo *Basic Settings > Network > IPv4* consente di attivare o disattivare il DHCP.

Nota: Quando si utilizza la gestione di rete ConneXium Network Manager, verificare che il DHCP assegni l'indirizzo IP originale a tutti i dispositivi.

L'allegato contiene una configurazione esemplificativa del server BOOTP/DHCP.

Esempio di un file di configurazione DHCP:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

le righe che iniziano con il carattere `#` contengono commenti.

Le righe che precedono i dispositivi elencati singolarmente si riferiscono alle impostazioni che si applicano al dispositivo seguente.

La riga a indirizzo fisso assegna un indirizzo IP permanente al dispositivo.

Per ulteriori informazioni, consultare il manuale del server DHCP.

2.6.2 IPv6

Il Dynamic Host Configuration Protocol version 6 (DHCPv6) è un protocollo di rete utilizzato per specificare in modo dinamico gli indirizzi IPv6. Questo protocollo è l'equivalente IPv6 del protocollo DHCP per l'IPv4. Il protocollo DHCPv6 è descritto nell'RFC 8415.

Il dispositivo utilizza un DHCP Unique Identifier (DUID) per inviare una richiesta al server DHCPv6. Nel dispositivo, il DUID rappresenta il *Client ID* che il server DHCPv6 utilizza per individuare il dispositivo che ha richiesto un indirizzo IPv6.

Il *Client ID* è visualizzato nella finestra di dialogo *Basic Settings > Network > IPv6*, nel riquadro *DHCP*.

Il dispositivo può ricevere solo un indirizzo IPv6 dal server DHCPv6, con una *PrefixLength* di `128`. Non è fornita nessuna informazione *Gateway address*. Se necessario, è possibile specificare le informazioni *Gateway address* manualmente.

Nell'impostazione di default, il protocollo DHCPv6 è disattivato. È possibile attivare o disattivare il protocollo nella finestra di dialogo *Basic Settings > Network > IPv6*. Verificare che il pulsante di opzione *DHCPv6* sia selezionato nel riquadro *Configuration*.

Per ottenere un indirizzo IPv6 dinamicamente con una *PrefixLength* diversa da `128`, selezionare il pulsante di opzione *Auto*. Ne è un esempio l'utilizzo di un Router Advertisement Daemon (radvd). Il radvd utilizza messaggi *Router Solicitation* e *Router Advertisement* per configurare automaticamente un indirizzo IPv6.

Nell'impostazione di default, il pulsante di opzione *Auto* è selezionato. È possibile selezionare o deselezionare il pulsante di opzione *Auto* nella finestra di dialogo *Basic Settings > Network > IPv6*, nel riquadro *Configuration*.

Selezionando il pulsante di opzione *All*, il dispositivo riceve i suoi parametri IPv6 utilizzando tutte le alternative per le assegnazioni dinamiche e manuali.

2.7 Rilevamento conflitti tra indirizzi di gestione

È possibile assegnare un indirizzo IP al dispositivo utilizzando diversi metodi. Questa funzione aiuta il dispositivo a rilevare conflitti tra gli indirizzi IP su una rete dopo l'avvio, e il dispositivo controlla periodicamente anche durante il funzionamento. Questa funzione è descritta nell'RFC 5227.

Quando è abilitata, il dispositivo invia una SNMP trap comunicando di aver rilevato un conflitto tra gli indirizzi IP.

L'elenco seguente contiene le impostazioni di default per questa funzione:
- *Operation*: `On`
- *Detection mode*: `active and passive`
- *Send periodic ARP probes*: `selezionato`
- *Detection delay [ms]*: `200`
- *Release delay [s]*: `15`
- *Address protections*: `3`
- *Protection interval [ms]*: `200`
- *Send trap*: `selezionato`

2.7.1 Rilevamento attivo e passivo

La verifica attiva della rete contribuisce a impedire che il dispositivo si colleghi alla rete con un indirizzo IP duplicato. Dopo aver connesso il dispositivo a una rete o dopo aver configurato l'indirizzo IP, il dispositivo verifica immediatamente se il suo indirizzo IP è presente all'interno della rete. Per verificare la presenza di conflitti tra gli indirizzi nella rete, il dispositivo invia nella rete 4 sonde ARP con il ritardo di rilevazione impostato a 200°millisecondi. Quando l'indirizzo IP è presente, il dispositivo tenta di tornare alla configurazione precedente e tenta di eseguire un altro controllo dopo il tempo di ritardo di rilascio configurato.

Quando si disabilita il rilevamento attivo, il dispositivo invia 2 annunci APR gratuiti a intervalli di 2 secondi. Utilizzando gli annunci ARP con il rilevamento passivo abilitato, il dispositivo interroga la rete per stabilire se vi sia un conflitto tra gli indirizzi. Dopo aver risolto un conflitto tra indirizzi o dopo un tempo di ritardo di rilascio scaduto, il dispositivo si ricollega alla rete. Dopo 10 conflitti rilevati, quando l'intervallo di ritardo di rilascio configurato è inferiore a 60 secondi, il dispositivo imposta l'intervallo di ritardo di rilascio su 60 secondi.

Dopo che il dispositivo esegue il rilevamento attivo o dopo la disabilitazione della funzione di rilevamento attivo, con il rilevamento passivo abilitato, il dispositivo resta in ascolto sulla rete per rilevare altri dispositivi che utilizzano lo stesso indirizzo IP. Quando il dispositivo rileva un indirizzo IP duplicato, difende inizialmente il suo indirizzo utilizzando il meccanismo ACD in modalità di rilevamento passivo e invia ARP gratuiti. Il numero di protezioni che il dispositivo invia e l'intervallo di protezione sono configurabili. Per risolvere i conflitti, se il dispositivo remoto rimane connesso alla rete, l'interfaccia di rete del dispositivo locale si scollega dalla rete.

Quando un server DHCP assegna un indirizzo IP al dispositivo e si verifica un conflitto tra indirizzi, il dispositivo restituisce un messaggio di rifiuto DHCP.

Il dispositivo utilizza il metodo della sonda ARP. Questo presenta i seguenti vantaggi:
- Le cache ARP su altri dispositivi rimangono invariate.
- Il metodo è robusto grazie alle trasmissioni multiple della sonda ARP.

2.8 Duplicate Address Detection

La funzione *Duplicate Address Detection* determina l'unicità di un indirizzo unicast IPv6 su un'interfaccia. La funzione è eseguita quando un indirizzo IPv6 è configurato utilizzando il metodo manuale, *DHCPv6* o *Auto*. La funzione è attivata anche da una modifica dello stato del link, ad esempio lo stato del link passa da down a up.

La funzione *Duplicate Address Detection* utilizza i messaggi *Neighbor Solicitation* e *Neighbor Advertisement*. È possibile impostare il numero di messaggi *Neighbor Solicitation* consecutivi che il dispositivo invia. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Network > IPv6*.
- ☐ Nel riquadro *Duplicate Address Detection* impostare il valore necessario nel campo*Number of neighbor solicitants*.
  Possibili valori:
  - `0`
    La funzione è disabilitata.
  - `1..5` (impostazione di default: `1`)
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

`enable`	Passare alla modalità Privileged EXEC.
`network ipv6 dad-transmits <0..5>`	Impostare il numero di messaggi *Neighbor Solicitation* che il dispositivo invia. Il valore `0` disabilita la funzione.

Nota: Se la funzione *Duplicate Address Detection* scopre che un indirizzo IPv6 non è unico su un link, il dispositivo non registra questo evento nel file di registro (System Log).

3 Accesso al dispositivo

3.1 Ruoli di accesso

Le funzioni del dispositivo sono disponibili all'utente in base al ruolo di accesso. Se l'utente ha effettuato l'accesso con uno specifico ruolo di accesso, avrà a disposizione le funzioni del ruolo di accesso.

I comandi disponibili all'utente dipendono anche dalla modalità della Command Line Interface in cui l'utente sta attualmente lavorando. Vedi “Gerarchia di comando basata sulla modalità” a pagina 25.

Il dispositivo offre i seguenti ruoli di accesso:

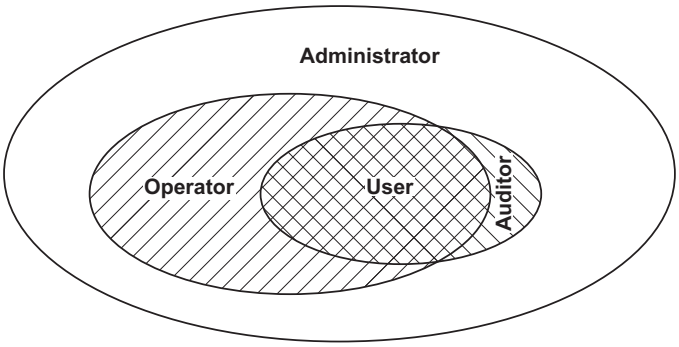


Tabella 13:Ruoli di accesso e ambito delle autorizzazioni utente

Ruolo di accesso	Autorizzazioni utente
`User`	Gli utenti che hanno effettuato l'accesso con il ruolo di accesso `User` sono autorizzati a monitorare il dispositivo.
`Auditor`	Gli utenti che hanno effettuato l'accesso con il ruolo di accesso `Auditor` sono autorizzati a monitorare il dispositivo ed a salvare il file di registro nella finestra di dialogo *Diagnostics > Report > Audit Trail*.
`Operator`	Gli utenti che hanno effettuato l'accesso con il ruolo di accesso `Operator` sono autorizzati a monitorare il dispositivo ed a modificare le impostazioni, ad eccezione delle impostazioni di sicurezza per l'accesso al dispositivo.
`Administrator`	Gli utenti che hanno effettuato l'accesso con il ruolo di accesso `Administrator` sono autorizzati a monitorare il dispositivo ed a modificare le impostazioni.
`Unauthorized`	Gli utenti non autorizzati sono bloccati e il dispositivo rifiuta l'accesso dell'utente. Assegnare questo valore per bloccare temporaneamente l'account utente. In caso di errore riconosciuto durante un cambio di ruolo di accesso, il dispositivo assegna questo accesso all'account utente.

3.2 Primo accesso (modifica password)

Per contribuire a evitare accessi indesiderati al dispositivo, è imperativo modificare la password predefinita durante la configurazione iniziale.

Eseguire i seguenti passaggi:

- ☐ Aprire l'interfaccia grafica utente , l'SE Viewapplicazione , o la Command Line Interface la prima volta che si esegue l'accesso.
- ☐ Eseguire l'accesso con la password di default.
  Il dispositivo suggerisce l'immissione di una nuova password.
- ☐ Digitare la nuova password.
  Per contribuire ad aumentare la sicurezza, scegliere una password contenente almeno 8 caratteri, che includa lettere maiuscole, lettere minuscole, cifre numeriche e caratteri speciali.
- ☐ Quando si esegue l'accesso con la Command Line Interface, il dispositivo suggerisce di confermare la nuova password.
- ☐ Eseguire nuovamente l'accesso con la nuova password.

Nota: Se ha dimenticato la password, contatti il suo team di supporto locale.

3.3 Elenchi di autenticazione

Quando un utente accede al dispositivo utilizzando una connessione specifica, il dispositivo verifica le credenziali di accesso dell'utente in un elenco di autenticazione che contiene i criteri applicati dal dispositivo per l'autenticazione.

Il prerequisito per l'accesso di un utente alla gestione del dispositivo è che almeno un criterio sia assegnato all'elenco di autenticazione dell'applicazione attraverso cui si effettua l'accesso.

3.3.1 Applicazioni

Il dispositivo fornisce un applicazione ad ogni tipo di connessione attraverso cui qualcuno accede al dispositivo:
- Accesso alla Command Line Interface utilizzando una connessione seriale: `Console(V.24)`
- Accesso alla Command Line Interface utilizzando SSH: `SSH`
- Accesso alla Command Line Interface utilizzando Telnet: `Telnet`
- Accesso all'interfaccia grafica utente: `WebInterface`

Il dispositivo fornisce anche un'applicazione per controllare l'accesso alla rete da dispositivi finali connessi utilizzando il controllo di accesso basato su porta: `8021x`

3.3.2 Criteri

Quando un utente accede con dati di accesso validi, il dispositivo consente all'utente l'accesso alla sua gestione del dispositivo. Il dispositivo autentica gli utenti utilizzando i seguenti criteri:
- Gestione utenti del dispositivo
- LDAP
- RADIUS

Quando il dispositivo finale accede con dati di login validi, il dispositivo consente ai dispositivi finali connessi di accedere alla rete con il controllo di accesso basato su porta in base a IEEE 802.1X. Il dispositivo autentica i dispositivi finale utilizzando i seguenti criteri:
- RADIUS
- IAS (Integrated Authentication Server)

Il dispositivo offre l'opzione di una soluzione fallback. A tale scopo, specificare più di un criterio nell'elenco di autenticazione. Quando l'autenticazione non riesce utilizzando l'attuale criterio, il dispositivo applica il criterio specificato successivo.

3.3.3 Gestione degli elenchi di autenticazione

Gli elenchi di autenticazione si gestiscono nell'interfaccia grafica utente o nella Command Line Interface. A tale scopo, eseguire i seguenti passaggi:

☐ Aprire la finestra di dialogo *Device Security > Authentication List*.

La finestra di dialogo visualizza gli elenchi di autenticazione che sono configurati.

`show authlists`	Visualizza gli elenchi di autenticazione che sono configurati.

☐ Disattivare l'elenco di autenticazione per quelle applicazioni tramite le quali non viene eseguito alcun accesso al dispositivo, ad esempio `8021x`.

☐ Nella colonna *Active* dell'elenco di autenticazione `defaultDot1x8021AuthList`, deselezionare la casella di spunta.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`authlists disable defaultDot1x8021AuthList`	Disattiva l'elenco di autenticazione `defaultDot1x8021AuthList`.

3.3.4 Adeguamento delle impostazioni

Esempio: configurare un elenco di autenticazione separato per l'applicazione `WebInterface` che è inclusa di default nell'elenco di autenticazione `defaultLoginAuthList`.

Il dispositivo inoltra le richieste di autenticazione ad un server RADIUS nella rete. Come soluzione fallback, il dispositivo autentica gli utenti utilizzando la gestione utenti locale. A tale scopo, eseguire i seguenti passaggi:

☐ Creare un elenco di autenticazione `loginGUI`.

☐ Aprire la finestra di dialogo *Device Security > Authentication List*.

☐ Fare clic sul pulsante ➕.
La finestra di dialogo mostra la finestra *Create*.

☐ Inserire un nome significativo nel campo *Name*.
In questo esempio, immettere il nome `loginGUI`.

☐ Fare clic sul pulsante *Ok*.
Il dispositivo aggiunge una nuova voce tabella.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`authlists add loginGUI`	Creare l'elenco di autenticazione `loginGUI`.

☐ Selezionare i criteri per l'elenco di autenticazione `loginGUI`.

☐ Selezionare il valore *`radius`* nella colonna *Policy 1*.

☐ Selezionare il valore *`local`* nella colonna *Policy 2*.

☐ Nelle colonne da *Policy 3* a *Policy 5*, selezionare il valore *`reject`* per evitare un ulteriore fallback.

☐ Nella colonna *Active*, selezionare la casella di spunta.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`authlists set-policy loginGUI radius local reject reject reject`	Assegna i criteri `radius`, `local` e `reject` all'elenco di autenticazione `loginGUI`.
`show authlists`	Visualizza gli elenchi di autenticazione che sono configurati.
`authlists enable loginGUI`	Attiva l'elenco di autenticazione `loginGUI`.

☐ Assegnare un'applicazione all'elenco di autenticazione `loginGUI`.

☐ Nella finestra di dialogo *Device Security > Authentication List*, evidenziare l'elenco di autenticazione `loginGUI`.

☐ Fare clic sul pulsante e poi sulla voce *Allocate applications*.
La finestra di dialogo mostra la finestra *Allocate applications*.

☐ Nella colonna sinistra, evidenziare l'applicazione `WebInterface`.

☐ Fare clic sul pulsante .
Ora la colonna destra visualizza l'applicazione `WebInterface`.

☐ Fare clic sul pulsante *Ok*.
La finestra di dialogo visualizza le impostazioni aggiornate:
- La colonna *Dedicated applications* dell'elenco di autenticazione `loginGUI` visualizza l'applicazione `WebInterface`.
- La colonna *Dedicated applications* dell'elenco di autenticazione `defaultLoginAuthList` non visualizza più l'applicazione `WebInterface`.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

`show appllists`	Visualizza le applicazioni e gli elenchi allocati.
`appllists set-authlist WebInterface loginGUI`	Assegna l'applicazione `loginGUI` all'elenco di autenticazione `WebInterface`.

3.4 Gestione degli utenti

Quando un utente accede con dati di accesso validi, il dispositivo consente all'utente l'accesso alla sua gestione del dispositivo. Il dispositivo autentica gli utenti utilizzando la gestione utenti locale o con un server RADIUS nella rete. Affinché il dispositivo utilizzi la gestione utenti, assegnare il criterio `local` ad un elenco di autenticazione, vedere la finestra di dialogo *Device Security > Authentication List*.

Nella gestione degli utenti locale, si gestiscono gli account utenti. Solitamente un account utente è associato a ogni utente.

3.4.1 Ruoli di accesso

Il dispositivo consente l'utilizzo di un modello di autorizzazione basato sul ruolo per controllare in modo specifico l'accesso alla gestione del dispositivo. Gli utenti a cui è assegnato uno specifico profilo di autorizzazione hanno il diritto di utilizzare comandi e funzioni dallo stesso profilo di autorizzazione oppure uno inferiore.

Il dispositivo utilizza i profili di autorizzazione su ogni applicazione con cui è possibile accedere alla gestione del dispositivo.

Ogni account utente è collegato ad un ruolo di accesso che regola l'accesso alle funzioni individuali del dispositivo. In funzione dell'attività pianificata per il rispettivo utente, si assegna un ruolo di accesso predefinito all'utente. Il dispositivo differenzia tra i seguenti ruoli di accesso.

Tabella 14:Ruoli di accesso per gli account utenti

Role	Descrizione	Autorizzato per le seguenti attività
Administrator	L'utente è autorizzato a monitorare ed amministrare il dispositivo.	Tutte le attività con accesso in lettura/scrittura, comprese le seguenti attività riservate ad un amministratore: ▶ Aggiungere, modificare o cancellare gli account utenti ▶ Attivare, disattivare o sbloccare gli account utenti ▶ Modificare ogni password ▶ Configurare la gestione della password ▶ Impostare o modificare l'orario di sistema ▶ Caricare i file sul dispositivo, ad esempio le configurazioni dispositivo, i certificati o le immagini software ▶ Resettare le impostazioni e le impostazioni correlate alla sicurezza allo stato di fornitura. ▶ Configurare il server RADIUS e gli elenchi di autenticazione ▶ Applicare gli script utilizzando la Command Line Interface ▶ Abilitare/disabilitare il registro CLI e il registro SNMP ▶ Attivazione e disattivazione della memoria esterna ▶ Attivazione e disattivazione del monitor di sistema ▶ Abilitare/disabilitare i servizi per l'accesso alla gestione del dispositivo (ad esempio SNMP). ▶ Configurare le limitazioni di accesso all'interfaccia grafica utente o alla Command Line Interface in base agli indirizzi IP
Operator	L'utente è autorizzato a monitorare e a configurare il dispositivo - con l'eccezione di impostazioni correlate alla sicurezza.	Tutte le attività con accesso in lettura/scrittura, ad eccezione delle attività sopra indicate che sono riservate ad un amministratore:

Tabella 14:Ruoli di accesso per gli account utenti (cont

Role	Descrizione	Autorizzato per le seguenti attività
Auditor	L'utente è autorizzato a monitorare il dispositivo e a memorizzare il file di registro nella finestra di dialogo *Diagnostics > Report > Audit Trail*.	Monitoraggio delle attività con accesso in lettura.
Guest	L'utente è autorizzato a monitorare il dispositivo ad eccezione delle impostazioni correlate alla sicurezza.	Monitoraggio delle attività con accesso in lettura.
Unauthorized	Nessun accesso al dispositivo possibile. ▶ In qualità di amministratore si assegna questo ruolo di accesso per bloccare temporaneamente un account utente. ▶ Se un amministratore assegna un ruolo di accesso differente all'account utente e viene rilevato un errore, il dispositivo assegna questo ruolo di accesso all'account utente.	Nessuna attività consentita.

3.4.2 Gestione degli account utenti

Gli account utenti si gestiscono nell'interfaccia grafica utente o nella Command Line Interface. A tale scopo, eseguire i seguenti passaggi:

☐ Aprire la finestra di dialogo *Device Security > User Management*.

La finestra di dialogo visualizza gli account utenti che sono configurati.

`show users`	Visualizza gli account utenti che sono configurati.

3.4.3 Impostazione di default

Allo stato di fornitura, gli account utenti `admin` e `user` sono configurati nel dispositivo.

Tabella 15:Impostazioni di default per gli account utenti delle impostazioni di fabbrica

Parametro	Impostazione di default	
User name	`admin`	`user`
Password	`private`	`public`
Role	`administrator`	`guest`
User locked	`non selezionato`	`non selezionato`
Policy check	`non selezionato`	`non selezionato`
SNMP auth type	`hmacmd5`	`hmacmd5`
SNMP encryption type	`des`	`des`

Modificare la password per l'account utente `admin` prima di rendere il dispositivo disponibile nella rete.

3.4.4 Modifica delle password di default

Per evitare accessi indesiderati, modificare la password degli account utenti di default. A tale scopo, eseguire i seguenti passaggi:

☐ Modificare le password per gli account utenti `admin` e `user`.

☐ Aprire la finestra di dialogo *Device Security > User Management*.

La finestra di dialogo visualizza gli account utenti che sono configurati.

☐ Per ottenere un livello superiore di complessità per la password, selezionare la casella di spunta nella colonna*Policy check*.
Prima di salvarla, il dispositivo verifica la password in base ai criteri specificati nel riquadro *Password policy*.

Nota: La verifica password può comportare un messaggio nel riquadro *Security status* nella finestra di dialogo *Basic Settings > System*. Specificare le impostazioni che causano questo messaggio nella finestra di dialogo *Basic Settings > System*.

☐ Fare clic sulla riga dell'account utente rilevante nel campo *Password*. Immettere una password di almeno 6 caratteri.
Sono consentiti fino a 64 caratteri alfanumerici.
- ▶ Il dispositivo differenzia tra maiuscole e minuscole.
- ▶ La lunghezza minima della password è specificata nel riquadro *Configuration*. Il dispositivo verifica costantemente la lunghezza minima della password.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`users password-policy-check <user> enable`	Attiva la verifica della password per l'account utente `<user>` basato sui criteri specificati. In questo modo, si ottiene un livello superiore di complessità per la password.

Nota: Quando si visualizza lo stato di sicurezza, la verifica della password può comportare un messaggio (`show security-status all`). Specificare le impostazioni che causano questo messaggio con il comando `security-status monitor pwd-policy-inactive`.

`users password <user> SECRET`	Specifica la password `SECRET` per l'account utente `<user>`. Immettere almeno 6 caratteri.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

3.4.5 Impostazione di un nuovo account utente

Allocare un account utente separato ad ogni utente che accede alla gestione dispositivo. In questo modo è possibile controllare specificamente le autorizzazioni per l'accesso.

Nel seguente esempio, configureremo l'account utente per un utente `USER` con il ruolo `operator`. Gli utenti con il ruolo `operator` sono autorizzati a monitorare e configurare il dispositivo - ad eccezione delle impostazioni correlate alla sicurezza. A tale scopo, eseguire i seguenti passaggi:
☐ Creare un nuovo account utente.

- ☐ Aprire la finestra di dialogo *Device Security > User Management*.
- ☐ Fare clic sul pulsante  .
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Inserire il nome nel campo *User name*.
  In questo esempio, attribuiamo all'account utente il nome `USER`.
- ☐ Fare clic sul pulsante *Ok*.
- ☐ Per ottenere un livello superiore di complessità per la password, selezionare la casella di spunta nella colonna*Policy check*.
  Prima di salvarla, il dispositivo verifica la password in base ai criteri specificati nel riquadro *Password policy*.
- ☐ Nel campo *Password*, immettere una password di almeno 6 caratteri.
  Sono consentiti fino a 64 caratteri alfanumerici.
  - ▶ Il dispositivo differenzia tra maiuscole e minuscole.
  - ▶ La lunghezza minima della password è specificata nel riquadro *Configuration*. Il dispositivo verifica costantemente la lunghezza minima della password.
- ☐ Nella colonna *Role*, selezionare il ruolo dell'utente.
  In questo esempio, selezioniamo il valore `operator`.
- ☐ Per attivare l'account utente, selezionare la casella di spunta nella colonna *Active*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .
  La finestra di dialogo visualizza gli account utenti che sono configurati.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`users add USER`	Crea l'account utente `USER`.
`users password-policy-check USER enable`	Attiva la verifica della password per l'account utente `USER` basato sui criteri specificati. In questo modo, si ottiene un livello superiore di complessità per la password.

`users password USER SECRET`	Specifica la password `SECRET` per l'account utente `USER`. Immettere almeno 6 caratteri.
`users access-role USER  operator`	Assegnare il ruolo utente `operator` all'account utente `USER`.
`users enable USER`	Attiva l'account utente `USER`.
`show users`	Visualizza gli account utenti che sono configurati.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

Nota: Quando si configura un nuovo account utente nella Command Line Interface, ricordarsi di allocare la password.

3.4.6 Disattivazione dell'account utente

Dopo che un account utente è disattivato, il dispositivo nega il relativo accesso dell'utente alla gestione del dispositivo. A differenza della completa eliminazione, la disattivazione di un account utente consente di mantenere le impostazioni e di riutilizzarle in futuro. A tale scopo, eseguire i seguenti passaggi:

☐ Per mantenere le impostazioni dell'account utente e riutilizzarle in futuro, disattivare temporaneamente l'account utente.

☐ Aprire la finestra di dialogo *Device Security > User Management*.
La finestra di dialogo visualizza gli account utenti che sono configurati.

☐ Nella riga per l'account utente rilevante, deselezionare la casella di spunta nella colonna *Active*.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`users disable <user>`	Per disabilitare l'account utente.
`show users`	Visualizza gli account utenti che sono configurati.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

☐ Per disattivare permanentemente le impostazioni account utenti, eliminare l'account utente.

☐ Evidenziare la riga per l'account utente rilevante.

☐ Fare clic sul pulsante  .

`users delete <user>`	Elimina l'account utente `<user>`.
`show users`	Visualizza gli account utenti che sono configurati.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

3.4.7 Adattamento dei parametri per le password

Il dispositivo consente di verificare se le password per gli account utenti corrispondono ai parametri specificati. Quando le password corrispondono ai parametri, si ottiene un livello superiore di complessità per le password.

La gestione utenti del dispositivo consente di attivare o disattivare la verifica separatamente in ogni account utente. Quando si seleziona la casella di spunta e la nuova password soddisfa i requisiti dei criteri, il dispositivo accetta la modifica della password.

Nelle impostazioni di default, i valori effettivi per i criteri sono configurati nel dispositivo. È possibile adeguare i criteri alle esigenze dell'utente. A tale scopo, eseguire i seguenti passaggi:
☐ Adeguare i criteri per le password per soddisfare le esigenze dell'utente.

☐ Aprire la finestra di dialogo *Device Security > User Management*.

Nel riquadro *Configuration*, specificare il numero di tentativi di accesso degli utenti prima che il dispositivo blocchi l'utente. Si specifica anche il numero minimo di caratteri che definisce una password.

Nota: Il dispositivo consente solo agli utenti con l'autorizzazione *`administrator`* la rimozione del blocco.

Il numero di tentativi di accesso e il possibile blocco dell'utente si applicano solo quando si accede alla gestione del dispositivo attraverso:
- l'interfaccia grafica utente
- il protocollo SSH
- il protocollo Telnet

Nota: Quando si accede alla gestione del dispositivo utilizzando la Command Line Interface attraverso una connessione seriale, il numero di tentativi di accesso è illimitato.

☐ Specificare i valori per soddisfare le specifiche esigenze.
- Nel campo *Login attempts* specificare il numero di volte in cui un utente tenta di eseguire l'accesso. Il campo consente di definire questo valore nell'intervallo `0..5`.
  Nel suddetto esempio, il valore `0` disattiva la funzione.
- Il campo *Min. password length* consente di immettere valori nell'intervallo `1..64`.

La finestra di dialogo visualizza i criteri configurati nel riquadro *Password policy*.

☐ Adeguare i valori per soddisfare le specifiche esigenze dell'utente.
- Sono consentiti i valori nell'intervallo `1` - `16`.
  Il valore `0` disattiva i criteri rilevanti.

Per applicare le voci specificate nei riquadri *Configuration* e *Password policy*, selezionare la casella di spunta nella colonna *Policy check* per un particolare utente.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`passwords min-length 6`	Specifica i criteri per la lunghezza minima della password.
`passwords min-lowercase-chars 1`	Specifica i criteri per il numero minimo di lettere minuscole nella password.
`passwords min-numeric-chars 1`	Specifica i criteri per il numero minimo di cifre nella password.
`passwords min-special-chars 1`	Specifica i criteri per il numero minimo di caratteri speciali nella password.
`passwords min-uppercase-chars 1`	Specifica i criteri per il numero minimo di lettere maiuscole nella password.
`show passwords`	Visualizza i criteri che sono configurati.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

3.5 LDAP

Gli amministratori del server gestiscono le Active Directory che contengono le credenziali di accesso dell'utente per le applicazioni utilizzate nell'ambiente di ufficio. La Active Directory ha una struttura gerarchica e contiene i nomi utente, le password e i livelli di autorizzazione di lettura/scrittura consentiti per ciascun utente.

Questo dispositivo utilizza il Protocollo LDAP (Lightweight Directory Access Protocol) per recuperare le informazioni di accesso dell'utente e i livelli di autorizzazione da una Active Directory. Ciò consente di utilizzare un sistema di "single sign on" per i dispositivi di rete. Il recupero delle credenziali di accesso dell'utente da una Active Directory consente all'utente di accedere utilizzando le stesse credenziali di accesso che utilizza nell'ambiente di ufficio.

Quando inizia una sessione LDAP, il dispositivo contatta il Directory System Agent (DSA) per interrogare la Active Directory di un server LDAP. Se il server trova più voci per un utente nella Active Directory, il server invia il livello di autorizzazione più elevato trovato. Il DSA resta in ascolto per le richieste di informazioni e invia le risposte sulla porta TCP `389` per LDAP o sulla porta TCP `636` per LDAP tramite SSL (LDAPS). Client e server codificano le richieste e le risposte LDAPS utilizzando il sistema Basic Encoding Rules (BER). Il dispositivo apre un nuovo collegamento per ogni richiesta e lo chiude dopo aver ricevuto una risposta dal server.

Il dispositivo consente di caricare un certificato CA per convalidare il server per sessioni Secure Socket Level (SSL) e Transport Layer Security (TLS). In questo contesto, il certificato per le sessioni TLS è opzionale.

Il dispositivo è in grato di salvare nella memoria cache le credenziali di accesso per fino a 1024 utenti. Se i server active directory non sono raggiungibili, gli utenti possono comunque eseguire l'accesso utilizzando le proprie credenziali di accesso di ufficio.

3.5.1 Coordinamento con l'amministratore del server

Per configurare la funzione *LDAP* è necessario che l'amministratore di rete richieda all'amministratore del server le seguenti informazioni:

- Il nome del server o l'indirizzo IP
- La posizione della Active Directory sul server
- Il tipo di collegamento utilizzato
- La porta TCP in ascolto
- Se necessario, la posizione del certificato CA
- Il nome dell'attributo contenente il nome di accesso dell'utente
- I nomi degli attributi contenenti i livelli di autorizzazione dell'utente

L'amministratore del server può assegnare i livelli di autorizzazione individualmente utilizzando un attributo come `description`, oppure ad un gruppo utilizzando l'attributo `memberOf`. Nella finestra di dialogo *Device Security > LDAP > Role Mapping* specificare quali attributi ricevono i diversi livelli di autorizzazione.

È inoltre possibile recuperare il nome degli attributi contenenti il nome di accesso dell'utente e i livelli di autorizzazione utilizzando un browser LDAP, come JXplorer o Softerra.

3.5.2 Configurazione esemplificativa

Il dispositivo è in grado di stabilire un collegamento crittografato ad un server locale utilizzando solo il nome del server o ad un server di una rete diversa utilizzando un indirizzo IP. L'amministratore del server utilizza gli attributi per individuare le credenziali di accesso di un utente e assegnare i livelli di autorizzazione individuali e di gruppo.

Utilizzando le informazioni ricevute dall'amministratore del server, specificare quali attributi nella Active Directory contengono le credenziali di accesso e il livello di atuorizzazione dell'utente. Il dispositivo confronta poi le credenziali di accesso dell'utente con i livelli di autorizzazione specificati nel dispositivo e consente all'utente di accedere al livello di autorizzazione assegnato.

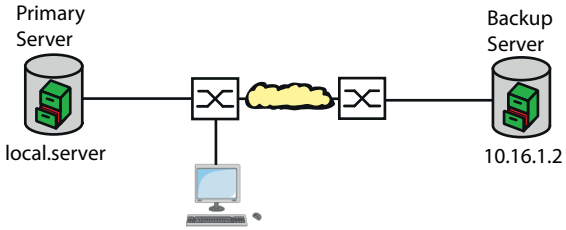


Figura 18: Configurazione esemplificativa LDAP

Per questo esempio l'amministratore del server ha inviato le seguenti informazioni:

Informazioni	Primary Server	Backup Server
Il nome del server o l'indirizzo IP	`local.server`	`10.16.1.2`
La posizione della Active Directory sul server	`Paese/Città/Utente`	`Paese/Società/Utente`
Il tipo di collegamento utilizzato	`TLS` (con certificato)	`SSL`
L'amministratore del server ha inviato il certificato CA tramite un'e-mail.	Certificato CA per server primario salvato localmente	Certificato CA per server di backup salvato localmente
La porta TCP in ascolto	`389 (tls)`	`636 (ssl)`
Nome dell'attributo contenente il nome di accesso dell'utente	`userPrincipalName`	`userPrincipalName`
I nomi degli attributi contenenti i livelli di autorizzazione dell'utente	`OPERATOR` `ADMINISTRATOR`	`OPERATOR` `ADMINISTRATOR`

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Authentication List*.
- ☐ Per configurare il dispositivo in modo che recuperi le credenziali di accesso dell'utente utilizzando l'interfaccia grafica utente, dalla Active Directory prima specificare per l'elenco `defaultLoginAuthList` il valore `ldap` nella colonna *Policy 1*.
- ☐ Aprire la finestra di dialogo *Device Security > LDAP > Configuration*.
- ☐ Il dispositivo consente di specificare l'intervallo di tempo nel quale le credenziali di accesso dell'utente sono salvate nella cache. Per salvare nella cache le credenziali di accesso dell'utente per un giorno, nel riquadro *Configuration*, campo *Client cache timeout [min]* inserire il valore `1440`.

- La voce *Bind user* è opzionale. Se specificato, gli utenti eseguono l'accesso inserendo solo il proprio nome utente. L'utente del servizio può essere chiunque abbia le credenziali di accesso elencate nella Active Directory con l'attributo specificato nella colonna *User name attribute*. Nella colonna *Bind user*, immettere il nome utente e il dominio.
- Il *Base DN* è una combinazione della componente dominio (dc) e dell'unità organizzativa (ou). Il *Base DN* consente al dispositivo di localizzare un server in un dominio (dc) e trovare la Active Directory (ou). Specificare la posizione della Active Directory. Nella colonna *Base DN*, specificare il valore `ou=Users,ou=City,ou=Country,dc=server,dc=local`.
- Nella colonna *User name attribute* immettere il valore `userPrincipalName` per specificare l'attributo in base al quale l'amministratore del server elenca gli utenti.

Il dispositivo utilizza un certificato CA per verificare il server.

- Se il certificato si trova sul PC o su un'unità di rete, trascinare il certificato nell'area . In alternativa, fare clic sull'area per selezionare il certificato.
- Per trasferire il certificato CA sul dispositivo, fare clic sul pulsante *Start*.
- Per aggiungere una voce tabella, fare clic sul pulsante .
- Per specificare una descrizione, immettere il valore `Primary AD Server` nella colonna *Description*.
- Per specificare il nome del server e il dominio del server primario, nella colonna *Address* immettere il valore `local.server`.
- Il server primario comunica utilizzando la porta TCP `389`, che è il valore di default *Destination TCP port*.
- Il server primario utilizza TLS per crittografare la comunicazione e un certificato CA per convalidare il server. Nella colonna *Connection security*, specificare il valore `startTLS`.
- Per attivare la voce, selezionare la casella di spunta nella colonna *Active*.
- Utilizzando le informazioni ricevute dall'amministratore del server per il server di backup, aggiungere, configurare e attivare un'altra riga.

- Aprire la finestra di dialogo *Device Security > LDAP > Role Mapping*.
- Per aggiungere una voce tabella, fare clic sul pulsante .

Se un utente esegue l'accesso con LDAP configurato e abilitato, il dispositivo interroga la Active Directory per le credenziali di accesso dell'utente. Se il dispositivo trova un nome utente e la password è corretta, il dispositivo cerca il valore specificato nella colonna *Type*. Se il dispositivo trova l'attributo e il testo nella colonna *Parameter* corrisponde al testo nella Active Directory, il dispositivo consente all'utente di accedere con il livello di autorizzazione assegnato. Se il valore `attribute` è specificato nella colonna *Type*, specificare il valore nella colonna *Parameter* nella seguente forma: `attributeName=attributeValue`.

- Nella colonna *Role* immettere il valore `operator` per specificare il ruolo utente.
- Per attivare la voce, selezionare la casella di spunta nella colonna *Active*.
- Fare clic sul pulsante .
  La finestra di dialogo mostra la finestra *Create*.
  Immettere i valori ricevuti dall'amministratore del server per il ruolo `administrator`.
  Per attivare la voce, selezionare la casella di spunta nella colonna *Active*.
- Aprire la finestra di dialogo *Device Security > LDAP > Configuration*.
- Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.

La seguente tabella descrive come configurare la funzione *LDAP* nel dispositivo utilizzando la Command Line Interface. La tabella indica i comandi per `Index 1`. Per configurare `Index 2` utilizzare gli stessi comandi e sostituire le informazioni appropriate.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`ldap cache-timeout 1440`	Specificare al dispositivo di svuotare la memoria non volatile dopo un giorno.
`ldap client server add 1 local.server port 389`	Aggiungere una connessione all'autenticazione remota client-server con il nome host `local.server` e la porta UDP `389`.
`ldap client server modify 1 security startTLS`	Specificare il tipo di sicurezza utilizzata per la connessione.
`ldap client server modify 1 description Primary_AD_Server`	Specificare il nome di configurazione della voce.
`ldap basedn ou=Users,ou=City,ou=Country,dc=server, dc=local`	Specificare il Base Domain Name utilizzato per trovare la Active Directory sul server.
`ldap search-attr userPrincipalName`	Specificare l'attributo da cercare nella Active Directory che contiene le credenziali di accesso degli utenti.
`ldap bind-user user@company.com`	Specificare il nome e il dominio dell'utente del servizio.
`ldap bind-passwd Ur-123456`	Specificare la password dell'utente del servizio.
`ldap client server enable 1`	Specificare il nome e il dominio dell'utente del servizio.
`ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR`	Aggiungere una voce di mappatura dei ruoli per l'autenticazione remota per il ruolo `Operator`. Mappare il ruolo `operator` all'attributo contenente la parola `OPERATOR`.
`ldap mapping enable 1`	Abilitare la voce di mappatura del ruolo per l'autenticazione remota.
`ldap operation`	Abilitare la funzione di autenticazione remota.

3.6 Accesso SNMP

Il protocollo SNMP consente di lavorare con un sistema di gestione di rete, per monitorare il dispositivo tramite la rete e modificare le relative impostazioni.

3.6.1 Accesso SNMPv1/v2

Utilizzando SNMPv1 o SNMPv2 il sistema di gestione di rete e il dispositivo comunicano in modo non crittografato. Ogni pacchetto SNMP contiene il nome della comunità in testo non crittografato e l'indirizzo IP del mittente.

I nomi della community `user` per gli accessi in lettura e `admin` per gli accessi in scrittura sono preimpostati nel dispositivo. Se SNMPv1/v2 è abilitato, il dispositivo consente l'accesso al dispositivo a chiunque conosca il nome della community.

Rende più difficili gli accessi indesiderati al dispositivo. A tale scopo, eseguire i seguenti passaggi:

- ☐ Modificare i nomi della comunità di default nel dispositivo.
  Trattare con discrezione i nomi della community.
  Chiunque conosca il nome della comunità per l'accesso in scrittura può modificare le impostazioni del dispositivo.
- ☐ Specificare un nome community differente rispetto a quello per l'accesso in lettura/scrittura.
- ☐ Utilizzare SNMPv1 oppure SNMPv2 solo in ambienti protetti da intercettazione. I protocolli non utilizzano la crittografia.
- ☐ Raccomandiamo di utilizzare SNMPv3 e disabilitare l'accesso tramite SNMPv1 ed SNMPv2 nel dispositivo.

3.6.2 Accesso SNMPv3

Utilizzando SNMPv3 il sistema di gestione di rete e il dispositivo comunicano in modo non crittografato. Il sistema di gestione della rete si autentica con il dispositivo utilizzando le credenziali di accesso di un utente. Il prerequisito per l'accesso SNMPv3 è che nel sistema di gestione di rete si utilizzano le stesse impostazioni definite nel dispositivo.

Il dispositivo consente di specificare i parametri *SNMP auth type* e *SNMP encryption type* individualmente in ogni account utente.

Quando si configura un nuovo account utente nel dispositivo, i parametri sono preimpostati di modo che il sistema di gestione di rete ConneXium Network Manager raggiunga il dispositivo immediatamente.

Gli account utente configurati nel dispositivo utilizzano le stesse password nell'interfaccia grafica utente, nella Command Line Interface, e per l'SNMPv3.

Per adattare i parametri SNMPv3 delle impostazioni account utente alle impostazioni nel sistema di gestione di rete, effettuare i seguenti passi:

- ☐ Aprire la finestra di dialogo *Device Security > User Management*.

La finestra di dialogo visualizza gli account utenti che sono configurati.

- ☐ Fare clic sulla riga dell'account utente rilevante nel campo *SNMP auth type*. Selezionare l'impostazione desiderata.
- ☐ Fare clic sulla riga dell'account utente rilevante nel campo *SNMP encryption type*. Selezionare l'impostazione desiderata.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`users snmpv3 authentication <user> md5 | sha1`	Assegnazione del protocollo HMAC-MD5 o HMACSHA per richieste di autenticazione all'account utente `<user>`.
`users snmpv3 encryption <user> des | aescfb128 | none`	Assegna l'algoritmo DES o AES-128 all'account utente `<user>`. Con questo algoritmo il dispositivo crittografa le richieste di autenticazione. Il valore `none` rimuove la crittografia.
`show users`	Visualizzare gli account utenti che sono state configurati.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

3.7 Accesso Out of Band

Il dispositivo è dotato di una porta separata che consente di accedere alla gestione del dispositivo out-of-band. In presenza di un carico in banda elevato sulle porte switching, è ancora possibile utilizzare questa porta separata per accedere alla gestione del dispositivo.

Il prerequisito è il collegamento della network management station direttamente alla porta USB. Quando si utilizza Microsoft Windows, installare il driver RNDIS, ove necessario. Dopo averla collegata, la network management station può comunicare con la gestione del dispositivo tramite un collegamento alla rete virtuale.

Nell'impostazione di default, è possibile accedere alla gestione del dispositivo attraverso questa porta utilizzando i seguenti parametri IP:
- *IP address* `91.0.0.100`
- *Netmask* `255.255.255.0`

Il dispositivo consente di accedere alla gestione del dispositivo utilizzando i protocolli seguenti:
- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP

3.7.1 Definizione dei parametri IP

Quando si collega la management station tramite la porta USB, il dispositivo assegna l'indirizzo IP dell'interfaccia di rete USB, aumentato di 1, alla management station (`91.0.0.101` nell'impostazione di default). Il dispositivo consente di modificare i parametri IP per adattare il dispositivo ai requisiti del proprio ambiente.

Verificare che la sottorete IP di questa interfaccia di rete non si stia sovrapponendo ad alcuna sottorete collegata a un'altra interfaccia del dispositivo:
- Interfaccia di gestione

Se la network management station accede alla gestione del dispositivo attraverso la porta USB, il dispositivo scollega l'interfaccia grafica utente e la Command Line Interface subito dopo aver eseguito le modifiche.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Out of Band over USB*.
- ☐ Sovrascrivere l'indirizzo IP nel riquadro *IP parameter*, campo *IP address*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

```
enable
```
Passare alla modalità Privileged EXEC.

```
network usb parms 192.168.1.1
255.255.255.0
```
Definire l'indirizzo IP `192.168.1.1` e la maschera di rete `255.255.255.0` per l'interfaccia di rete USB.

```
show network usb
```
Visualizzare le impostazioni dell'interfaccia di rete USB.

```
Out-of-band USB management settings
-----------------------------------
Management operation.....................enabled
IP address..............................192.168.1.1
Subnet mask.............................255.255.255.0
Host MAC address........................64:60:38:1f:85:85
Device MAC address......................64:60:38:1f:85:86
```

```
save
```
Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

3.7.2 Disabilitare l'interfaccia di rete USB

Nell'impostazione di default, l'interfaccia di rete USB è abilitata. Se non si desidera che qualcuno acceda alla gestione del dispositivo attraverso la porta USB, il dispositivo consente di disabilitare l'interfaccia di rete USB.

Se la network management station accede alla gestione del dispositivo attraverso la porta USB, il dispositivo scollega l'interfaccia grafica utente e la Command Line Interface subito dopo aver eseguito le modifiche.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Out of Band over USB*.
- ☐ Per disabilitare l'interfaccia di rete USB, selezionare il pulsante di opzione *Off* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

```
enable
```
Passare alla modalità Privileged EXEC.

```
no network usb operation
```
Disabilitare l'interfaccia di rete USB.

```
Out-of-band USB management settings
-----------------------------------
Management operation.....................disabled
IP address..............................192.168.1.1
Subnet mask.............................255.255.255.0
Host MAC address........................64:60:38:1f:85:85
Device MAC address......................64:60:38:1f:85:86
```

```
save
```
Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

4 Sincronizzazione in rete dell'orario di sistemad

Molte applicazioni si basano su un orario di sistema che è il più corretto possibile. L'accuratezza necessaria, e quindi la deviazione consentita dall'ora attuale, dipende dall'area di applicazione.

I campi di applicazione possono essere:
- Voci di registro
- Time stamp dei dati di produzione
- Controllo di processo

Il dispositivo consente la sincronizzazione dell'ora sulla rete utilizzando le seguenti opzioni:
- Il Simple Network Time Protocol (SNTP) è una semplice soluzione per requisiti di bassa accuratezza. In condizioni ideali, SNTP raggiunge un'accuratezza nell'intervallo di millisecondi. L'accuratezza dipende dal ritardo del segnale.
- L'IEEE 1588 con il Precision Time Protocol (PTP) raggiunge un livello di precisione nell'ordine delle frazioni di microsecondi. Questo metodo è adatto anche per le applicazioni esigenti, fino al controllo di processo incluso.

Se i dispositivi coinvolti supportano il protocollo PTP, questo è la scelta migliore. Il PTP è più accurato, dispone di metodi avanzati di correzione degli errori e causa un ridotto carico della rete. L'implementazione del PTP è relativamente semplice.

Nota: Secondo gli standard PTP e SNTP, entrambi i protocolli operano in parallelo nella stessa rete. Tuttavia, poiché entrambi i protocolli influenzano l'orario di sistema del dispositivo, possono verificarsi situazioni in cui entrano in conflitto l'uno con l'altro.

4.1 Impostazioni di base

Nella finestra di dialogo *Time > Basic Settings*, si specificano le impostazioni generali per l'ora.

4.1.1 Impostazione dell'ora

Quando non è disponibile alcuna origine ora di riferimento, è possibile impostare l'orario nel dispositivo.

Dopo un avvio a freddo o un riavvio, se non è disponibile un orologio con orario reale oppure l'orologio con orario reale contiene un orario non valido, il dispositivo inizializza l'orologio con il valore 1 gennaio 00:00h. Dopo il disinserimento dell'alimentazione di tensione, il dispositivo effettua il buffer delle impostazioni del real time clock fino a 24 ore.

In alternativa, si configurano le impostazioni nel dispositivo in modo che ottenga automaticamente l'ora corrente da un clock PTP o da un server SNTP.

In alternativa, si configurano le impostazioni nel dispositivo in modo che ottenga automaticamente l'ora corrente da un server SNTP.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Time > Basic Settings*.
- ▶ Il campo *System time (UTC)* visualizza l'attuale UTC (Universal Time Coordinated) del dispositivo. L'UTC è l'ora che fa riferimento al tempo coordinato universale. L'UTC è lo stesso in tutto il mondo e non tiene in considerazione i cambi di orario locali.
- ▶ L'ora nel campo *System time* deriva dal valore *System time (UTC)* più il valore *Local offset [min]* ed un possibile cambio dovuto all'ora legale.

Nota: Il PTP invia il tempo atomico internazionale (TAI). Al 1° luglio 2020, il tempo TAI ha 37 secondi di anticipo rispetto al tempo UTC. Quanto la fonte orario di riferimento PTP dell'offset UTC è impostata correttamente il dispositivo corregge automaticamente tale differenza sullo schermo, nel campo *System time (UTC)*.

- ☐ Per indurre il dispositivo ad applicare l'orario del proprio PC al campo *System time*, fare clic sul pulsante *Set time from PC*.
  Sulla base del valore nel campo *Local offset [min]*, il dispositivo calcola l'orario nel campo *System time (UTC)*: Il valore *System time (UTC)* deriva dal valore *System time* meno il valore *Local offset [min]* ed un possibile cambio dovuto all'ora legale.
- ▶ Il campo *Time source* visualizza l'origine dei dati sull'orario. Il dispositivo seleziona la fonte automaticamente con la maggiore precisione possibile.
  La fonte è inizialmente `local`.
  Se SNTP è attivo e il dispositivo riceve un pacchetto SNTP valido, il dispositivo imposta la propria fonte orario su `sntp`.
  Se il PTP è attivo e il dispositivo riceve un pacchetto PTP valido, il dispositivo imposta la propria fonte orario su `ptp`. Il dispositivo dà priorità al PTP rispetto al SNTP.
- ▶ Il valore *Local offset [min]* specifica la differenza di orario tra ora locale e *System time (UTC)*.
- ☐ Per indurre il dispositivo a stabilire il fuso orario del proprio PC, fare clic sul pulsante *Set time from PC*. Il dispositivo calcola la differenza dell'ora locale da UTC e immette la differenza nel campo *Local offset [min]*.

Nota: Il dispositivo offre l'opzione di ottenere l'offset locale da un server DHCP.

- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	Impostare l'orario di sistema del dispositivo.
`clock timezone offset <-780..840>`	Immettere la differenza tra l'ora locale e l'ora UTC ricevuta in minuti.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

4.1.2 Cambio automatico all'ora legale

Quando si utilizza il dispositivo in un fuso orario che prevede il cambio all'ora legale, si imposta il cambio automatico all'ora legale nella scheda *Daylight saving time*.

Se è abilitata l'ora legale, il dispositivo imposta l'orario di sistema locale 1 ora in avanti all'inizio dell'ora legale. Al termine dell'ora legale, il dispositivo imposta nuovamente l'orario di sistema locale 1 ora indietro. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Time > Basic Settings*, scheda *Daylight saving time*.
- ☐ Per selezionare un profilo preimpostato per l'inizio e la fine dell'ora legale, fare clic sul pulsante *Profile...* nel riquadro *Operation*.
- ☐ Se non è disponibile alcun profilo di ora legale corrispondente, per specificare quando viene effettuato il cambio di orario, utilizzare i campi *Summertime begin* e *Summertime end*. Per entrambi i punti nel tempo, si specificano il mese, la settimana in questo mese, il giorno della settimana e l'ora del giorno.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`clock summer-time mode <disable|recurring|eu|usa>`	Configurare il cambio automatico all'ora legale: abilitare/disabilitare o attivare con un profilo.
`clock summer-time recurring start`	Inserire l'ora di inizio del cambio.
`clock summer-time recurring end`	Inserire l'ora di fine del cambio.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

4.2 SNTP

Il Simple Network Time Protocol (SNTP) consente di sincronizzare l'orario di sistema nella rete. Il dispositivo supporta il client SNTP e la funzione di server SNTP.

Il server SNTP mette a disposizione l'UTC (Universal Time Coordinated). L'UTC è l'ora che fa riferimento al tempo coordinato universale. L'UTC è lo stesso in tutto il mondo e ignora i cambi di orario locali.

SNTP è una versione semplificata di NTP (Network Time Protocol). I pacchetti di dati sono identici con SNTP e NTP. Perciò, i server NTP ed SNTP fungono da fonte orario per i client SNTP.

Nota: Le indicazioni fornite in questo capitolo in merito a server SNTP esterni sono quindi valide anche per server NTP.

SNTP conosce i seguenti modi operativi per la trasmissione dell'orario :

- *Unicast*
  Nel modo operativo *Unicast*, un client SNTP invia richieste ad un server SNTP e si aspetta una risposta da questo server.
- *Broadcast*
  Nel modo operativo *Broadcast*, un server SNTP invia messaggi SNTP alla rete a specifici intervalli. I client SNTP ricevono questi messaggi SNTP e li valutano.

In un ambiente IPv6, la modalità operativa *Broadcast* funziona come segue:

- Il client SNTP ascolta solo i messaggi del server SNTP che hanno l'indirizzo IPv6 *Multicast* impostato su `ff05::101` come indirizzo IPv6 di destinazione.
- Il server SNTP invia solo messaggi SNTP all'indirizzo *Multicast*`ff05::101`. Il server SNTP non invia messaggi SNTP con l'indirizzo link-local come indirizzo IPv6 sorgente.

Tabella 16:Classi di indirizzo IPv4 target per modo operativo Broadcast

Indirizzo IPv4 di destinazione	Invia pacchetti SNTP a
`0.0.0.0`	Nessuno
`224.0.1.1`	Indirizzo *Multicast* per messaggi SNTP
`255.255.255.255`	Indirizzo *Broadcast*

Nota: Un server SNTP in modo operativo *Broadcast* risponde inoltre a richieste dirette da client SNTP, utilizzando *Unicast*. Per contro, i client SNTP lavorano in modo operativo *Unicast* oppure *Broadcast*.

4.2.1 Preparazione

Eseguire i seguenti passaggi:

- ☐ Per avere una panoramica sulla trasmissione dell'orario, definire un piano di rete che comprenda i dispositivi inclusi nell'SNTP
  In fase di pianificazione, tenere presente che l'accuratezza dell'orario dipende dai ritardi dei messaggi SNTP. Per minimizzare i ritardi e la relativa variazione, posizionare un server SNTP in ogni segmento di rete. Ciascuno di questi server SNTP sincronizza il suo orario di sistema come un client SNTP con il server SNTP principale (cascata SNTP). Il server SNTP in posizione più elevata nella cascata SNTP ha l'accesso più diretto alla fonte orario di riferimento.

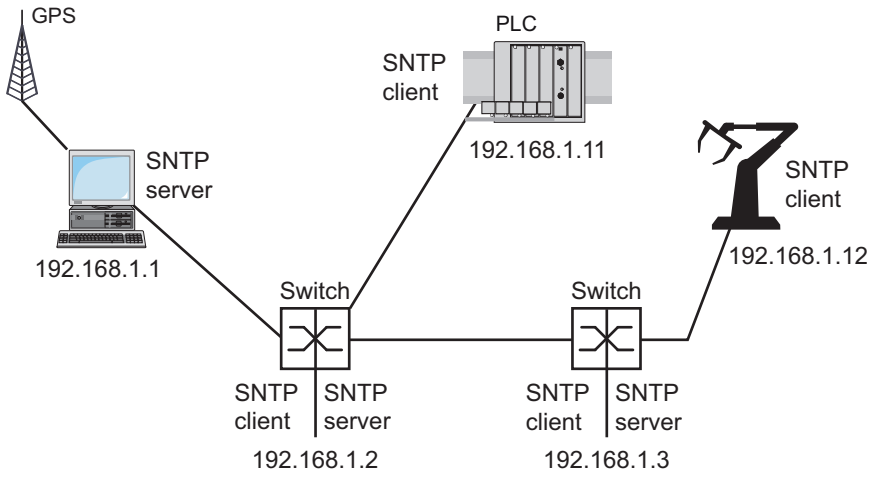


Figura 19: Esempio di cascata SNTP

Nota: Per una distribuzione precisa dell'orario, tra server SNTP e client SNTP si utilizzano preferibilmente componenti di rete (router e switch) che inoltrano i pacchetti SNTP con un tempo di trasmissione limitato e uniforme (latenza).

- Un client SNTP invia le sue richieste fino a 4 server SNTP configurati. Se non c'è risposta dal 1° server SNTP, il client SNTP invia le sue richieste al 2° server SNTP. Se anche questa richiesta non ha successo, invia la richiesta al 3° e infine al 4° server SNTP. Se nessuno di questi server SNTP risponde, il client SNTP perde la sua sincronizzazione. Il client SNTP invia ciclicamente richieste ad ogni server SNTP finché un server fornisce un orario valido.

Nota: Il dispositivo offre l'opzione di ottenere una lista di indirizzi IP server SNTP da un server DHCP.

- Se non è disponibile alcuna fonte orario di riferimento, definire un dispositivo con un server SNTP come fonte orario di riferimento. Regolare l'orario di sistema a intervalli regolari.

4.2.2 Definizione delle impostazioni del client SNTP

Come un client SNTP, il dispositivo ottiene le informazioni sull'orario dal server SNTP o NTP e sincronizza l'orologio di sistema in modo corrispondente. A tale scopo, eseguire i seguenti passaggi:

- Aprire la finestra di dialogo *Time > SNTP > Client*.
- Impostare il modo operativo SNTP.
  Nel riquadro *Configuration*, selezionare uno dei seguenti valori nel campo *Mode*:
  - `unicast`
    Il dispositivo invia richieste a un server SNTP e si aspetta una risposta da questo server.
  - `broadcast`
    Il dispositivo attende messaggi *Broadcast* o *Multicast* da server SNTP sulla rete.
- Per sincronizzare l'orario una sola volta, selezionare la casella di spunta *Disable client after successful sync*.
  Dopo la sincronizzazione , il dispositivo disabilita la funzione *SNTP Client*.
- La tabella visualizza il server SNTP a cui il client SNTP invia una richiesta nel modo operativo *Unicast*. La tabella contiene fino a 4 definizioni server SNTP.
- Per aggiungere una voce tabella, fare clic sul pulsante  .
- Specificare i dati di connessione del server SNTP.
- Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .
- Il campo *State* visualizza lo stato corrente della funzione *SNTP Client*.

Tabella 17:Impostazioni del client SNTP per l'esempio

Dispositivo	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Funzione *SNTP Client*	`Off`	`On`	`On`	`On`	`On`

Tabella 17:Impostazioni del client SNTP per l'esempio (cont

Dispositivo	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Configuration: *Mode*	unicast	unicast	unicast	unicast	unicast
Request interval [s]	30	30	30	30	30
Indirizzo(i) *SNTP Server*	–	192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.3 192.168.1.2 192.168.1.1

4.2.3 Specifica delle impostazioni server SNTP

Quando il dispositivo funziona come un server SNTP, fornisce l'orario di sistema in tempo coordinato universale (UTC) nella rete. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Time > SNTP > Server*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Per abilitare il modo operativo *Broadcast*, selezionare il pulsante di opzione *Broadcast admin mode* nel riquadro *Configuration*.
  Nel modo operativo *Broadcast*, il server SNTP invia messaggi SNTP alla rete a specifici intervalli. Il server SNTP risponde inoltre a richieste dai client SNTP nel modo operativo *Unicast*.
  - ☐ Nel campo *Broadcast destination address*, si imposta l'indirizzo IPv4 a cui il server SNTP invia i pacchetti SNTP. Impostare l'indirizzo *Broadcast* o un indirizzo *Multicast*.
    In un ambiente IPv6 non è possibile impostare l'indirizzo IPv6 a cui il server SNTP invia i pacchetti SNTP. Il server SNTP utilizza l'indirizzo *Multicast*`ff05::101` come indirizzo IPv6 di destinazione.
  - ☐ Nel campo *Broadcast UDP port*, si specifica il numero di porta UDP a cui il server SNTP invia i pacchetti SNTP in modo operativo *Broadcast*.
  - ☐ Nel campo *Broadcast VLAN ID*, si specifica l'ID della VLAN a cui il server SNTP invia i pacchetti SNTP nel modo operativo *Broadcast*.
  - ☐ Nel campo *Broadcast send interval [s]*, si immette l'intervallo di tempo in base a cui il server SNTP del dispositivo invia a SNTP pacchetti *Broadcast*.

Nota: Ad eccezione del campo *Broadcast destination address*, le impostazioni restanti si applicano ai server SNTP IPv4 come a quelli IPv6.

- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.
- ▶ Il campo *State* visualizza lo stato corrente della funzione *SNTP Server*.

Tabella 18:Impostazioni per l'esempio

Dispositivo	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Funzione *SNTP Server*	*On*	*On*	*On*	*Off*	*Off*
UDP port	123	123	123	123	123
Broadcast admin mode	non selezionato	non selezionato	non selezionato	non selezionato	non selezionato
Broadcast destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast UDP port	123	123	123	123	123

Tabella 18:Impostazioni per l'esempio (cont

Dispositivo	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Broadcast VLAN ID	1	1	1	1	1
Broadcast send interval [s]	128	128	128	128	128
Disable server at local time source	non selezionato	non selezionato	non selezionato	non selezionato	non selezionato

4.3 PTP

Affinché le applicazioni a controllo LAN funzionino senza latenza è necessaria una gestione dell'orario precisa. Con il PTP (Precision Time Protocol), l'IEEE 1588 descrive un metodo che consente di sincronizzare in modo preciso i clock della rete.

Il PTP consente la sincronizzazione con una precisione di appena 100 ns. Il PTP utilizza Multicasts per i messaggi di sincronizzazione, mantenendo limitato il carico della rete.

4.3.1 Tipi di clock

Il PTP definisce i ruoli "master" e "slave" per i clock della rete:
- Un master clock (fonte orario di riferimento) distribuisce il suo orario.
- Uno slave clock si sincronizza con il segnale orario ricevuto dal master clock.

Boundary clock

Il tempo di trasmissione (latenza) nei router e negli switch ha un effetto misurabile sulla precisione della trasmissione oraria. Per correggere queste variazioni, il PTP definisce quelli che sono detti boundary clock.

In un segmento di rete, un boundary clock è la fonte orario di riferimento (master clock) con cui si sincronizzano gli slave clock subordinati. In genere i routere e gli switch svolgono il ruolo di boundary clock.

Il boundary clock ottiene a sua volta l'orario da una fonte orario di riferimento di livello superiore (Grandmaster).

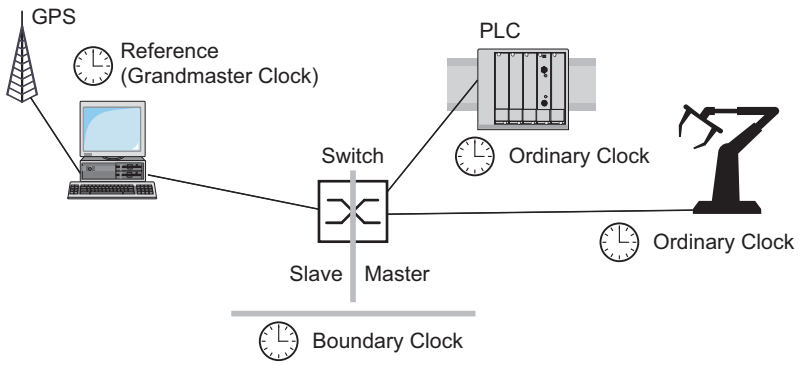


Figura 20: Posizione di un boundary clock in una rete

Transparent Clock

Gli switch in genere assumono il ruolo Transparent Clock per consentire un'elevata precisione nelle cascate. Il Transparent Clock è uno Slave clock che corregge la sua trasmissione oraria quando inoltra i messaggi di sincronizzazione ricevuti.

Ordinary Clock

Il PTP designa il clock di un dispositivo finale come "Ordinary Clock". Un Ordinary Clock funge da master clock oppure da slave clock.

4.3.2 Algoritmo Best Master Clock

I dispositivi che partecipano al PTP designano un dispositivo nella rete come fonte orario di riferimento (Grandmaster). In questo caso viene utilizzato l'algoritmo "Best Master Clock", che stabilisce la precisione dei clock disponibili nella rete.

L'algoritmo "Best Master Clock" valuta i seguenti criteri:
- *Priority 1*
- *Clock class*
- *Clock accuracy*
- *Clock variance*
- *Priority 2*

L'algoritmo valuta prima il valore nel campo *Priority 1* dei dispositivi coinvolti. Il dispositivo con il valore inferiore nel campo *Priority 1* diventa la fonte orario di riferimento (Grandmaster). Se il valore è uguale per diversi dispositivi, l'algoritmo applica il criterio successivo. Se anche questo è uguale, l'algoritmo applica l'ulteriore criterio successivo. Se questi criteri sono uguali per diversi dispositivi, il dispositivo fonte orario di riferimento (Grandmaster) viene selezionato in base al valore inferiore nel campo *Clock identity*.

Nelle impostazioni del boundary clock, il dispositivo consente di specificare individualmente i valori per *Priority 1* e *Priority 2*. In questo modo è possibile influenzare quale dispositivo sarà la fonte orario di riferimento (Grandmaster) nella rete.

4.3.3 Misurazione del ritardo

Il ritardo dei messaggi di sincronizzazione tra i dispositivi influenza la precisione. La misurazione del ritardo consente ai dispositivi di considerare il ritardo medio.

Il PTP versione 2 offre i seguenti metodi di misurazione del ritardo:
- `e2e` (End to End)
  Lo slave clock misura il ritardo dei messaggi di sincronizzazione con il master clock.
- `e2e-optimized`
  Lo slave clock misura il ritardo dei messaggi di sincronizzazione con il master clock.
  Questo metodo è disponibile solo per i transparent clock. Il dispositivo inoltra i messaggi di sincronizzazione inviati utilizzando Multicast solo al master clock, mantenendo basso il carico della rete. Se il dispositivo riceve un messaggio di sincronizzazione da un altro master clock, inoltra i messaggi di sincronizzazione solo a questa porta nuova.
  Se il dispositivo non conosce un master clock, inoltra i messaggi di sincronizzazione a tutte le porte.
- `p2p` (Peer to Peer)
  Lo slave clock misura il ritardo dei messaggi di sincronizzazione con il master clock.
  Inoltre, il master clock misura il ritardo verso ogni slave clock, anche attraverso le porte bloccate. A tale scopo è necessario che il master clock e lo slave clock supportino il Peer-to-Peer (`p2p`).
  In caso di interruzione di un anello ridondante, ad esempio, lo slave clock diventa il master clock e viceversa. Questo scambio avviene senza perdita di precisione, perché i clock conoscono già il ritardo nella direzione opposta.

4.3.4 Domini PTP

Il dispositivo trasmette i messaggi di sincronizzazione solo da e verso i dispositivi nello stesso dominio PTP. Il dispositivo consente di impostare individualmente il dominio per il boundary clock e per il transparent clock.

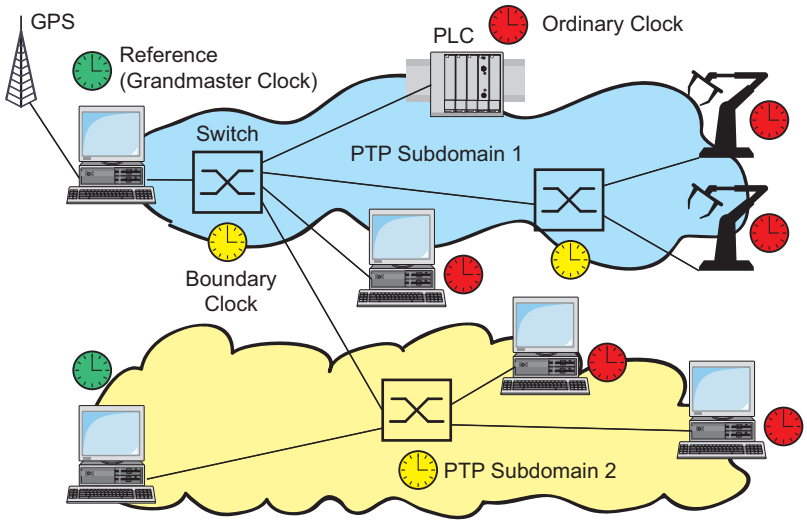


Figura 21: Esempio di domini PTP

4.3.5 Utilizzare il PTP

Per sincronizzare i clock in modo preciso con il PTP, utilizzare solo gli switch con un boundary clock o un transparent clock come nodi.

Eseguire i seguenti passaggi:

- ☐ Per avere una panoramica della distribuzione dei clock, definire un piano di rete che comprenda i dispositivi inclusi nel PTP.
- ☐ Specificare il ruolo per ciascuno switch coinvolto (boundary clock o transparent clock). Nel dispositivo questa impostazione è detta *PTP mode*.

Tabella 19:Impostazioni possibili per la modalità PTP

Modalità PTP	Applicazione
`v2-boundary-clock`	In quanto boundary clock, il dispositivo distribuisce i messaggi di sincronizzazione agli slave clock nel segmento di rete subordinato. Il boundary clock ottiene a sua volta l'orario da una fonte orario di riferimento di livello superiore (Grandmaster).
`v2-transparent-clock`	In quanto transparent clock, il dispositivo inoltra i messaggi di sincronizzazione ricevuti dopo che sono stati corretti per il ritardo del transparent clock.

- ☐ Abilitare il PTP su tutti gli switch coinvolti.
  Il PTP è quindi configurato su una base prevalentemente automatica.
- ☐ Abilitare il PTP sui dispositivi finali.
- ☐ Il dispositivo consente di influenzare quale dispositivo della rete viene selezionato come clock di riferimento (Grandmaster). Pertanto, modificare il valore di default nei campi *Priority 1* e *Priority 2* per il *Boundary Clock*.

5 Gestione dei profili di configurazione

Se si modificano le impostazioni del dispositivo durante il funzionamento, questo memorizza le modifiche nella propria memoria (*RAM*). Dopo un riavvio, le impostazioni vanno perse.

Per mantenere le modifiche dopo un riavvio, il dispositivo consente di salvare le impostazioni in un profilo di configurazione all'interno della memoria non-volatile (*NVM*). Per consentire il passaggio rapido ad altre impostazioni, la memoria non-volatile offre spazio di memorizzazione per più profili di configurazione.

Se è collegata una memoria esterna, il dispositivo salva automaticamente una copia del profilo di configurazione nella memoria esterna (*ENVM*). È possibile disabilitare tale funzione.

5.1 Rilevamento delle impostazioni modificate

Il dispositivo memorizza le modifiche apportate alle impostazioni durante il funzionamento nella sua memoria volatile (*RAM*). Il profilo di configurazione nella memoria non volatile (*NVM*) rimane invariato fino a quando l'utente salva espressamente le impostazioni modificate. Fino a questo momento, i profili di configurazione nella memoria e nella memoria non volatile sono diversi. Il dispositivo aiuta a rilevare le impostazioni modificate.

5.1.1 Memoria volatile (RAM) e memoria non volatile (NVM).

È possibile riconoscere quando il profilo di configurazione nella memoria volatile (*RAM*) è diverso dal profilo di configurazione "selezionato" nella memoria non volatile (*NVM*). A tale scopo, eseguire i seguenti passaggi:

- ☐ Verificare la barra di stato nella parte superiore del menu:
  - – Quando è visualizzata un'icona lampeggiante, i profili di configurazione sono differenti.
  - – Quando non è visualizzata alcuna icona, i profili di configurazione corrispondono.

Oppure:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.
- ☐ Verificare lo stato della casella di spunta nel riquadro *Information*:
  - – Se la casella di spunta non è selezionata i profili di configurazione sono differenti.
  - – Se la casella di spunta è selezionata i profili di configurazione corrispondono.

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV.....................out of sync
...
```

5.1.2 Memoria esterna (EAM) e memoria non volatile (NVM)

È possibile inoltre riconoscere quando la copia nella memoria esterna (EAM) è diversa dal profilo di configurazione nella memoria non volatile (*NVM*). A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.
- ☐ Verificare lo stato della casella di spunta nel riquadro *Information*:
  - Se la casella di spunta non è selezionata i profili di configurazione sono differenti.
  - Se la casella di spunta è selezionata i profili di configurazione corrispondono.

```
show config status

Configuration Storage sync State
--------------------------------
...
NV to EAM.................................out of sync
...
```

5.2 Salvataggio delle impostazioni

5.2.1 Salvataggio del profilo di configurazione nel dispositivo

Se si modificano le impostazioni del dispositivo durante il funzionamento, questo memorizza le modifiche nella propria memoria (RAM). Per mantenere le modifiche dopo un riavvio, salvare il profilo di configurazione nella memoria non volatile (*NVM*).

Salvataggio di un profilo di configurazione

Il dispositivo memorizza le impostazioni nel profilo di configurazione “selezionato” all'interno della memoria non volatile (*NVM*).

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.
- ☐ Verificare che il profilo di configurazione richiesto sia “Selezionato”.
  È possibile rilevare il profilo di configurazione “selezionato” in quanto la casella di spunta nella colonna *Selected* è selezionata.
- ☐ Fare clic sul pulsante  .

`show config profiles nvm`	Mostrerà i profili di configurazione contenuti nella memoria non volatile (nvm).
`enable`	Passare alla modalità Privileged EXEC.
`save`	Salvare le impostazioni nella memoria non volatile (nvm) all'interno del profilo di configurazione “selezionato”.

Copia delle impostazioni in un profilo di configurazione

Il dispositivo consente di memorizzare le impostazioni salvate nella memoria (RAM) all'interno di un profilo di configurazione diverso da quello “selezionato”. In questo modo si crea un nuovo profilo di configurazione nella memoria non volatile (*NVM*) o se ne sovrascrive uno esistente.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.
- ☐ Fare clic sul pulsante  e poi sulla voce *Save as...*.
  La finestra di dialogo mostra la finestra *Save as...*.
- ☐ Nel campo *Name*, modificare il nome del profilo di configurazione. Se si mantiene il nome proposto, il dispositivo sovrascriverà un profilo di configurazione esistente con lo stesso nome.
- ☐ Fare clic sul pulsante *Ok*.

Il nuovo profilo di configurazione è designato come “Selezionato”.

`show config profiles nvm`	Mostrerà i profili di configurazione contenuti nella memoria non volatile (`nvm`).
`enable`	Passare alla modalità Privileged EXEC.
`copy config running-config nvm profile <string>`	Salvare le impostazioni correnti nel profilo di configurazione chiamato `<string>` all'interno della memoria non volatile (`nvm`). Se presente, il dispositivo sovrascrive un profilo di configurazione con lo stesso nome. Il nuovo profilo di configurazione è designato come “Selezionato”.

Selezione di un profilo di configurazione

Quando la memoria non volatile (*NVM*) comprende più profili di configurazione, è possibile selezionare qualsiasi profilo di configurazione. Il dispositivo memorizza le impostazioni nel profilo di configurazione “selezionato”. Al riavvio, il dispositivo carica le impostazioni del profilo di configurazione “selezionato” all'interno della memoria (`RAM`).

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.

La tabella mostra i profili di configurazione presenti nel dispositivo. È possibile rilevare il profilo di configurazione “selezionato” in quanto la casella di spunta nella colonna *Selected* è selezionata.

- ☐ Nella tabella, selezionare la voce del profilo di configurazione richiesto memorizzato all'interno della memoria non volatile (*NVM*).
- ☐ Fare clic sul pulsante e poi sulla voce *Select*.

Nella colonna *Selected*, la casella di spunta del profilo di configurazione è adesso `selezionata`.

`enable`	Passare alla modalità Privileged EXEC.
`show config profiles nvm`	Mostrerà i profili di configurazione contenuti nella memoria non volatile (`nvm`).
`configure`	Passare alla modalità di configurazione.
`config profile select nvm 1`	Identificativo del profilo di configurazione. Prendere nota del nome del profilo di configurazione vicino.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

5.2.2 Salvataggio del profilo di configurazione nella memoria esterna

Quando una memoria esterna è collegata e si salva un profilo di configurazione, il dispositivo salva automaticamente una copia all'interno della *Selected external memory*. Nell'impostazione di default, la funzione è abilitata. È possibile disabilitare tale funzione.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > External Memory*.
- ☐ Selezionare la casella di spunta nella colonna *Backup config when saving* per consentire al dispositivo di salvare automaticamente una copia nella memoria esterna durante il processo di salvataggio.
- ☐ Per disattivare la funzione, deselezionare la casella di spunta nella colonna *Backup config when saving*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`config envm config-save usb`	Abilitare la funzione. Quando si salva un profilo di configurazione, il dispositivo salva una copia nella memoria esterna. `usb` = Memoria USB esterna
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

5.2.3 Eseguire il backup del profilo di configurazione su un server remoto

Il dispositivo consente di eseguire automaticamente il backup del profilo di configurazione su un server remoto. Il prerequisito è che si attivi la funzione prima di salvare il profilo di configurazione.

Dopo aver salvato il profilo di configurazione nella memoria non volatile (*NVM*), il dispositivo invia una copia all'URL specificato.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.
  Nel riquadro *Backup config on a remote server when saving*, eseguire i seguenti passaggi:
- ☐ Nel campo *URL*, specificare il server così come il percorso e il nome del file del profilo di configurazione per il quale si realizza il backup.
- ☐ Fare clic sul pulsante *Set credentials*.
  La finestra di dialogo mostra la finestra *Credentials*.
- ☐ Immettere le credenziali necessarie per autenticarsi sul server remoto.
- ☐ Abilitare la funzione nell'elenco opzioni *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`show config remote-backup`	Verificare lo stato della funzione.
`configure`	Passare alla modalità di configurazione.
`config remote-backup destination`	Immettere l'URL di destinazione per il backup del profilo di configurazione.
`config remote-backup username`	Immettere il nome utente per autenticarsi sul server remoto.
`config remote-backup password`	Immettere la password per autenticarsi sul server remoto.
`config remote-backup operation`	Abilitare la funzione.

Se il trasferimento al server remoto fallisce, il dispositivo registra questo evento nel file di registro (System Log).

5.2.4 Esportazione di un profilo di configurazione

Il dispositivo consente di salvare un profilo di configurazione su un server in formato XML. Se si utilizza l'interfaccia grafica utente, è possibile salvare il file XML direttamente sul proprio PC.

Prerequisiti:
- Per salvare il file su un server è necessario un server configurato sulla rete.
- Per salvare il file su un server SCP o SFTP sono necessari anche nome utente e password per l'accesso a questo server.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.
- ☐ Nella tabella, selezionare la voce del profilo di configurazione richiesto.

Esportare il profilo di configurazione sul proprio PC. A tale scopo, eseguire i seguenti passaggi:

- ☐ cliccare sul link nella colonna *Profile name*.
- ☐ Selezionare la locazione di memoria e specificare il nome del file.
- ☐ Fare clic sul pulsante *Ok*.

Il profilo di configurazione è ora salvato in formato XML nella posizione specificata.

Esportare il profilo di configurazione su un server remoto. A tale scopo, eseguire i seguenti passaggi:

- ☐ Fare clic sul pulsante ☰ e poi sulla voce *Export...*.
  La finestra di dialogo mostra la finestra *Export...*.
- ☐ Nel campo *URL*, specificare l'URL del file sul server remoto.
  - ☐ Per salvare il file su un server FTP, specificare l'URL per il file nella forma seguente:
    `ftp://<utente>:<password>@<indirizzo IP>:<porta>/<nome file>`
  - ☐ Per salvare il file su un server TFTP, specificare l'URL per il file nella forma seguente:
    `tftp://<indirizzo IP>/<percorso>/<nome file>`
  - ☐ Per salvare il file su un server SCP o SFTP, specificare l'URL per il file in una delle forme seguenti:
    `scp://` oppure `sftp://<user>:<password>@<IP address>/<path>/<file name>`
    `scp://` oppure `sftp://<IP address>/<path>/<file name>`
    Quando si fa clic sul pulsante *Ok*, il dispositivo mostra la finestra *Credentials*. Qui si immettono *User name* e *Password* per accedere al server.
- ☐ Fare clic sul pulsante *Ok*.
  Il profilo di configurazione è ora salvato in formato XML nella posizione specificata.

`show config profiles nvm`	Mostrerà i profili di configurazione contenuti nella memoria non volatile (`nvm`).
`enable`	Passare alla modalità Privileged EXEC.
`copy config running-config remote tftp://<IP_address>/ <path>/<file_name>`	Salvare le impostazioni correnti su un server TFTP.
`copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>`	Salvare il profilo di configurazione selezionato nella memoria non volatile (`nvm`) su un server SFTP.
`copy config nvm profile config3 remote tftp://<IP_address>/ <path>/<file_name>`	Salvare il profilo di configurazione `config3` nella memoria non volatile (`nvm`) su un server TFTP.
`copy config nvm profile config3 remote ftp://<IP_address>:<port>/<path>/<file_name>`	Salvare il profilo di configurazione `config3` nella memoria non volatile (`nvm`) su un server FTP.

5.3 Caricamento delle impostazioni

Se si salvano più profili di configurazione nella memoria, è possibile caricare un profilo di configurazione diverso.

5.3.1 Attivazione di un profilo di configurazione

La memoria non volatile del dispositivo può contenere più profili di configurazione. Se si attiva un profilo di configurazione memorizzato nella memoria non volatile (*NVM*), si modificano immediatamente le impostazioni nel dispositivo. Il dispositivo non richiede un riavvio.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.
- ☐ Nella tabella, selezionare la voce del profilo di configurazione richiesto.
- ☐ Fare clic sul pulsante  e poi sulla voce *Activate*.

Il dispositivo copia le impostazioni nella memoria (RAM) e si scollega dall'interfaccia grafica utente. Il dispositivo utilizza immediatamente le impostazioni del profilo di configurazione.

- ☐ Ricaricare l'interfaccia grafica utente.
- ☐ Accedere nuovamente.

Nella colonna *Selected*, la casella di spunta precedentemente attivata del profilo di configurazione è selezionata.

`show config profiles nvm`	Mostrerà i profili di configurazione contenuti nella memoria non volatile (nvm).
`enable`	Passare alla modalità Privileged EXEC.
`copy config nvm profile config3 running-config`	Attivare le impostazioni del profilo di configurazione config3 nella memoria non volatile (nvm). Il dispositivo copia le impostazioni nella memoria volatile e interrompe il collegamento alla Command Line Interface. Il dispositivo utilizza immediatamente le impostazioni del profilo di configurazione config3.

5.3.2 Caricamento del profilo di configurazione dalla memoria esterna

Se una memoria esterna è collegata, il dispositivo carica automaticamente un profilo di configurazione dalla memoria esterna al riavvio. Il dispositivo consente di salvare tali impostazioni in un profilo di configurazione all'interno della memoria non volatile.

Quando la memoria esterna comprende il profilo di configurazione di un dispositivo identico, è possibile trasferire le impostazioni da un dispositivo all'altro.

Eseguire i seguenti passaggi:

- ☐ Verificare che il dispositivo carichi un profilo di configurazione dalla memoria esterna al riavvio. Nell'impostazione di default, la funzione è abilitata. Se la funzione è disabilitata, abilitarla nuovamente come segue:

- ☐ Aprire la finestra di dialogo *Basic Settings > External Memory*.
- ☐ Selezionare il valore `first` nella colonna *Config priority*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`config envm load-priority usb first`	Abilitare la funzione. Al riavvio, il dispositivo carica un profilo di configurazione dalla memoria esterna. `usb` = Memoria USB esterna
`show config envm settings`	Mostra le impostazioni della memoria esterna (`envm`).

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
usb    ok          [x]         [x]           first
```

`save`	Salvare le impostazioni in un profilo di configurazione all'interno della memoria non volatile (*`NVM`*) del dispositivo.

Tramite la Command Line Interface, il dispositivo consente di copiare le impostazioni dalla memoria esterna direttamente all'interno della memoria non volatile (*`NVM`*).

`show config profiles nvm`	Mostrerà i profili di configurazione contenuti nella memoria non volatile (`nvm`).
`enable`	Passare alla modalità Privileged EXEC.
`copy config envm profile config3 nvm`	Copiare il profilo di configurazione `config3` dalla memoria esterna (`envm`) alla memoria non volatile (`nvm`).

Il dispositivo è in grado, inoltre, di caricare automaticamente un profilo di configurazione da un file di script durante l'inizializzazione.

Prerequisiti:

- ▶ Verificare che la memoria esterna sia collegata prima di avviare il dispositivo.
- ▶ La directory principale della memoria esterna comprende un file di testo `startup.txt` con il contenuto `script=<nome_file>`. Il placeholder `<nome_file>` rappresenta il file di script che il dispositivo esegue durante l'inizializzazione.
- ▶ La directory principale della memoria esterna contiene il file di script. È possibile salvare lo script con un nome specificato dall'utente. Salvare il file con l'estensione `.cli`.

Nota: Verificare che lo script salvato nella memoria esterna non sia vuoto. Se lo script è vuoto, il dispositivo carica il profilo di configurazione successivo secondo le impostazioni di priorità della configurazione.

Dopo l'applicazione dello script, il dispositivo salva automaticamente il profilo di configurazione dal file di script in formato XML all'interno della memoria esterna. Quando si digita il comando appropriato all'interno del file di script, è possibile disabilitare questa funzione:

☐ `no config envm config-save usb`
Il dispositivo non crea una copia nella memoria USB esterna.

Quando il file di script contiene un comando errato, il dispositivo non applica tale comando durante l'inizializzazione. Il dispositivo registra l'evento nel file di registro (System Log).

5.3.3 Importazione di un profilo di configurazione

Il dispositivo consente di importare un profilo di configurazione in formato XML da un server. Se si utilizza l'interfaccia grafica utente, è possibile importare il file XML direttamente dal proprio PC.

Prerequisiti:
- Per salvare il file su un server è necessario un server configurato sulla rete.
- Per salvare il file su un server SCP o SFTP sono necessari anche nome utente e password per l'accesso a questo server.

Eseguire i seguenti passaggi:

☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.

☐ Fare clic sul pulsante ☰ e poi sulla voce *Import...*.
La finestra di dialogo mostra la finestra *Import...*.

☐ Nell'elenco a discesa *Select source*, selezionare la posizione da cui il dispositivo importa il profilo di configurazione.
- *PC/URL*
  Il dispositivo importa il profilo di configurazione dal PC locale o da un server remoto.
- *External memory*
  Il dispositivo importa il profilo di configurazione dalla memoria esterna.

Importare il profilo di configurazione dal PC locale o da un server remoto. A tale scopo, eseguire i seguenti passaggi:

- ☐ Importare il profilo di configurazione:
  - ☐ Quando il file si trova su un server FTP, specificare l'URL per il file nella forma seguente:
    `ftp://<utente>:<password>@<indirizzo IP>:<porta>/<nome file>`
  - ☐ Quando il file si trova su un server TFTP, specificare l'URL per il file nella forma seguente:
    `tftp://<indirizzo IP>/<percorso>/<nome file>`
  - ☐ Quando il file si trova su un server SCP o SFTP, specificare l'URL per il file in una delle forme seguenti:
    `scp://` oppure `sftp://<IP address>/<path>/<file name>`
    Quando si fa clic sul pulsante *Start*, il dispositivo mostra la finestra *Credentials*. Qui si immettono *User name* e *Password* per accedere al server.
    `scp://` oppure `sftp://<user>:<password>@<IP address>/<path>/<file name>`
- ☐ Nel riquadro *Destination*, specificare dove il dispositivo salva il profilo di configurazione importato:
  - ☐ Nel campo *Profile name*, specificare il nome sotto al quale il dispositivo salva il profilo di configurazione.
  - ☐ Nel campo *Storage type*, specificare la locazione di memoria per il profilo di configurazione.
- ☐ Fare clic sul pulsante *Ok*.

Il dispositivo copia il profilo di configurazione nella memoria specificata.

Se è stato specificato il valore `ram` nel riquadro *Destination*, il dispositivo scollega l'interfaccia grafica utente e utilizza immediatamente le impostazioni.

Importare il profilo di configurazione dalla memoria esterna. A tale scopo, eseguire i seguenti passaggi:

- ☐ Nel riquadro *Import profile from external memory*, elenco a discesa *Profile name*, selezionare il nome del profilo di configurazione da importare.
  Il prerequisito è che la memoria esterna contenga un profilo di configurazione esportato.
- ☐ Nel riquadro *Destination*, specificare dove il dispositivo salva il profilo di configurazione importato:
  - ☐ Nel campo *Profile name*, specificare il nome sotto al quale il dispositivo salva il profilo di configurazione.
- ☐ Fare clic sul pulsante *Ok*.

Il dispositivo copia il profilo di configurazione nella memoria non volatile (*NVM*) del dispositivo.

Se è stato specificato il valore `ram` nel riquadro *Destination*, il dispositivo scollega l'interfaccia grafica utente e utilizza immediatamente le impostazioni.

`enable`	Passare alla modalità Privileged EXEC.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> running-config`	Importare e attivare le impostazioni di un profilo di configurazione salvato su un server FTP. Il dispositivo copia le impostazioni nella memoria volatile e interrompe il collegamento alla Command Line Interface. Il dispositivo utilizza immediatamente le impostazioni del profilo di configurazione importato.
`copy config remote tftp://<IP_address>/ <path>/<file_name> running-config`	Importare e attivare le impostazioni di un profilo di configurazione salvato su un server TFTP. Il dispositivo copia le impostazioni nella memoria volatile e interrompe il collegamento alla Command Line Interface. Il dispositivo utilizza immediatamente le impostazioni del profilo di configurazione importato.
`copy config remote sftp://<user name>:<password>@<IP_address>/<path>/<file_name> running-config`	Importare e attivare le impostazioni di un profilo di configurazione salvato su un server SFTP. Il dispositivo copia le impostazioni nella memoria volatile e interrompe il collegamento alla Command Line Interface. Il dispositivo utilizza immediatamente le impostazioni del profilo di configurazione importato.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> nvm profile config3`	Importare le impostazioni di un profilo di configurazione salvato su un server FTP e salvare le impostazioni nel profilo di configurazione `config3` all'interno della memoria non volatile (`nvm`).
`copy config remote tftp://<IP_address>/<path>/<file_name> nvm profile config3`	Importare le impostazioni di un profilo di configurazione salvato su un server TFTP e salvare le impostazioni nel profilo di configurazione `config3` all'interno della memoria non volatile (`nvm`).

5.4 Ripristinare il dispositivo allo stato di fornitura

Se si ripristinano nel dispositivo le impostazioni allo stato di fornitura, esso cancella i profili di configurazione nella memoria volatile e nella memoria non volatile.

Se una memoria esterna è collegata, il dispositivo cancella anche i profili di configurazione salvati nella memoria esterna.

Il dispositivo poi si riavvia e carica le impostazioni di fabbrica.

5.4.1 Utilizzo dell'interfaccia grafica utente o della Command Line Interface

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.
- ☐ Cliccare sul pulsante , poi *Back to factory...*.
  La finestra di dialogo mostra un messaggio.
- ☐ Fare clic sul pulsante *Ok*.

Il dispositivo cancella i profili di configurazione nella memoria (`RAM`) e nella memoria non volatile (*`NVM`*).

Se una memoria esterna è collegata, il dispositivo cancella anche i profili di configurazione salvati nella memoria esterna.

Dopo un breve periodo, il dispositivo si riavvia e carica le impostazioni di default.

`enable`	Passare alla modalità Privileged EXEC.
`clear factory`	Cancella i profili di configurazione dalla memoria non volatile e dalla memoria esterna. Se una memoria esterna è collegata, il dispositivo cancella anche i profili di configurazione salvati nella memoria esterna. Dopo un breve periodo, il dispositivo si riavvia e carica le impostazioni di default.

5.4.2 Utilizzo del monitor di sistema

Prerequisito:
- Il PC è collegato con il collegamento seriale del dispositivo tramite un cavo terminale.

Eseguire i seguenti passaggi:
- ☐ Riavviare il dispositivo.
- ☐ Per passare al monitor di sistema, premere il tasto <1> entro 3 secondi quando richiesto durante il riavvio.
  Il dispositivo carica il monitor di sistema.
- ☐ Per passare dal menù principale al menù `Manage configurations`, premere il tasto <4>.
- ☐ Per eseguire il comando `Clear configs and boot params`, premere il tasto <1>.

- Per caricare le impostazioni di fabbrica, premere il tasto <Enter>.
  Il dispositivo cancella i profili di configurazione nella memoria (RAM) e nella memoria non volatile (NVM).
  Se una memoria esterna è collegata, il dispositivo cancella anche i profili di configurazione salvati nella memoria esterna.
- Per passare al menù principale, premere il tasto <q>.
- Per riavviare il dispositivo con le impostazioni di fabbrica, premere il tasto <q>.

6 Caricamento degli aggiornamenti software

Schneider Electric lavora costantemente al miglioramento e allo sviluppo del proprio software. Verificare regolarmente la disponibilità di una versione software aggiornata con ulteriori vantaggi per l'utente. Le informazioni e i software da scaricare si trovano nelle Schneider Electric pagine dei prodotti all'indirizzo www.schneider-electric.com.

Il dispositivo fornisce le seguenti opzioni per l'aggiornamento software:
- Aggiornamento software dal PC
- Aggiornamento software da un server
- Aggiornamento software dalla memoria esterna
- Caricamento di una versione precedente del software

Nota: una volta aggiornato il software, le impostazioni del dispositivo sono archiviate.

La versione software del dispositivo installato è visualizzabile nella finestra di dialogo di accesso dell'interfaccia grafica utente.

Per visualizzare la versione del software installato quando si è già eseguito l'accesso, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Software*.
  Il campo *Running version* mostra il numero della versione e la data di creazione del software del dispositivo caricato durante l'ultimo riavvio e attualmente in esecuzione.

`enable`	Passare alla modalità Privileged EXEC.
`show system info`	Mostra le informazioni di sistema come il numero della versione e la data di creazione del software del dispositivo caricato durante l'ultimo riavvio e attualmente in esecuzione.

6.1 Aggiornamento software dal PC

Il prerequisito è che il file immagine del software del dispositivo sia salvato su un supporto dati accessibile dal proprio PC.

Eseguire i seguenti passaggi:

- ☐ spostarsi nella cartella in cui è stato salvato il file immagine del software del dispositivo.
- ☐ Aprire la finestra di dialogo *Basic Settings > Software*.
- ☐ Trascinare il file immagine nell'area  . In alternativa, fare clic sull'area per selezionare il file.
- ☐ Per avviare la procedura di aggiornamento, cliccare sul pulsante *Start*.
  Una volta completata la procedura di aggiornamento, il dispositivo comunica che il software è stato aggiornato con successo.
  Al riavvio, il dispositivo carica il software del dispositivo installato.

6.2 Aggiornamento software da un server

Per aggiornare il software tramite SFTP o SCP è necessario un server su cui è salvato il file immagine del software del dispositivo.

Per aggiornare il software tramite TFTP, SFTP o SCP è necessario un server su cui è salvato il file immagine del software del dispositivo.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Software*.
- ☐ Nel riquadro *Software update*, campo *URL*, immettere l'URL per il file immagine nella forma seguente:
  - ▶ Quando il file immagine è salvato su un server FTP:
    `ftp://<indirizzo_IP>:<porta>/<percorso>/<nome_file_immagine>.bin`
  - ▶ Quando il file immagine è salvato su un server TFTP:
    `tftp://<indirizzo_IP>/<percorso>/<nome_file_immagine>.bin<`
  - ▶ Quando il file immagine è salvato su un server SCP o SFTP:
    `scp://` oppure `sftp://<IP_address>/<path>/<image_file_name>.bin`
    `scp://` oppure `sftp://<username>:<password>@<IP_address>/<path>/<image_file_name>.bin`
    Quando si immette l'URL senza nome utente e password, il dispositivo mostra la finestra *Credentials*. Immettere qui le credenziali necessarie per accedere al server.
- ☐ Per avviare la procedura di aggiornamento, cliccare sul pulsante *Start*.
  Il dispositivo copia il software del dispositivo attualmente in esecuzione all'interno della memoria di backup.
  Una volta completata la procedura di aggiornamento, il dispositivo comunica che il software è stato aggiornato con successo.
  Al riavvio, il dispositivo carica il software del dispositivo installato.

`enable`	Passare alla modalità Privileged EXEC.
`copy firmware remote tftp://10.0.1.159/product.bin system`	Trasferire il file `product.bin` dal server TFTP con l'indirizzo IP `10.0.1.159` al dispositivo.

6.3 Aggiornamento software dalla memoria esterna

6.3.1 Manuale—avviato dall'amministratore

Il dispositivo consente di aggiornare il software con pochi clic del mouse. Il prerequisito è che il file immagine del software del dispositivo si trovi nella memoria esterna.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Software*.
- ☐ Nella tabella, selezionare la riga che mostra il nome del file immagine desiderato nella memoria esterna.
- ☐ Cliccare con il tasto destro per visualizzare il menù contestuale.
- ☐ Per avviare la procedura di aggiornamento, cliccare sulla voce *Update* nel menù contestuale.
  Il dispositivo copia il software del dispositivo attualmente in esecuzione all'interno della memoria di backup.
  Una volta completata la procedura di aggiornamento, il dispositivo comunica che il software è stato aggiornato con successo.
  Al riavvio, il dispositivo carica il software del dispositivo installato.

6.3.2 Automaticamente—avviato dal dispositivo

Quando i file seguenti si trovano nella memoria esterna durante un riavvio, il dispositivo aggiorna automaticamente il proprio software:
- il file immagine del software del dispositivo
- un file di testo `startup.txt` con il contenuto `autoUpdate=<Image_file_name>.bin`

Il prerequisito è che all'interno della finestra di dialogo *Basic Settings > External Memory* si selezioni la casella di spunta nella colonna *Software auto update*. Questa è l'impostazione di default nel dispositivo.

Eseguire i seguenti passaggi:
- ☐ Copiare il file immagine del nuovo software del dispositivo all'interno della directory principale della memoria esterna. Utilizzare solamente un file immagine adatto per il dispositivo.
- ☐ Creare un file di testo `startup.txt` nella directory principale della memoria esterna.
- ☐ Aprire il file `startup.txt` nell'editor di testo e aggiungere la riga seguente:
  `autoUpdate=<Image_file_name>.bin`
- ☐ Installare la memoria esterna nel dispositivo.

☐ Riavviare il dispositivo.
Durante l'inizializzazione, il dispositivo verifica automaticamente i seguenti criteri:
- Vi è una memoria esterna collegata?
- Vi è un file `startup.txt` nella directory principale della memoria esterna?
- Vi è il file immagine specificato nel file `startup.txt`?
- La versione software del file immagine è più recente del software attualmente in esecuzione nel dispositivo.

Quando i criteri sono soddisfatti, il dispositivo avvia la procedura di aggiornamento.
Il dispositivo copia il software del dispositivo attualmente in esecuzione all'interno della memoria di backup.
Non appena la procedura di aggiornamento è completata con successo, il dispositivo si riavvia automaticamente e carica la nuova versione software.

☐ Verificare il risultato della procedura di aggiornamento. Il file di registro nella finestra di dialogo *Diagnostics > Report > System Log* comprende uno dei seguenti messaggi:
- `S_watson_AUTOMATIC_SWUPDATE_SUCCESS`
  Aggiornamento software completato con successo
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED`
  Aggiornamento software interrotto
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE`
  Aggiornamento software interrotto: file immagine errato
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
  Aggiornamento software interrotto: il dispositivo non ha salvato il file immagine.

6.4 Caricamento di una versione precedente del software

Il dispositivo consente di sostituire il proprio software con una versione precedente. Le impostazioni di base nel dispositivo sono archiviate dopo la sostituzione del software del dispositivo.

Nota: Vanno perse solo le impostazioni per le funzioni disponibili nella nuova versione software del dispositivo.

7 Configurazione delle porte

Sono disponibili le seguenti funzioni di configurazione delle porte.

- Abilitazione/disabilitazione della porta
- Selezione del modo operativo
- Modalità Gigabit Ethernet per le porte

7.1 Abilitazione/disabilitazione della porta

Nell'impostazione di default, ogni porta è abilitata. Per una sicurezza di accesso di livello superiore, disabilitare le porte scollegate. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
- ☐ Per abilitare una porta, selezionare la casella di spunta nella colonna *Port on*.
- ☐ Per disabilitare una porta, deselezionare la casella di spunta nella colonna *Port on*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`no shutdown`	Abilitare l'interfaccia.

7.2 Selezione del modo operativo

Nell'impostazione di default, le porte sono impostate secondo il modo operativo *Automatic configuration*.

Nota: La configurazione automatica attiva ha priorità rispetto alla configurazione manuale.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
- ☐ Se il dispositivo collegato a questa porta presuppone un'impostazione fissa, eseguire i seguenti passaggi:
  - ☐ Disattivare la funzione. Deselezionare la casella di spunta nella colonna *Automatic configuration*.
  - ☐ Nella colonna *Manual configuration*, immettere il modo operativo desiderato (capacità di trasferimento, modalità duplex).
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`no auto-negotiate`	Disabilitare la modalità di configurazione automatica.
`speed 100 full`	Velocità della porta 100 MBit/s, duplex pieno

7.3 Modalità Gigabit Ethernet per le porte

Il dispositivo supporta 2.5 Gbit/s su diverse interfacce con uno dei seguenti ricetrasmettitori SFP:
- M-SFP-2.5-MM/LC EEC
- M-SFP-2.5-SM-/LC EEC
- M-SFP-2.5-SM/LC EEC
- M-SFP-2.5-SM+/LC EEC

Il tipo di ricetrasmettitore inserito nello slot determina la velocità della porta. Il dispositivo non può impostare manualmente la velocità. Le porte con velocità della porta pari a 2.5 Gbit/s non sono in grado di supportare data rate pari a 100 Mbit/s.

Nota: Per ulteriori informazioni sul numero dell'ordine dei ricetrasmettitori consultare il capitolo “Accessori” del manuale utente “Installazione”.

7.3.1 Esempio

Si utilizza la modalità Gigabit Ethernet per ottenere una larghezza di banda superiore per gli uplink. Per utilizzare questa funzione, inserire un tipo di ricetrasmettitore applicabile nello slot appropriato.

Eseguire i seguenti passaggi:

☐ Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.

La colonna *Manual configuration* mostra il valore `2.5 Gbit/s FDX` per le porte da 2.5 Gbit/s con un ricetrasmettitore SFP inserito.

Non è possibile modificare la velocità.

```
show port 1/1
```

Mostra i parametri per la porta `1` dello slot `1`. La voce dell'elenco `Physical Mode` mostra il valore `2500 full` per le porte da 2.5 Gbit/s con ricetrasmettitore SFP inserito.

```
Interface.....................1/1
Name..........................My interface
--
Cable-crossing Setting........-
Physical Mode.................2500 full
Physical Status...............-
```

8 Assistenza nella protezione da accesso non autorizzato

Il dispositivo offre funzioni che aiutano a proteggere il dispositivo dall'accesso non autorizzato.

Dopo la configurazione, effettuare i seguenti passaggi per ridurre il possibile accesso non autorizzato al dispositivo.

- Passaggio alla community SNMPv1/v2
- Disabilitazione SNMPv1/v2
- Disabilitazione HTTP
- Utilizzo del proprio certificato HTTPS
- Utilizzo della propria chiave SSH
- Disabilitazione Telnet
- Disabilitazione Ethernet Switch Configurator
- Abilitazione limitazione accesso IP
- Adattamento dei timeout sessione

8.1 Passaggio alla community SNMPv1/v2

SNMPv1/v2 lavora non crittografato. Ogni pacchetto SNMP contiene l'indirizzo IP del mittente e il nome della community in testo non crittografato con il quale il mittente accede al dispositivo. Se SNMPv1/v2 è abilitato, il dispositivo consente l'accesso al dispositivo a chiunque conosca il nome della community.

I nomi della community `user` per gli accessi in lettura e `admin` per gli accessi in scrittura sono preimpostati. In caso di utilizzo di SNMPv1 o SNMPv2, modificare il nome della community predefinita. Trattare con discrezione i nomi della community. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > SNMPv1/v2 Community*.

La finestra di dialogo visualizza le community che sono configurate.

- ☐ Per la community `Write`, specificare il nome della community nella colonna *Name*.
  - Sono consentiti fino a 32 caratteri alfanumerici.
  - Il dispositivo differenzia tra maiuscole e minuscole.
  - Specificare un nome community differente rispetto a quello per l'accesso in lettura.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`snmp community rw <community name>`	Specificare la community per l'accesso in lettura/scrittura.
`show snmp community`	Visualizzare le community che sono state configurate.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

8.2 Disabilitazione SNMPv1/v2

Se è necessario SNMPv1 o SNMPv2, utilizzare questi protocolli solo in ambienti protetti da intercettazione. SNMPv1 e SNMPv2 non utilizzano la crittografia. I pacchetti SNMP contengono la community in testo non crittografato. Raccomandiamo di utilizzare SNMPv3 nel dispositivo e di disabilitare l'accesso utilizzando SNMPv1 e SNMPv2. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *SNMP*.

La finestra di dialogo visualizza le impostazioni del server SNMP.

- ☐ Per disattivare il protocollo SNMPv1, deselezionare la casella di spunta *SNMPv1*.
- ☐ Per disattivare il protocollo SNMPv2, deselezionare la casella di spunta *SNMPv2*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`no snmp access version v1`	Disattivare il protocollo SNMPv1.
`no snmp access version v2`	Disattivare il protocollo SNMPv2.
`show snmp access`	Visualizza le impostazioni del server SNMP.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

8.3 Disabilitazione HTTP

Il server Web fornisce l'interfaccia grafica utente con il protocollo HTTP o HTTPS. Le connessioni HTTPS sono crittografate, mentre le connessioni HTTP non sono crittografate.

Il protocollo HTTP è abilitato di default. Disabilitando l'HTTP, non è possibile alcun accesso non crittografato all'interfaccia grafica utente. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *HTTP*.
- ☐ Per disabilitare il protocollo HTTP, selezionare il pulsante di opzione `Off` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`no http server`	Disabilitare il protocollo HTTP.

Se il protocollo HTTP è disabilitato, è possibile raggiungere l'interfaccia grafica utente del dispositivo solo tramite l'HTTPS. Nella barra dell'indirizzo del browser web, immettere la stringa `https://` prima dell'indirizzo IP del dispositivo.

Se il protocollo HTTPS è disabilitato e, si disabilita anche l'HTTP, l'interfaccia grafica utente non è accessibile. Per lavorare con l'interfaccia grafica utente, abilitare il server HTTPS utilizzando la Command Line Interface. A tale scopo, eseguire i seguenti passaggi:

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`https server`	Abilitare il protocollo HTTPS.

8.4 Disabilitazione Telnet

Il dispositivo consente l'accesso remoto alla gestione del dispositivo utilizzando Telnet o SSH. Le connessioni HTTPS non sono crittografate, mentre le connessioni SSH sono crittografate.

Il server Telnet è abilitato di default nel dispositivo.. Disabilitando Telnet, non è possibile alcun accesso remoto non crittografato alla Command Line Interface. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *Telnet*.
- ☐ Per disabilitare il server Telnet, selezionare il pulsante di opzione `Off` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`no telnet server`	Disattivare il server Telnet.

Se il server SSH è disabilitato e si disabilita anche Telnet, l'accesso all'interfaccia a riga di comando è possibile solo attraverso l'interfaccia seriale del dispositivo. Per lavorare in remoto con la Command Line Interface, abilitare l'SSH. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *SSH*.
- ☐ Per abilitare il server *SSH*, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`ssh server`	Abilitare il server SSH.

8.5 Disabilitazione dell'accesso Ethernet Switch Configurator

Ethernet Switch Configurator consente l'assegnazione dei parametri IP al dispositivo tramite la rete durante la messa in funzione. Ethernet Switch Configurator comunica nella VLAN di gestione del dispositivo senza crittografia e autenticazione.

Dopo la messa in funzione del dispositivo, raccomandiamo di impostare Ethernet Switch Configurator in sola lettura o di disabilitare completamente l'accesso Ethernet Switch Configurator. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Network*.
- ☐ Per rimuovere il permesso in scrittura dal software Ethernet Switch Configurator, nel riquadro *Ethernet Switch Configurator protocol v1/v2*, specificare il valore `readOnly` nel campo *Access*.
- ☐ Per disabilitare completamente l'accesso Ethernet Switch Configurator, selezionare il pulsante di opzione `Off` nel riquadro *Ethernet Switch Configurator protocol v1/v2*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

`enable`	Passare alla modalità Privileged EXEC.
`network ethernet-switch-conf mode read-only`	Disabilitare il permesso in scrittura del software Ethernet Switch Configurator.
`no network ethernet-switch-conf operation`	Disabilitare l'accesso Ethernet Switch Configurator.

8.6 Attivazione della limitazione di accesso IP

Nell'impostazione predefinita, si accede alla gestione del dispositivo da qualsiasi indirizzo IP e con i protocolli supportati.

La limitazione di accesso IP consente di limitare l'accesso alla gestione dei dispositivo a intervalli di indirizzo IP selezionati e a protocolli basati su IP selezionati.

Esempio:

Il dispositivo deve essere accessibile solo dalla rete aziendale utilizzando l'interfaccia grafica utente. L'amministratore ha un accesso remoto supplementare utilizzando SSH. La rete aziendale ha l'intervallo di indirizzi `192.168.1.0/24` e accesso remoto da una rete mobile con l'intervallo di indirizzi IP `109.237.176.0/24`. Il programma applicativo SSH conosce l'impronta della chiave RSA.

Tabella 20:Parametri per la limitazione di accesso IP

Parametro	Rete aziendale	Rete radiomobile
Indirizzo di rete	`192.168.1.0`	`109.237.176.0`
Subnet mask	`24`	`24`
Protocolli desiderati	https, snmp	ssh

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > IP Access Restriction*.
- ☐ Deselezionare la casella di spunta nella colonna *Active* per la voce.
  Questa voce consente agli utente l'accesso al dispositivo da qualsiasi indirizzo IP e dai protocolli supportati.

Intervallo di indirizzi della rete aziendale:

- ☐ Per aggiungere una voce tabella, fare clic sul pulsante  .
- ☐ Specificare l'intervallo di indirizzi della rete aziendale nella colonna *IP address range*: `192.168.1.0/24`
- ☐ Per l'intervallo di indirizzi delle rete aziendale, disattivare i protocolli indesiderati. Le caselle di spunta *HTTPS*, *SNMP* e *Active* rimangono selezionate.

Intervallo di indirizzi della rete radiomobile:

- ☐ Per aggiungere una voce tabella, fare clic sul pulsante  .
- ☐ Specificare l'intervallo di indirizzi della rete mobile nella colonna *IP address range*: `109.237.176.0/24`
- ☐ Per l'intervallo di indirizzi delle rete mobile, disattivare i protocolli indesiderati. Le caselle di spunta *SSH* e *Active* rimangono selezionate.

Prima di attivare questa funzione, verificare che almeno una voce attiva nella tabella consenta l'accesso. In caso contrario, se si modificano le impostazioni, termina la connessione al dispositivo. L'accesso alla gestione del dispositivo è possibile solo utilizzando la Command Line Interface attraverso l'interfaccia seriale del dispositivo.

- ☐ Per abilitare la limitazione di accesso IP, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

`enable`	Passare alla modalità Privileged EXEC.
`show network management access global`	Visualizza se la limitazione di accesso IP è abilitata o disabilitata.
`show network management access rules`	Visualizzare le voci che sono state configurate.
`no network management access operation`	Disabilitare la limitazione di accesso IP
`network management access add 2`	Creare la voce per l'intervallo di indirizzi della rete aziendale. Numero del successivo indice disponibile in questo esempio: `2`.
`network management access modify 2 ip 192.168.1.0`	Specificare l'indirizzo IP della rete aziendale.
`network management access modify 2 mask 24`	Specificare la netmask della rete aziendale.
`network management access modify 2 ssh disable`	Disattivare SSH per l'intervallo di indirizzi della rete aziendale. Ripetere il funzionamento per ogni protocollo indesiderato.
`network management access add 3`	Creare una voce per l'intervallo di indirizzi della rete radiomobile. Numero del successivo indice disponibile in questo esempio: `3`.
`network management access modify 3 ip 109.237.176.0`	Specificare l'indirizzo IP della rete radiomobile.
`network management access modify 3 mask 24`	Specificare la netmask della rete radiomobile.
`network management access modify 3 snmp disable`	Disattivare SNMP per l'indirizzo di indirizzi della rete radiomobile. Ripetere il funzionamento per ogni protocollo indesiderato.
`no network management access status 1`	Disattivare la voce di default. Questa voce consente agli utente l'accesso al dispositivo da qualsiasi indirizzo IP e dai protocolli supportati.
`network management access status 2`	Attivare una voce per l'intervallo di indirizzi della rete aziendale.
`network management access status 3`	Attivare una voce per l'intervallo di indirizzi della rete radiomobile.
`show network management access rules`	Visualizzare le voci che sono state configurate.
`network management access operation`	Abilitare la limitazione di accesso IP.

8.7 Adattamento dei timeout sessione

Il dispositivo consente di terminare automaticamente la sessione in caso di inattività dell'utente connesso. Il timeout della sessione è il periodo di inattività dopo l'ultima azione utente.

È possibile specificare un timeout di sessione per le seguenti applicazioni:
- Sessioni Command Line Interface utilizzando una connessione SSH
- Sessioni Command Line Interface utilizzando una connessione Telnet
- Sessioni Command Line Interface utilizzando una connessione seriale
- Interfaccia grafica utente

Timeout per sessioni Command Line Interface utilizzando una connessione SSH

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *SSH*.
- ☐ Specificare il periodo di timeout in minuti nel riquadro *Configuration*, campo *Session timeout [min]*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`ssh timeout <0..160>`	Specificare il periodo di timeout in minuti per sessioni Command Line Interface utilizzando una connessione SSH.

Timeout per sessioni Command Line Interface utilizzando una connessione Telnet

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *Telnet*.
- ☐ Specificare il periodo di timeout in minuti nel riquadro *Configuration*, campo *Session timeout [min]*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`telnet timeout <0..160>`	Specificare il periodo di timeout in minuti per sessioni Command Line Interface utilizzando una connessione Telnet.

Timeout per sessioni Command Line Interface utilizzando una connessione seriale

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > CLI*, scheda *Global*.
- ☐ Specificare il periodo di timeout in minuti nel riquadro *Configuration*, campo *Serial interface timeout [min]*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`cli serial-timeout <0..160>`	Specificare il periodo di timeout in minuti per sessioni Command Line Interface utilizzando una connessione seriale.

Timeout di sessione per l'interfaccia grafica utente

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Web*.
- ☐ Specificare il periodo di timeout in minuti nel riquadro *Configuration*, campo *Web interface session timeout [min]*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`network management access web timeout <0..160>`	Specificare il periodo di timeout in minuti per sessioni con interfaccia grafica utente

9 Controllo del traffico dati

Il dispositivo controlla i pacchetti dati da inoltrare secondo le regole definite. I pacchetti dati a cui si applicano le regole sono inoltrati dal dispositivo o bloccati. Se i pacchetti dati non corrispondono ad alcuna regola, il dispositivo li blocca.

Le porte di routing prive di regole assegnate consentono ai pacchetti di passare. Non appena una regola è assegnata, le regole assegnate sono processate prima. Dopo, l'azione standard specificata del dispositivo ha effetto.

Il dispositivo fornisce le seguenti funzioni per il controllo del flusso di dati:
- Controllo delle richieste di servizio (Denial of Service, DoS)
- Negare l'accesso ai dispositivi in base al loro IP o indirizzo MAC (elenco di controllo accessi)

Il dispositivo osserva e monitora il flusso di dati. Il dispositivo ottiene i risultati dell'osservazione e del monitoraggio e li combina con le regole per la sicurezza di rete al fine di creare la cosiddetta tabella di stato. In base alla tabella di stato, il dispositivo decide se accettare, scartare o rifiutare i dati.

I pacchetti dati passano attraverso le funzioni di filtraggio del dispositivo in questa sequenza:
- DoS … se `permit` o `accept`, poi avanzare alla regola successiva
- ACL … se `permit` o `accept`, poi avanzare alla regola successiva

9.1 Contribuire a proteggere dagli accessi non autorizzati

Con questa funzione, il dispositivo fornisce supporto contribuendo a proteggere da pacchetti dati non validi o falsificati che mirano a certi dispositivi o servizi. È possibile specificare i filtri per limitare il flusso di dati al fine di proteggere da attacchi “Denial of Service”. I filtri attivati controllano i pacchetti dati in ingresso e li rifiutano non appena trovano una corrispondenza con i criteri del filtro.

La finestra di dialogo *Network Security > DoS > Global* comprende 2 riquadri in cui si attivano diversi filtri. Per attivarli, selezionare le caselle di spunta corrispondenti.

Nel riquadro *TCP/UDP* si attivano fino a 4 filtri che influenzano solo i pacchetti TCP e UDP. Utilizzando questo filtro, si disattivano le scansioni delle porte utilizzate dagli aggressori per provare a rilevare i dispositivi e i servizi offerti. I filtri operano come segue:

Tabella 21:Filtri DoS per TCP

Filtro	Azione
Attivare il filtro Null Scan	Il dispositivo rileva e rifiuta i pacchetti TCP in ingresso con le seguenti proprietà: - Nessun flag TCP impostato. - Il numero di sequenza TCP è 0.

Tabella 21:Filtri DoS per TCP

Filtro	Azione
Attivare il filtro Xmas	Il dispositivo rileva e rifiuta i pacchetti TCP in ingresso con le seguenti proprietà: ▶ I flag TCP *FIN*, *URG* e *PSH* sono impostati contemporaneamente. ▶ Il numero di sequenza TCP è 0.
Attivare il filtro SYN/FIN	Il dispositivo rileva e rifiuta i pacchetti TCP in ingresso per i quali sono impostati contemporaneamente i flag TCP *SYN* e *FIN*.
Attivare il filtro header minimo	Il dispositivo rileva e rifiuta i pacchetti TCP in ingresso per i quali lo header TCP è troppo breve.

Il riquadro *ICMP* offre 2 opzioni di filtro per pacchetti ICMP. La frammentazione dei pacchetti ICMP in ingresso rivela un attacco. Se si attiva questo filtro, il dispositivo rileva i pacchetti ICMP frammentati e li rifiuta. Utilizzando il parametro *Allowed payload size [byte]* è possibile inoltre specificare le massime dimensioni consentite del carico utile dei pacchetti ICMP. Il dispositivo rifiuta i pacchetti dati che superano questa specifica di byte.

Nota: È possibile combinare i filtri in qualsiasi modo all'interno della finestra di dialogo *Network Security > DoS > Global*. Quando sono selezionati diversi filtri, si applica un O logico: se il primo o il secondo (o il terzo, etc.) filtro si applica a un pacchetto dati, il dispositivo lo rifiuta.

9.2 ACL

In questo menù è possibile immettere i parametri per le Access Control List (ACL).

Il dispositivo utilizza le ACL per filtrare i pacchetti dati ricevuti sulle VLAN o su porte multiple o singole. In una ACL, si specificano le regole utilizzate dal dispositivo per filtrare i pacchetti dati. Quando tale regola si applica a un pacchetto, il dispositivo applica al pacchetto le azioni specificate nella regola. Le azioni disponibili sono le seguenti:
- consentire (`permit`)
- rifiutare (`deny`)
- deviare a una determinata porta (vedere il campo *Redirection port*)
- specchio (vedere il campo *Mirror port*)

L'elenco di seguito comprende i criteri che si applicano per filtrare i pacchetti dati:
- Indirizzo di origine o di destinazione di un pacchetto (MAC)
- Indirizzo di origine o di destinazione di un pacchetto dati (IPv4)
- Porta di origine o di destinazione di un pacchetto dati (IPv4)

È possibile specificare i seguenti tipi di ACL:
- ACL IP per VLAN
- ACL IP per porte
- ACL MAC per VLAN
- ACL MAC per porte

Quando si assegna una ACL IP e una ACL MAC alla stessa interfaccia, il dispositivo utilizza prima la ACL IP per filtrare il flusso di dati. Il dispositivo applica le regole della ACL MAC solo dopo il filtraggio dei pacchetti attraverso la ACL IP. La priorità di una ACL è indipendente dall'indice di una regola.

All'interno di una ACL, il dispositivo elabora le regole in ordine. L'indice delle regole corrispondenti determina l'ordine in cui il dispositivo filtra il flusso di dati. Quando si assegna una ACL a una porta o a una VLAN, è possibile specificare la sua priorità con l'indice. Più è basso il numero, più è alta la priorità. Il dispositivo elabora prima la regola con la priorità più alta.

Se nessuna delle regole specificare in una ACL si applica a un pacchetto dati, si applica la regola implicita `deny`. Di conseguenza, il dispositivo scarta i pacchetti dati ricevuti.

Tenere a mente che il dispositivo implementa direttamente la regola implicita `deny`.

Nota: Il numero delle ACL disponibili dipende dal dispositivo. Sono presenti ulteriori informazioni sui valori ACL nel capitolo “Dati tecnici” a pagina 375.

Nota: È possibile assegnare un'unica ACL a qualsiasi numero di porte o VLAN.

Il menù *ACL* include le seguenti finestre di dialogo:
- *ACL IPv4 Rule*
- *ACL MAC Rule*
- *ACL Assignment*

Queste finestre di dialogo forniscono le seguenti opzioni:
- Per specificare le regole per i vari tipi di ACL.
- Per fornire le regole con le priorità richieste.
- Per assegnare le ACL alle porte o alle VLAN.

9.2.1 Creazione e modifica delle regole IPv4

Durante il filtraggio dei pacchetti dati IPv4, il dispositivo consente di:
- creare nuovi gruppi e regole
- aggiungere nuove regole a gruppi esistenti
- modificare una regola esistente
- attivare e disattivare gruppi e regole
- eliminare regole e gruppi esistenti
- modificare l'ordine delle regole esistenti

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Network Security > ACL > IPv4 Rule*.
- ☐ Fare clic sul pulsante  .
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Per creare un gruppo, specificare un nome significativo nel campo *Group name*. È possibile combinare diverse regole in un gruppo.
- ☐ Per aggiungere una regola a un gruppo esistente, selezionare il nome del gruppo nel campo *Group name*.
- ☐ Nel campo *Index* si specifica il numero per la regola all'interno della ACL.
  Tale numero definisce la priorità della regola.
- ☐ Fare clic sul pulsante *Ok*.
  Il dispositivo aggiunge la regola alla tabella.
  Il gruppo e il ruolo sono attivi immediatamente.
  Per disattivare il gruppo o le regole, deselezionare la casella di spunta nella colonna *Active*.
  Per rimuovere una regola, evidenziare la voce della tabella interessata e fare clic sul pulsante  .
- ☐ Modificare i parametri della regola nella tabella.
  Per modificare un valore, fare doppio clic sul campo corrispondente.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

Nota: Il dispositivo consente di utilizzare i metacaratteri con i parametri *Source IP address* e *Destination IP address*. Se si immette `192.168.?.?`, ad esempio, il dispositivo autorizza gli indirizzi che iniziano con `192.168`.

Nota: Il prerequisito per la modifica dei valori nelle colonne *Source TCP/UDP port* e *Destination TCP/UDP port* è che si specifichi il valore `tcp` o `udp` all'interno della colonna *Protocol*.

Nota: Il prerequisito per la modifica del valore nelle colonne *Redirection port* e *Mirror port* è che si specifichi il valore `permit` all'interno della colonna *Action*.

9.2.2 Creazione e configurazione di una ACL IP tramite la Command Line Interface

Nell'esempio seguente, si configurano ACL per bloccare le comunicazioni dai computer B e C al computer A tramite IP (TCP, UDP etc.).

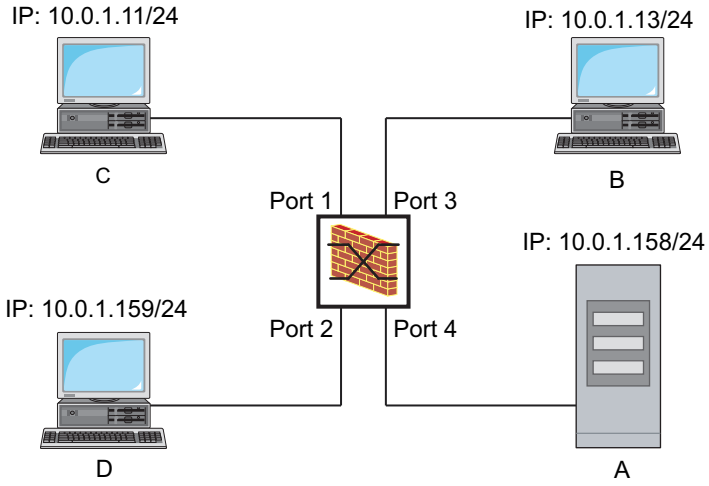


Figura 22: Esempio di una ACL IP

Eseguire i seguenti passaggi:

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`ip access-list extended name filter1 deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	Aggiungere ACL IP con il nome `filter1`. Aggiungere una regola rifiutando i pacchetti dati IP da `10.0.1.11` a `10.0.1.158`. Priorità `1` (priorità massima).
`ip access-list extended name filter1 permit src any dst any`	Aggiungere una regola all'ACL IP ammettendo i pacchetti dati IP.
`show access-list ip filter1`	Visualizzare le regole dell'ACL IP `filter1`.
`ip access-list extended name filter2 deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	Aggiungere ACL IP con il nome `filter2`. Aggiungere una regola rifiutando i pacchetti dati IP da `10.0.1.13` a `10.0.1.158`. Priorità `1` (priorità massima).
`show access-list ip filter2`	Visualizzare le regole dell'ACL IP `filter2`.

9.2.3 Creazione e modifica delle regole MAC

Durante il filtraggio dei pacchetti dati MAC, il dispositivo consente di:
- creare nuovi gruppi e regole
- aggiungere nuove regole a gruppi esistenti
- modificare una regola esistente
- attivare e disattivare gruppi e regole
- eliminare regole e gruppi esistenti
- modificare l'ordine delle regole esistenti

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Network Security > ACL > MAC Rule*.
- ☐ Fare clic sul pulsante  .
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Per creare un gruppo, specificare un nome significativo nel campo *Group name*. È possibile combinare diverse regole in un gruppo.
- ☐ Per aggiungere una regola a un gruppo esistente, selezionare il nome del gruppo nel campo *Group name*.
- ☐ Nel campo *Index* si specifica il numero per la regola all'interno della ACL.
  Tale numero definisce la priorità della regola.
- ☐ Fare clic sul pulsante *Ok*.
  Il dispositivo aggiunge la regola alla tabella.
  Il gruppo e il ruolo sono attivi immediatamente.
  Per disattivare il gruppo o le regole, deselezionare la casella di spunta nella colonna *Active*.
  Per rimuovere una regola, evidenziare la voce della tabella interessata e fare clic sul pulsante  .
- ☐ Modificare i parametri della regola nella tabella.
  Per modificare un valore, fare doppio clic sul campo corrispondente.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

Nota: Nei campi *Source MAC address* e *Destination MAC address* è possibile utilizzare metacaratteri nelle forme `FF:??:??:??:??:??` o `??:??:??:??:00:01`. Utilizzare lettere maiuscole qui.

9.2.4 Creazione e configurazione di una ACL MAC tramite la Command Line Interface

Nell'esempio seguente, AppleTalk e IPX devono essere filtrati dall'intera rete. A tale scopo, eseguire i seguenti passaggi:

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`mac acl add 1 macfilter`	Aggiunge una ACL MAC con l'ID `1` e il nome `macfilter`.
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	Aggiunge una regola alla posizione `1` della ACL MAC con l'ID `1` rifiutando i pacchetti con EtherType `0x809B (AppleTalk)`.
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	Aggiunge una regola alla posizione `2` della ACL MAC con l'ID `1` rifiutando i pacchetti con EtherType `0x8137 (IPX alt)`.
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	Aggiunge una regola alla posizione `3` della ACL MAC con l'ID `1` rifiutando i pacchetti con EtherType `0x8138 (IPX)`.
`mac acl rule add 1 4 permit src any any dst any any`	Aggiunge una regola alla posizione `4` della ACL MAC con i pacchetti di inoltro ID `1`.
`show acl mac rules 1`	Mostra le regole della ACL MAC con l'ID `1`.
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	Passare alla modalità di configurazione delle interfacce dalla `1/1` alla `1/6`.

`acl mac assign 1 in 1`	Assegna la ACL MAC con l'ID `1` ai pacchetti dati in ingresso (`1/1`) sulle interfacce dalla `1/6` alla `in`.
`exit`	Abbandona la modalità interfaccia.
`show acl mac assignment 1`	Mostra l'assegnazione della ACL MAC con l'ID `1` alle interfacce o alle VLAN.

9.2.5 Assegnazione delle ACL a una porta o a una VLAN.

Quando si assegnano ACL a una porta o a una VLAN, il dispositivo fornisce le seguenti opzioni:
- Per selezionare la porta o la VLAN.
- Per specificare la priorità della ACL.
- Per selezionare la ACL utilizzando il nome del gruppo.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Network Security > ACL > Assignment*.
- ☐ Fare clic sul pulsante  .
  La finestra di dialogo mostra la finestra *Create*.
  - ☐ Nel campo *Port/VLAN*, specificare la porta desiderata o la VLAN desiderata.
  - ☐ Nel campo *Priority*, specificare la priorità.
  - ☐ Nel campo *Direction*, specificare i pacchetti dati a cui il dispositivo applica la regola.
  - ☐ Nel campo *Group name*, specificare la regola assegnata dal dispositivo alla porta o alla VLAN.
- ☐ Fare clic sul pulsante *Ok*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

9.3 Bypass di autenticazione MAC

La funzione *MAC authorized bypass* consente ai client che non supportano l'802.1X, come le stampanti e i fax, di autenticarsi alla rete utilizzando il loro indirizzo MAC. Il dispositivo consente di specificare il formato dell'indirizzo MAC utilizzato per autenticare i client sul server RADIUS.

Esempio:

Dividere l'indirizzo MAC in 6 gruppi da 2 caratteri. Utilizzare le lettere maiuscole e i due punti come separatori: `AA:BB:CC:DD:EE:FF`

Utilizzare la password `xY-45uM_e`. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Network Security > 802.1X Port Authentication > Global*.
  Nel riquadro *MAC authentication bypass format options*, eseguire i seguenti passaggi:
- ☐ Nell'elenco a discesa *Group size*, selezionare il valore `2`.
  Il dispositivo divide l'indirizzo MAC in 6 gruppi da 2 caratteri.
- ☐ Nell'elenco a discesa *Group separator*, selezionare il carattere `:`.
- ☐ Nell'elenco a discesa *Upper or lower case*, selezionare la voce `upper-case`.
- ☐ Nel campo *Password*, inserire la password `xY-45uM_e`.
  Il dispositivo utilizza tale password per ogni client che si autentica al server RADIUS. Se si lascia il campo vuoto, il dispositivo utilizza l'indirizzo MAC formattato anche come password.
- ☐ Per salvare temporaneamente le impostazioni, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`dot1x mac-authentication-bypass format group-size 2`	Specificare le dimensioni del gruppo `2`.
`dot1x mac-authentication-bypass format group-separator :`	Specificare il separatore del gruppo `:`.
`dot1x mac-authentication-bypass format letter-case upper-case`	Specificare la formattazione dei dati di autenticazione in lettere maiuscole da parte del dispositivo.
`dot1x mac-authentication-bypass password xY-45uM_e`	Specificare la password `xY-45uM_e`. Il dispositivo utilizza tale password per autenticare ogni client al server RADIUS.

10 Controllo del carico di rete

Il dispositivo presenta una serie di funzioni che aiutano a ridurre il carico di rete:
- Distribuzione mirata di pacchetti
- Multicasts
- Limitatore del carico
- Priorizzazione - QoS
- Controllo di flusso

10.1 Distribuzione mirata di pacchetti

Il dispositivo riduce il carico di rete con la distribuzione mirata di pacchetti.

Su ciascuna delle sue porte, il dispositivo apprende l'indirizzo MAC del mittente dei pacchetti dati ricevuti. Il dispositivo memorizza la combinazione “porta e indirizzo MAC” nella sua tabella indirizzi MAC (FDB).

Applicando il metodo “Store and Forward”, il dispositivo esegue il buffering dei dati ricevuti e ne verifica la validità prima di inoltrarli. Il dispositivo rifiuta i pacchetti dati non validi e difettosi.

10.1.1 Apprendimento degli indirizzi MAC

Quando il dispositivo riceve un pacchetto dati, controlla se l'indirizzo MAC del mittente è già memorizzato nella tabella indirizzi MAC (FDB). Quando l'indirizzo MAC del mittente è sconosciuto, il dispositivo genera una nuova voce. Il dispositivo confronta poi l'indirizzo MAC di destinazione del pacchetto dati con le voci memorizzate nella tabella indirizzi MAC (FDB):
- Il dispositivo inoltra i pacchetti con un indirizzo MAC di destinazione noto direttamente alle porte che hanno già ricevuto pacchetti dati da questo indirizzo MAC.
- Il dispositivo invia in modo generalizzato i pacchetti dati con indirizzi di destinazione sconosciuti, ovvero, il dispositivo inoltra questi pacchetti dati a tutte le porte.

10.1.2 Obsolescenza degli indirizzi MAC appresi

Il dispositivo cancella dalla tabella indirizzi MAC (FDB) gli indirizzi che non ha rilevato per un periodo di tempo regolabile (aging time). Un riavvio o il ripristino della tabella indirizzi MAC cancella le voci nella tabella indirizzi MAC (FDB).

10.1.3 Voci di indirizzo statico

Oltre ad apprendere l'indirizzo MAC del mittente, il dispositivo fornisce anche la possibilità di impostare indirizzi MAC manualmente. Questi indirizzi MAC rimangono configurati e sopravvivono al ripristino della tabella indirizzi MAC (FDB) così come al riavvio del dispositivo.

Le voci di indirizzo statico consentono al dispositivo di inoltrare pacchetti dati direttamente alle porte selezionate. Se non si specifica una porta di destinazione, il dispositivo rifiuta i pacchetti dati corrispondenti.

Le voci di indirizzo statico si gestiscono nell'interfaccia grafica utente o nella Command Line Interface.

Eseguire i seguenti passaggi:

☐ Creare una voce di indirizzo statico.

☐ Aprire la finestra di dialogo *Switching > Filter for MAC Addresses*.

☐ Aggiungere un indirizzo MAC configurabile dall'utente:

- Fare clic sul pulsante .
  La finestra di dialogo mostra la finestra *Create*.
- Nel campo *Address* specificare l'indirizzo MAC di destinazione.
- Nel campo *VLAN ID* specificare l'ID della VLAN.
- Nell'elenco *Port*, selezionare le porte a cui il dispositivo inoltra i pacchetti dati con l'indirizzo MAC di destinazione specificato nella VLAN specificata.
  Dopo aver definito un indirizzo MAC Unicast nel campo *Address*, selezionare una sola porta.
  Dopo aver definito un indirizzo MAC Multicast nel campo *Address*, selezionare una o più porte.
  Per far sì che il dispositivo rifiuti i pacchetti dati con l'indirizzo MAC di destinazione, non selezionare nessuna porta.
- Fare clic sul pulsante *Ok*.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`mac-filter <MAC address> <VLAN ID>`	Creare un filtro per indirizzo MAC composto da un indirizzo MAC e da un ID VLAN.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`mac-filter <MAC address> <VLAN ID>`	Assegnare la porta a un filtro per indirizzo MAC creato in precedenza.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

☐ Convertire un indirizzo MAC appreso in una voce di indirizzo statico.

☐ Aprire la finestra di dialogo *Switching > Filter for MAC Addresses*.

☐ Per convertire un indirizzo MAC appreso in una voce di indirizzo statico, selezionare il valore `permanent` nella colonna *Status*.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

☐ Disabilitare una voce di indirizzo statico.

☐ Aprire la finestra di dialogo *Switching > Filter for MAC Addresses*.

☐ Per disabilitare una voce di indirizzo statico, selezionare il valore `invalid` nella colonna *Status*.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`no mac-filter <MAC address> <VLAN ID>`	Annullare l'assegnazione del filtro per indirizzo MAC sulla porta.
`exit`	Passare alla modalità di configurazione.
`no mac-filter <MAC address> <VLAN ID>`	Cancellazione del filtro per indirizzo MAC composto da un indirizzo MAC e da un ID VLAN.
`exit`	Passare alla modalità Privileged EXEC.
`save`	Salvare le impostazioni nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

☐ Cancellare gli indirizzi MAC appresi.

☐ Per cancellare gli indirizzi appresi dalla tabella indirizzi MAC (FDB), aprire la finestra di dialogo *Basic Settings > Restart* e cliccare sul pulsante *Reset MAC address table*.

`clear mac-addr-table`	Cancellare gli indirizzi MAC appresi dalla tabella indirizzi MAC (FDB).

10.2 Multicasts

Di default, il dispositivo invia in modo generalizzato i pacchetti dati con un indirizzo Multicast, ovvero, il dispositivo inoltra i pacchetti dati a tutte le porte. Ne consegue un carico di rete aumentato.

L'utilizzo dell'IGMP snooping può ridurre il carico di rete causato dal traffico dati Multicast. L'IGMP snooping consente al dispositivo di inviare pacchetti dati Multicast solo su quelle porte a cui i dispositivi “interessati” al Multicast sono collegati.

10.2.1 Esempio di un'applicazione Multicast

Le videocamere di sorveglianza trasmettono immagini ai monitor presenti nella sala macchine e nella sala di monitoraggio. Con una trasmissione IP Multicast, le videocamere trasmettono i propri dati grafici attraverso la rete in pacchetti Multicast.

L'Internet Group Management Protocol (IGMP) organizza il traffico dati Multicast tra i monitor e i router Multicast. Gli switch nella rete tra monitor e router Multicast monitorano costantemente il traffico dati IGMP (“IGMP Snooping”).

Gli switch registrano gli accessi per ricevere un flusso Multicast (report IGMP). Il dispositivo crea poi una voce nella tabella indirizzi MAC (FDB) e inoltra i pacchetti Multicast solo alle porte su cui ha precedentemente ricevuto report IGMP.

10.2.2 IGMP Snooping

L'Internet Group Management Protocol (IGMP) descrive la distribuzione delle informazioni Multicast tra router e destinatari collegati sul Layer 3. L'IGMP Snooping descrive la funzione di continuo monitoraggio del traffico IGMP e di ottimizzazione delle impostazioni di trasmissione di uno switch per questo traffico dati.

La funzione *IGMP Snooping* nel dispositivo opera secondo la RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

I router Multicast dotati di una funzione *IGMP* attiva richiedono (query) periodicamente la registrazione di flussi Multicast al fine di determinare i membri del gruppo IP Multicast associati. I membri del gruppo IP Multicast rispondono con un messaggio di rapporto. Questo messaggio di rapporto contiene i parametri richiesti dalla funzione *IGMP*. Il router Multicast immette gli indirizzi del gruppo IP Multicast dal messaggio di rapporto nella sua routing table. Ciò causa l'inoltro dei pacchetti dati con questo gruppo IP Multicast nel campo dell'indirizzo di destinazione in conformità alla sua routing table.

Quando abbandonano un gruppo Multicast (IGMP versione 2 e superiore), i destinatari si scollegano con un messaggio “Leave” e non inviano più alcun messaggio di rapporto. Se non riceve più alcun messaggio di rapporto da questo destinatario entro un certo tempo (aging time), il router Multicast rimuove la voce della routing table di un destinatario.

Quando diversi router IGMP Multicast sono nella stessa rete, il dispositivo con l'indirizzo IP più basso assume la funzione query. Quando non vi sono router Multicast sulla rete, è possibile abilitare la funzione query in uno switch adeguatamente attrezzato.

Uno switch collegato a un destinatario Multicast con un router Multicast analizza le informazioni IGMP con il metodo IGMP snooping.

Il metodo IGMP snooping consente inoltre l'utilizzo della funzione *IGMP* da parte degli switch. Uno switch memorizza gli indirizzi MAC derivati dagli indirizzi IP dei destinatari Multicast come indirizzi Multicast riconosciuti nella sua tabella indirizzi MAC (FDB). Inoltre, lo switch identifica le porte su cui ha ricevuto report per un indirizzo Multicast specifico. In questo modo, lo switch inoltra pacchetti Multicast solo alle porte a cui i destinatari Multicast sono collegati. Le altre porte non ricevono questi pacchetti.

Una funzione particolare del dispositivo è la possibilità di determinare l'elaborazione di pacchetti dati con indirizzi Multicast sconosciuti. In base all'impostazione, il dispositivo rifiuta questi pacchetti dati o li inoltra a tutte le porte. Di default, il dispositivo trasmette i pacchetti dati solo alle porte con dispositivi collegati, che a loro volta ricevono pacchetti query. È inoltre consentito l'invio ulteriore di pacchetti Multicast noti a porte query.

Configurazione dell'IGMP snooping

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > IGMP Snooping > Global*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.

Quando la funzione *IGMP Snooping* è disabilitata, il dispositivo si comporta come segue:

- ▶ Il dispositivo ignora i messaggi di rapporto e query ricevuti.
- ▶ Il dispositivo inoltra (invia in modo generalizzato) i pacchetti dati ricevuti con un indirizzo Multicast come indirizzo di destinazione a tutte le porte.

- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

☐ Definizione delle impostazioni per una porta:

- ☐ Aprire la finestra di dialogo *Switching > IGMP Snooping > Configuration*, scheda *Port*.
- ☐ Per attivare la funzione *IGMP Snooping* su una porta, selezionare la casella di spunta nella colonna *Active* per la porta interessata.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

☐ Definizione delle impostazioni per una VLAN:

- ☐ Aprire la finestra di dialogo *Switching > IGMP Snooping > Configuration*, scheda *VLAN ID*.
- ☐ Per attivare la funzione *IGMP Snooping* per una VLAN specifica, selezionare la casella di spunta nella colonna *Active* per la VLAN interessata.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

Configurazione della funzione IGMP querier

Il dispositivo stesso invia in via opzionale messaggi di query attivi; in alternativa risponde a messaggi di query o rileva altri querier Multicast nella rete (funzione *IGMP Snooping Querier*).

Prerequisito:

La funzione *IGMP Snooping* è abilitata globalmente.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > IGMP Snooping > Querier*.
- ☐ Nel riquadro *Operation*, abilitare/disabilitare la funzione *IGMP Snooping Querier* del dispositivo globalmente.
- ☐ Per attivare la funzione *IGMP Snooping Querier* per una VLAN specifica, selezionare la casella di spunta nella colonna *Active* per la VLAN interessata.
- ▶ Il dispositivo svolge un semplice processo di selezione: quando l'indirizzo sorgente IP dell'altro querierMulticast è inferiore al suo, il dispositivo passa allo stato passivo in cui non invia più alcuna richiesta di query.
- ▶ Nella colonna *Address*, si specifica l'indirizzo IP Multicast che il dispositivo inserisce come indirizzo del mittente nelle richieste di query generate. Si utilizza l'indirizzo del router Multicast.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

Ottimizzazioni dell'IGMP snooping (tabella)

La finestra di dialogo *Switching > IGMP Snooping > Snooping Enhancements* fornisce accesso alle impostazioni ottimizzate per la funzione *IGMP Snooping*. Si attivano o disattivano le impostazioni su base per porta in una VLAN.

Sono possibili le seguenti impostazioni:

- ▶ `Static`
  Utilizzare questa impostazione per definire la porta come porta query statica. Il dispositivo inoltra ogni messaggio IGMP su una porta query statica, anche se non ha precedentemente ricevuto messaggi query IGMP su questa porta. Quando l'opzione statica è disabilitata e il dispositivo ha precedentemente ricevuto messaggi query IGMP, esso inoltra i messaggi IGMP su questa porta. In questo caso, la voce mostra `L` (“learned”).
- ▶ `Learn by LLDP`
  Una porta con queste impostazioni rileva automaticamente altri Schneider Electric dispositivi utilizzando l'LLDP (Link Layer Discovery Protocol). Il dispositivo apprende poi lo stato query IGMP di questa porta da questi Schneider Electric dispositivi e configura la funzione *IGMP Snooping Querier* di conseguenza. La voce `ALA` indica che la funzione `Learn by LLDP` è attivata. Quando il dispositivo ha trovato un altro dispositivo Schneider Electric su questa porta in questa VLAN, la voce mostra anche una `A` (“automatic”).
- ▶ `Forward All`
  Con questa impostazione, il dispositivo inoltra a questa porta i pacchetti dati indirizzati a un indirizzo Multicast. L'impostazione è adatta nelle seguenti situazioni, ad esempio:
  - Ai fini diagnostici.
  - Per dispositivi in un MRP ring: dopo la commutazione dell'anello, la funzione `Forward All` consente di riconfigurare rapidamente la rete per i pacchetti dati con indirizzi di destinazione Multicast registrati. Attivare la funzione `Forward All` su tutte le porte ring.

Prerequisito:

La funzione *IGMP Snooping* è abilitata globalmente.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > IGMP Snooping > Snooping Enhancements*.
- ☐ Fare doppio clic sulla porta desiderata nella VLAN desiderata.
- ☐ Per attivare una o più funzioni, selezionare le opzioni corrispondenti.
- ☐ Fare clic sul pulsante *Ok*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`vlan database`	Passare alla modalità di configurazione VLAN.
`igmp-snooping vlan-id 1 forward-all 1/1`	Attivare la funzione `Forward All` per la porta `1/1` nella VLAN `1`.

Configurare i Multicasts

Il dispositivo consente di configurare lo scambio di pacchetti dati Multicast. Il dispositivo fornisce opzioni diverse a seconda che i pacchetti dati debbano essere inviati a destinatari Multicast noti o sconosciuti.

Le impostazioni per indirizzi Multicast sconosciuti sono globali per l'intero dispositivo. È possibile selezionare le seguenti opzioni:
- Il dispositivo rifiuta i Multicasts sconosciuti.
- Il dispositivo inoltra i Multicasts sconosciuti a tutte le porte.

Nota: Le impostazioni di scambio per gli indirizzi Multicast sconosciuti si applicano agli indirizzi IP riservati dal “Local Network Control Block” (`224.0.0.0..224.0.0.255`). Questo comportamento può influenzare i protocolli di routing di livello superiore.

Per ciascuna VLAN si specifica l'invio di pacchetti Multicast a indirizzi Multicast noti separatamente. È possibile selezionare le seguenti opzioni:
- Il dispositivo inoltra Multicasts noti alle porte che hanno precedentemente ricevuto messaggi di query (porte query) e alle porte registrate. Le porte registrate sono porte con destinatari Multicast registrati con il gruppo Multicast corrispondente. Questa opzione contribuisce a garantire che il trasferimento funzioni con applicazioni di base senza ulteriore configurazione.
- Il dispositivo inoltra i Multicasts noti solo alle porte registrate. Questa impostazione ha il vantaggio di sfruttare al massimo la larghezza di banda disponibile tramite una distribuzione diretta.

Prerequisito:

La funzione *IGMP Snooping* è abilitata globalmente.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > IGMP Snooping > Multicasts*.
- ☐ Nel riquadro *Configuration*, si specifica in che modo il dispositivo invia i pacchetti dati agli indirizzi Multicast sconosciuti.
  - ▶ *send to registered ports*
    Il dispositivo inoltra i pacchetti con l'indirizzo Multicast sconosciuto a tutte le porte query.
- ☐ Nella colonna *Known multicasts*, si specifica in che modo il dispositivo invia i pacchetti dati agli indirizzi Multicast noti nella VLAN corrispondente. Cliccare sul campo interessato e selezionare il valore desiderato.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

10.3 Limitatore del carico

La funzione di limitazione del carico garantisce un funzionamento stabile limitando il traffico sulle porte, anche con volumi di traffico elevati. La limitazione del carico è eseguita singolarmente per ciascuna porta, nonché separatamente per il traffico in ingresso e in uscita.

Se la velocità di trasmissione dei dati supera il limite definito, il dispositivo rifiuta il sovraccarico su questa porta.

La limitazione del carico si verifica interamente sul Layer 2. Durante il processo, la funzione di limitazione del carico ignora le informazioni del protocollo ai livelli superiori, come l'IP o il TCP. Ciò può influenzare il traffico TCP.

Per minimizzare questi effetti, utilizzare le seguenti opzioni:
- Limitare la limitazione del carico a certi tipi di pacchetti, ad esempio Broadcasts, Multicasts, e Unicasts con un indirizzo di destinazione sconosciuto.
- Limitare il traffico dati in uscita invece del traffico in entrata. La limitazione del carico in uscita funziona meglio con il controllo di flusso TCP grazie al buffering interno al dispositivo dei pacchetti dati.
- Aumentare l'aging time per gli indirizzi Unicast appresi.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > Rate Limiter*.
- Attivare il limitatore del carico e impostare i limiti per la velocità di trasmissione dei dati. Le impostazioni si applicano su base per porta e sono suddivise per tipo di traffico:
  - Pacchetti dati Broadcast ricevuti
  - Pacchetti dati Multicast ricevuti
  - Pacchetti dati Unicast ricevuti con un indirizzo di destinazione sconosciuto

  Per attivare la limitazione del carico su una porta, selezionare la casella di spunta per almeno una categoria. Nella colonna *Threshold unit*, si specifica se il dispositivo interpreta i valori di soglia come percentuale della larghezza di banda della porta o come pacchetti al secondo. Il valore di soglia `0` disattiva il limitatore del carico.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

10.4 QoS/Priorità

La QoS (Quality of Service) è una procedura definita nella IEEE 802.1D, utilizzata per distribuire risorse nella rete. La QoS consente di dare priorità ai dati delle applicazioni necessarie.

In presenza di un carico di rete pesante, la priorizzazione contribuisce a evitare che il traffico dati con priorità inferiore interferisca con il traffico dati sensibile a ritardi. Il traffico dati sensibile ai ritardi include, ad esempio, i dati vocali, video e in tempo reale.

10.4.1 Descrizione della priorizzazione

Per la priorizzazione del traffico dati, le classi di traffico sono definite nel dispositivo. Il dispositivo dà priorità a classi di traffico superiori rispetto a classi di traffico inferiori. Il numero delle classi di traffico dipende dal tipo di dispositivo.

Per fornire un flusso dati ottimale per dati sensibili al ritardo, si assegnano classi di traffico superiori a questi dati. Si assegnano classi di traffico inferiori ai dati meno sensibili al ritardo.

Assegnazione delle classi di traffico ai dati

Il dispositivo assegna automaticamente le classi di traffico ai dati in entrata (classificazione del traffico). Il dispositivo prende in considerazione i seguenti criteri di classificazione:

- Metodi utilizzati dal dispositivo per l'assegnazione dei pacchetti dati ricevuti alle classi di traffico:
  - `trustDot1p`
    Il dispositivo utilizza la priorità del pacchetto dati contenuto nella tag VLAN.
  - `trustIpDscp`
    Il dispositivo utilizza le informazioni QoS contenute nello header IP (ToS/DiffServ).
  - `untrusted`
    Il dispositivo ignora le possibili informazioni di priorità all'interno dei pacchetti dati e utilizza direttamente la priorità della porta destinataria.
- La priorità assegnata alla porta destinataria.

È possibile configurare entrambi i criteri di classificazione.

Durante la classificazione del traffico, il dispositivo utilizza le seguenti regole:

- Quando la porta destinataria è impostata su `trustDot1p` (impostazione di default), il dispositivo utilizza la priorità del pacchetto dati contenuta nella tag VLAN. Quando i pacchetti dati non contengono una tag VLAN, il dispositivo è guidato dalla priorità della porta destinataria.
- Quando la porta destinataria è impostata su `trustIpDscp`, il dispositivo utilizza le informazioni QoS (ToS/DiffServ) nello header IP. Quando i pacchetti dati non contengono pacchetti IP, il dispositivo è guidato dalla priorità della porta destinataria.
- Quando la porta destinataria è impostata su `untrusted`, il dispositivo è guidato dalla priorità della porta destinataria.

Priorizzazione delle classi di traffico

Per la priorizzazione delle classi di traffico, il dispositivo utilizza i seguenti metodi:

- `Strict`
  Quando la trasmissione dei dati di una classe di traffico superiore non è più in corso o i dati interessati sono ancora in coda, il dispositivo invia i dati della classe di traffico corrispondente. Se ciascuna classe di traffico è priorizzata secondo il metodo `Strict`, in caso di carico di rete elevato il dispositivo può bloccare i dati delle classi di traffico inferiori in modo permanente.
- `Weighted Fair Queuing`
  La classe di traffico è assegnata a una larghezza di banda specifica. Ciò contribuisce a garantire che il dispositivo invii il traffico dati di questa classe di traffico, sebbene vi sia un notevole traffico dati nelle classi di traffico superiori.

10.4.2 Trattamento di informazioni ricevute in merito alla priorità

Le applicazioni etichettano i pacchetti dati con le seguenti informazioni di priorizzazione:

- Priorità VLAN secondo la IEEE 802.1Q/ 802.1D (Layer 2)
- Type-of-Service (ToS) o DiffServ (DSCP) per pacchetti IP di gestione VLAN (Layer 3)

Il dispositivo consente di valutare queste informazioni di priorità utilizzando le seguenti opzioni:

- `trustDot1p`
  Il dispositivo assegna i pacchetti dati taggati VLAN alle diverse classi di traffico secondo le priorità delle loro VLAN. L'assegnazione corrispondente è configurabile. Il dispositivo assegna la priorità della porta destinataria ai pacchetti dati che riceve senza una tag VLAN.
- `trustIpDscp`
  Il dispositivo assegna i pacchetti IP alle diverse classi di traffico secondo il valore DSCP nello header IP, sebbene il pacchetto fosse anche taggato VLAN. L'assegnazione corrispondente è configurabile. Il dispositivo dà priorità ai pacchetti non-IP secondo la priorità della porta destinataria.
- `untrusted`
  Il dispositivo ignora le informazioni di priorità nei pacchetti dati e assegna loro la priorità della porta destinataria.

10.4.3 Tagging VLAN

Per le funzioni di priorizzazione e VLAN, la norma tecnica IEEE 802.1Q prevede l'integrazione di un frame MAC nella tag VLAN. La tag VLAN è costituita da 4 byte e si trova tra il campo dell'indirizzo sorgente (“Campo indirizzo sorgente”) e il campo del tipo (“Lunghezza / Campo del tipo”).

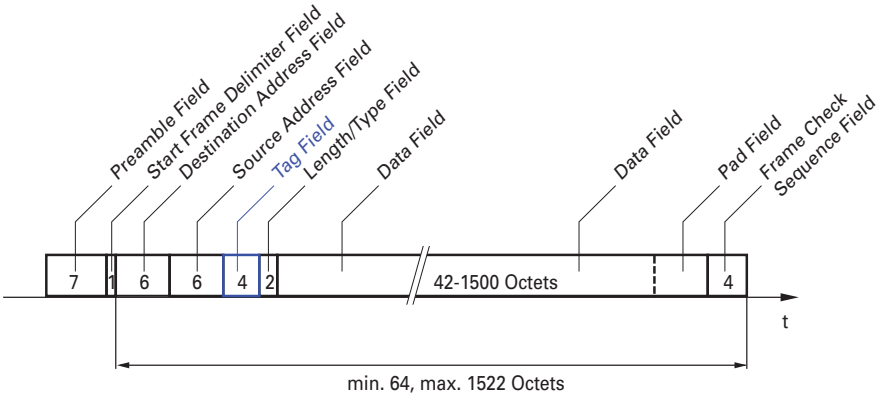


Figura 23: Pacchetto dati ethernet con tag

Per i pacchetti dati con tag VLAN, il dispositivo valuta le seguenti informazioni:
- Informazioni di priorità
- Quando le VLAN sono configurate, tagging VLAN

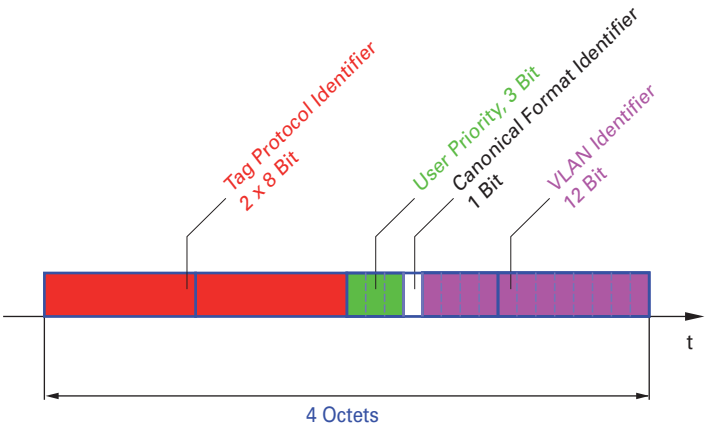


Figura 24: Struttura del tagging VLAN

I pacchetti dati le cui tag VLAN contengono informazione di priorità ma non informazioni VLAN (ID VLAN = 0), prendono il nome di “Priority Tagged Frames”.

Nota: I protocolli di rete e i meccanismi di ridondanza utilizzano la massima classe di traffico 7. Di conseguenza, selezionare altre classi di traffico per i dati di applicazione.

Quando si utilizza la priorizzazione VLAN, considerare le seguenti caratteristiche speciali:
- La priorizzazione end-to-end richiede la trasmissione delle tag VLAN all'intera rete. Il prerequisito è che ogni componente di rete sia compatibile con la VLAN.
- I router non sono in grado di inviare e ricevere pacchetti con tag VLAN attraverso interfacce di router basate su porta.

10.4.4 ToS IP (Tipo di servizio)

Il campo del Type-of-Service (ToS) nello header IP era già parte del protocollo IP dall'inizio, ed è utilizzato per differenziare vari servizi nelle reti IP. Già allora si pensava a un trattamento differenziato dei pacchetti IP per via della ridotta larghezza di banda disponibile e dei percorsi di connessione inaffidabili. Grazie all'aumento progressivo delle larghezze di banda disponibili, non sussisteva la necessità di ricorrere al campo ToS.

Il campo ToS è divenuto nuovamente importante solo grazie ai requisiti di trasmissione in tempo reale delle reti odierne. La selezione del byte ToS dello header IP consente di distinguere i diversi servizi. Tuttavia, questo campo non è ampiamente utilizzato nella pratica.

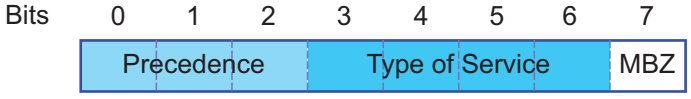


Tabella 22:Campo ToS nello header IP

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput	

Tabella 22:Campo ToS nello header IP (cont

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

10.4.5 Gestione delle classi di traffico

Il dispositivo fornisce le seguenti opzioni per la gestione delle classi di traffico:
- Strict Priority
- Weighted Fair Queuing
- Strict Priority combinata con Weighted Fair Queuing
- Gestione delle code

Descrizione della Strict Priority

Con l'impostazione Strict Priority, il dispositivo trasmette innanzitutto i pacchetti dati con classe di traffico superiore (priorità superiore) prima di trasmettere un pacchetto dati con la massima classe di traffico successiva. In assenza di altri pacchetti dati restanti nella coda, il dispositivo trasmette un pacchetto dati con la classe di traffico più bassa (priorità più bassa). Nei casi sfavorevoli, se vi è un elevato volume di traffico a elevata priorità in attesa di essere inviato su questa porta, il dispositivo non invia pacchetti con una bassa priorità.

In applicazioni sensibili al ritardo, come il VoIP o il video, la Strict Priority consente l'invio immediato dei dati.

Descrizione della Weighted Fair Queuing

Con la Weighted Fair Queuing, detta anche Weighted Round Robin (WRR), l'utente assegna una larghezza di banda minima o riservata a ciascuna classe di traffico. Questo contribuisce a garantire l'invio di pacchetti dati con priorità inferiore anche in caso di elevato carico di rete.

I valori riservati vanno dallo 0% al 100% della larghezza di banda disponibile, a passi dell'1%.
- Una prenotazione di 0 corrisponde a un'impostazione “nessuna larghezza di banda”.
- La somma delle larghezze di banda individuali può arrivare fino al 100%.

Quando si assegna la Weighted Fair Queuing a ogni classe di traffico, l'intera larghezza di banda della porta corrispondente è disponibile.

Combinazione di Strict Priority e Weighted Fair Queuing

Quando si combina la Weighted Fair Queuing con la Strict Priority, verificare che la massima classe di traffico della Weighted Fair Queuing sia inferiore alla classe di traffico più bassa della Strict Priority.

Se si combina la Weighted Fair Queuing con la Strict Priority, un carico di rete elevato Strict Priority può ridurre notevolmente la larghezza di banda disponibile per la Weighted Fair Queuing.

10.4.6 Gestione delle code

Queue Shaping

Queue Shaping accelera la velocità di trasmissione dei pacchetti da parte delle code. Ad esempio, utilizzando Queue Shaping si limita la velocità di una coda con strict-priority superiore di modo che consenta l'invio di pacchetti da parte di una coda con strict-priority inferiore anche nel caso in cui i pacchetti a priorità superiore siano ancora disponibili per la trasmissione. Il dispositivo consente di impostare la Queue Shaping per qualsiasi coda. Si specifica la Queue Shaping alla massima velocità di passaggio del traffico attraverso una coda assegnando una percentuale della larghezza di banda disponibile.

Definizione delle impostazioni per la gestione delle code

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > QoS/Priority > Queue Management*.

La larghezza di banda totale assegnata nella colonna *Min. bandwidth [%]* è pari al 100%.

- ☐ Per attivare la Weighted Fair Queuing per la *Traffic class* = `0`, procedere come segue:
  - ▶ Deselezionare la casella di spunta nella colonna *Strict priority*.
  - ▶ Nella colonna *Min. bandwidth [%]*, specificare il valore `5`.
- ☐ Per attivare la Weighted Fair Queuing per la *Traffic class* = `1`, procedere come segue:
  - ▶ Deselezionare la casella di spunta nella colonna *Strict priority*.
  - ▶ Nella colonna *Min. bandwidth [%]*, specificare il valore `20`.
- ☐ Per attivare la Weighted Fair Queuing per la *Traffic class* = `2`, procedere come segue:
  - ▶ Deselezionare la casella di spunta nella colonna *Strict priority*.
  - ▶ Nella colonna *Min. bandwidth [%]*, specificare il valore `30`.
- ☐ Per attivare la Weighted Fair Queuing per la *Traffic class* = `3`, procedere come segue:
  - ▶ Deselezionare la casella di spunta nella colonna *Strict priority*.
  - ▶ Nella colonna *Min. bandwidth [%]*, specificare il valore `20`.
- ☐ Per attivare la Weighted Fair Queuing e la Queue Shaping per la *Traffic class* = `4`, procedere come segue:
  - ▶ Deselezionare la casella di spunta nella colonna *Strict priority*.
  - ▶ Nella colonna *Min. bandwidth [%]*, specificare il valore `10`.
  - ▶ Nella colonna *Max. bandwidth [%]*, specificare il valore `10`.

  Durante l'utilizzo di una combinazione di Weighted Fair Queuing e Queue Shaping per una specifica classe di traffico, si specifica un valore superiore nella colonna *Max. bandwidth [%]* rispetto al valore specificato nella colonna *Min. bandwidth [%]*.

- ☐ Per attivare la Weighted Fair Queuing per la *Traffic class* = 5, procedere come segue:
  - ▶ Deselezionare la casella di spunta nella colonna *Strict priority*.
  - ▶ Nella colonna *Min. bandwidth [%]*, specificare il valore 5.
- ☐ Per attivare la Weighted Fair Queuing per la *Traffic class* = 6, procedere come segue:
  - ▶ Deselezionare la casella di spunta nella colonna *Strict priority*.
  - ▶ Nella colonna *Min. bandwidth [%]*, specificare il valore 10.
- ☐ Per attivare la Strict Priority e la Queue Shaping per la *Traffic class* = 7, procedere come segue:
  - ▶ Selezionare la casella di spunta nella colonna *Strict priority*.
  - ▶ Nella colonna *Max. bandwidth [%]*, specificare il valore 10.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`cos-queue weighted 0`	Abilitazione della Weighted Fair Queuing per la classe di traffico 0.
`cos-queue min-bandwidth: 0 5`	Assegnazione di un peso pari al 5 % alla classe di traffico 0.
`cos-queue weighted 1`	Abilitazione della Weighted Fair Queuing per la classe di traffico 1.
`cos-queue min-bandwidth: 1 20`	Assegnazione di un peso pari al 20 % alla classe di traffico 1.
`cos-queue weighted 2`	Abilitazione della Weighted Fair Queuing per la classe di traffico 2.
`cos-queue min-bandwidth: 2 30`	Assegnazione di un peso pari al 30 % alla classe di traffico 2.
`cos-queue weighted 3`	Abilitazione della Weighted Fair Queuing per la classe di traffico 3.
`cos-queue min-bandwidth: 3 20`	Assegnazione di un peso pari al 20 % alla classe di traffico 3.

```
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         0               0               strict
5         0               0               strict
6         0               0               strict
7         0               0               strict
```

Combinazione di Weighted Fair Queuing e Queue Shaping

Eseguire i seguenti passaggi:

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`cos-queue weighted 4`	Abilitazione della Weighted Fair Queuing per la classe di traffico 4.

`cos-queue min-bandwidth: 4 10`	Assegnazione di un peso pari al `10` % alla classe di traffico `4`.
`cos-queue max-bandwidth: 4 10`	Assegnazione di un peso pari al `10` % alla classe di traffico `4`.
`cos-queue weighted 5`	Abilitazione della Weighted Fair Queuing per la classe di traffico `5`.
`cos-queue min-bandwidth: 5 5`	Assegnazione di un peso pari al `5` % alla classe di traffico `5`.
`cos-queue weighted 6`	Abilitazione della Weighted Fair Queuing per la classe di traffico `6`.
`cos-queue min-bandwidth: 6 10`	Assegnazione di un peso pari al `10` % alla classe di traffico `6`.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

Impostazione della Queue Shaping

Eseguire i seguenti passaggi:

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`cos-queue max-bandwidth: 7 10`	Assegnazione di un peso pari al `10` % alla classe di traffico `7`.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

10.4.7 Priorizzazione della gestione

Per consentire l'accesso costante alla gestione del dispositivo, sebbene vi sia un elevato carico di rete, il dispositivo consente di dare priorità ai pacchetti di gestione.

Quando si dà priorità ai pacchetti di gestione, il dispositivo invia i pacchetti di gestione con le informazioni di priorità.

- Sul Layer 2, il dispositivo modifica la priorità VLAN nella tag VLAN.
  Il prerequisito per questa funzione è che le porte corrispondenti siano impostate per consentire l'invio dei pacchetti con una tag VLAN.
- Sul Layer 3, il dispositivo modifica il valore IP DSCP.

10.4.8 Impostazione dell'ordine di priorità

Assegnazione di priorità di porta

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > QoS/Priority > Port Configuration*.
- ☐ Nella colonna *Port priority*, si specifica la priorità con cui il dispositivo inoltra i pacchetti dati ricevuti su questa porta senza una tag VLAN.
- ☐ Nella colonna *Trust mode*, si specificano i criteri utilizzati dal dispositivo per assegnare una classe di traffico ai pacchetti dati ricevuti.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`vlan priority 3`	Assegnare all'interfaccia `1/1` la priorità di porta `3`.
`exit`	Passare alla modalità di configurazione.

Assegnazione della priorità VLAN a una classe di traffico

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > QoS/Priority > 802.1D/p Mapping*.
- ☐ Per assegnare una classe di traffico a una priorità VLAN, immettere il valore associato nella colonna *Traffic class*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`classofservice dot1p-mapping 0 2`	Assegnazione di una priorità VLAN pari a `0` alla classe di traffico `2`.
`classofservice dot1p-mapping 1 2`	Assegnazione di una priorità VLAN pari a `1` alla classe di traffico `2`.
`exit`	Passare alla modalità Privileged EXEC.
`show classofservice dot1p-mapping`	Visualizza l'assegnazione.

Assegnare la priorità della porta ai pacchetti dati ricevuti

Eseguire i seguenti passaggi:

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`classofservice trust untrusted`	Assegnazione della modalità `untrusted` all'interfaccia.
`classofservice dot1p-mapping 0 2` `classofservice dot1p-mapping 1 2`	Assegnazione di una priorità VLAN pari a `0` alla classe di traffico `2`. Assegnazione di una priorità VLAN pari a `1` alla classe di traffico `2`.
`vlan priority 1`	Definizione del valore `1` per la priorità della porta.
`exit`	Passare alla modalità di configurazione.
`exit`	Passare alla modalità Privileged EXEC.
`show classofservice trust`	Visualizzazione della modalità Trust delle porte/interfacce.

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

Assegnazione del DSCP a una classe di traffico

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > QoS/Priority > IP DSCP Mapping*.
- ☐ Specificare il valore desiderato nella colonna *Traffic class*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

```
enable                                  Passare alla modalità Privileged EXEC.
configure                               Passare alla modalità di configurazione.
classofservice  ip-dscp-mapping cs1 1   Assegnazione del valore DSCP CS1 alla classe di traffico 1.
show classofservice  ip-dscp-mapping    Visualizzazione delle assegnazioni IP DSCP

    IP DSCP       Traffic Class
 -------------    -------------
   be                  2
   1                   2
   .                   .
   .                   .
   (cs1)               1
   .                   .
```

Assegnare la priorità DSCP ai pacchetti dati IP ricevuti

Eseguire i seguenti passaggi:

```
enable                                  Passare alla modalità Privileged EXEC.
configure                               Passare alla modalità di configurazione.
interface 1/1                           Passare alla modalità di configurazione di interfaccia 1/1.
classofservice trust ip-dscp            Assegnazione della modalità trust ip-dscp globalmente.
exit                                    Passare alla modalità di configurazione.
show classofservice trust               Visualizzazione della modalità Trust delle porte/interfacce.

 Interface     Trust Mode
 ----------    -------------
 1/1           ip-dscp
 1/2           dot1p
 1/3           dot1p
 .             .
 .             .
 1/5           dot1p
 .             .
```

Specifica la traffic shaping su una porta

Eseguire i seguenti passaggi:

```
enable                                  Passare alla modalità Privileged EXEC.
configure                               Passare alla modalità di configurazione.
interface 1/2                           Passare alla modalità di configurazione di interfaccia 1/2.
traffic-shape bw 50                     Limitazione della massima larghezza di banda della porta 1/2 al 50%.
exit                                    Passare alla modalità di configurazione.
```

```
exit
```
Passare alla modalità Privileged EXEC.

```
show traffic-shape
```
Mostrare la configurazione del Traffic Shaping.

```
Interface  Shaping rate
---------  ------------
1/1        0  %
1/2        50 %
1/3        0  %
1/4        0  %
```

Configurazione della priorità di gestione Layer 2

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > QoS/Priority > Global*.
- ☐ Nel campo *VLAN priority for management packets*, specificare la priorità VLAN con cui il dispositivo invia i pacchetti dati di gestione.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

```
enable
```
Passare alla modalità Privileged EXEC.

```
network management priority dot1p 7
```
Assegnazione della priorità VLAN 7 ai pacchetti di gestione. Il dispositivo invia i pacchetti di gestione con la massima priorità.

```
show network parms
```
Visualizzazione della priorità della VLAN in cui si trova la gestione del dispositivo.

```
IPv4 Network
------------
...
Management VLAN priority.....................7
...
```

Configurazione della priorità di gestione Layer 3

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > QoS/Priority > Global*.
- ☐ Nel campo *IP DSCP value for management packets*, specificare il valore DSCP con cui il dispositivo invia pacchetti dati di gestione.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

```
enable
```
Passare alla modalità Privileged EXEC.

```
network management priority ip-dscp 56
```

Assegnazione del valore DSCP 56 ai pacchetti di gestione. Il dispositivo invia i pacchetti di gestione con la massima priorità.

```
show network parms
```

Visualizzazione della priorità della VLAN in cui si trova la gestione del dispositivo.

```
IPv4 Network
------------
...
Management IP-DSCP value.....................56
```

10.5 Controllo di flusso

La ricezione simultanea di un grande numero di pacchetti dati nella coda di priorità di una porta può causare l'esubero della memoria della porta. Ciò accade, ad esempio, quando il dispositivo riceve dati su una porta Gigabit e li inoltra ad una porta con una larghezza di banda inferiore. Il dispositivo rifiuta i pacchetti dati in eccesso.

Il meccanismo del controllo di flusso descritto nella norma tecnica IEEE 802.3 contribuisce a garantire che nessun pacchetto dati sia perso a causa dell'esubero della memoria di una porta. Poco prima che la memoria di una porta sia completamente piena, il dispositivo segnala ai dispositivi collegati l'indisponibilità ad accettare altri pacchetti dati provenienti da essi.

- Nella modalità duplex pieno, il dispositivo invia un pacchetto dati “pause”.
- Nella modalità semi duplex, il dispositivo simula una collisione.

La figura seguente mostra come funziona il controllo di flusso. Le postazioni di lavoro 1, 2 e 3 desiderano trasmettere contemporaneamente un'ampia quantità di dati alla postazione di lavoro 4. La larghezza di banda combinata delle postazioni di lavoro 1, 2 e 3 è maggiore della larghezza di banda della postazione di lavoro 4. Ciò causa un esubero nella coda di ricezione della porta 4. L'imbuto di sinistra simboleggia lo stato.

Quando la funzione del controllo di flusso sulle porte 1, 2 e 3 del dispositivo è abilitata, il dispositivo reagisce prima che l'imbuto trabocchi. L'imbuto sulla destra illustra l'invio di un messaggio da parte delle porte 1, 2 e 3 ai dispositivi trasmittenti per controllare la velocità di trasmissione. Di conseguenza la porta destinataria non è più sopraffatta ed è in grado di elaborare il traffico in ingresso.

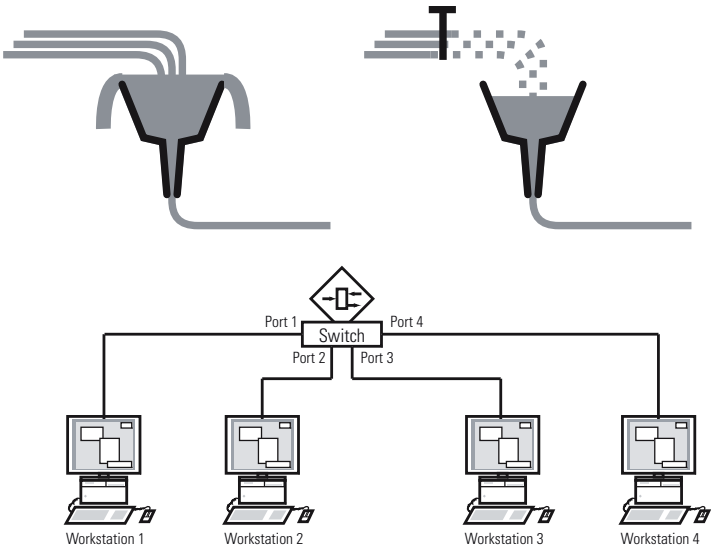


Figura 25: Esempio di controllo di flusso

10.5.1 Collegamento semi duplex o duplex pieno

Controllo di flusso con un collegamento semi duplex

Nell'esempio vi è un collegamento semi duplex tra la postazione di lavoro 2 e il dispositivo.

Prima che nella coda di invio della porta 2 si verifichi un esubero, il dispositivo rimanda i dati alla postazione di lavoro 2. La postazione di lavoro 2 rileva una collisione e interrompe la trasmissione.

Controllo di flusso con un collegamento duplex pieno

Nell'esempio, vi è un collegamento duplex pieno tra la postazione di lavoro 2 e il dispositivo.

Prima che nella coda di invio della porta 2 si verifichi un esubero, il dispositivo invia una richiesta alla postazione di lavoro 2 per includere una piccola interruzione nella trasmissione d'invio.

10.5.2 Configurazione del controllo di flusso

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > Global*.
- ☐ Selezionare la casella di spunta *Flow control*.
  Con questa impostazione si abilita il controllo di flusso nel dispositivo.
- ☐ Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
- ☐ Per abilitare il controllo di flusso su una porta, selezionare la casella di spunta nella colonna *Flow control*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

Nota: Quando si utilizza una funzionalità di ridondanza, si disattiva il controllo di flusso sulle porte interessate. Se la funzionalità di ridondanza e il controllo del flusso sono attivi contemporaneamente, è possibile che la funzionalità di ridondanza operi in modo diverso dal previsto.

11 Configurazione di TSN basata su template

11.1 Riferimenti

Quando si utilizza la funzione *TSN* si applicano le seguenti condizioni di base:

- Il dispositivo utilizza il metodo "Store and Forward". Pertanto, il dispositivo deve ricevere il pacchetto dati completo prima di decidere di eseguire l'inoltro.
- Specificare il base time e il cycle time una volta nel dispositivo. Entrambe le impostazioni sono valide per ciascuna porta che partecipa nella TSN.
- Per un'impostazione più semplice, configurare un Gate Control List per porta basato sui template predefiniti.
- Verificare che la somma delle voci di ingresso del Gate Control List sia inferiore o pari al cycle time specificato.
- Il dispositivo utilizza una banda di guardia per contribuire a proteggere la finestra temporale per i pacchetti con priorità elevata dai pacchetti "persi" dalla finestra temporale precedente. Il fattore decisivo per la durata dell'intervallo della banda di guardia è la velocità della porta mittente. Per la banda di guardia raccomandiamo le seguenti durate di intervallo. I valori si basano sulla velocità della porta e sulle dimensioni minime consentite dei pacchetti Ethernet:
  - 2.5 Gbit/s: 5 µs
  - 1 Gbit/s: 13 µs
  - 100 Mbit/s: 124 µs
- L'intervallo del cycle time è 50 000..10 000 000 ns.
- L'intervallo del Gate Control List è 1 000..10 000 000 ns.
- Verificare che entrambi gli intervalli del cycle time e del Gate Control List siano multipli di 1 µs, 2 µs o 4 µs.

Tabella 23:Dipendenza tra cycle time e granularità .

Cycle time	Granularità
50 µs..4 ms	1 µs
4.002 ms..8 ms	2 µs
8.004 ms..10 ms	4 µs

11.2 Esempio

Questo esempio descrive come configurare i dispositivi nel caso di uno scenario con le seguenti condizioni:
- Cycle time = 1 ms
- Finestra temporale per pacchetti ad alta priorità = 500 µs
- Finestra temporale per pacchetti a bassa priorità = 487 µs

In questo esempio ogni dispositivo è collegato alla rete con una velocità della porta di 1 Gbit/s.

Tabella 24:Struttura del ciclo

Finestra temporale	Classi di traffico	Durata
Pacchetti ad alta priorità	7	500 µs
Pacchetti a bassa priorità	0,1,2,3,4,5,6	487 µs
Banda di guardia	–	13 µs

11.2.1 Calcolo del tempo

Il dispositivo calcola automaticamente la durata della finestra temporale per i pacchetti a bassa priorità. Il calcolo si basa sui seguenti parametri:
- Cycle time
- Durata della finestra temporale per i pacchetti ad alta priorità
- Durata della banda di guardia

11.2.2 Configurare i dispositivi

Utilizzando i tempi sopra specificati, configurare i dispositivi utilizzando l'interfaccia grafica utente o la Command Line Interface. Eseguire i seguenti passaggi per ogni dispositivo coinvolto.

Verificare e adeguare il cycle time

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > TSN > Configuration*.
- ☐ Verificare nel riquadro *Configuration* il valore nel campo *Cycle time [ns]*.
- ☐ Se necessario, adeguare il valore.

- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

```
enable                                          Passare alla modalità Privileged EXEC.
configure                                       Passare alla modalità di configurazione.
show tsn configuration
Port  Status                 Conf. cycle time[ns]  Conf. base time
      Default gate states    Curr. cycle time[ns]  Curr. base time
      Config change pending                        Time of last activation
----  ---------------------  --------------------  ------------------------------
 1/1  [x]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01 00:00:00.000000000
      [ ]                                          2018-07-12 08:10:58.813000000

 1/2  [x]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01 00:00:00.000000000
      [ ]                                          2018-07-11 07:24:35.204000000

 1/3  [ ]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01 00:00:00.000000000
      [ ]                                          1970-01-01 00:00:00.000000000

 1/4  [ ]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01 00:00:00.000000000
      [ ]                                          1970-01-01 00:00:00.000000000

tsn cycle-time 1000000                          Se necessario, adeguare il valore.
```

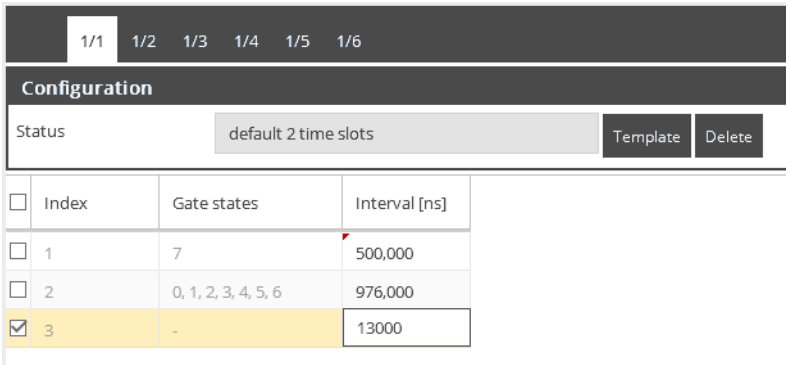
Selezionare un template e configurare il Gate Control List

Il dispositivo fornisce template predefiniti per facilitare la configurazione del Gate Control List. In questo esempio si utilizza il template *default 2 time slots*. Dopo aver selezionato il template è possibile adeguare la durata delle finestre temporali. Eseguire i seguenti passaggi per ogni porta in cui si desidera utilizzare la funzione *TSN*.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > TSN > Gate Control List > Configured*.
- ☐ Selezionare la scheda per la porta per la quale si desidera specificare le impostazioni.

- ☐ Selezionare un template nel riquadro *Configuration*.
  Eseguire i seguenti passaggi:
  - Fare clic sul pulsante *Template*.
  - Selezionare la voce `default 2 time slots`.
  - Fare clic sul pulsante *Ok*.
- ☐ Adeguare i valori nella colonna *Interval [ns]*:
  - Immettere il valore `500000` nella riga per i pacchetti ad alta priorità.
  - Immettere il valore `13000` nella riga per la banda di guardia.
  - Il dispositivo calcola il terzo valore automaticamente quando vengono salvate le modifiche.



- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`tsn gcl modify 1 interval 500000`	Adeguare la durata in nanosecondi della finestra temporale per i pacchetti ad alta priorità.
`tsn gcl modify 3 interval 13000`	Adeguare la durata in nanosecondi della finestra temporale per la banda di guardia. Il dispositivo calcola automaticamente la durata della finestra temporale per i pacchetti a bassa priorità. Non è possibile impostare la finestra temporale per i pacchetti a bassa priorità.

12 VLAN

Nel caso più semplice, una VLAN (VLAN) è costituita da un gruppo di utenze in un segmento di rete che possono comunicare tra loro come se appartenessero a una LAN separata.

Le VLAN più complesse si estendono lungo più segmenti di rete e si basano, inoltre, su porte logiche (invece che unicamente fisiche) tra le utenze. Le VLAN sono elementi di progettazione flessibile della rete. È più semplice riconfigurare centralmente porte logiche rispetto a porte cablate.

Il dispositivo supporta l'apprendimento VLAN indipendente in conformità alla norma IEEE 802.1Q che definisce la funzione *VLAN*.

L'utilizzo delle VLAN presenta molti vantaggi. L'elenco seguente mostra i vantaggi principali:

- Limitazione del carico di rete.
  Le VLAN riducono notevolmente il carico di rete mentre il dispositivo trasmette pacchetti Broadcast, Multicast, e Unicast con indirizzi di destinazione (non appresi) sconosciuti solo all'interno della VLAN. Il resto della rete di dati inoltra il traffico come di consueto.
- Flessibilità
  È possibile formare gruppi di utenti in base alla funzione dei partecipanti, indipendentemente dalla loro posizione fisica o dal loro supporto.
- Trasparenza
  Le VLAN forniscono alla rete una struttura trasparente e semplificano la manutenzione.

12.1 Esempi di VLAN

I seguenti esempi pratici forniscono una rapida introduzione alla struttura di una VLAN.

Nota: Quando si configurano le VLAN si utilizza un'interfaccia per accedere alla gestione del dispositivo che rimarrà invariata. Per questo esempio, per configurare le VLAN si utilizza l'interfaccia 1/6 o la porta seriale.

12.1.1 Esempio 1

L'esempio mostra una configurazione VLAN minima (VLAN basata su porta). Un amministratore ha connesso più dispositivi finali a un dispositivo di trasmissione e li ha assegnati a 2 VLAN. Ciò impedisce di fatto qualsiasi trasmissione dati tra le VLAN, i cui membri comunicano solo all'interno delle proprie VLAN.

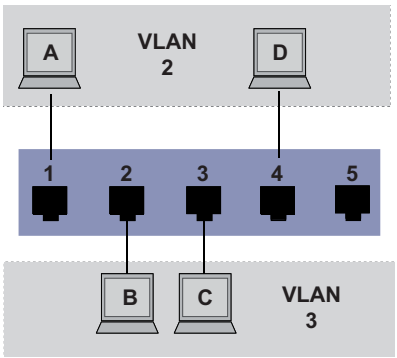


Figura 26: Esempio di una VLAN semplice basata su porta

Durante la configurazione delle VLAN si creano regole di comunicazione per ciascuna porta, che si inseriscono in tabelle di ingresso (ingress) e di uscita (egress).

La tabella di ingresso stabilisce quale ID VLAN viene assegnato da una porta ai pacchetti di dati in ingresso. Si utilizza così l'indirizzo della porta del dispositivo finale per assegnarlo a una VLAN.

La tabella di uscita specifica su quali porte il dispositivo invia i pacchetti da questa VLAN.
- `T` = Taggato (con un campo tag, contrassegnato)
- `U` = Non taggato (senza un campo tag, non contrassegnato)

Per questo esempio, lo stato del campo TAG dei pacchetti dati non ha alcuna rilevanza, pertanto si utilizza l'impostazione `U`.

Tabella 25:Tabella di ingresso

Dispositivo finale	Porta	Identificativo della porta VLAN (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Tabella 26:Tabella di uscita

ID VLAN	Porta				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Eseguire i seguenti passaggi:
☐ Impostazione della VLAN

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Configuration*.
- ☐ Fare clic sul pulsante  .
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Specificare il valore `2` nel campo *VLAN ID*.
- ☐ Fare clic sul pulsante *Ok*.
- ☐ Per la VLAN, specificare il nome `VLAN2`:
  Fare doppio clic nella colonna *Name* e specificare il nome.
  Per la VLAN `1`, nella colonna *Name*, modificare il valore `Default` in `VLAN1`.
- ☐ Ripetere i precedenti passaggi per creare una VLAN `3` con il nome `VLAN3`.

`enable`	Passare alla modalità Privileged EXEC.
`vlan database`	Passare alla modalità di configurazione VLAN.
`vlan add 2`	Crea una nuova VLAN con l'ID VLAN `2`.
`name 2 VLAN2`	Assegnare il nome `2` alla VLAN `VLAN2`.
`vlan add 3`	Crea una nuova VLAN con l'ID VLAN `3`.
`name 3 VLAN3`	Assegnare il nome `3` alla VLAN `VLAN3`.
`name 1 VLAN1`	Assegnare il nome `1` alla VLAN `VLAN1`.
`exit`	Passare alla modalità Privileged EXEC.
`show vlan brief`	Mostrare la configurazione VLAN corrente.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ Impostazione delle porte

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Per assegnare la porta a una VLAN, specificare il valore desiderato nella colonna corrispondente.
  Possibili valori:
  - `T` = La porta fa parte della VLAN. La porta trasmette i pacchetti dati taggati.
  - `U` = La porta fa parte della VLAN. La porta trasmette i pacchetti dati non taggati.
  - `F` = La porta non fa parte della VLAN.
    Le modifiche tramite la funzione *GVRP* sono disabilitate.
  - `-` = La porta non fa parte di questa VLAN.
    Le modifiche tramite la funzione *GVRP* sono consentite.

  Dato che i dispositivi finali solitamente interpretano i pacchetti dati non taggati, si specifica il valore `U`.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.
- ☐ Aprire la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Nella colonna *Port-VLAN ID*, specificare l'ID VLAN della relativa VLAN:
  `2` o `3`
- ☐ Dato che i dispositivi finali solitamente interpretano i pacchetti dati non taggati, nella colonna *Acceptable packet types* si specifica il valore `admitAll` per le porte del dispositivo finale.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Il valore nella colonna *Ingress filtering* non ha alcun effetto sul funzionamento di questo esempio.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.

`vlan participation include 2`	La porta `1/1` entra a far parte della VLAN `2` e trasmette i pacchetti dati senza una tag VLAN.
`vlan pvid 2`	Assegnare l'ID VLAN `1/1` della porta alla porta `2`.
`exit`	Passare alla modalità di configurazione.
`interface 1/2`	Passare alla modalità di configurazione di interfaccia `1/2`.
`vlan participation include 3`	La porta `1/2` entra a far parte della VLAN `3` e trasmette i pacchetti dati senza una tag VLAN.
`vlan pvid 3`	Assegnare l'ID VLAN `1/2` della porta alla porta `3`.
`exit`	Passare alla modalità di configurazione.
`interface 1/3`	Passare alla modalità di configurazione di interfaccia `1/3`.
`vlan participation include 3`	La porta `1/3` entra a far parte della VLAN `3` e trasmette i pacchetti dati senza una tag VLAN.
`vlan pvid 3`	Assegnare l'ID VLAN `1/3` della porta alla porta `3`.
`exit`	Passare alla modalità di configurazione.
`interface 1/4`	Passare alla modalità di configurazione di interfaccia `1/4`.
`vlan participation include 2`	La porta `1/4` entra a far parte della VLAN `2` e trasmette i pacchetti dati senza una tag VLAN.
`vlan pvid 2`	Assegnare l'ID VLAN `1/4` della porta alla porta `2`.
`exit`	Passare alla modalità di configurazione.
`exit`	Passare alla modalità Privileged EXEC.
`show vlan id 3`	Mostra dettagli per la VLAN `3`.

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1            -      Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4            -      Autodetect   Tagged
1/5            -      Autodetect   Tagged
```

12.1.2 Esempio 2

Il secondo esempio mostra una configurazione più compressa con 3 VLAN (da 1 a 3). Insieme allo Switch dell'esempio 1 si utilizza un 2° Switch (sulla destra nell'esempio).

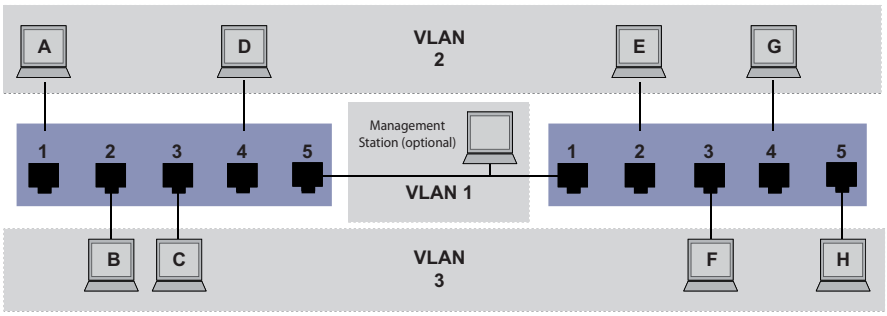


Figura 27: Esempio di una configurazione VLAN più complessa

I dispositivi dispositivi finali delle singole VLAN (da A ad H) si estendono lungo 2 dispositivi di trasmissione (Switch). Queste VLAN prendono pertanto il nome di VLAN distribuite. Se la VLAN è configurata correttamente, compare anche una network management station opzionale, che consente l'accesso a tutti i componenti di rete.

Nota: In questo caso, la VLAN 1 non ha alcuna rilevanza per la comunicazione del dispositivo finale, ma è necessaria per l'amministrazione dei dispositivi di trasmissione tramite la cosiddetta VLAN di gestione.

Procedere a un'assegnazione univoca a una VLAN delle porte con i rispettivi dispositivi finali connessi, come riportato nell'esempio precedente. Con la porta diretta tra i 2 dispositivi di trasmissione (uplink) le porte trasportano i pacchetti per entrambe le VLAN. Per differenziare questi uplink si utilizza il “tagging VLAN”, che gestisce i pacchetti dati in maniera adeguata. Di conseguenza, si mantiene l'assegnazione alle rispettive VLAN.

Eseguire i seguenti passaggi:
- ☐ Aggiungere la porta Uplink 5 alle tabelle di ingresso e di uscita dell'esempio 1.
- ☐ Creare nuove tabelle di ingresso e di uscita per lo switch corretto, come descritto nel primo esempio.

La tabella di uscita specifica su quali porte il dispositivo invia i pacchetti da questa VLAN.
- ▶ `T` = Taggato (con un campo tag, contrassegnato)
- ▶ `U` = Non taggato (senza un campo tag, non contrassegnato)

In questo esempio, i pacchetti taggati sono utilizzati nella comunicazione tra i dispositivi di trasmissione (Uplink), dal momento che i pacchetti per le diverse VLAN sono differenziati su queste porte.

Tabella 27:Tabella di ingresso dispositivo a sinistra

Dispositivo finale	Porta	Identificativo della porta VLAN (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Tabella 28:Tabella di ingresso dispositivo a destra

Dispositivo finale	Porta	Identificativo della porta VLAN (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

Tabella 29:Tabella di uscita dispositivo a sinistra

ID VLAN	Porta				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Tabella 30:Tabella di uscita dispositivo a destra

ID VLAN	Porta				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

Le relazioni di comunicazione sono le seguenti: i dispositivi finali sulle porte 1 e 4 del dispositivo di sinistra e i dispositivi finali sulle porte 2 e 4 del dispositivo di destra fanno parte della VLAN 2 e possono pertanto comunicare tra loro. Il comportamento è lo stesso per i dispositivi finali sulle porte 2 e 3 del dispositivo di sinistra e per i dispositivi finali sulle porte 3 e 5 del dispositivo di destra. Questi appartengono alla VLAN 3.

I dispositivi finali “vedono” la loro parte corrispondente della rete. I partecipanti all'esterno di questa VLAN non sono raggiungibili. Il dispositivo invia anche pacchetti Broadcast, Multicast, e Unicast con indirizzi di destinazione (non appresi) sconosciuti solo all'interno di una VLAN.

Qui, i dispositivi utilizzano il tagging VLAN (IEEE 801.1Q) all'interno della VLAN con l'ID 1 (Uplink). La lettera `T` nella tabella di uscita delle porte indica il tagging VLAN.

La configurazione dell'esempio è la stessa per il dispositivo a destra. Procedere allo stesso modo, utilizzando le tabelle di ingresso e di uscita create sopra per adattare il dispositivo a sinistra precedentemente configurato al nuovo ambiente.

Eseguire i seguenti passaggi:
- ☐ Impostazione della VLAN

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Configuration*.
- ☐ Fare clic sul pulsante  .
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Nel campo *VLAN ID*, specificare l'ID VLAN, ad esempio `2`.

- ☐ Fare clic sul pulsante *Ok*.
- ☐ Per la VLAN, specificare il nome `VLAN2`:
  Fare doppio clic nella colonna *Name* e specificare il nome.
  Per la VLAN `1`, nella colonna *Name*, modificare il valore `Default` in `VLAN1`.
- ☐ Ripetere i precedenti passaggi per creare una VLAN `3` con il nome `VLAN3`.

`enable`	Passare alla modalità Privileged EXEC.
`vlan database`	Passare alla modalità di configurazione VLAN.
`vlan add 2`	Crea una nuova VLAN con l'ID VLAN `2`.
`name 2 VLAN2`	Assegnare il nome `2` alla VLAN `VLAN2`.
`vlan add 3`	Crea una nuova VLAN con l'ID VLAN `3`.
`name 3 VLAN3`	Assegnare il nome `3` alla VLAN `VLAN3`.
`name 1 VLAN1`	Assegnare il nome `1` alla VLAN `VLAN1`.
`exit`	Passare alla modalità Privileged EXEC.
`show vlan brief`	Mostrare la configurazione VLAN corrente.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ Impostazione delle porte

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Per assegnare la porta a una VLAN, specificare il valore desiderato nella colonna corrispondente.
  Possibili valori:
  - `T` = La porta fa parte della VLAN. La porta trasmette i pacchetti dati taggati.
  - `U` = La porta fa parte della VLAN. La porta trasmette i pacchetti dati non taggati.
  - `F` = La porta non fa parte della VLAN.
    Le modifiche tramite la funzione *GVRP* sono disabilitate.
  - `-` = La porta non fa parte di questa VLAN.
    Le modifiche tramite la funzione *GVRP* sono disabilitate.

  Dato che i dispositivi finali solitamente interpretano i pacchetti dati non taggati, si specifica il valore `U`.
  Si specifica l'impostazione `T` sulla porta uplink su qui le VLAN comunicano tra loro.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.
- ☐ Aprire la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Nella colonna *Port-VLAN ID*, specificare l'ID VLAN della relativa VLAN:
  `1`, `2` o `3`
- ☐ Dato che i dispositivi finali solitamente interpretano i pacchetti dati non taggati, nella colonna *Acceptable packet types* si specifica il valore `admitAll` per le porte del dispositivo finale.

- ☐ Per la porta uplink, nella colonna *Acceptable packet types* si specifica il valore `admitOnlyVlanTagged`.
- ☐ Contrassegnare la casella di spunta nella colonna *Ingress filtering* per favorire la valutazione delle tag VLAN da parte delle porte uplink su questa porta.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`vlan participation include 1`	La porta `1/1` entra a far parte della VLAN `1` e trasmette i pacchetti dati senza una tag VLAN.
`vlan participation include 2`	La porta `1/1` entra a far parte della VLAN `2` e trasmette i pacchetti dati senza una tag VLAN.
`vlan tagging 2 enable`	La porta `1/1` entra a far parte della VLAN `2` e trasmette i pacchetti dati con una tag VLAN.
`vlan participation include 3`	La porta `1/1` entra a far parte della VLAN `3` e trasmette i pacchetti dati senza una tag VLAN.
`vlan tagging 3 enable`	La porta `1/1` entra a far parte della VLAN `3` e trasmette i pacchetti dati con una tag VLAN.
`vlan pvid 1`	Assegnazione dell'ID VLAN `1` della porta alla porta `1/1`.
`vlan ingressfilter`	Attivare il filtraggio in ingresso sulla porta `1/1`.
`vlan acceptframe vlanonly`	La porta `1/1` inoltra solo pacchetti con una tag VLAN.
`exit`	Passare alla modalità di configurazione.
`interface 1/2`	Passare alla modalità di configurazione di interfaccia `1/2`.
`vlan participation include 2`	La porta `1/2` entra a far parte della VLAN `2` e trasmette i pacchetti dati senza una tag VLAN.
`vlan pvid 2`	Assegnazione dell'ID VLAN `2` della porta alla porta `1/2`.
`exit`	Passare alla modalità di configurazione.
`interface 1/3`	Passare alla modalità di configurazione di interfaccia `1/3`.
`vlan participation include 3`	La porta `1/3` entra a far parte della VLAN `3` e trasmette i pacchetti dati senza una tag VLAN.
`vlan pvid 3`	Assegnazione dell'ID VLAN `3` della porta alla porta `1/3`.
`exit`	Passare alla modalità di configurazione.
`interface 1/4`	Passare alla modalità di configurazione di interfaccia `1/4`.
`vlan participation include 2`	La porta `1/4` entra a far parte della VLAN `2` e trasmette i pacchetti dati senza una tag VLAN.
`vlan pvid 2`	Assegnazione dell'ID VLAN `2` della porta alla porta `1/4`.
`exit`	Passare alla modalità di configurazione.
`interface 1/5`	Passare alla modalità di configurazione di interfaccia `1/5`.

```
vlan participation include 3
```
La porta 1/5 entra a far parte della VLAN 3 e trasmette i pacchetti dati senza una tag VLAN.

```
vlan pvid 3
```
Assegnazione dell'ID VLAN 3 della porta alla porta 1/5.

```
exit
```
Passare alla modalità di configurazione.

```
exit
```
Passare alla modalità Privileged EXEC.

```
show vlan id 3
```
Mostra dettagli per la VLAN 3.

```
VLAN ID.....................3
VLAN Name...................VLAN3
VLAN Type...................Static
VLAN Creation Time...........0 days, 00:07:47 (System Uptime)
VLAN Routing.................disabled

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged
```

12.2 Guest VLAN / VLAN non autenticata

Una Guest VLAN consente a un dispositivo di fornire il controllo dell'accesso alla rete basato sulla porta (IEEE 802.1x) ai supplicanti incompatibili con 802.1x. Questa caratteristica fornisce un meccanismo per consentire agli ospiti di accedere solo alle reti esterne. Se si connettono supplicanti incompatibili con 802.1x a una porta 802.1x attiva non autorizzata, i supplicanti non inviano alcuna risposta alle richieste 802.1x. Dato che i supplicanti non inviano alcuna risposta, la porta rimane in stato non autorizzato. I supplicanti non hanno accesso alle reti esterne.

Il supplicante della Guest VLAN è una configurazione su base per porta. Quando si configura una porta come Guest VLAN e si connettono supplicanti incompatibili con 802.1x a questa porta, il dispositivo assegna i supplicanti alla Guest VLAN. L'aggiunta di supplicanti a una Guest VLAN causa il passaggio della porta allo stato autorizzato, consentendo ai supplicanti di accedere alle reti esterne.

Una VLAN non autenticata consente al dispositivo di fornire il servizio a supplicanti compatibili con 802.1x che si autenticano in maniera errata. Questa funzione consente ai supplicanti non autorizzati di accedere a servizi limitati. Se si configura una VLAN non autenticata su una porta con autenticazione della porta 802.1x e con funzione globale abilitata, il dispositivo posiziona la porta in una VLAN non autenticata. Quando un supplicante compatibile con 802.1x si autentica in maniera errata sulla porta, il dispositivo aggiunge il supplicante alla VLAN non autenticata. Se si configura anche una Guest VLAN sulla porta, i supplicanti incompatibili con 802.1x utilizzano la Guest VLAN.

Se la porta dispone di una Unauthenticated VLAN assegnata, il timer per la nuova autenticazione esegue il conto alla rovescia. Quando il tempo specificato nella colonna *Reauthentication period [s]* scade e i supplicanti sono presenti nella porta, la Unauthenticated VLAN si autentica nuovamente. In assenza di supplicanti, il dispositivo posiziona la porta nella Guest VLAN configurata.

L'esempio seguente spiega come creare una Guest VLAN. Creare una VLAN non autorizzata nello stesso modo.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Configuration*.
- ☐ Fare clic sul pulsante  .
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Specificare il valore `10` nel campo *VLAN ID*.
- ☐ Fare clic sul pulsante *Ok*.
- ☐ Per la VLAN, specificare il nome `Ospite`:
  Fare doppio clic nella colonna *Name* e specificare il nome.
- ☐ Fare clic sul pulsante  .
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Specificare il valore `20` nel campo *VLAN ID*.
- ☐ Fare clic sul pulsante *Ok*.
- ☐ Per la VLAN, specificare il nome `Non autorizzato`:
  Fare doppio clic nella colonna *Name* e specificare il nome.
- ☐ Aprire la finestra di dialogo *Network Security > 802.1X Port Authentication > Global*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

- ☐ Aprire la finestra di dialogo *Network Security > 802.1X Port Authentication > Port Configuration*.
- ☐ Specificare le seguenti impostazioni per la porta `1/4`:
  - Il valore `auto` nella colonna *Port control*
  - Il valore `10` nella colonna *Guest VLAN ID*
  - Il valore `20` nella colonna *Unauthenticated VLAN ID*
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`enable`	Passare alla modalità Privileged EXEC.
`vlan database`	Passare alla modalità di configurazione VLAN.
`vlan add 10`	Crea la VLAN `10`.
`vlan add 20`	Crea la VLAN `20`.
`name 10 Guest`	Rinomina la VLAN `10` con il nome `Guest`.
`name 20 Unauth`	Rinomina la VLAN `20` con il nome `Unauth`.
`exit`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`dot1x system-auth-control enable`	Abilitare la funzione *802.1X Port Authentication* globalmente.
`dot1x port-control auto`	Abilita il controllo della porta sulla porta `1/4`.
`interface 1/4`	Passare alla modalità di configurazione di interfaccia `1/4`.
`dot1x guest-vlan 10`	Assegnare la Guest VLAN alla porta `1/4`.
`dot1x unauthenticated-vlan 20`	Assegnare la vlan non autorizzata alla porta `1/4`.
`exit`	Passare alla modalità di configurazione.

12.3 Assegnazione RADIUS VLAN

La caratteristica di assegnazione RADIUS VLAN consente l'associazione di un attributo RADIUS VLAN-ID a un client autenticato. Quando un client si autentica con successo, e il server RADIUS invia un attributo VLAN, il dispositivo associa il client alla VLAN assegnata al RADIUS. Di conseguenza, il dispositivo aggiunge la porta fisica come membro alla VLAN appropriata e imposta l'ID VLAN (PVID) con il valore dato. La porta trasmette i pacchetti dati senza un tag VLAN.

12.4 Creazione di una Voice VLAN

Utilizzare la funzione Voice VLAN per separare traffico dati e vocale su una porta, in base a VLAN e/o priorità. Uno dei vantaggi principali di utilizzare la Voice VLAN è la salvaguardia della qualità del suono del telefono IP nei casi in cui vi sia un traffico dati elevato sulla porta.

Il dispositivo utilizza l'indirizzo MAC di origine per identificare e dare priorità al flusso di dati vocali. L'utilizzo di un indirizzo MAC per identificare i dispositivi contribuisce a evitare che un client rogue si colleghi alla stessa porta, causando il deterioramento del traffico vocale.

Un altro vantaggio della funzione Voice VLAN è che il telefono VoIP ottiene un ID VLAN o informazioni di priorità tramite l'LLDP-MED. Di conseguenza, il telefono VoIP invia dati vocali taggati, taggati come prioritari o non taggati. Ciò dipende dalla configurazione dell'interfaccia Voice VLAN.

Sono possibili le seguenti modalità di interfaccia Voice VLAN. I primi 3 metodi separano e danno priorità al traffico vocale e dati. Risultati di separazione del traffico in una qualità del traffico vocale aumentata durante periodi di traffico elevato.

- La configurazione della porta per l'utilizzo della modalità `vlan` consente al dispositivo di taggare i dati vocali provenienti da un telefono VoIP con l'ID VLAN vocale definito dall'utente. Il dispositivo assegna dati normali al VLAN-ID della porta di default.
- La configurazione della porta per l'utilizzo della modalità `dot1p-priority` consente al dispositivo di taggare i dati provenienti da un telefono VoIP con la VLAN 0 e la priorità definita dall'utente. Il dispositivo assegna la priorità di default della porta ai dati normali.
- Configurare l'ID VLAN vocale e la priorità utilizzando la modalità `vlan/dot1p-priority`. In questa modalità il telefono VoIP invia dati vocali con le informazioni di priorità e l'ID VLAN vocale definito dall'utente. Il dispositivo assegna la priorità e il PVID di default della porta ai dati normali.
- Quando è configurato come `untagged`, il telefono invia pacchetti non taggati.
- Quando è configurato come `none`, il telefono utilizza la propria configurazione per inviare traffico vocale.

13 Ridondanza

13.1 Topologia di rete vs. protocolli di ridondanza

Quando si utilizza l'Ethernet, un prerequisito fondamentale è che i pacchetti dati seguano un solo (unico) percorso dal mittente al destinatario. Le seguenti topologie di rete supportano tale prerequisito:

- Topologia lineare
- Topologia a stella
- Topologia ad albero

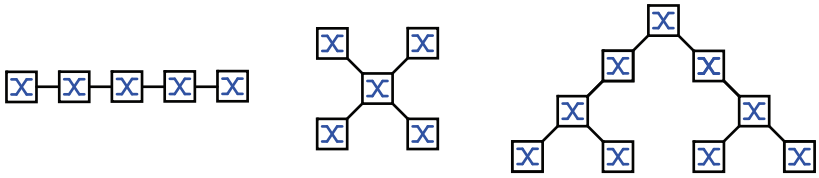


Figura 28: Rete con topologie lineari, a stella e ad albero

Per mantenere la comunicazione in caso venga rilevata un'interruzione del collegamento, installare ulteriori collegamenti fisici tra i nodi di rete. I protocolli di ridondanza contribuiscono a garantire che gli ulteriori collegamenti rimangano spenti mentre il collegamento originale è ancora attivo. Quando viene rilevata un'interruzione del collegamento, il protocollo di ridondanza genera un nuovo percorso dal mittente al destinatario attraverso la porta alternativa.

Per introdurre la ridondanza sul Layer 2 di una rete, si definisce prima la topologia di rete necessaria. In base alla topologia di rete selezionata, si sceglie poi tra i protocolli di ridondanza utilizzabili con questa topologia di rete.

13.1.1 Topologie di rete

Topologia a maglia

Per le reti dotate di topologie a stella o ad albero, le procedure di ridondanza sono possibili insieme alla creazione di loop fisici. Il risultato è una topologia a maglia.

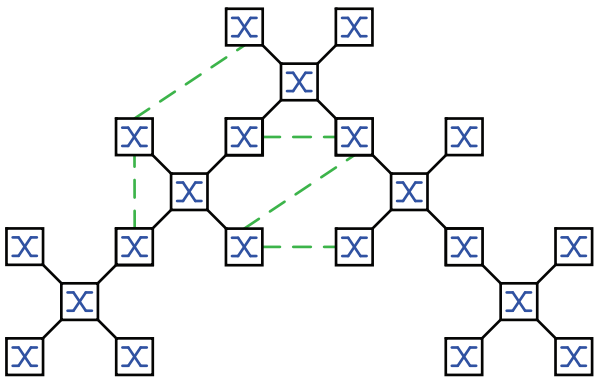


Figura 29: Topologia a maglia: topologia ad albero con loop fisici

Per funzionare in questa topologia di rete, il dispositivo fornisce i seguenti protocolli di ridondanza:
- Rapid Spanning Tree (RSTP)

Topologia ad anello

Nelle reti con una topologia lineare è possibile utilizzare procedure di ridondanza collegando le estremità della linea. Ciò crea una topologia ad anello.

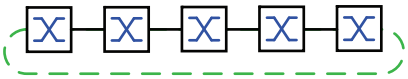


Figura 30: Topologia ad anello: topologia lineare con estremità collegate

Per funzionare in questa topologia di rete, il dispositivo fornisce i seguenti protocolli di ridondanza:
- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree (RSTP)

13.1.2 Protocolli di ridondanza

Per funzionare in topologie di rete diverse, il dispositivo fornisce i seguenti protocolli di ridondanza:

Tabella 31:Panoramica dei protocolli di ridondanza

Protocollo di ridondanza	Topologia di rete	Commenti
MRP	Anello	Il tempo di commutazione è selezionabile ed è praticamente indipendente dal numero di dispositivi. Un MRP Ring è costituito da un massimo di 50 dispositivi che supportano il protocollo MRP in conformità alla IEC 62439. Quando si utilizzano solo dispositivi Schneider Electric, nell'MRP Ring sono possibili fino a 100 dispositivi.
Subring	Anello	La funzione *Sub Ring* consente di collegare facilmente i segmenti di rete ad anelli di ridondanza esistenti.
Collegamento ad anello/rete	Anello	
RCP	Anello	
RSTP	Struttura casuale	Il tempo di commutazione dipende dalla topologia di rete e dal numero di dispositivi. - tipo < 1 s con RSTP - tipo < 30 s con STP
Aggregazione dei collega-menti	Struttura casuale	Un gruppo di Link Aggregation è la combinazione di 2 o più link punto-punto full duplex che funzionano alla stessa velocità su un solo switch per aumentare la larghezza di banda.
Backup dei link	Struttura casuale	Quando rileva un errore sul link primario, il dispositivo trasferisce il traffico al link di backup. In genere si utilizza il backup dei link nelle reti del fornitore di servizi o aziendali.
Client HIPER Ring	Anello	Estendere un HIPER ring esistente o sostituire un dispositivo che partecipa già in qualità di client in un HIPER ring.
HIPER Ring tramite LAG	Anello	Collegare i dispositivi attraverso un gruppo di Link Aggregation (LAG). I ring client e il Ring Manager si comportano allo stesso modo di un anello senza un'istanza di LAG.

Se la funzionalità di ridondanza e il controllo del flusso sono attivi contemporaneamente, è possibile che la funzionalità di ridondanza operi in modo diverso dal previsto.

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Se si sta utilizzando una funzionalità di ridondanza, si disattiva il controllo di flusso sulle porte interessate del dispositivo.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

13.1.3 Combinazioni di ridondanze

Tabella 32:Panoramica dei protocolli di ridondanza

	MRP	RSTP	Aggreg. dei collegamenti	Backup dei link	Subring	HIPER Ring
MRP	▲	– – –	– – –	– – –	– – –	– – –
RSTP	▲ 1)	▲	– – –	– – –	– – –	– – –
Aggreg. dei collegamenti	▲ 2)	▲ 2)	▲	– – –	– – –	– – –
Backup dei link	▲	▲	▲	▲	– – –	– – –
Subring	▲	▲	▲ 2)	▲	▲	– – –
HIPER Ring	▲	▲ 1)	▲ 2)	▲	▲	▲

▲ Combinazione applicabile

1) Il link ridondante tra queste topologie di rete potrebbe condurre a loop.
Per eseguire un link ridondante di queste topologie, vedere il capitolo “FuseNet” a pagina 222.

2) Combinazione applicabile sulla stessa porta.

13.2 Media Redundancy Protocol (MRP)

Dal maggio 2008, il Media Redundancy Protocol (MRP) è stato una soluzione standardizzata per la ridondanza ad anello nell'ambiente industriale.

L'MRP è compatibile con il collegamento ad anello ridondante, supporta le VLAN e si contraddistingue per i brevissimi tempi di riconfigurazione.

Un MRP Ring è costituito da un massimo di 50 dispositivi che supportano il protocollo MRP in conformità alla IEC 62439. Quando si utilizzano solo dispositivi Schneider Electric, nell'MRP Ring sono possibili fino a 100 dispositivi.

Quando si utilizza la porta ridondante MRP fissa (Backup fisso) e viene rilevata un'interruzione del collegamento dell'anello primario, il Ring Manager inoltra i dati al collegamento dell'anello secondario. Quando il collegamento primario è ripristinato, il collegamento secondario continua a essere utilizzato.

13.2.1 Struttura di rete

Il concetto di ridondanza ad anello consente di costruire strutture di rete ad anello ad alta disponibilità.

Con l'aiuto della funzione (**R**ing**M**anager) dell'RM, è possibile chiudere le due estremità di un backbone in una struttura lineare formando un anello ridondante. Il Ring Manager mantiene aperta la linea ridonante finché la struttura lineare è intatta. Quando un segmento diviene inutilizzabile, il Ring Manager chiude immediatamente la linea ridondante e la struttura lineare è nuovamente intatta.

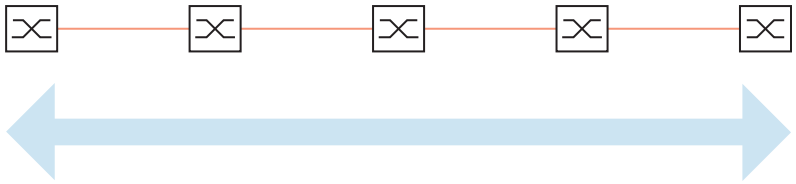


Figura 31: Struttura lineare

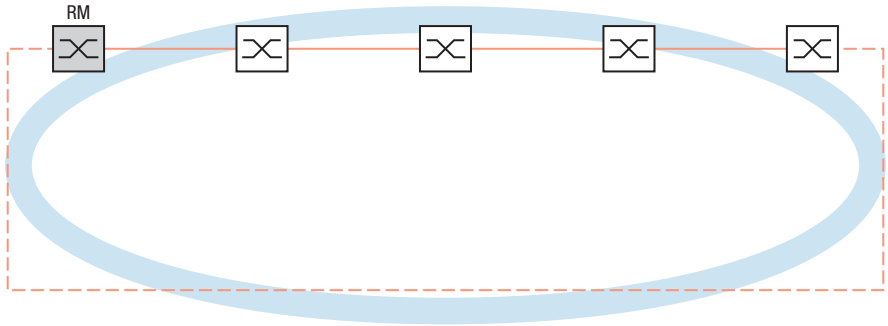


Figura 32: Struttura dell'anello ridondante
RM = Ring Manager
—— linea principale
- - - linea ridondante

13.2.2 Tempo di riconfigurazione

In caso venga rilevato il malfunzionamento di una sezione lineare, il Ring Manager modifica il protocollo MRP nella rete facendolotornare a una struttura lineare. Si definisce il tempo massimo per la riconfigurazione della linea nel Ring Manager.

I valori possibili per il tempo massimo di ritardo:
- *500ms*
- *30ms*

Nota: Se tutti i dispositivi nell'anello supportano il tempo di ritardo più breve, è possibile configurare il tempo di riconfigurazione con un valore inferiore a *500ms*.

Altrimenti i dispositivi che supportano solo tempi di ritardo più lunghi potrebbero essere irraggiungibili a causa del sovraccarico. I loop possono verificarsi di conseguenza.

13.2.3 Modalità avanzata

Per tempi ancora inferiori ai tempi di riconfigurazione specificati, il dispositivo fornisce la modalità avanzata. Quando i partecipanti all'anello comunicano al Ring Manager le interruzioni nell'anello attraverso notifiche link-down, la modalità avanzata accelera il riconoscimenti dei guasti del link.

Schneider Electric dispositivi supportano le notifiche link-down. Di conseguenza, generalmente si attiva la modalità avanzata nel Ring Manager.

Quando si utilizzano dispositivi che non supportano le notifiche link-down, il Ring Manager riconfigura la linea nel tempo massimo di riconfigurazione selezionato.

13.2.4 Prerequisiti per l'MRP

Prima di impostare un MRP Ring, verificare che le seguenti condizioni siano soddisfatte:
- ▶ Tutti i partecipanti all'anello supportano l'MRP.
- ▶ I partecipanti all'anello sono collegati tra loro tramite le Ring port. A parte quelli vicini al dispositivo, nessun altro partecipante all'anello è collegato al relativo dispositivo.
- ▶ Tutti i partecipanti all'anello supportano il tempo di configurazione specificato nel Ring Manager.
- ▶ Vi è solo un Ring Manager nell'anello.

Se si utilizzano VLAN, configurare ciascuna Ring port con le seguenti impostazioni:
- ☐ Disattivare il filtraggio in ingresso - vedere la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Definire l'ID VLAN della porta (PVID) - vedere la finestra di dialogo *Switching > VLAN > Port*.
  - – PVID = `1` nei casi in cui il dispositivo trasmette i pacchetti dati MRP non taggati (ID VLAN = `0` nella finestra di dialogo *Switching > L2-Redundancy > MRP*)
    Impostando il PVID = `1`, il dispositivo assegna automaticamente i pacchetti non taggati ricevuti alla VLAN 1.
  - – PVID = `any` nei casi in cui il dispositivo trasmette i pacchetti dati MRP in una VLAN (ID VLAN ≥ `1` nella finestra di dialogo *Switching > L2-Redundancy > MRP*)
- ☐ Definire le regole di uscita - vedere la finestra di dialogo *Switching > VLAN > Configuration*.
  - – `U` (non taggato) per le Ring port della VLAN 1 nei casi in cui il dispositivo trasmette i pacchetti dati MRP non taggati (ID VLAN = `0` nella finestra di dialogo *Switching > L2-Redundancy > MRP*, l'MRP ring non è assegnato a una VLAN).
  - – `T` (taggato) per le Ring port della VLAN che si assegna all'MRP ring. Selezionare `T` nei casi in cui il dispositivo trasmette i pacchetti dati MRP in una VLAN (ID VLAN ≥ `1` nella finestra di dialogo *Switching > L2-Redundancy > MRP*).

13.2.5 Configurazione esemplificativa

Un backbone di rete contiene 3 dispositivi in una struttura lineare. Per aumentare la disponibilità della rete, si converte la struttura lineare in una struttura ad anello ridondante. Si utilizzano i dispositivi di diversi produttori. Tutti i dispositivi supportano l'MRP Su ciascun dispositivo si definiscono le porte 1.1 e 1.2 come Ring port.

Quando viene rilevato un malfunzionamento del link di dati dell'anello primario, il Ring Manager invia dati sul link di dati dell'anello secondario. Quando il link primario è ripristinato, il link secondario torna alla modalità di backup.

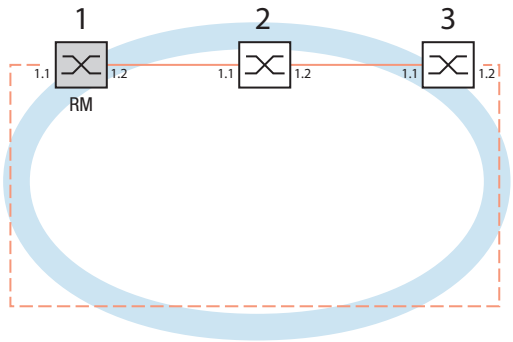


Figura 33: Esempio di MRP Ring
RM = Ring Manager
—— linea principale
- - - linea ridondante

La seguente configurazione esemplificativa descrive la configurazione del dispositivo Ring Manager (1). Si configurano gli altri 2 dispositivi (da 2 a 3) nello stesso modo, ma senza attivare la funzione *Ring manager*. Questo esempio non utilizza una VLAN. Si specifica il valore *30ms* come tempo di ripristino dell'anello. Ciascun dispositivo supporta la modalità avanzata del Ring Manager.

- ☐ Impostare la rete in base alle proprie esigenze.
- ☐ Configurare ciascuna porta di modo che la velocità di trasmissione e le impostazioni duplex delle linee corrispondano alla seguente tabella:

Tabella 33:Impostazioni della porta per Ring port

Tipo di porta	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
TX	1 Gbit/s	selezionato	selezionato	–
Ottico	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
Ottico	1 Gbit/s	selezionato	selezionato	–
Ottico	2.5 Gbit/s	selezionato	–	*2.5 Gbit/s FDX*

Nota: Si configurano le porte ottiche senza supporto per l'autonegoziazione (configurazione automatica) con 100 Mbit/s duplex pieno (FDX) o 1000 Mbit/s duplex pieno (FDX).

Nota: Si configurano le porte ottiche senza supporto per l'autonegoziazione (configurazione automatica) con 100 Mbit/s duplex pieno (FDX).

Nota: Configurare ciascun dispositivo dell'MRP Ring separatamente. Prima di collegare la linea ridondante, verificare di aver completato la configurazione di tutti i dispositivi dell'MRP Ring. In questo modo si contribuisce a evitare la formazione di loop durante la fase di configurazione.

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per aiutare a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della configurazione *MRP*. Prima di connettere le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione ad anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Si disattiva il controllo di flusso sulle porte interessate.

Se la funzionalità di ridondanza e il controllo del flusso sono attivi contemporaneamente, è possibile che la funzionalità di ridondanza operi in modo diverso dal previsto. (Impostazione di default: controllo di flusso disattivato globalmente e attivato su tutte le porte.)

Disabilitare la funzione *Spanning Tree* su tutti i dispositivi nella rete. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Disabilitare la funzione.
  Nello stato di fornitura, lo Spanning Tree è abilitato nel dispositivo.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`no spanning-tree operation`	Spegne lo Spanning Tree.
`show spanning-tree global`	Mostra i parametri per il controllo.

Abilitare l'MRP su tutti i dispositivi nella rete: A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > MRP*.
- ☐ Specificare le Ring port desiderate.

Nell'interfaccia a riga di comando si definisce prima un parametro aggiuntivo, l'ID del dominio MRP. Configurare ciascun partecipante all'anello con lo stesso ID del dominio MRP. L'ID del dominio MRP è una sequenza di 16 blocchi numerici (valori da 8 bit).

Quando esegue la configurazione con l'interfaccia grafica utente, il dispositivo utilizza il valore predefinito `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

`mrp domain add default-domain`	Crea un nuovo dominio MRP con l'ID `default-domain`.
`mrp domain modify port primary 1/1`	Specifica la porta *1/1* come Ring port `1`.
`mrp domain modify port secondary 1/2`	Specifica la porta *1/2* come Ring port `2`.

Abilitare la porta *Fixed backup*. A tale scopo, eseguire i seguenti passaggi:

- ☐ Abilitare il Ring Manager.
  Per gli altri dispositivi nell'anello, lasciare le impostazioni su *Off*.
- ☐ Per consentire al dispositivo di continuare a inviare dati sulla porta secondaria dopo il ripristino dell'anello, selezionare la casella di spunta *Fixed backup*.

Nota: Quando il dispositivo torna alla porta primaria, il tempo massimo di ripristino dell'anello può essere superato.

Quando si deseleziona la casella di spunta *Fixed backup* e l'anello è ripristinato, il Ring Manager blocca la porta secondaria e sblocca la porta primaria.

```
mrp domain modify port secondary 1/2
fixed-backup enable
```

Attiva la funzione *Fixed backup* sulla porta secondaria. La porta secondaria continua a inoltrare dati dopo il ripristino dell'anello.

- ☐ Abilitare il Ring Manager.
  Per gli altri dispositivi nell'anello, lasciare le impostazioni su *Off*.

```
mrp domain modify mode   manager
```

Specifica che il dispositivo funziona come *Ring manager*. Per gli altri dispositivi nell'anello, lasciare le impostazioni di default.

- ☐ Selezionare la casella di spunta nel campo *Advanced mode*.

```
mrp domain modify   advanced-mode
enabled
```

Attiva la modalità avanzata.

- ☐ Selezionare il valore *30ms* nel campo *Ring recovery*.

```
mrp domain modify   recovery-delay
200ms
```

Specifica il valore *30ms* come tempo massimo di ritardo per la riconfigurazione dell'anello.

Nota: Se la selezione del valore *30ms* per il ripristino dell'anello non fornisce all'anello la stabilità necessaria per soddisfare i requisiti di rete, selezionare il valore *500ms*.

- ☐ Attivare la funzione dell'MPR Ring.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

```
mrp domain modify operation   enable
```

Attiva l'MRP Ring.

Quando tutti i partecipanti all'anello sono configurati, chiudere la linea per l'anello. A tale scopo, si collegano i dispositivi alle estremità della linea tramite le loro Ring port.

Controllare i messaggi dal dispositivo. A tale scopo, eseguire i seguenti passaggi:

`show mrp` Mostra i parametri per il controllo.

Il campo *Operation* mostra il modo operativo della Ring port.

Possibili valori:
- `forwarding`
  La porta è abilitata, il collegamento è presente.
- `blocked`
  La porta è bloccata, il collegamento è presente.
- `disabled`
  La porta è disabilitata.
- `not-connected`
  Nessun collegamento presente.

Il campo *Information* mostra messaggi per la configurazione della ridondanza e le possibili cause degli errori rilevati.

Quando il dispositivo funziona come un ring client o un Ring Manager, sono possibili i seguenti messaggi:
- *Redundancy available*
  La ridondanza è configurata. Quando un componente dell'anello non funziona, la linea ridondante assume la sua funzione.
- *Configuration error: Error on ringport link.*
  È stato rilevato un errore nel cablaggio delle porte ring.

Quando il dispositivo funziona come un Ring Manager, sono possibili i seguenti messaggi:
- *Configuration error: Packets from another ring manager received.*
  Nell'anello vi è un altro dispositivo che funziona come Ring Manager.
  Attivare la funzione *Ring manager* su un solo dispositivo nell'anello.
- *Configuration error: Ring link is connected to wrong port.*
  Una linea nell'anello è collegata con una porta diversa invece che con una Ring port. Il dispositivo riceve solo pacchetti dati di test su una Ring port.

Ove applicabile, integrare un MRP ring in una VLAN. A tale scopo, eseguire i seguenti passaggi:

- ☐ Nel campo *VLAN ID*, definire l'ID VLAN MRP. L'ID VLAN MRP determina in quale delle VLAN configurate il dispositivo trasmette i pacchetti MRP.
  Per impostare l'ID VLAN MRP, configurare prima le VLAN e le regole di uscita corrispondenti nella finestra di dialogo *Switching > VLAN > Configuration*.
  - Se l'MRP Ring non è assegnato a una VLAN (come in questo esempio), lasciare come ID VLAN `0`.
    Nella finestra di dialogo *Switching > VLAN > Configuration*, specificare l'appartenenza alla VLAN come `U` (non taggata) per le Ring port nella VLAN `1`.
  - Se l'MRP Ring è assegnato a una VLAN, immettere un ID VLAN > `0`.
    Nella finestra di dialogo *Switching > VLAN > Configuration*, specificare l'appartenenza alla VLAN come `T` (taggata) per le Ring port nella VLAN selezionata.

`mrp domain modify vlan <0..4042>` Assegna l'ID VLAN.

13.2.6 MRP tramite LAG

I dispositivi Schneider Electric consentono di combinare i gruppi di Link Aggregation (LAG) a una maggiore larghezza di banda con la ridondanza fornita dal protocollo Media Redundancy Protocol (MRP). La funzione consente di aumentare la larghezza di banda sui singoli segmenti o su tutta la rete.

La funzione *Link Aggregation* contribuisce a superare i limiti di larghezza di banda delle singole porte. La LAG consente di combinare 2 o più link in parallelo, creando un link logico tra 2 dispositivi. I link paralleli aumentano la larghezza di banda per il flusso di dati tra i 2 dispositivi.

Un MRP ring è costituito da un massimo di 50 dispositivi che supportano il protocollo MRP in conformità alla IEC 62439. Quando si utilizzano solo dispositivi Schneider Electric, il protocollo consente di configurare MRP ring con fino a 100 dispositivi.

Si utilizza l'MRP tramite LAG nei seguenti casi:
- per aumentare la larghezza di banda solo su segmenti specifici di un MRP ring
- per aumentare la larghezza di banda sull'intero MRP ring

Struttura di rete

Quando si configura un MRP ring con LAG, il Ring Manager (RM) monitora la continuità di entrambe le estremità del backbone. Il RM blocca i dati sulla porta secondaria (ridondante) finché il backbone è intatto. Se il RM rileva un'interruzione del flusso di dati sul ring, inizia a inoltrare i dati sulla porta secondaria, ripristinando la continuità del backbone.

Si utilizzano le istanze LAG negli MRP ring solo per aumentare la larghezza di banda, in questo caso la ridondanza è fornita dall'MRP.

Affinché il RM rilevi un'interruzione sul ring, l'MRP necessita che un dispositivo blocchi tutte le porte nell'istanza di LAG nei casi in cui una porta dell'istanza sia disattivata.

LAG su un singolo segmento di un MRP ring

Il dispositivo consente di configurare un'istanza di LAG su segmenti specifici di un MRP ring.

Si utilizza il metodo LAG a switch unico per i dispositivi nell'MRP ring. Il metodo a switch unico offre una soluzione economica per ampliare la rete utilizzando solo un dispositivo su ciascuna parte di un segmento per le porte fisiche. Si raggruppano le porte del dispositivo in un'istanza di LAG per ottenere una maggiore larghezza di banda su segmenti specifici, se necessario.

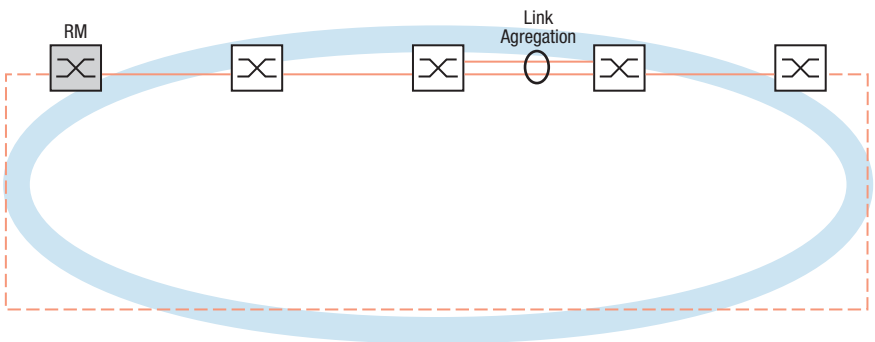


Figura 34: Link Aggregation tramite un link unico di un MRP ring.

LAG su un intero MRP ring

Oltre a consentire la configurazione di un'istanza di LAG su segmenti specifici di un MRP ring, i dispositivi Schneider Electric permettono anche di configurare le istanze di LAG su ogni segmento, ampliando la larghezza di banda dell'intero MRP ring.

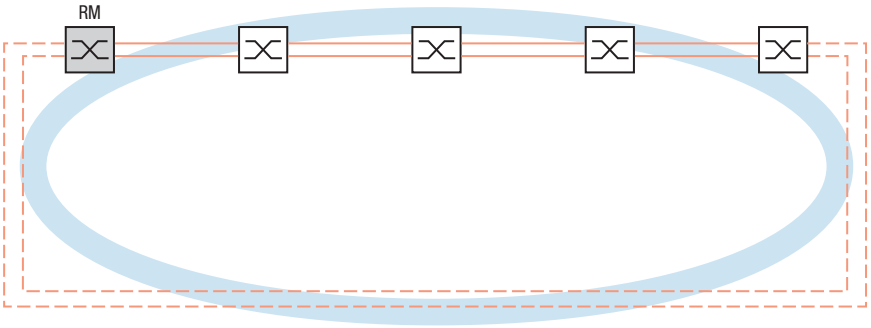


Figura 35: Link Aggregation sull'intero MRP ring.

Rilevare le interruzioni sul ring

Quando si configura l'istanza di LAG, specificare il valore *Active ports (min.)* in modo che corrisponda al numero totale di porte utilizzate nell'istanza di LAG. Quando un dispositivo rileva un'interruzione su una porta nell'istanza di LAG, blocca i dati sulle altre porte dell'istanza. Se tutte le porte di un'istanza sono bloccate, il RM rileva che l'anello è aperto e inizia a inoltrare i dati sulla porta secondaria. In questo modo il RM è in grado di ripristinare la continuità ai dispositivi dall'altra parte del segmento interrotto.

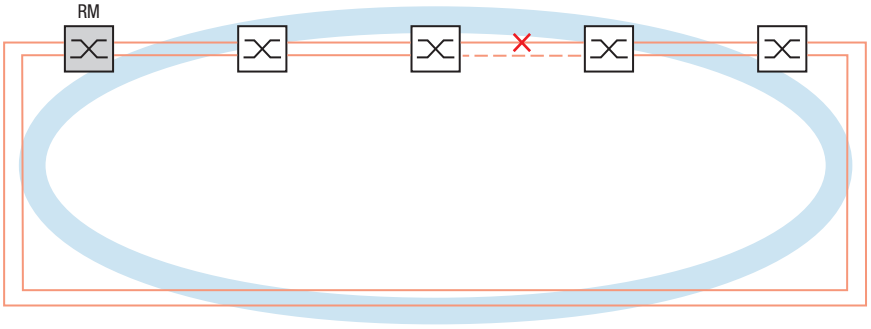


Figura 36: Interruzione di un link in un MRP ring.

Configurazione esemplificativa

Nel seguente esempio, lo switch A e lo switch B collegano due dipartimenti. I dipartimenti producono un traffico troppo intenso per essere gestito dalla larghezza di banda della porta singola. Si configura un'istanza di LAG per il segmento singolo dell'MRP ring, aumentando la larghezza di banda del segmento.

Il prerequisito per la configurazione dell'esempio è che si inizi con un MRP ring operativo.

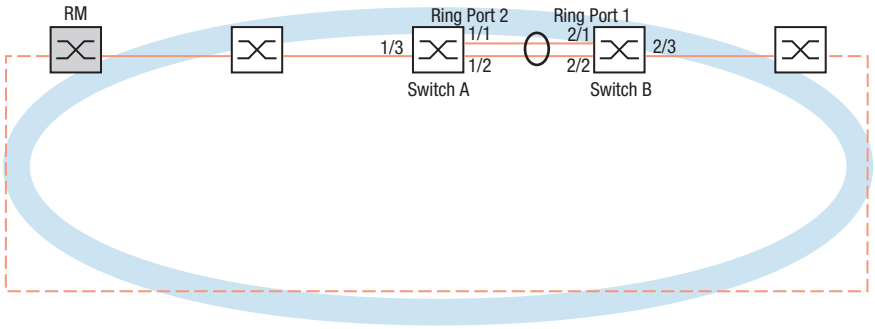


Figura 37: MRP tramite LAG Esempio di configurazione

Configurare prima lo switch A. A tale scopo, eseguire i seguenti passaggi. In seguito, configurare lo switch B seguendo gli stessi passaggi e sostituendo in modo appropriato i numeri della porta e della Ring port.

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Link Aggregation*.
- ☐ Fare clic sul pulsante .
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Nell'elenco a discesa *Trunk port*, selezionare il numero dell'istanza del gruppo di Link Aggregation.
- ☐ Nell'elenco a discesa *Port*, selezionare la porta *1/1*.
- ☐ Fare clic sul pulsante *Ok*.
- ☐ Ripetere i passaggi precedenti e selezionare la porta *1/2*.
- ☐ Fare clic sul pulsante *Ok*.
- ☐ Nella colonna *Active ports (min.)* immettere `2`, che in questo caso è il numero totale di porte nell'istanza. Quando si combinano MRP e LAG, specificare il numero totale di porte come *Active ports (min.)*. Quando il dispositivo rileva un'interruzione su una porta, blocca le altre porte nell'istanza facendo aprire il ring. Il Ring Manager rileva che l'anello è aperto e inizia a inoltrare i dati sulla Ring port secondaria, ripristinando la connessione agli altri dispositivi nella rete.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .
- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > MRP*.
- ☐ Nel riquadro *Ring port 2* selezionare la porta `lag/1` nell'elenco a discesa *Port*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`link-aggregation add lag/1`	Crea un gruppo di Link Aggregation `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Aggiunge la porta *1/1* al gruppo di Link Aggregation.

`link-aggregation modify lag/1 addport 1/2`	Aggiunge la porta *1/2* al gruppo di Link Aggregation.
`mrp domain modify port secondary lag/1`	Specifica la porta `lag/1` come Ring port `2`.
`copy config running-config nvm`	Salvare le impostazioni correnti nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

13.3 Client HIPER Ring

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per aiutare a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della configurazione *HIPER Ring*. Prima di connettere le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione ad anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Il concetto di ridondanza ad anello HIPER consente di realizzare strutture di rete ad anello ad alta disponibilità. La funzione client *HIPER Ring* consente all'amministratore di rete di estendere un HIPER Ring esistente o di sostituire un dispositivo client che partecipa già all'HIPER Ring.

Quando il dispositivo rileva l'interruzione del collegamento su una Ring port, il dispositivo invia un pacchetto LinkDown al Ring Manager (RM) e risciacqua la tabella FDB. Quando l'RM riceve il pacchetto LinkDown, inoltra immediatamente il flusso di dati attraverso le Ring port primarie e secondarie. In questo modo, l'RM è in grado di mantenere l'integrità dell'HIPER Ring.

Il dispositivo supporta solo porte Fast Ethernet e Gigabit Ethernet come Ring port. Inoltre, è possibile includere le Ring port in un'istanza LAG.

Allo stato di default, il client HIPER Ring non è attivo, e le porte primarie e secondarie sono impostate su `no Port`.

Nota: Disattivare lo Spanning Tree Protocol (STP) per le Ring port nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, in quanto l'STP e l'HIPER Ring presentano diversi tempi di reazione.

Tabella 34:Impostazioni della porta per Ring port

Tipo di porta	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`selezionato`	`non selezionato`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`selezionato`	`selezionato`	–
Ottico	100 Mbit/s	`selezionato`	`non selezionato`	*`100 Mbit/s FDX`*
Ottico	1 Gbit/s	`selezionato`	`selezionato`	–
Ottico	2.5 Gbit/s	`selezionato`	–	*`2.5 Gbit/s FDX`*

13.3.1 VLAN sull'HIPER Ring

Il dispositivo consente di inoltrare i dati VLAN attraverso l'HIPER Ring. In questo modo, il dispositivo fornisce ridondanza per i dati VLAN. Il dispositivo ring inoltra i dati di gestione intorno all'anello, ad esempio sulla VLAN 1. Per far sì che i dati raggiungano la network management station, i dispositivi ring inoltrano i dati di gestione non taggati sulle Ring port. Inoltre, specificare le Ring port come membri nella VLAN 1.

Quando si hanno altre VLAN che attraversano i dispositivi ring, questi inoltrano i dati dell'altra VLAN come taggati.

Specificare le impostazioni della VLAN. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Configuration*.
- ☐ Inoltrare dati di gestione VLAN non taggati sulle Ring port.
  Nella riga VLAN 1, selezionare la voce `U` nell'elenco a discesa nelle colonne relative alla Ring port.
- ☐ Bloccare l'inoltro dei pacchetti di gestione alle porte non-ring.
  Nella riga VLAN 1, selezionare la voce `-` nell'elenco a discesa nelle colonne **non** relative alla Ring port.
- ☐ Consentire a un dispositivo ring di inoltrare dati VLAN alle e dalle porte con appartenenza VLAN.
  Nella riga VLAN, selezionare la voce `T` nell'elenco a discesa nelle colonne relative alla Ring port.
- ☐ Aprire la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Assegnare l'appartenenza VLAN 1 alle Ring port.
  Immettere il valore `1` nella colonna *Port-VLAN ID* delle righe della Ring port.
- ☐ Assegnare l'appartenenza VLAN alle porte non-ring.
  Immettere l'ID VLAN appropriato nella colonna *Port-VLAN ID* delle righe della porta non ring.

13.3.2 HIPER Ring tramite LAG

La funzione *HIPER Ring* consente di collegare i dispositivi tra loro attraverso un gruppo di Link Aggregation (LAG). I ring client e il Ring Manager si comportano allo stesso modo di un anello senza un'istanza di LAG.

Se un link LAG si interrompe, si interrompe anche l'altro link nell'istanza creando un'interruzione nel ring. Dopo aver rilevato un'interruzione nel ring, le porte interessate inviano un pacchetto di Link Down al Ring Manager. Il Ring Manager sblocca la porta secondaria, inviando i dati in entrambe le direzioni sul ring, e risponde con un pacchetto Delete. Alla ricezione di un pacchetto Delete, i partecipanti all'anello cancellano la propria FDB.

13.4 Spanning Tree

Nota: Lo Spanning Tree Protocol è un protocollo per switch MAC. Per questo motivo, la seguente descrizione utilizza il termine switch per il dispositivo.

Le reti locali crescono costantemente. Sia in termini di estensione geografica sia in termini di numero di utenti della rete stessa. Di conseguenza, è vantaggioso utilizzare più switch, ad esempio:
- per ridurre il carico di rete nelle sottoaree,
- per impostare collegamenti ridondanti e
- per risolvere problemi legati alle distanze.

Tuttavia, l'utilizzo di più switch con più collegamenti ridondanti tra le sottoreti può condurre alla formazione di loop e, di conseguenza all'interruzione della comunicazione attraverso la rete. Per contribuire a impedire ciò è possibile utilizzare lo Spanning Tree. Lo Spanning Tree consente di evitare la formazione di loop tramite la disattivazione sistematica di connessioni ridondanti. La ridondanza consente la riattivazione sistematica dei singoli collegamenti in base alle necessità.

L'RSTP è un'evoluzione ulteriore dello Spanning Tree Protocol (STP) ed è compatibile con esso. Quando un collegamento o uno switch diventano inutilizzabili, l'STP necessita di un massimo di 30 secondi per riconfigurarsi. Questo non è più accettabile nelle applicazioni sensibili al fattore tempo. L'RSTP ottiene tempi medi di riconfigurazione inferiori a un secondo. Quando si utilizza l'RSTP in una topologia ad anello contenente tra i 10 e i 20 dispositivi, è possibile ottenere tempi di riconfigurazione nell'ordine dei millisecondi.

Nota: L'RSTP trasforma una topologia di rete layer 2 con percorsi ridondanti in una struttura ad albero (Spanning Tree) che non contiene più alcun percorso ridondante. Uno dei dispositivi assume qui il ruolo di root switch. Il numero massimo di dispositivi consentito in un ramo attivo, (dal root switch alla punta del ramo) è specificato dalla variabile *Max age* per il root switch corrente. Il valore presente per la *Max age* è `20`, aumentabile fino a `40`.

Se il dispositivo, che funziona da root, risulta inutilizzabile e al suo posto subentra un altro dispositivo, l'impostazione *Max age* del nuovo root switch determina il numero massimo di dispositivi consentiti in un ramo.

Nota: Lo standard RSTP richiede che tutti i dispositivi all'interno di una rete operino secondo lo Spanning Tree Algorithm (Rapid). Quando l'STP e l'RSTP sono utilizzati contemporaneamente, i vantaggi di una più rapida riconfigurazione tramite l'RSTP si perdono nei segmenti di rete gestiti in combinazione.

Un dispositivo che supporta solo l'RSTP, opera insieme a dispositivi MSTP non assegnando a se stesso non una regione MST, bensì il CST (Common Spanning Tree).

13.4.1 Fondamenti

Poiché l'RSTP è un'ulteriore evoluzione dell'STP, tutte le seguenti descrizioni dell'STP si applicano anche per l'RSTP.

Le funzioni dell'STP

Lo Spanning Tree Algorithm riduce le topologie di rete costruite con switch e contenenti strutture ad anello a causa di collegamenti ridondanti a una struttura ad albero. Così facendo, l'STP apre le strutture ad anello secondo le regole predefinite disattivando percorsi ridondanti. Quando un percorso è interrotto a causa del guasto di un componente di rete, l'STP riattiva nuovamente il percorso precedentemente disattivato. Questo consente ai link ridondanti di aumentare la disponibilità della comunicazione.

L'STP determina uno switch che rappresenta la base della struttura ad albero STP. Questo switch è chiamato root switch.

Caratteristiche dell'algoritmo STP:
- riconfigurazione automatica della struttura ad albero qualora uno switch diventi inutilizzabile o in caso di interruzione di un percorso di dati
- la struttura ad albero è stabilizzata fino alle dimensioni massime di rete,
- stabilizzazione della topologia entro un breve periodo di tempo
- la topologia può essere specificata e riprodotta dall'amministratore,
- trasparenza per i dispositivi finali
- basso carico di rete rispetto alla capacità di trasmissione disponibile dovuto alla struttura ad albero creata

Parametri switch

Nell'ambito dello Spanning Tree, ciascuno switch e i suoi collegamenti sono descritti in modo univoco dai seguenti parametri:
- Identificativo dello switch
- Costi di percorso root per le porte switch,
- Identificativo della porta

Identificativo dello switch

L'identificativo dello switch è costituito da 8 byte. I 2 byte di valore più alto sono la priorità. Quando si configura la rete, l'agente di gestione può modificare l'impostazione di default per il numero di priorità, che è `32768` (8000H). I 6 byte di valore più basso dell'identificativo dello switch costituiscono l'indirizzo MAC dello switch. L'indirizzo MAC consente a ciascuno switch di avere un identificativo dello switch univoco.

Lo switch con il numero più basso per l'identificativo dello switch ha la massima priorità.

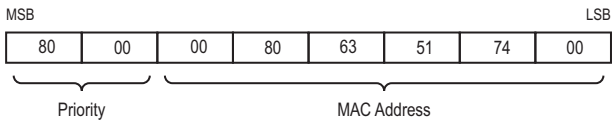


Figura 38: Identificativo dello switch, esempio, (valori espressi in esadecimali)

Costi di percorso root

A ciascun percorso che collega 2 switch è assegnato un costo di trasmissione (costo di percorso). Il dispositivo determina questo valore in base alla velocità di trasmissione (vedi tabella 35). Il dispositivo assegna un costo di percorso superiore ai percorsi con velocità di trasmissione inferiori.

In alternativa, l'amministratore può impostare il costo di percorso. Come il dispositivo, l'amministratore assegna un costo di percorso superiore ai percorsi con velocità di trasmissione inferiori. Però poiché l'amministratore può scegliere questo valore liberamente, ha a disposizione uno strumento con cui può dare la precedenza a un determinato percorso, in caso di percorsi ridondanti.

Il costo di percorso è la somma dei costi individuali di quei percorsi che un pacchetto dati deve attraversare da una porta di uno switch collegata al root switch.

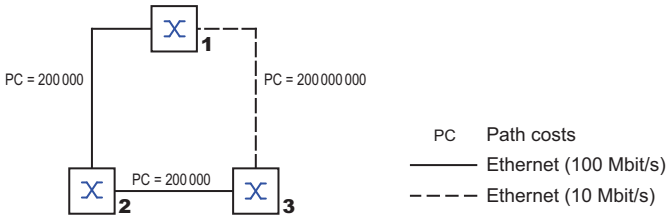


Figura 39: Costi di percorso

Tabella 35:Costi di percorso consigliati per l'RSTP in base alla velocità di trasmissione dei dati.

Velocità di trasmissione dati	Valore consigliato	Campo consigliato	Campo possibile
≤100 kbit/s	200 000000[1]	20000000-200000000	1-200000000
1 Mbit/s	20000000[a]	2000000-200000000	1-200000000
10 Mbit/s	2000000[a]	200000-20000000	1-200000000
100 Mbit/s	200000[a]	20000-2000000	1-200000000
1 Gbit/s	20000	2000-200000	1-200000000
10 Gbit/s	2000	200-20000	1-200 000000
100 Gbit/s	200	20-2000	1-200000000
1 TBit/s	20	2-200	1-200000000
10 TBit/s	2	1-20	1-200000000

1. Gli switch conformi alla IEEE 802.1D-1998, che supportano solamente valori a 16 bit per i costi di percorso, utilizzano il valore 65535 (FFFFH) per i costi di percorso nei casi in cui siano utilizzati assieme agli switch che supportano valori a 32 bit per i costi di percorso.

Identificativo della porta

L'identificatore della porta è costituito da 2 byte. Una parte, il byte di minor valore, contiene il numero fisico della porta. Ciò fornisce un identificativo univoco per la porta di questo switch. La seconda parte, di valore superiore, è la priorità della porta, specificata dall'amministratore (impostazione di default: 128). Vale anche in questo caso che la porta con il numero minore per l'identificativo della porta abbia la massima priorità.

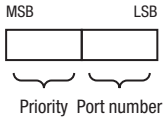


Figura 40: Identificativo della porta

Diametro ed età massima

I valori “Età massima” e “Diametro” determinano ampiamente la massima espansione di una rete Spanning Tree.

Diametro

Il numero di collegamenti tra i dispositivi più distanti tra loro nella rete è noto come diametro di rete.

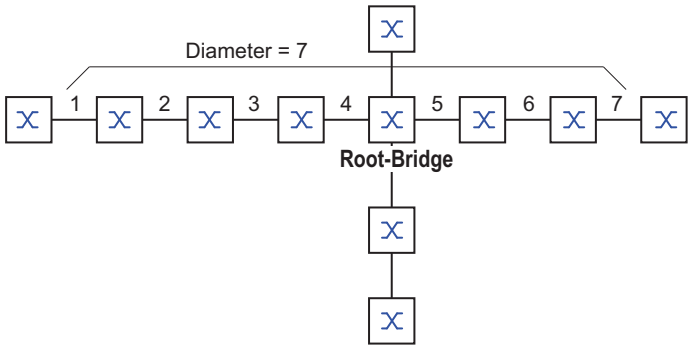


Figura 41: Definizione di diametro

Il diametro di rete ottenibile nella rete è EtàMassima-1.

In stato di fornitura, l'EtàMassima = 20 e il massimo diametro ottenibile = 19. Quando si imposta il valore massimo per l'EtàMassima pari a 40, il diametro massimo ottenibile è = 39.

EtàMassima

Ciascuna STP-BPDU contiene un contatore di “EtàMessaggio”. Quando uno switch è attraversato, il contatore aumenta di 1.

Prima di inoltrare una STP-BPDU, lo switch confronta il contatore di “EtàMessaggio” con il valore di “EtàMassima” specificato nel dispositivo:

- Quando l'EtàMessaggio è inferiore all'EtàMassima, lo switch inoltra l'STP-BPDU allo switch successivo.
- Quando l'EtàMessaggio è uguale all'EtàMassima, lo switch rifiuta l'STP-BPDU.

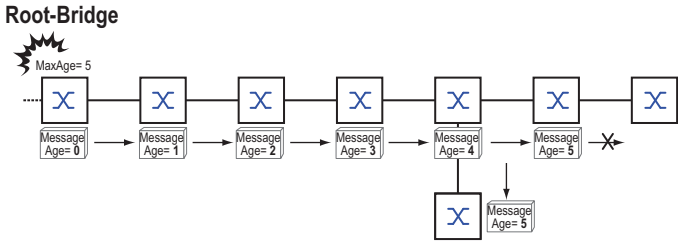


Figura 42: La trasmissione di una STP-BPDU dipende dall'EtàMassima.

13.4.2 Regole per la creazione della struttura ad albero

Informazioni sullo switch

Per determinare la struttura ad albero, gli switch necessitano di informazioni più dettagliate sugli altri switch situati nella rete.

Per ottenere tali informazioni, ciascuno switch invia una BPDU (Switch Protocol Data Unit) agli altri switch.

Il contenuto di una BPDU include:

- Identificativo dello switch
- Costi di percorso root
- Identificativo della porta

(vedere IEEE 802.1D)

Configurazione di una struttura ad albero

Lo switch con il numero più piccolo per l'identificativo dello switch è chiamato root switch. È (o diventerà) il root della struttura ad albero.

La struttura dell'albero dipende dai costi di percorso root. Lo Spanning Tree seleziona la struttura di modo che i costi di percorso tra ciascun singolo switch e il root switch si riducano il più possibile.

- Quando vi sono più percorsi con gli stessi costi di percorso root, lo switch lontano dal root decide quale porta bloccare. A tale scopo, utilizza gli identificativi dello switch più vicino al root. Lo switch blocca la porta che conduce allo switch con l'ID numericamente superiore (un ID numericamente superiore è quello logicamente peggiore). Quando 2 switch hanno la stessa priorità, quello con l'indirizzo MAC numericamente più ampio ha l'ID numericamente superiore, che è quello logicamente peggiore.
- Quando più percorsi con gli stessi costi di percorso root conducono da uno switch allo stesso switch, lo switch lontano dal root utilizza l'identificativo della porta dell'altro switch come ultimo criterio (vedi figura 40). Nel frattempo, lo switch blocca la porta che conduce alla porta con l'ID numericamente superiore (un ID numericamente superiore è quello logicamente peggiore). Quando 2 porte hanno la stessa priorità, la porta con il numero di porta superiore ha l'ID numericamente superiore, che è quello logicamente peggiore.

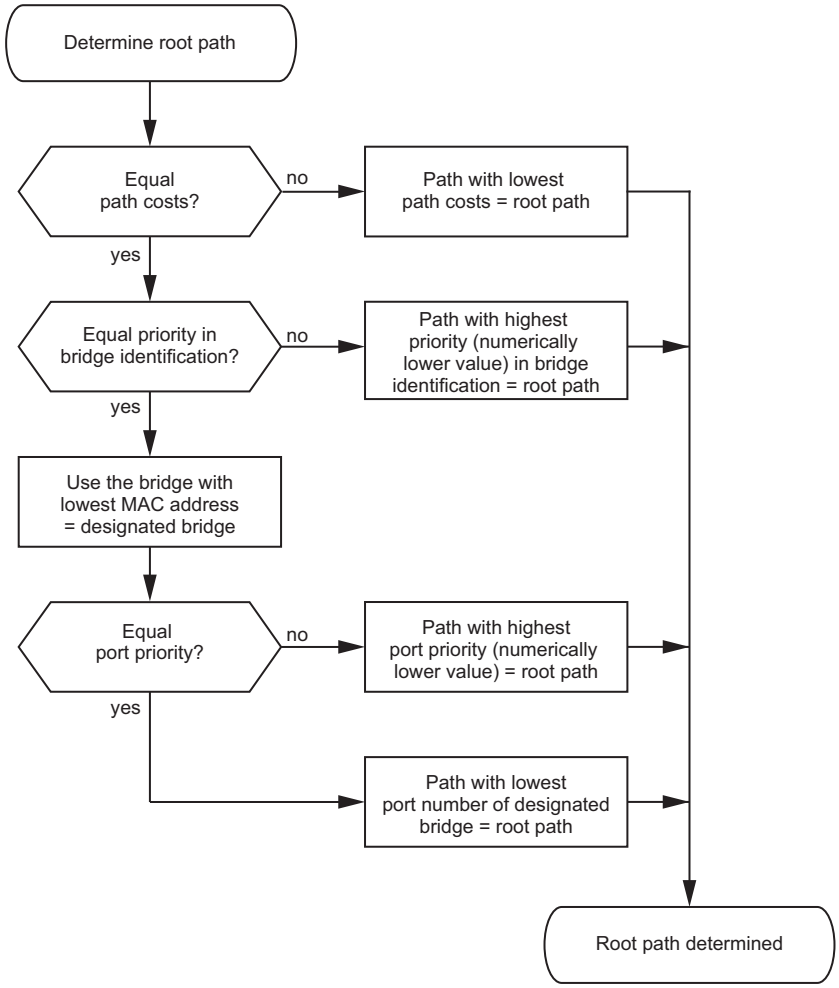


Figura 43: Diagramma di flusso per la specifica del percorso root

13.4.3 Esempi

Esempio di determinazione del percorso root

Si può utilizzare il piano di rete (vedi figura 44) per seguire l'organigramma (vedi figura 43) al fine di determinare il percorso root. L'amministratore ha specificato una priorità nell'identificativo dello switch per ciascuno switch. Lo switch con il valore numerico più piccolo per l'identificativo dello switch assume il ruolo di root switch, in questo caso switch 1. Nell'esempio, tutti i sub-path hanno gli stessi costi di percorso. Il protocollo blocca il percorso tra lo switch 2 e lo switch 3, poiché un collegamento dallo switch 3 verso il root switch tramite lo switch 2 comporterebbe costi di percorso superiori.

Il percorso dallo switch 6 al root switch è interessante:

- Il percorso tramite lo switch 5 e lo switch 3 crea gli stessi costi di percorso root del percorso tramite lo switch 4 e lo switch 2.
- L'STP seleziona il percorso tramite lo switch dotato dell'indirizzo MAC più basso nell'identificativo switch (switch 4 nell'illustrazione).
- Vi sono anche 2 percorsi tra lo switch 6 e lo switch 4.
  L'identificativo della porta è decisivo qui (Porta 1 inferiore alla Porta 3).

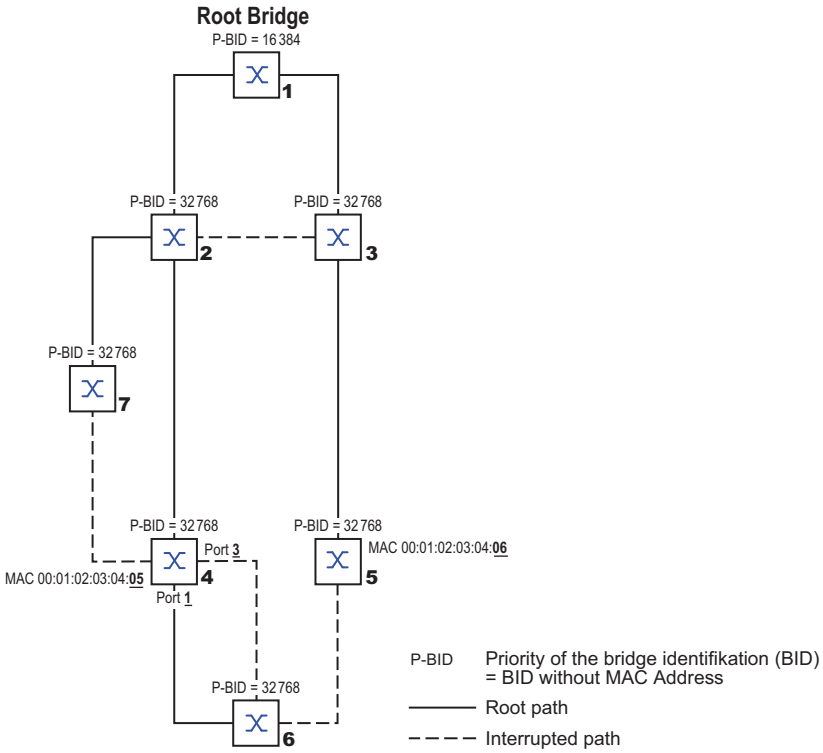


Figura 44: Esempio di determinazione del percorso root

Nota: Quando il root switch corrente si interrompe, l'indirizzo MAC nell'identificativo switch determina da solo quale switch diventa il nuovo root switch, in quanto l'amministratore non modifica i valori di default per le priorità degli switch nell'identificativo switch, a parte il valore per il root switch.

Esempio di manipolazione del percorso root

Si può utilizzare il piano di rete (vedi figura 45) per seguire l'organigramma (vedi figura 43) al fine di determinare il percorso root. L'amministratore ha eseguito quanto segue:

- Ha lasciato il valore di default di 32768 (8000H) per ciascuno switch a parte gli switch 1 e 5, e
- ha assegnato allo switch 1 il valore 16384 (4000H), creando così il root switch.
- Allo switch 5 ha assegnato il valore 28672 (7000H).

Il protocollo blocca il percorso tra lo switch 2 e lo switch 3, poiché un collegamento dallo switch 3 verso il root switch tramite lo switch 2 comporterebbe costi di percorso superiori.

Il percorso dallo switch 6 al root switch è interessante:

▶ Gli switch selezionano il percorso tramite lo switch 5 poiché il valore 28672 per la priorità nell'identificatore dello switch è inferiore al valore 32768.

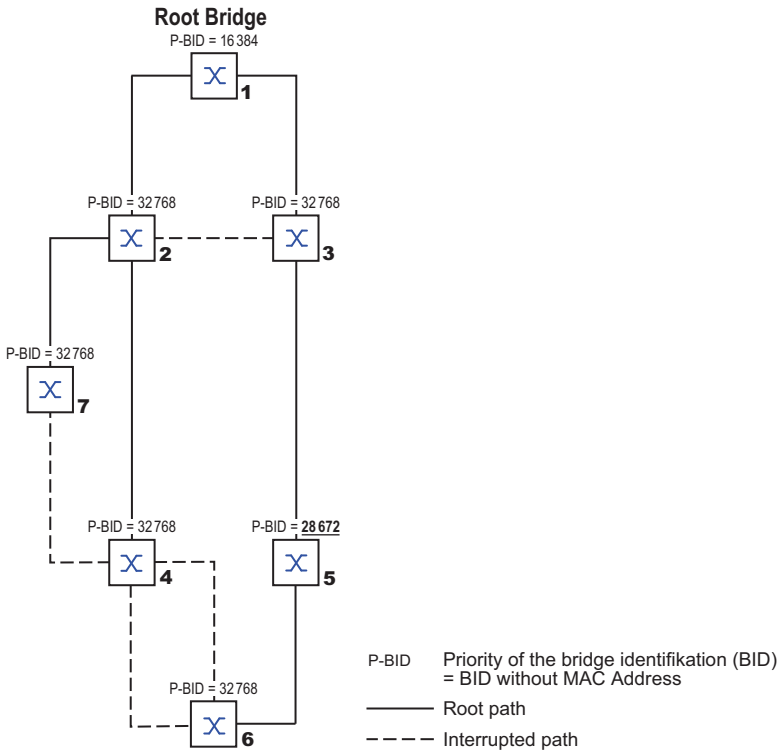


Figura 45: Esempio di manipolazione del percorso root

Esempio di manipolazione di struttura ad albero

L'agente di gestione scopre presto che questa configurazione con lo switch 1 come root switch non è valida. Sui percorsi dallo switch 1 allo switch 2 e dallo switch 1 allo switch 3, i pacchetti di controllo inviati dal root switch a tutti gli altri switch si sommano.

Quando l'agente di gestione configura lo switch 2 come root switch, il carico dei pacchetti di controllo sulle sottoreti è distribuito in modo molto più equo. Il risultato è la configurazione mostrata qui (vedi figura 46). I costi di percorso per la maggior parte degli switch verso il root switch sono diminuiti.

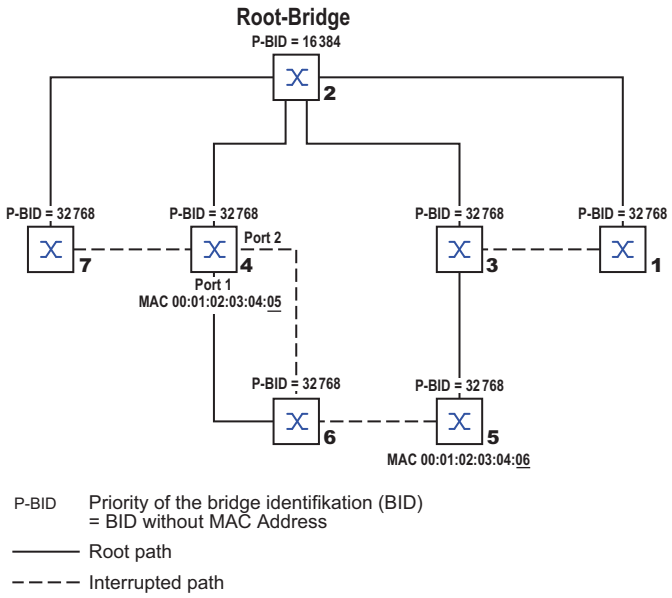


Figura 46: Esempio di manipolazione di struttura ad albero

13.5 Il protocollo Rapid Spanning Tree

L'RSTP utilizza lo stesso algoritmo dell'STP per la determinazione della struttura ad albero. Quando un collegamento o uno switch diventano inutilizzabili, l'RSTP si limita a modificare i parametri e aggiunge nuovi parametri e meccanismi che velocizzano la riconfigurazione.

Le porte hanno un ruolo fondamentale in questo contesto.

13.5.1 Ruoli della porta

L'RSTP assegna a ciascuna porta switch uno dei seguenti ruoli (vedi figura 47):

- Porta root
  Questa è la porta in cui lo switch riceve i pacchetti dati con i costi di percorso più bassi dal root switch.
  Quando vi sono più porte con costi di percorso root ugualmente bassi, l'ID dello switch che conduce al root (switch designato) decide a quale delle sue porte lo switch lontano dal root assegnerà il ruolo di Root Port.
  Quando uno switch dispone di più porte con costi di percorso ugualmente bassi verso lo stesso switch, lo switch utilizza l'ID della porta dello switch che conduce al root (switch designato) per decidere quale porta selezionare localmente come Root Port (vedi figura 43).
  Lo stesso root switch non dispone di una Root Port.
- Porta designata:
  lo switch in un segmento di rete con i costi di percorso root più bassi è lo switch designato. Quando vi è più di uno switch con gli stessi costi di percorso root, lo switch con l'identificatore switch dal valore più basso diventa lo switch designato. La porta designata su questo switch è la porta che collega un segmento di rete che conduce lontano dal root switch. Quando uno switch è collegato ad un segmento di rete con più di una porta (tramite un hub, ad esempio), lo switch attribuisce il ruolo di porta designata alla porta con l'ID della porta migliore.
- Porta edge
  Ciascun segmento di rete senza ulteriori switch RSTP è collegato con una sola porta designata. In questo caso la porta designata è anche una porta edge. La distinzione di una porta edge è data dal fatto che non riceve alcuna RST BPDU (Rapid Spanning Tree Switch Protocol Data Units).
- Porta alternativa
  Quando il collegamento al root switch si interrompe, questa porta bloccata assume il compito della porta root. La porta alternativa fornisce un backup per il collegamento al root switch.

- Porta di backup
  Questa è una porta bloccata che funge da backup in caso di interruzione del collegamento alla porta designata di questo segmento di rete (senza alcuno switch RSTP).
- Porta disabilitata
  Questa porta non partecipa allo Spanning Tree Operation, ciò significa che la porta è spenta o non dispone di alcun collegamento.

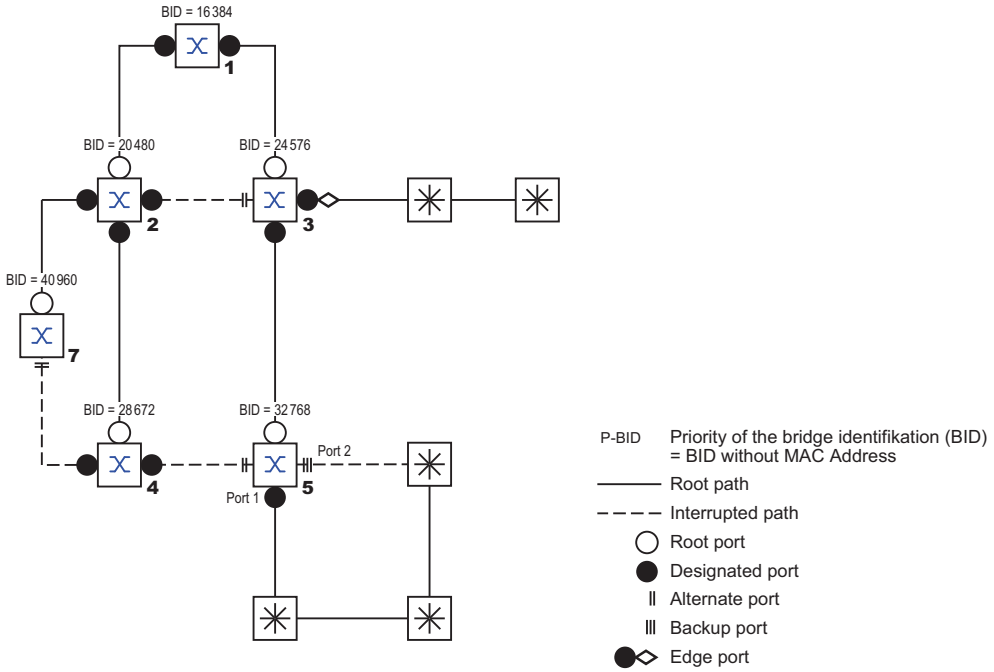


Figura 47: Assegnazione dei ruoli porta

13.5.2 Status porta

A seconda della struttura ad albero e dello stato dei percorsi di collegamento selezionati, l'RSTP assegna alle porte i loro stati.

Tabella 36:Relazione tra i valori di stato della porta per STP e RSTP

Stato porta STP	Stato porta switch amministrativo	MAC operativo	Stato della porta RSTP	Topologia attiva (ruolo della porta)
DISABLED	Disabilitato	FALSE	Discarding[1]	Escluso (disabilitato)
DISABLED	Abilitato	FALSE	Discarding[a]	Escluso (disabilitato)
BLOCKING	Abilitato	TRUE	Discarding[2]	Escluso (alternativa, backup)
LISTENING	Abilitato	TRUE	Discarding[b]	Incluso (root, designato)
LEARNING	Abilitato	TRUE	Learning	Incluso (root, designato)
FORWARDING	Abilitato	TRUE	Forwarding	Incluso (root, designato)

1. Il dot1d-MIB mostra “Disabilitato”.
2. Il dot1d-MIB mostra “Bloccato”.

Significato degli stati della porta RSTP:
- Disabilitato: la porta non appartiene alla topologia attiva
- Rifiuto: nessun apprendimento indirizzi nell'FDB, nessun traffico dati eccetto per STP-BPDU

- Apprendimento: apprendimento indirizzi attivo (FDB), nessun traffico dati eccetto da STP-BPDU
- Inoltro: apprendimento indirizzi attivo (FDB), invio e ricezione di tutti i tipi di pacchetto (non solo STP-BPDU)

13.5.3 Spanning Tree Priority Vector

Per assegnare ruoli alle porte, gli switch RSTP si scambiano le informazioni di configurazione. Queste informazioni sono note come Spanning Tree Priority Vector. Sono parte delle RST-BPDU e includono le seguenti informazioni:

- Identificazione dello switch del root switch
- Costi del percorso root dello switch di invio
- Switch ID dello switch di invio
- Identificativi delle porte tramite cui è stato inviato il messaggio
- Identificativi delle porte tramite cui è stato ricevuto il messaggio

In base a queste informazioni, gli switch partecipanti all'RSTP sono in grado da soli di determinare i ruoli della porta e di definire gli stati delle proprie porte.

13.5.4 Riconfigurazione rapida

Perché l'RSTP può reagire a un'interruzione del percorso root in modo più rapido rispetto a un STP?

- Introduzione alle porte edge:
  Durante una riconfigurazione, l'RSTP imposta una porta edge nell'ambito della modalità di trasmissione dopo 3 secondi (impostazione di default). Per assicurarsi che nessuno switch che invia BPDU sia collegato, l'RSTP attende lo scadere dell'“Hello Time”.
  Se l'utente verifica che un dispositivo finale sia e rimanga collegato a questa porta, non vi sono tempi di attesa presso questa porta nel caso di una riconfigurazione.
- Introduzione alle porte alternative:
  Mentre i ruoli della porta sono già distribuiti in un funzionamento normale, uno switch può passare immediatamente dalla Root Port alla porta alternativa dopo l'interruzione del collegamento al root switch.
- Comunicazione con gli switch adiacenti (collegamenti punto-punto):
  La comunicazione diretta e decentralizzata tra gli switch adiacenti consente la reazione senza periodi di attesa alle modifiche dello stato nella topologia Spanning Tree.
- Tabella indirizzi:
  Con l'STP, l'età delle voci nell'FDB determina l'aggiornamento della comunicazione. L'RSTP cancella immediatamente le voci nelle porte interessate da una riconfigurazione.
- Reazione agli eventi:
  Senza doversi attenere ad alcuna specifica temporale, l'RSTP reagisce immediatamente a eventi quali le interruzioni dei collegamenti, i ripristini dei collegamenti, etc.

Nota: I pacchetti dati potrebbero essere duplicati e/o arrivare al destinatario nell'ordine sbagliato durante la fase di riconfigurazione della topologia RSTP. È possibile anche utilizzare lo Spanning Tree Protocol o selezionare un'altra procedura di ridondanza descritta in questo manuale.

13.5.5 Configurazione del dispositivo

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per aiutare a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della configurazione *Spanning Tree*. Prima di collegare le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione *Spanning Tree*.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

L'RSTP configura la topologia di rete in modo completamente autonomo. Il dispositivo con la priorità switch più bassa diventa automaticamente il root switch. Tuttavia, per definire una struttura di rete specifica in ogni caso, si specifica un dispositivo come root switch. In generale, un dispositivo nel backbone assume questo ruolo.

Eseguire i seguenti passaggi:
- ☐ Impostare la rete in base alle proprie esigenze, inizialmente senza linee ridondanti.
- ☐ Si disattiva il controllo di flusso sulle porte interessate.
  Se la funzionalità di ridondanza e il controllo del flusso sono attivi contemporaneamente, è possibile che la funzionalità di ridondanza operi in modo diverso dal previsto. (Impostazione di default: controllo di flusso disattivato globalmente e attivato su tutte le porte.)
- ☐ Disabilitare l'MRP su tutti i dispositivi.
- ☐ Abilitare lo Spanning Tree su tutti i dispositivi nella rete.
  In stato di fornitura, lo Spanning Tree è attivo nel dispositivo.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Abilitare la funzione.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`spanning-tree operation`	Abilita lo Spanning Tree.
`show spanning-tree global`	Mostra i parametri per il controllo.

Adesso collegare le linee ridondanti.

Definire le impostazioni per il dispositivo che assume il ruolo di root switch.

Eseguire i seguenti passaggi:

- ☐ Nel campo *Priority* si immette un valore numericamente inferiore.
  Lo switch con lo switch ID numericamente più basso ha la massima priorità e diventa il root switch della rete.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`spanning-tree mst priority 0 <0..61440>`	Specifica la priorità switch del dispositivo. **Nota:** Specifica la priorità switch nell'intervallo `0..61440` in step da 4069.

Dopo il salvataggio, la finestra di dialogo mostra le seguenti informazioni:
- La casella di spunta *Bridge is root* è selezionata.
- Il campo *Root port* mostra il valore `0.0`.
- Il campo *Root path cost* mostra il valore `0`.

`show spanning-tree global`	Mostra i parametri per il controllo.

- ☐ Se applicabile, modificare i valori nei campi *Forward delay [s]* e *Max age*.
  - Il root switch trasmette i valori modificati agli altri dispositivi.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`spanning-tree forward-time <4..30>`	Specifica il tempo di ritardo per la modifica dello stato in secondi.
`spanning-tree max-age <6..40>`	Specifica la lunghezza massima del ramo consentita, ad esempio il numero di dispositivi fino al root switch.
`show spanning-tree global`	Mostra i parametri per il controllo.

Nota: I parametri *Forward delay [s]* e *Max age* hanno le seguenti relazioni:

Forward delay [s] ≥ (*Max age*/2) + 1

Se all'interno dei campi si inseriscono valori che contraddicono questa relazione, il dispositivo sostituisce tali valori con gli ultimi valori validi o con il valore di default.

Nota: Quando possibile, non modificare il valore nel campo “Hello Time”.

Verificare i seguenti valori negli altri dispositivi:
- lo switch ID (priorità switch e indirizzo MAC) del dispositivo corrispondente e il root switch.
- Numero della porta del dispositivo che conduce al root switch.
- Costo di percorso dalla Root Port del dispositivo al root switch.

Eseguire i seguenti passaggi:

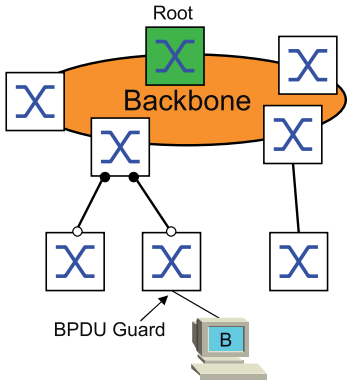
`show spanning-tree global`	Mostra i parametri per il controllo.

13.5.6 Guard

Il dispositivo consente di attivare varie funzioni di protezione (guard) nelle porte del dispositivo.

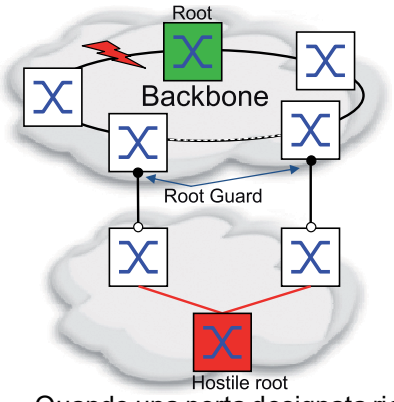
Le seguenti funzioni di protezione contribuiscono a proteggere la propria rete da configurazioni errate, loop e attacchi con STP-BPDU:

- BPDU Guard – per le porte edge specificate manualmente (porte del dispositivo finale)
  Si attiva questa funzione di protezione globalmente nel dispositivo.



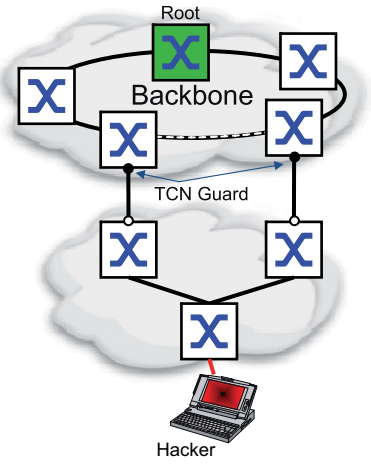
Di norma, le porte del dispositivo finale non ricevono alcuna STP-BPDU. Se un aggressore prova ancora a introdurre le STP-BPDU su questa porta, il dispositivo disattiva la porta del dispositivo.

- Root Guard – per porte designate
  Si attiva questa funzione di protezione separatamente per ciascuna porta del dispositivo.

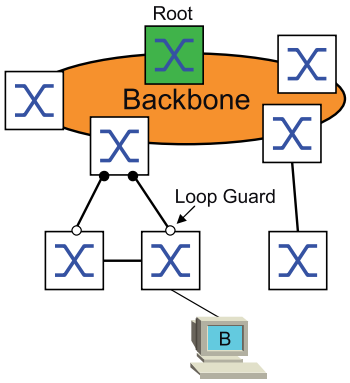


Quando una porta designata riceve una STP-BPDU con migliori informazioni sul percorso verso il root switch, il dispositivo la rifiuta e imposta lo stato di trasmissione della porta su `discarding` invece che `root`.
Quando non vi sono STP-BPDU con migliori informazioni sul percorso verso il root switch, dopo 2 x *Hello time [s]* il dispositivo ripristina lo stato della porta su un valore conforme al ruolo della porta.

- TCN Guard – per le porte che ricevono STP-BPDU con un flag di modifica della topologia
  Si attiva questa funzione di protezione separatamente per ciascuna porta del dispositivo.



  Se la funzione di protezione è attivata, il dispositivo ignora i flag di modifica della topologia nelle STP-BPDU ricevute. Ciò non modifica il contenuto della tabella indirizzi (FDB) della porta del dispositivo. Tuttavia, nella BPDU, il dispositivo elabora ulteriori informazioni che modificano la topologia.
- Loop Guard – per porte di backup, alternative e root
  Si attiva questa funzione di protezione separatamente per ciascuna porta del dispositivo.



  Se la porta non riceve più alcuna STP-BPDU, questa funzione di protezione aiuta a prevenire la modifica involontaria dello stato di trasmissione di una porta su `forwarding`. Se ciò accade, il dispositivo designa lo stato di loop della porta come incoerente, ma non inoltra alcun pacchetto dati.

Attivazione del BPDU Guard

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Selezionare la casella di spunta *BPDU guard*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.

`configure`	Passare alla modalità di configurazione.
`spanning-tree bpdu-guard`	Attiva il BPDU Guard.
`show spanning-tree global`	Mostra i parametri per il controllo.

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*.
- ☐ Passare alla scheda *CIST*.
- ☐ Per le porte dei dispositivi finali, selezionare la casella di spunta nella colonna *Admin edge port*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`interface <x/y>`	Passare alla modalità di configurazione di interfaccia `<x/y>`.
`spanning-tree edge-port`	Designa la porta come porta del dispositivo finale (porta edge).
`show spanning-tree port x/y`	Mostra i parametri per il controllo.
`exit`	Abbandona la modalità interfaccia.

Quando una porta edge riceve una STP-BPDU, il dispositivo si comporta come segue:

- ▶ Il dispositivo disattiva questa porta.
  Nella finestra di dialogo *Basic Settings > Port*, scheda *Configuration*, la casella di spunta per questa porta nella colonna *Port on* è `non selezionata`.
- ▶ Il dispositivo designa la porta.

È possibile stabilire se una porta si è disabilitata a causa di un BPDU ricevuto. A tale scopo, eseguire i seguenti passaggi:

Nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, scheda *Guards*, la casella di spunta nella colonna *BPDU guard effect* è `selezionata`.

`show spanning-tree port x/y`	Mostra i parametri della porta per il controllo. Il valore del parametro *BPDU guard effect* è `enabled`.

Ripristinare lo stato della porta del dispositivo sul valore `forwarding`. A tale scopo, eseguire i seguenti passaggi:

- ☐ Quando la porta riceve ancora BPDU:
  - – Rimuovere la definizione manuale di porta edge (porta del dispositivo finale).
    oppure
  - – Disattivare il BPDU Guard.
- ☐ Attivare nuovamente la porta del dispositivo.

Attivazione Root Guard / TCN Guard / Loop Guard

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*.
- ☐ Passare alla scheda *Guards*.
- ☐ Per le porte designate, selezionare la casella di spunta nella colonna *Root guard*.
- ☐ Per le porte che ricevono STP-BPDU con un flag di modifica della topologia, selezionare la casella di spunta nella colonna *TCN guard*.
- ☐ Per porte di backup, alternative o root, selezionare la casella di spunta nella colonna *Loop guard*.

Nota: Le funzioni *Root guard* e *Loop guard* si escludono a vicenda. Se si prova ad attivare la funzione *Root guard* mentre la funzione *Loop guard* è attiva, il dispositivo disattiva la funzione *Loop guard*.

- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface <x/y>`	Passare alla modalità di configurazione di interfaccia `<x/y>`.
`spanning-tree guard-root`	Attiva il Root Guard presso la porta designata.
`spanning-tree guard-tcn`	Attiva il TCN Guard presso la porta che riceve STP-BPDU con una bandiera di modifica della topologia.
`spanning-tree guard-loop`	Attiva il Loop Guard presso la porta di backup, alternativa o root.
`exit`	Abbandona la modalità interfaccia.
`show spanning-tree port x/y`	Mostra i parametri della porta per il controllo.

13.6 Dual RSTP (MCSESM-E)

Le applicazioni industriali richiedono una grande disponibilità delle reti. Ciò implica inoltre tempi di interruzione brevi e deterministici per la comunicazione qualora uno dei componenti di rete diventi inutilizzabile.

Una topologia ad anello contribuisce a fornire tempi di interruzione ridotti con un impiego minimo di risorse. Utilizzando il protocollo *Spanning Tree*, il tempo di interruzione dipende dalle dimensioni della rete. Per ottimizzare il tempo di interruzione si possono dividere reti *Spanning Tree* di grandi dimensioni in segmenti ad anello più piccoli.

La funzione *Dual RSTP* è utilizzata insieme alla funzione *RCP*. Utilizzando la funzione *RCP* si ha la possibilità di collegare uno o più RSTP ring all'istanza RSTP in un anello primario. Quando si collegano due segmenti *Spanning Tree*, l'anello secondario rappresenta un'istanza RSTP separata per la quale si applicano le impostazioni della funzione *Dual RSTP*. Tale istanza *Dual RSTP* agisce in maniera indipendente dall'istanza RSTP dell'anello primario e degli altri anelli secondari. Quando l'RSTP è il protocollo utilizzato in uno solo degli anelli da collegare, la funzione *Dual RSTP* non è necessaria.

13.7 Aggregazione dei collegamenti

La funzione *Link Aggregation* tramite il metodo a switch unico contribuisce a superare i 2 limiti con i collegamenti Ethernet, ovvero larghezza di banda e ridondanza.

La funzione *Link Aggregation* contribuisce a superare i limiti di larghezza di banda delle singole porte. La funzione *Link Aggregation* consente di combinare 2 o più link in parallelo, creando 1 link logico tra 2 dispositivi. I link paralleli aumentano la larghezza di banda per il traffico tra i 2 dispositivi.

In genere si utilizza la funzione *Link Aggregation* sul backbone della rete. La funzione fornisce un modo conveniente per aumentare progressivamente la larghezza di banda.

Inoltre, la funzione *Link Aggregation* fornisce ridondanza con un failover senza soluzione di continuità. Quando un link è interrotto, con 2 o più link configurati in parallelo, gli altri link nel gruppo continuano a inoltrare traffico.

Le impostazioni di default per una nuova istanza di *Link Aggregation* sono le seguenti:
- Nella colonna *Active*, la casella di spunta è selezionata.
- Nella colonna *Send trap (Link up/down)*, la casella di spunta è selezionata.
- Nella colonna *Static link aggregation*, la casella di spunta non è selezionata.
- Nella colonna *Active ports (min.)*, il valore è `1`.

13.7.1 Metodi di funzionamento

Il dispositivo utilizza il metodo a switch unico. Il metodo a switch unico fornisce un modo economico per far crescere la propria rete. Secondo il metodo a switch unico, per le porte fisiche è necessario un dispositivo su ciascun lato di un link. Il dispositivo bilancia il carico del traffico attraverso le porte dei membri del gruppo.

Il dispositivo utilizza anche il metodo della stessa velocità di collegamento in cui le porte dei membri del gruppo sono collegamenti duplex pieno, punto-punto, dotati della stessa velocità di trasmissione. La prima porta che l'utente aggiunge al gruppo è la porta master e determina la larghezza di banda per le altre porte dei membri del gruppo di Link Aggregation.

Il dispositivo consente di impostare fino a 2 gruppi di Link Aggregation. Il numero delle porte utilizzabili per il gruppo di Link Aggregation dei collegamenti dipende dal dispositivo.

13.7.2 Esempio di Link Aggregation

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per aiutare a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della configurazione *Link Aggregation*. Prima di collegare le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione *Link Aggregation*.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Collegare più postazioni di lavoro utilizzando un gruppo di link aggregati tra Switch 1 e 2. Aggregando più link è possibile ottenere velocità superiori senza un aggiornamento hardware.

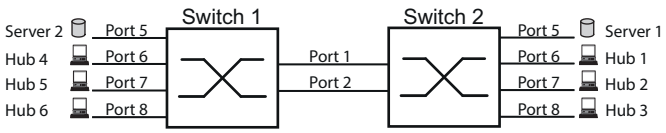


Figura 48: Rete di Link Aggregation da switch a switch

Configurare Switch 1 e 2 nell'interfaccia grafica utente. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Link Aggregation*.
- ☐ Fare clic sul pulsante .
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Nell'elenco a discesa *Trunk port*, selezionare il numero dell'istanza del gruppo di Link Aggregation.
- ☐ Nell'elenco a discesa *Port*, selezionare la porta *1/1*.
- ☐ Fare clic sul pulsante *Ok*.
- ☐ Ripetere i passaggi precedenti e selezionare la porta *1/2*.
- ☐ Fare clic sul pulsante *Ok*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`link-aggregation add lag/1`	Crea un gruppo di Link Aggregation `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Aggiunge la porta *1/1* al gruppo di Link Aggregation.
`link-aggregation modify lag/1 addport 1/2`	Aggiunge la porta *1/2* al gruppo di Link Aggregation.

13.8 Backup dei link

Il backup dei link fornisce un collegamento ridondante per il traffico sui dispositivi Layer 2. Quando rileva un errore sul link primario, il dispositivo trasferisce il traffico al link di backup. In genere si utilizza il backup dei link nelle reti del fornitore di servizi o aziendali.

Si impostano link di backup a coppie, uno come primario e uno come backup. Quando si fornisce ridondanza per reti aziendali, ad esempio, il dispositivo consente di impostare più di una coppia. Il numero massimo di coppie di backup dei link è: numero totale di porte fisiche / 2. Inoltre, quando lo stato di una porta partecipante a una coppia di backup dei link cambia, il dispositivo invia una trap SNMP.

Quando si configurano coppie di backup dei link, ricordare le seguenti regole:
- Una coppia di link è costituita da qualsiasi combinazione di porte fisiche. Per esempio, una porta è da 100 Mbit e l'altra è una porta SFP da 1000 Mbit.
- Una porta specifica è membro di una coppia di backup dei link in qualsiasi momento.
- Verificare che le porte di una coppia di backup dei link siano membri della stessa VLAN con lo stesso ID VLAN. Quando la porta primaria o la porta di backup sono membri di una VLAN, assegnare la seconda porta della coppia alla stessa VLAN.

L'impostazione di default per questa funzione non è attiva senza alcuna coppia di backup dei link.

Nota: Verificare che il protocollo Spanning Tree sia disabilitato sulle porte di backup dei link.

13.8.1 Descrizione del fail back

Il backup dei link consente inoltre di impostare un'opzione di fail back. Quando si attiva la funzione di fail back e il link primario torna al funzionamento normale, il dispositivo blocca prima il traffico sulla porta di backup e poi lo inoltra sulla porta primaria. Questo processo contribuisce impedire che il dispositivo causi loop nella rete.

Quando la porta primaria ritorna allo stato attivo e di link up, il dispositivo supporta 2 modalità operative:
- Quando si disattiva il *Fail back*, la porta primaria rimane in stato di blocco fino a quando il link di backup non si interrompe.
- Quando si attiva il *Fail back*, e dopo lo scadere del timer *Fail back delay [s]*, la porta primaria ritorna allo stato di inoltro e la porta di backup si disattiva.

Nei casi sopra elencati, la porta che forza il proprio link a inoltrare il traffico, invia prima un pacchetto “flush FDB” al dispositivo remoto. Il pacchetto flush aiuta il dispositivo remoto a riapprendere rapidamente gli indirizzi MAC.

13.8.2 Configurazione esemplificativa

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per aiutare a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della configurazione *Link Backup*. Prima di collegare le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione *Link Backup*.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Nella rete esemplificativa di seguito, si collegano le porte *2/3* e *2/4* sullo Switch A agli Switch uplink B e C. Quando si impostano le porte come coppia di backup dei link, una delle porte inoltra il traffico e l'altra porta è in modalità di blocco.

La porta primaria *2/3* sullo Switch A è la porta attiva e inoltra il traffico alla porta 1 sullo Switch B. La porta *2/4* sullo Switch A è la porta di backup e blocca il traffico.

Quando lo Switch A disabilita la porta *2/3* a causa di un errore rilevato, la porta *2/4* sullo Switch A inizia a inoltrare il traffico alla porta 2 sullo Switch C.

Quando la porta *2/3* torna allo stato attivo, “nessun spegnimento”, con *Fail back* attivato, e *Fail back delay [s]* impostato su 30 secondi. Alla scadenza del timer, prima la porta *2/4* blocca il traffico e poi e la porta *2/3* inizia a inoltrare il traffico.

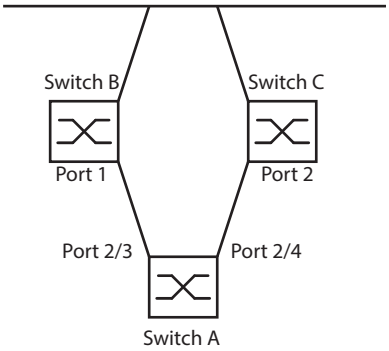


Figura 49: Rete esemplificativa Link Backup

Nelle seguenti tabelle sono riportati esempi dei parametri per la configurazione dello Switch A.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Link Backup*.
- ☐ Immettere una nuova coppia di backup dei link nella tabella:
  - ☐ Fare clic sul pulsante .
    La finestra di dialogo mostra la finestra *Create*.
  - ☐ Nell'elenco a discesa *Primary port*, selezionare la porta *2/3*.
    Nell'elenco a discesa *Backup port*, selezionare la porta *2/4*.
  - ☐ Fare clic sul pulsante *Ok*.
- ☐ Nella casella di testo *Description*, immettere `Link_Backup_1` come nome per la coppia di backup.

- ☐ Per attivare la funzione *Fail back* per la coppia di backup dei link, selezionare la casella di spunta *Fail back*.
- ☐ Impostare il timer di fail back per la coppia di backup dei link, immettere `30` secondi in *Fail back delay [s]*.
- ☐ Per attivare la coppia di backup dei link, selezionare la casella di spunta *Active*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 2/3`	Passare alla modalità di configurazione dell'interfaccia *2/3*.
`link-backup add 2/4`	Crea un'istanza di backup dei link in cui la porta *2/3* è la porta primaria e la porta *2/4* è la porta di backup.
`link-backup modify 2/4 description Link_Backup_1`	Specifica la stringa `Link_Backup_1` come nome della coppia di backup.
`link-backup modify 2/4 failback-status enable`	Abilitare il timer di fail back.
`link-backup modify 2/4 failback-time 30`	Specificare il tempo di ritardo di fail back su `30` secondi.
`link-backup modify 2/4 status enable`	Abilitare l'istanza del backup dei link.
`exit`	Passare alla modalità di configurazione.
`link-backup operation`	Abilita la funzione *Link Backup* globalmente nel dispositivo.

13.9 FuseNet

I protocolli *FuseNet* consentono di collegare gli anelli che funzionano con uno dei seguenti protocolli di ridondanza:

- MRP
- HIPER ring
- RSTP

Nota: Il prerequisito per collegare una rete all'anello principale utilizzando il protocollo *Ring/Network Coupling* è che la rete collegata contenga solo dispositivi di rete che supportano il protocollo *Ring/Network Coupling*.

Utilizzare la seguente tabella per selezionare il protocollo di collegamento *FuseNet* da utilizzare nella propria rete:

Anello principale	**Rete connessa**		
	MRP	**HIPER ring**	**RSTP**
MRP	*Sub Ring*[1)]	– *Redundant Coupling Protocol* – *Ring/Network Coupling*	– *Redundant Coupling Protocol* – *Ring/Network Coupling*
HIPER ring	*Sub Ring*	*Ring/Network Coupling*	– *Redundant Coupling Protocol* – *Ring/Network Coupling*
RSTP	*Redundant Coupling Protocol*	*Redundant Coupling Protocol*	*Dual RSTP* + *Redundant Coupling Protocol*

– nessun protocollo di collegamento idoneo

1) con *MRP* configurate su VLAN diverse

13.10 Subring

La funzione *Sub Ring* è un'estensione del Media Redundancy Protocol (MRP). Questa funzione consente di collegare un subring a un anello principale tramite varie strutture di rete.

Il protocollo del Subring fornisce ridondanza per dispositivi collegando entrambe le estremità di una rete altrimenti piatta a un anello principale.

La configurazione dei subring presenta i seguenti vantaggi:
- Mediante il processo di collegamento si include il nuovo segmento nel concetto di ridondanza.
- I subring consentono la facile integrazione di nuove aree all'interno di reti esistenti.
- I subring consentono la facile mappatura della struttura organizzativa di un'area in una topologia di rete.
- In un MRP Ring, i tempi di failover del subring nei casi di ridondanza sono generalmente inferiori a 100 < millisecondi.

13.10.1 Descrizione del subring

Il concetto di subring consente di collegare nuovi segmenti di rete a dispositivi adeguati in un anello esistente (anello principale). I dispositivi con cui si collega il subring all'anello principale sono i Subring Manager (SRM).

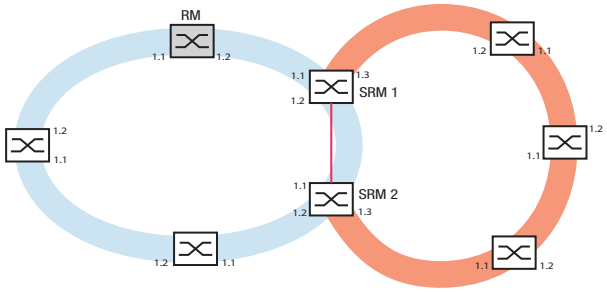


Figura 50: Esempio di una struttura subring
anello blu = Anello principale
anello arancione = Subring
linea rossa = Collegamento ridondante del subring
SRM = Subring Manager
RM = Ring Manager

I dispositivi compatibili con il Subring Manager supportano fino a 8 istanze e di conseguenza gestiscono fino a 8 subring contemporaneamente.

La funzione *Sub Ring* consente di integrare dispositivi che supportano MRP come partecipanti. I dispositivi con cui si collega il subring all'anello principale necessitano della funzione *Sub Ring* Manager.

Ciascun subring può essere costituito da un massimo di 200 partecipanti, esclusi i Subring Manager stessi e i dispositivi tra i Subring Manager nell'anello principale.

Le seguenti figure mostrano esempi delle possibili topologie di subring:

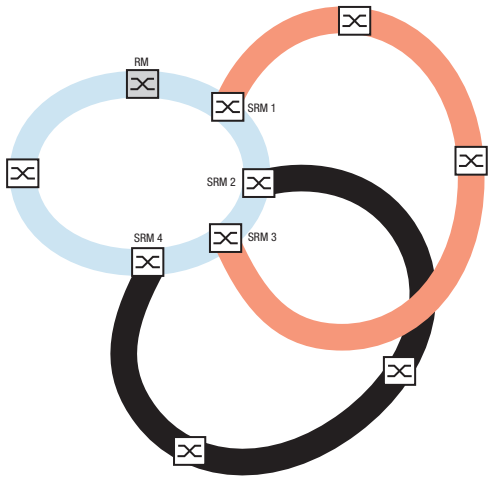


Figura 51: Esempio di una struttura subring sovrapposta

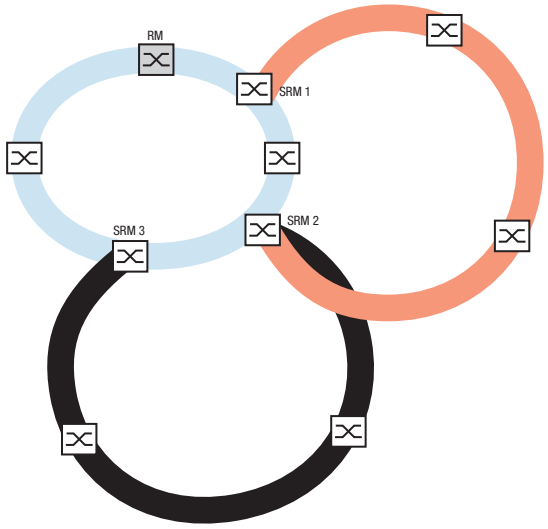


Figura 52: Caso speciale: un Subring Manager gestisce 2 subring (2 istanze). Il Subring Manager è in grado di gestire fino a 8 istanze.

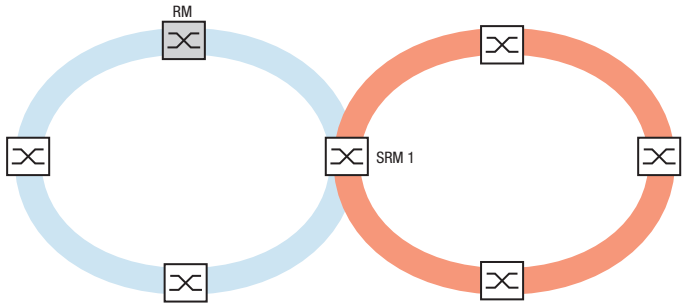


Figura 53: Caso speciale: un Subring Manager gestisce entrambe le estremità di un subring su porte diverse (Subring Manager singolo).

Nota: Nei precedenti esempi, i Subring Manager collegano subring solo agli anelli principali esistenti. La funzione *Sub Ring* impedisce i subring a cascata, ad esempio il collegamento di un nuovo subring ad un altro subring esistente.

Se si utilizza l'MRP per l'anello principale e il subring, specificare le impostazioni VLAN come segue:

- VLAN `X` per l'anello principale
  - sulle Ring port dei partecipanti all'anello principale
  - sulle Ring port principali del Subring Manager
- VLAN `Y` per il Subring
  - sulle Ring port dei partecipanti al Subring
  - sulle porte subring del Subring Manager

  Si può utilizzare la stessa VLAN per più subring.

13.10.2 Esempio di Subring

Nell'esempio seguente, si collega un nuovo segmento di rete con 3 dispositivi a un anello principale esistente che utilizza il protocollo MRP. Quando si collega la rete a entrambe le estremità invece che a una, il subring fornisce disponibilità aumentata con la configurazione corrispondente.

Si collega il nuovo segmento di rete come subring. Si collega il subring ai dispositivi esistenti dell'anello principale tramite i seguenti tipi di configurazione.

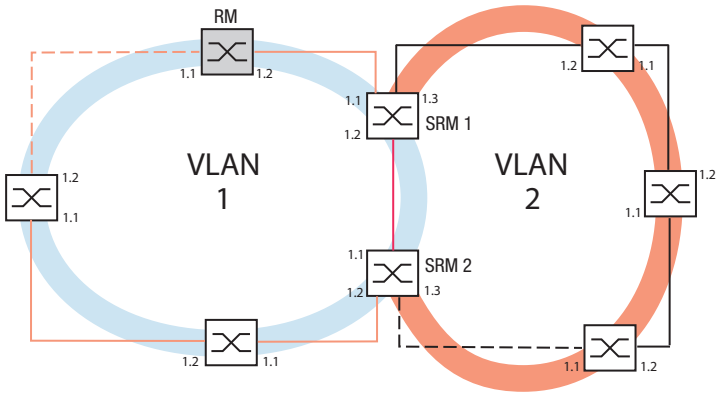


Figura 54: Esempio di una struttura subring
linea arancione = membri dell'anello principale nella VLAN 1
linea nera = membri del Subring nella VLAN 2
linea tratteggiata arancione = loop dell'anello principale aperto
linea tratteggiata nera = loop del Subring aperto
linea rossa = membro del collegamento ridondante nella VLAN 1
SRM = Subring Manager
RM = Ring Manager

Per configurare il subring eseguire i seguenti passaggi:

- ☐ Configurare i tre dispositivi del nuovo segmento di rete come partecipanti in un MRP ring:
  - Configurare la velocità di trasmissione e la modalità duplex per le Ring port in conformità alla seguente tabella:

Tabella 37:Impostazioni della porta per porte subring

Tipo di porta	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`selezionato`	`non selezionato`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`selezionato`	`selezionato`	–

Tabella 37:Impostazioni della porta per porte subring

Tipo di porta	Bit rate	Port on	Automatic configuration	Manual configuration
Ottico	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
Ottico	1 Gbit/s	selezionato	selezionato	–
Ottico	2.5 Gbit/s	selezionato	–	*2.5 Gbit/s FDX*

I passaggi seguenti contengono ulteriori impostazioni per la configurazione del subring:

- ☐ Per contribuire a evitare la formazione di loop durante la configurazione, disattivare la funzione Subring Manager su anello principale e dispositivi subring. Dopo aver configurato completamente tutti i dispositivi partecipanti all'anello principale e i subring, attivare la funzione *Sub Ring* globale e i Subring Manager.
- ☐ Disabilitare la funzione RSTP sulle porte MRP ring utilizzate nel subring.
- ☐ Controllare che la funzione *Link Aggregation* non sia attiva sulle porte partecipanti ad anello principale e subring.
- ☐ Specificare un'appartenenza VLAN diversa per le Ring port principali e per le porte subring anche se l'anello principale utilizza il protocollo MRP. Per esempio, utilizzare l'ID VLAN 1 per l'anello principale e il collegamento ridondante, poi utilizzare l'ID VLAN 2 per il subring.
  - – Per i dispositivi partecipanti all'anello principale ad esempio, aprire la finestra di dialogo *Switching > VLAN > Configuration*. Creare la VLAN 1 nella tabella della VLAN statica. Per taggare le Ring port principali per l'appartenenza alla VLAN 1, selezionare la voce T nell'elenco a discesa delle colonne adeguate della porta.
  - – Per i dispositivi partecipanti al subring utilizzare il passaggio di cui sopra e aggiungere le porte alla VLAN 2 nella tabella della VLAN statica.
- ☐ Attivare la funzione *MRP* per l'anello principale e i dispositivi subring.
  - – Nella finestra di dialogo *Switching > L2-Redundancy > MRP*, configurare le 2 Ring port partecipanti all'anello principale sui dispositivi ring principali.
  - – Per i dispositivi partecipanti al subring utilizzare il passaggio di cui sopra e configurare le 2 Ring port partecipanti al subring sui dispositivi subring.
  - – Assegnare lo stesso ID del dominio MRP all'anello principale e ai dispositivi subring. Quando si utilizzano solo Schneider Electric dispositivi, i valori di default sono sufficienti all'ID del dominio MRP.

Nota: *MRP domain* è una sequenza di 16 numeri nell'intervallo da 0 a 255. Il valore di default è 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255. Un *MRP domain* costituito interamente da zero non è valido.

Una finestra di dialogo *Sub Ring* consente di modificare l'ID del dominio MRP. In alternativa, utilizzare la Command Line Interface. A tale scopo, eseguire i seguenti passaggi:

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`mrp domain delete`	Cancella il dominio MRP attuale.
`mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111.222.123.0.0.66.99`	Crea un nuovo dominio MRP con l'ID del dominio MRP specificato. Qualsiasi modifica successiva del dominio MRP si applica all'ID di questo dominio.

13.10.3 Configurazione esemplificativa subring

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per aiutare a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della configurazione *Sub Ring*. Prima di connettere le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione ad anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Nota: Contribuire a evitare la formazione di loop durante la configurazione. Configurare ciascun dispositivo del subring separatamente. Prima di attivare il collegamento ridondante, configurare completamente tutti i dispositivi subring.

Configurare i 2 Subring Manager nell'esempio. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Sub Ring*.
- ☐ Per aggiungere una voce tabella, fare clic sul pulsante  .
- ☐ Nella colonna *Port*, selezionare la porta che collega il dispositivo al subring.
  Utilizzare la porta *1/3* per questo esempio.
  Per il collegamento, utilizzare una delle porte disponibili a eccezione delle porte già collegate all'anello principale.
- ☐ Nella colonna *Name*, assegnare un nome al subring.
  Per questo esempio immettere `Test`.
- ☐ Nella colonna *SRM mode*, selezionare la modalità Subring Manager.
  Si specifica così quale porta per il collegamento del subring all'anello principale diventa Redundant Manager.
  Le opzioni per il collegamento sono:
  - `manager`
    Quando si specificano entrambi i Subring Manager con lo stesso valore, il dispositivo con l'indirizzo MAC superiore gestisce il link ridondante.
  - `redundant manager`
    Il dispositivo gestisce il link ridondante finché non si specifica l'altro Subring Manager come `manager`. Altrimenti il dispositivo con l'indirizzo MAC superiore gestisce il link ridondante.

  Specificare il Subring Manager 1 come `manager`, in conformità alla figura che rappresenta questo esempio.
- ☐ Lasciare invariati i valori nella colonna *VLAN* e *MRP domain*.
  I valori di default sono corretti per la configurazione esemplificativa.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`sub-ring add 1`	Crea un nuovo subring con il subring ID `1`.
`sub-ring modify 1 port 1/3`	Specificare la porta *1/3* come porta subring.
`sub-ring modify 1 name Test`	Assegnare il nome `Test` al subring `1`.

`sub-ring modify 1 mode manager`	Assegnare la modalità `manager` al subring `1`.
`show sub-ring ring`	Mostrare lo stato dei subring su questo dispositivo.
`show sub-ring global`	Mostrare lo stato globale del subring su questo dispositivo.

- ☐ Configurare il 2° Subring Manager nello stesso modo.
  Specificare il Subring Manager 2 come `redundant manager`, in conformità alla figura rappresentata in questo esempio.

- ☐ Per attivare la funzione Subring Manager, selezionare la casella di spunta *Active* nella riga appropriata.
- ☐ Dopo aver configurato entrambi i Subring Manager e i dispositivi partecipanti al subring, abilitare la funzione e chiudere il collegamento ridondante.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`sub-ring enable 1`	Attivare il subring `1`.
`sub-ring enable 2`	Attivare il subring `2`.
`exit`	Passare alla modalità Privileged EXEC.
`show sub-ring ring <Domain ID>`	Mostrare le impostazioni dei subring selezionati.
`show sub-ring global`	Mostrare le impostazioni globali del subring.
`copy config running-config nvm profile Test`	Salvare le impostazioni correnti nel profilo di configurazione chiamato `Test` nella memoria non volatile (`nvm`).

13.11 Subring con LAG

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per aiutare a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della configurazione *Sub Ring*. Prima di connettere le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione ad anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Quando tra due dispositivi esistono almeno due linee di collegamento ridondanti parallele (cosiddetto trunk) combinate in un collegamento logico, vi è un collegamento con Link Aggregation (LAG).

Il dispositivo consente di utilizzare le porte LAG come Ring port con il protocollo *Sub Ring*.

13.11.1 Esempio

L'esempio seguente è un'impostazione semplice tra un MRP ring e un Subring.

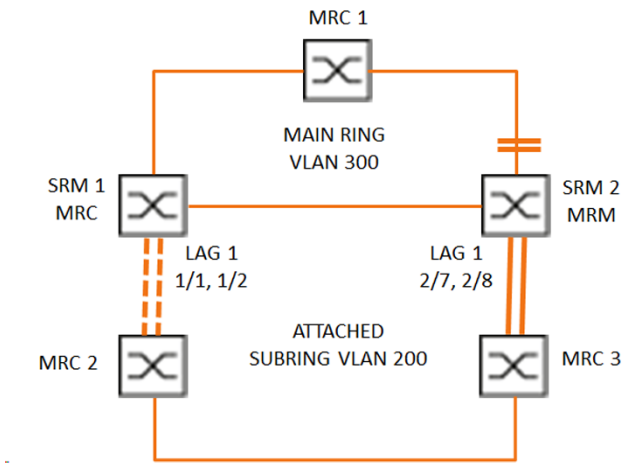


Figura 55: Subring con Link Aggregation

La seguente tabella descrive i ruoli del dispositivo come indicato nella figura di cui sopra. La tabella fornisce informazioni su come utilizzare le Ring port e le porte subring come porte LAG.

Tabella 38:Dispositivi, Porte e Ruoli

Nome dispositivo	Ring port	Ruolo anello principale	Ruolo subring	Porta subring
MRC1	1/3, 1/4	Client MRP	-	-
SRM1	1/3, 1/4	Client MRP	Redundant Manager	lag/1
SRM2	2/4, 2/5	MRP Manager	Manager	lag/1
MRC2	lag/1, 1/3	-	Client MRP	-
MRC3	lag/1, 1/3	-	Client MRP	-

Configurazione MRP ring

I dispositivi che partecipano all'anello principale sono membri della VLAN 300.

Eseguire i seguenti passaggi:

`SRM2`

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`mrp domain add default-domain`	Crea un nuovo dominio MRP con l'ID `default-domain`.
`mrp domain modify port primary 2/4`	Specifica la porta *2/4* come Ring port `1`.
`mrp domain modify port secondary 2/5`	Specifica la porta *2/5* come Ring port `2`.
`mrp domain modify mode manager`	Specifica che il dispositivo funziona come *Ring manager*. Non attivare la funzione *Ring manager* su altri dispositivi.
`mrp domain modify operation enable`	Attiva l'MRP Ring.
`mrp domain modify vlan 300`	Specifica l'ID VLAN come `300`.
`mrp operation`	Abilitare la funzione *MRP* nel dispositivo.

`MRC1, SRM1`

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`mrp domain add default-domain`	Crea un nuovo dominio MRP con l'ID `default-domain`.
`mrp domain modify port primary 1/3`	Specifica la porta *1/3* come Ring port `1`.
`mrp domain modify port secondary 1/4`	Specifica la porta *1/4* come Ring port `2`.
`mrp domain modify mode client`	Specifica il ruolo del dispositivo come ring client.
`mrp domain modify operation enable`	Attiva l'MRP Ring.
`mrp domain modify vlan 300`	Specifica l'ID VLAN come `300`.
`mrp operation`	Abilitare la funzione *MRP* nel dispositivo.

Configurazione subring

I dispositivi che partecipano al subring collegato sono membri della VLAN 200.

Eseguire i seguenti passaggi:

SRM1

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`link-aggregation add lag/1`	Crea un gruppo di Link Aggregation `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Aggiunge la porta *1/1* al gruppo di Link Aggregation.
`link-aggregation modify lag/1 addport 1/2`	Aggiunge la porta *1/2* al gruppo di Link Aggregation.
`link-aggregation modify lag/1 adminmode`	Attivare il gruppo di Link Aggregation.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`sub-ring add 1`	Crea un nuovo subring con il subring ID `1`.
`sub-ring modify 1 name SRM1`	Assegnare il nome `SRM1` al subring `1`.
`sub-ring modify 1 mode redundant-manager vlan 200 port lag/1`	Assegnare al dispositivo il ruolo `Sub-ring redundant manager` nel subring `1`. Se il subring è chiuso, il dispositivo blocca la Ring port. La VLAN `200` è impostata per l'ID VLAN del dominio. La porta `lag/1` è impostata come membro nella VLAN `200`.
`sub-ring enable 1`	Attivare il subring `1`.
`sub-ring operation`	Abilitare la funzionalità globale Subring Manager su questo dispositivo.

SRM2

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`link-aggregation add lag/1`	Crea un gruppo di Link Aggregation `lag/1`.
`link-aggregation modify lag/1 addport 2/7`	Aggiunge la porta *2/7* al gruppo di Link Aggregation.
`link-aggregation modify lag/1 addport 2/8`	Aggiunge la porta *2/8* al gruppo di Link Aggregation.
`link-aggregation modify lag/1 adminmode`	Attivare il gruppo di Link Aggregation.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`sub-ring add 1`	Crea un nuovo subring con il subring ID `1`.

`sub-ring modify 1 mode manager vlan 200 port lag/1`	Assegnare al dispositivo il ruolo `Subring manager` nel subring `1`. La VLAN `200` è impostata per l'ID VLAN del dominio. La porta `lag/1` è impostata come membro nella VLAN `200`.
`sub-ring modify 1 name SRM2`	Assegnare il nome `SRM2` al subring `1`.
`sub-ring enable 1`	Attivare il subring `1`.
`sub-ring operation`	Abilitare la funzionalità globale Subring Manager su questo dispositivo.

`MRC 2, 3`

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`mrp domain add default-domain`	Crea un nuovo dominio MRP con l'ID `default-domain`.
`mrp domain modify port primary lag/1`	Specifica la porta `lag/1` come Ring port `1`.
`mrp domain modify port secondary 1/3`	Specifica la porta *1/3* come Ring port `2`.
`mrp domain modify mode client`	Specifica il ruolo del dispositivo come ring client.
`mrp domain modify operation enable`	Attiva l'MRP Ring.
`mrp domain modify vlan 200`	Specifica l'ID VLAN come `200`.
`mrp operation`	Abilitare la funzione *MRP* nel dispositivo.

Disabilitare STP

Disabilitare la funzione *Spanning Tree* su tutte le porte specificate come porta MRP o subring. Il seguente esempio utilizza la porta *1/3*.

Eseguire i seguenti passaggi:

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/3`	Passare alla modalità di configurazione dell'interfaccia *1/3*.
`no spanning-tree operation`	Disabilitare la funzione *Spanning Tree* sulla porta.

13.12 Ring/Network Coupling

In base all'anello, la funzione *Ring/Network Coupling* collega gli anelli o i segmenti di rete in modo ridondante. Il *Ring/Network Coupling* collega 2 anelli/segmenti di rete attraverso 2 percorsi separati.

Quando i dispositivi nella rete collegata sono dispositivi Schneider Electric, la funzione *Ring/Network Coupling* supporta i seguenti protocolli di collegamento degli anelli negli anelli primari e secondari:
- HIPER Ring
- Fast HIPER Ring
- MRP

La funzione *Ring/Network Coupling* consente inoltre di collegare segmenti di rete di un bus e strutture a maglia.

13.12.1 Metodi di Ring/Network Coupling

Il collegamento a uno switch

Due porte di **un** dispositivo nel primo anello/rete collegano ciascuno dei due dispositivi nel secondo anello/rete (vedi figura 56) a una porta. Nel metodo di collegamento a uno switch, la linea principale inoltra i dati e il dispositivo blocca la linea ridondante.

Quando la linea principale non funziona più, il dispositivo sblocca immediatamente la linea ridondante. Quando la linea principale è ripristinata, il dispositivo blocca i dati sulla linea ridondante. La linea principale inoltra nuovamente i dati.

Il collegamento ad anello rileva e gestisce un errore entro 500 millisecondi (in genere 150 millisecondi).

Il collegamento a due switch

Una porta ciascuno da **due** dispositivi nel primo anello/rete collega ciascuno dei due dispositivi nel secondo anello/rete (vedi figura 58) a una porta ciascuno.

Il dispositivo nella linea ridondante e il dispositivo nella linea principale utilizzano i pacchetti di controllo per informarsi reciprocamente sui loro modi operativi tramite l'Ethernet o una linea di controllo.

Quando la linea principale non funziona più, il dispositivo ridondante (stand-by) sblocca immediatamente la linea ridondante. Non appena la linea principale è ripristinata, il dispositivo sulla linea principale lo comunica al dispositivo ridondante. Il dispositivo stand-by blocca i dati sulla linea ridondante. La linea principale inoltra nuovamente i dati.

Il collegamento ad anello rileva e gestisce un errore entro 500 millisecondi (in genere 150 millisecondi).

Il tipo di configurazione del collegamento è prevalentemente determinato dalla topologia della rete e dal livello di disponibilità desiderato (vedi tabella 39).

Tabella 39:Criteri di selezione per i tipi di configurazione per il collegamento ridondante.

	Collegamento a uno switch	Collegamento a due switch	Collegamento a due switch con linea di controllo
Applicazione	I 2 dispositivi sono disposti in posizioni topologiche sfavorevoli. Di conseguenza, un collegamento tra loro sarebbe quindi impegnativo nel caso di un collegamento a due switch.	I 2 dispositivi sono disposti in posizioni topologiche favorevoli. L'installazione di una linea di controllo richiederebbe un grande sforzo.	I 2 dispositivi sono disposti in posizioni topologiche favorevoli. L'installazione di una linea di controllo non richiederebbe un grande sforzo.
Svantaggio	Se lo Switch configurato per il collegamento ridondante diventa inutilizzabile, non vi è più alcun collegamento tra le reti.	Maggior sforzo per il collegamento di 2 dispositivi alla rete (rispetto al collegamento a uno switch).	Maggior sforzo per il collegamento di due dispositivi alla rete (rispetto al collegamento a uno switch e a due switch).
Vantaggio	Minor sforzo necessario per il collegamento di 2 dispositivi alla rete (rispetto al collegamento a due switch).	Quando uno dei dispositivi configurati per il collegamento ridondante diviene inutilizzabile, le reti collegate sono ancora connesse.	Quando uno dei dispositivi configurati per il collegamento ridondante diviene inutilizzabile, le reti collegate sono ancora connesse. Il rilevamento del partner tra i dispositivi di collegamento avviene in modo più rapido e sicuro che senza la linea di controllo.

13.12.2 Preparare il Ring/Network Coupling

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per aiutare a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della configurazione *Ring/Network Coupling*. Prima di connettere le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione ad anello.

Per contribuire a evitare loop, utilizzare la funzione *Ring/Network Coupling* solo sulle porte in cui il Rapid Spanning Tree Protocol non è attivo.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Attraverso le immagini nella finestra di dialogo si definisce il ruolo dei dispositivi all'interno del *Ring/Network Coupling*.

Negli screenshot e nei diagrammi seguenti sono utilizzate le seguenti convenzioni:
- Le linee e le caselle blu indicano i dispositivi o i collegamenti delle voci attualmente in fase di descrizione.
- Le linee fisse indicano un collegamento principale.
- Le linee tratteggiate indicano un collegamento stand-by.
- Le linee punteggiate indicano la linea di controllo.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Nel riquadro *Mode*, elenco opzioni *Type*, selezionare il pulsante di opzioni richiesto.
  - *one-switch coupling*
  - *two-switch coupling, master*
  - *two-switch coupling, slave*
  - *two-switch coupling with control line, master*
  - *two-switch coupling with control line, slave*

Collegamento a uno switch

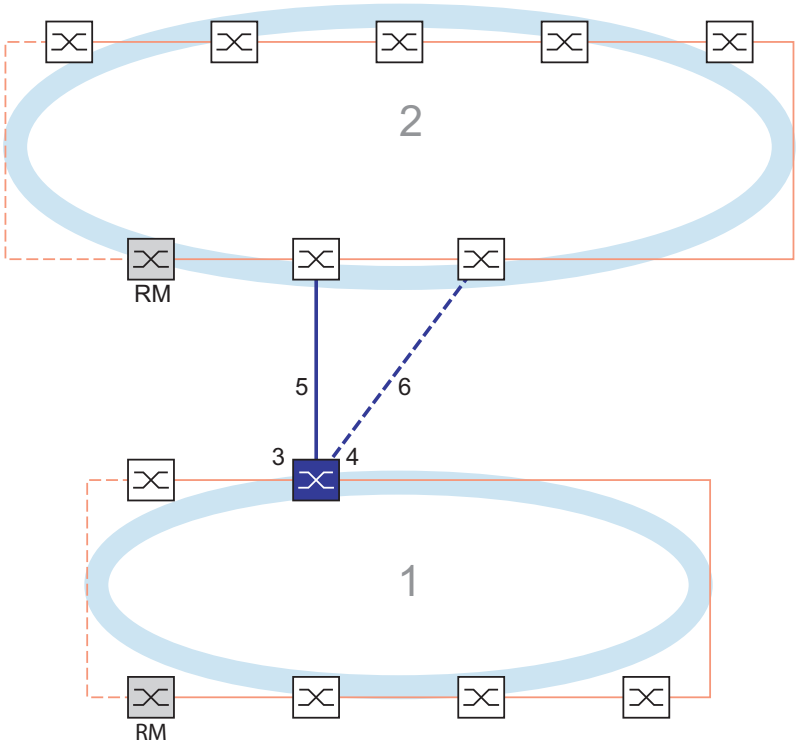


Figura 56: Esempio di collegamento a uno switch
1: Anello
2: Backbone
3: Porta di collegamento partner
4: Porta di collegamento
5: Linea principale
6: Linea ridondante

La linea principale, indicata dalla linea blu fissa collegata alla porta di collegamento partner, fornisce collegamento tra le due reti nel modo operativo normale. Se la linea principale è inutilizzabile, la linea ridondante indicata dalla linea blu tratteggiata, collegata alla porta di collegamento, subentra nel collegamento dell'anello/rete. **Uno** switch esegue la commutazione del collegamento.

Le seguenti impostazioni si applicano al dispositivo visualizzato in blu nella grafica selezionata.

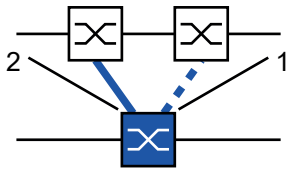


Figura 57: Collegamento a uno switch
1: Porta di collegamento
2: Porta di collegamento partner

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Nel riquadro *Mode*, elenco opzioni *Type*, selezionare il pulsante di opzione *one-switch coupling*.

Nota: Configurare la *Partner coupling port* e le Ring port su porte diverse.

- ☐ Nel riquadro *Coupling port*, selezionare la porta a cui si collega la linea ridondante nell'elenco a discesa *Port*.
- ☐ Nel riquadro *Partner coupling port*, selezionare la porta a cui si collega la linea principale nell'elenco a discesa *Port*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.
- ☐ Collegare la linea ridondante alla porta di collegamento partner.
  Nel riquadro *Partner coupling port*, il campo *State* mostra lo stato della porta di collegamento partner.
- ☐ Collegare la linea principale alla porta di collegamento.
  Nel riquadro *Coupling port*, il campo *State* mostra lo stato della porta di collegamento.

Nel riquadro *Information*, il campo *Redundancy available* mostra se la ridondanza è disponibile. Il campo *Configuration failure* mostra se le impostazioni sono complete e corrette.

Per le porte di collegamento eseguire i seguenti passaggi:

Nota: Le seguenti impostazioni sono necessarie per le porte di collegamento.

- ☐ Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
- ☐ Per le porte selezionate come porte di collegamento, specificare le impostazioni in base ai parametri nella seguente tabella.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

Tabella 40:Impostazioni della porta per Ring port

Tipo di porta	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
TX	1 Gbit/s	selezionato	selezionato	–
Ottico	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
Ottico	1 Gbit/s	selezionato	selezionato	–
Ottico	2.5 Gbit/s	selezionato	–	*2.5 Gbit/s FDX*

Se sono state configurate delle VLAN sulle porte di collegamento, specificare le impostazioni della VLAN sulle porte di collegamento e di collegamento partner. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Modificare l'impostazione *Port-VLAN ID* con il valore dell'ID VLAN configurato sulle porte.
- ☐ Deselezionare la casella di spunta *Ingress filtering* per entrambe le porte di collegamento.
- ☐ Aprire la finestra di dialogo *Switching > VLAN > Configuration*.
- ☐ Per taggare i collegamenti ridondanti per `VLAN 1` e l'appartenenza alla VLAN, immettere il valore `T` nelle celle corrispondenti a entrambe le porte di collegamento sulla riga `VLAN 1`.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

I dispositivi di collegamento inviano i pacchetti di ridondanza con la massima priorità sulla `VLAN 1`.

- ☐ Nel riquadro *Configuration*, elenco opzioni *Redundancy mode*, specificare il tipo di ridondanza:
  - ▶ Con l'impostazione *redundant ring/network coupling*, la linea principale o la linea ridondante è attiva. L'impostazione consente ai dispositivi di passare da una linea all'altra.
  - ▶ Quando si attiva l'impostazione *extended redundancy*, la linea principale e la linea ridondante sono attive contemporaneamente. Questa impostazione consente di aggiungere ridondanza alla rete di collegamento. Quando il collegamento tra i dispositivi di collegamento nella seconda rete diviene inutilizzabile, i dispositivi di collegamento continuano a trasmettere e ricevere dati.

Nota: Durante l'intervallo di riconfigurazione si possono verificare duplicazioni di pacchetti. Di conseguenza, se i dispositivi rilevano duplicazioni di pacchetti, selezionare questa impostazione.

La *Coupling mode* descrive il tipo di rete backbone a cui si collega la rete ad anello (vedi figura 56).

- ☐ Nel riquadro *Configuration*, elenco opzioni *Coupling mode*, specificare il tipo della seconda rete:
  - ☐ Se si esegue il collegamento a una rete ad anello, selezionare il pulsante di opzione *ring coupling*.
  - ☐ Se si esegue il collegamento a una struttura a maglia o bus, selezionare il pulsante di opzione *network coupling*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Ripristinare le impostazioni di collegamento allo stato di default. A tale scopo, eseguire i seguenti passaggi:

- ☐ Fare clic sul pulsante ☰ e poi sulla voce *Reset*.

Collegamento a due switch

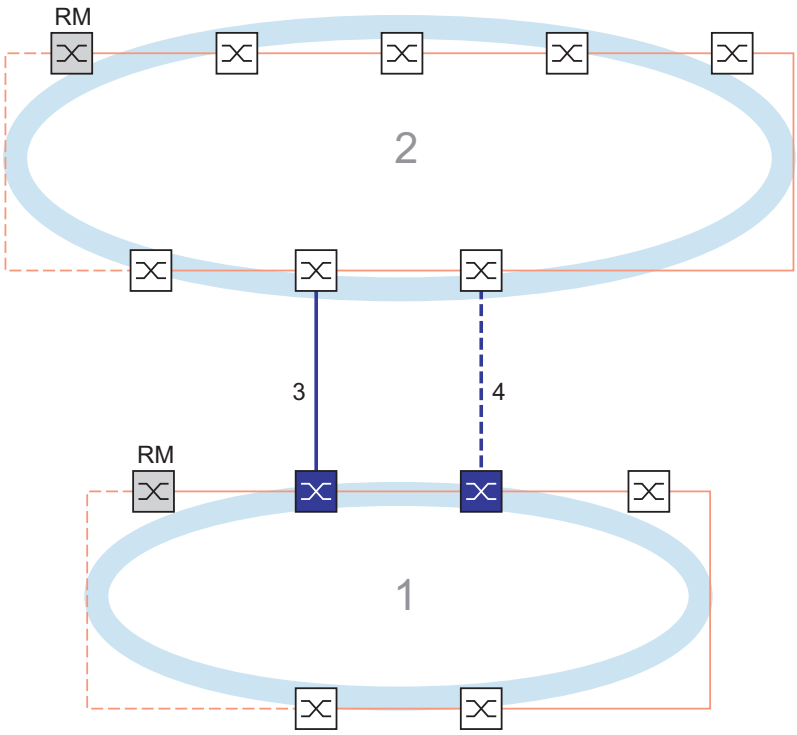


Figura 58: Esempio di collegamento a due switch
1: Anello
2: Backbone
3: Linea principale
4: Linea ridondante

Il collegamento tra 2 reti è eseguito dalla linea principale, indicata da una linea blu fissa. Se la linea principale o uno dei dispositivi adiacenti diviene inutilizzabile, la linea ridondante, indicata dalla linea nera tratteggiata, subentra nel collegamento di rete. Il collegamento è eseguito da 2 dispositivi.

I dispositivi si inviano pacchetti di controllo tra loro attraverso l'Ethernet.

Il dispositivo primario collegato alla linea principale, e il dispositivo stand-by collegato alla linea ridondante sono partner per quanto riguarda il collegamento.
☐ Collegare i 2 partner tramite le Ring port.

Collegamento a due switch, dispositivo primario

Le seguenti impostazioni si applicano al dispositivo visualizzato in blu nella grafica selezionata.

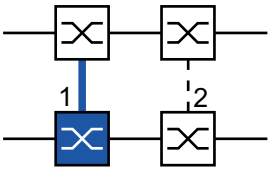


Figura 59: Collegamento a due switch, dispositivo primario
1: Porta di collegamento
2: Porta di collegamento partner

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Nel riquadro *Mode*, elenco opzioni *Type*, selezionare il pulsante di opzione *two-switch coupling, master*.
- ☐ Nel riquadro *Coupling port*, selezionare la porta a cui si collegano i segmenti di rete nell'elenco a discesa *Port*.
  Configurare la *Coupling port* e le Ring port su porte diverse.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.
- ☐ Collegare la linea principale alla *Coupling port*.
  Nel riquadro *Coupling port*, il campo *State* mostra lo stato della porta di collegamento.
  Quando il partner sta già operando nella rete, il campo *IP address* nel riquadro *Partner coupling port* mostra l'indirizzo IP della porta partner.

Nel riquadro *Information*, il campo *Redundancy available* mostra se la ridondanza è disponibile. Il campo *Configuration failure* mostra se le impostazioni sono complete e corrette.

Nota: Se si utilizza la funzione *Ring manager* e una funzione di collegamento a due switch sullo stesso dispositivo, è possibile creare un loop.

Per contribuire a prevenire la formazione di loop continui mentre i collegamenti sono attivi sulle porte di collegamento all'anello, eseguire una delle seguenti azioni. Il dispositivo imposta lo stato della porta di collegamento su “spento”:
- disabilitare il funzionamento
- modificare la configurazione

Per le porte di collegamento eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
- ☐ Per le porte selezionate come porte di collegamento, specificare le impostazioni in base ai parametri nella seguente tabella.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Tabella 41:Impostazioni della porta per Ring port

Tipo di porta	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
TX	1 Gbit/s	selezionato	selezionato	–
Ottico	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
Ottico	1 Gbit/s	selezionato	selezionato	–
Ottico	2.5 Gbit/s	selezionato	–	*2.5 Gbit/s FDX*

Se sono state configurate delle VLAN sulle porte di collegamento, specificare le impostazioni della VLAN sulle porte di collegamento e di collegamento partner. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Modificare l'impostazione *Port-VLAN ID* con il valore dell'ID VLAN configurato sulle porte.
- ☐ Deselezionare la casella di spunta *Ingress filtering* per entrambe le porte di collegamento.
- ☐ Aprire la finestra di dialogo *Switching > VLAN > Configuration*.
- ☐ Per taggare i collegamenti ridondanti per `VLAN 1` e l'appartenenza alla VLAN, immettere il valore `T` nelle celle corrispondenti a entrambe le porte di collegamento sulla riga `VLAN 1`.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

I dispositivi di collegamento inviano i pacchetti di ridondanza con la massima priorità sulla `VLAN 1`.

Collegamento a due switch, dispositivo stand-by

Le seguenti impostazioni si applicano al dispositivo visualizzato in blu nella grafica selezionata.

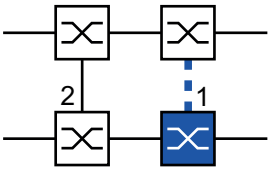


Figura 60: Collegamento a due switch, dispositivo stand-by
1: Porta di collegamento
2: Porta di collegamento partner

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Nel riquadro *Mode*, elenco opzioni *Type*, selezionare il pulsante di opzione *two-switch coupling, slave*.
- ☐ Nel riquadro *Coupling port*, selezionare la porta a cui si collegano i segmenti di rete nell'elenco a discesa *Port*.
  Configurare la *Coupling port* e le Ring port su porte diverse.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.

- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.
- ☐ Collegare la linea ridondante alla *Coupling port*.
  Nel riquadro *Coupling port*, il campo *State* mostra lo stato della porta di collegamento. Quando il partner sta già operando nella rete, il campo *IP address* nel riquadro *Partner coupling port* mostra l'indirizzo IP della porta partner.

Nel riquadro *Information*, il campo *Redundancy available* mostra se la ridondanza è disponibile. Il campo *Configuration failure* mostra se le impostazioni sono complete e corrette.

Nota: Se si utilizza la funzione *Ring manager* e una funzione di collegamento a due switch sullo stesso dispositivo, è possibile creare un loop.

Per contribuire a prevenire la formazione di loop continui mentre i collegamenti sono attivi sulle porte di collegamento all'anello, eseguire una delle seguenti azioni. Il dispositivo imposta lo stato della porta di collegamento su “spento”:

- disabilitare il funzionamento
- modificare la configurazione

Per le porte di collegamento eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
- ☐ Per le porte selezionate come porte di collegamento, specificare le impostazioni in base ai parametri nella seguente tabella.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

Tabella 42:Impostazioni della porta per Ring port

Tipo di porta	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
TX	1 Gbit/s	selezionato	selezionato	–
Ottico	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
Ottico	1 Gbit/s	selezionato	selezionato	–
Ottico	2.5 Gbit/s	selezionato	–	*2.5 Gbit/s FDX*

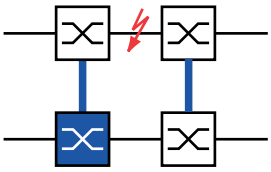
Se sono state configurate delle VLAN sulle porte di collegamento, specificare le impostazioni della VLAN sulle porte di collegamento e di collegamento partner. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Modificare l'impostazione *Port-VLAN ID* con il valore dell'ID VLAN configurato sulle porte.
- ☐ Deselezionare la casella di spunta *Ingress filtering* per entrambe le porte di collegamento.
- ☐ Aprire la finestra di dialogo *Switching > VLAN > Configuration*.
- ☐ Per taggare i collegamenti ridondanti per `VLAN 1` e l'appartenenza alla VLAN, immettere il valore `T` nelle celle corrispondenti a entrambe le porte di collegamento sulla riga `VLAN 1`.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

I dispositivi di collegamento inviano i pacchetti di ridondanza con la massima priorità sulla `VLAN 1`.

Specificare le impostazioni *Redundancy mode* e *Coupling mode*. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Nel riquadro *Configuration*, elenco opzioni *Redundancy mode*, selezionare uno dei seguenti pulsanti di opzione:
  - ▶ `redundant ring/network coupling`
    Con questa impostazione, la linea principale o la linea ridondante è attiva. L'impostazione consente ai dispositivi di passare da una linea all'altra.
  - ▶ `extended redundancy`
    Con questa impostazione, la linea principale e la linea ridondante sono attive contemporaneamente. L'impostazione consente di aggiungere ridondanza alla seconda rete. Quando il collegamento tra i dispositivi di collegamento nella seconda rete diviene inutilizzabile, i dispositivi di collegamento continuano a trasmettere e ricevere dati.

    Durante l'intervallo di riconfigurazione si possono verificare duplicazioni di pacchetti. Di conseguenza, selezionare questa impostazione solo se i dispositivi rilevano duplicazioni di pacchetti.
- ☐ Nel riquadro *Configuration*, elenco opzioni *Coupling mode*, selezionare uno dei seguenti pulsanti di opzione:
  - ☐ Se si esegue il collegamento a una rete ad anello, selezionare il pulsante di opzione *ring coupling*.
  - ☐ Se si esegue il collegamento a una struttura a maglia o bus, selezionare il pulsante di opzione *network coupling*.

  La *Coupling mode* descrive il tipo di rete backbone a cui si collega la rete ad anello (vedi figura 58).
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

Ripristinare le impostazioni di collegamento allo stato di default. A tale scopo, eseguire i seguenti passaggi:

- ☐ Fare clic sul pulsante e poi sulla voce *Reset*.

Collegamento a due switch con linea di controllo

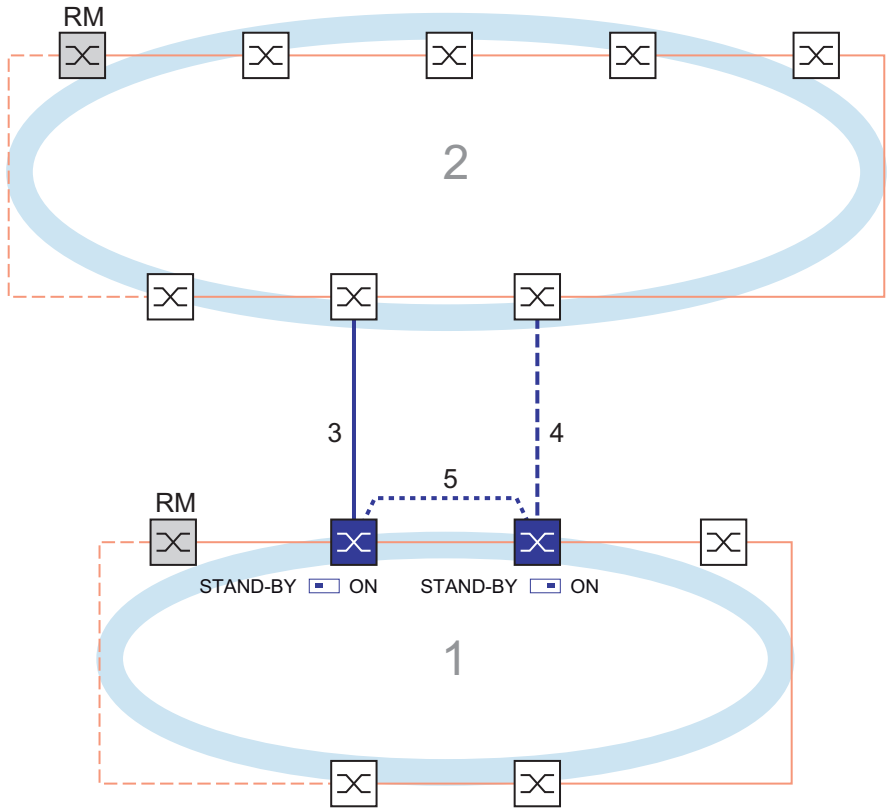


Figura 61: Esempio di collegamento a due switch con linea di controllo
1: Anello
2: Backbone
3: Linea principale
4: Linea ridondante
5: Linea di controllo

Il collegamento tra 2 reti è eseguito dalla linea principale, indicata da una linea blu fissa. Se la linea principale o uno dei dispositivi adiacenti diviene inutilizzabile, la linea ridondante, indicata dalla linea blu tratteggiata, subentra nel collegamento di 2 reti. Il collegamento di rete è eseguito da 2 dispositivi.

I dispositivi inviano pacchetti di controllo lungo una linea di controllo indicata dalla linea blu punteggiata nella figura di seguito (vedi figura 62).

Il dispositivo primario collegato alla linea principale, e il dispositivo stand-by collegato alla linea ridondante sono partner per quanto riguarda il collegamento.
☐ Collegare i 2 partner tramite le Ring port.

Collegamento a due switch con linea di controllo, dispositivo primario

Le seguenti impostazioni si applicano al dispositivo visualizzato in blu nella grafica selezionata.

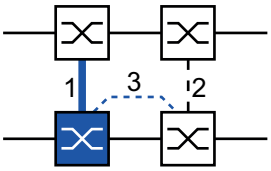


Figura 62: Collegamento a due switch con linea di controllo, dispositivo primario
1: Porta di collegamento
2: Porta di collegamento partner
3: Linea di controllo

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Nel riquadro *Mode*, elenco opzioni *Type*, selezionare il pulsante di opzione `two-switch coupling with control line, master`.
- ☐ Nel riquadro *Coupling port*, selezionare la porta a cui si collegano i segmenti di rete nell'elenco a discesa *Port*.
  Configurare la *Coupling port* e le Ring port su porte diverse.
- ☐ Nel riquadro *Control port*, selezionare la porta a cui si collega la linea di controllo nell'elenco a discesa *Port*.
  Configurare la *Coupling port* e le Ring port su porte diverse.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .
- ☐ Collegare la linea ridondante alla porta di collegamento.
  Nel riquadro *Coupling port*, il campo *State* mostra lo stato della porta di collegamento.
  Quando il partner sta già operando nella rete, il campo *IP address* nel riquadro *Partner coupling port* mostra l'indirizzo IP della porta partner.
- ☐ Collegare la linea di controllo alla porta di controllo.
  Nel riquadro *Control port*, il campo *State* mostra lo stato della porta di controllo.
  Quando il partner sta già operando nella rete, il campo *IP address* nel riquadro *Partner coupling port* mostra l'indirizzo IP della porta partner.

Nel riquadro *Information*, il campo *Redundancy available* mostra se la ridondanza è disponibile. Il campo *Configuration failure* mostra se le impostazioni sono complete e corrette.

Nota: Se si utilizza la funzione *Ring manager* e una funzione di collegamento a due switch sullo stesso dispositivo, è possibile creare un loop.

Per contribuire a prevenire la formazione di loop continui mentre i collegamenti sono attivi sulle porte di collegamento all'anello, eseguire una delle seguenti azioni. Il dispositivo imposta lo stato della porta di collegamento su “spento”:
- disabilitare il funzionamento
- modificare la configurazione

Per le porte di collegamento eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
- ☐ Per le porte selezionate come porte di collegamento, specificare le impostazioni in base ai parametri nella seguente tabella.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Tabella 43:Impostazioni della porta per Ring port

Tipo di porta	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
TX	1 Gbit/s	selezionato	selezionato	–
Ottico	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
Ottico	1 Gbit/s	selezionato	selezionato	–
Ottico	2.5 Gbit/s	selezionato	–	*2.5 Gbit/s FDX*

Se sono state configurate delle VLAN sulle porte di collegamento, specificare le impostazioni della VLAN sulle porte di collegamento e di collegamento partner. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Modificare l'impostazione *Port-VLAN ID* con il valore dell'ID VLAN configurato sulle porte.
- ☐ Deselezionare la casella di spunta *Ingress filtering* per entrambe le porte di collegamento.
- ☐ Aprire la finestra di dialogo *Switching > VLAN > Configuration*.
- ☐ Per taggare i collegamenti ridondanti per `VLAN 1` e l'appartenenza alla VLAN, immettere il valore `T` nelle celle corrispondenti a entrambe le porte di collegamento sulla riga `VLAN 1`.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

I dispositivi di collegamento inviano i pacchetti di ridondanza con la massima priorità sulla `VLAN 1`.

Collegamento a due switch con linea di controllo, dispositivo stand-by

Le seguenti impostazioni si applicano al dispositivo visualizzato in blu nella grafica selezionata.

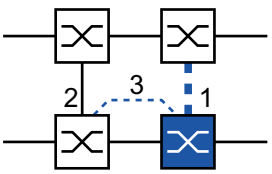


Figura 63: Collegamento a due switch con linea di controllo, dispositivo stand-by
1: Porta di collegamento
2: Porta di collegamento partner
3: Linea di controllo

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Nel riquadro *Mode*, elenco opzioni *Type*, selezionare il pulsante di opzione *two-switch coupling with control line, slave*.
- ☐ Nel riquadro *Coupling port*, selezionare la porta a cui si collegano i segmenti di rete nell'elenco a discesa *Port*.
  Configurare la *Coupling port* e le Ring port su porte diverse.
- ☐ Nel riquadro *Control port*, selezionare la porta a cui si collega la linea di controllo nell'elenco a discesa *Port*.
  Configurare la *Coupling port* e le Ring port su porte diverse.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.
- ☐ Collegare la linea ridondante alla porta di collegamento.
  Nel riquadro *Coupling port*, il campo *State* mostra lo stato della porta di collegamento.
  Quando il partner sta già operando nella rete, il campo *IP address* nel riquadro *Partner coupling port* mostra l'indirizzo IP della porta partner.
- ☐ Collegare la linea di controllo alla porta di controllo.
  Nel riquadro *Control port*, il campo *State* mostra lo stato della porta di controllo.
  Quando il partner sta già operando nella rete, il campo *IP address* nel riquadro *Partner coupling port* mostra l'indirizzo IP della porta partner.

Nel riquadro *Information*, il campo *Redundancy available* mostra se la ridondanza è disponibile. Il campo *Configuration failure* mostra se le impostazioni sono complete e corrette.

Nota: Se si utilizza la funzione *Ring manager* e una funzione di collegamento a due switch sullo stesso dispositivo, è possibile creare un loop.

Per contribuire a prevenire la formazione di loop continui mentre i collegamenti sono attivi sulle porte di collegamento all'anello, eseguire una delle seguenti azioni. Il dispositivo imposta lo stato della porta di collegamento su “spento”:

- disabilitare il funzionamento
- modificare la configurazione

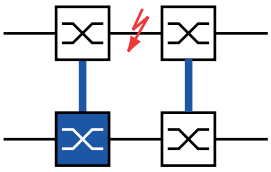
Per le porte di collegamento eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > VLAN > Port*.
- ☐ Modificare l'impostazione *Port-VLAN ID* con il valore dell'ID VLAN configurato sulle porte.
- ☐ Deselezionare la casella di spunta *Ingress filtering* per entrambe le porte di collegamento.
- ☐ Aprire la finestra di dialogo *Switching > VLAN > Configuration*.
- ☐ Per taggare i collegamenti ridondanti per `VLAN 1` e l'appartenenza alla VLAN, immettere il valore `T` nelle celle corrispondenti a entrambe le porte di collegamento sulla riga `VLAN 1`.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

I dispositivi di collegamento inviano i pacchetti di ridondanza con la massima priorità sulla `VLAN 1`.

Specificare le impostazioni *Redundancy mode* e *Coupling mode*. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Nel riquadro *Configuration*, elenco opzioni *Redundancy mode*, selezionare uno dei seguenti pulsanti di opzione:
  - ▶ `redundant ring/network coupling`
    Con questa impostazione, la linea principale o la linea ridondante è attiva. L'impostazione consente ai dispositivi di passare da una linea all'altra.
  - ▶ `extended redundancy`
    Con questa impostazione, la linea principale e la linea ridondante sono attive contemporaneamente. L'impostazione consente di aggiungere ridondanza alla seconda rete. Quando il collegamento tra i dispositivi di collegamento nella seconda rete diviene inutilizzabile, i dispositivi di collegamento continuano a trasmettere e ricevere dati.

    Durante l'intervallo di riconfigurazione si possono verificare duplicazioni di pacchetti. Di conseguenza, selezionare questa impostazione solo se i dispositivi rilevano duplicazioni di pacchetti.
- ☐ Nel riquadro *Configuration*, elenco opzioni *Coupling mode*, selezionare uno dei seguenti pulsanti di opzione:
  - ☐ Se si esegue il collegamento a una rete ad anello, selezionare il pulsante di opzione *ring coupling*.
  - ☐ Se si esegue il collegamento a una struttura a maglia o bus, selezionare il pulsante di opzione *network coupling*.

  La *Coupling mode* descrive il tipo di rete backbone a cui si collega la rete ad anello (vedi figura 61).
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Ripristinare le impostazioni di collegamento allo stato di default. A tale scopo, eseguire i seguenti passaggi:

- ☐ Fare clic sul pulsante ☰ e poi sulla voce *Reset*.

13.13 RCP

Le applicazioni industriali richiedono una grande disponibilità delle reti. Ciò implica inoltre tempi di interruzione brevi e deterministici per la comunicazione qualora un dispositivo di rete diventi inutilizzabile.

Una topologia ad anello offre tempi di transizione ridotti con un impiego minimo di risorse. Tuttavia, la topologia ad anello comporta la sfida di collegare questi anelli tra loro in modo ridondante.

Il Redundant Coupling Protocol *RCP* consente di collegare gli anelli che funzionano con uno dei seguenti protocolli di ridondanza:
- MRP
- HIPER ring
- RSTP

La funzione *RCP* consente inoltre di collegare più anelli secondari a un anello primario (vedi figura 64). Solo gli switch che collegano gli anelli necessitano della funzione *RCP*.

È inoltre possibile utilizzare dispositivi diversi dai dispositivi Schneider Electric presenti nelle reti collegate.

La funzione *RCP* si avvale di un dispositivo master e di un dispositivo slave per trasferire dati tra le reti. Solo il dispositivo master inoltra frame tra gli anelli.

Utilizzando messaggi multicast proprietari Schneider Electric, i dispositivi *RCP* master e slave si informano reciprocamente sul loro modo operativo. All'interno dell'anello, configurare i dispositivi diversi dai dispositivi di collegamento per inoltrare i seguenti indirizzi multicast.
- `01:80:63:07:00:09`
- `01:80:63:07:00:0A`

Collegare i dispositivi master e slave come vicini diretti.

Si utilizzano 4 porte per dispositivo per creare collegamenti ridondanti. Installare i dispositivi di collegamento con 2 porte interne e 2 porte esterne in ciascuna rete.

- La porta interna collega i dispositivi master e slave tra loro.
- La porta esterna collega i dispositivi alla rete.

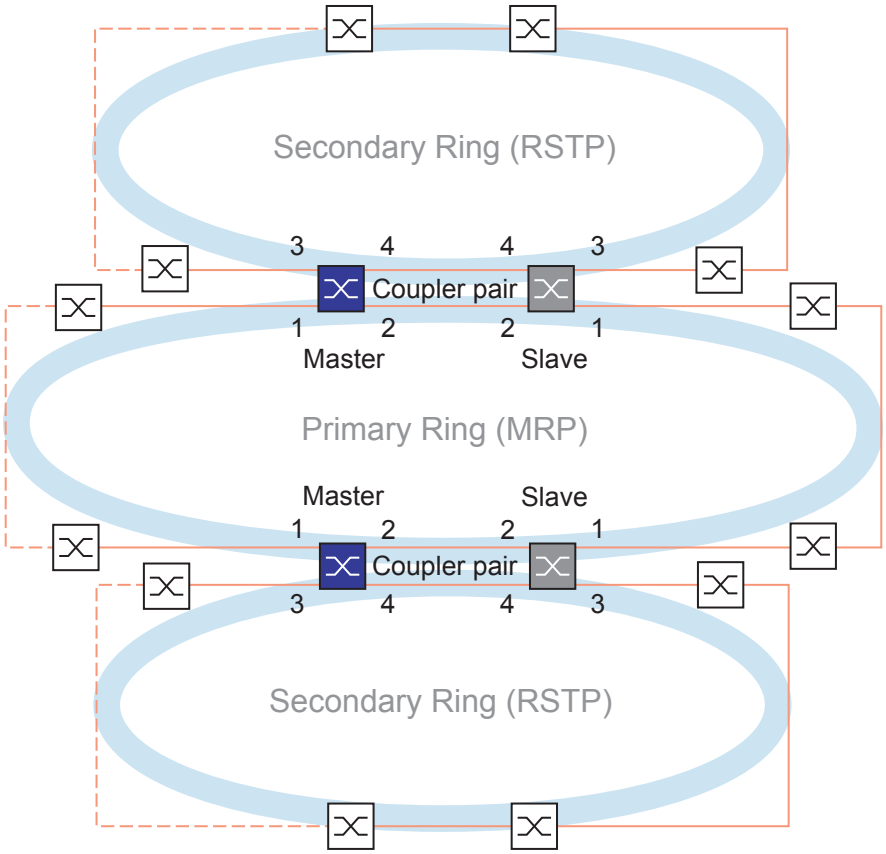


Figura 64: Esempio di collegamento ridondante a due switch
1: Porta di collegamento esterna nell'anello primario
2: Porta di collegamento interna nell'anello primario
3: Porta di collegamento esterna nell'anello secondario
4: Porta di collegamento interna nell'anello secondario

Quando il ruolo è impostato sul valore *auto*, i dispositivi coupler selezionano automaticamente il loro ruolo come *master* o *slave*. Quando si desidera un dispositivo master o slave permanente, configurare i ruoli manualmente.

Nota: Il ruolo `single` è utilizzato solamente insieme alla funzione *Dual RSTP*. Vedi “Collegamento di 2 ring RSTP tramite la funzione Dual RSTP” a pagina 254.

Se il master non è più raggiungibile tramite le porte di collegamento interne, il dispositivo slave attende la scadenza del periodo di timeout prima di assumere il ruolo di master. Durante il periodo di timeout specificato, lo slave tenta di raggiungere il master tramite le porte di collegamento esterne. Quando il master non è raggiungibile, lo slave assume il ruolo di master. Per mantenere la stabilità nella rete collegata alle porte di collegamento esterne, configurare il periodo di timeout per una durata superiore al tempo di ripristino negli anelli collegati.

Nota: Disabilitare l'RSTP sulle porte interne ed esterne di collegamento ridondante *RCP* non collegate all'anello RSTP. Nella configurazione esemplificativa, si disabilita il RSTP sulle porte `1` e `2` di tutti i dispositivi.

13.13.1 Esempio di applicazione per il collegamento RCP

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per aiutare a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della configurazione *RCP*. Prima di connettere le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione ad anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

I Schneider Electric dispositivi supportano i due metodi di switch Redundant Coupling Protocol. Si può utilizzare la funzione *RCP* per fornire una rete installata in un treno, per esempio. La rete fornisce ai passeggeri informazioni relative alla posizione del treno o alle diverse fermate sulla linea. Inoltre, la rete può inoltre fornire ai passeggeri sicurezza, per esempio utilizzando la videosorveglianza.

Gli anelli primari nella figura rappresentano una rete ad anello *MRP* all'interno di una macchina. Gli anelli secondari nella figura sono reti ad anello RSTP. Ciascun anello contiene 4 dispositivi (vedi figura 65).

Per semplificare la topologia del treno nella figura, le Ring port *MRP* e le porte interne ed esterne *RCP* sono assegnate agli stessi numeri di porta. Specificare gli stessi valori per i parametri delle porte in conformità alla loro funzione nella rete. Per esempio, specificare le porte *1/1* e *1/2* sullo Switch 1D e 1C come Ring port MRP. La porta *1/4* come porta interna *RCP*, e la porta *1/3* come porta esterna *RCP*.

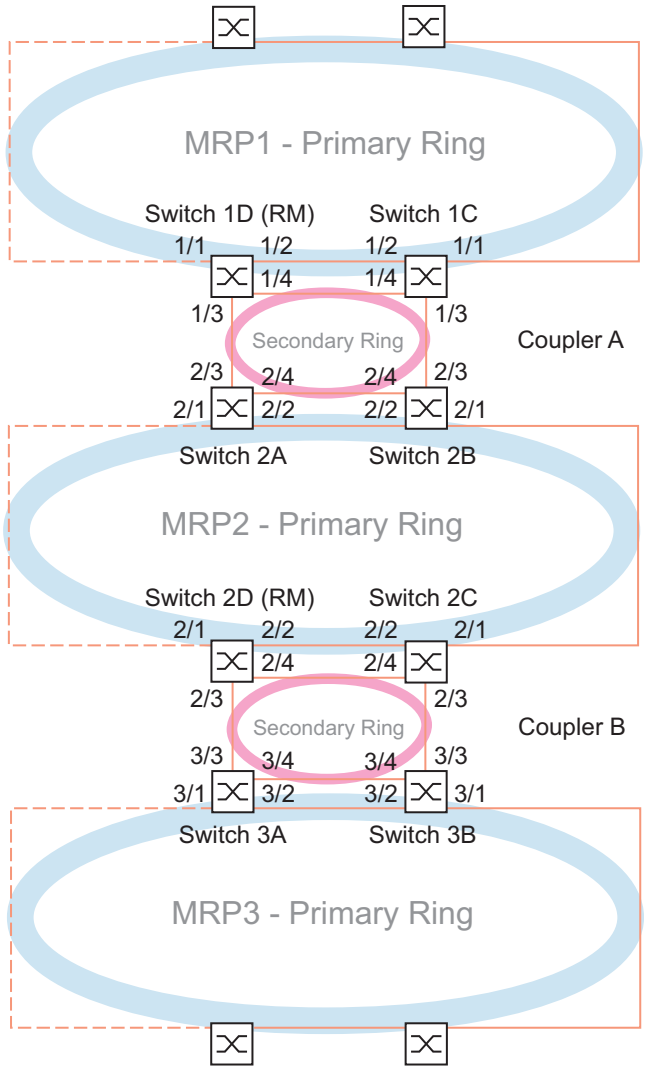


Figura 65: Topologia del treno Redundant coupling protocol

Il seguente elenco specifica i ruoli delle porte su ciascun dispositivo.
1: le porte 1 e 2 sono MRPporte ring
2: la porta 3 è una RCPporta esterna
3: la porta 4 è una porta interna RCP.

I seguenti passaggi descrivono come specificare i parametri per lo Switch 1D in Coupler A. Configurare gli altri dispositivi utilizzati per il Coupler A e i dispositivi utilizzati per il Coupler B nello stesso modo.

Disabilitare la funzione RSTP nell'MRP Ring

L'*MRP* e l'RSTP non lavorano insieme. Di conseguenza, disattivare la funzione RSTP sulle porte *RCP* utilizzate nell'*MRP* ring. Nella configurazione esemplificativa, le porte `x/1` e `x/2` sono utilizzate per l'*MRP* ring. Attivare la funzione RSTP solo sulle porte interne ed esterne *RCP* utilizzate nell'anello secondario. Per esempio, attivare la funzione RSTP sulle porte `x/3` e `x/4`.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, scheda *CIST*.
- ☐ Nelle impostazioni di default, la funzione RSTP è attiva sulle porte. Per disattivare la funzione RSTP sulle Ring port *MRP*, deselezionare le caselle di spunta *STP active* per le porte `x/1` e `x/2`.
- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface x/1`	Passare alla modalità di configurazione di interfaccia `x/1`.
`no spanning-tree mode`	Disabilitare la funzione *Spanning Tree* sulla porta.
`exit`	Passare alla modalità di configurazione.
`interface x/2`	Passare alla modalità di configurazione di interfaccia `x/2`.
`no spanning-tree mode`	Disabilitare la funzione *Spanning Tree* sulla porta.
`exit`	Passare alla modalità di configurazione.
`spanning-tree operation`	Abilitare la funzione *Spanning Tree*.

Specificare il Ring Master nell'MRP ring.

Nella figura, lo Switch D di ciascun *MRP* ring è designato come ring manager (vedi figura 65). Specificare gli altri switch negli anelli come client ring.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > MRP*.
- ☐ Specificare la prima Ring port nel frame *Ring port 1*.
  Nell'elenco a discesa *Port*, selezionare la porta `x/1`.
- ☐ Specificare la seconda Ring port nel frame *Ring port 2*.
  Nell'elenco a discesa *Port*, selezionare la porta `x/2`.
- ☐ Per designare il dispositivo come Ring Manager, attivare la funzione nel frame *Ring manager*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`mrp domain add default-domain`	Creare un nuovo dominio *MRP* con l'ID `default-domain`.
`mrp domain modify port primary x/1`	Specificare la porta `x/1` come Ring port `1`.
`mrp domain modify port secondary x/2`	Specificare la porta `x/2` come Ring port `2`.
`mrp domain modify mode manager`	Specificare il funzionamento del dispositivo come *Ring manager*. Per gli altri dispositivi nell'anello, lasciare le impostazioni di default.
`mrp domain modify operation enable`	Abilitare la funzione *MRP*.

Specificare i dispositivi nel coupler ridondante

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > RCP*.
- ☐ Specificare l'*Inner port* nel frame *Primary ring/network*.
  Selezionare la porta `x/2`.
- ☐ Specificare l'*Outer port* nel frame *Primary ring/network*.
  Selezionare la porta `x/1`.
- ☐ Specificare l'*Inner port* nel frame *Secondary ring/network*.
  Selezionare la porta `x/4`.
- ☐ Specificare l'*Outer port* nel frame *Secondary ring/network*.
  Selezionare la porta `x/3`.

- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`redundant-coupling port primary inner x/2`	Specificare la porta `x/2` come porta interna primaria.
`redundant-coupling port primary outer x/1`	Specificare la porta `x/1` come porta esterna primaria.
`redundant-coupling port secondary inner x/4`	Specificare la porta `x/4` come porta interna secondaria.
`redundant-coupling port secondary outer x/3`	Specificare la porta `x/3` come porta esterna secondaria.
`redundant-coupling operation`	Abilitare la funzione *RCP* nel dispositivo.
`copy config running-config nvm`	Salvare le impostazioni correnti nella memoria non volatile (`nvm`) all'interno del profilo di configurazione “selezionato”.

13.13.2 Collegamento di 2 ring RSTP tramite la funzione Dual RSTP

Se si desidera utilizzare l'RSTP per gli anelli primari e secondari, la funzione *RCP* assegna le porte dell'anello secondario all'istanza *Dual RSTP*. Ciò crea due reti RSTP indipendenti accoppiate da *RCP*.

È possibile utilizzare fino a 16 MCSESM-E dispositivi in un anello secondario. Questo include i 2 dispositivi dell'anello primario che collegano l'anello secondario. Quando un componente di rete diviene inutilizzabile nell'anello secondario, la funzione *RCP* può ottenere solitamente un tempo di riconfigurazione pari a 50 millisecondi.

Si possono inoltre utilizzare fino a 16 MCSESM-E dispositivi in un anello primario. In questo modo, la funzione *RCP* e la funzione *Dual RSTP* possono inoltre ottenere solitamente un tempo di riconfigurazione pari a 50 millisecondi nell'anello primario. È possibile collegare fino a 8 anelli secondari a un anello primario. In questo modo è possibile collegare fino a 128 switch (8 × 14 + 16). In questa rete è possibile ottenere di solito un tempo di riconfigurazione end-to-end pari a 50 millisecondi con ridondanza dei dispositivi.

Quando i requisiti per il tempo di riconfigurazione nell'anello primario sono inferiori, è possibile:
- Aumentare il numero di switch nell'anello primario.
- Collegare più anelli secondari all'anello primario.

È inoltre possibile utilizzare dispositivi diversi dai MCSESM-E negli anelli, ma solo nei casi in cui i dispositivi sono sufficientemente veloci nell'aggiornare le modifiche della topologia RSTP. Per esempio, quando un componente di rete diviene inutilizzabile.

Proprietà delle porte primarie e secondarie dell'istanza.

Per le porte di un'istanza primaria o secondaria, considerare le seguenti note:
- Solo quelle porte dello switch *RCP* configurate come Ring port esterne o interne dell'anello secondario appartengono all'istanza *Dual RSTP*. Le altre porte appartengono all'istanza primaria dello switch.
- È possibile collegare i dispositivi finali o le reti che non eseguono lo *Spanning Tree* a una porta che appartiene implicitamente a un'istanza primaria dello switch *RCP*.
  Queste topologie non forniscono né la ridondanza del dispositivo né la ridondanza del link.
- È possibile realizzare una rete a maglia nell'anello primario o secondario stabilendo più collegamenti tra le porte della stessa istanza.
  In queste topologie, un tempo massimo di riconfigurazione end-to-end definito di 50 millisecondi non trova applicazione.

Collegamento di 2 ring RSTP tramite un solo switch RCP

Se si desidera collegare 2 ring RSTP tramite un solo switch, utilizzare il ruolo `single`.

Per lo switch *RCP* con il ruolo `single`, le porte interne ed esterne hanno la stessa funzione. È possibile scambiare le porte interne ed esterne di un'istanza specifica.

Quando si utilizza uno switch per collegare gli anelli, è possibile collegare fino a 16 anelli secondari a un anello primario. Ciò include lo switch *RCP* che collega gli anelli. In questo modo è possibile collegare fino a 256 switch (16 × 15 + 16). In questa rete è possibile ottenere un tempo massimo di riconfigurazione end-to-end pari a 50 millisecondi in una rete con ridondanza di collegamento.

Quando i requisiti per il tempo di riconfigurazione nell'anello primario sono inferiori, è possibile:
- Aumentare il numero di switch nell'anello primario.
- Collegare più anelli secondari all'anello primario.

Possibilità di topologie per la funzione Dual RSTP

Il seguente esempio mostra la struttura di base di un anello primario collegato a 3 anelli secondari. Gli anelli secondari 1 e 2 sono collegati all'anello primario tramite 2 switch *RCP* ciascuno, e l'anello secondario 3 con 1 switch *RCP*. Si presume che i costi di percorso per ciascun collegamento in un anello siano gli stessi.

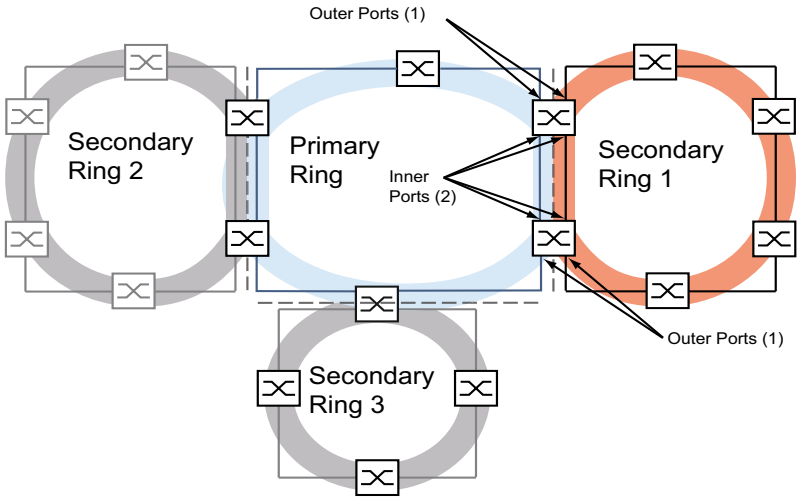


Figura 66: Anello primario con 3 anelli secondari collegati tramite RCP

Configurazione dell'anello primario

I seguenti capitoli descrivono la configurazione in linea di principio e, di conseguenza non includono passaggi operativi.

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Quando si esegue una vera configurazione, adottare misure per contribuire a evitare la formazione di loop.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Per specificare il root switch e il backup root switch nell'anello primario, configurare le loro priorità switchRSTP globali. Quando il root switch e il backup root switch sono l'uno di fronte l'altro nell'anello primario, si ottiene un tempo di riconfigurazione breve ottimale nell'anello primario. Questo è il caso in cui il backup root switch ha 2 percorsi verso il root switch, il cui numero di dispositivi al root switch si differenziano di un massimo di 1.

Configurare gli altri switch nell'anello primario, posizionati tra il root switch e il backup root switch di modo che le priorità switch si riducano (ovvero aumentino numericamente) mentre la loro distanza dal root switch aumenta.

La figura mostra un esempio con i dettagli RSTP per l'anello primario. La topologia si limita all'anello primario e a un anello secondario. Durante la configurazione, la network management station è collegata all'anello primario per contribuire a evitare interruzioni della comunicazione verso gli switch nell'anello secondario.

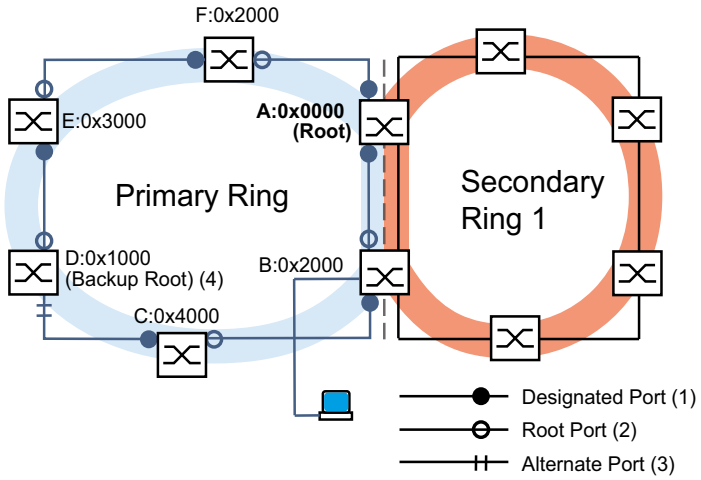


Figura 67: Anello primario con un anello secondario collegato, con dettagli per l'anello primario
A..F: identificatori dello switch
0x0000..0x4000: priorità dello switch nell'anello primario

Configurazione dell'anello secondario

Per specificare il root switch e il backup root switch nell'anello secondario, configurare la priorità switch *Dual RSTP* per gli switch *RCP*. Per gli altri switch nell'anello secondario, configurare solamente la loro priorità switchRSTP globale. Quando il root switch e il backup root switch sono l'uno di fronte l'altro nell'anello secondario, si ottiene un tempo di riconfigurazione breve ottimale nell'anello secondario.

Configurare anche gli altri switch nell'anello secondario di modo che le priorità switch diminuiscano (ovvero aumentino numericamente) mentre la loro distanza dal root switch aumenta.

La figura mostra un esempio con i dettagli RSTP per l'anello secondario.

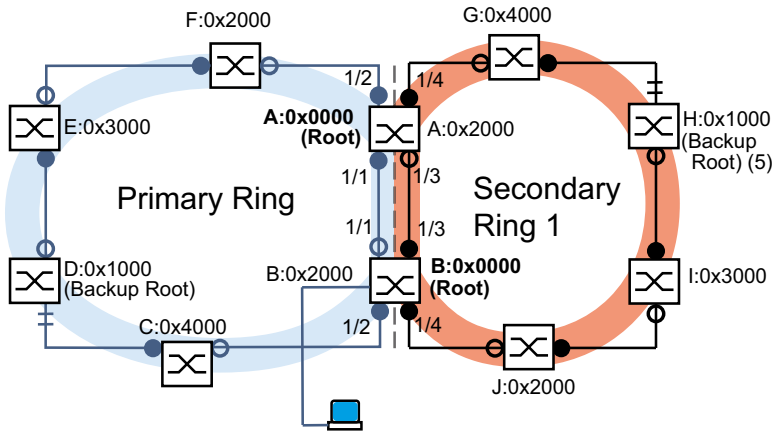


Figura 68: Anello primario con un anello secondario collegato, con dettagli per l'anello secondario
A, B, da G a J: identificatori dello switch nell'anello secondario
0x0000..0x4000: priorità switch
per gli switch A e B: Dual RSTP priorità switch
per gli switch da G a J: priorità switch RSTP globale
5: backup root switch per l'anello secondario

I ruoli del root switch nell'anello primario e nell'anello secondario sono indipendenti l'uno dall'altro. Uno switch può essere il root RSTP per:
- Entrambi gli anelli
- Un anello
- Nessun anello

Azionare l'anello secondario solamente con l'RSTP.

Configurazione del collegamento degli anelli

Per gli switch *RCP*, definire le porte interne ed esterne per gli anelli primari e secondari.

Tabella 44:Ring port per gli switch RCP

Porte	RCP master (B)	RCP slave (A)
Anello primario		
Porta interna	1/1	1/1
Porta esterna	1/2	1/2
Anello secondario		
Porta interna	1/3	1/3
Porta esterna	1/4	1/4

Dopodiché, configurare il ruolo per ciascuno switch *RCP*.

La figura mostra un esempio.

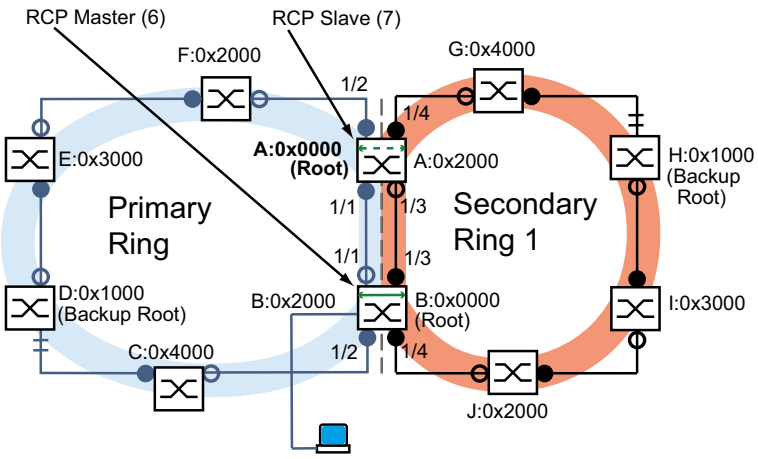


Figura 69: Anello primario con un anello secondario collegato, con numeri delle porte e RCP ruoli
6: RCP master
7: RCP slave

I ruoli del root switch e i ruoli di collegamento sono indipendenti l'uno dall'altro. Uno switch può essere *RCP* master e funzionare contemporaneamente al root RSTP per:
- Entrambi gli anelli
- Un anello
- Nessun anello

Lo stesso vale per l'*RCP* slave.

Dopodiché, abilitare la funzione *RCP*.

13.13.3 Esempio di applicazione per il collegamento RCP tramite Dual RSTP

In un capannone destinato alla produzione vi sono varie unità produttive. I dispositivi in un'unità produttiva sono collegati a una struttura di rete lineare. Questa rete è collegata alla rete di livello superiore nel capannone destinato alla produzione. La rete del capannone destinato alla produzione è interconnessa in modo ridondante e funziona con l'RSTP. Tutti i dispositivi sono di tipo MCSESM-E.

I requisiti:
- Impostare la rete lineare esistente nelle unità di produzione con una rapida ridondanza del dispositivo.
- Collegare le unità produttive in modo ridondante alla rete del capannone destinato alla produzione.
- Riconfigurare la rete del capannone destinato alla produzione di modo che aiuti a fornire tempi di riconfigurazione brevi e deterministici.

Topologia della rete esistente, limitata a una unità di produzione:

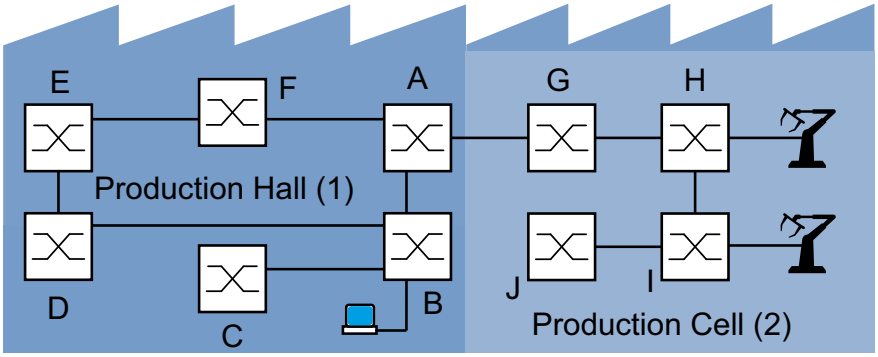


Figura 70: Esempio di un'unità produttiva in un capannone destinato alla produzione, topologia prima dell'utilizzo della funzione RCP e Dual RSTP
1: capannone destinato alla produzione
2: unità produttiva

Topologia di rete *Dual RSTP* desiderata:

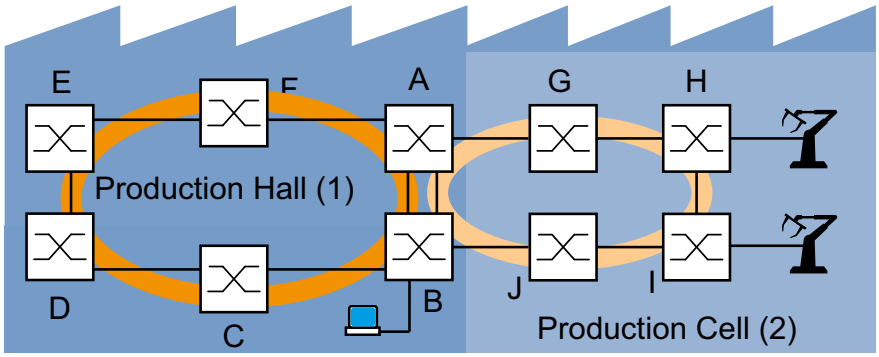


Figura 71: Esempio di un'unità produttiva in un capannone destinato alla produzione, topologia durante l'utilizzo della funzione RCP e Dual RSTP
1: capannone destinato alla produzione
2: unità produttiva

Rappresentazione schematica della topologia di rete *Dual RSTP* desiderata:

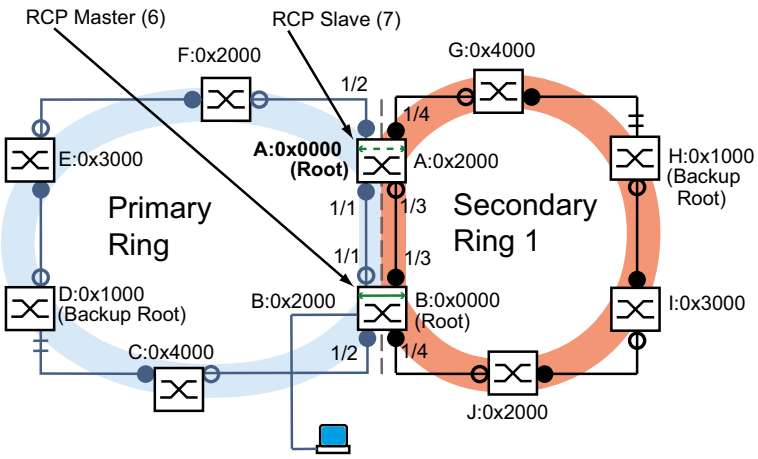


Figura 72: Rappresentazione schematica della topologia di rete Dual RSTP
6: RCP master
7: RCP slave

La tabella seguente evidenzia che un numero ridotto di impostazioni è sufficiente a configurare la nuova topologia. Si inseriscono solo le impostazioni *Dual RSTP* sui dispositivi A e B.

Tabella 45:Valori per la configurazione degli switch dell'esempio Dual RSTP

Parametro	A	B	C	D	E	F	G	H	I	J
Impostazioni RSTP										
Priorità switch (esadecimale)[1]	0x0000	0x2000	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Impostazioni Dual RSTP										
Priorità switch (esadecimali)[a]	0x2000	0x0000	-	-	-	-	-	-	-	-
Impostazioni RCP										
Anello primario, porta interna	1/1	1/1	-	-	-	-	-	-	-	-
Anello primario, porta esterna	1/2	1/2	-	-	-	-	-	-	-	-
Anello secondario, porta interna	1/3	1/3	-	-	-	-	-	-	-	-
Anello secondario, porta esterna	1/4	1/4	-	-	-	-	-	-	-	-
Ruolo di collega-mento	Slave	Master	-	-	-	-	-	-	-	-

1. Per le priorità switch espresse con valori esadecimali e decimali, vedere tabella 46.

Tabella 46:Possibili priorità switch espresse con valori esadecimali e decimali

Priorità switch								
Esadecimale	0x0000	0x1000	0x2000	0x3000	0x4000	0x5000	0x6000	0x7000
Decimale	0	4096	8192	12288	16384	20480	24576	28672

Tabella 46:Possibili priorità switch espresse con valori esadecimali e decimali

Priorità switch								
Esadecimale	0x8000	0x9000	0xA000	0xB000	0xC000	0xD000	0xE000	0xF000
Decimale	32768	36864	40960	45056	49152	53248	57344	61440

Requisiti necessari per l'ulteriore configurazione:
- Nella topologia precedente, il collegamento per l'interconnessione esistente dell'anello secondario tra gli switch B e D non è attivo. È possibile fare ciò, ad esempio, disattivando manualmente le porte corrispondenti sugli switch B e D oppure interrompendo il collegamento.
- I collegamenti tra gli switch C e D e tra gli switch J e B non sono attivi. È possibile fare ciò, per esempio disattivando manualmente le porte corrispondenti sugli switch prima di ristabilire il collegamento.
- Il collegamento per l'anello secondario tra gli switch A e B non è attivo.
- L'RSTP è attivo su tutti i dispositivi e i parametri sono in stato di fornitura.
- La network management station è collegata all'anello primario.
- È stata aperta l'interfaccia grafica utente o la Command Line Interface per i dispositivi A e B.
- È possibile accedere alle interfacce utente dei dispositivi da C a J.

⚠ AVVERTENZA

PERICOLO DI LOOP
- Configurare ciascun dispositivo della configurazione *RCP* e *Dual RSTP* individualmente. Prima di connettere le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione ad anello.
- Configurare il timeout nella configurazione di collegamento *RCP* di modo che sia più lungo della più lunga interruzione prevedibile per l'istanza più rapida del protocollo di ridondanza.
- In una topologia con 2 switch di collegamento, configurare i ruoli di collegamento di entrambi i dispositivi solo come *master*, *slave* o *auto*.
- Collegare l'istanza primaria e secondaria solo tramite 1 switch *RCP* (per una topologia con 1 switch *RCP*) o tramite 2 switch *RCP* (per una topologia con 2 switch *RCP*). Mantenere le porte dell'istanza primaria separate dalle porte di ciascuna istanza secondaria.
- Attivare le impostazioni *Admin edge port* su una porta solo nei casi in cui un dispositivo finale è connesso alla porta.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Configurazione dei parametri RSTP globali degli switch RCP

Dalle specifiche dell'attività in tabella 45, sono necessarie le priorità switch RSTP per gli switch A e B. Nella seguente tabella è riportato un riepilogo di questi valori.

Tabella 47:Priorità switch RSTP per gli switch A e B

Parametro RSTP	A	B
Priorità switch (esadecimale)	0x0000	0x2000
Priorità switch (decimale)	0	8192

Nota: Le seguenti istruzioni descrivono la configurazione degli switch *RCP* (A e B) in dettaglio; quelle degli altri switch (da C a J) solo in forma abbreviata.

Configurare il dispositivo A A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Nel riquaro *Bridge configuration*, selezionare il valore `0` dall'elenco a discesa *Priority*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`spanning-tree mst priority 0 0`	Impostare la priorità switchRSTP dell'istanza MST `0` sul valore `0`. L'istanza MST `0` è l'istanza MST globale o l'istanza di default.

Configurare il dispositivo B A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Nel riquaro *Bridge configuration*, selezionare il valore `8192` dall'elenco a discesa *Priority*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`spanning-tree mst priority 0 8192`	Impostare la priorità switchRSTP dell'istanza MST globale sul valore `8192`.

Configurazione dei parametri RSTP globali degli altri switch

Configurare ora gli altri switch. Dalle specifiche delle attività, sono necessarie le priorità switchRSTP. Nella seguente tabella è riportato un riepilogo di questi valori.

Tabella 48:Priorità switch RSTP per gli switch da C a J

Parametro RSTP	C	D	E	F	G	H	I	J
Priorità switch (esadecimale)	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Priorità switch (decimale)	16384	4096	12288	8192	16384	4096	12288	8192

Eseguire i seguenti passaggi:

- ☐ Impostare la priorità switchRSTP del dispositivo C su `16384 (0x4000)` e attivare l'impostazione.
- ☐ Impostare la priorità switchRSTP del dispositivo D su `4096 (0x1000)` e attivare l'impostazione.
- ☐ Impostare la priorità switchRSTP del dispositivo E su `12288 (0x3000)` e attivare l'impostazione.
- ☐ Impostare la priorità switchRSTP del dispositivo F su `8192 (0x2000)` e attivare l'impostazione.

- ☐ Impostare la priorità switchRSTP del dispositivo G su `16384 (0x4000)` e attivare l'impostazione.
- ☐ Impostare la priorità switchRSTP del dispositivo H su `4096 (0x1000)` e attivare l'impostazione.
- ☐ Impostare la priorità switchRSTP del dispositivo I su `12288 (0x3000)` e attivare l'impostazione.
- ☐ Impostare la priorità switchRSTP del dispositivo J su `8192 (0x2000)` e attivare l'impostazione.

Configurazione dei parametri Dual RSTP degli switch RCP

Dalle specifiche delle attività, sono necessari i parametri specifici *Dual RSTP* per gli switch A e B. Queste sono le *Dual RSTP* priorità switch, le Ring port, e i ruoli di collegamento. Nelle seguenti tabelle è riportato un riepilogo di questi valori.

Tabella 49:Parametri Dual RSTP per gli switch A e B

Parametro Dual RSTP	A	B
Dual RSTP Priorità switch (esadecimale)	`0x2000`	`0x0000`
Dual RSTP Priorità switch (decimale)	`8192`	`0`

Tabella 50:Parametri RCP per gli switch A e B

Parametro Dual RSTP	A	B
Anello primario, porta interna	`1/1`	`1/1`
Anello primario, porta esterna	`1/2`	`1/2`
Anello secondario, porta interna	`1/3`	`1/3`
Anello secondario, porta esterna	`1/4`	`1/4`
Ruolo di collegamento	`Slave`	`Master`

Configurare il dispositivo A A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching* > *L2-Redundancy* > *FuseNet* > *RCP*.
- ☐ Nel riquaro *Primary ring/network*, selezionare il valore `1/1` dall'elenco a discesa *Inner port*.
- ☐ Nel riquaro *Primary ring/network*, selezionare il valore `1/2` dall'elenco a discesa *Outer port*.
- ☐ Nel riquaro *Secondary ring/network*, selezionare il valore `1/3` dall'elenco a discesa *Inner port*.
- ☐ Nel riquaro *Secondary ring/network*, selezionare il valore `1/4` dall'elenco a discesa *Outer port*.
- ☐ Nel riquaro *Coupler configuration*, selezionare il valore *`slave`* dall'elenco a discesa *Role*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.
- ☐ Aprire la finestra di dialogo *Switching* > *L2-Redundancy* > *Spanning Tree* > *Dual RSTP*.
- ☐ Nel riquaro *Bridge configuration*, selezionare il valore `8192` dall'elenco a discesa *Priority*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`spanning-tree drstp mst priority 0 8192`	Impostare la priorità switchRSTP dell'istanza *Dual RSTP* sul valore `8192`.
`redundant-coupling port primary inner 1/1`	Selezionare la porta *1/1* come porta interna per l'anello primario *RCP*.
`redundant-coupling port primary outer 1/2`	Selezionare la porta *1/2* come porta esterna per l'anello primario *RCP*.
`redundant-coupling port secondary inner 1/3`	Selezionare la porta *1/3* come porta interna per l'anello secondario *RCP*.
`redundant-coupling port secondary outer 1/4`	Selezionare la porta *1/4* come porta esterna per l'anello secondario *RCP*.
`redundant-coupling role slave`	Configurare questo dispositivo come *RCP* slave.
`exit`	Passare alla modalità Privileged EXEC.

Configurare il dispositivo B A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > FuseNet > RCP*.
- ☐ Nel riquaro *Primary ring/network*, selezionare il valore `1/1` dall'elenco a discesa *Inner port*.
- ☐ Nel riquaro *Primary ring/network*, selezionare il valore `1/2` dall'elenco a discesa *Outer port*.
- ☐ Nel riquaro *Secondary ring/network*, selezionare il valore `1/3` dall'elenco a discesa *Inner port*.
- ☐ Nel riquaro *Secondary ring/network*, selezionare il valore `1/4` dall'elenco a discesa *Outer port*.
- ☐ Nel riquaro *Coupler configuration*, selezionare il valore *`master`* dall'elenco a discesa *Role*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.
- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*.
- ☐ Nel riquaro *Bridge configuration*, selezionare il valore `0` dall'elenco a discesa *Priority*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`spanning-tree drstp mst priority 0 0`	Impostare la priorità switchRSTP dell'istanza *Dual RSTP* sul valore `0`.
`redundant-coupling port primary inner 1/1`	Selezionare la porta *1/1* come porta interna per l'anello primario *RCP*.
`redundant-coupling port primary outer 1/2`	Selezionare la porta *1/2* come porta esterna per l'anello primario *RCP*.
`redundant-coupling port secondary inner 1/3`	Selezionare la porta *1/3* come porta interna per l'anello secondario *RCP*.
`redundant-coupling port secondary outer 1/4`	Selezionare la porta *1/4* come porta esterna per l'anello secondario *RCP*.
`redundant-coupling role master`	Configurare questo dispositivo come *RCP* master.
`exit`	Passare alla modalità Privileged EXEC.

Verifica della configurazione

Attivare le nuove connessioni ridondanti:
- La connessione delle porte interne per l'anello secondario tra dispositivo A, porta *1/3* e dispositivo B, porta *1/3*.
- Chiusura dell'anello per l'anello secondario tra i dispositivi G e H.
- Chiusura dell'anello primario tra i dispositivi C e D.

Confrontare i ruoli switch attuali nell'anello primario con i ruoli necessari dello switch:

lo switch A dovrebbe essere il root switch

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Nel frame *Topology information*, controllare l'impostazione della casella di spunta *Bridge is root*.

```
show spanning-tree global

Spanning Tree Information:
--------------------------
Spanning Tree Mode.....................RSTP
Spanning Tree Trap Mode.................enabled
Bridge is root..........................true
...
```

Confrontare le 4 porte configurate come porte interne ed esterne negli anelli primari e secondari con le specifiche in tabella 45.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > FuseNet > RCP*.
- ☐ Nei frame *Primary ring/network* e *Secondary ring/network*, verificare le porte mostrate.

```
show redundant-coupling global

Redundant coupling protocol global settings
-------------------------------------------
RCP global state.......................enabled
RCP device configured role..............slave
RCP inner primary interface.............1/1
RCP outer primary interface.............1/2
RCP inner secondary interface...........1/3
RCP outer secondary interface...........1/4
RCP timeout............................45 milliseconds
```

Confrontare i ruoli attuali dello switch nell'anello secondario con i ruoli necessari dello switch. Lo switch B dovrebbe essere il root switch.

Eseguire i seguenti passaggi:

- Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*.
- Nel frame *Topology information*, controllare l'impostazione della casella di spunta *Bridge is root*.

```
show spanning-tree drstp

Dual Spanning Tree Information:
-------------------------------
Spanning Tree Mode.........................RSTP
Spanning Tree Trap Mode....................enabled
Bridge is root.............................true
...
```

Confrontare i ruoli attuali delle porte degli switch nell'anello primario con i ruoli necessari della porta:

- Per le porte dello switch D che conducono allo switch C:
  Ruolo `alternate`
- Per le altre porte degli switch che conducono in direzione del root switch A:
  Ruolo `root`
- Per le altre porte degli switch che conducono in direzione del backup root switch D:
  Ruolo `designated`

Eseguire i seguenti passaggi:

- Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*.
- Nella colonna *Port role*, verificare il valore `alternate`, `root` o `designated` di cui sopra.

```
show spanning-tree mst port 0 1/<port>
```

Confrontare i ruoli attuali delle porte degli switch nell'anello secondario con i ruoli necessari delle porte:

- Per le porte dello switch H che conducono allo switch G:
  Ruolo `alternate`
- Per le altre porte degli switch che conducono in direzione del root switch B:
  Ruolo `root`
- Per le altre porte degli switch che conducono in direzione del backup root switch H:
  Ruolo `designated`

Eseguire i seguenti passaggi:

- Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*.
- Nella colonna *Port role*, verificare il valore `alternate`, `root` o `designated` di cui sopra.

```
show spanning-tree mst port 0 1/<port>
```

Quando la funzione *RCP* o *Spanning Tree* è disabilitata, il dispositivo disattiva automaticamente la funzione *Dual RSTP*.

Verificare lo stato della funzione *Dual RSTP*.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*. Nel frame *Operation*, il pulsante di opzione *Off* è selezionato.

```
show redundant-coupling status

Redundant coupling protocol status
------------------------------------------
RCP global state.........................forwarding
RCP device actual role...................disabled
Redundancy state availability............redNotAvailable
Primary ring protocol....................NONE
Secondary ring protocol..................NONE
```

Conclusione della configurazione

Per i dispositivi da A a J, salvare le impostazioni nella memoria non volatile. Seguire le istruzioni nella sezione “Salvataggio di un profilo di configurazione” a pagina 101.

14 Diagnosi di funzionamento

Il dispositivo offre i seguenti strumenti di diagnosi:
- Invio di trap SNMP
- Monitoraggio dello stato del dispositivo
- Segnalazione Out-of-Band tramite contatto di segnalazione.
- Indicazione di stato porta
- Contatore eventi a livello di porta
- Rilevamento incompatibilità tra modalità duplex
- Auto-Disable
- Visualizzazione dello stato SFP
- Riconoscimento della topologia
- Rilevamento di conflitti tra indirizzi IP
- Rilevamento di loop
- Contribuire a proteggere da loop di rete di Layer 2.
- Rapporti
- Monitoraggio del traffico dati su una porta (mirroring porte)
- Syslog
- Event log
- Causa e gestione azioni durante il test automatico

14.1 Invio di trap SNMP

Il dispositivo riferisce immediatamente alla network management station eventi inusuali che si verificano durante il normale funzionamento. L'operazione viene eseguita tramite messaggi definiti trap SNMP che bypassano la procedura di polling (“polling” significa interrogare le stazioni dati a intervalli regolari). Le trap SNMP consentono di reagire rapidamente a eventi inusuali.

Tali eventi possono essere:
- Reset hardware
- Modifiche alla configurazione
- Segmentazione di una porta

Il dispositivo invia trap SNMP a diversi host per aumentare l'affidabilità della trasmissione per i messaggi. Il messaggio trap SNMP non confermato è costituito da un pacchetto contenente informazioni su un evento inusuale.

Il dispositivo invia trap SNMP a quegli host immessi nella tabella di destinazione delle trap. Il dispositivo consente la configurazione della tabella di destinazione delle trap con la network management station utilizzando SNMP.

14.1.1 Elenco di trap SNMP

La seguente tabella visualizza possibili SNMP trap inviate dal dispositivo.

Tabella 51:Trap SNMP possibili

Nome del trap SNMP	Significato
authenticationFailure	Quando una stazione tenta di accedere ad un agente senza autorizzazione, questa trap viene inviata.
coldStart	Inviata dopo un riavvio.
sa2DevMonSenseExtNvmRemoval	Quando la memoria esterna è stata rimossa, questa trap viene inviata.
linkDown	Quando la connessione a una porta è interrotta, questa trap viene inviata.
linkUp	Quando la connessione a una porta è stabilita, questa trap viene inviata.
sa2DevMonSensePSState	Quando lo stato di un alimentatore cambia, questa trap viene inviata.
sa2SigConStateChange	Quando lo stato di un contatto di segnalazione cambia durante il monitoraggio di funzionamento, questa trap viene inviata.
newRoot	Quando l'agente mittente diventa la nuova radice dello spanning tree, questa trap viene inviata.
topologyChange	Quando la porta cambia da blocking a forwarding o da forwarding a blocking, questa trap viene inviata.
alarmRisingThreshold	Quando l'input RMON è maggiore della soglia superiore, questa trap viene inviata.
alarmFallingThreshold	Quando l'input RMON è minore della soglia inferiore, questa trap viene inviata.
sa2AgentPortSecurityViolation	Quando un indirizzo MAC rilevato su questa porta non corrisponde alle impostazioni correnti del parametro sa2AgentPortSecurityEntry, questo trap è inviato.
sa2DiagSelftestActionTrap	Quando si effettua un test automatico per le quattro categorie “attività”, “risorsa”, “software” e “hardware”in base alle impostazioni configurate, questa trap viene inviata.
sa2MrpReconfig	Quando la configurazione dell'MRP ring cambia, questa trap viene inviata.
sa2DiagIfaceUtilizationTrap	Quando la soglia dell'interfaccia è maggiore o minore della soglia superiore o inferiore specificata, questa trap viene inviata.
sa2LogAuditStartNextSector	Quando, dopo aver completato un settore, ne inizia uno nuovo, questa trap viene inviata.
sa2PtpSynchronizationChance	Quando lo stato della sincronizzazione su PTP è stato modificato, questa trap viene inviata.
sa2ConfigurationSavedTrap	Dopo che il dispositivo ha completato il salvataggio locale della configurazione, questa trap viene inviata.
sa2ConfigurationChangedTrap	Quando si modifica per la prima volta la configurazione del dispositivo dopo il salvataggio locale, questa trap viene inviata.
sa2PlatformStpInstanceLoopInconsistentStartTrap	Quando la porta in questa istanza STP passa allo stato “loop inconsistent”, questa trap viene inviata.
sa2PlatformStpInstanceLoopInconsistentEndTrap	Quando la porta in questa istanza STP lascia lo stato “loop inconsistent” ricevendo un pacchetto BPDU, questa trap viene inviata.

14.1.2 Trap SNMP per attività di configurazione

Dopo aver salvato una configurazione in memoria, il dispositivo invia una `sa2ConfigurationSavedTrap`. Questo trap SNMP contiene entrambe le variabili di stato della memoria non volatile (*NVM*) e della memoria esterna (*ENVM*), indicanti se la configurazione in esecuzione è in sincrono con la memoria non volatile e con la memoria esterna. È anche possibile attivare questa trap SNMP copiando un file di configurazione sul dispositivo, sostituendo la configurazione salvata attiva

Inoltre, il dispositivo invia una `sa2ConfigurationChangedTrap`, ogni volta che si cambia la configurazione locale, indicando una mancata corrispondenza tra la configurazione in esecuzione e quella salvata.

14.1.3 Impostazione trap SNMP

Il dispositivo consente di inviare una trap SNMP come una reazione a specifici eventi. Creare almeno una destinazione trap che riceve trap SNMP.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)*.
- ☐ Fare clic sul pulsante .
  La finestra di dialogo mostra la finestra *Create*.
- ☐ Nel riquadro *Name*, specificare il nome che il dispositivo utilizza per identificarsi come l'origine della trap SNMP.
- ☐ Nel riquadro *Address*, specificare l'indirizzo IP della destinazione delle trap a cui il dispositivo invia le trap SNMP.
- ☐ Nella colonna *Active*, selezionare le voci che il dispositivo ha in considerazione quando invia trap SNMP.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

Ad esempio, nelle seguenti finestre di dialogo si specifica se il dispositivo attiva una trap SNMP:

- Finestra di dialogo *Basic Settings > Port*
- Finestra di dialogo *Basic Settings > Power over Ethernet > Global*
- Finestra di dialogo *Network Security > Port Security*
- Finestra di dialogo *Switching > L2-Redundancy > Link Aggregation*
- Finestra di dialogo *Diagnostics > Status Configuration > Device Status*
- Finestra di dialogo *Diagnostics > Status Configuration > Security Status*
- Finestra di dialogo *Diagnostics > Status Configuration > Signal Contact*
- Finestra di dialogo *Diagnostics > Status Configuration > MAC Notification*
- Finestra di dialogo *Diagnostics > System > IP Address Conflict Detection*
- Finestra di dialogo *Diagnostics > System > Selftest*
- Finestra di dialogo *Diagnostics > Ports > Port Monitor*
- Finestra di dialogo *Advanced > Digital IO Module*

14.1.4 Messaggi ICMP

Il dispositivo consente l'uso di Internet Control Message Protocol (ICMP) per applicazioni diagnostiche, ad esempio ping and trace route. Il dispositivo utilizza ICMP anche per messaggi time-to-live e discarding in cui il dispositivo rinvia un messaggio ICMP al dispositivo origine del pacchetto.

Utilizzare lo strumento di ping network per verificare il percorso ad un particolare host attraverso una rete IP. Lo strumento di diagnostica traceroute visualizza i percorsi e i ritardi di transito dei pacchetti attraverso una rete.

14.2 Monitoraggio dello stato del dispositivo

Lo stato del dispositivo fornisce una panoramica delle condizioni generali del dispositivo. Diversi sistemi di visualizzazione del processo registrano lo stato del dispositivo per un dispositivo, allo scopo di presentarne la sua condizione in forma grafica.

Il dispositivo visualizza il suo stato attuale come `error` o `ok` nel riquadro *Device status*. Il dispositivo determina questo stato sulla base dei singoli risultati del monitoraggio.

Il dispositivo consente di:
- Segnalazione Out-of-Band tramite un contatto di segnalazione.
- Segnalare lo stato modificato del dispositivo inviando una trap SNMP
- rilevare lo stato del dispositivo nella finestra di dialogo *Basic Settings > System* dell'interfaccia grafica utente.
- Eseguire una query dello stato del dispositivo nell'interfaccia a riga di comando

La scheda *Global* della finestra di dialogo *Diagnostics > Status Configuration > Device Status* consente la configurazione del dispositivo per inviare una trap alla management station per i seguenti eventi:
- Tensione di alimentazione non corretta
  - Almeno una delle 2 tensioni di alimentazione non funziona
  - La tensione di alimentazione interna non funziona
- Quando il dispositivo funziona al di fuori della soglia di temperatura definita dall'utente
- Perdita di ridondanza (in modalità Ring Manager)
- L'interruzione della(e) connessione(i) di link
  Configurare almeno una porta per questa funzionalità. Quando il link non è attivo, si specificano quali porte il dispositivo segnala nella scheda *Port* della finestra di dialogo *Diagnostics > Status Configuration > Device Status* nella riga *Propagate connection error*.
- La rimozione della memoria esterna.
  La configurazione nella memoria esterna è fuori sincrono con la configurazione nel dispositivo.

Selezionare le voci corrispondenti per decidere quali eventi comprende lo stato del dispositivo.

Nota: Con un'alimentazione di tensione non ridondante, il dispositivo riferisce l'assenza di una tensione di alimentazione. Per disabilitare questo messaggio, alimentare la tensione di alimentazione attraverso i due ingressi oppure ignorare il monitoraggio.

14.2.1 Eventi che possono essere monitorati

Tabella 52:Eventi Device Status

Nome	Significato
Temperature	Esegue il monitoraggio in caso la temperatura ecceda o sia al di sotto del valore specificato.
Ring redundancy	Quando la ridondanza ad anello è presente, abilitare questa funzione.
Connection errors	Abilitare questa funzione per monitorare ogni evento link porta in cui la casella di spunta *Propagate connection error* è attiva.
External memory removal	Abilitare questa funzione per monitorare la presenza di un dispositivo di archiviazione esterno.
External memory not in sync	Questo dispositivo monitora la sincronizzazione tra la configurazione del dispositivo e la configurazione memorizzata sulla memoria esterna (*ENVM*).
Power supply	Abilitare questa funzione per monitorare l'alimentazione di tensione.

14.2.2 Configurazione dello stato dispositivo

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Device Status*, scheda *Global*.
- ☐ Per i parametri da monitorare, selezionare la casella di spunta nella colonna *Monitor*.
- ☐ Per inviare una trap SNMP alla management station, attivare la funzione *Send trap* nel riquadro *Traps*.
- ☐ Nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)*, creare almeno una destinazione trap che riceve trap SNMP.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.
- ☐ Aprire la finestra di dialogo *Basic Settings > System*.
- ☐ Per monitorare la temperatura, in fondo al riquadro *System data*, si specificano le soglie di temperatura.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`device-status trap`	Quando lo stato del dispositivo cambia, invia una trap SNMP.
`device-status monitor envm-not-in-sync`	Monitora i profili di configurazione nel dispositivo e nella memoria esterna. Il riquadro *Device status* cambia in `error` nelle seguenti situazioni: • Il profilo di configurazione esiste solamente nel dispositivo. • Il profilo di configurazione nel dispositivo differisce dal profilo di configurazione nella memoria esterna.
`device-status monitor envm-removal`	Monitora la memoria esterna attiva. Rimuovendo la memoria esterna attiva dal dispositivo, nel riquadro *Device status* il valore cambia in `error`.
`device-status monitor power-supply 1`	Monitora l'alimentatore `1`. Se il dispositivo presenta un errore di alimentazione di tensione rilevato, nel riquadro*Device status* il valore cambia in `error`.
`device-status monitor ring-redundancy`	Monitora la ridondanza ad anello. Il riquadro *Device status* cambia in `error` nelle seguenti situazioni: • La funzionalità di ridondanza si attiva (perdita della riserva di ridondanza). • Il dispositivo è un normale partecipante dell'anello e rileva un errore nelle sue impostazioni.
`device-status monitor temperature`	Monitora la temperatura nel dispositivo. Quando la temperatura eccede o è inferiore al limite specificato, il valore nel riquadro *Device status* cambia in `error`.

Per abilitare il dispositivo a monitorare un link attivo senza una connessione, abilitare prima la funzione globale, poi abilitare le singole porte.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Device Status*, scheda *Global*.
- ☐ Per il parametro *Connection errors*, selezionare la casella di spunta nella colonna *Monitor*.
- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Device Status*, scheda *Port*.
- ☐ Per il parametro *Propagate connection error*, selezionare la casella di spunta nella colonna delle porte da monitorare.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`device-status monitor link-failure`	Monitorare le porte/il link interfacce. Se il link si interrompe su una porta/interfaccia monitorata, il valore nel riquadro*Device status* cambia in `error`.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`device-status link-alarm`	Monitora il link porta/interfaccia. Se il link si interrompe sulla porta/interfaccia monitorata, il valore nel riquadro*Device status* cambia in `error`.

Nota: I comandi di cui sopra attivano il monitoraggio e il trapping per i componenti supportati. Quando si desidera attivare o disattivare il monitoraggio per i componenti individuali, la sintassi corrispondente è disponibile nel Manuale di riferimento “Command Line Interface” o nella guida della console della Command Line Interface. Per visualizzare la guida nella Command Line Interface, inserire il punto di domanda `?` e premere il tasto <Enter>.

14.2.3 Visualizzazione stato dispositivo

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > System*.

`show device-status all`	Nella modalità Privileged EXEC: visualizza lo stato del dispositivo e l'impostazione per la determinazione dello stato del dispositivo.

14.3 Stato di sicurezza

Lo stato di sicurezza fornisce una panoramica della sicurezza generale del dispositivo. Molti processo facilitano la visualizzazione del sistema registrando lo stato di sicurezza del dispositivo e poi presentando la sua condizione in forma grafica. Il dispositivo visualizza lo stato di sicurezza generale nella finestra di dialogo *Basic Settings > System*, riquadro *Security status*.

Nella scheda *Global* della finestra di dialogo *Diagnostics > Status Configuration > Security Status* il dispositivo visualizza lo stato corrente come `error` o `ok` nel riquadro *Security status*. Il dispositivo determina questo stato sulla base dei singoli risultati del monitoraggio.

Il dispositivo consente di:
- Segnalazione Out-of-Band tramite un contatto di segnalazione.
- Segnalare lo stato di sicurezza modificato del dispositivo inviando una trap SNMP
- rilevare lo stato di sicurezza nella finestra di dialogo *Basic Settings > System* dell'interfaccia grafica utente.
- Eseguire una query dello stato di sicurezza nell'interfaccia a riga di comando

14.3.1 Eventi che possono essere monitorati

Eseguire i seguenti passaggi:
- ☐ Specificare gli eventi monitorati dal dispositivo.
- ☐ Per il parametro corrispondente, selezionare la casella di spunta nella colonna *Monitor*.

Tabella 53:Eventi Security Status

Nome	Significato
Password default settings unchanged	Dopo l'installazione, cambiare le password per incrementare la sicurezza. Quando attivo e le password di default rimangono invariate, il dispositivo visualizza un allarme.
Min. password length < 8	Creare password con più di 8 caratteri per mantenere un livello di sicurezza elevato. Quando attivo, il dispositivo monitora le impostazioni *Min. password length*.
Password policy settings deactivated	Il dispositivo monitora le impostazioni che si trovano nella finestra di dialogo *Device Security > User Management*.
User account password policy check deactivated	Il dispositivo monitora le impostazioni della casella di controllo *Policy check*. Quando *Policy check* è inattivo, il dispositivo invia una trap SNMP.
Telnet server active	Il dispositivo monitora quando si abilita la funzione *Telnet*.
HTTP server active	Il dispositivo monitora quando si abilita la funzione *HTTP*.
SNMP unencrypted	Il dispositivo monitora quando si abilita la funzione *SNMPv1* o *SNMPv2*.
Access to system monitor with serial interface possible	Il dispositivo monitora lo stato del monitor di sistema.
Saving the configuration profile on the external memory possible	Il dispositivo monitora la possibilità di salvare configurazioni nella memoria non volatile esterna.
Link interrupted on enabled device ports	Il dispositivo monitora lo stato del link delle porte attive.
Access with Ethernet Switch Configurator possible	Il dispositivo monitora quando si abilita la funzione Ethernet Switch Configurator di accesso in lettura/scrittura.

Tabella 53:Eventi Security Status (cont

Nome	Significato
Load unencrypted config from external memory	Il dispositivo monitora le impostazioni di sicurezza per caricare la configurazione dalla NVM esterna.
IEC61850-MMS active	Il dispositivo monitora le impostazioni di attivazione del protocollo IEC 61850-MMS.
Modbus TCP active	Il dispositivo monitora le impostazioni di attivazione del protocollo Modbus TCP/IP.
Self-signed HTTPS certificate present	Il dispositivo monitora il server HTTPS per i certificato digitali autogenerati.

14.3.2 Configurazione dello stato di sicurezza

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Security Status*, scheda *Global*.
- ☐ Per i parametri da monitorare, selezionare la casella di spunta nella colonna *Monitor*.
- ☐ Per inviare una trap SNMP alla management station, attivare la funzione *Send trap* nel riquadro *Traps*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.
- ☐ Nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)*, creare almeno una destinazione trap che riceve trap SNMP.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`security-status monitor pwd-change`	Monitora la password per gli account utente `user` e `admin` configurati localmente. Quando la password per gli account utente `user` o `admin` è l'impostazione di default, il valore nel riquadro *Security status* cambia in *`error`*.
`security-status monitor pwd-min-length`	Monitora il valore specificato nel criterio *Min. password length*. Quando il valore per il criterio *Min. password length* è inferiore a `8`, nel riquadro *Security status* il valore cambia in *`error`*.
`security-status monitor pwd-policy-config`	Monitora le impostazioni dei criteri per le password. Quando il valore per almeno uno dei seguenti criteri è `0`, nel riquadro *Security status* il valore cambia in *`error`*. • *Upper-case characters (min.)* • *Lower-case characters (min.)* • *Digits (min.)* • *Special characters (min.)*
`security-status monitor pwd-policy-inactive`	Monitora le impostazioni dei criteri per le password. Quando il valore per almeno uno dei seguenti criteri è `0`, nel riquadro *Security status* il valore cambia in *`error`*.
`security-status monitor telnet-enabled`	Monitora il server Telnet. Abilitando il server Telnet, nel riquadro *Security status* il valore cambia in *`error`*.

`security-status monitor http-enabled`	Monitora il server HTTP. Abilitando il server HTTP, nel riquadro *Security status* il valore cambia in `error`.
`security-status monitor snmp-unsecure`	Monitora il server SNMP. Quando si applica almeno una delle seguenti condizioni, nel riquadro *Security status* il valore cambia in `error`: • È abilitata la funzione *SNMPv1*. • È abilitata la funzione *SNMPv2*. • La crittografia per SNMPv3 è disabilitata. Abilitare la crittografia nella finestra di dialogo *Device Security > User Management*, nel campo *SNMP encryption type*.
`security-status monitor sysmon-enabled`	Per monitorare l'attivazione della funzione System Monitor nel dispositivo.
`security-status monitor extnvm-upd-enabled`	Per monitorare l'attivazione dell'aggiornamento della memoria non volatile esterna.
`security-status monitor iec61850-mms-enabled`	Monitora la funzione *IEC61850-MMS*. Abilitando la funzione *IEC61850-MMS*, il valore nel riquadro *Security status* cambia in `error`.
`security-status trap`	Quando lo stato del dispositivo cambia, invia una trap SNMP.

Per abilitare il dispositivo a monitorare un link attivo senza una connessione, abilitare prima la funzione globale, poi abilitare le singole porte.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Security Status*, scheda *Global*.
- ☐ Per il parametro *Link interrupted on enabled device ports*, selezionare la casella di spunta nella colonna *Monitor*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.
- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Device Status*, scheda *Port*.
- ☐ Per il parametro *Link interrupted on enabled device ports*, selezionare la casella di spunta nella colonna delle porte da monitorare.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`security-status monitor no-link-enabled`	Monitora il link sulle porte attive. Se il link si interrompe su una porta attiva, nel riquadro*Security status* il valore cambia in `error`.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`security-status monitor no-link`	Monitora il link sull'interfaccia/porta `1`.

14.3.3 Visualizzazione dello stato dispositivo

Eseguire i seguenti passaggi:

☐ Aprire la finestra di dialogo *Basic Settings > System*.

```
show security-status all
```

Nella modalità Privileged EXEC: visualizzare lo stato di sicurezza e l'impostazione per la determinazione dello stato di sicurezza.

14.4 Segnalazione Out-of-Band

Il dispositivo utilizza il contatto di segnalazione per controllare i dispositivi esterni e monitorare le funzioni del dispositivo. Il monitoraggio delle funzioni consente l'esecuzione della diagnostica remota.

Il dispositivo indica lo stato di funzionamento utilizzando un'interruzione nel contatto di segnalazione privo di potenziale (contato relè, circuito chiuso) per la modalità selezionata. Il dispositivo monitora le seguenti funzioni:

- Tensione di alimentazione non corretta
  - Almeno una delle 2 tensioni di alimentazione non funziona
  - La tensione di alimentazione interna non funziona
- Quando il dispositivo funziona al di fuori della soglia di temperatura definita dall'utente
- Eventi per la ridondanza ad anello
  Perdita di ridondanza (in modalità Ring Manager)
  Nell'impostazione di default, il monitoraggio ridondanza ad anello è inattivo. Il dispositivo è un normale partecipante dell'anello e rileva un errore nella configurazione locale.
- L'interruzione della(e) connessione(i) di link
  Configurare almeno una porta per questa funzionalità. Nel riquadro *Propagate connection error*, specificare per quali porte il dispositivo segnala un'interruzione di link. Nell'impostazione di default, il monitoraggio link è inattivo.
- La rimozione della memoria esterna.
  La configurazione nella memoria esterna non corrisponde alla configurazione nel dispositivo.

Selezionare le voci corrispondenti per decidere quali eventi comprende lo stato del dispositivo.

Nota: Con un'alimentazione di tensione non ridondante, il dispositivo riferisce l'assenza di una tensione di alimentazione. Per disabilitare questo messaggio, alimentare la tensione di alimentazione attraverso i due ingressi oppure ignorare il monitoraggio.

14.4.1 Controllo del contatto di segnalazione

Tramite la modalità `Manual setting` si controlla in remoto questo contatto di segnalazione.

Possibilità di applicazione:

- Simulazione di un errore rilevato durante il monitoraggio errori PLC.
- Controllo remoto di un dispositivo tramite SNMP, ad es.tramite attivazione di una videocamera

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Signal Contact*, scheda *Global*.
- ☐ Per controllare il contatto di segnalazione manualmente, nel riquadro *Configuration*, selezionare la voce `Manual setting` nella lista a discesa *Mode*.
- ☐ Per aprire il contatto di segnalazione, selezionare il pulsante di opzione `open` nel riquadro *Configuration*.
- ☐ Per chiudere il contatto di segnalazione, selezionare il pulsante di opzione `close` nel riquadro *Configuration*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`signal-contact 1 mode manual`	Selezionare la modalità di impostazione manuale per il contatto di segnalazione `1`.
`signal-contact 1 state open`	Aprire il contatto di segnalazione `1`.
`signal-contact 1 state closed`	Chiudere il contatto di segnalazione `1`.

14.4.2 Monitoraggio degli stati del dispositivo e di sicurezza

Nel campo *Configuration*, specificare quali eventi il contatto di segnalazione indica.

- *`Device status`*
  Utilizzando questa impostazione il contatto di segnalazione indica lo stato dei parametri monitorati nella finestra di dialogo *Diagnostics > Status Configuration > Device Status*.
- *`Security status`*
  Utilizzando questa impostazione il contatto di segnalazione indica lo stato dei parametri monitorati nella finestra di dialogo *Diagnostics > Status Configuration > Security Status*.
- *`Device/Security status`*
  Utilizzando questa impostazione il contatto di segnalazione indica lo stato dei parametri monitorati nella finestra di dialogo *Diagnostics > Status Configuration > Device Status* e la finestra di dialogo *Diagnostics > Status Configuration > Security Status*.

Configurazione del monitoraggio di funzionamento

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Signal Contact*, scheda *Global*.
- ☐ Per monitorare le funzioni del dispositivo utilizzando il contatto di segnalazione, nel riquadro *Configuration*, specificare il valore *`Monitoring correct operation`* nel campo *Mode*.
- ☐ Per i parametri da monitorare, selezionare la casella di spunta nella colonna *Monitor*.
- ☐ Per inviare una trap SNMP alla management station, attivare la funzione *Send trap* nel riquadro *Traps*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.
- ☐ Nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)*, creare almeno una destinazione trap che riceve trap SNMP.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.
- ☐ Specificare le soglie di temperatura per il monitoraggio della temperatura nella finestra di dialogo *Basic Settings > System*.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`signal-contact 1 monitor temperature`	Monitora la temperatura nel dispositivo. Quando la temperatura eccede / è inferiore ai valori soglia, il contatto di segnalazione si apre.

`signal-contact 1 monitor ring-redundancy`	Monitora la ridondanza ad anello. Il contatto di segnalazione si: apre nelle seguenti situazioni: • La funzionalità di ridondanza si attiva (perdita della riserva di ridondanza). • Il dispositivo è un normale partecipante dell'anello e rileva un errore nelle sue impostazioni.
`signal-contact 1 monitor link-failure`	Monitorare le porte/il link interfacce. Quando il link si interrompe su una porta/interfaccia monitorata, il contatto di segnalazione si apre.
`signal-contact 1 monitor envm-removal`	Monitora la memoria esterna attiva. Rimuovendo la memoria esterna attiva dal dispositivo, il contatto di segnalazione si apre.
`signal-contact 1 monitor envm-not-in-sync`	Monitora i profili di configurazione nel dispositivo e nella memoria esterna. Il contatto di segnalazione si: apre nelle seguenti situazioni: • Il profilo di configurazione esiste solamente nel dispositivo. • Il profilo di configurazione nel dispositivo differisce dal profilo di configurazione nella memoria esterna.
`signal-contact 1 monitor power-supply 1`	Monitora l'alimentatore `1`. Quando il dispositivo presenta un errore di alimentazione di tensione rilevato, il contatto di segnalazione si apre.
`signal-contact 1 monitor module-removal 1`	Monitora il modulo `1`. Quando si rimuove il modulo `1` dal dispositivo, il contatto di segnalazione si apre.
`signal-contact 1 trap`	Abilita il dispositivo a inviare un trap SNMP quando lo stato del monitoraggio di funzionamento cambia.
`no signal-contact 1 trap`	Disabilitazione della trap SNMP

Per abilitare il dispositivo a monitorare un link attivo senza una connessione, abilitare prima la funzione globale, poi abilitare le singole porte.

Eseguire i seguenti passaggi:

- ☐ Nella colonna *Monitor*, attivare la funzione *Link interrupted on enabled device ports*.
- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Device Status*, scheda *Port*.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`signal-contact 1 monitor link-failure`	Monitorare le porte/il link interfacce. Quando il link si interrompe su una porta/interfaccia monitorata, il contatto di segnalazione si apre.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`signal-contact 1 link-alarm`	Monitora il link porta/interfaccia. Se il link si interrompe sulla porta/interfaccia selezionata, il contatto di segnalazione si apre.

Eventi che possono essere monitorati

Tabella 54:Eventi Device Status

Nome	Significato
Temperature	Quando la temperatura eccede o è al di sotto del valore specificato.
Ring redundancy	Quando la ridondanza ad anello è presente, abilitare questa funzione di monitoraggio.
Connection errors	Abilitare questa funzione per monitorare ogni evento link porta in cui la casella di spunta *Propagate connection error* è attiva.
External memory not in sync with NVM	Questo dispositivo monitora la sincronizzazione tra la configurazione del dispositivo e la configurazione memorizzata sulla memoria esterna (*ENVM*).
External memory removed	Abilitare questa funzione per monitorare la presenza di un dispositivo di archiviazione esterno.
Power supply	Abilitare questa funzione per monitorare l'alimentazione di tensione.

Visualizzazione dello stato del contatto di segnalazione

Il dispositivo fornisce opzioni supplementari per visualizzare lo stato del contatto di segnalazione:
- Visualizzare nell'interfaccia grafica utente
- Eseguire una query nell'interfaccia a riga di comando

Eseguire i seguenti passaggi:

☐ Aprire la finestra di dialogo *Basic Settings > System*.
Il riquadro *Signal contact status* visualizza lo stato del contratto di segnalazione e informa sugli allarmi che si sono verificati. Se esiste già un allarme, il riquadro è evidenziato.

```
show signal-contact 1 all
```

Visualizza le impostazioni del contatto di segnalazione per il contatto di segnalazione specificato.

14.5 Indicazione di stato porta

Per visualizzare lo stato delle porte eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > System*.

La finestra di dialogo visualizza il dispositivo con la configurazione corrente. Inoltre, la finestra di dialogo indica lo stato delle singole porte con un simbolo.

I seguenti simboli rappresentano lo stato delle porte individuali. In alcune situazioni, questi simboli interferiscono uno con l'altro. Quando si posiziona il puntatore del mouse sopra l'icona della porta, una nota a bolla visualizza una descrizione dettagliata dello stato della porta.

Tabella 55:Simboli che identificano lo stato delle porte

Criterio	Icona
Larghezza di banda della porta	10 Mbit/s Porta attivata, connessione ok, modalità full-duplex 100 Mbit/s Porta attivata, connessione ok, modalità full-duplex 1000 Mbit/s Porta attivata, connessione ok, modalità full-duplex
Modo operativo	Modalità half-duplex abilitata Vedere la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*, casella di selezione*Automatic configuration*, campo *Manual configuration* e campo *Manual cable crossing (Auto. conf. off)*. Autonegoziazione abilitata Vedere la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*, casella di selezione *Automatic configuration*. La porta è bloccata da una funzione di ridondanza.
AdminLink	La porta è disattivata, connessione Ok La porta è disattivata, nessuna connessione configurata Vedere la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*, casella di selezione*Port on* e campo *Link/Current settings*.

14.6 Contatore eventi porta

La tabella di statistiche porta consente agli amministratori di rete di identificare possibili problemi rilevati nella rete.

Questa tabella visualizza i contenuti di vari contatori di eventi. I contatori di pacchetti sommano gli eventi inviati e gli eventi ricevuti. Nella finestra di dialogo *Basic Settings > Restart*, è possibile azzerare i contatori eventi.

Tabella 56:Esempi di indicazione di punti deboli individuati

Contatore	Indicazione di possibili punti deboli individuati
Frammenti ricevuti	• Controller non funzionante del dispositivo connesso • Interferenza elettromagnetica nel mezzo di trasmissione
Errore CRC	• Controller non funzionante del dispositivo connesso • Interferenza elettromagnetica nel mezzo di trasmissione • Componente inutilizzabile nella rete
Collisioni	• Controller non funzionante del dispositivo connesso • Rete troppo estesa/linee troppo lunghe • Collisione o un errore riconosciuto con un pacchetto dati

Eseguire i seguenti passaggi:

- ☐ Per visualizzare il contatore eventi, aprire la finestra di dialogo *Basic Settings > Port*, scheda *Statistics*.
- ☐ Per azzerare i contatori, nella finestra di dialogo *Basic Settings > Restart*, fare clic sul pulsante *Clear port statistics*.

14.6.1 Rilevamento incompatibilità tra modalità duplex

I problemi si verificano quando 2 porte direttamente connesse l'una con l'altra hanno modalità duplex non corrispondenti. Questi problemi sono difficili da individuare. Il rilevamento e segnalazione automatiche di questa situazione presentano il vantaggio di riconoscere modalità duplex non corrispondenti ancor prima che il problema si presenti.

Questa situazione deriva da una configurazione errata, ad esempio in caso di disattivazione della configurazione automatica sulla porta remota.

Un tipico effetto di tale incompatibilità è che, sebbene la connessione sembri funzionare a bassa velocità dati, ad un elevato livello di traffico bidirezionale il dispositivo locale registra troppi errori CRC e la connessione rimane di molto inferiore alla portata nominale.

Il dispositivo consente di individuare questa situazione e di segnalarla alla network management station. Durante il processo, il dispositivo analizza qui il contatore di errori rilevati della porta in funzione delle impostazioni di quest'ultima.

Possibili cause degli eventi di errore porta

La seguente tabella riporta i modi operativi duplex per porte TX insieme ai possibili eventi di errore. Il significato dei termini utilizzati nella tabella sono i seguenti:

- Collisioni
  In modalità half-duplex, le collisioni indicano il funzionamento normale.
- Problema duplex
  Modalità duplex non corrispondenti.
- EMI
  Interferenza elettromagnetica.
- Estensione della rete
  La rete è troppo estesa oppure sono presenti troppi hub in cascata.
- Collisioni, Late Collisions
  In modalità full-duplex, nessun incremento dei contatori porta per collisioni o Late Collisions.
- Errore CRC
  Il dispositivo analizza questi errori rilevati come modalità duplex non corrispondenti nella modalità full-duplex manuale.

Tabella 57:Analisi di non corrispondenza della modalità duplex

N.	Configurazione automatica	Modalità duplex corrente	Eventi di errore rilevati (≥ 10 dopo link up)	Modalità duplex	Possibili cause
1	selezionato	Half-duplex	Nessuna	OK	
2	selezionato	Half-duplex	Collisioni	OK	
3	selezionato	Half-duplex	Late Collisions	Rilevato problema duplex	Problema duplex, EMI, estensione della rete
4	selezionato	Half-duplex	Errore CRC	OK	EMI
5	selezionato	Full-duplex	Nessuna	OK	
6	selezionato	Full-duplex	Collisioni	OK	EMI
7	selezionato	Full-duplex	Late Collisions	OK	EMI
8	selezionato	Full-duplex	Errore CRC	OK	EMI
9	non selezionato	Half-duplex	Nessuna	OK	
10	non selezionato	Half-duplex	Collisioni	OK	
11	non selezionato	Half-duplex	Late Collisions	Rilevato problema duplex	Problema duplex, EMI, estensione della rete
12	non selezionato	Half-duplex	Errore CRC	OK	EMI
13	non selezionato	Full-duplex	Nessuna	OK	
14	non selezionato	Full-duplex	Collisioni	OK	EMI
15	non selezionato	Full-duplex	Late Collisions	OK	EMI
16	non selezionato	Full-duplex	Errore CRC	Rilevato problema duplex	Problema duplex, EMI

14.7 Auto-Disable

Il dispositivo può disabilitare una porta per diverse ragioni configurabili. Ogni ragione comporta la “disattivazione” della porta. Per recuperare la porta dallo stato di disattivazione, è possibile eliminare manualmente la condizione che causa la disattivazione della porta oppure specificare un timer per riabilitare automaticamente la porta.

Se la configurazione visualizza una porta come abilitata, ma il dispositivo rileva un errore o cambiamento della condizione, il software disattiva quella porta. In altre parole, il software del dispositivo disabilità la porta a causa di un errore rilevato o cambiamento nella condizione.

Se una porta è disabilitata automaticamente, il dispositivo effettivamente disattiva la porta e la porta blocca il traffico. Il LED della porta lampeggia di verde 3 volte per periodo e identifica la ragione della disattivazione. Inoltre, il dispositivo crea un file di registro che elenca le cause della disattivazione. Quando si riabilita la porta dopo un timeout utilizzando la funzione *Auto-Disable*, il dispositivo genera una voce di registro.

La funzione *Auto-Disable* offre una funzione di recupero che abilita automaticamente una porta con disabilitazione automatica dopo un tempo definito dall'utente. Quando questa funzione abilita una porta, il dispositivo invia una trap SNMP con il numero di porta, ma senza un valore per il parametro *Reason*.

La funzione *Auto-Disable* serve ai seguenti scopi:
- Assiste l'amministratore di rete nell'analisi della porta.
- Riduce la possibilità che questa porta causi instabilità della rete.

La funzione *Auto-Disable* è disponibile per le seguenti funzioni:
- *Link flap* (funzione *Port Monitor*)
- *CRC/Fragments* (funzione *Port Monitor*)
- Rilevamento Duplex Mismatch (funzione *Port Monitor*)
- *DHCP Snooping*
- *Dynamic ARP Inspection*
- *Spanning Tree*
- *Port Security*
- *Overload detection* (funzione *Port Monitor*)
- *Link speed/Duplex mode detection* (funzione *Port Monitor*)

Nel seguente esempio si configura il dispositivo per disabilitare una porta a causa di violazioni rilevate e relative alle soglie specificate nella finestra di dialogo *Diagnostics > Ports > Port Monitor*, scheda *CRC/Fragments*, e poi riabilitare automaticamente la porta disabilitata.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Ports > Port Monitor*, scheda *CRC/Fragments*.
- ☐ Verificare che le soglie specificate nella tabella coincidano con le preferenze dell'utente per la porta `1/1`.
- ☐ Aprire la finestra di dialogo *Diagnostics > Ports > Port Monitor*, scheda *Global*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Per consentire al dispositivo di disabilitare la porta a causa degli errori rilevati, selezionare la casella di spunta nella colonna *CRC/Fragments on* per la porta `1/1`.

- Nella colonna *Action*, è possibile selezionare come il dispositivo reagisce agli errori rilevati. In questo esempio, il dispositivo disabilita la porta `1/1` per violazioni di soglia e poi automaticamente riabilita la porta.
  - Per consentire al dispositivo di disabilitare e riabilitare automaticamente la porta, selezionare il valore `auto-disable` e configurare la funzione *Auto-Disable*. Il valore `auto-disable` funziona in combinazione con la funzione *Auto-Disable*.

  Il dispositivo può anche disabilitare una porta senza riabilitare automaticamente.
  - Per consentire al dispositivo di disabilitare solo la porta, selezionare il valore `disable port`.

    Per riabilitare manualmente una porta disabilitata, evidenziare la porta.

    Fare clic sul pulsante ☰ e poi sulla voce *Reset*.
  - Quando si configura la funzione *Auto-Disable*, il valore `disable port` riabilita automaticamente la porta.
- Aprire la finestra di dialogo *Diagnostics > Ports > Port Monitor*, scheda *Auto-disable*.
- Per consentire al dispositivo di riabilitare automaticamente la porta dopo che è stata disabilitata a causa delle violazioni di soglia, selezionare la casella di spunta nella colonna *CRC error*.
- Aprire la finestra di dialogo *Diagnostics > Ports > Port Monitor*, scheda *Port*.
- Specificare il tempo di ritardo di 120 s nella colonna *Reset timer [s]* per le porte che si desiderano abilitare.

Nota: La voce *Reset* consente di abilitare la porta prima che il tempo specificato nella colonna *Reset timer [s]* conti in senso decrescente.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`port-monitor condition crc-fragments count 2000`	Specificazione del contatore frammenti CRC a 2000 parti per milione.
`port-monitor condition crc-fragments interval 15`	Imposta l'intervallo di misurazione a 15 secondi per il rilevamento dei frammenti CRC
`auto-disable timer 120`	Specifica il periodo di attesa di `120` secondi, dopodiché la funzione *Auto-disable* riabilita la porta.
`exit`	Passare alla modalità di configurazione.
`auto-disable reason crc-error`	Attivare la funzione CRC di disabilitazione automatica
`port-monitor condition crc-fragments mode`	Attivare la condizione di frammenti CRC per attivare un'azione.
`port-monitor operation`	Attivare la funzione *Port Monitor*.

Quando il dispositivo disabilita una porta a causa di violazioni delle soglie, consente di utilizzare i seguenti comandi per resettare manualmente la porta disabilitata.

Eseguire i seguenti passaggi:

`enable`	Passare alla modalità Privileged EXEC.

```
configure
```
Passare alla modalità di configurazione.

```
interface 1/1
```
Passare alla modalità di configurazione di interfaccia `1/1`.

```
auto-disable reset
```
Consente di abilitare la porta prima che il timer conti in senso decrescente.

14.8 Visualizzazione dello stato SFP

La visualizzazione di stato SFP consente di visualizzare le connessioni correnti del modulo SFP e delle rispettive proprietà. Le proprietà includono:

- Tipo di modulo
- Numero di serie del modulo media
- Temperatura in ° C
- Potenza di trasmissione in mW
- Potenza di ricezione in mW

Eseguire il seguente passaggio:

1. Aprire la finestra di dialogo *Diagnostics > Ports > SFP*.

14.9 Riconoscimento della topologia

IEEE 802.1AB definisce il Link Layer Discovery Protocol (LLDP). Il protocollo LLDP consente di rilevare automaticamente la topologia della rete LAN.

Dispositivi con LLDP attivo:
- Trasmettono le proprie informazioni di connessione e gestione ai dispositivi adiacenti sulla LAN condivisa. Quando il dispositivo ricevente ha attiva la funzione *LLDP*, si verifica la valutazione dei dispositivi.
- Ricevono le informazioni di connessione e gestione dai dispositivi adiacenti sulla LAN condivisa, a condizione che questi dispositivi adiacenti abbiano anch'essi LLDP attivo.
- Compila un database di informazioni di gestione e definizioni oggetto per la memorizzazione delle informazioni sui dispositivi adiacenti con LLDP attivo.

Come l'elemento principale, le informazioni di connessione contengono un identificatore esatto, univoco per l'endpoint di connessione: MAC (Service Access Point). Si tratta di un identificatore dispositivo che è univoco sull'intera rete e un identificatore porta univoco per questo dispositivo.
- Identificativo chassis (rispettivo indirizzo MAC)
- Identificativo porta (rispettivo indirizzo MAC di porta)
- Descrizione della porta
- Nome sistema
- Descrizione del sistema
- Funzionalità sistema supportate
- Funzionalità sistema attualmente attiva
- ID d'interfaccia dell'indirizzo di gestione
- ID VLAN della porta
- Stato di autonegoziazione sulla porta
- Impostazione mezzo, half/full duplex e impostazione della velocità porta
- Informazione in merito alle VLAN installate nel dispositivo (ID VLAN e nome della VLAN; indipendentemente dal fatto che la porta sia un partecipante della VLAN).

Una network management station può richiamare queste informazioni dai dispositivi con LLDP attivato. Grazie a queste informazioni, la stazione di gestione della rete è in grado di descrivere graficamente la topologia della rete.

Normalmente, i dispositivi non-LLDP bloccano l'indirizzo MAC IEEE LLDP Multicast speciale utilizzato per lo scambio di informazioni. Pertanto, i dispositivi non-LLDP scartano i pacchetti LLDP. Se si posiziona un dispositivo che supporta non-LLDP tra 2 dispositivi che supportano LLDP, il dispositivo che supporta non-LLDP proibisce gli scambi di informazioni tra i 2 dispositivi che supportano°LLDP.

Il Management Information Base (MIB) per un dispositivo che supporta l'LLDP trattiene le informazioni LLDP nell'lldp MIB e in SA2-LLDP-EXT-HM-MIB e SA2-LLDP-MIB privati.

14.9.1 Visualizzazione dei risultati del riconoscimento della topologia

Visualizzare la topologia della rete. A tale scopo, eseguire i seguenti passaggi:

☐ Aprire la finestra di dialogo *Diagnostics > LLDP > Topology Discovery*, scheda *LLDP*.

Quando si utilizza una porta per connettere diversi dispositivi, ad esempio tramite un hub, la tabella contiene una riga per ogni dispositivo connesso.

Attivando la visualizzazione delle voci FDB nella parte inferiore della tabella consente di visualizzare i dispositivi senza supporto LLDP attivo nella tabella. In questo caso, il dispositivo comprende anche informazioni del rispettivo FDP (forwarding database).

Se si connette la porta ai dispositivi con la funzione di riconoscimento della topologia, i dispositivi scambiano unità dati LLDP (LLDPDU) e la tabella topologia visualizza questi dispositivi adiacenti.

Quando una porta connette solo dispositivi senza un riconoscimento della topologia attivo, la tabella contiene una riga per questa porta al fine di rappresentare i dispositivi connessi. La ria contiene il numero di dispositivi connessi.

La tabella di indirizzi dell'FDB contiene indirizzi MAC dei dispositivi che la tabella topologia contiene per chiarezza.

14.9.2 LLDP-MED

LLDP per Media Endpoint Devices (LLDP-MED) è un'estensione di LLDP che funziona tra i dispositivi endpoint. Gli endpoint includono dispositivi quali telefoni IP, o altri dispositivi Voice over IP (VoIP) oppure server e dispositivi di rete quali gli switch. Fornisce specificamente il supporto per applicazioni VoIP. LLDP-MED fornisce questo supporto utilizzando un set supplementare di messaggi di annuncio type-length-value (TLV), per il riconoscimento delle funzionalità, i criteri di rete, Power over Ethernet, gestione inventario e informazioni di posizione.

Il dispositivo supporta i seguenti messaggi TLV:
- Funzionalità TLV
  Consente agli endpoint LLDP-MED di determinare le funzionalità che il dispositivo connesso supporta e quali funzionalità il dispositivo ha abilitato.
- TLV criteri di rete
  Consente sia ai dispositivi di connettività di rete che agli endpoint di annunciare configurazioni VLAN e gli attributi associati per l'applicazione specifica sul quella porta. Ad esempio, il dispositivo notifica ad un telefono il numero della VLAN. Il telefono si connette a uno switch, ottiene il numero della VLAN, e poi avvia la comunicazione con il controllo di chiamata.

LLDP-MED fornisce le seguenti funzioni:
- Riconoscimento dei criteri di rete, compresi ID VLAN, priorità 802.1p e Diffserv code point (DSCP)
- Posizione del dispositivo e riconoscimento della topologia sulla base di informazioni MAC/porta a livello di LAN
- Notifica di rilevamento spostamento endpoint, dal dispositivo di connettività di rete all'applicazione di gestione VoIP associata
- Identificazione del dispositivo estesa per la gestione inventario
- Identificazione delle funzionalità di connettività di rete endpoint, ad esempio, telefono IP multiporta con switch incorporato o funzionalità bridge
- Interazioni del livello di applicazione con gli elementi del protocollo LLDP per fornire l'avvio puntuale di LLDP per supportare una disponibilità rapida in caso di servizio chiamata di emergenza
- Applicabilità di LLDP-MED ad ambienti wireless LAN, supporto per Voice over wireless LAN

14.10 Rilevamento di loop

I loop nella rete provocano interruzioni di connessione o perdita di dati. Questa condizione si applica anche ai loop temporanei. Il rilevamento e la segnalazione automatici di questa situazione, ne consentono una più rapida individuazione e una più facile diagnosi.

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per favorire l'assenza di loop durante la fase di configurazione, configurare ogni dispositivo dell'anello in modo individuale. Prima di connettere le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione ad anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Una configurazione non corretta causa loop, ad esempio, disattivando lo spanning tree.

Il dispositivo consente di rilevare i tipici effetti causati da loop e di segnalare automaticamente tale situazione alla network management station. Qui è disponibile l'opzione di specificare la portata degli effetti di loop che attivano l'invio di un rapporto da parte del dispositivo.

I frame BPDU inviati dalla porta designata e ricevuti su una porta differente dello stesso dispositivo oppure sulla stessa porta entro un breve periodo di tempo, sono un tipico effetto di un loop.

Per verificare sei il dispositivo ha rilevato un loop, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, scheda *CIST*.
- ☐ Verificare il valore nei campi *Port state* e *Port role*. Se il campo *Port state* visualizza il valore `discarding` e il campo *Port role* visualizza il valore `backup`, la porta è in uno stato di loop.

oppure

- ☐ Aprire la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, scheda *Guards*.
- ☐ Verificare il valore nella colonna *Loop state*. Se il campo visualizza il valore `true`, la porta è in uno stato di loop.

14.11 Contribuire a proteggere da loop di rete di Layer 2.

Il dispositivo contribuisce a proteggere da loop di rete di Layer 2.

Un loop di rete può causare un blocco della rete per sovraccarico. Una possibile motivazione è la continua duplicazione dei pacchetti dati a causa di una configurazione errata. La causa potrebbe essere, ad esempio, un cavo collegato in modo errato o impostazioni nel dispositivo sbagliate.

Ad esempio, se non sono attivi protocolli di ridondanza, un loop di rete di Layer 2 può verificarsi nei seguenti casi:
- Due porte dello stesso dispositivo sono direttamente collegate l'una con l'altra.
- Si stabilisce più di una connessione attiva tra due dispositivi.

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per contribuire a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della rete di Layer 2. Prima di collegare le linee ridondanti, completare la configurazione degli altri dispositivi della rete di Layer 2.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

14.11.1 Esempio di applicazione

La figura mostra esempi dei possibili loop di Layer 2 in una rete. La funzione *Loop Protection* è abilitata in tutti i dispositivi.

▶ **A**: *Modalità active*
Le porte che devono collegare i dispositivi finali funzionano in modalità *active*. Il dispositivo valuta e invia i pacchetti di *rilevazione loop* su queste porte.

- **P**: *Modalità passive*
  Le porte che appartengono agli anelli ridondanti funzionano in modalità *passive*. Il dispositivo valuta solo i pacchetti di *rilevazione loop* su queste porte.
- **Loop 1**..**Loop 4**
  Loop di rete di Layer 2 configurati inavvertitamente.

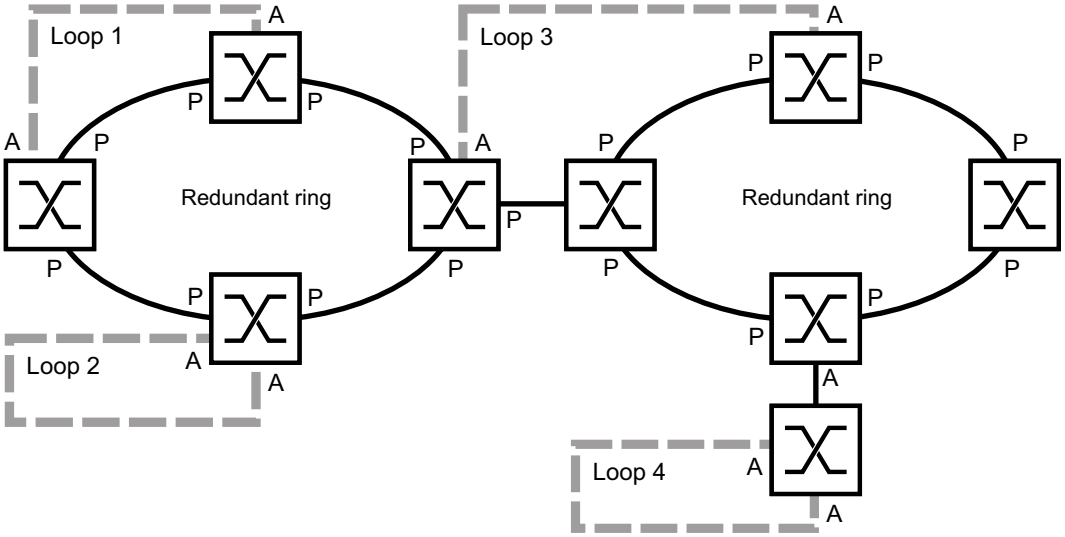


Figura 73: Esempi di loop di rete di Layer 2 imprevisti

Assegnare le impostazioni Loop Protection alle porte

Per ogni porta *attiva* e *passiva* assegnare le impostazioni della funzione *Loop Protection*.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Loop Protection*.
- ☐ Se necessario adeguare il valore nel riquadro *Global*, campo *Transmit interval*.
- ☐ Se necessario adeguare il valore nel riquadro *Global*, campo *Receive threshold*.
- ☐ Nella colonna *Mode* specificare il comportamento della funzione *Loop Protection* sulla porta:
  - `active` per le porte destinate a collegare i dispositivi finali
  - `passive` per le porte che appartengono agli anelli ridondanti
- ☐ Nella colonna *Action* specificare il valore *all*.
  Se il dispositivo rileva un loop di Layer 2 su questa porta, invia una trap e disabilita la porta utilizzando la funzione *Auto-Disable*. Se necessario, adeguare il valore.
- ☐ Nella colonna *Active*, selezionare la casella di spunta.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`loop-protection tx-interval 5`	Se necessario specificare l'intervallo di trasmissione.
`loop-protection rx-threshold 1`	Se necessario specificare la soglia di ricezione.
`interface 1/1`	Passare alla modalità di interfaccia. Esempio: porta *1/1*.

`loop-protection mode active`	Specificare la modalità `active` per le porte destinate a collegare i dispositivi finali.
`loop-protection mode passive`	Specificare la modalità `passive` per le porte che appartengono agli anelli ridondanti.
`loop-protection action all`	Specificare l'azione che il dispositivo esegue se rileva un loop di rete di Layer 2 su questa porta.
`loop-protection operation`	Attivare la funzione *Loop Protection* sulla porta.
`exit`	Passare alla modalità di configurazione.

Attivare la funzione Auto-Disable

Dopo aver assegnato le impostazioni *Loop Protection* alle porte, attivare la funzione *Auto-Disable*.

Eseguire i seguenti passaggi:

- ☐ Nel riquadro *Configuration* selezionare la casella di spunta *Auto-disable*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`loop-protection auto-disable`	Attivare la funzione *Auto-Disable*.

Abilitare la funzione Loop Protection nel dispositivo

Conclusa la procedura, abilitare la funzione *Loop Protection* nel dispositivo.

Eseguire i seguenti passaggi:

- ☐ Nel riquadro *Operation* selezionare il pulsante di opzione *On*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`loop-protection operation`	Abilitare la funzione *Loop Protection* nel dispositivo.

14.11.2 Raccomandazioni per le porte ridondanti

In base alle impostazioni *Loop Protection*, il dispositivo disabilita le porte utilizzando la funzione *Auto-Disable* se rileva un loop di rete di Layer 2.

Se su una porta è attiva una funzione di ridondanza, non attivare la modalità *active* su tale porta. In caso contrario può verificarsi la disattivazione della porta sui percorsi di rete ridondanti. Nell'esempio riportato sopra si tratta delle porte che appartengono agli anelli ridondanti.

Verificare che un percorso di rete ridondante sia disponibile come supporto di backup. Il dispositivo passa al percorso ridondante se il percorso primario non è disponibile.

Le seguenti impostazioni contribuiscono a evitare la disattivazione della porta sui percorsi di rete ridondanti:

- ☐ Disabilitare la funzione *Loop Protection* sulle porte ridondanti.
  oppure
- ☐ Abilitare la modalità *passive* sulle porte ridondanti.

La funzione *Loop Protection* e la funzione *Spanning Tree* hanno un effetto l'una sull'altra. I seguenti passaggi contribuiscono a evitare un comportamento imprevisto del dispositivo:

- ☐ Disabilitare la funzione *Spanning Tree* sulla porta su cui si desidera abilitare la funzione *Loop Protection*. Vedere la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, colonna *STP active*.
- ☐ Disabilitare la funzione *Spanning Tree* sulla porta collegata di ciascun dispositivo collegato. Vedere la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree*.

14.12 Utilizzo della funzione Email Notification

Il dispositive consente di informare gli utenti sugli eventi che si sono verificati tramite e-mail. Il prerequisito è che un server di posta sia disponibile nella rete su cui il dispositivo trasmette le e-mail.

Per impostare l'invio delle e-mail da parte del dispositivo, eseguire i passaggi dei seguenti capitoli:
- ☐ Specificare l'indirizzo del mittente
- ☐ Specificare gli eventi che determinano la notifica
- ☐ Specificare i destinatari
- ☐ Specificare il server di posta
- ☐ Abilitare/disabilitare la funzione Email Notification
- ☐ Inviare un'e-mail di prova

14.12.1 Specificare l'indirizzo del mittente

L'indirizzo del mittente è l'indirizzo e-mail che indica il dispositivo che ha inviato l'e-mail. Nel dispositivo, l'impostazione di default è .

Modificare il valore attuale. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Email Notification > Global*.
- ☐ Nel riquadro *Sender*, modificare il valore nel campo *Address*.
  Aggiungere un indirizzo e-mail valido.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`logging email from-addr <user@doma.in>`	Modificare l'indirizzo del mittente.

14.12.2 Specificare gli eventi che determinano la notifica

Il dispositivo differenzia tra i seguenti livelli di gravità:

Tabella 58:Significato del livello di gravità degli eventi

Livello di gravità	Significato
`emergency`	Il dispositivo non è pronto per il funzionamento
`alert`	È richiesto l'intervento immediato dell'utente
`critical`	Stato critico
`error`	Stato di errore
`warning`	Avvertenza
`notice`	Stato normale, significativo
`informational`	Messaggio informale
`debug`	Messaggio di debug

È possibile specificare gli eventi per i quali il dispositivo informa l'utente. A tale scopo, assegnare il livello minimo di gravità desiderato ai livelli di notifica del dispositivo.

Il dispositivo informa i destinatari come indicato di seguito:

- *Notification immediate*
  Se si verifica un evento con il livello di gravità assegnato o superiore, il dispositivo invia un'e-mail immediatamente.
- *Notification periodic*
  - Se si verifica un evento con il livello di gravità assegnato o superiore, il dispositivo registra l'evento in un buffer.
  - Il dispositivo invia un'e-mail con il file di registro periodicamente o quando il buffer è pieno.
  - Se si verifica un evento di gravità inferiore, il dispositivo non lo registra.

Eseguire i seguenti passaggi:

☐ Aprire la finestra di dialogo *Diagnostics > Email Notification > Global*.

Nel riquadro *Notification immediate*, specificare le impostazioni per le e-mail che il dispositivo invia immediatamente.

☐ Nel campo *Severity*, specificare il livello di gravità minimo.
☐ Nel campo *Subject*, specificare l'oggetto dell'e-mail.

Nel riquadro *Notification periodic*, specificare le impostazioni per le e-mail che il dispositivo invia periodicamente.

☐ Nel campo *Severity*, specificare il livello di gravità minimo.
☐ Nel campo *Subject*, specificare l'oggetto dell'e-mail.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`logging email severity immediate <level>`	Specifica il livello di gravità minimo degli eventi per cui il dispositivo invia un'e-mail immediatamente.
`logging email severity periodic <level>`	Specifica il livello di gravità minimo degli eventi per cui il dispositivo invia un'e-mail periodicamente.
`logging email subject add <immediate | periodic> TEXT`	Crea una linea oggetto con contenuto `TEXT`.

14.12.3 Modificare l'intervallo di invio

Il dispositivo consente di specificare l'intervallo nel quale invia le e-mail con il file di registro. L'impostazione di default è `30` minuti.

Eseguire i seguenti passaggi:

☐ Aprire la finestra di dialogo *Diagnostics > Email Notification > Global*.

Nel riquadro *Notification periodic*, specificare le impostazioni per le e-mail che il dispositivo invia periodicamente.

☐ Modificare il valore nel campo *Sending interval [min]* per modificare l'intervallo.

☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`logging email duration <30..1440>`	Specifica l'intervallo nel quale il dispositivo invia le e-mail con il file di registro.

14.12.4 Specificare i destinatari

Il dispositivo consente di specificare fino a 10 destinatari.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Email Notification > Recipients*.
- ☐ Per aggiungere una voce tabella, fare clic sul pulsante .
- ☐ Nella colonna *Notification type* specificare se il dispositivo invia le e-mail a questo destinatario immediatamente o periodicamente.
- ☐ Nella colonna *Address*, specificare l'indirizzo e-mail del destinatario.
- ☐ Nella colonna *Active*, selezionare la casella di spunta.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`logging email to-addr add <1..10> addr <user@doma.in> msgtype <immediately | periodically>`	Specifica il destinatario con l'indirizzo e-mail `user@doma.in`. Il dispositivo gestisce le impostazioni in memoria `1..10`.

14.12.5 Specificare il server di posta

Il dispositivo supporta le connessioni al server di posta crittografate e non crittografate.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Email Notification > Mail Server*.
- ☐ Per aggiungere una voce tabella, fare clic sul pulsante .
- ☐ Nella colonna *IP address* specificare l'indirizzo IP o il nome DNS del server.
- ☐ Nella colonna *Encryption* specificare il protocollo che crittografa la connessione tra il dispositivo e il server di posta.
- ☐ Se un server di posta utilizza un porta diversa da quella nota, specificare la porta TCP nella colonna *Destination TCP port*.

Se il server di posta richiede un'autenticazione:

- ☐ Nelle colonne *User name* e *Password*, specificare le credenziali dell'account che il dispositivo utilizza per autenticarsi sul server di posta.

- ☐ Nella colonna *Description*, immettere un nome significativo per il server di posta.
- ☐ Nella colonna *Active*, selezionare la casella di spunta.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`logging email mail-server add <1..5> addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]`	Specifica il server di posta con indirizzo IP `IP ADDRESS`. Il dispositivo gestisce le impostazioni in memoria `1..5`.

14.12.6 Abilitare/disabilitare la funzione Email Notification

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Email Notification > Global*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`logging email operation`	Abilita l'invio di e-mail.
`no logging email operation`	Disabilita l'invio di e-mail.

14.12.7 Inviare un'e-mail di prova

Il dispositivo consente di verificare le impostazioni tramite l'invio di un'e-mail di prova.

Prerequisito:
- ▶ Le impostazioni delle e-mail sono specificate completamente.
- ▶ È abilitata la funzione *Email Notification*.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Email Notification > Mail Server*.
- ☐ Fare clic sul pulsante ☰ e poi sulla voce *Connection test*.
  La finestra di dialogo mostra la finestra *Connection test*.
- ☐ Nell'elenco a discesa *Recipient* selezionare a quali destinatari il dispositivo invia l'e-mail di prova.
- ☐ Nel campo *Message text*, specificare il testo dell'e-mail di prova.
- ☐ Fare clic sul pulsante *Ok* per inviare un'e-mail di prova.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`logging email test msgtype <urgent|non-urgent> TEXT`	Invia ai destinatari un'e-mail con il contenuto `TEXT`.

Se non si visualizzano messaggi di errore rilevati e i destinatari ricevono l'e-mail, le impostazioni del dispositivo sono corrette.

14.13 Rapporti

Di seguito un elenco di rapporti e pulsanti disponibili per la diagnostica:
- File di registro di sistema
  Il file di registro è un file HTML in cui il dispositivo scrive gli eventi interni al dispositivo.
- Audit Trail
  Registra i comandi riusciti e i commenti degli utenti. Il file comprende anche il registro SNMP.
- Registrazione continua
  Quando è presente una memoria esterna, il dispositivo salva le voci di registro in un file nella memoria esterna. Questi file sono disponibili dopo lo spegnimento. È possibile configurare le dimensioni massime, il numero massimo di file memorizzabili e la gravità degli eventi registrati. Dopo aver conseguito le dimensioni massime o il numero massimo definiti dall'utente per i file memorizzabili, il dispositivo archivia le voci e avvia un nuovo file. Il dispositivo cancella il vecchio file e rinomina gli altri file per mantener il numero di file configurato. Per riesaminare questi file, utilizzare la Command Line Interface o copiarli su un server esterno come futuro riferimento.
- *Download support information*
  Questo pulsante consente di scaricare le informazioni di sistema sotto forma di archivio ZIP.

In situazioni di assistenza, questi rapporti forniscono al tecnico le informazioni necessarie.

14.13.1 Impostazioni globali

Utilizzando questa finestra di dialogo, si abilita o disabilita la posizione in cui il dispositivo invia rapporti, ad esempio ad una console, ad un server Syslog oppure ad una connessione alla Command Line Interface. Inoltre, si imposta con quale livello di gravità il dispositivo scrive eventi nei rapporti.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Report > Global*.
- ☐ Per inviare un rapporto alla console, specificare il livello desiderato nel riquadro *Console logging*, campo*Severity*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Console logging*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

Il dispositivo bufferizza gli eventi registrati in 2 area di archiviazione separate, in modo che il dispositivo mantenga le voci di registro di eventi urgenti. Specificare la gravità minima per eventi che il dispositivo registra nell'area di archiviazione bufferizzata con una priorità superiore.

Eseguire i seguenti passaggi:

- ☐ Per inviare eventi al buffer, specificare il livello desiderato nel riquadro *Buffered logging*, campo*Severity*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

Quando si attiva la registrazione di richieste SNMP, il dispositivo registra le richieste come eventi nel Syslog. La funzione *Log SNMP get request* registra le richieste dell'utente di informazioni sulla configurazione del dispositivo. La funzione *Log SNMP set request* registra gli eventi di configurazione del dispositivo. Specificare il livello minimo per gli eventi che il dispositivo registra nel Syslog.

Eseguire i seguenti passaggi:

- ☐ Abilitare la funzione *Log SNMP get request* per il dispositivo, in modo da inviare richieste di lettura SNMP come eventi al server Syslog.
  Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *SNMP logging*.
- ☐ Abilitare la funzione *Log SNMP set request* per il dispositivo, in modo da inviare richieste di scrittura SNMP come eventi al server Syslog.
  Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *SNMP logging*.
- ☐ Selezionare il livello di gravità desiderato per le richieste get&set.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

Quando è attivo, il dispositivo registra le modifiche di configurazione effettuate all'audit trail, utilizzando la Command Line Interface. Questa funzionalità si basa sullo standard IEEE 1686 per dispositivi elettronici intelligenti di substazione.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Report > Global*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *CLI logging*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

Il dispositivo consente il salvataggio delle seguenti informazioni di sistema in un unico file ZIP sul proprio PC:

- `audittrail.html`
- `defaultconfig.xml`
- `script`
- `runningconfig.xml`
- `supportinfo.html`
- `systeminfo.html`
- `systemlog.html`

Il dispositivo crea il nome dell'archivio ZIP automaticamente nel formato `<IP_address>_<system_name>.zip`.

Eseguire i seguenti passaggi:

- ☐ Fare clic sul pulsante e poi sulla voce *Download support information*.
- ☐ Selezionare la directory nella quale si desidera salvare le informazioni di supporto.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

14.13.2 Syslog

Il dispositivo consente di inviare messaggi relativi a eventi interni al dispositivo, a uno o più server Syslog (fino a 8). Inoltre, è possibile anche includere le richieste SNMP al dispositivo come eventi nel Syslog.

Nota: Per visualizzare gli eventi registrati, aprire la finestra di dialogo *Diagnostics > Report > Audit Trail* o la finestra di dialogo *Diagnostics > Report > System Log*.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Syslog*.
- ☐ Per aggiungere una voce tabella, fare clic sul pulsante  .
- ☐ Nella colonna *IP address* immettere l'indirizzo IP o *Hostname* del server Syslog.
  È possibile specificare un indirizzo IPv4 o IPv6 valido per il server Syslog.
- ☐ Nella colonna *Destination UDP port*, specificare la porta TCP o UDP sulla quale il server Syslog prevede le voci di registro.
- ☐ Nella colonna *Min. severity*, specificare il livello di gravità minimo che un evento richiede affinché il dispositivo invii una voce di registro al server Syslog.
- ☐ Selezionare la casella di spunta nella colonna *Active*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

Nel riquadro *SNMP logging*, configurare le seguenti impostazioni per richieste di scrittura e lettura SNMP:

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Report > Global*.
- ☐ Abilitare la funzione *Log SNMP get request* per il dispositivo, in modo da inviare richieste di lettura SNMP come eventi al server Syslog.
  Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *SNMP logging*.
- ☐ Abilitare la funzione *Log SNMP set request* per il dispositivo, in modo da inviare richieste di scrittura SNMP come eventi al server Syslog.
  Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *SNMP logging*.
- ☐ Selezionare il livello di gravità desiderato per le richieste get&set.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`logging host add 1 addr 10.0.1.159 severity 3`	Aggiunge un nuovo destinatario nell'elenco dei server Syslog. Il valore `3` specifica il livello di gravità dell'evento che il dispositivo registra. Il valore `3` indica `error`.
`logging host add 2 addr 2001::1 severity 4`	Aggiungere un nuovo destinatario IPv6 nell'elenco dei server Syslog. Il valore `4` indica `warning`.
`logging syslog operation`	Abilitare la funzione *Syslog*.
`exit`	Passare alla modalità Privileged EXEC.

```
show logging host                          Visualizzare le impostazioni host Syslog.
No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active
2      2001::1        514    warning         systemlog   active
configure                                  Passare alla modalità di configurazione.
logging snmp-requests get operation        Registra le richieste SNMP GET.
logging snmp-requests get severity 5       Il valore 5 specifica il livello di gravità dell'evento
                                           che il dispositivo registra in caso di richieste SNMP
                                           GET. Il valore 5 indica notice.
logging snmp-requests set operation        Registra le richieste SNMP SET.
logging snmp-requests set severity 5       Il valore 5 specifica il livello di gravità dell'evento
                                           che il dispositivo registra in caso di richieste SNMP
                                           SET. Il valore 5 indica notice.
exit                                       Passare alla modalità Privileged EXEC.
show logging snmp                          Visualizzare le impostazioni del registro SNMP.
Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

14.13.3 Registro di sistema

Il dispositivo consente di richiamare un file di registro degli eventi di sistema. La tabella nella finestra di dialogo *Diagnostics > Report > System Log*.

Eseguire i seguenti passaggi:

- ☐ Per aggiornare il contenuto del registro, fare clic sul pulsante .
- ☐ Per salvare il contenuto del registro come file html, fare clic sul pulsante e poi sulla voce *Reset*.
- ☐ Per cancellare il contenuto del registro, fare clic sul pulsante e poi sulla voce *Reset*.
- ☐ Per interrogare il contenuto del registro per cercare una parola chiave, utilizzare la funzione di ricerca del browser web dell'utente.

Nota: Esiste anche l'opzione di inviare gli eventi registrati ad uno o più server Syslog.

14.13.4 Syslog tramite TLS

Il Transport Layer Security (TLS) è un protocollo crittografico pensato per consentire una comunicazione sicura su una rete di computer. L'obiettivo primario del protocollo TLS è fornire privacy e integrità dei dati tra due applicazioni informatiche in comunicazione.

Dopo l'avviamento di una connessione con un server Syslog, il dispositivo convalida il certificato ricevuto dal server utilizzando un handshake TLS. A tale scopo, trasferire il certificato PEM da un server remoto o da una memoria esterna al dispositivo. Verificare che l'indirizzo IP o il nome DNS del server configurato corrisponda alle informazioni riportate nel certificato. Le informazioni si trovano nei campi Common Name o Subject Alternative Name del certificato.

Il dispositivo invia i messaggi Syslog crittografati con TLS attraverso la porta TCP specificata nella colonna *Destination UDP port*.

Nota: Specificare l'indirizzo IP o il nome DNS sul server in modo che corrisponda all'indirizzo IP o al nome DNS specificato nel certificato del server. I valori immessi si trovano nel certificato, indicati come Common Name oppure Subject Alternative Name.

Esempio

L'esempio dato descrive la configurazione della funzione *Syslog*. Eseguendo questi passaggi il dispositivo consente di inviare i messaggi Syslog crittografati con TLS attraverso la porta TCP specificata nella colonna *Destination UDP port*.

I messaggi Syslog inviati da un dispositivo a un server Syslog possono attraversare reti non protette. Per configurare un server Syslog tramite TLS, trasferire il certificato dell'autorità di certificazione (CA) sul dispositivo.

Nota: Per abilitare le modifiche dopo il caricamento di un nuovo certificato, riavviare la funzione *Syslog*.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Syslog*.
- ☐ Per avviare la connessione con i server Syslog, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✔.

Il dispositivo convalida il certificato ricevuto. Inoltre, il dispositivo autentica il server e avvia l'invio di messaggi Syslog.

- ☐ Trasferire il certificato PEM dal server remoto o da una memoria esterna al dispositivo.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`logging host add 1 addr 192.168.3.215`	Aggiungere l'indice `1` al server Syslog con indirizzo IPv4`192.168.3.215`.
`logging host add 2 addr 2001::1`	Aggiungere l'indice `2` al server Syslog con indirizzo IPv6`2001::1`..
`logging host modify 1 port 6512 type systemlog`	Specificare il numero di porta `6512` e registrare gli eventi nel registro di sistema.
`logging host modify 1 transport tls`	Specificare il tipo di trasmissione come `tls`.

`logging host modify 1 severity informational`	Specificare il tipo di evento da registrare nel registro di sistema come `informational`.
`exit`	Passare alla modalità Privileged EXEC.
`copy syslogcacert evmm`	Copiare i certificati CA dalla memoria esterna al dispositivo.
`show logging host`	Visualizzare le impostazioni host Syslog.

14.13.5 Audit Trail

La finestra di dialogo *Diagnostics > Report > Audit Trail* contiene le informazioni di sistema e le modifiche alla configurazione del dispositivo effettuate tramite Command Line Interface ed SNMP. In caso di modifiche della configurazione del dispositivo, la finestra di dialogo visualizza chi ha cambiato che cosa e quando.

La finestra di dialogo *Diagnostics > Syslog* consente di specificare fino a 8 server Syslog a cui il dispositivo invia Audit Trail.

Il seguente elenco contiene gli eventi di registro:
- Modifiche dei parametri di configurazione
- Comandi (a eccezione dei comandi `show`) utilizzando la Command Line Interface.
- Comando `logging audit-trail <string>` utilizzando la Command Line Interface che registra il commento.
- Modifiche automatiche dell'orario di sistema
- Eventi watchdog
- Bloccaggio di un utente dopo diversi tentativi di accesso non riusciti
- Accesso utente, locale o remoto, utilizzando la Command Line Interface.
- Disconnessione avviata dall'utente, manuale
- Disconnessione a tempo dopo un periodo di inattività definito dall'utente nella Command Line Interface.
- Operazione di trasferimento di file, compresi un update del firmware
- Modifiche della configurazione utilizzando Ethernet Switch Configurator
- Configurazione automatica o aggiornamenti firmware utilizzando la memoria esterna
- Blocco dell'accesso alla gestione del dispositivo dovuto a tentativi di accesso non validi
- Riavvio
- Apertura e chiusura di SNMP tramite tunnel HTTPS
- Rilevati guasti di alimentazione

14.14 Analisi di rete con TCPdump

Tcpdump è un'utility UNIX di analisi pacchetti, utilizzata dagli amministratori di rete per analizzare e valutare il traffico su una rete. Alcune delle ragioni per analizzare il traffico su una rete, è verificare la connettività tra host, oppure per analizzare il traffico che attraversa la rete.

TCPDump nel dispositivo offre la possibilità di decodificare o acquisire i pacchetti ricevuti e trasmessi dalla CPU di gestione. Questa funzione è disponibile utilizzando il comando `debug`. Consultare il manuale di riferimento “Command Line Interface” per ulteriori informazioni sulla funzione TCPDump.

14.15 Monitoraggio del traffico dati

Il dispositivo consente di inoltrare i pacchetti di dati che passano attraverso il dispositivo ad una porta di destinazione. Qui è possibile monitorare e valutare i pacchetti di dati.

Il dispositivo offre le seguenti opzioni:
- Port Mirroring

14.15.1 Port Mirroring

La funzione *Port Mirroring* consente la copia dei pacchetti di dati dalle porte di una origine fisica ad una porta di destinazione fisica.

Monitorare il traffico dati sulle porte di origine nelle direzioni di invio e ricezione con uno strumento di gestione connesso alla porta di destinazione, ad esempio una sonda RMON. La funzione non ha effetto sul traffico dati sulle porte di origine.

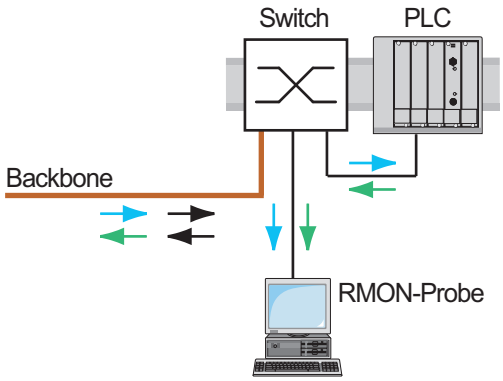


Figura 74: Esempio

Sulla porta di destinazione, il dispositivo inoltra solamente i pacchetti di dati copiati dalle porte sorgente.

Prima di attivare la funzione *Port Mirroring*, selezionare la casella di spunta *Allow management* per accedere alla gestione del dispositivo tramite la porta di destinazione. Il dispositivo consente agli utenti l'accesso alla gestione del dispositivo utilizzando la porta di destinazione senza interrompere la sessione *Port Mirroring* attiva.

Nota: Il dispositivo duplica multicast, broadcast e unicast sconosciuti sulla porta di destinazione.

Le impostazioni VLAN sulla porta di destinazione rimangono invariate. Il prerequisito per l'accesso alla gestione del dispositivo sulla porta di destinazione è che la porta di destinazione faccia parte della VLAN di gestione del dispositivo.

Attivazione della funzione Port Mirroring

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > Ports > Port Mirroring*.
- ☐ Specificare le porte sorgente.
  Selezionare la casella di spunta nella colonna *Enabled* per le porte rilevanti.
- ☐ Specificare la porta di destinazione.
  Nel riquadro *Destination port*, selezionare la porta desiderata nell'elenco a discesa *Primary port*.
  L'elenco a discesa visualizza solamente le porte disponibili. Le porte che sono già specificate come porte sorgente non sono disponibili.
- ☐ Se necessario, specificare una seconda porta di destinazione.
  Nel riquadro *Destination port*, selezionare la porta desiderata nell'elenco a discesa *Secondary port*.
  Il prerequisito è che sia già specificata la porta di destinazione primaria.
- ☐ Per accedere alla gestione del dispositivo tramite la porta di destinazione:
  Nel riquadro *Destination port*, selezionare la casella di spunta *Allow management*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

Per disattivare la funzione *Port Mirroring*, fare clic sul pulsante e poi sulla voce *Reset config*.

14.16 Test automatico

Il dispositivo verifica le sue risorse durante il processo di avvio e occasionalmente anche in un secondo momento. Il dispositivo verifica la disponibilità o la conclusione di attività di sistema e la quantità di memoria disponibile. Inoltre, il dispositivo verifica nel processore la funzionalità dell'applicazione e qualsiasi riduzione delle prestazioni dell'hardware.

Se il dispositivo rileva una perdita di integrità, il dispositivo reagisce alla riduzione delle prestazioni con un'azione definita dall'utente. Le seguenti categorie sono disponibili per la configurazione.

- `task`
  Azione da eseguire in caso di attività non riuscita.
- `resource`
  Azione da eseguite a causa della mancanza di risorse.
- `software`
  Azione eseguita per perdita di integrità del software; ad esempio, checksum del segmento codice o violazioni in accesso.
- `hardware`
  Azione eseguita a causa della riduzione delle prestazioni dell'hardware

Configurare ogni categoria per produrre un'azione in caso il dispositivo rilevi una perdita di integrità. Le seguenti azioni sono disponibili per la configurazione.

- `log only`
  Questa azione scrive un messaggio per il file di registro.
- `send trap`
  Invia una trap SNMP alla destinazione della trap.
- `reboot`
  Se attivato, un errore rilevato nella categoria causerà il riavvio del dispositivo.

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Diagnostics > System > Selftest*.
- ☐ Nella colonna *Action*, specificare l'azione da eseguire per una causa.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`selftest action task log-only`	Per inviare un messaggio al registro dell'evento quando un'attività non è riuscita.
`selftest action resource send-trap`	Quando vi sono risorse insufficienti, inviare una trap SNMP.
`selftest action software send-trap`	Quando si è persa l'integrità del software, inviare una trap SNMP.
`selftest action hardware reboot`	Per riavviare il dispositivo quando si verifica la riduzione delle prestazioni dell'hardware.

Disabilitare queste funzioni consente di ridurre il tempo necessario per riavviare il dispositivo dopo un avvio a freddo. Queste opzioni sono disponibili nella finestra di dialogo *Diagnostics > System > Selftest*, riquadro *Configuration*.

- *RAM test*
  Attiva/disattiva la funzione *RAM test* durante un avvio a freddo.

- *SysMon1 is available*
  Attiva/disattiva la funzione System Monitor durante un avvio a freddo.
- *Load default config on error*
  Attiva/disattiva il caricamento della configurazione del dispositivo di default nel caso in cui, durante un riavvio, non sia disponibile alcuna configurazione leggibile.

Le seguenti impostazioni bloccano l'accesso al dispositivo in modo permanente nel caso in cui il dispositivo non rilevi nessun profilo di configurazione leggibile al riavvio.
- La casella di spunta *SysMon1 is available* è impostata su unmarked (Non selezionato).
- La casella di spunta *Load default config on error* è impostata su unmarked (Non selezionato).

Questo è ad esempio il caso quando la password del profilo di configurazione che si sta caricando differisce dalla password impostata nel dispositivo. Per avere di nuovo il dispositivo sbloccato, contattare il partner delle vendite.

Eseguire i seguenti passaggi:

`selftest ramtest`	Abilitare il test automatico RAM all'avvio a freddo.
`no selftest ramtest`	Disabilitare la funzione “ramtest”.
`selftest system-monitor`	Abilitare la funzione “SysMon1”.
`no selftest system-monitor`	Disabilitare la funzione “SysMon1”.
`show selftest action`	Mostrare lo stato delle azioni da eseguire in caso di riduzione delle prestazioni del dispositivo.
`show selftest settings`	Visualizzare le impostazioni per “ramtest” e “SysMon” nel caso di un avvio a freddo.

14.17 Test dei cavi in rame

Utilizzare questa funzione per sottoporre a test i cavi in rame collegati a un'interfaccia per un corto-circuito o un circuito aperto. I test interrompe il flusso del traffico, quando è in corso, su questa porta.

La tabella visualizza lo stato e le lunghezze di ogni singolo doppino. Il dispositivo restituisce un risultato con il seguente significato:

- normale - indica che il cavo funziona correttamente
- aperto - indica un'interruzione nel cavo
- cortocircuito - indica un cortocircuito nel cavo
- non testato - indica un cavo non sottoposto a test
- Sconosciuto - cavo scollegato

15 Funzioni avanzate del dispositivo

15.1 Utilizzo del dispositivo come un server DHCP

Un server DHCP (“Dynamic Host Configuration Protocol”) assegna indirizzi IP, Gateways, e altre definizioni di rete quai parametri DNS ed NTP ai client.

Le operazioni DHCP rientrano in 4 fasi base: riconoscimento IP, IP lease offer, richiesta IP, e riconoscimento IP lease. Utilizzare l'acronimo DORA, che significa Discovery, Offer, Request e Acknowledgement per aiutarsi a ricordare le fasi. Il server riceve i dati client sulla porta UDP 67 e inoltra i dati al client sulla porta UDP 68.

Il server DHCP fornisce un pool di indirizzi IP o “pool” da cui assegna indirizzi IP ai client. Il pool è composto da un elenco di voci. Una voce definisce un indirizzo IP specifico oppure un intervallo di indirizzi IP.

Il dispositivo consente di attivare il server DHCP globalmente e per interfaccia.

15.1.1 Indirizzi IP assegnati per porta o per VLAN

Il server DHCP assegna un indirizzo IP statico oppure un intervallo dinamico di indirizzi IP ad un client connesso ad una porta o ad una VLAN. Il dispositivo consente la creazione di voci per una porta o una VLAN. Quando si crea una voce per assegnare un indirizzo IP ad una VLAN, la voce della porta viene visualizzata in grigio. Quando si crea una voce per assegnare un indirizzo IP ad una porta, la voce VLAN viene visualizzata in grigio.

Con il termine di allocazione statica, si intende che il server DHCP assegna lo stesso indirizzo IP ad uno specifico client. Il server DHCP identifica il client usando un ID hardware univoco. Una voce indirizzo statica contiene un indirizzo IP e lo applica ad una porta o alla VLAN su cui il server riceve una richiesta da un client specifico. Per un'allocazione statica, creare una voce pool per le porte o per una specifica porta, immettere l'indirizzo IP e lasciare vuota la colonna *Last IP address*. Specificare un ID hardware con il quale il server DHCP identifica univocamente il client. Questo ID è un indirizzo MAC, un client ID, un ID remoto o un ID circuito. Se un client contatta il server con l'ID hardware configurato, il server DHCP alloca l'indirizzo IP statico.

Il dispositivo consente anche di assegnare un intervallo di indirizzi IP dinamici a porte o VLAN da cui il server DHCP alloca un indirizzo IP libero da un pool. Per aggiungere una voce pool dinamica per le porte o VLAN, specificare il primo e l'ultimo indirizzo IP per l'intervallo di indirizzi IP, lasciando le colonne *MAC address*, *Client ID*, *Remote ID* e *Circuit ID* vuote. Creare più voci pool consente di avere intervalli di indirizzi IP che contengono buchi.

15.1.2 Esempio di indirizzo IP statico per il server DHCP

In questo esempio, configurare il dispositivo per allocare un indirizzo IP statico ad una porta. Il dispositivo riconosce cliente con un'identificazione hardware univoca. In questo caso, l'ID hardware è l'indirizzo MAC del client `00:24:E8:D6:50:51`. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Advanced > DHCP Server > Pool*.
- ☐ Per aggiungere una voce tabella, fare clic sul pulsante  .
- ☐ Nella colonna *IP address*, specificare il valore `192.168.23.42`.
- ☐ Nella colonna *Port*, specificare il valore `1/1`.
- ☐ Nella colonna *MAC address*, specificare il valore `00:24:E8:D6:50:51`.
- ☐ Per assegnare l'indirizzo IP al client all'infinito, nella colonna *Lease time [s]* specificare il valore `4294967295`.
- ☐ Selezionare la casella di spunta nella colonna *Active*.
- ☐ Aprire la finestra di dialogo *Advanced > DHCP Server > Global*.
- ☐ Per la porta `1/1`, selezionare la casella di spunta nella colonna *DHCP server active*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`dhcp-server pool add 1 static 192.168.23.42`	Creare una voce con indice `1` e aggiungere l'indirizzo IP `192.168.23.42` al pool statico.
`dhcp-server pool modify 1 mode interface 1/1`	Assegnare l'indirizzo statico nell'indice `1` all'interfaccia `1/1`.
`dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51`	Assegnare l'indirizzo IP nell'indice `1` al dispositivo con l'indirizzo MAC `00:24:E8:D6:50:51`.
`dhcp-server pool mode 1`	Abilitare la voce pool indice `1`.
`dhcp-server pool modify 1 leasetime infinite`	Per allocare l'indirizzo IP al client all'infinito, modificare la voce con indice `1`.
`dhcp-server operation`	Abilitare il server DHCP globalmente.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`dhcp-server operation`	Attivare la funzione server *DHCP Server* su questa porta.

15.1.3 Esempio di intervalli di indirizzi IP dinamici per il server DHCP

Il dispositivo consente la creazione di intervalli di indirizzi IP dinamici. Lasciare i campi *MAC address*, *Client ID*, *Remote ID* e *Circuit ID* vuoti. Per creare intervalli di indirizzi IP dinamici con buchi, tra gli intervalli aggiungere diverse voci alla tabella. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Advanced > DHCP Server > Pool*.
- ☐ Per aggiungere una voce tabella, fare clic sul pulsante  .
- ☐ Nella colonna *IP address*, specificare il valore `192.168.23.92`. Questo è il primo indirizzo IP dell'intervallo.
- ☐ Nella colonna *Last IP address*, specificare il valore `192.168.23.142`. Questo è l'ultimo indirizzo IP dell'intervallo.

Nella colonna *Lease time [s]*, l'impostazione di default è 60 giorni.

- ☐ Nella colonna *Port*, specificare il valore `1/2`.
- ☐ Selezionare la casella di spunta nella colonna *Active*.
- ☐ Aprire la finestra di dialogo *Advanced > DHCP Server > Global*.
- ☐ Per la porta `1/2`, selezionare la casella di spunta nella colonna *DHCP server active*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142`	Aggiungere un pool dinamico con un intervallo IP da `192.168.23.92` a `192.168.23.142`.
`dhcp-server pool modify 2 leasetime {seconds | infinite}`	Immettere il Lease Time in secondi o all'infinito.
`dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180`	Aggiungere un pool dinamico con un intervallo IP da `192.168.23.172` a `192.168.23.180`.
`dhcp-server pool modify 3 leasetime {seconds | infinite}`	Immettere il Lease Time in secondi o all'infinito.
`dhcp-server pool mode 2`	Abilitare la voce pool indice `2`.
`dhcp-server pool mode 3`	Abilitare la voce pool indice `3`.
`dhcp-server operation`	Abilitare il server DHCP globalmente.
`interface 2/1`	Passare alla modalità di configurazione di interfaccia `2/1`.
`dhcp-server operation`	Attivare la funzione server *DHCP Server* su questa porta.

15.2 Relè L2 DHCP

Nel pannello anteriore del dispositivo è visualizzato il seguente messaggio di pericolo:

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO

Non cambiare le posizioni dei cavi se l'Opzione 82 DHCP è abilitata. Controllare il manuale utente prima dell'intervento di manutenzione.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Un amministratore di rete utilizza il DHCP *relay agent* Layer 2 per aggiungere informazioni del client DHCP. Queste informazioni sono richieste dai *relay agent* Layer 3 e dai server DHCP per assegnare un indirizzo e una configurazione a un client.

Quando un client e un server DHCP si trovano nello stesso sottoinsieme IP, questi scambiano direttamente le richieste dell'indirizzo IP e le risposte. Possedere un server DHCP in ciascun sottoinsieme è, tuttavia, dispendioso e spesso poco funzionale. Un'alternativa ad avere un server DHCP in ciascun sottoinsieme consiste nell'utilizzare i dispositivi di rete per inoltrare pacchetti tra un client DHCP e un server DHCP collocati in un sottoinsieme diverso.

Un *relay agent* Layer 3 è in genere un router che possiede interfacce IP in entrambi i sottoinsiemi client e server e indirizza il traffico tra loro. Nelle reti commutate Layer 2, tuttavia, sono presenti uno o più dispositivi di rete, ad esempio switch, tra il client e il *relay agent* Layer 3 o il server DHCP. In questo caso, il dispositivo fornisce un *relay agent* Layer 2 per aggiungere le informazioni che il *relay agent* Layer 3 e il server DHCP richiedono per eseguire i loro ruoli di assegnazione di un indirizzo e di una configurazione.

L'elenco seguente contiene le impostazioni di default per questa funzione:
- Impostazione globale:
  - Impostazione attiva: disabilita
- Impostazioni di interfaccia
  - Impostazione attiva: disabilita
  - Porta trusted: disabilita
- Impostazioni VLAN:
  - Impostazione attiva: disabilita
  - *ID circuito*: abilita
  - Tipo *ID remoto*: mac
  - *ID remoto*: vuoto

Per il protocollo DHCPv6 viene utilizzato un *relay agent* per aggiungere le opzioni del *relay agent* ai pacchetti DHCPv6 scambiati tra un client e un server DHCPv6. Il Lightweight DHCPv6 Relay Agent (LDRA) è descritto in RFC 6221.

Il LDRA elabora 2 tipi di messaggio:
- Il primo tipo di messaggio è il messaggio *relay forward* che contiene informazioni uniche del client.
- Il secondo tipo di messaggio è il messaggio *relay reply* che il server DHCPv6 invia al *relay agent*. In seguito, il *relay agent* convalida il messaggio per includere le informazioni contenute nel messaggio *relay forward* iniziale e, se è valido, invia il pacchetto al client.

Il messaggio *relay forward* contene le informazioni dell'*ID di interfaccia*, dette anche di *Option 18*. Questa opzione fornisce informazioni che identificano l'interfaccia su cui è stata inviata la richiesta del client. Il dispositivo rifiuta i pacchetti DHCPv6 che non contengono informazioni di *Option 18*.

15.2.1 ID circuito e remoti

In un ambiente IPv4, prima di inoltrare la richiesta di un client al server DHCP, il dispositivo aggiunge l'*ID circuito* e l'*ID remoto* al campo *Option 82* del pacchetto di richiesta DHCP.
- L'*ID circuito* viene memorizzato nella porta sulla quale il dispositivo ha ricevuto la richiesta del client.
- L'*ID remoto* contiene l'indirizzo MAC, l'indirizzo IP, il nome del sistema oppure una stringa di caratteri definiti dall'utente. Utilizzando questo ID, i dispositivi partecipanti identificano il *relay agent* che ha ricevuto la richiesta del client.

Il dispositivo e altri *relay agent* utilizzano queste informazioni per reindirizzare la risposta dal DHCP *relay agent* al client originale. Il server DHCP è in grado di analizzare questi dati, ad esempio, per assegnare al client un indirizzo IP da un pool di indirizzi specifico.

Il pacchetto di risposta del server DHCP, inoltre, contiene l'*ID circuito* e l'*ID remoto*. Prima di inoltrare la risposta al client, il dispositivo rimuove le informazioni dal campo *Option 82*.

15.2.2 Configurazione del relè L2 DHCP

La finestra di dialogo *Advanced > DHCP L2 Relay > Configuration* consente di attivare la funzione sulle porte attive e sulle VLAN. Nel riquadro *Operation*, selezionare il pulsante di opzione *On*. Poi fare clic sul pulsante .

Il dispositivo inoltra i pacchetti DHCPv4 con le informazioni di *Option 82* e i pacchetti DHCPv6 con le informazioni di *Option 18* sulle porte per cui è selezionata la casella di spunta nella colonna *DHCP L2 Relay* e nella colonna *Trusted port*. In genere, si tratta di porte che si trovano nella rete del server DHCP.

Per le porte a cui sono collegati i client DHCP, attivare la funzione *DHCP L2 Relay*, ma lasciare la casella di controllo *Trusted port* non selezionata. Su queste porte il dispositivo rifiuta i pacchetti DHCPv4 con informazioni di *Option 82* e i pacchetti DHCPv6 con informazioni *Option 18*.

Di seguito si riporta un esempio di configurazione per la DHCPv4 L2 relay. Le fasi di configurazione per la funzione DHCPv6 L2 relay sono simili, ad eccezione delle voci *ID circuito* e *ID remoto* che possono essere specificate solo per *Option 82*.

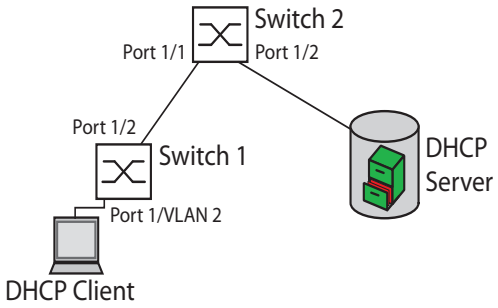


Figura 75: Rete di esempio di DHCP Layer 2

Effettuare i seguenti passi sullo Switch 1:

- ☐ Aprire la finestra di dialogo *Advanced > DHCP L2 Relay > Configuration*, scheda *Interface*.
- ☐ Per la porta `1/1`, specificare le impostazioni come segue:
  - Selezionare la casella di spunta nella colonna *Active*.
- ☐ Per la porta `1/2`, specificare le impostazioni come segue:
  - Selezionare la casella di spunta nella colonna *Active*.
  - Selezionare la casella di spunta nella colonna *Trusted port*.
- ☐ Aprire la finestra di dialogo *Advanced > DHCP L2 Relay > Configuration*, scheda *VLAN ID*.
- ☐ Specificare le impostazioni per la VLAN 2 come segue:
  - Selezionare la casella di spunta nella colonna *Active*.
  - Selezionare la casella di spunta nella colonna *Circuit ID*.
  - Per utilizzare l'indirizzo IP del dispositivo come *ID remoto*, nella colonna *Remote ID type* specificare il valore `ip`.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Effettuare i seguenti passi sullo Switch 2:

- ☐ Aprire la finestra di dialogo *Advanced > DHCP L2 Relay > Configuration*, scheda *Interface*.
- ☐ Per la porta `1/1` e `1/2`, specificare le impostazioni come segue:
  - Selezionare la casella di spunta nella colonna *Active*.
  - Selezionare la casella di spunta nella colonna *Trusted port*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Verificare che sia presente VLAN 2. In seguito eseguire i seguenti passaggi sullo Switch 1:

☐ Configurare la VLAN 2 e specificare la porta `1/1` come appartenente alla VLAN 2.

`enable`	Passare alla modalità Privileged EXEC.
`vlan database`	Passare alla modalità di configurazione VLAN.
`dhcp-l2relay circuit-id 2`	Attivare l'ID circuito e l'opzione 82 DHCP sulla VLAN `2`.
`dhcp-l2relay remote-id ip 2`	Specificare l'indirizzo IP del dispositivo come ID remoto sulla VLAN `2`.

`dhcp-l2relay mode 2`	Attivare la funzione *DHCP L2 Relay* sulla VLAN `2`.
`exit`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`dhcp-l2relay mode`	Attivare la funzione *DHCP L2 Relay* sulla porta.
`exit`	Passare alla modalità di configurazione.
`interface 1/2`	Passare alla modalità di configurazione di interfaccia `1/2`.
`dhcp-l2relay trust`	Specificare la porta come *Trusted port*.
`dhcp-l2relay mode`	Attivare la funzione *DHCP L2 Relay* sulla porta.
`exit`	Passare alla modalità di configurazione.
`dhcp-l2relay mode`	Abilitare la funzione *DHCP L2 Relay* nel dispositivo.

Effettuare i seguenti passi sullo Switch 2:

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`dhcp-l2relay trust`	Specificare la porta come *Trusted port*.
`dhcp-l2relay mode`	Attivare la funzione *DHCP L2 Relay* sulla porta.
`exit`	Passare alla modalità di configurazione.
`interface 1/2`	Passare alla modalità di configurazione di interfaccia `1/2`.
`dhcp-l2relay trust`	Specificare la porta come *Trusted port*.
`dhcp-l2relay mode`	Attivare la funzione *DHCP L2 Relay* sulla porta.
`exit`	Passare alla modalità di configurazione.
`dhcp-l2relay mode`	Abilitare la funzione *DHCP L2 Relay* nel dispositivo.

15.3 Utilizzo del dispositivo come client DNS

Il client DNS (Domain Name System) richiede ai server DNS di tradurre i nomi host e gli indirizzi IP dei dispositivi di rete. Analogamente ad un elenco telefonico, il client DNS converte i nomi dei dispositivi in indirizzi IP. Quando il client DNS riceve una richiesta di traduzione di un nome, il client DNS cerca l'informazione interrogando prima il suo database statico interno, poi i server DNS assegnati. Il client DNS salva le informazioni cercate in una cache per le richieste future.

Il dispositivo consente di configurare il client DNS dal server DHCP utilizzando la VLAN di gestione del dispositivo. Il dispositivo consente inoltre di assegnare staticamente i nomi host agli indirizzi IP.

Il client DNS fornisce le seguenti funzioni utente:
- Elenco server DNS, con spazio per 4 indirizzi IP di server di nomi di dominio
- mappatura statica del nome host all'indirizzo IP, con spazio per 64 host statici configurabili
- cache degli host, con spazio per 128 voci

15.3.1 Esempio di configurazione di un server DNS

Nomniare il client DNS e configurarlo in modo che chieda ad un server DNS di tradurre i nomi host. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Advanced > DNS > Client > Static*.
- ☐ Nel riquadro *Configuration*, campo *Configuration source*, specificare il valore `user`.
- ☐ Nel riquadro *Configuration*, campo *Domain name*, specificare il valore `device1`.
- ☐ Per aggiungere una voce tabella, fare clic sul pulsante  .
- ☐ Nella colonna *Address*, specificare il valore `192.168.3.5` come indirizzo IPv4 del server DNS. È inoltre possibile specificare un indirizzo IPv6 valido come indirizzo IP del server DNS.
- ☐ Selezionare la casella di spunta nella colonna *Active*.
- ☐ Aprire la finestra di dialogo *Advanced > DNS > Client > Global*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`dns client source user`	Specificare che l'utente configura manualmente le impostazioni del client DNS.
`dns client domain-name device1`	Specificare la stringa `device1` come nome di dominio unico per il dispositivo.
`dns client servers add 1 ip 192.168.3.5`	Per aggiungere un server DNS con un indirizzo IPv4 di `192.168.3.5` come indice `1`.
`dns client servers add 2 ip 2001::1`	Aggiungere un server DNS con un indirizzo IPv6 di `2001::1` come indice `2`.
`dns client adminstate`	Abilitare la funzione *DNS Client* globalmente.

Configurare il client DNS per mappare gli host statici con gli indirizzi IP. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Advanced > DNS > Client > Static Hosts*.
- ☐ Per aggiungere una voce tabella, fare clic sul pulsante  .
- ☐ Nella colonna *Name* immettere il valore `example.com`.
  Questo è il nome di un dispositivo nella rete.
- ☐ Nella colonna *IP address*, specificare il valore `192.168.3.9`.
- ☐ Selezionare la casella di spunta nella colonna *Active*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante  .

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`dns client host add 1 name example.com ip 192.168.3.9`	Aggiungere `example.com` come host statico con un indirizzo IP di `192.168.3.9`.
`dns client adminstate`	Abilitare la funzione *DNS Client* globalmente.

15.4 GARP

Il protocollo Generic Attribute Registration Protocol (*GARP*) è definito da IEEE per fornire un framework generico, in modo che gli switch possono registrare e deregistrare i valori di attributo, quali gli identificatori VLAN e l'appartenenza al gruppo Multicast.

Se un attributo per un partecipante è registrato o deregistrato in base alla funzione *GARP*, il partecipante viene modificato in base a specifiche regole. I partecipanti sono un insieme di stazioni finali raggiungibili e di dispositivi di rete. L'insieme di partecipanti definito in qualsiasi momento, in combinazione con i relativi attributi, è l'albero di raggiungibilità per il sottoinsieme della topologia di rete. Il dispositivo inoltra i frame di dati solo alle stazioni finali registrate. La registrazione della stazione aiuta ad evitare i tentativi di inviare dati alle stazioni finali che non sono raggiungibili.

15.4.1 Configurazione GMRP

Il protocollo GARP Multicast Registration Protocol (*GMRP*) è un protocollo Generic Attribute Registration Protocol (*GARP*), il quale offre un meccanismo che consente ai dispositivi di rete e alle stazioni finali di registrare in modo dinamico l'appartenenza al gruppo. I dispositivi registrano le informazioni di appartenenza al gruppo con i dispositivi collegati allo stesso segmento LAN. La funzione *GARP* consente anche ai dispositivi di diffondere le informazioni trai i dispositivi della rete che supportano servizi di filtraggio avanzati.

Nota: Prima di abilitare la funzione *GMRP*, verificare che la funzione *MMRP* è disabilitata.

Il seguente esempio descrive la configurazione della funzione *GMRP*. Il dispositivo fornisce uno strumento di flooding vincolato su una porta selezionata. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching* > *GARP* > *GMRP*.
- ☐ Per fornire un Multicast Flooding vincolato su una porta, selezionare la casella di spunta nella colonna *GMRP active*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`garp gmrp operation`	Abilitare la funzione *GMRP* sulla porta.
`exit`	Passare alla modalità di configurazione.
`garp gmrp operation`	Abilitare la funzione *GMRP* globalmente.

15.4.2 Configurazione GVRP

Utilizzare la funzione *GVRP* per consente al dispositivo di scambiare le informazioni di configurazione VLAN con altri dispositivi *GVRP*. Pertanto, ridurre il traffico Broadcast non necessario e il traffico Unicast sconosciuto. Inoltre, la funzione *GVRP* crea dinamicamente e gestisce VLAN su dispositivi connessi attraverso porte trunk 802.1Q.

Il seguente esempio descrive la configurazione della funzione *GVRP*. Il dispositivo consente di scambiare le informazioni di configurazione VLAN con altri dispositivi *GVRP*. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > GARP > GVRP*.
- ☐ Per scambiare le informazioni di configurazione VLAN con altri dispositivi *GVRP*, selezionare la casella di spunta nella colonna *GVRP active* per la porta.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ☑.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 3/1`	Passare alla modalità di configurazione di interfaccia `3/1`.
`garp gvrp operation`	Abilitare la funzione *GVRP* sulla porta.
`exit`	Passare alla modalità di configurazione.
`garp gvrp operation`	Abilitare la funzione *GVRP* globalmente.

15.5 MRP-IEEE

La modifica IEEE 802.1ak allo standard IEEE 802.1Q ha introdotto il protocollo Multiple Registration Protocol (MRP) per sostituire il protocollo Generic Attribute Registration Protocol (*GARP*). IEEE modifica e sostituisce anche le applicazioni *GARP*, *GARP* Multicast Registration Protocol (*GMRP*) e *GARP* VLAN Registration Protocol (*GVRP*), con il protocollo Multiple MAC Registration Protocol (*MMRP*) e il protocollo Multiple VLAN Registration Protocol (*MVRP*).

Per confinare il traffico alle aree necessarie di una rete, le applicazioni MRP distribuiscono i valori attributo a dispositivi abilitati MRP in una LAN. Le applicazioni MRP registrano e deregistrano le appartenenze al gruppo Multicast e gli identificatori VLAN.

Nota: Il protocollo Multiple Registration Protocol (MRP) richiede una rete senza loop. Per evitare loop nella rete, utilizzare un protocollo di rete quale il protocollo Media Redundancy Protocol, Spanning Tree Protocol, oppure Rapid Spanning Tree Protocol con MRP.

15.5.1 Funzionamento MRP

Ogni partecipante contiene un componente applicante e un componente MRP Attribute Declaration (MAD). Il componente applicante è responsabile della formazione di valori attributo e della rispettiva registrazione e deregistrazione. Il componente MAD genera messaggi MRP per la trasmissione e l'elaborazione di processi ricevuti da altri partecipanti. Il componente MAD codifica e trasmette gli attributi ad altri partecipanti nelle unità dati MRP (MRPDU). Nello switch, un componente MRP Attribute Propagation (MAP) distribuisce gli attributi alle porte partecipanti.

Un partecipante esiste per ogni applicazione MRP e ogni porta LAN. Ad esempio, un'applicazione partecipante esiste su un dispositivo finale e un'altra applicazione esiste su una porta switch. La macchina a stati applicante registra l'attributo e la porta per ogni dichiarazione MRP partecipante su un dispositivo finale o switch. Le modifiche delle variabili macchina di stato applicante attivano la trasmissione di MRPDU per comunicare la dichiarazione o il ritiro.

Per stabilire un'istanza *MMRP*, un dispositivo finale invia innanzitutto un messaggio Join empty (JoinMt) con gli attributi appropriati. Lo switch poi propaga il JoinMt alle porte partecipanti e agli switch adiacenti. Gli switch adiacenti propagano il messaggio alla porta partecipante ecc., stabilendo un percorso per il traffico del gruppo.

15.5.2 Timer MRP

Le impostazioni del timer di default evitano dichiarazioni e ritiri di attributo non necessari. Le impostazioni del timer consentono ai partecipanti di ricevere ed elaborare messaggi MRP prima che i timer Leave o LeaveAll scadano.

Quando si riconfigurano i timer, mantenere le seguenti relazioni:
- Per consentire la ri-registrazione dopo un evento Leave o LeaveAll, sebbene vi sia un messaggio perso, impostare il valore del LeaveTime come di seguito: ≥ (2x JoinTime) + 60 in 1/100 s
- Per minimizzare il volume del traffico riunito generato in seguito ad un LeaveAll, specificare il valore per il timer LeaveAll superiore al LeaveTime.

Il seguente elenco contiene diversi eventi MRP che il dispositivo trasmette:
- Join - Controlla l'intervallo per la trasmissione del join message successivo
- Leave - Controlla la lunghezza del tempo che uno switch attende nello stato Leave prima di passare allo stato di ritiro
- LeaveAll - Controlla la frequenza con cui lo switch genera i messaggi LeaveAll

Quando è scaduto, il timer periodico avvia un messaggio Join request MRP che lo switch invia a partecipanti sulla LAN. Gli switch utilizzano questo messaggio per evitare ritiri non necessari.

15.5.3 MMRP

Quando un dispositivo riceve traffico Broadcast, Multicast o sconosciuto su una porta, il dispositivo propaga il traffico alle altre porte. Questo processo causa un uso non necessario di larghezza di banda sulla LAN.

Il protocollo Multiple MAC Registration Protocol (*MMRP*) consente di controllare la propagazione del traffico, distribuendo una dichiarazione di attributo a partecipanti su una LAN. I valori di attributo che il componente MAD codifica e trasmette sulla LAN in messaggi MRP sono informazioni sui requisiti di assistenza di gruppo e indirizzi MAC a 48 bit.

Lo switch memorizza gli attributi in un database filtri come voci di registrazione indirizzo MAC. Il processo di inoltro utilizza le voce del database filtri solo per trasmettere li dati attraverso quelle porte necessarie per raggiungere le LAN membri del gruppo.

Gli switch facilitano i meccanismi di distribuzione del gruppo sulla base del concetto di open host group, che riceve pacchetti sulle porte attive e li inoltra solamente a porte con membri del gruppo. In questo modo, qualsiasi partecipante *MMRP* che richiede pacchetti trasmessi ad un particolare gruppo o gruppi, richiede l'appartenenza al gruppo. Gli utenti dell'assistenza MAC inviano pacchetti ad un particolare gruppo da qualunque posizione sulla LAN. Un gruppo riceve questi pacchetti sulle LAN collegate ai partecipanti *MMRP* registrati. *MMRP* e le voci MAC Address Registration vincolano quindi i pacchetti a segmenti necessari di una LAN senza loop.

Per mantenere lo stato di registrazione e deregistrazione e per ricevere traffico, una porta dichiara periodicamente il proprio interesse. Ogni dispositivo su una LAN con la funzione *MMRP* abilitata mantiene un database filtri e inoltra il traffico con gli indirizzi MAC del gruppo a partecipanti elencati.

Esempio MMRP

In questo esempio, Host A intende ascoltare il traffico al gruppo G1. Lo switch A elabora la richiesta *MMRP* Join ricevuta da un host A e invia la richiesta ad entrambi gli switch adiacenti. Ora i dispositivi sulla LAN riconoscono che vi è un host interessato alla ricezione di traffico destinato al gruppo G1. Quando l'host B avvia la trasmissione di dati destinati al gruppo G1, i dati fluiscono sul percorso delle registrazioni e l'host A li riceve.

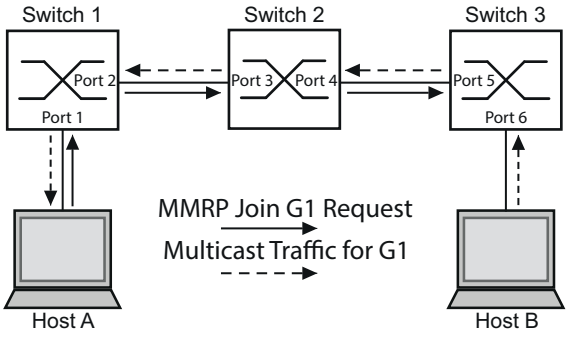


Figura 76: Rete MMRP per registrazione indirizzo MAC

Abilitare la funzione *MMRP* sugli switch. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > MRP-IEEE > MMRP*, scheda *Configuration*.
- ☐ Per attivare la porta `1` e la porta `2` come partecipanti *MMRP*, selezionare la casella di spunta nella colonna *MMRP* per la porta `1` e la porta `2` sullo switch 1.
- ☐ Per attivare la porta `3` e la porta `4` come partecipanti *MMRP*, selezionare la casella di spunta nella colonna *MMRP* per la porta `3` e la porta `4` sullo switch 2.
- ☐ Per attivare la porta `5` e la porta `6` come partecipanti *MMRP*, selezionare la casella di spunta nella colonna *MMRP* per la porta `5` e la porta `6` sullo switch 3.
- ☐ Per inviare eventi periodici, consentendo al dispositivo di mantenere la registrazione del gruppo di indirizzi MAC, abilitare la *Periodic state machine*. Selezionare il pulsante di opzione `On` nel riquadro *Configuration*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Per abilitare le porte *MMRP* sullo switch 1, utilizzare i seguenti comandi. Sostituendo le interfacce appropriate nei comandi, si abilitano le funzioni *MMRP* e le porte sugli switch 2 e 3.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia `1/1`.
`mrp-ieee mmrp operation`	Abilitare la funzione *MMRP* sulla porta.
`interface 1/2`	Passare alla modalità di configurazione di interfaccia `1/2`.
`mrp-ieee mmrp operation`	Abilitare la funzione *MMRP* sulla porta.
`exit`	Passare alla modalità di configurazione.
`mrp-ieee mrp periodic-state-machine`	Abilitare la funzione *Periodic state machine* globalmente.
`mrp-ieee mmrp operation`	Abilitare la funzione *MMRP* globalmente.

15.5.4 MVRP

Il protocollo Multiple VLAN Registration Protocol (*MVRP*) è un'applicazione MRP che fornisce la registrazione VLAN dinamica e servizi di ritiro su una LAN.

La funzione *MVRP* fornisce un meccanismo di manutenzione per le voci di registrazione VLAN dinamica, e per trasmettere le informazioni ad altri dispositivi. Queste informazioni consentono a dispositivi che riconoscono *MVRP* di stabilire e aggiornare le informazioni di appartenenza alla VLAN. Quando su una VLAN sono presenti membri, le informazioni indicano attraverso quali porte lo switch inoltra il traffico per raggiungere questi membri.

L'obiettivo principale della funzione *MVRP* è quello di consentire agli switch di scoprire alcune delle informazioni VLAN che altrimenti si dovrebbero impostare manualmente. La scoperta di queste informazioni consente agli switch di superare le limitazioni di consumo di banda e di tempo di convergenza in grandi reti VLAN.

Esempio di MVRP

Configurare una rete composta da switch che riconoscono MVRP (1 - 4) connessi ad anello con gruppi di dispositivi finali, A1, A2, B1, e B2 in 2 diverse VLAN, A e B. Con STP abilitato sugli switch, le porte che connettono lo switch 1 allo switch 4 sono in stato discarding, evitando una condizione di loop.

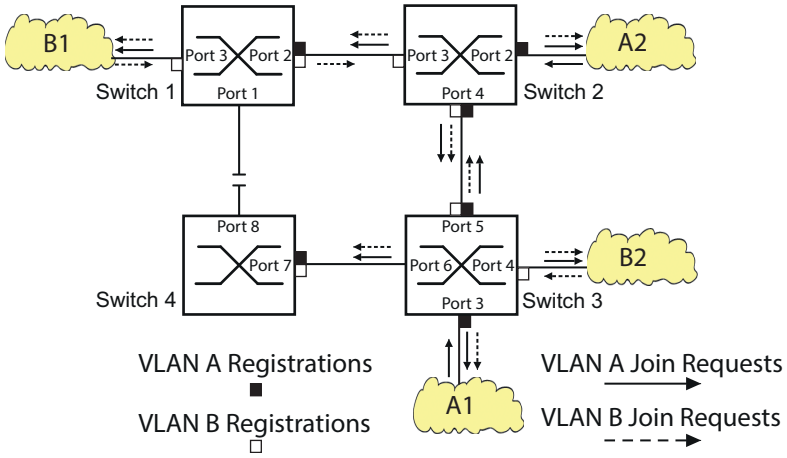


Figura 77: Rete di esempio MVRP per registrazione VLAN

Nella rete di esempio MVRP, le LAN inviano prima una richiesta Join agli switch. Lo switch immette la registrazione VLAN nel forwarding database per la porta che riceve i frame.

Poi, lo switch propaga la richiesta ad altre porte, e invia la richiesta alle LAN e agli switch adiacenti. Questo processo continua finché gli switch hanno registrato le VLAN nel forwarding database della porta ricevente.

Abilitare MVRP sugli switch. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching* > *MRP-IEEE* > *MVRP*, scheda *Configuration*.
- ☐ Per attivare le porte da 1 a 3 come partecipanti *MVRP*, selezionare la casella di spunta nella colonna *MVRP* per le porte da 1 a 3 sullo switch 1.
- ☐ Per attivare le porte da 2 a 4 come partecipanti *MVRP*, selezionare la casella di spunta nella colonna *MVRP* per le porte da 2 a 4 sullo switch 2.

- ☐ Per attivare le porte da 3 a 6 come partecipanti *MVRP*, selezionare la casella di spunta nella colonna *MVRP* per le porte da 3 a 6 sullo switch 3.
- ☐ Per attivare la porta 7 e la porta 8 come partecipanti *MVRP*, selezionare la casella di spunta nella colonna *MVRP* per la porta 7 e la porta 8 sullo switch 4.
- ☐ Per mantenere la registrazione delle VLAN, abilitare *Periodic state machine*. Selezionare il pulsante di opzione *On* nel riquadro *Configuration*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione *On* nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Per abilitare le porte *MVRP* sullo switch 1, utilizzare i seguenti comandi. Sostituendo le interfacce appropriate nei comandi, si abilitano le funzioni *MVRP* e le porte sugli switch 2, 3 e 4.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`interface 1/1`	Passare alla modalità di configurazione di interfaccia 1/1.
`mrp-ieee mvrp operation`	Abilitare la funzione *MVRP* sulla porta.
`interface 1/2`	Passare alla modalità di configurazione di interfaccia 1/2.
`mrp-ieee mvrp operation`	Abilitare la funzione *MVRP* sulla porta.
`exit`	Passare alla modalità di configurazione.
`mrp-ieee mvrp periodic-state-machine`	Abilitare la funzione *Periodic state machine* globalmente.
`mrp-ieee mvrp operation`	Abilitare la funzione *MVRP* globalmente.

16 Protocolli industriali

16.1 IEC 61850/MMS

Lo IEC 61850/MMS è un protocollo standardizzato di comunicazione industriale dell'International Electrotechnical Commission (IEC). Il protocollo si trova nell'automazione di sottostazione, ad esempio nella tecnica di comando dei fornitori di energia.

Questo protocollo, che funziona a pacchetti, si basa sul protocollo di trasporto TCP/IP e utilizza la Manufacturing Messaging Specification (MMS) per la comunicazione client-server. Il protocollo è orientato all'oggetto e definisce un linguaggio standardizzato di configurazione che comprende, tra le altre cose, funzioni per SCADA, dispositivi elettronici intelligenti (IED) e per la tecnica di comando della rete.

La parte 6 della norma IEC 61850 definisce il linguaggio di configurazione SCL (linguaggio di configurazione della sottostazione). SCL descrive le proprietà del dispositivo e la struttura del sistema in una forma automaticamente elaborabile. Le proprietà del dispositivo descritte con l'SCL sono memorizzate nel file ICD all'interno del dispositivo.

16.1.1 Modello di switch per IEC 61850

Il report tecnico, IEC 61850 90-4, specifica un modello di switch. Il modello di switch rappresenta le funzioni di uno switch come oggetti di un dispositivo elettronico intelligente (IED). Un client MMS (ad esempio il software della sala di comando) utilizza questi oggetti per monitorare e configurare il dispositivo.

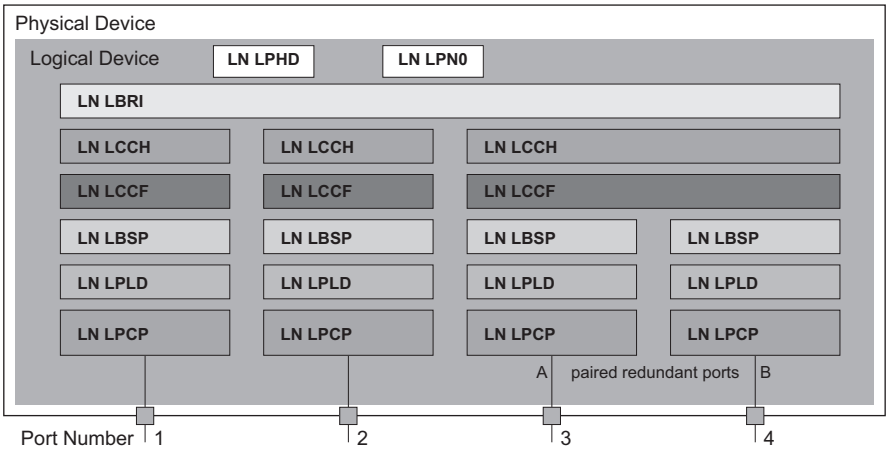


Figura 78: Modello di switch basato sul report tecnico IEC 61850 90-4

Tabella 59:Classi del modello di switch basate sul report tecnico IEC61850 90-4

Classe	Descrizione
LN LLN0	Nodo logico del Zero dello IED del Bridge: Definisce le proprietà logiche del dispositivo.
LN LPHD	Nodo logico del Physical Device dello IED del Bridge: Definisce le proprietà fisiche del dispositivo.
LN LBRI	Nodo logico del Bridge: Rappresenta le impostazioni generali delle funzioni dello switch del dispositivo.
LN LCCH	Nodo logico del Communication Channel: Definisce il Communication Channel logico che consiste in una o più porte fisiche del dispositivo.
LN LCCF	Nodo logico del Channel Communication Filtering: Definisce le impostazioni della VLAN o del Multicast per il Communication Channel di livello superiore.
LN LBSP	Nodo logico del Port Spanning Tree Protocol: Definisce gli stati e le impostazioni dello Spanning Tree per la relativa porta fisica del dispositivo.
LN LPLD	Nodo logico del Port Layer Discovery: Definisce gli stati e le impostazioni dell'LLDP per la relativa porta fisica del dispositivo.
LN LPCP	Nodo logico del Physical Communication Port: Rappresenta la relativa porta fisica del dispositivo.

16.1.2 Integrazione in un sistema di controllo

Preparazione del dispositivo

Eseguire i seguenti passaggi:

- ☐ Verificare che il dispositivo abbia un indirizzo IP assegnato.
- ☐ Aprire la finestra di dialogo *Advanced > Industrial Protocols > IEC61850-MMS*.
- ☐ Per avviare il server MMS, selezionare il pulsante di opzione *On* nel riquadro *Operation*, e fare clic sul pulsante ✓.
  Successivamente, un client MMS è in grado di connettersi al dispositivo e leggere e monitorare gli oggetti definiti nel modello di switch.

Lo IEC61850/MMS non fornisce alcun meccanismo di autenticazione. Se l'accesso in scrittura allo IEC61850/MMS è attivato, ogni client in grado di accedere al dispositivo utilizzando il TCP/IP può modificarne le impostazioni. Ciò può causare una configurazione errata del dispositivo e possibili problemi nella rete.

AVVISO
RISCHIO DI ACCESSO AL DISPOSITIVO NON AUTORIZZATO Attivare l'accesso in scrittura solo se si sono adottate misure ulteriori (ad esempio firewall, VPN, etc.) per ridurre possibili accessi non autorizzati. **Il mancato rispetto di queste istruzioni può causare danni alle apparecchiature.**

☐ Per consentire al client MMS di modificare le impostazioni, selezionare la casella di spunta *Write access*, e fare clic sul pulsante ✓.

Configurazione offline

Il dispositivo consente di scaricare il file ICD utilizzando l'interfaccia grafica utente. Questo file contiene le proprietà del dispositivo descritto con l'SCL e consente di configurare la sottostazione senza connettersi direttamente al dispositivo.

☐ Aprire la finestra di dialogo *Advanced > Industrial Protocols > IEC61850-MMS*.

☐ Per caricare il file ICD nel proprio PC, fare clic sul pulsante ☰ e poi sulla voce *Download*.

Monitoraggio del dispositivo

Il server IEC61850/MMS integrato nel dispositivo consente di monitorare più stati del dispositivo tramite il Report Control Block (RCB). Per un Report Control Block si può registrare fino a un massimo di 5 client MMS contemporaneamente.

Il dispositivo consente di monitorare i seguenti stati:

Tabella 60:Gli stati del dispositivo monitorabili con IEC 61850/MMS

Classe	Oggetto RCB	Descrizione
LN LPHD	TmpAlm	Quando la temperatura misurata nel dispositivo supera o scende al di sotto delle soglie di temperatura impostate, lo stato cambia.
	PhyHealth	Quando lo stato dell'oggetto RCB LPHD.TmpAlm cambia, lo stato cambia.
LN LPHD	TmpAlm	Quando la temperatura misurata nel dispositivo supera o scende al di sotto delle soglie di temperatura impostate, lo stato cambia.
	PwrSupAlm	Quando una delle alimentazioni di tensione ridondanti si interrompe o si riavvia, lo stato cambia.
	PhyHealth	Quando lo stato dell'oggetto RCB LPHD.PwrSupAlm o LPHD.TmpAlm cambia, lo stato cambia.

Tabella 60:Gli stati del dispositivo monitorabili con IEC 61850/MMS (cont

Classe	Oggetto RCB	Descrizione
LN LBRI	RstpRoot	Quando il dispositivo assume o rinuncia al ruolo di root switch, lo stato cambia.
	RstpTopoCnt	Quando la topologia cambia a causa del cambio del root switch, lo stato cambia.
LN LCCH	ChLiv	Quando lo stato del link della porta fisica cambia, lo stato cambia.
LN LPCP	PhyHealth	Quando lo stato del link della porta fisica cambia, lo stato cambia.

16.2 Modbus TCP

Modbus TCP è un protocollo di messaggistica a livello applicativo che fornisce comunicazione client/server tra il client e i dispositivi collegati nelle reti Ethernet TCP/IP.

La funzione *Modbus TCP* consente di installare il dispositivo nelle reti che già utilizzano *Modbus TCP* e di recuperare le informazioni salvate nei registri del dispositivo.

16.2.1 Modalità Modbus TCP/IP client/server

Il dispositivo supporta il modello client/server del Modbus TCP/IP. Tale dispositivo opera come un server all'interno della costellazione e richiede le informazioni salvate nei registri da un client.

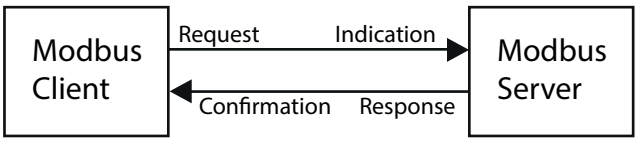


Figura 79: Modalità Modbus TCP/IP client/server

Il modello client/server utilizza quattro tipi di messaggi per scambiare i dati tra client e server:
- Richiesta Modbus TCP/IP, il client crea una richiesta di informazioni e la invia al server.
- Indicazione Modbus TCP/IP, il server riceve una richiesta a indicare che il client necessita di informazioni.
- Risposta Modbus TCP/IP, quando le informazioni richieste sono disponibili, il server invia una risposta contenente le informazioni richieste. Quando le informazioni richieste non sono disponibili, il server invia un messaggio di errore per comunicare al client l'errore rilevato durante l'elaborazione. Il messaggio di errore include un codice di eccezione che indica il motivo dell'errore rilevato.
- Conferma Modbus TCP/IP, il client riceve dal server una risposta contenente le informazioni richieste.

16.2.2 Funzioni supportate e mappatura della memoria

Il dispositivo supporta funzioni con i codici pubblici `0x03` (`Read Holding Registers`) e `0x05` (`Write Single Coil`). I codici consentono di leggere le informazioni salvate nei registri come le informazioni di sistema, incluso il nome di sistema, la posizione di sistema, la versione del software, l'indirizzo IP, l'indirizzo MAC. Inoltre, i codici consentono di leggere le informazioni e le statistiche della porta. Il codice `0x05` consente di ripristinare i contatori della porta individualmente o globalmente.

L'elenco seguente contiene le definizioni dei valori inseriti nella colonna `Format`:
- Bitmap: un gruppo da 32°bit, codificato in ordine Big-endian e salvato in due registri. I sistemi Big-endian salvano i byte più importanti di una parola nell'indirizzo più piccolo e salvano i byte meno importanti nell'indirizzo più grande.
- F1: 16-bit unsigned integer
- F2: Enumeration - power supply alarm
  - 0 = power supply good
  - 1 = power supply failure detected
- F3: Enumeration - OFF/ON
  - 0 = Off
  - 1 = On

- F4: Enumeration - port type
  - 0 = Giga - Gigabit Interface Converter (GBIC)
  - 1 = Copper - Twisted Pair (TP)
  - 2 = Fiber - 10 Mb/s
  - 3 = Fiber - 100 Mb/s
  - 4 = Giga - 10/100/1000 Mb/s (triple speed)
  - 5 = Giga - Copper 1000 Mb/s TP
  - 6 = Giga - Small Form-factor Pluggable (SFP)
- F9: 32-bit unsigned long
- Stringa: ottetti, salvati in sequenza, 2 ottetti per registro.

Codici Modbus TCP/IP

La tabella di seguito elenca gli indirizzi che consentono al client di ripristinare i contatori della porta e di recuperare informazioni specifiche dai registri del dispositivo.

Informazioni della porta

Tabella 61:Informazioni della porta

Indirizzo (Address)	Qtà.	Descrizione	Min	Max	Passaggio	Unità	Formato
0400	1	Port 1 Type	0	6	1	-	F4
0401	1	Port 2 Type	0	6	1	-	F4
		...					
043F	1	Port 64 Type	0	6	1	-	F4
0440	1	Port 1 Link Status	0	1	1	-	F1
0441	1	Port 2 Link Status	0	1	1	-	F1
		...					
047F	1	Port 64 Link Status	0	1	1	-	F1
0480	1	Port 1 STP State	0	1	1	-	F1
0481	1	Port 2 STP State	0	1	1	-	F1
		...					
04BF	1	Port 64 STP State	0	1	1	-	F1
04C0	1	Port 1 Activity	0	1	1	-	F1
04C1	1	Port 2 Activity	0	1	1	-	F1
		...					
04FF	1	Port 64 Activity	0	1	1	-	F1
0500	1	Port 1 Counter Reset	0	1	1	-	F1
0501	1	Port 2 Counter Reset	0	1	1	-	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	-	F1

Statistiche della porta

Tabella 62:Statistiche della porta

Indirizzo (Address)	Qtà.	Descrizione	Min	Max	Passaggio	Unità	Formato
0800	1	Port1 - Number of bytes received	0	4294967295	1	-	F9
0802	1	Port1 - Number of bytes sent	0	4294967295	1	-	F9
0804	1	Port1 - Number of frames received	0	4294967295	1	-	F9
0806	1	Port1 - Number of frames sent	0	4294967295	1	-	F9
0808	1	Port1 - Total bytes received	0	4294967295	1	-	F9
080A	1	Port1 - Total frames received	0	4294967295	1	-	F9
080C	1	Port1 - Number of broadcast frames received	0	4294967295	1	-	F9
080E	1	Port1 - Number of multicast frames received	0	4294967295	1	-	F9
0810	1	Port1 - Number of frames with CRC error	0	4294967295	1	-	F9
0812	1	Port1 - Number of oversized frames received	0	4294967295	1	-	F9
0814	1	Port1 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0816	1	Port1 - Number of jabber frames received	0	4294967295	1	-	F9
0818	1	Port1 - Number of collisions occurred	0	4294967295	1	-	F9
081A	1	Port1 - Number of late collisions occurred	0	4294967295	1	-	F9
081C	1	Port1 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
081E	1	Port1 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0820	1	Port1 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0822	1	Port1 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0824	1	Port1 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0826	1	Port1 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
0828	1	Port1 - Number of Mac Error Packets	0	4294967295	1	-	F9
082A	1	Port1 - Number of dropped received packets	0	4294967295	1	-	F9
082C	1	Port1 - Number of multicast frames sent	0	4294967295	1	-	F9
082E	1	Port1 - Number of broadcast frames sent	0	4294967295	1	-	F9
0830	1	Port1 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
		...					
147E	1	Port64 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9

16.2.3 Configurazione esemplificativa

In questo esempio, configurare il dispositivo per rispondere alle richieste del client. Il prerequisito per questa configurazione è che il dispositivo del cliente sia configurato con un indirizzo IP entro l'intervallo dato. La funzione *Write access* rimane inattiva per questo esempio. Quando si attiva la funzione *Write access*, il dispositivo consente il ripristino esclusivo dei contatori della porta. Nella configurazione predefinita, le funzioni *Modbus TCP* e *Write access* sono inattive.

Il protocollo *Modbus TCP* non fornisce alcun meccanismo di autenticazione. Se l'accesso in scrittura per *Modbus TCP* è attivato, ogni cliente in grado di accedere al dispositivo utilizzando il TCP/IP è in grado di modificarne le impostazioni. Ciò può causare una configurazione errata del dispositivo e possibili problemi nella rete.

AVVISO
RISCHIO DI ACCESSO AL DISPOSITIVO NON AUTORIZZATO Attivare l'accesso in scrittura solo se si sono adottate misure ulteriori (ad esempio firewall, VPN, etc.) per ridurre possibili accessi non autorizzati. **Il mancato rispetto di queste istruzioni può causare danni alle apparecchiature.**

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > IP Access Restriction*.
- ☐ Aggiunge una voce tabella. A tale scopo, fare clic sul pulsante .
- ☐ Specificare l'intervallo di indirizzo IP nella riga dove la colonna *Index* ha il valore `2`. A tale scopo, eseguire i seguenti passaggi:
  - Nella colonna *Address*: `10.17.1.0`
  - Nella colonna *Netmask*: `255.255.255.248`
- ☐ Verificare che la casella di spunta nella colonna *Modbus TCP* sia selezionata.
- ☐ Attivare l'intervallo di indirizzo IP. A tale scopo, selezionare la casella di spunta nella colonna *Active*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .
- ☐ Aprire la finestra di dialogo *Diagnostics > Status Configuration > Security Status*, scheda *Global*.
- ☐ Verificare che la casella di spunta relativa al parametro *Modbus TCP active* sia selezionata.
- ☐ Aprire la finestra di dialogo *Advanced > Industrial Protocols > Modbus TCP*.
- ☐ La porta di ascolto *Modbus TCP* standard, porta `502`, è il valore predefinito. Tuttavia, quando si desidera ascoltare un'altra porta TCP, inserire il valore per la porta di ascolto nel campo *TCP port*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante .

Quando si abilita la funzione *Modbus TCP*, la funzione *Security Status* rileva l'attivazione e visualizza un allarme nella finestra di dialogo *Basic Settings > System*, riquadro *Security status*.

`enable`	Passare alla modalità Privileged EXEC.
`network management access add 2`	Crea la voce per l'intervallo dell'indirizzo nella rete. Numero del successivo indice disponibile in questo esempio: `2`.
`network management access modify 2 ip 10.17.1.0`	Specifica l'indirizzo IP.
`network management access modify 2 mask 29`	Specifica la maschera di rete.
`network management access modify 2 modbus-tcp enable`	Specifica che il dispositivo consente l'accesso di *Modbus TCP* alla gestione dei dispositivo.
`network management access operation`	Abilita la limitazione di accesso IP.
`configure`	Passare alla modalità di configurazione.
`security-status monitor modbus-tcp-enabled`	Specifica che il dispositivo monitora l'attivazione del server *Modbus TCP*.
`modbus-tcp operation`	Attiva il server *Modbus TCP*.
`modbus-tcp port <1..65535>`	Specificare la porta TCP per la comunicazione *Modbus TCP* (opzionale). Il valore predefinito è porta `502`.
`show modbus-tcp`	Visualizzare le impostazioni del server *Modbus TCP*.

```
Modbus TCP/IP server settings
-----------------------------
Modbus TCP/IP server operation.................enabled
Write-access...................................disabled
Listening port.................................502
Max number of sessions.........................5
Active sessions................................0
```

`show security-status monitor`	Visualizzare le impostazioni stato-sicurezza.

```
Device Security Settings
Monitor
---------------------------------
Password default settings unchanged...........monitored
...
Write access using Ethernet Switch Configurator is possible....monitored
Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled......................monitored
Modbus TCP/IP server active...................monitored
```

`show security-status event`	Visualizzare gli eventi dello stato di sicurezza avvenuti.

```
Time stamp             Event                        Info
--------------------   ----------------------    ------
2014-01-01 01:00:39   password-change(10)           -
.................................................
2014-01-01 01:00:39   ext-nvm-load-unsecure(21)     -
2014-01-01 23:47:40   modbus-tcp-enabled(23)        -
show network management access rules 1
```

Visualizzare le regole di accesso limitato alla gestione per l'indice 1.

```
Restricted management access settings
-------------------------------------
Index.....................................1
IP Address................................10.17.1.0
Prefix Length.............................29
HTTP......................................yes
SNMP......................................yes
Telnet....................................yes
SSH.......................................yes
HTTPS.....................................yes
IEC61850-MMS..............................yes
Modbus TCP/IP.............................yes
Active....................................[x]
```

16.3 EtherNet/IP

EtherNet/IP è accettato a livello mondiale come protocollo standardizzato di comunicazione industriale ed è mantenuto da Open DeviceNet Vendor Association (ODVA). Il protocollo è basato sui protocolli di trasporto Ethernet standard ampiamente utilizzati TCP/IP e UDP/IP. *EtherNet/IP* è supportato da produttori leader, fornendo così un'ampia base per la comunicazione efficace dei dati nel settore industriale.

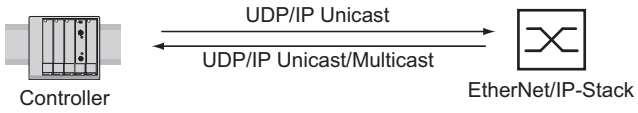


Figura 80: rete EtherNet/IP

EtherNet/IP aggiunge il protocollo industriale CIP (Common Industrial Protocol) ai protocolli Ethernet standard. *EtherNet/IP* implementa il CIP al livello della sessione e oltre, e adatta il CIP alla tecnologia *EtherNet/IP* specifica al livello di trasporto e al di sotto di esso. Nel caso delle applicazioni nel campo dell'automazione, *EtherNet/IP* implementa il CIP al livello dell'applicazione. Di conseguenza, *EtherNet/IP* è ideale per il settore della tecnica di comando industriale.

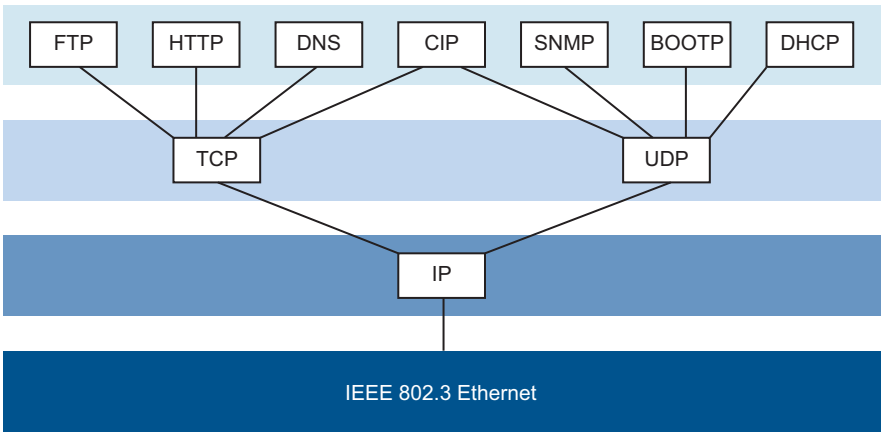


Figura 81: IEEE802.3 EtherNet/IP

Per informazioni dettagliate su *EtherNet/IP*, vedere il sito web ODVA all'indirizzo www.odva.org.

16.3.1 Integrazione in un sistema di controllo

Eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Switching > IGMP Snooping > Global*.
  Verificare che la funzione *IGMP Snooping* sia abilitata.
- ☐ Aprire la finestra di dialogo *Advanced > Industrial Protocols > EtherNet/IP*.
  Verificare che la funzione *EtherNet/IP* sia abilitata.
- ☐ Aprire la finestra di dialogo *Advanced > Industrial Protocols > EtherNet/IP*.
- ☐ Per salvare l'EDS come archivio Zip sul proprio PC, fare clic su *Download*.
  L'archivio ZIP include il file di configurazione *EtherNet/IP* e l'icona utilizzata per configurare il controller da connettere al dispositivo.

16.3.2 Parametri entità EtherNet/IP

I seguenti paragrafi identificano gli object e le operazioni supportate dal dispositivo.

Operazioni supportate

Tabella 63:Panoramica delle richieste EtherNet/IP supportate per le istanze object

Service Code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object
0x01 Get Attribute All	All attributes	All attributes	All attributes	All attributes	All attributes
0x02 Set Attribute All	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA)	Settable attributes (0x6, 0x9)	–	–
0x0e Get Attribute Single	All attributes	All attributes	All attributes	All attributes	All attributes
0x10 Set Attribute Single	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA, 0x64)	Settable attributes (0x6, 0x9, 0x65, 0x67, 0x68, 0x69, 0x6C)	Settable attributes (0x5, 0x7)	–
0x05 Reset	Parameter (0x0, 0x1)	–	–	–	–
0x35 Save Configuration Vendor specific	–	–	–	Save switch configuration	–
0x36 Mac Filter Vendor specific	–	–	–	Add MAC filter STRUCT of: USINT VlanId ARRAY of: 6 USINT Mac DWORD PortMask	–

Identity object

Il dispositivo supporta l'identity object (Class Code 0x01) di *EtherNet/IP*. L'ID del produttore Schneider Electric è 634. Schneider Electric utilizza l'ID 44 (0x2C) per indicare il tipo di prodotto "Managed Ethernet Switch".

Tabella 64:Attributi dell'istanza (solo l'istanza 1 è disponibile)

Id	Attribute	Access Rule	Data type	Description
0x1	Vendor ID	Get	UINT	Schneider Electric634
0x2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
0x3	Product Code	Get	UINT	Product Code: mapping is defined for every device type
0x4	Revision	Get	STRUCT of: USINT Major USINT Minor	Revision of the EtherNet/IP implementation, 2.1.
0x5	Status	Get	WORD	Support for the following Bit status only: 0: Owned (always 1) 2: Configured (always 1) 4: Extend Device Status 5: 0x3: No I/O connection established 6: 0x7: At least one I/O connection established, all in idle mode. 7:
0x6	Serial number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
0x7	Product name	Get	SHORT-STRING	Displayed as "Schneider Electric" + product family + product ID + software variant.

TCP/IP Interface Object

Il dispositivo supporta solo l'istanza 1 del TCP/IP Interface Object (Class Code 0xF5) di *EtherNet/IP*.

A seconda dello stato di accesso in scrittura, il dispositivo memorizza la configurazione completa nella propria memoria flash. Il salvataggio del file di configurazione può impiegare fino a 10 secondi. Se la procedura di salvataggio è interrotta, ad esempio a causa di un'alimentazione di tensione non funzionante, il funzionamento del dispositivo potrebbe risultare impossibile.

Nota: Il dispositivo risponde alla modifica della configurazione `Get Request` con una `Response` sebbene la configurazione non sia ancora stata salvata completamente.

Tabella 65:Attributi delle classi

Id	Attribute	Access Rule	Data type	Description
0x1	Revision	Get	UINT	Revision of this object: 3
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances currently created: 1

Tabella 66:Attributi dell'istanza 1

Id	Attribute	Access Rule	Data type	Description
0x1	Status	Get	DWORD	0: Interface Status (0=Interface not configured, 1=Interface contains valid config)
				6: ACD status (default 0)
				7: ACD fault (default 0)
0x2	Interface Capability flags	Get	DWORD	0: BOOTP Client
				1: DNS Client
				2: DHCP Client
				3: DHCP-DNS Update
				4: Configuration setable (within CIP) Other bits reserved (0)
				7: ACD capable (0=not capable, 1=capable)
0x3	Config Control	Set/Get	DWORD	0: 0x0=using stored config 1: 0x1=using BOOTP 2: 0x2=using DHCP 3:
				4: One device uses DNS for name lookup (always 0 because it is not supported) Other bits reserved (0)
0x4	Physical Link Object	Get	STRUCT of:	Path to the Physical Link Object, always {0x20, 0xF6, 0x24, 0x01} describing instance 1 of the Ethernet Link Object.
			UINT PathSize	
			EPATH Path	
0x5	Interface Configuration	Set/Get	STRUCT of:	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).
			UDINT IpAddress	
			UDINT Netmask	
			UDINT GatewayAddress	
			UDINT NameServer1	
			UDINT NameServer2	
			STRING DomainName	
0x6	Host Name	Set/Get	STRING	Host Name (for DHCP DNS Update)
0x7	Safety Network Number			Not supported
0x8	TTL Value	Get/Set	USINT	Time to live value for IP multicast packets Range 1..255 (default = 1)

Tabella 66:Attributi dell'istanza 1 (cont

Id	Attribute	Access Rule	Data type	Description
0x9	Mcast Config	Get/Set	STRUCT of: USINT AllocControl USINT reserved UINT NumMcast UDINT McastStartAddr	Alloc Control = 0 Number of IP multicast addresses = 32 Multicast start address = 239.192.1.0
0xA	Selected Acd	Get/Set	BOOL	0=ACD disable 1=ACD enable (default)
0xB	Last Conflict Detected	Get	STRUCT of: USINT AcdActivity ARRAY of: 6 USINT RemoteMac ARRAY of: 28 USINT ArpPdu	ACD Diagnostic Parameters

Tabella 67:Schneider Electric estensioni del TCP/IP Interface Object

Id	Attribute	Access Rule	Data type	Description
0x64	Cable Test	Set/Get	STRUCT of: USINT Interface USINT Status	Interface Status (1=Active, 2=Success, 3=Failure, 4=Uninitialized)
0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of: 2 Pair for 100BASE 4 Pair for 1000BASE

Tabella 67:Schneider Electric estensioni del TCP/IP Interface Object (cont

Id	Attribute	Access Rule	Data type	Description

0x66	Cable Test Result	Get	STRUCT of:
			USINT Interface
			USINT CablePair
			USINT CableStatus
			USINT CableMinLength
			USINT CableMaxLength
			USINTCableFailureLocation
				100BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}
				1000BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair3, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair4, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}

Ethernet Link object

Le informazioni nelle due tabelle seguenti fanno parte dell'Ethernet Link Object. Per accedere alle informazioni, utilizzare i seguenti valori:

- Class(####)
- Instance(###)
- Attribute(#)

Per esempio, i valori *class*, *instance*, e *attribute* sono valori da accesso alle informazioni per l'utilizzo dell'allarme utilizzando i seguenti messaggi espliciti:

- Class = 0xF6
- Instance = 1
- Attribute = 6

Tabella 68:Attributi dell'istanza ed Schneider Electric estensioni Ethernet Link Object

Id	Attribute	Access Rule	Data type	Description
Attributi dell'istanza				
0x1	Interface Speed	Get	UDINT	Used interface speed in MBit/s (10, 100, 1000, …). 0 is used when the speed has not been determined or is invalid because of detected errors.
0x2	Interface Flags	Get	DWORD	Interface Status Flags: 0: Link State (0=No link, 1=Link) 1: Duplex mode (0=Half, 1=Full) 2: Auto-Negotiation Status 3: 0x0=Auto-Negotiation in progress 4: 0x1=Auto-Negotiation failed 0x2=Failed but speed detected 0x3=Auto-Negotiation success 0x4=No Auto-Negotiation 5: Manual configuration require reset (always 0 because it is not needed) 6: Hardware error
0x3	Physical Address	Get	ARRAY of: 6 USINT	MAC address of physical interface
0x4	Interface Counters	Get	STRUCT of: UDINT InMibIICounter1 UDINT InMibIICounter2 …	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors
0x5	Media Counters	Get	STRUCT of: UDINT EthernetMibCounter1 UDINT EthernetMibCounter2 …	Errori rilevati: Alignment, FCS, single collision, multiple collision, SQE Test, deferred transmissions, late collisions, excessive collisions, MAC TX, carrier sense, frame too long, MAC RX

Tabella 68:Attributi dell'istanza ed Schneider Electric estensioni Ethernet Link Object (cont

Id	Attribute	Access Rule	Data type	Description
0x6	Interface Control	Get/Set	STRUCT of:	Control Bits:
			WORD ControlBits	0: Auto-negotiation enable/disable (0=disable, 1=enable)
				1: Duplex mode (0=Half, 1=Full), if Auto-negotiation disabled
			UINT ForcedInterface Speed	Interface speed in MBits/s: 10,100,…, if Auto-negotiation disabled
0x7	Interface type	Get	USINT	Type of interface: 0: Unknown interface type 1: The interface is internal 2: Twisted-pair 3: Optical fiber
0x8	Interface state	Get	USINT	Current state of the interface: 0: Unknown interface state 1: The interface is enabled 2: The interface is disabled 3: The interface is testing
0x9	Admin State	Set/Get	USINT	Administrative state: 1: Enable the interface 2: Disable the interface
0xA	Interface label	Get	SHORT-STRING	Human readable ID
Schneider Electric estensioni al Ethernet Link Object				
0x64	Ethernet Interface Index	Get	USINT	Interface/Port Index (ifIndex out of MIBII)
0x65	Port Control	Get/Set	DWORD	0: Link state (0=link down, 1=link up)
				1: Link admin state (0=disabled, 1=enabled)
				8: Access violation alarm (read-only)
				9: Utilization alarm (read-only)
0x66	Interface Utilization	Get	USINT	The existing Counter out of the private MIB hm2IDiagfaceUtilization is used. Utilization in percentage (Unit 1%=100, %/100). RX Interface Utilization.
0x67	Interface Utilization Alarm Upper Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Upper Limit.
0x68	Interface Utilization Alarm Lower Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Lower Limit.
0x69	Broadcast limit	Get/Set	USINT	Broadcast limiter Service (Egress BC-Frames limitation, 0=disabled), Frames/second

Tabella 68:Attributi dell'istanza ed Schneider Electric estensioni Ethernet Link Object (cont

Id	Attribute	Access Rule	Data type	Description
0x6A	Ethernet Interface Description	Get/Set	STRING	Interface/Port Description (from MIB II ifDescr), for example "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX" or "unavailable", max. 64 Bytes.
0x6B	Port Monitor	Get/Set	DWORD	0: Link Flap (0=Off, 1=On)
				1: CRC/Fragment (0=Off, 1=On)
				2: Duplex Mismatch (0=Off, 1=On)
				3: Overload-Detection (0=Off, 1=On)
				4: Link-Speed/ Duplex Mode (0=Off, 1=On)
				5: Deactivate port action (0=Off, 1=On)
				6: Send trap action (0=Off, 1=On)
				7: Active Condition (displays which condition caused an action to occur) 8: 9: 10: 11: 00001_B: Link Flap 00010_B: CRC/Fragments 00100_B: Duplex Mismatch 01000_B: Overload-Detection 10000_B: Link-Speed/ Duplex mode
				12: Reserved (always 0)
				13: Reserved (always 0)
				14: Reserved (always 0)
				15: Reserved (always 0)
0x6C	Quick Connect	Get/Set	USINT	Quick Connect on the interface (0=Off, 1=On) If you enable Quick Connect, then the device sets the port speed to 100FD, disables Auto-Negotiation, and Spanning Tree on the interface.
0x6D	SFP Diagnostics	Get	STRUCT of:	
			STRING ModuleType	
			SHORT-STRING SerialNumber	
			USINT Connector	
			USINT Supported	
			DINT Temperature	in °C
			DINT TxPower	in mW
			DINT RxPower	in mW
			DINT RxPower	in dBm
			DINT TxPower	in dBm

Tabella 69:Attribuzione delle porte alle istanze Ethernet Link Object

Ethernet Port	Ethernet Link Object Instance
CPU	1
1	2
2	3
3	4
4	5
…	…

Nota: Il numero delle porte dipende dal tipo di hardware utilizzato. L'Ethernet Link Object esiste solo se la porta è connessa.

Switch Agent object

Il dispositivo supporta l'Ethernet Switch Agent Object Schneider Electric specifico (Class Code 0x95) per la configurazione del dispositivo e i parametri informativi con l'istanza 1.

Tabella 70:Attributi delle classi

Id	Attribute	Access Rule	Data type	Description	
0x1	Switch Status	Get	DWORD	0:	Like the signal contact, the value indicates the Device Overall state (0=ok, 1=failed)
				1:	Device Security Status (0=ok, 1=failed)
				2:	Power Supply 1 (0=ok, 1=failed)
				3:	Power Supply 2 (0=ok, 1=failed or not existing)
				4:	Reserved
				5:	Reserved
				6:	Signal Contact 1 (0=closed, 1=open)
				7:	Signal Contact 2 (0=closed, 1=open or not existing)
				8:	Reserved
				9:	Temperature (0=ok, 1=failure)
				10:	Module removed (1=removed)
				11:	EAM removed (1=removed)
				12:	EAM-SD removed (1=removed)
				13:	Reserved
				14:	Reserved
				15:	Reserved
				16:	Reserved
				17:	Reserved
				18:	Reserved
				19:	Reserved
				20:	Reserved
				21:	Reserved
				22:	Reserved
				23:	MRP (0=disabled, 1=enabled)
				24:	Reserved
				25:	Reserved
				26:	RSTP (0=disabled, 1=enabled)
				27:	LAG (0=disabled, 1=enabled)
				28:	Reserved
				29:	Reserved
				30:	Reserved
				31:	Connection Error (1=failure)

Tabella 70:Attributi delle classi (cont

Id	Attribute	Access Rule	Data type	Description
0x2	Switch Temperature	Get	STRUCT of:	
			INT TemperatureF	in °F
			INT TemperatureC	in °C
0x3	Reserved	Get	UDINT	Reserved for future use (always 0)
0x4	Switch Max Ports	Get	UINT	Maximum number of Ethernet Switch Ports
0x5	Multicast Settings (IGMP Snooping)	Get/Set	WORD	0: IGMP Snooping (0=disabled, 1=enabled) 1: IGMP Querier (0=disabled, 1=enabled) 2: IGMP Querier Mode (read-only) (0=Non-Querier, 1=Querier) 3: 4: 5: 6: 7: IGMP Querier Packet Version Off=0 IGMP Querier disabled V1=1 V2=2 V3=3 8: 9: 10: Treatment of Unknown Multicasts: 0=Send To All Ports 2=Discard
0x6	Switch Existing Ports	Get	ARRAY of: DWORD	Bitmask of existing switch ports Per bit starting with Bit 0 (=Port 1) (0=Port not available, 1=Port existing) Array (bit mask) size is adjusted to the size of maximum number of switch ports (for max. 28 Ports 1 DWORD is used)
0x7	Switch Port Control	Get/Set	ARRAY of: DWORD	Bitmask Link Admin Status switch ports Per bit starting with Bit 0 (=Port 1) (0=Port enabled, 1=Port disabled) Array (bit mask) size is adjusted to the size of maximum number of Switch ports (for max. 28 Ports 1 DWORD is used)
0x8	Switch Ports Mapping	Get	ARRAY of: USINT	Instance number of the Ethernet-Link-Object Starting with Index 0 (=Port 1) All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N, maximum number of ports). When the entry is 0, the Ethernet Link Object for this port does not exist

Tabella 70:Attributi delle classi (cont

Id	Attribute	Access Rule	Data type	Description
0x9	Switch Action Status	Get	DWORD	Status of the last executed action (for example config save, software update, etc.)
				0: Flash Save Configuration In Progress/Flash Write In Progress
				1: Flash Save Configuration Failed/Flash Write Failed
				4: Configuration changed (configuration not in sync. between running configuration

L'Ethernet Switch Agent Object Schneider Electric specifico fornisce il servizio supplementare specifico del venditore, con il Service Code 0x35 per il salvataggio della configurazione dello switch. Quando si invia una richiesta dal proprio PC per salvare la configurazione di un dispositivo, questo invia una risposta dopo aver salvato la configurazione nella memoria flash.

Base Switch object

Il Base Switch object fornisce l'interfaccia di livello applicativo CIP allo stato base dell'informazione per uno switch Ethernet gestito (revisione 1).

È disponibile solo l'istanza 1 del Base Switch (Class Code 0x51).

Tabella 71:Attributi dell'istanza

Id	Attribute	Access Rule	Data type	Description
0x1	Device Up Time	Get	UDINT	Time since the device powered up
0x2	Total port count	Get	UDINT	Number of physical ports
0x3	System Firmware Version	Get	SHORT-STRING	Human readable representation of System Firmware Version
0x4	Power source	Get	WORD	Status of switch power source
0x5	Port Mask Size	Get	UINT	Number of DWORD in port array attributes
0x6	Existing ports	Get	ARRAY of:	Port Mask
			DWORD	
0x7	Global Port Admin State	Get	ARRAY of:	Port Admin Status
			DWORD	
0x8	Global Port link Status	Get	ARRAY of:	Port Link Status
			DWORD	
0x9	System Boot Loader Version	Get	SHORT-STRING	Readable System Firmware Version
0xA	Contact Status	Get	UDINT	Switch Contact Closure

Tabella 71:Attributi dell'istanza (cont

Id	Attribute	Access Rule	Data type	Description
0xB	Aging Time	Get	UDINT	Range 10..1000000 · 1/10 seconds (default=300) 0=Learning off
0xC	Temperature C	Get	UINT	Switch temperature in degrees Celsius
0xD	Temperature F	Get	UINT	Switch temperature in degrees Fahrenheit

RSTP Bridge Object (MCSESM-E)

RSTP è un protocollo a 2 livelli che consente l'impiego di una tipologia Ethernet ridondante (ad esempio di un anello). RSTP viene specificato al capitolo 17 dello standard IEEE 802.1D-2004.

Il dispositivo supporta l'RSTP Bridge Object specifico di Schneider Electric (Class Code 64_H, 100) per i parametri di configurazione e informazione del dispositivo.

Il dispositivo supporta 2 istanze:
- l'istanza 1 rappresenta l'istanza RSTP primaria del Bridge e
- l'istanza 2 rappresenta l'istanza RSTP secondaria (Dual).

Per ulteriori informazioni in merito a questi parametri e alle rispettive modalità di impostazione, consultare il manuale di riferimento “Interfaccia grafica utente”.

Tabella 72:Schneider Electric RSTP Bridge Object

Id	Attribute	Access rule	Data type	Description
1	Bridge Identifier Priority	Set	UDINT	Range: 0 to 61,440 in steps of 4,096, default: 32,768 (refer to IEEE, 802.1D-2004, § 17.13.7)
2	Transmit Hold Count	Set	UINT	Range: 1 to 40, default: 10 (refer to IEEE 802.1D-2004, §17.13.12)
3	Force Protocol Version	Set	UINT	Default:2 (refer to IEEE 802.1D-2004, §17.13.4 and dot1d-StpVersion in RFC 4318)
4	Bridge Hello Time	Set	UDINT	Range: 100 to 200, unit: centi-seconds (1/100 of a second), default: 200 (refer to IEEE 802.1D-2004, §17.13.6 and dot1d-StpHoldTime in RFC 4188)
5	Bridge Forward Delay	Set	UDINT	Range: 400 to 3000, unit: centi-seconds, default: 2100 (refer to IEEE 802.1D-2004, §17.13.5 and dot1d-StpForwardDelay in RFC 4188)
6	Bridge Max. Age	Set	UINT	Range: 600 to 4000, unit: centi-seconds, default: 4000 (refer to IEEE 802.1D-2004, §17.13.8 and dot1d-StpBridgeMaxAge in RFC 4188)
7	Time Since Topology Change	Get	UDINT	Unit: centi-seconds (refer to dot1dStpTimeSinceTopologyChange in RFC 4188)

Tabella 72:Schneider Electric RSTP Bridge Object (cont

Id	Attribute	Access rule	Data type	Description
8	Topology Change	Get	UDINT	Refer to dot1dStpTopChanges in RFC 4188
100	InnerPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance‘s inner port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance‘s inner port.
101	OuterPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance‘s outer port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance‘s outer port.

RSTP Port Object (MCSESM-E)

Il dispositivo supporta l'RSTP Port Object specifico di Schneider Electric (Class Code 65_H, 101) per i parametri di configurazione e di informazione della porta RSTP con almeno un'istanza (Instance 1).

l'istanza 1 rappresenta la CPU Ethernet Interface, l'istanza 2 rappresenta la porta fisica 1, l'istanza 3 la porta fisica 2 ecc.

Per ulteriori informazioni in merito a questi parametri e alle rispettive modalità di impostazione, consultare il manuale di riferimento “Interfaccia grafica utente”.

Tabella 73:Schneider Electric RSTP Port Object

Id	Attribute	Access rule	Data type	Description
1	Port Identifier Priority	Set	UDINT	Range: 0 to 240 in steps of 16, default: 128 (refer to IEEE, 802.1D-2004, § 17.13.10).
2	mcheck	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.19.13 and dot1d-StpPortProtocolMigration in RFC 4318).
3	Port Path Cost	Set	UDINT	Range: 1 to 200,00,000, default:auto (0) (refer to IEEE 802.1D-2004, §17.13.11 and dot1d-StpPortAdminPathCost in RFC 4318).
4	Port Admin Edge Port	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.13.1 and dot1d-StpPortAdminEdgePort in RFC 4318).
5	Port Oper Edge Port	Get	BOOL	True (1), False (2) (refer to dot1dStpPortOperEdgePort in RFC 4318).
6	Port Admin PointToPoint	Set	UINT	forceTrue (0), forceFalse (1), auto (2) (refer to dot1dStpPortAdminPointToPoint in RFC 4318).
7	Port Oper PointToPoint	Get	UINT	True (1), False (2) (refer to dot1dStpPortOperPointToPoint in RFC 4318).

Tabella 73:Schneider Electric RSTP Port Object (cont

Id	Attribute	Access rule	Data type	Description
8	Port Enable	Set	UINT	Enabled (1), Disabled (2) (Refer to dot1dStpPortEnable in RFC 4188).
9	Port State	Get	UINT	Disabled (1), Blocking (2), Listening (3), Learning (4), Forwarding (5), Broken (6) (refer to dot1dStpPortState in RFC 4188).
10	Port Role	Get	UNT	Unknown (0), Alternate/Backup (1), Root (2), Designated (3) (refer to dot1dStpTopChanges in RFC 4188).
100	DRSTP	Get	UINT	Schneider Electric-specific object. True (1), False (2).

Servizi, collegamenti e dati I/O

Il dispositivo supporta i seguenti tipi e parametri di collegamento.

Tabella 74:Impostazioni per l'integrazione di un nuovo modulo

Setting	I/O connection	Input only	Listen only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/Program
IP Address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

Tabella 75:Struttura dei dati I/O del dispositivo

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
Device Status	Bitmask (see Switch Agent Attribute 0x1)	Input	DWORD
Link Status	Bitmask, 1 Bit per port (0=No link, 1=Link up)	Input	DWORD
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, for example for controller access port. (0=Port enabled, 1=Port disabled)	Input	DWORD
Utilization Alarm[2]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Access Violation Alarm[3]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Multicast Connections	Integer, number of connections	Input	DINT

Tabella 75:Struttura dei dati I/O del dispositivo (cont

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
TCP/IP Connections	Integer, number of connections	Input	DINT
Quick Connect Mask	Bitmask (1 Bit per port) (0=Quick Connect disabled, 1=Quick Connec enabled)	Input	DINT
Link Admin State	Bitmask, 1 Bit per port (0=Port enabled, 1=Port disabled)	Output	DWORD

1. La dimensione predefinita dei bitmask della porta è 32 bit (DWORD). Per i dispositivi dotati di più di 28 porte, i bitmask della porta sono stati estesi a n * DWORD.
2. Specificare le impostazioni dell'utilization alarm nella finestra di dialogo *Basic Settings > Port*, scheda *Utilization*. La soglia massima è il limite in cui la condizione di allarme si attiva. La soglia minima è il limite in cui una condizione di allarme attiva si disattiva.
3. Specificare le impostazioni dell'Access Violation alarm nella finestra di dialogo *Network Security > Port Security*. La soglia massima è il limite in cui la condizione di allarme si attiva. La soglia minima è il limite in cui una condizione di allarme attiva si disattiva.

Tabella 76:Mappatura dei tipi di dati secondo le dimensioni dei bit

Tipo di oggetto	Dimensioni del bit
BOOL	1 bit
DINT	32 bit
DWORD	32 bit
SHORT-STRING	max. 32 bytes
STRING	max. 64 bytes
UDINT	32 bit
UINT	16 bit
USINT	8 bit
WORD	16 bit

A Impostazione dell'ambiente di configurazione

A.1 Configurazione di un server DHCP/BOOTP

Il seguente esempio descrive la configurazione di un server DHCP utilizzando il software haneWIN DHCP Server. Questo software shareware è un prodotto di IT-Consulting Dr. Herbert Hanewinkel. È possibile scaricare il software da www.hanewin.net. È possibile provare il software per 30 giorni di calendario, dalla data della prima installazione e poi decidere se si desidera acquistare una licenza.

Eseguire i seguenti passaggi:
- ☐ Installate il server DHCP sul proprio PC.
  Per effettuare l'installazione, seguire le indicazioni dell'assistente per l'installazione.
- ☐ Avviare il programma *haneWIN DHCP Server*.

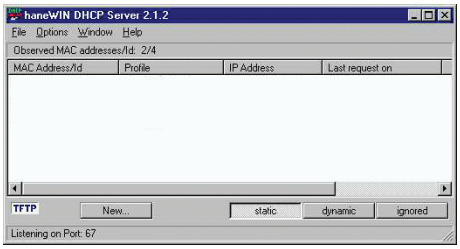


Figura 82: Avviare la finestra del programma haneWIN DHCP Server

Nota: Se Windows è attivato, la procedura di installazione comprende un servizio, che si avvia automaticamente nella configurazione di base. Questo servizio è attivo anche se il programma stesso non è stato avviato. Una volta avviato, il servizio risponde alle richieste DHCP.

- ☐ Nella barra dei menu, fare clic sulle voci *Options > Preferences* per aprire la finestra di impostazioni dell programma.
- ☐ Selezionare la scheda *DHCP*.
- ☐ Specificare le impostazioni visualizzate in figura.

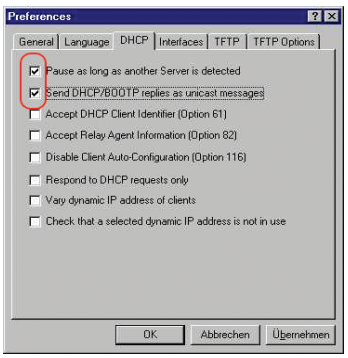


Figura 83: Impostazione DHCP

- ☐ Fare clic sul pulsante *OK*.
- ☐ Per inserire i profili di configurazione, fare clic nella barra dei menu sulla voce *Options > Configuration Profiles*

☐ Specificare il nome per il nuovo profilo di configurazione.

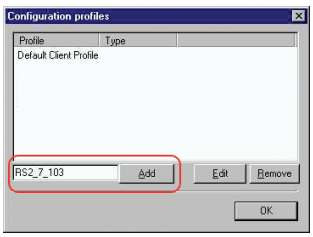


Figura 84: Aggiunta di profili di configurazione

☐ Fare clic sul pulsante *Add*.
☐ Specificare la netmask.

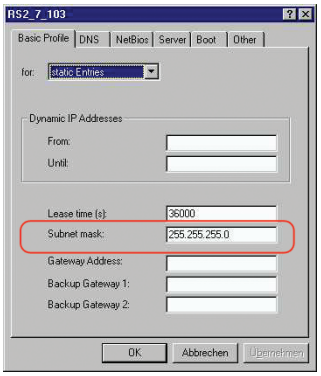


Figura 85: Maschera di rete nel profilo di configurazione

☐ Fare clic sul pulsante *Apply*.
☐ Selezionare la scheda *Boot*.
☐ Digitare l'indirizzo IP del server tftp.
☐ Immettere il percorso e il nome attribuito al file di configurazione.

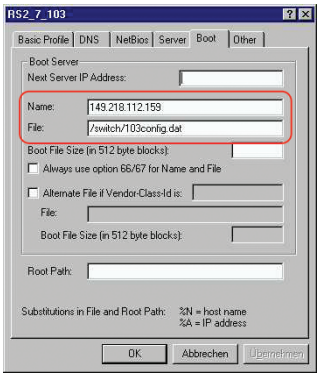


Figura 86: File di configurazione sul server tftp

☐ Fare clic sul pulsante *Apply* e poi sul pulsante *OK*.

☐ Aggiungere un profilo per ogni tipo di dispositivo.
Quando dispositivi dello stesso tipo hanno diverse configurazioni, si aggiunge un profilo per ogni configurazione.

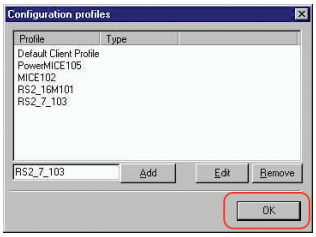


Figura 87: Gestione dei profili di configurazione

☐ Per completare l'aggiunta dei profili di configurazione, fare clic sul pulsante *OK*.
☐ Per inserire indirizzi statici, nella finestra principale, fare clic sul pulsante *Static*.

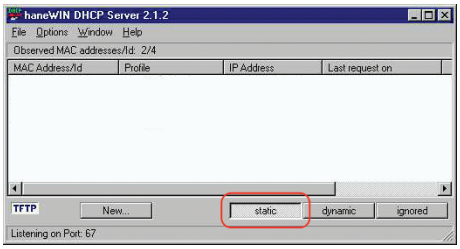


Figura 88: Immissione di indirizzi statici

☐ Fare clic sul pulsante *Add*.

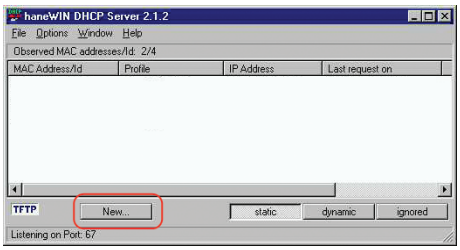


Figura 89: Aggiunta di indirizzi statici

☐ Immettere l'indirizzo MAC del dispositivo.
☐ Digitare l'indirizzo IP del dispositivo.

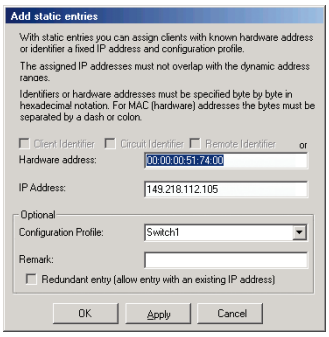


Figura 90: Voci per indirizzi statici

☐ Selezionare il profilo di configurazione del dispositivo.

- Fare clic sul pulsante *Apply* e poi sul pulsante *OK*.
- Aggiungere una voce per ogni dispositivo che deve ricevere i rispettivi parametri dal server DHCP.

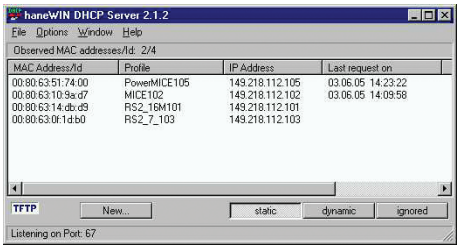


Figura 91: Server DHCP con voci

A.2 Impostazione di un server DHCP con opzione 82

Il seguente esempio descrive la configurazione di un server DHCP utilizzando il software haneWIN DHCP Server. Questo software shareware è un prodotto di IT-Consulting Dr. Herbert Hanewinkel. È possibile scaricare il software da www.hanewin.net. È possibile provare il software per 30 giorni di calendario, dalla data della prima installazione e poi decidere se si desidera acquistare una licenza.

Eseguire i seguenti passaggi:

- ☐ Installate il server DHCP sul proprio PC.
  Per effettuare l'installazione, seguire le indicazioni dell'assistente per l'installazione.
- ☐ Avviare il programma *haneWIN DHCP Server*.

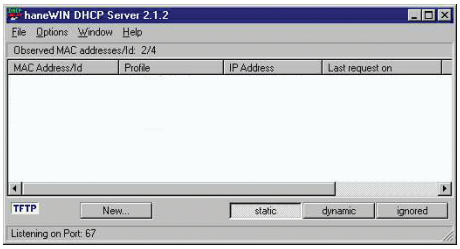


Figura 92: Avviare la finestra del programma haneWIN DHCP Server

Nota: Se Windows è attivato, la procedura di installazione comprende un servizio, che si avvia automaticamente nella configurazione di base. Questo servizio è attivo anche se il programma stesso non è stato avviato. Una volta avviato, il servizio risponde alle richieste DHCP.

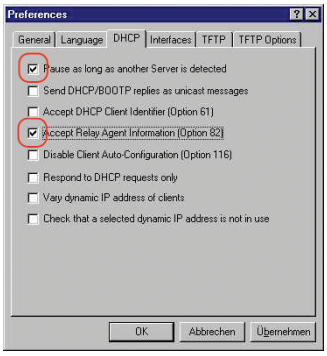


Figura 93: Impostazione DHCP

- ☐ Per l'immissione degli indirizzi statici, fare clic sul pulsante *Add*.

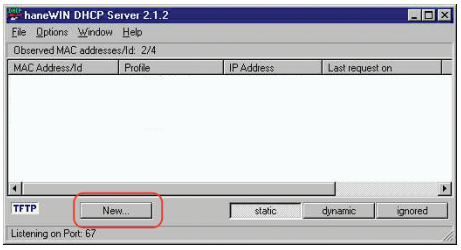


Figura 94: Aggiunta di indirizzi statici

- ☐ Selezionare la casella di spunta *Circuit Identifier*.
- ☐ Selezionare la casella di spunta *Remote Identifier*.

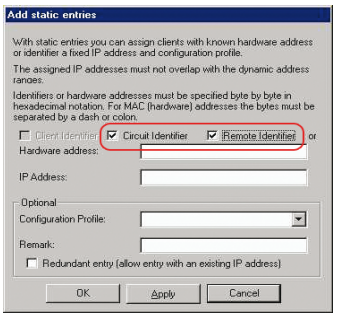


Figura 95: Impostazione di default per l'assegnazione di indirizzi fissi

- ☐ Nel campo *Hardware address*, specificare il valore *Circuit Identifier* e il valore *Remote Identifier* per switch e porta.
  Il server DHCP assegna l'indirizzo IP specificato nel campo *IP address* al dispositivo che si connette alla porta specificata nel campo *Hardware address*.
  L'indirizzo hardware presenta la seguente forma:
  `ciclvvvvssmmpprirlxxxxxxxxxxxx`
  - `ci`
    Subidentificatore per il tipo dell'ID circuito
  - `cl`
    Lunghezza dell'ID circuito.
  - Identificativo Schneider Electric:
    `01` quando un dispositivo Schneider Electric è connesso alla porta, altrimenti `00`.
  - `vvvv`
    ID VLAN della richiesta DHCP.
    Impostazione di default: `0001` = VLAN 1
  - `ss`
    La presa del dispositivo su cui si trova il modulo con quella porta a cui il dispositivo è

connesso. Specificare il valore `00`.

- `mm`
  Modulo con la porta a cui il dispositivo è connesso.
- `pp`
  Porta a cui il dispositivo è connesso.
- `ri`
  Subidentificatore per il tipo dell'ID remoto
- `rl`
  Lunghezza dell'ID remoto.
- `xxxxxxxxxxxx`
  ID remoto del dispositivo (ad esempio indirizzo MAC) a cui il dispositivo è connesso.

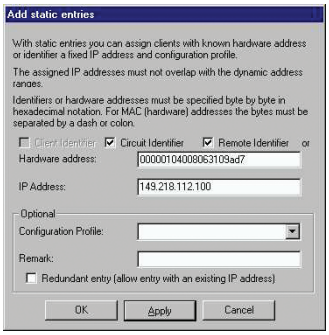


Figura 96: Specificazione degli indirizzi

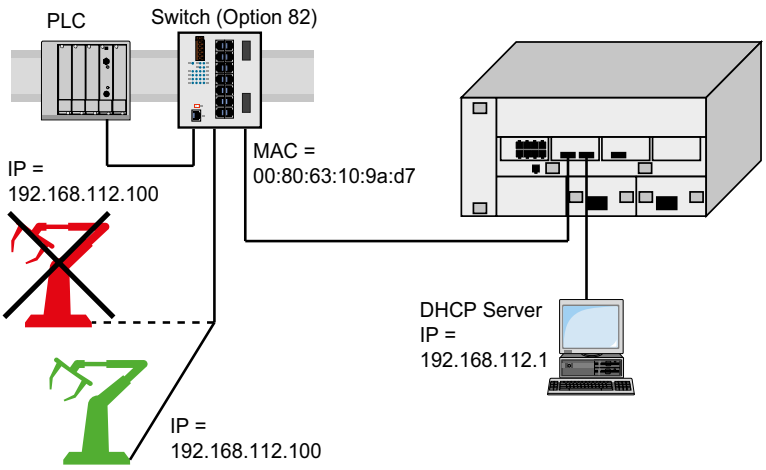


Figura 97: Esempio di applicazione utilizzando l'opzione 82

A.3 Preparazione di accesso SSH

È possibile collegarsi al dispositivo utilizzando SSH. A tale scopo, eseguire i seguenti passaggi:
- Generare una chiave nel dispositivo.
  oppure
- Trasferire la propria chiave sul dispositivo.
- Preparare l'accesso al dispositivo nel programma client SSH.

Nota: Nell'impostazione di default, la chiave esiste già ed è abilitato l'accesso utilizzando SSH.

A.3.1 Generazione di una chiave nel dispositivo.

Il dispositivo consente di generare la chiave direttamente nel dispositivo. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *SSH*.
- ☐ Per disabilitare il server SSH, selezionare il pulsante di opzione `Off` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.
- ☐ Per creare una chiave RSA, nel riquadro *Signature*, fare clic sul pulsante *Create*.
- ☐ Per abilitare il server SSH, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`ssh key rsa generate`	Generare una nuova chiave RSA.

A.3.2 Caricamento della propria chiave sul dispositivo

OpenSSH fornisce agli amministratori di rete esperti l'opzione di generare una propria chiave. Per generare la chiave, digitare i seguenti comandi sul PC:

```
ssh-keygen(.exe) -q -t rsa -f rsa.key -C '' -N ''
rsaparam -out rsaparam.pem 2048
```

Il dispositivo consente il trasferimento della propria chiave SSH sul dispositivo. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *SSH*.
- ☐ Per disabilitare il server SSH, selezionare il pulsante di opzione `Off` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.
- ☐ Se la chiave host si trova sul PC o su un'unità di rete, trascinare il file che contiene la chiave nell'area . In alternativa, fare clic sull'area per selezionare il file.

- ☐ Fare clic sul pulsante *Start* nel riquadro *Key import* per caricare la chiave sul dispositivo.
- ☐ Per abilitare il server SSH, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

Eseguire i seguenti passaggi:
- ☐ Copiare la chiave autogenerata dal PC sulla memoria esterna.
- ☐ Copiare la chiave dalla memoria esterna al dispositivo.

`enable`	Passare alla modalità Privileged EXEC.
`copy sshkey envm <file name>`	Caricare la propria chiave sul dispositivo dalla memoria esterna.

A.3.3 Preparazione del programma client SSH

Il programma *PuTTY* consente l'accesso al dispositivo utilizzando SSH. È possibile scaricare il software da www.putty.org.

Eseguire i seguenti passaggi:
- ☐ Avviare il programma con un doppio clic.

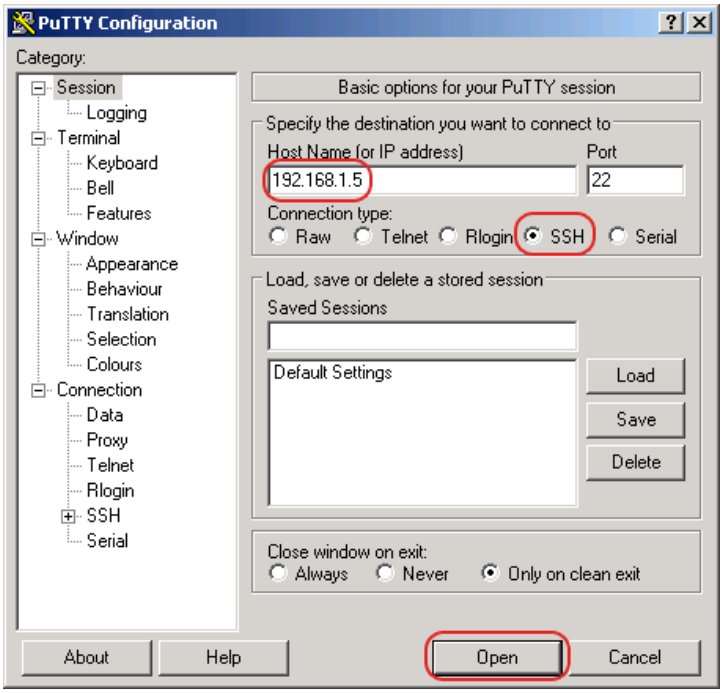


Figura 98: Schermata di immissione di PuTTY

- ☐ Nel campo *Host Name (or IP address)* si specifica l'indirizzo IP del dispositivo. L'indirizzo IP (a.b.c.d) è costituito da 4 numeri decimali con valori da `0` a `255`. I 4 numeri decimali sono separati da punti.
- ☐ Per scegliere il tipo di connessione, selezionare il pulsante di opzione *SSH* nell'elenco opzioni *Connection type*.
- ☐ Fare clic sul pulsante *Open* per impostare la connessione dati al dispositivo.

Prima di stabilire la connessione, il programma *PuTTY* visualizza un avviso di protezione e consente la verifica dell'impronta digitale della chiave.

Figura 99: Richiesta di conferma per l'impronta digitale.

Prima di stabilire la connessione, il programma *PuTTY* visualizza un avviso di protezione e consente la verifica dell'impronta digitale della chiave.

- ☐ Verificare l'impronta digitale della chiave per essere sicuri di avere connesso il dispositivo desiderato.
- ☐ Se l'impronta digitale corrisponde a quella della chiave, fare clic sul pulsante *Yes*.

Per amministratori di rete esperti, un altro modo di accedere al dispositivo attraverso un SSH è utilizzare la OpenSSH Suite. Per impostare la connessione dati, immettere il seguente comando:

```
ssh admin@10.0.112.53
```

`admin` è il nome utente.

`10.0.112.53` è l'indirizzo IP del dispositivo

A.4 Certificato HTTPS

Il browser web stabilisce la connessione al dispositivo utilizzando il protocollo HTTPS. Il prerequisito è quello di abilitare la funzione *HTTPS server* nella finestra di dialogo*Device Security > Management Access > Server*, scheda *HTTPS*.

Nota: Il software di terzi quali i browser web validano i certificati sulla base di criteri quali la data di scadenza e le attuali raccomandazioni per parametri crittografici. I certificati obsoleti potrebbero causare problemi dovuti a informazioni non valide o non aggiornate. Esempio: un certificato scaduto oppure modifica delle raccomandazioni crittografiche. Per risolvere i conflitti di validazione con il software di terzi, trasferire il certificato aggiornato al dispositivo oppure rigenerare il certificato con il firmware più aggiornato.

A.4.1 Gestione del certificato HTTPS

Per la crittografia è richiesto un certificato standard secondo X.509/PEM (infrastruttura a chiave pubblica (PKI)). Nell'impostazione di default, un certificato autogenerato è già presente nel dispositivo. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *HTTPS*.
- ☐ Per creare un certificato X509/PEM, nel riquadro *Certificate*, fare clic sul pulsante *Create*.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.
- ☐ Riavviare il server HTTPS per attivare la chiave. Riavviare il server utilizzando la Command Line Interface.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`https certificate generate`	Generare un certificato https X.509/PEM.
`no https server`	Disabilitare la funzione *HTTPS*.
`https server`	Abilitare la funzione *HTTPS*.

☐ Il dispositivo consente inoltre il trasferimento di un certificato X.509/PEM generato esternamente sul dispositivo:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *HTTPS*.
- ☐ Se il certificato si trova sul PC o su un'unità di rete, trascinare il certificato nell'area . In alternativa, fare clic sull'area per selezionare il certificato.
- ☐ Fare clic sul pulsante *Start* per copiare il certificato sul dispositivo.
- ☐ Salvare temporaneamente le modifiche. A tale scopo, fare clic sul pulsante ✓.

`enable`	Passare alla modalità Privileged EXEC.
`copy httpscert envm <file name>`	Copiare il certificato HTTPS dal dispositivo esterno con memoria non volatile.

`configure`	Passare alla modalità di configurazione.
`no https server`	Disabilitare la funzione *HTTPS*.
`https server`	Abilitare la funzione *HTTPS*.

Nota: Per attivare il certificato dopo averlo creato o trasferito, effettuare il riavvio del dispositivo o riavviare il server HTTPS. Riavviare il server HTTPS utilizzando la Command Line Interface.

A.4.2 Accesso attraverso HTTPS

L'impostazione di default per la connessione dati HTTPS è la porta TCP `443`. Cambiando il numero della porta HTTPS, effettuare il riavvio del dispositivo o del server HTTPS. In questo modo la modifica diventa efficace. A tale scopo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Device Security > Management Access > Server*, scheda *HTTPS*.
- ☐ Per abilitare la funzione, selezionare il pulsante di opzione `On` nel riquadro *Operation*.
- ☐ Per accedere al dispositivo tramite HTTPS, immettere HTTPS anziché HTTP nel browser, seguito dall'indirizzo IP del dispositivo.

`enable`	Passare alla modalità Privileged EXEC.
`configure`	Passare alla modalità di configurazione.
`https port 443`	Specifica il numero della porta TCP sulla quale il server Web riceve le richieste HTTPS dai client.
`https server`	Abilitare la funzione *HTTPS*.
`show https`	Visualizza lo stato del server *HTTPS* e il numero di porta.

Se si effettuano modifiche al numero di porta HTTPS, disabilitare il server HTTPS e abilitarlo nuovamente per rendere efficaci le modifiche.

Il dispositivo utilizza il protocollo HTTPS e stabilisce un nuova connessione dati. Se l'utente si disconnette al termine della sessione, il dispositivo termina la connessione dati.

B Appendice

B.1 Management Information Base (MIB)

The Management Information Base (MIB) è progettato come una struttura ad albero astratta.

I punti di diramazione sono le classi di oggetto. Le “foglie” del MIB sono definite classi di oggetto generiche.

Se necessario per un'identificazione univoca, le classi di oggetto generiche sono istanziate, questo significa che la struttura astratta è mappata rispetto alla realtà, specificando la porta o l'indirizzo di origine.

I valori (interi, cicli durata, contatori o stringhe di ottetti) sono assegnate a queste istanze; questi valori possono essere letti e, in alcuni casi, modificati. La descrizione oggetto o l'ID oggetto (OID) identificano la classe di oggetto. Il subidentificatore (SID) è utilizzato per istanziarle.

Esempio:

La classe di oggetto generica `sa2PSState` (`OID` = `1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1`) è la descrizione dell'informazione astratta `stato alimentazione di tensione`. Tuttavia, non è possibile leggere alcun valore da ciò, poiché il sistema non sa quale alimentazione di tensione si intende.

La specifica del subidentificatore `2` mappa queste informazioni astratte rispetto alla realtà (le istanzia), identificandole come il modo operativo dell'alimentazione di tensione `2`. A questa istanza è assegnato un valore che può essere letto. L'istanza `get 1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1` restituisce la risposta `1`, che indica che l'alimentazione di tensione è pronta per il funzionamento.

Definizione dei termini sintattici utilizzati:	
Integer	Un valore integer nell'intervallo -2^{31} - 2^{31}-1
Indirizzo IP	`xxx.xxx.xxx.xxx` (`xxx` = valore integer nell'intervallo `0..255`)
Indirizzo MAC	Numero esadecimale a 12 cifre secondo ISO/CEI 8802-3
Object Identifier	x.x.x.x… (ad esempio 1.3.6.1.1.4.1.3833...)
Octet String	Stringa di caratteri ASCII
PSID	Identificatore alimentazione di tensione (numero dell'alimentatore)
TimeTicks	Cronografo, tempo trascorso = valore numerico / 100 (in secondi) valore numerico = valore integer nell'intervallo 0-2^{32}-1
Timeout	Valore di tempo in centesimi di secondo valore di tempo = valore integer nell'intervallo 0-2^{32}-1
Campo Tipo	Numero esadecimale a 4 cifre secondo ISO/IEC 8802-3
Contatore	Valore integer (0-2^{32}-1), quando si verificano determinati eventi il valore aumenta di `1`.

B.2 Elenco degli RFC

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2863	The Interfaces Group MIB
RFC 2865	RADIUS Client
RFC 2866	RADIUS Accounting

RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 2869bis	RADIUS support for EAP
RFC 2933	IGMP MIB
RFC 3164	The BSD Syslog Protocol
RFC 3376	IGMPv3
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3580	802.1X RADIUS Usage Guidelines
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 3621	Power Ethernet MIB
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4251	SSH protocol architecture
RFC 4291	IPv6 Addressing Architecture
RFC 4252	SSH authentication protocol
RFC 4253	SSH transport layer protocol
RFC 4254	SSH connection protocol
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 4861	Neighbor Discovery for IPv6
RFC 5321	Simple Mail Transfer Protocol
RFC 6221	Leightweight DHCPv6 Relay Agent
RFC 8200	IPv6 Specification
RFC 8415	DHCPv6

B.3 Standard°IEEE di riferimento

IEEE 802.1AB	Station and Media Access Control Connectivity Discovery
IEEE 802.1D	MAC Bridges (switching function)
IEEE 802.1Q	Virtual LANs (VLANs, MRP, Spanning Tree)
IEEE 802.1X	Port Authentication
IEEE 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

B.4 Norme IEC di riferimento

IEC 62439	High availability automation networks MRP – Media Redundancy Protocol based on a ring topology

B.5 Norme ANSI di riferimento

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.6 Dati tecnici

16.3.3 Switching

Dimensione della tabella di indirizzi MAC (incl. filtri statici)	16384
Numero max di filtri per indirizzi MAC configurati staticamente	100
Numero max di filtri per indirizzi MAC apprendibili tramite IGMP Snooping	1024
Numero max. di voci relative agli indirizzi MAC (MMRP)	64
Numero code di priorità	8 Code
Priorità porta impostabili	0..7
MTU (lunghezza massima consentita dei pacchetti che una porta può ricevere o trasmettere)	9720 Byte

16.3.4 VLAN

Intervallo VLAN ID	1..4042
Numero di VLAN	max 128 simultaneamente per dispositivo max 128 simultaneamente per porta

16.3.5 Elenchi di controllo di accesso (ACL)

Numero max. di ACL	50
Numero massimo di regole per ACL	256
Numero massimo di regole per porta	256
Numero totale di regole configurabili	2048 (8 × 256)
Numero massimo di assegnazioni VLAN	12
Numero max. di regole che registrano un evento	128
Numero max. di regole di ingresso	514

B.7 Copyright del software integrato

Il prodotto contiene, tra le altre cose, i file del software open source sviluppato da terzi e concesso in licenza con una licenza software open source.

I termini della licenza sono disponibili nell'interfaccia grafica utente della finestra di dialogo *Help* > Licenses.

B.8 Abbreviazioni utilizzate

ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DUID	DHCP Unique Identifier
EUI	Extended Unique Identifier
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv6	Internet Protocol version 6
LDRA	Lightweight DHCPv6 Relay Agent
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
NDP	Neighbor Discovery Protocol
NMS	Network Management System
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol

URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

C Indice

R

V

W