Modicon

MCSESM, MCSESM-E, MCSESP Switch con Management
Manuale di riferimento GUI

QGH59089.02

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.

Note sull'interfaccia grafica utente

Il dispositivo supporta i seguenti sistemi operativi:
- Windows 10
- Linux

L'interfaccia grafica utente del dispositivo è divisa come illustrato di seguito:
- Area di navigazione
- Area finestra di dialogo
- Pulsanti

Area di navigazione

L'area di navigazione si trova sul lato sinistro dell'interfaccia grafica utente.

L'area di navigazione include i seguenti elementi:
- Barra degli strumenti
- Filtro
- Menu

È possibile comprimere l'intera area di navigazione, ad esempio quando si visualizza l'interfaccia grafica utente su schermi piccoli. Per la compressione o l'espansione, fare clic sulla freccetta in alto nell'area di navigazione.

Barra degli strumenti

La barra degli strumenti in alto nella barra di navigazione contiene diversi pulsanti.
- Posizionando il puntatore del mouse sopra un pulsante, una descrizione comando visualizza ulteriori informazioni.
- In caso di perdita di connessione al dispositivo, la barra degli strumenti è di colore grigio.

Il dispositivo aggiorna automaticamente le informazioni della barra degli strumenti ogni 5 secondi.

Facendo clic sul pulsante si aggiorna manualmente la barra degli strumenti.

Posizionando il puntatore del mouse sopra il pulsante, una descrizione comando visualizza le seguenti informazioni:
- *User:*
  Nome dell'utente che ha effettuato l'accesso
- *Device name:*
  Nome del dispositivo

Facendo clic sul pulsante, si apre la finestra di dialogo *Device Security > User Management*.

Posizionando il puntatore del mouse sopra il pulsante, una descrizione comando visualizza il riepilogo della finestra di dialogo *Diagnostics > System > Configuration Check*.

Facendo clic sul pulsante, si apre la finestra di dialogo *Diagnostics > System > Configuration Check*.

Facendo clic sul pulsante, si chiude la sessione dell'utente attuale e compare la finestra di dialogo di accesso.

Se il profilo di configurazione nella memoria volatile (*RAM*) e il profilo di configurazione “Selezionato” nella memoria non volatile (*NVM*) sono diversi, il dispositivo mostra la finestra di dialogo *Warning*.

- Per salvare le modifiche in maniera permanente, fare clic sul pulsante *Yes* nella finestra di dialogo *Warning*.
- Per rifiutare le modifiche, fare clic sul pulsante *No* nella finestra di dialogo *Warning*.

Visualizza il tempo rimanente in secondi, finché si chiude automaticamente la sessione dell'utente inattivo.

Facendo clic sul pulsante, si apre la finestra di dialogo *Device Security > Management Access > Web*. Qui è possibile specificare il timeout.

Questo pulsante è visibile quando il profilo di configurazione nella memoria volatile (*RAM*) differisce dal profilo di configurazione “Selected” (Selezionato) nella memoria non volatile (*NVM*). Altrimenti il pulsante è nascosto.

Facendo clic sul pulsante, si apre la finestra di dialogo *Basic Settings > Load/Save*.

Facendo clic con il tasto destro del mouse sul pulsante, è possibile salvare le impostazioni attuali nella memoria non volatile (*NVM*).

Posizionando il puntatore del mouse sopra il pulsante, una descrizione comando visualizza le seguenti informazioni:

- *Device Status:* Questa sezione visualizza una schermata compressa del frame *Device status* nella finestra di dialogo *Basic Settings > System*. Questa sezione visualizza l'allarme che è attualmente attivo e il cui verificarsi è stato registrato per primo.
- *Security Status:* Questa sezione visualizza una schermata compressa del frame *Security status* nella finestra di dialogo *Basic Settings > System*. Questa sezione visualizza l'allarme che è attualmente attivo e il cui verificarsi è stato registrato per primo.
- *Boot Parameter:* Salvando costantemente le modifiche delle impostazioni e almeno un parametro di avvio differisce dal profilo di configurazione utilizzato durante l'ultimo riavvio, questa sezione visualizza una nota.
  Le seguenti impostazioni determinano la modifica dei parametri di avvio:
  - Finestra di dialogo *Basic Settings > External Memory*, parametro *Software auto update*
  - Finestra di dialogo *Basic Settings > External Memory*, parametro *Config priority*
  - Finestra di dialogo *Device Security > Management Access > Server*, scheda *SNMP*, parametro *UDP port*
  - Finestra di dialogo *Diagnostics > System > Selftest*, parametro *RAM test*
  - Finestra di dialogo *Diagnostics > System > Selftest*, parametro *SysMon1 is available*
  - Finestra di dialogo *Diagnostics > System > Selftest*, parametro *Load default config on error*

Facendo clic sul pulsante, si apre la finestra di dialogo *Diagnostics > Status Configuration > Device Status*.

Filtro

Il filtro consente la riduzione del numero di voci di menu nel menu. Applicando il filtro, il menu visualizza solo voci di menu che corrispondono alla stringa di ricerca immessa nel campo del filtro.

Menu

Il menu visualizza le voci di menu.

È possibile applicare filtri alle voci di menu. Vedere la sezione “Filtro”.

Per visualizzare la finestra di dialogo corrispondente nell'area della finestra, selezionare la voce di menu desiderata. Se la voce di menu selezionata è un nodo contenente sottovoci, il nodo si espande o comprime con un clic. L'area della finestra di dialogo mantiene visualizzata la finestra precedente.

È possibile espandere o comprimere contemporaneamente ogni nodo del menu. Facendo clic con il tasto destro del mouse in qualunque punto del menu, un menu contestuale visualizza le seguenti voci:

- *Expand*
  Espande contemporaneamente ogni nodo del menu. Il menu visualizza le voci di menu per ogni livello.
- *Collapse*
  Comprime contemporaneamente ogni nodo del menu. Il menu visualizza le voci di menu di livello superiore.

Area finestra di dialogo

L'area finestra di dialogo si trova sul lato destro dell'interfaccia grafica utente. Facendo clic su una voce di menu nell'area di navigazione, l'area finestra di dialogo visualizza la finestra corrispondente.

Aggiornamento della visualizzazione

Se una finestra di dialogo rimane aperta per un periodo di tempo piuttosto lungo, è possibile che nel frattempo i valori nel dispositivo siano cambiati.

- ☐ Per aggiornare la visualizzazione della finestra di dialogo, fare clic sul pulsante  . Le informazioni non salvate nella finestra di dialogo vanno perse.

Salvataggio delle impostazioni

Salvataggio, trasferimento delle impostazioni modificate sulla memoria volatile (*RAM*) del dispositivo. Eseguire il seguente passaggio:

- ☐ Fare clic sul pulsante  .

Per mantenere le impostazioni modificate anche dopo il riavvio del dispositivo, eseguire i seguenti passaggi:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.
- ☐ Nella tabella, evidenziare il profilo di configurazione desiderato.
- ☐ Quando nella colonna *Selected* la casella di spunta è `non selezionato`, fare clic sul pulsante  e poi sulla voce *Select*.
- ☐ Fare clic sul pulsante  e poi sulla voce *Save*.

Nota: Le modifiche involontarie delle impostazioni possono interrompere il collegamento tra il proprio PC e il dispositivo. Per mantenere il dispositivo accessibile, attivare la funzione *Undo configuration modifications* nella finestra di dialogo *Basic Settings > Load/Save*, prima di modificare qualsiasi impostazione. Utilizzando la funzione, il dispositivo continua a controllare se è ancora raggiungibile dall'indirizzo IP del PC utilizzato. In caso di perdita di connessione al dispositivo, il dispositivo carica il profilo di configurazione salvato nella memoria non volatile (*NVM*) dopo il tempo specificato. Dopodiché, è possibile accedere nuovamente al dispositivo.

Lavoro con le tabelle

La finestra di dialogo visualizza le numerosi impostazioni in forma tabellare.

Modificando una cella della tabella, la cella della tabella visualizza un contrassegno rosso nell'angolo sinistro superiore. Il contrassegno rosso indica che le modifiche non sono state ancora trasferite nella memoria volatile (*RAM*) del dispositivo.

È possibile personalizzare l'aspetto delle tabelle in base alle proprie esigenze. Posizionando il puntatore del mouse sopra l'intestazione di una colonna, l'intestazione visualizza un pulsante con elenco a discesa. Facendo clic su questo pulsante, l'elenco a discesa visualizza le seguenti voci:

- ▶ Ordine crescente
  Organizza le voci della tabella in ordine crescente sulla base delle voci della colonna selezionata.
  Una freccia nell'intestazione colonna indica l'ordine delle voci della tabella.

- Ordine decrescente
  Organizza le voci della tabella in ordine decrescente sulla base delle voci della colonna selezionata.
  Una freccia nell'intestazione colonna indica l'ordine delle voci della tabella.
- Colonne
  Visualizza o nasconde le colonne.
  Si riconoscono le colonne nascoste da una casella di spunta non selezionata nell'elenco a discesa.
- Filtri
  La tabella visualizza solamente le voci il cui contenuto corrisponde ai criteri filtro specificati della colonna selezionata.
  Un'intestazione colonna evidenziata indica le voci della tabella con filtro.

È possibile selezionare più voci della tabella simultaneamente e quindi applicarvi un'azione. È utile quando si intende rimuovere contemporaneamente più voci della tabella.

- Selezionare diverse voci consecutive della tabella:
  - ☐ Fare clic sulla prima voce d'interesse della tabella per evidenziarla.
  - ☐ Premere e tenere premuto il tasto <MAIUSC>.
  - ☐ Fare clic sull'ultima voce d'interesse della tabella per evidenziare ogni voce d'interesse della tabella.
- Selezionare più singole voci della tabella:
  - ☐ Fare clic sulla prima voce d'interesse della tabella per evidenziarla.
  - ☐ Premere e tenere premuto il tasto <CTRL>.
  - ☐ Fare clic sulla voce d'interesse successiva per evidenziarla.
    Ripetere finché sono evidenziate tutte le voce d'interesse della tabella.

Pulsanti

Qui è riportata la descrizione dei pulsanti standard. Questi speciali pulsanti specifici della finestra di dialogo sono descritti nel corrispondente testo della guida della finestra.

Trasferisce le modifiche alla memoria volatile (*RAM*) del dispositivo e le applica al dispositivo. Per salvare le modifiche nella memoria non volatile, procedere come di seguito illustrato:

- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save*.
- ☐ Nella tabella, evidenziare il profilo di configurazione desiderato.
- ☐ Quando nella colonna *Selected* la casella di spunta è `non selezionato`, fare clic sul pulsante  e poi sulla voce *Select*.
- ☐ Fare clic sul pulsante  per salvare le attuali modifiche.

Aggiorna i campi con i valori che sono salvati nella memoria volatile (*RAM*) del dispositivo.

Trasferisce le impostazioni dalla memoria volatile (*RAM*) nel profilo di configurazione definito come “Selected” (Selezionato) nella memoria non volatile (*NVM*).

Quando nella finestra di dialogo *Basic Settings > External Memory* è selezionata la casella di spunta nella colonna *Backup config when saving*, il dispositivo genera una copia del profilo di configurazione nella memoria esterna.

Visualizza un sottomenu con voci di menu corrispondenti alla relativa finestra di dialogo.

Apre la finestra di dialogo *Wizard*.

Aggiunge una nuova voce tabella.

Rimuove la voce tabella evidenziata.

Apre la guida online.

1 Basic Settings

Il menu include le seguenti finestre di dialogo:
- System
- Network
- Out of Band over USB
- Software
- Load/Save
- External Memory
- Port
- Power over Ethernet (MCSESP)
- Restart

1.1 System

[Basic Settings > System]

In questa finestra di dialogo si monitorano i singoli modi operativi.

Device status

I campi in questo frame mostrano lo stato del dispositivo e informano sugli allarmi che si sono attivati. Quando un allarme è attualmente attivo, il frame è evidenziato.

Si specificano i parametri che il dispositivo monitora nella finestra di dialogo *Diagnostics > Status Configuration > Device Status*.

Nota: Se si collega un solo alimentatore per la tensione di alimentazione a un dispositivo con un alimentatore ridondante, il dispositivo segnala un allarme. Per contribuire a evitare questo allarme si disattiva il monitoraggio degli alimentatori mancanti nella finestra di dialogo *Diagnostics > Status Configuration > Device Status*.

Alarm counter

Mostra il numero di allarmi attualmente attivi.

Quando vi è almeno un allarme attualmente attivo, l'icona è visibile.

Quando si posiziona il puntatore del mouse sull'icona, un suggerimento mostra la causa degli allarmi attualmente attivi e l'orario in cui il dispositivo ha innescato l'allarme.

Se un parametro monitorato è diverso dallo stato desiderato, il dispositivo innesca un allarme. La finestra di dialogo *Diagnostics > Status Configuration > Device Status*, scheda *Status* mostra una panoramica degli allarmi.

Security status

I campi in questo frame mostrano lo stato di sicurezza e informano sugli allarmi che si sono attivati. Quando un allarme è attualmente attivo, il frame è evidenziato.

Si specificano i parametri che il dispositivo monitora nella finestra di dialogo *Diagnostics > Status Configuration > Security Status*.

Alarm counter

Mostra il numero di allarmi attualmente attivi.

Quando vi è almeno un allarme attualmente attivo, l'icona è visibile.

Quando si posiziona il puntatore del mouse sull'icona, un suggerimento mostra la causa degli allarmi attualmente attivi e l'orario in cui il dispositivo ha innescato l'allarme.

Se un parametro monitorato è diverso dallo stato desiderato, il dispositivo innesca un allarme. La finestra di dialogo *Diagnostics > Status Configuration > Security Status*, scheda *Status* mostra una panoramica degli allarmi.

Signal contact status

I campi in questo frame mostrano lo stato del contatto di segnalazione e informano sugli allarmi che si sono verificati. Quando un allarme è attualmente attivo, il frame è evidenziato.

Si specificano i parametri che il dispositivo monitora nella finestra di dialogo *Diagnostics > Status Configuration > Signal Contact > Signal Contact 1*/*Signal Contact 2*.

Alarm counter

Mostra il numero di allarmi attualmente attivi.

Quando vi è almeno un allarme attualmente attivo, l'icona è visibile.

Quando si posiziona il puntatore del mouse sull'icona, un suggerimento mostra la causa degli allarmi attualmente attivi e l'orario in cui il dispositivo ha innescato l'allarme.

Se un parametro monitorato è diverso dallo stato desiderato, il dispositivo innesca un allarme. La finestra di dialogo *Diagnostics > Status Configuration > Signal Contact > Signal Contact 1*/*Signal Contact 2*, scheda *Status* mostra una panoramica degli allarmi.

System data

I campi in questo frame mostrano i dati operativi e le informazioni sulla posizione del dispositivo.

System name

Specifica il nome per il quale il dispositivo è conosciuto nella rete.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri
  Sono consentiti i seguenti caratteri:
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`
  - `<device name>-<MAC address>` (impostazione di default)

Durante la creazione di certificati HTTPS X.509, l'applicazione che genera il certificato utilizza il valore specificato come nome di dominio e nome comune.

Le seguenti funzioni utilizzano il valore specificato come nome dell'host o FQDN (Fully Qualified Domain Name). Per motivi di compatibilità, si raccomanda l'utilizzo esclusivo di lettere minuscole dato che non tutti i sistemi confrontano lo stile del testo nel FQDN. Verificare che questo nome sia univoco nell'intera rete.

- Client DHCP
- *Syslog*
- *IEC61850-MMS*

Location

Specifica la posizione del dispositivo.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Contact person

Specifica il referente per questo dispositivo.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Device type

Mostra il nome del prodotto del dispositivo.

Power supply 1
Power supply 2

Mostra lo stato dell'alimentatore sul collegamento dell'alimentazione di tensione corrispondente.

Possibili valori:

- *present*
- *defective*

- *not installed*
- *unknown*

Uptime

Mostra il tempo trascorso dall'ultimo riavvio del dispositivo.

Possibili valori:

- Ora nel formato `giorno/i, ...h, ...m, ...s`.

Temperature [°C]

Mostra la temperatura attuale nel dispositivo in °C.

Il monitoraggio delle soglie della temperatura si attiva nella finestra di dialogo *Diagnostics > Status Configuration > Device Status*.

Upper temp. limit [°C]

Specifica la soglia superiore della temperatura in °C.

Possibili valori:

- `-99..99` (integer)
  Se la temperatura nel dispositivo supera questo valore, il dispositivo genera un allarme.

Lower temp. limit [°C]

Specifica la soglia inferiore della temperatura in °C.

Possibili valori:

- `-99..99` (integer)
  Se la temperatura nel dispositivo scende al di sotto di questo valore, il dispositivo genera un allarme.

LED status

Questo frame mostra gli stati dei LED di stato del dispositivo al momento dell'ultimo aggiornamento. Il manuale utente di “Installazione” comprende informazioni dettagliate sui LED di stato del dispositivo.

Parametri	Colore	Significato
Status	●	Attualmente non vi è alcun allarme di stato del dispositivo. Lo stato del dispositivo è OK.
	●	Attualmente vi è almeno un allarme di stato del dispositivo. Di conseguenza, vedere il frame *Device status* di cui sopra.
Power	●	Versione del dispositivo con 2 alimentatori: Una sola tensione di alimentazione è attiva.
	●	Versione del dispositivo con 1 alimentatore: La tensione di alimentazione è attiva. Versione del dispositivo con 2 alimentatori: Entrambe le tensioni di alimentazione sono attive.

Parametri	Colore	Significato
EAM	●	Nessuna memoria esterna collegata.
	●	La memoria esterna è collegata, ma non è pronta per il funzionamento.
	●	La memoria esterna è collegata ed è pronta per il funzionamento.

Port status

Questo frame mostra una vista semplificata delle porte del dispositivo al momento dell'ultimo aggiornamento.

Le icone rappresentano lo stato delle singole porte. In alcune situazioni, le seguenti icone interferiscono l'una con l'altra. Quando si posiziona il puntatore del mouse sull'icona della porta appropriata, un tooltip mostra informazioni dettagliate sullo stato della porta.

Parametri	Stato	Significato
`<Numero di porta>`		La porta non è attiva. La porta non invia o riceve alcun dato.
		La porta non è attiva. Il cavo è collegato. Collegamento attivo.
		La porta è attiva. Nessun cavo collegato o collegamento attivo.
		La porta è attiva. Il cavo è collegato. Collegamento okay. Collegamento attivo. Modalità full-duplex
		La modalità half-duplex è abilitata. Verificare le impostazioni nella finestra di dialogo *Basic Settings > Ports*, scheda *Configuration*.
		La porta è in stato di blocco dovuto alla funzionalità di ridondanza.
		La porta funziona come un'interfaccia di router.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

1.2 Network

[Basic Settings > Network]

Il menu include le seguenti finestre di dialogo:
- Global
- IPv4
- IPv6

1.2.1 Global

[Basic Settings > Network > Global]

Questa finestra di dialogo consente di specificare VLAN e Ethernet Switch Configurator impostazioni richieste per l'accesso alla gestione del dispositivo attraverso la rete.

Management interface

Questo frame consente di specificare la VLAN in cui è possibile accedere alla gestione del dispositivo.

VLAN ID

Specifica la VLAN in cui è possibile accedere alla gestione del dispositivo attraverso la rete. È possibile accedere alla gestione del dispositivo attraverso le porte che fanno parte di questa VLAN.

Possibili valori:

- `1..4042` (impostazione di default: `1`)
  Il prerequisito è che la VLAN sia già configurata. Vedere la finestra di dialogo *Switching > VLAN > Configuration*.

Quando si fa clic sul pulsante ☑ dopo aver cambiato il valore, si apre la finestra *Information*. Selezionare la porta attraverso la quale si effettuerà il collegamento al dispositivo in futuro. Dopo aver fatto clic sul pulsante *Ok*, le nuove impostazioni VLAN di gestione del dispositivo sono assegnate alla porta.

- In seguito, la porta fa parte della VLAN e trasmette i pacchetti dati senza una tag VLAN (non taggata). Vedere la finestra di dialogo *Switching > VLAN > Configuration*.
- Il dispositivo assegna la porta ID VLAN della VLAN di gestione del dispositivo alla porta. Vedere la finestra di dialogo *Switching > VLAN > Port*.

Dopo un breve periodo il dispositivo è raggiungibile attraverso la nuova porta nella nuova VLAN di gestione del dispositivo.

MAC address

Mostra l'indirizzo MAC del dispositivo. La gestione del dispositivo è accessibile attraverso la rete utilizzando l'indirizzo MAC.

Ethernet Switch Configurator protocol v1/v2

Questo frame consente di specificare le impostazioni per l'accesso al dispositivo utilizzando il protocollo Ethernet Switch Configurator.

Su un PC, il software Ethernet Switch Configurator mostra i Schneider Electric dispositivi accessibili nella rete su cui la funzione Ethernet Switch Configurator è abilitata. È possibile accedere a tali dispositivi anche se dispongono di parametri IP non validi o se non dispongono di alcun parametro IP assegnato. Il software Ethernet Switch Configurator consente di assegnare o modificare i parametri IP nel dispositivo.

Nota: Con il software Ethernet Switch Configurator è possibile accedere al dispositivo solo attraverso le porte che fanno parte delle stesse VLAN della gestione del dispositivo. Nella finestra di dialogo *Switching > VLAN > Configuration* si specifica a quale VLAN è assegnata una certa porta.

Operation

Abilita/disabilita la funzione Ethernet Switch Configurator nel dispositivo.

Possibili valori:

- *On* (impostazione di default)
  Ethernet Switch Configurator è abilitato.
  È possibile utilizzare il software Ethernet Switch Configurator per accedere al dispositivo dal proprio PC.
- *Off*
  Ethernet Switch Configurator è disabilitato.

Access

Abilita/disabilita l'accesso in scrittura al dispositivo utilizzando Ethernet Switch Configurator.

Possibili valori:

- *readWrite* (impostazione di default)
  Il software Ethernet Switch Configurator dispone dell'accesso in scrittura al dispositivo.
  Con queste impostazioni è possibile modificare i parametri IP nel dispositivo.
- *readOnly*
  Il software Ethernet Switch Configurator dispone dell'accesso in sola lettura al dispositivo.
  Con queste impostazioni è possibile vedere i parametri IP nel dispositivo.

Raccomandazione: modificare queste impostazioni sul valore *readOnly* solo dopo aver azionato il dispositivo.

Signal

Attiva/disattiva il lampeggiamento dei LED della porta così come la funzione omonima nel software Ethernet Switch Configurator. La funzione consente di identificare il dispositivo nel campo.

Possibili valori:

- selezionato
  Il lampeggiamento dei LED della porta è attivo.
  I LED della porta lampeggiano finché non si disabilita nuovamente la funzione.
- non selezionato (impostazione di default)
  Il lampeggiamento dei LED della porta non è attivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

1.2.2 IPv4

[Basic Settings > Network > IPv4]

Questa finestra di dialogo consente di specificare le impostazioni IPv4 richieste per l'accesso alla gestione del dispositivo attraverso la rete.

Management interface

IP address assignment

Specifica l'origine da cui la gestione del dispositivo riceve i suoi parametri IP.

Possibili valori:

- `Local`
  Il dispositivo utilizza i parametri IP dalla memoria interna. Le impostazioni per fare ciò devono essere specificate nel frame *IP parameter*.
- `BOOTP`
  Il dispositivo riceve i suoi parametri IP da un server BOOTP o DHCP.
  Il server valuta l'indirizzo MAC del dispositivo, poi assegna i parametri IP.
- `DHCP` (impostazione di default)
  Il dispositivo riceve i suoi parametri IP da un server DHCP.
  Il server valuta l'indirizzo MAC, il nome DHCP, o altri parametri del dispositivo, poi assegna i parametri IP.
  Quando il server fornisce anche gli indirizzi dei server DNS, il dispositivo li visualizza nella finestra di dialogo *Advanced > DNS > Cache > Current*.

Nota: In caso di mancata risposta dal server BOOTP o DHCP, il dispositivo imposta l'indirizzo IP su `0.0.0.0` ed esegue un altro tentativo di ottenere un indirizzo IP valido.

BOOTP/DHCP

Client ID

Mostra l'ID client DHCP che il dispositivo invia al server BOOTP o DHCP. Se il server è configurato di conseguenza, riserva un indirizzo IP per questo ID client DHCP. Di conseguenza, il dispositivo riceve lo stesso IP dal server ogni volta che lo richiede.

L'ID client DHCP che il dispositivo invia è il nome del dispositivo specificato nel campo *System name* nella finestra di dialogo *Basic Settings > System*.

DHCP option 66/67/4/42

Abilita/disabilita la funzione *DHCP option 66/67/4/42* nel dispositivo.

Possibili valori:

- *On* (impostazione di default)
  È abilitata la funzione *DHCP option 66/67/4/42*.
  Il dispositivo carica il profilo di configurazione e riceve le informazioni del server orario utilizzando le seguenti opzioni DHCP:
  - `Option 66: TFTP server name`
    `Option 67: Boot file name`
    Il dispositivo carica automaticamente il profilo di configurazione dal server DHCP nella memoria volatile (*RAM*) utilizzando il protocollo TFTP. Il dispositivo utilizza le impostazioni del profilo di configurazione importato nel `running-config`.
  - `Option 4: Time Server`
    `Option 42: Network Time Protocol Servers`
    Il dispositivo riceve le informazioni del server orario da un server DHCP.
- *Off*
  È disabilitata la funzione *DHCP option 66/67/4/42*.
  - Il dispositivo non carica il profilo di configurazione utilizzando le Opzioni DHCP 66/67:
  - Il dispositivo non riceve le informazioni del server orario utilizzando le Opzioni DHCP 4/42.

IP parameter

Questo frame consente di assegnare i parametri IP manualmente. In caso di selezione del pulsante di opzione `Local` nel frame *Management interface*, elenco delle opzioni *IP address assignment*, è possibile modificare questi campi.

IP address

Specifica l'indirizzo IP sotto il quale è possibile accedere alla gestione del dispositivo attraverso la rete.

Possibili valori:

- Indirizzo IPv4 valido

Netmask

Specifica la maschera di rete.

Possibili valori:

- Maschera di rete IPv4 valida

Gateway address

Specifica l'indirizzo IP di un router attraverso il quale il dispositivo accede ad altri dispositivi all'esterno della propria rete.

Possibili valori:

- Indirizzo IPv4 valido

Remaining lease time

Lease time [s]

Visualizza il tempo rimanente in secondi nel quale è ancora valido l'indirizzo IP che il server DHCP ha assegnato alla gestione del dispositivo.

Per aggiornare la visualizzazione, fare clic sul pulsante  .

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

1.2.3 IPv6

[Basic Settings > Network > IPv6]

Questa finestra di dialogo consente di specificare le impostazioni IPv6 richieste per l'accesso alla gestione del dispositivo attraverso la rete.

Operation

Operation

Abilita/disabilita il protocollo IPv6 nel dispositivo.

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.

Possibili valori:

- *On* (impostazione di default)
  Il protocollo IPv6 è attivato.
- *Off*
  Il protocollo IPv6 è disattivato.
  Per far in modo che il dispositivo operi solamente utilizzando il protocollo IPv4 disattivare il protocolo IPv6 nel dispositivo.

Configuration

Dynamic IP address assignment

Specifica l'origine da cui la gestione del dispositivo riceve i suoi parametri IPv6.

Possibili valori:

- *None*
  Il dispositivo riceve i suoi parametri IPv6 manualmente.
  È possibile specificare un numero massimo di 4 indirizzi IPv6. Non è possibile specificare indirizzi loopback, link-local e *Multicast* come indirizzi IPv6 statici.
- *Auto* (Impostazione di default)
  Il dispositivo riceve i suoi parametri IPv6 dinamicamente. Il dispositivo riceve un massimo di 2 indirizzi IPv6.
  Ne è un esempio il Router Advertisement Daemon (radvd). Il radvd utilizza messaggi *Router Solicitation* e *Router Advertisement* per configurare automaticamente un indirizzo IPv6. I messaggi *Router Solicitation* e *Router Advertisement* sono descritti in RFC 4861.
- *DHCPv6*
  Il dispositivo riceve i suoi parametri IPv6da un server DHCPv6.
- *All*
  Selezionando il pulsante di opzione *All*, il dispositivo riceve i suoi parametri IPv6 utilizzando tutte le alternative per le assegnazioni dinamiche e manuali.

DHCP

Client ID

Mostra l'ID client DHCPv6 che il dispositivo invia al server DHCPv6. Se il server è configurato di conseguenza, riceve un indirizzo IPv6 per questo ID client DHCPv6.

L'indirizzo IPv6 ricevuto dal server DHCPv6 ha un *PrefixLength* di `128`. Secondo RFC 8415, al momento un server DHCPv6 non può essere utilizzato per fornire informazioni *Gateway address* o *PrefixLength*.

Il dispositivo può ricevere solamente un indirizzo IPv6 dal server DHCPv6.

IP parameter

Gateway address

Specifica l'indirizzo IPv6 di un router attraverso il quale il dispositivo accede ad altri dispositivi all'esterno della propria rete.

Possibili valori:

- Indirizzo IPv6 valido (eccetto indirizzi di loopback e *Multicast*)

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.

Duplicate Address Detection

In questo campo è possibile specificare il numero di messaggi *Neighbor Solicitation* consecutivi che il dispositivo invia per la funzione *Duplicate Address Detection*. Questa funzione serve per determinare l'unicità di un indirizzo unicast IPv6 sull'interfaccia.

Number of neighbor solicitants

Specifica il numero di messaggi *Neighbor Solicitation* che il dispositivo invia per la funzione *Duplicate Address Detection*.

Possibili valori:

- `0`
  La funzione è disabilitata.
- `1..5` (impostazione di default: `1`)

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).

Tabella

Questa tabella visualizza un elenco degli indirizzi IPv6 configurati per la gestione del dispositivo.

Prefix

Visualizza il prefisso dell'indirizzo IPv6 in formato compresso. Il prefisso mostra i bit più a sinistra di un indirizzo IPv6, ovvero la parte della rete dell'indirizzo.,

PrefixLength

Visualizza la lunghezza del prefisso dell'indirizzo IPv6.

Diversamente da un indirizzo IPv4, l'indirizzo IPv6 non utilizza una maschera di sottorete per identificare la parte della rete di un'indirizzo. Nel IPv6 questo ruolo è svolto dalla lunghezza del prefisso.

Possibili valori:

- `0..128`

IP address

Visualizza l'intero indirizzo IPv6 in formato compresso.

Il formato compresso viene applicato automaticamente a tutti gli indirizzi IPv6, indipendentemente dall'origine da cui la gestione del dispositivo riceve i parametri del suo IPv6.

Possibili valori:

- Indirizzo IPv6 valido
  Per utilizzare un indirizzo IPv6 in un URL utilizzare la seguente sintassi URL: `https://[<ipv6_indirizzo>]`.

Per ulteriori informazioni sulle regole di compressione e i tipi di indirizzo IPv6, consultare il manuale "Configurazione".

EUI option

Specifica se la funzione *EUI option* è applicata all'indirizzo IPv6.

Selezionando questa casella di spunta, l'ID di interfaccia dell'indirizzo IPv6 viene configurato automaticamente. 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 solamente per gli indirizzi IPv6 che hanno una lunghezza di prefisso uguale a `64`.

Possibili valori:

- `selezionato`
  La funzione *EUI option* è attiva.
- `non selezionato` (impostazione di default)
  La funzione *EUI option* non è attiva.

Origin

Specifica il modo in cui il dispositivo ha ricevuto i suoi parametri IPv6.

Possibili valori:

- *Autoconf*
  Il dispositivo ha ricevuto l'indirizzo IPv6 dinamicamente se il pulsante di opzione *Auto* è selezionato.
- *Manual*
  Il dispositivo ha ricevuto l'indirizzo IPv6 manualmente.
- *DHCP*
  Il dispositivo ha ricevuto l'indirizzo IPv6da un server DHCPv6.
- *Linklayer*
  Il dispositivo configura automaticamente un indirizzo IPv6 di tipo link-local. Non è possibile modificare l'indirizzo loopback.

Status

Visualizza lo stato attuale dell'indirizzo IPv6.

Possibili valori:

- *active*
  L'indirizzo IPv6 è attivo.
- *notInService*
  L'indirizzo IPv6 non è attivo.
- *notReady*
  L'indirizzo IPv6 è specificato ma attualmente non *active* perché mancano ancora alcuni parametri.

Nota: Se l'indirizzo IPv6 viene specificato manualmente è possibile passare manualmente tra gli stati *active* e *notInService*. Per eseguire questa modifica selezionare lo stato necessario nell'elenco a discesa relativo alla voce interessata nella colonna *Status*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

1.3 Out of Band over USB

[Basic Settings > Out of Band over USB]

Il dispositivo è dotato di un'interfaccia di rete USB 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 l'interfaccia di rete USB per accedere alla gestione del dispositivo.

Il dispositivo consente di accedere alla gestione del dispositivo attraverso l'interfaccia di rete USB utilizzando i seguenti protocolli:

- HTTP
- HTTPS

- SSH
- Telnet
- SNMP
- FTP
- TFTP
- SFTP
- SCP

Durante l'accesso alla gestione del dispositivo vi sono le seguenti restrizioni:
- La stazione di gestione è collegata direttamente alla porta USB.
- L' interfaccia di rete USB non supporta le seguenti caratteristiche:
  - Pacchetti taggati per priorità
  - Pacchetti che includono una tag *VLAN*
  - *DHCP L2 Relay*
  - *LLDP*
  - *DiffServ*
  - *ACL*
  - *Industrial Protocols*

In questa finestra di dialogo, il dispositivo consente di modificare i parametri IP e di disabilitare l'interfaccia di rete USB, se necessario.

Operation

Operation

Abilita/disabilita l'interfaccia di rete USB.

Possibili valori:
- `On` (impostazione di default)
  Il dispositivo consente di accedere alla gestione del dispositivo attraverso l'interfaccia di rete USB.
- `Off`
  Il dispositivo non consente di accedere alla gestione del dispositivo attraverso l'interfaccia di rete USB.

Management interface

Device MAC address

Visualizza l'indirizzo MAC dell'interfaccia di rete USB.

Host MAC address

Visualizza l'indirizzo MAC della network management station collegata.

IP parameter

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

IP address

Specifica l'indirizzo IP della gestione del dispositivo per accedere attraverso l'interfaccia di rete USB.

Possibili valori:

- Indirizzo IPv4 valido
  (Impostazione di default: `91.0.0.100`)
  Il dispositivo assegna questo indirizzo IP, aumentato di 1, alla network management station collegata al dispositivo.
  Esempio: `91.0.0.100` per l'interfaccia di rete USB, `91.0.0.101` per la network management station.

Netmask

Specifica la maschera di rete.

Possibili valori:

- Maschera di rete IPv4 valida
  (Impostazione di default: `255.255.255.0`)

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

1.4 Software

[Basic Settings > Software]

Questa finestra di dialogo consente di aggiornare il software del dispositivo e di mostrare le sue informazioni.

È inoltre possibile ripristinare un backup del software del dispositivo salvato nel dispositivo.

Nota: Prima di aggiornare il software del dispositivo seguire le note specifiche di versione nel file di testo `Readme`.

Version

Stored version

Mostra il numero della versione e la data di creazione del software del dispositivo memorizzato nella memoria flash. Il dispositivo carica il software del dispositivo durante il riavvio successivo.

Running version

Mostra il numero della versione e la data di creazione del software del dispositivo caricato dal dispositivo durante l'ultimo riavvio e attualmente in uso.

Backup version

Mostra il numero della versione e la data di creazione del software del dispositivo salvato come backup nella memoria flash. Il dispositivo ha copiato il software di questo dispositivo nella memoria di backup durante l'ultimo aggiornamento del software o dopo aver fatto clic sul pulsante *Restore*.

Restore

Ripristina il software del dispositivo salvato come backup. Durante il processo, il dispositivo modifica il *Stored version* e il *Backup version* del software del dispositivo.

Dopo il riavvio, il dispositivo carica il *Stored version*.

Bootcode

Mostra il numero della versione e la data di creazione del codice di avvio.

Software update

In alternativa, quando il file immagine è posizionato nella memoria esterna, il dispositivo consente di aggiornare il software del dispositivo facendo clic con il tasto destro nella tabella.

URL

Specifica il percorso e il nome del file del file immagine con cui si aggiorna il software del dispositivo.

Il dispositivo fornisce le seguenti opzioni per l'aggiornamento del software del dispositivo:

- Aggiornamento del software dal PC
  Quando il file è posizionato sul proprio PC o su un drive di rete, trascinare il file nell'area  . In alternativa, fare clic sull'area per selezionare il file.
- Aggiornamento del software da un server FTP
  Quando il file è posizionato su un server FTP, specificare l'URL per il file nella forma seguente:
  `ftp://<Utente>:<Password>@<Indirizzo IP>:<Porta>/<Nome file>`
- Aggiornamento del software da un server TFTP
  Quando il file è posizionato su un server TFTP, specificare l'URL per il file nella forma seguente:
  `tftp://<Indirizzo IP>/<Percorso>/<Nome file>`
- Aggiornamento del software da un server SCP o SFTP
  Quando il file è posizionato su un server SCP o SFTP, specificare l'URL per il file in una delle forme seguenti:
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`
    Facendo clic sul pulsante *Start*, il dispositivo visualizza la finestra *Credentials*. Qui si inseriscono *User name* e *Password* per accedere al server.
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`

Start

Aggiorna il software del dispositivo.

Il dispositivo installa il file selezionato nella memoria flash, sostituendo il software del dispositivo precedentemente salvato. Al riavvio, il dispositivo carica il software del dispositivo installato.

Il dispositivo copia il software esistente all'interno della memoria di backup.

Per mantenere l'accesso al dispositivo durante l'aggiornamento del software muovere il puntatore del mouse di tanto in tanto. In alternativa, specificare un valore sufficientemente elevato nella finestra di dialogo *Device Security > Management Access > Web*, campo *Web interface session timeout [min]* prima dell'aggiornamento del software.

Tabella

File location

Mostra la locazione di memoria del software del dispositivo.

Possibili valori:

- *ram*
  Memoria volatile del dispositivo

- *flash*
  Mostra non volatile (*NVM*) del dispositivo.
- *usb*
  Memoria USB esterna (EAM)

Index

Mostra l'indice del software del dispositivo.

Per il software del dispositivo nella memoria flash, l'indice ha il seguente significato:

- 1
  Al riavvio, il dispositivo carica il software di questo dispositivo.
- 2
  Il dispositivo ha copiato il software di questo dispositivo nell'area di backup durante l'ultimo aggiornamento del software.

File name

Mostra il nome del file interno al dispositivo del software del dispositivo.

Firmware

Mostra il numero della versione e la data di creazione del software del dispositivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

1.5 Load/Save

[Basic Settings > Load/Save]

Questa finestra di dialogo consente di salvare le impostazioni del dispositivo in maniera permanente in un profilo di configurazione.

Il dispositivo può contenere diversi profili di configurazione. Quando si attiva un profilo di configurazione alternativo si passa ad altre impostazioni del dispositivo. È possibile esportare i profili di configurazione sul proprio PC o su un server. È inoltre possibile importare nel dispositivo i profili di configurazione dal proprio PC o da un server.

Nelle impostazioni di default, il dispositivo salva i profili di configurazione non crittografati. Se si inserisce una password nel frame *Configuration encryption*, il dispositivo salva i profili di configurazione attuali e futuri in un formato crittografato.

Le modifiche involontarie delle impostazioni possono interrompere il collegamento tra il proprio PC e il dispositivo. Per mantenere il dispositivo accessibile, abilitare la funzione *Undo configuration modifications* prima di modificare qualsiasi impostazione. Se il collegamento è interrotto, il dispositivo carica il profilo di configurazione salvato nella memoria non volatile (*NVM*) dopo l'orario specificato.

External memory

Selected external memory

Mostra il tipo di memoria esterna.

Possibili valori:

- *usb*
  Memoria USB esterna (EAM)

Status

Mostra il modo operativo della memoria esterna.

Possibili valori:

- *notPresent*
  Nessuna memoria esterna collegata.
- *removed*
  Qualcuno ha rimosso la memoria esterna dal dispositivo durante il funzionamento.
- *ok*
  La memoria esterna è collegata ed è pronta per il funzionamento.
- *outOfMemory*
  Lo spazio di memoria è occupato nella memoria esterna.
- *genericErr*
  Il dispositivo ha rilevato un errore.

Configuration encryption

Active

Mostra se la crittografia della configurazione è attiva/non è attiva nel dispositivo.

Possibili valori:

- `selezionato`
  La crittografia della configurazione è attiva.
  Se il profilo di configurazione è crittografato e la password corrisponde a quella memorizzata nel dispositivo, il dispositivo carica un profilo di configurazione dalla memoria non volatile (*NVM*).
- `non selezionato`
  La crittografia della configurazione non è attiva.
  Se il profilo di configurazione non è crittografato, il dispositivo carica un profilo di configurazione solo dalla memoria non volatile (*NVM*).

Se nella finestra di dialogo *Basic Settings > External Memory* , la colonna *Config priority* presenta il valore `first` e il profilo di configurazione non è crittografato, il frame *Security status* nella finestra di dialogo *Basic Settings > System* mostra un allarme.

Nella finestra di dialogo *Diagnostics > Status Configuration > Security Status*, scheda *Global*, colonna *Monitor* si specifica se il dispositivo monitora il parametro *Load unencrypted config from external memory*.

Set password

Apre la finestra *Set password* che aiuta a inserire la password necessaria per la crittografia del profilo di configurazione. La crittografia dei profili di configurazione complica l'accesso non autorizzato. A tale scopo, eseguire i seguenti passaggi:

- ☐ Quando si modifica una password esistente, inserire la password esistente nel campo *Old password*. Per mostrare la password in chiaro invece che con gli ***** (asterischi), contrassegnare la casella di spunta *Display content*.
- ☐ Inserire la password nel campo *New password*.
  Per mostrare la password in chiaro invece che con gli ***** (asterischi), contrassegnare la casella di spunta *Display content*.
- ☐ Contrassegnare la casella di spunta *Save configuration afterwards* per utilizzare la crittografia anche per il profilo di configurazione Selezionato nella memoria non volatile (*NVM*) e nella memoria esterna.

Nota: Se un massimo di un profilo di configurazione è memorizzato nella memoria non volatile (*NVM*) del dispositivo, utilizzare solo questa funzione. Prima di creare ulteriori profili di configurazione, decidere a favore o contro la crittografia della configurazione attivata in modo permanente nel dispositivo. Salvare gli ulteriori profili di configurazione, crittografati o non crittografati, con la stessa password.

Se si sta sostituendo un dispositivo con un profilo di configurazione crittografato, per esempio a causa di un dispositivo non funzionante, eseguire i seguenti passaggi:

- ☐ Riavviare il nuovo dispositivo e assegnare i parametri IP.
- ☐ Aprire la finestra di dialogo *Basic Settings > Load/Save* sul nuovo dispositivo.
- ☐ Crittografare il profilo di configurazione nel nuovo dispositivo. Vedere sopra. Inserire la stessa password utilizzata nel dispositivo non funzionante.

- ☐ Installare la memoria esterna dal dispositivo non funzionante all'interno del nuovo dispositivo.
- ☐ Riavviare il nuovo dispositivo.
  Quando si riavvia il dispositivo, questo carica il profilo di configurazione con le impostazioni del dispositivo non funzionante dalla memoria esterna. Il dispositivo copia le impostazioni nella memoria volatile (*RAM*) e nella memoria non volatile (*NVM*).

Delete

Apre la finestra *Delete* che aiuta a cancellare la crittografia della configurazione nel dispositivo. Per cancellare la crittografia della configurazione, eseguire i seguenti passaggi:

- ☐ Inserire la password esistente nel campo *Old password*.
  Per mostrare la password in chiaro invece che con gli ***** (asterischi), contrassegnare la casella di spunta *Display content*.
- ☐ Contrassegnare la casella di spunta *Save configuration afterwards* per rimuovere la crittografia anche per il profilo di configurazione Selezionato nella memoria non volatile (*NVM*) e nella memoria esterna.

Nota: Se si mantengono ulteriori profili di configurazione crittografati nella memoria, il dispositivo aiuta a prevenire l'attivazione o la designazione di questi profili di configurazione come “Selezionati”.

Information

NVM in sync with running config

Mostra se il profilo di configurazione nella memoria volatile (*RAM*) e il profilo di configurazione “Selezionato” nella memoria non volatile (*NVM*) sono uguali.

Possibili valori:

- `selezionato`
  I profili di configurazione sono uguali.
- `non selezionato`
  I profili di configurazione sono diversi.

External memory in sync with NVM

Mostra se il profilo di configurazione “Selezionato” nella memoria esterna e il profilo di configurazione “Selezionato” nella memoria non volatile (*NVM*) sono uguali.

Possibili valori:

- `selezionato`
  I profili di configurazione sono uguali.
- `non selezionato`
  I profili di configurazione sono diversi.
  Possibili cause:
  - Nessuna memoria esterna è collegata al dispositivo.
  - Nella finestra di dialogo *Basic Settings > External Memory*, la funzione *Backup config when saving* è disabilitata.

Backup config on a remote server when saving

Operation

Abilita/disabilita la funzione *Backup config on a remote server when saving*.

Possibili valori:

- `Enabled`
  È abilitata la funzione *Backup config on a remote server when saving*.
  Quando si salva il profilo di configurazione nella memoria non volatile (*NVM*), il dispositivo esegue automaticamente il backup del profilo di configurazione sul server remoto specificato nel campo *URL*.
- `Disabled` (impostazione di default)
  È disabilitata la funzione *Backup config on a remote server when saving*.

URL

Specifica il percorso e il nome del file del profilo di configurazione sottoposto a backup sul server remoto.

Possibili valori:

- Stringa di caratteri ASCII con 0 .. 128 caratteri
  Esempio: `tftp://192.9.200.1/cfg/config.xml`
  Il dispositivo supporta i seguenti metacaratteri:
  - `%d`
    Data di sistema nel formato `YYYY-mm-dd`
  - `%t`
    Orario di sistema nel formato `HH_MM_SS`
  - `%i`
    Indirizzo IP del dispositivo
  - `%m`
    Indirizzo MAC del dispositivo nel formato `AA-BB-CC-DD-EE-FF`
  - `%p`
    Nome del prodotto del dispositivo

Set credentials

Apre la finestra *Credentials* che aiuta a inserire le credenziali necessarie per autenticarsi sul server remoto. A tale scopo, eseguire i seguenti passaggi:

- ☐ Inserire il nome utente nel campo *User name*.
  Per mostrare il nome utente in chiaro invece che con gli ***** (asterischi), selezionare la casella di spunta *Display content*.
  Possibili valori:
  - Stringa di caratteri ASCII alfanumerici con 1..32 caratteri
- ☐ Inserire la password nel campo *Password*.
  Per mostrare la password in chiaro invece che con gli ***** (asterischi), contrassegnare la casella di spunta *Display content*.
  Possibili valori:
  - Stringa di caratteri ASCII alfanumerici con 6..64 caratteri
    Sono consentiti i seguenti caratteri:

    ```
    a..z
    A..Z
    0..9
    !#$%&'()*+,-./:;<=>?@[\\]^_`{}~
    ```

Undo configuration modifications

Operation

Abilita/disabilita la funzione *Undo configuration modifications*. Utilizzando la funzione, il dispositivo continua a controllare se è ancora raggiungibile dall'indirizzo IP del PC utilizzato. Se dopo un intervallo di tempo specificato la porta è interrotta, il dispositivo carica il profilo di configurazione “Selezionato” dalla memoria non volatile (*NVM*). Dopodiché, è possibile accedere nuovamente al dispositivo.

Possibili valori:

- *On*
  la funzione è abilitata.
  - Si specifica l'intervallo di tempo tra l'interruzione del collegamento e il caricamento del profilo di configurazione nel campo *Timeout [s] to recover after connection loss*.
  - Quando la memoria non volatile (*NVM*) contiene diversi profili di configurazione, il dispositivo carica il profilo di configurazione designato come “Selezionato”.
- *Off* (impostazione di default)
  La funzione è disabilitata.
  Disabilitare nuovamente la funzione prima di chiudere l'interfaccia grafica utente. In questo modo si contribuisce a evitare che il dispositivo ripristini il profilo di configurazione designato come “Selezionato”.

Nota: Prima di abilitare la funzione, salvare le impostazioni nel profilo di configurazione. Le modifiche attuali, salvate temporaneamente, sono pertanto mantenute nel dispositivo.

Timeout [s] to recover after connection loss

Specifica il tempo, in secondi, dopo il quale il dispositivo carica il profilo di configurazione “Selezionato” dalla memoria non volatile (*NVM*) se la porta è interrotta.

Possibili valori:

- `30..600` (impostazione di default: `600`)

Specificare un valore sufficientemente alto. Prendere in considerazione l'ora in cui si visualizzano le finestre di dialogo dell'interfaccia grafica utente senza modificarle o aggiornarle.

Watchdog IP address

Mostra l'indirizzo IP del PC su cui è stata abilitata la funzione.

Possibili valori:

- Indirizzo IPv4 (impostazione di default: `0.0.0.0`)

Tabella

Storage type

Mostra la locazione di memoria del profilo di configurazione.

Possibili valori:

- *RAM* (memoria volatile del dispositivo)
  Nella memoria volatile, il dispositivo memorizza le impostazioni per il funzionamento corrente.

- `NVM` (memoria non volatile del dispositivo)
  Quando applica la funzione *Undo configuration modifications* o durante un riavvio, il dispositivo carica il profilo di configurazione “Selezionato” dalla memoria non volatile.
  La memoria non volatile fornisce spazio per diversi profili di configurazione, a seconda del numero delle impostazioni salvate nel profilo di configurazione. Il dispositivo gestisce un massimo di 20 profili di configurazione nella memoria non volatile.
  È possibile caricare un profilo di configurazione nella memoria volatile (`RAM`): A tale scopo, eseguire i seguenti passaggi:
  - ☐ Evidenziare il profilo di configurazione nella tabella.
  - ☐ Fare clic sul pulsante ☰ e poi sulla voce *Activate*.
- `ENVM` (memoria esterna)
  Il dispositivo salva una copia di backup del profilo di configurazione “Selezionato” nella memoria esterna.
  Il prerequisito è che si selezioni la casella di spunta *Backup config when saving* nella finestra di dialogo *Basic Settings > External Memory*.

Profile name

Mostra il nome del profilo di configurazione.

Possibili valori:

- `running-config`
  Nome del profilo di configurazione nella memoria volatile (`RAM`).
- `config`
  Nome del profilo di configurazione impostato dalla fabbrica nella memoria non volatile (`NVM`).
- Nome definito dall'utente
  Il dispositivo consente di salvare un profilo di configurazione, con un nome specificato dall'utente, evidenziando un profilo di configurazione esistente nella tabella, facendo clic sul pulsante ☰ e poi sulla voce *Save as...*.

Per esportare il profilo di configurazione come file XML sul proprio PC, cliccare sul collegamento. Poi, selezionare la locazione di memoria e specificare il nome del file.

Per salvare il file su un server remoto, fare clic sul pulsante ☰ e poi sulla voce *Export...*.

Modification date (UTC)

Mostra l'orario (UTC) in cui un utente ha salvato per l'ultima volta il profilo di configurazione.

Selected

Mostra se il profilo di configurazione è designato come “Selezionato”.

Per designare un altro profilo di configurazione come “Selezionato”, si evidenzia il profilo di configurazione desiderato nella tabella, si clicca sul pulsante ☰ e poi sulla voce *Activate*.

Possibili valori:

- `selezionato`
  Il profilo di configurazione è designato come “Selezionato”.
  - Quando applica la funzione *Undo configuration modifications* o durante un riavvio, il dispositivo carica il profilo di configurazione nella memoria volatile (`RAM`).
  - Quando si fa clic sul pulsante 💾, il dispositivo salva le impostazioni salvate temporaneamente in questo profilo di configurazione.
- `non selezionato`
  Un altro profilo di configurazione è designato come “Selezionato”.

Encrypted

Mostra se il profilo di configurazione è crittografato.

Possibili valori:

- `selezionato`
  Il profilo di configurazione è crittografato.
- `non selezionato`
  Il profilo di configurazione non è crittografato.

Nel frame *Configuration encryption* si attiva/disattiva la crittografia del profilo di configurazione.

Encryption verified

Mostra se la password del profilo di configurazione crittografato corrisponde alla password memorizzata nel dispositivo.

Possibili valori:

- `selezionato`
  La password corrisponde. Il dispositivo è in grado di decrittare il profilo di configurazione.
- `non selezionato`
  Le password non coincidono. Il dispositivo non è in grado di decrittare il profilo di configurazione.

Software version

Mostra il numero della versione del software del dispositivo che lo stesso utilizza durante il salvataggio del profilo di configurazione.

Fingerprint

Mostra la somma di controllo salvata nel profilo di configurazione.

Quando si salvano le impostazioni, il dispositivo calcola la somma di controllo e la inserisce all'interno del profilo di configurazione.

Fingerprint verified

Mostra se la somma di controllo salvata nel profilo di configurazione è valida.

Il dispositivo calcola la somma di controllo del profilo di configurazione contrassegnato come “Selezionato” e la confronta con la somma di controllo salvata in questo profilo di configurazione.

Possibili valori:

- `selezionato`
  La somma di controllo calcolata e la somma di controllo salvata corrispondono.
  Le impostazioni salvate sono coerenti.
- `non selezionato`
  Per il profilo di configurazione contrassegnato come “Selezionato”:
  La somma di controllo calcolata e la somma di controllo salvata sono diverse.
  Il profilo di configurazione contiene impostazioni modificate.
  Possibili cause:
  - Il file è danneggiato.
  - Il file system nella memoria esterna è incoerente.
  - Un utente ha esportato il profilo di configurazione e ha modificato il file XML all'esterno del dispositivo.

  Per gli altri profili di configurazione il dispositivo non ha calcolato la somma di controllo.

Il dispositivo verifica correttamente la somma di controllo solo se il profilo di configurazione è stato precedentemente salvato come segue:

- su un dispositivo identico
- con la stessa versione del software utilizzata dal dispositivo

Nota: Questa funzione identifica le modifiche alle impostazioni nel profilo di configurazione. La funzione non fornisce protezione contro l'utilizzo del dispositivo con impostazioni modificate.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Rimuove il profilo di configurazione evidenziato nella tabella dalla memoria non volatile (*NVM*) o dalla memoria esterna.

Se il profilo di configurazione è designato come “Selezionato”, il dispositivo contribuisce a prevenire la rimozione del profilo di configurazione.

Save as..

Copia il profilo di configurazione evidenziato nella tabella e lo salva con un nome specificato dall'utente nella memoria non volatile (*NVM*). Il dispositivo designa il nuovo profilo di configurazione come “Selezionato”.

Nota: Prima di creare ulteriori profili di configurazione, decidere a favore o contro la crittografia della configurazione attivata in modo permanente nel dispositivo. Salvare gli ulteriori profili di configurazione, crittografati o non crittografati, con la stessa password.

Se nella finestra di dialogo *Basic Settings > External Memory*, la casella di spunta nella colonna *Backup config when saving* è selezionata, il dispositivo designa il profilo di configurazione omonimo nella memoria esterna come “Selezionato”.

Activate

Carica le impostazioni del profilo di configurazione evidenziato nella tabella nella memoria volatile (*RAM*).

- ▶ Il dispositivo termina il collegamento con l'interfaccia grafica utente. Per accedere nuovamente al dispositivo, eseguire i seguenti passaggi:
  - ☐ Ricaricare l'interfaccia grafica utente.
  - ☐ Accedere nuovamente.
- ▶ Il dispositivo utilizza immediatamente le impostazioni del profilo di configurazione al volo.

Abilitare la funzione *Undo configuration modifications* prima di attivare un altro profilo di configurazione. Se il collegamento è interrotto in seguito, il dispositivo carica l'ultimo profilo di configurazione designato come “Selezionato” dalla memoria non volatile (*NVM*). Il dispositivo è nuovamente accessibile.

Se la crittografia della configurazione non è attiva, il dispositivo carica un profilo di configurazione non crittografato. Se la crittografia della configurazione è attiva e la password corrisponde alla password memorizzata nel dispositivo, il dispositivo carica un profilo di configurazione crittografato.

Quando si attiva un profilo di configurazione precedente, il dispositivo rileva le impostazioni delle funzioni contenute in questa versione del software. Il dispositivo imposta i valori delle nuove funzioni sul loro valore di default.

Select

Designa il profilo di configurazione evidenziato nella tabella come “Selezionato”. Nella colonna *Selected*, la casella di spunta è poi `selezionata`.

Quando applica la funzione *Undo configuration modifications* o durante un riavvio, il dispositivo carica le impostazioni di questo profilo di configurazione nella memoria volatile (*RAM*).

- Se la crittografia della configurazione nel dispositivo è disabilitata, designare un solo profilo di configurazione non crittografato come “Selezionato”.
- Se la crittografia della configurazione nel dispositivo è abilitata e la password del profilo di configurazione corrisponde alla password memorizzata nel dispositivo, designare un solo profilo di configurazione crittografato come “Selezionato”.

Altrimenti, il dispositivo non è in grado di caricare e crittografare le impostazioni nel profilo di configurazione al riavvio successivo. In questo caso, nella finestra di dialogo *Diagnostics > System > Selftest*, si specifica se il dispositivo si avvia con le impostazioni di default o se conclude il riavvio e si arresta.

Nota: Si contrassegnano solo i profili di configurazione salvati nella memoria non volatile (*NVM*).

Se nella finestra di dialogo *Basic Settings > External Memory*, la casella di spunta nella colonna *Backup config when saving* è selezionata, il dispositivo designa il profilo di configurazione omonimo nella memoria esterna come “Selezionato”.

Import...

Apre la finestra *Import...* per importare un profilo di configurazione.

Il prerequisito è che il profilo di configurazione sia stato esportato utilizzando il pulsante *Export...* o utilizzando il collegamento nella colonna *Profile name*.

- ☐ Nell'elenco a discesa *Select source*, selezionare da dove 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.

☐ Quando *PC/URL* è selezionato sopra, nel frame *Import profile from PC/URL* si specifica il file del profilo di configurazione da importare.
- Importazione dal PC
  Quando il file è posizionato sul proprio PC o su un drive di rete, trascinare il file nell'area  .
  In alternativa, fare clic sull'area per selezionare il file.
- Importazione da un server FTP
  Quando il file è posizionato su un server FTP, specificare l'URL per il file nella forma seguente:
  `ftp://<Utente>:<Password>@<Indirizzo IP>:<Porta>/<Nome file>`
- Importazione da un server TFTP
  Quando il file è posizionato su un server TFTP, specificare l'URL per il file nella forma seguente:
  `tftp://<Indirizzo IP>/<Percorso>/<Nome file>`
- Importazione da un server SCP o SFTP
  Quando il file è posizionato su un server SCP o SFTP, specificare l'URL per il file in una delle forme seguenti:
  `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`
  Facendo clic sul pulsante *Start*, il dispositivo visualizza la finestra *Credentials*. Qui si inseriscono *User name* e *Password* per accedere al server.
  `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`

☐ Quando *External memory* è selezionato sopra, nel frame *Import profile from external memory* si specifica il file del profilo di configurazione da importare.
Nell'elenco a discesa *Profile name*, selezionare il nome del profilo di configurazione da importare.

☐ Nel frame *Destination* si specifica dove il dispositivo salva il profilo di configurazione importato.
Nel campo *Profile name* si specifica il nome sotto il quale il dispositivo salva il profilo di configurazione.
Nel campo *Storage type* si specifica la locazione di memoria per il profilo di configurazione. Il prerequisito è che nell'elenco a discesa *Select source* sia stato selezionata la voce *PC/URL*.
- ▶ *RAM*
  Il dispositivo salva il profilo di configurazione nella memoria volatile (*RAM*) del dispositivo. Questo sostituisce la `running-config`, il dispositivo utilizza immediatamente le impostazioni del profilo di configurazione importato. Il dispositivo termina il collegamento con l'interfaccia grafica utente. Ricaricare l'interfaccia grafica utente. Accedere nuovamente.
- ▶ *NVM*
  Il dispositivo salva il profilo di configurazione nella memoria non volatile (*NVM*) del dispositivo.

Quando si importa un profilo di configurazione, il dispositivo assume le impostazioni come segue:
- se il profilo di configurazione è stato esportato sullo stesso dispositivo o su un dispositivo dalla medesima dotazione e dello stesso tipo, allora:
  Il dispositivo rileva completamente le impostazioni.
- Se il profilo di configurazione è stato esportato su un altro dispositivo, allora:
  il dispositivo assume le impostazioni che può interpretare in base al suo livello di dotazione hardware e software.
  Le impostazioni restanti che il dispositivo assume dal propri profilo di configurazione `running-config`.

Per quanto riguarda la crittografia del profilo di configurazione, leggere anche il testo di aiuto del frame *Configuration encryption*. Il dispositivo importa un profilo di configurazione alle seguenti condizioni:
- La crittografia della configurazione del dispositivo non è attiva. Il profilo di configurazione non è crittografato.
- La crittografia della configurazione del dispositivo è attiva. Il profilo di configurazione è crittografato con la stessa password utilizzata attualmente dal dispositivo.

Export...

Esporta il profilo di configurazione evidenziato nella tabella e lo salva come file XML su un server remoto.

Per salvare il file sul proprio PC, fare clic sul collegamento nella colonna *Profile name* per selezionare la locazione di memoria e specificare il nome del file.

Il dispositivo fornisce le seguenti opzioni per l'esportazione di un profilo di configurazione:

- Esportare su un server FTP
  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>`
- Esportare su un server TFTP
  Per salvare il file su un server TFTP, specificare l'URL per il file nella forma seguente:
  `tftp://<Indirizzo IP>/<Percorso>/<Nome file>`
- Esportare su un server SCP o SFTP
  Per salvare il file su un server SCP o SFTP, specificare l'URL per il file in una delle forme seguenti:
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`
    Facendo clic sul pulsante *Ok*, il dispositivo visualizza la finestra *Credentials*. Qui si inseriscono *User name* e *Password* per accedere al server.
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`

Load running-config as script

Importa un file di script che modifica il profilo di configurazione `running config` corrente.

Il dispositivo fornisce le seguenti opzioni per importare un file di script:

- Importazione dal PC
  Quando il file è posizionato sul proprio PC o su un drive di rete, trascinare il file nell'area  . In alternativa, fare clic sull'area per selezionare il file.
- Importazione da un server FTP
  Quando il file è posizionato su un server FTP, specificare l'URL per il file nella forma seguente:
  `ftp://<Utente>:<Password>@<Indirizzo IP>:<Porta>/<Nome file>`
- Importazione da un server TFTP
  Quando il file è posizionato su un server TFTP, specificare l'URL per il file nella forma seguente:
  `tftp://<Indirizzo IP>/<Percorso>/<Nome file>`
- Importazione da un server SCP o SFTP
  Quando il file è posizionato su un server SCP o SFTP, specificare l'URL per il file in una delle forme seguenti:
  `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`

Nota: Il dispositivo applica i file di script in aggiunta alle impostazioni attuali. Verificare che il file di script non contenga alcuna parte che entri in conflitto con le impostazioni attuali.

Save running-config as script

Salva il profilo di configurazione `running config` come file di script sul PC locale. Questo consente di eseguire il backup delle impostazioni attuali del dispositivo o di utilizzarle su vari dispositivi.

Back to factory...

Ripristina le impostazioni nel dispositivo sui valori di default.

- Il dispositivo cancella i profili di configurazione salvati dalla memoria volatile (*RAM*) e dalla memoria non volatile (*NVM*).
- Il dispositivo cancella il certificato HTTPS utilizzato dal server web nel dispositivo.

- Il dispositivo cancella la chiave RSA (chiave host) utilizzata dal server SSH nel dispositivo.
- Quando è collegata una memoria esterna, il dispositivo cancella i profili di configurazione salvati nella memoria esterna.
- Dopo un breve periodo, il dispositivo si riavvia e carica i valori di default.

Back to default

Cancella le impostazioni operative (`running config`) attuali dalla memoria volatile (*RAM*).

1.6 External Memory

[Basic Settings > External Memory]

Questa finestra di dialogo consente di attivare le funzioni che il dispositivo esegue automaticamente in combinazione con la memoria esterna. La finestra di dialogo mostra anche il modo operativo e le caratteristiche identificative della memoria esterna.

Tabella

Type

Mostra il tipo di memoria esterna.

Possibili valori:

- *usb*
  Memoria USB esterna (EAM)

Status

Mostra il modo operativo della memoria esterna.

Possibili valori:

- *notPresent*
  Nessuna memoria esterna collegata.
- *removed*
  Qualcuno ha rimosso la memoria esterna dal dispositivo durante il funzionamento.
- *ok*
  La memoria esterna è collegata ed è pronta per il funzionamento.
- *outOfMemory*
  Lo spazio di memoria è occupato nella memoria esterna.
- *genericErr*
  Il dispositivo ha rilevato un errore.

Writable

Mostra se il dispositivo ha l'accesso in scrittura alla memoria esterna.

Possibili valori:

- selezionato
  Il dispositivo dispone dell'accesso in scrittura alla memoria esterna.
- non selezionato
  Il dispositivo dispone dell'accesso in sola lettura alla memoria esterna. Eventualmente, la protezione della scrittura può essere attivata nella memoria esterna.

Software auto update

Attiva/disattiva l'aggiornamento automatico del software del dispositivo durante il riavvio.

Possibili valori:

- `selezionato` (impostazione di default)
  L'aggiornamento automatico del software del dispositivo durante il riavvio è attivato. Il dispositivo aggiorna il software del dispositivo quando i file seguenti si trovano nella memoria esterna:
  - il file immagine del software del dispositivo
  - un file di testo `startup.txt` con il contenuto `autoUpdate=<Image_file_name>.bin`
- `non selezionato`
  L'aggiornamento automatico del software del dispositivo durante il riavvio è disattivato.

SSH key auto upload

Attiva/disattiva il caricamento della chiave RSA da una memoria esterna al riavvio.

Possibili valori:

- `selezionato` (impostazione di default)
  Il caricamento della chiave RSA è attivato.
  Durante un riavvio, il dispositivo carica la chiave RSA dalla memoria esterna quando i file seguenti si trovano nella memoria esterna:
  - file chiave SSH RSA
  - un file di testo `startup.txt` con il contenuto
    `autoUpdateRSA=<filename_of_the_SSH_RSA_key>`

  Il dispositivo mostra messaggi sulla console di sistema dell'interfaccia seriale.
- `non selezionato`
  Il caricamento della chiave RSA è disattivato.

Nota: Durante il caricamento della chiave RSA dalla memoria esterna (*ENVM*), il dispositivo sovrascrive le chiavi esistenti nella memoria non volatile (*NVM*).

Config priority

Specifica la memoria dalla quale il dispositivo carica il profilo di configurazione al riavvio.

Possibili valori:

- `disable`
  Il dispositivo carica il profilo di configurazione dalla memoria non volatile (*NVM*).
- `first`
  Il dispositivo carica il profilo di configurazione dalla memoria esterna.
  Quando il dispositivo non trova un profilo di configurazione nella memoria esterna, carica il profilo di configurazione dalla memoria non volatile (*NVM*).

Nota: Durante il caricamento del profilo di configurazione dalla memoria esterna (*ENVM*), il dispositivo sovrascrive le impostazioni del profilo di configurazione Selezionato nella memoria non volatile (*NVM*).

Se la colonna *Config priority* ha il valore `first` e il profilo di configurazione non è crittografato, il frame *Security status* nella finestra di dialogo *Basic Settings > System* mostra un allarme.

Nella finestra di dialogo *Diagnostics > Status Configuration > Security Status*, scheda *Global*, colonna *Monitor* si specifica se il dispositivo monitora il parametro *Load unencrypted config from external memory*.

Backup config when saving

Attiva/disattiva la creazione di una copia del profilo di configurazione nella memoria esterna.

Possibili valori:

- `selezionato` (impostazione di default)
  La creazione di una copia è attivata. Quando si fa clic nella finestra di dialogo *Basic Settings* > Load/Save, pulsante *Save*, il dispositivo genera una copia del profilo di configurazione sulla memoria esterna attiva.
- `non selezionato`
  La creazione di una copia è disattivata. Il dispositivo non genera una copia del profilo di configurazione.

Manufacturer ID

Mostra il nome del produttore della memoria.

Revision

Mostra il numero di revisione specificato dal produttore della memoria.

Version

Mostra il numero della versione specificato dal produttore della memoria.

Name

Mostra il nome del prodotto specificato del produttore della memoria.

Serial number

Mostra il numero di serie specificato dal produttore della memoria.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

1.7 Port

[Basic Settings > Port]

Questa finestra di dialogo consente di specificare le impostazioni per le singole porte. La finestra di dialogo mostra anche il modo operativo, lo stato del collegamento, il bit rate e la modalità duplex per ogni porta.

Questa finestra di dialogo include le seguenti schede:
- [Configuration]
- [Statistics]
- [Utilization]

[Configuration]

Tabella

Port

Visualizza il numero di porta.

Name

Nome della porta.

Possibili valori:
- Stringa di caratteri ASCII alfanumerici con 0 .. 64 caratteri
  Sono consentiti i seguenti caratteri:
  - `<space>`
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

Port on

Attiva/disattiva la porta.

Possibili valori:
- `selezionato` (impostazione di default)
  La porta è attiva.
- `non selezionato`
  La porta non è attiva. La porta non invia o riceve alcun dato.

State

Mostra se la porta è attualmente fisicamente abilitata o disabilitata.

Possibili valori:

- `selezionato`
  La porta è fisicamente abilitata.
- `non selezionato`
  La porta è fisicamente disabilitata.
  Quando la funzione *Port on* è attiva, la funzione *Auto-Disable* ha disabilitato la porta.
  Le impostazioni della funzione *Auto-Disable* si specificano nella finestra di dialogo *Diagnostics* > Ports > *Auto-Disable*.

Power state (port off)

Specifica se la porta è fisicamente attiva o spenta quando si disattiva la porta con la funzione *Port on*.

Possibili valori:

- `selezionato`
  La porta rimane fisicamente abilitata. Un dispositivo collegato riceve un collegamento attivo.
- `non selezionato` (impostazione di default)
  La porta è fisicamente disabilitata.

Auto power down

Specifica come si comporta la porta in assenza di cavi collegati.

Possibili valori:

- *`no-power-save`* (impostazione di default)
  La porta rimane attiva.
- *`auto-power-down`*
  La porta passa alla modalità di risparmio energetico.
- *`unsupported`*
  La porta non supporta questa funzione e rimane attiva.

Automatic configuration

Attiva/disattiva la selezione automatica del modo operativo per la porta.

Possibili valori:

- `selezionato` (impostazione di default)
  La selezione automatica del modo operativo è attiva.
  La porta negozia il modo operativo in maniera indipendente utilizzando la negoziazione automatica e rileva i dispositivi collegati alla porta TP in maniera automatica (Auto Cable Crossing).
  Queste impostazioni hanno priorità sull'impostazione manuale della porta.
  Trascorrono alcuni secondi finché la porta non ha impostato il modo operativo.
- `non selezionato`
  La selezione automatica del modo operativo non è attiva.
  La porta funziona con i valori specificati nella colonna *Manual configuration* e nella colonna *Manual cable crossing (Auto. conf. off)*.
- Visualizzazione in grigio
  Nessuna selezione automatica del modo operativo.

Manual configuration

Specifica il modo operativo delle porte quando la funzione *Automatic configuration* è disabilitata.

Possibili valori:

- `10 Mbit/s HDX`
  Collegamento half duplex
- `10 Mbit/s FDX`
  Collegamento full duplex
- `100 Mbit/s HDX`
  Collegamento half duplex
- `100 Mbit/s FDX`
  Collegamento full duplex
- `1000 Mbit/s FDX`
  Collegamento full duplex
- `2500 Mbit/s FDX`
  Collegamento full duplex

Nota: I modi operativi della porta attualmente disponibili dipendono dalla configurazione del dispositivo.

Link/Current settings

Mostra il modo operativo attualmente utilizzato dalla porta.

Possibili valori:

- `-`
  Nessun cavo collegato, nessun collegamento.
- `10 Mbit/s HDX`
  Collegamento half duplex
- `10 Mbit/s FDX`
  Collegamento full duplex
- `100 Mbit/s HDX`
  Collegamento half duplex
- `100 Mbit/s FDX`
  Collegamento full duplex
- `1000 Mbit/s FDX`
  Collegamento full duplex
- `2500 Mbit/s FDX`
  Collegamento full duplex

Nota: I modi operativi della porta attualmente disponibili dipendono dalla configurazione del dispositivo.

Manual cable crossing (Auto. conf. off)

Specifica i dispositivi collegati a una porta TP.

Il prerequisito è che la funzione *Automatic configuration* sia disabilitata.

Possibili valori:

- *mdi*
  Il dispositivo scambia le coppie di conduttori di invio e di ricezione sulla porta.

- `mdix` (impostazione di default sulle porte TP)
  Il dispositivo contribuisce a prevenire lo scambio tra le coppie di conduttori di invio e di ricezione sulla porta.
- `auto-mdix`
  Il dispositivo rileva la coppia di conduttori di invio e quella di ricezione del dispositivo collegato e si adatta automaticamente.
  Esempio: quando si esegue il collegamento a un terminale con un cavo incrociato, il dispositivo ripristina automaticamente la porta da `mdix` a `mdi`.
- `unsupported` (impostazione di default sulle porte ottiche o sulle porte TP-SFP)
  La porta non supporta questa funzione.

Flow control

Attiva/disattiva il controllo di flusso sulla porta.

Possibili valori:

- `selezionato` (impostazione di default)
  Il controllo di flusso sulla porta è attivo.
  L'invio e la valutazione dei pacchetti di pausa (funzionamento full-duplex) o delle collisioni (funzionamento half-duplex) sono attivati sulla porta.
  - ☐ Per abilitare il controllo del flusso nel dispositivo, attivare anche la funzione *Flow control* nella finestra di dialogo *Switching > Global*.
  - ☐ Attivare il controllo di flusso anche sulla porta del dispositivo collegato a questa porta.

  Su una porta uplink, l'attivazione del controllo di flusso potrebbe causare interruzioni indesiderate dell'invio nel segmento di rete di livello superiore (“wandering backpressure”).
- `non selezionato`
  Il controllo di flusso sulla porta non è attivo.

Se si sta utilizzando una funzionalità di ridondanza, disattivare il controllo di flusso sulle porte interessate. Se il controllo di flusso e la funzionalità di ridondanza sono attive contemporaneamente, è possibile che la funzionalità di ridondanza operi in modo diverso dal previsto.

Send trap (Link up/down)

Attiva/disattiva l'invio di trap SNMP quando il dispositivo rileva un cambiamento nello stato link up/down per questa porta.

Possibili valori:

- `selezionato` (impostazione di default)
  L'invio di trap SNMP è attivo.
  Quando il dispositivo rileva un cambiamento dello stato link up/down, il dispositivo invia una SNMP trap.
- `non selezionato`
  L'invio di trap SNMP non è attivo.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

MTU

Specifica le dimensioni massime consentite dei pacchetti Ethernet sulla porta in byte.

Possibili valori:

- `1518..9720` (impostazione di default: `1518`)
  Con le impostazioni `1518`, la porta trasmette i pacchetti Ethernet fino alle seguenti dimensioni:
  - 1518 byte senza tag VLAN
    (1514 byte + 4 byte CRC)
  - 1522 byte con tag VLAN
    (1518 byte + 4 byte CRC)

Queste impostazioni consentono di aumentare le dimensioni massime consentite dei pacchetti Ethernet che questa porta può ricevere o trasmettere.

L'elenco seguente contiene le possibili applicazioni:

- Quando si utilizza il dispositivo nella rete transfer con doppia tagging VLAN è possibile che sia necessario un *MTU* più grande di 4 byte.

Sulle altre interfacce si specificano le massime dimensioni consentite dei pacchetti Ethernet come segue:

- Interfacce *Link Aggregation*
  Finestra di dialogo *Switching > L2-Redundancy > Link Aggregation*, colonna *MTU*

Signal

Attiva/disattiva il lampeggiamento del LED della porta. Questa funzione consente di identificare la porta nel campo.

Possibili valori:

- `selezionato`
  Il lampeggiamento del LED della porta è attivo.
  Il LED della porta lampeggia finché non si disabilita nuovamente la funzione.
- `non selezionato` (impostazione di default)
  Il lampeggiamento del LED della porta non è attivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Clear port statistics

Ripristina il contatore per le statistiche della porta su `0`.

[Statistics]

Questa scheda mostra la seguente panoramica per porta:

- Numero di byte/pacchetti dati ricevuti nel dispositivo
  - *Received packets*
  - *Received octets*
  - *Received unicast packets*
  - *Received multicast packets*
  - *Received broadcast packets*
- Numero di byte/pacchetti dati inviati dal dispositivo
  - *Transmitted packets*
  - *Transmitted octets*
  - *Transmitted unicast packets*
  - *Transmitted multicast packets*
  - *Transmitted broadcast packets*
- Numero di errori rilevati dal dispositivo
  - *Received fragments*
  - *Detected CRC errors*
  - *Detected collisions*
- Numero di pacchetti dati per categoria di dimensione ricevuti sul dispositivo.
  - *Packets 64 bytes*
  - *Packets 65 to 127 bytes*
  - *Packets 128 to 255 bytes*
  - *Packets 256 to 511 bytes*
  - *Packets 512 to 1023 bytes*
  - *Packets 1024 to 1518 bytes*
- Numero di pacchetti dati rifiutati dal dispositivo
  - *Received discards*
  - *Transmitted discards*

Per ordinare la tabella secondo un criterio specifico fare clic sull'intestazione sulla riga corrispondente.

Per esempio, per ordinare la tabella in base al numero di byte ricevuti in ordine crescente, fare clic una sola volta sull'intestazione della colonna *Received octets*. Per ordinare in ordine decrescente fare clic nuovamente sull'intestazione.

Per ripristinare il contatore per le statistiche della porta nella tabella su `0`, eseguire i seguenti passaggi:

- ☐ Nella finestra di dialogo *Basic Settings > Port*, fare clic sul pulsante ☰ e poi sulla voce *Clear port statistics*.
  oppure
- ☐ Nella finestra di dialogo *Basic Settings > Restart*, fare clic sul pulsante *Clear port statistics*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Clear port statistics

Ripristina il contatore per le statistiche della porta su `0`.

[Utilization]

Questa tabella mostra l'utilizzo (carico di rete) per le singole porte.

Tabella

Port

Visualizza il numero di porta.

Utilization [%]

Mostra l'utilizzo corrente in percentuale in relazione all'intervallo di tempo specificato nella colonna *Control interval [s]*.

L'utilizzo è il rapporto tra la quantità di dati ricevuti e la massima quantità di dati possibile alla velocità di trasmissione dei dati attualmente configurata.

Lower threshold [%]

Specifica una soglia inferiore per l'utilizzo. Se l'utilizzo della porta scende al di sotto di questo valore, la colonna *Alarm* mostra un allarme.

Possibili valori:

- `0.00..100.00` (impostazione di default: `0.00`)

Il valore `0` disattiva la soglia più bassa.

Upper threshold [%]

Specifica una soglia superiore per l'utilizzo. Se l'utilizzo della porta supera tale valore, la colonna *Alarm* mostra un allarme.

Possibili valori:

- `0.00..100.00` (impostazione di default: `0.00`)

Il valore `0` disattiva la soglia superiore.

Control interval [s]

Specifica l'intervallo in secondi.

Possibili valori:

- `1..3600` (impostazione di default: `30`)

Alarm

Mostra lo stato dello Utilization Alarm.

Possibili valori:

- `selezionato`
  L'utilizzo della porta è al di sotto al valore specificato nella colonna *Lower threshold [%]* o al di sopra del valore specificato nella colonna *Upper threshold [%]*. Il dispositivo invia una trap SNMP.
- `non selezionato`
  L'utilizzo della porta è al di sopra del valore specificato nella colonna *Lower threshold [%]* e al di sotto del valore specificato nella colonna *Upper threshold [%]*.
  Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Clear port statistics

Ripristina il contatore per le statistiche della porta su `0`.

1.8 Power over Ethernet (MCSESP)

[Basic Settings > Power over Ethernet]

In Power over Ethernet (PoE), il Power Source Equipment (PSE) fornisce corrente ai dispositivi alimentati (PD) quali telefoni IP tramite il doppino ritorto.

Il codice prodotto e l'etichetta specifica del PoW sulla custodia del dispositivo PSE indica se il dispositivo supporta *Power over Ethernet*. Le porte PoE del dispositivo supportano Power over Ethernet secondo IEEE 802.3at.

Il sistema fornisce un bilancio di potenza interna massima per le porte. Le porte riservano la potenza in base alla classe rilevata di un dispositivo alimentato collegato. La potenza reale erogata è uguale o inferiore alla potenza di riserva.

È possibile gestire la potenza in uscita con il parametro *Priority*. Se la somma della potenza necessaria ai dispositivi collegati è superiore alla potenza disponibile, il dispositivo disattiva la potenza fornita alle porte in base alla priorità configurata. Il dispositivo disattiva la potenza fornita alle porte partendo dalle porte configurate con priorità bassa. Se diverse porte hanno una priorità bassa, il dispositivo disattiva la potenza partendo dalle porte con la numerazione più elevata.

Il menu include le seguenti finestre di dialogo:

- PoE Global
- PoE Port

1.8.1 PoE Global

[Basic Settings > Power over Ethernet > Global]

In base alle impostazioni specificate in questa finestra di dialogo, il dispositivo fornisce potenza ai dispositivi finali. Se il consumo di potenza raggiunge la soglia specificata dall'utente, il dispositivo invia una trap SNMP.

Operation

Operation

Abilita/disabilita la funzione *Power over Ethernet*.

Possibili valori:

- `On` (impostazione di default)
  È abilitata la funzione *Power over Ethernet*.
- `Off`
  È disabilitata la funzione *Power over Ethernet*.

Configuration

Send trap

Attiva/disattiva l'invio di trap SNMP.

Se il consumo di energia supera la soglia specificata dall'utente, il dispositivo invia una trap SNMP.

Possibili valori:

- `selezionato` (impostazione di default)
  Il dispositivo invia trap SNMP.
- `non selezionato`
  Il dispositivo non invia trap SNMP.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Threshold [%]

Specifica il valore di soglia per il consumo di energia in percentuale.

Se la potenza in uscita supera questa soglia, il dispositivo misura la potenza in uscita totale e invia una trap SNMP.

Possibili valori:

- `0..99` (impostazione di default: `90`)

System power

Budget [W]

Visualizza la somma di potenza disponibile per il bilancio globale.

Reserved [W]

Visualizza la potenza di riserva globale. La potenza di riserva del dispositivo in base alle classi rilevate dei dispositivi alimentati collegati. La potenza di riserva è uguale o inferiore alla potenza effettivamente erogata.

Delivered [W]

Visualizza la somma effettiva della potenza erogata ai moduli in watt.

Delivered [mA]

Visualizza la corrente effettiva erogata ai moduli in milliampere.

Tabella

Module

Modulo del dispositivo a cui si riferiscono le voci della tabella.

Configured power budget [W]

Specifica la potenza dei moduli per la distribuzione alle porte.

Possibili valori:

- `0..n` (impostazione di default: n)
  In questo caso `n` corrisponde al valore nella colonna *Max. power budget [W]*.

Max. power budget [W]

Visualizza la potenza massima disponibile per questo modulo.

Reserved power [W]

Visualizza la potenza di riserva per il modulo in base alle classi rilevat dei dispositivi alimentati collegati.

Delivered power [W]

Visualizza la potenza effettiva in watt fornita ai dispositivi alimentati collegati a questa porta.

Delivered current [mA]

Visualizza la corrente effettiva in milliampere fornita ai dispositivi alimentati collegati a questa porta.

Power source

Visualizza il Power Source Equipment per il dispositivo.

Possibili valori:

- *internal*
  Fonte di alimentazione interna
- *external*
  Fonte di alimentazione esterna

Threshold [%]

Specifica il valore soglia per il consumo di energia del modulo in percentuale. Se la potenza in uscita supera questa soglia, il dispositivo misura la potenza in uscita totale e invia una trap SNMP.

Possibili valori:

- `0..99` (impostazione di default: `90`)

Send trap

Attiva/disattiva l'invio di trap SNMP quando il dispositivo rileva il superamento del valore soglia per il consumo di energia.

Possibili valori:

- `selezionato`
  L'invio di trap SNMP è attivo.
  Se il consumo di energia del modulo supera la soglia specificata dall'utente, il dispositivo invia una trap SNMP.
- `non selezionato` (impostazione di default)
  L'invio di trap SNMP non è attivo.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

1.8.2 PoE Port

[Basic Settings > Power over Ethernet > Port]

Se il consumo di energia è superiore alla potenza erogabile, il dispositivo disattiva la potenza fornita ai dispositivi alimentati (PD) in base ai livelli di priorità e al numero della porta. Se il PD collegato necessita più potenza di quella fornita dal dispositivo, il dispositivo disattiva la funzione *Power over Ethernet* sulle porte. Il dispositivo disabilita prima la funzione *Power over Ethernet* sulle porte con priorità inferiore. Se diverse porte hanno la stessa priorità, il dispositivo disattiva prima la funzione *Power over Ethernet* sulle porte con la numerazione più elevata. Il dispositivo disattiva anche l'alimentazione ai dispositivi alimentati (PD) per un periodo di tempo specifico.

Tabella

Port

Visualizza il numero di porta.

PoE enable

Attiva/disattiva l'alimentazione PoE fornita alla porta.

Se la funzione è attivata o disattivata, il dispositivo registra un evento nel file di registro (System Log).

Possibili valori:

- `selezionato` (impostazione di default)
  L'alimentazione PoE alla porta è attiva.
- `non selezionato`
  L'alimentazione PoE alla porta è disattiva.

Fast startup

Attiva/disattiva la funzione Power over Ethernet Fast Startup sulla porta.

Il prerequisito è che la casella di spunta nella colonna *PoE enable* sia selezionata.

Possibili valori:

- `selezionato`
  La funzione Fast Startup è attiva. Il dispositivo invia potenza ai dispositivi alimentati (PD) immediatamente dopo l'accensione dell'alimentazione del dispositivo.
- `non selezionato` (impostazione di default)
  La funzione Fast Startup è disattiva. Il dispositivo invia potenza ai dispositivi alimentati (PD) dopo aver caricato la propria configurazione.

Priority

Specifica la priorità della porta.

Per contribuire a evitare sovraccarichi di corrente, il dispositivo disattiva prima le porte con priorità bassa. Per contribuire a evitare che il dispositivo disabiliti le porte che alimentano i dispositivi necessari, per queste porte specificare una priorità elevata.

Possibili valori:

- *critical*
- *high*
- *low* (impostazione di default)

Status

Visualizza lo stato del rilevamento del dispositivo alimentato (PD) della porta.

Possibili valori:

- *disabled*
  Il dispositivo è in stato DISABLED e non fornisce potenza ai dispositivi alimentati.
- *deliveringPower*
  Il dispositivo ha identificato la classe del PD collegato ed è in stato POWER ON.
- *fault*
  Il dispositivo è in stato TEST ERROR.
- *otherFault*
  Il dispositivo è in stato IDLE.
- *searching*
  Il dispositivo è in uno stato diverso da quelli elencati.
- *test*
  Il dispositivo è in modalità TEST.

Detected class

Visualizza la classe di potenza del dispositivo alimentato collegatoa alla porta.

Possibili valori:

- *Class 0*
- *Class 1*
- *Class 2*
- *Class 3*
- *Class 4*

Class 0
Class 1
Class 2
Class 3
Class 4

Attiva/disattiva la corrende delle classi da 0 a 4 sulla porta.

Possibili valori:

- selezionato (impostazione di default)
- non selezionato

Consumption [W]

Visualizza il consumo di energia attuale della porta in watt.

Possibili valori:

▶ `0,0..30,0`

Consumption [mA]

Visualizza la corrente fornita alla porta in milliampere.

Possibili valori:

▶ `0..600`

Power limit [W]

Specifica la potenza massima in watt che la porta eroga.

Questa funzione consente di distribuire il bilancio di potenza disponibile tra le porte PoE in base alle esigenze.

Per esempio, per un dispositivo collegato che non fornisce una "classe di potenza" la porta riserva una quantità fissa di 15,4 W (classe 0) anche se il dispositivo necessita di meno potenza. La potenza in eccesso non è disponibile per le altre porte.

Specificando un limite di potenza si riduce la potenza di riserva alle effettive necessità del dispositivo collegato. La potenza non utilizzata è disponibile per le altre porte.

Se non è noto il consumo di energia esatto del dispositivo alimentato collegato, il dispositivo visualizza il valore nella colonna *Max. consumption [W]*. Verificare che il limite di potenza sia superiore al valore nella colonna *Max. consumption [W]*.

Se la potenza massima osservata è superiore al limite di potenza impostato, il disposivito considera invalido il limite di potenza. In questo caso il dispositivo utilizza la classe PoE per eseguire il calcolo.

Possibili valori:

▶ `0,0..30,0` (impostazione di default: `0`)

Max. consumption [W]

Visualizza la potenza massima in watt che il dispositivo ha consumato fino a questo momento.

Quando si disattiva il PoE sulla porta o si interrompe il collegamento al dispositivo collegato, il valore viene resettato.

Name

Specifica il nome della porta.

Specifica il nome desiderato dall'utente.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..32 caratteri

Auto-shutdown power

Attiva/disattiva la funzione *Auto-shutdown power* in base alle impostazioni.

Possibili valori:

- `selezionato`
- `non selezionato` (impostazione di default)

Disable power at [hh:mm]

Specifica il tempo in cui il dispositivo disattiva l'alimentazione per la porta all'attivazione della funzione *Auto-shutdown power*.

Possibili valori:

- `00:00..23:59` (impostazione di default: `00:00`)

Re-enable power at [hh:mm]

Specifica il tempo in cui il dispositivo attiva l'alimentazione per la porta all'attivazione della funzione *Auto-shutdown power*.

Possibili valori:

- `00:00..23:59` (impostazione di default: `00:00`)

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

1.9 Restart

[Basic Settings > Restart]

Questa finestra di dialogo consente di riavviare il dispositivo, ripristinare i contatori della porta e le tabelle indirizzi, e cancellare i file di registro.

Restart

Restart in

Mostra il tempo residuo fino al riavvio del dispositivo.

Per aggiornare la visualizzazione del tempo residuo, fare clic sul pulsante  .

Cancel

Annulla un riavvio differito.

Cold start...

Apre la finestra di dialogo *Restart* per iniziare un riavvio immediato o differito del dispositivo.

Se il profilo di configurazione nella memoria volatile (`RAM`) e il profilo di configurazione “Selezionato” nella memoria non volatile (`NVM`) sono diversi, il dispositivo mostra la finestra di dialogo *Warning*.

- Per salvare le modifiche in maniera permanente, fare clic sul pulsante *Yes* nella finestra di dialogo *Warning*.
- Per rifiutare le modifiche, fare clic sul pulsante *No* nella finestra di dialogo *Warning*.
- Nel campo *Restart in* si specifica il tempo di ritardo per il riavvio differito.
  Possibili valori:
  – `00:00:00..596:31:23` (impostazione di default: `00:00:00`)

Quando il tempo di ritardo scade, il dispositivo si riavvia e attraversa le seguenti fasi:

- Se si attiva la funzione nella finestra di dialogo *Diagnostics > System > Selftest*, il dispositivo esegue un test della RAM.
- Il dispositivo avvia il software del dispositivo che il campo *Stored version* mostra nella finestra di dialogo *Basic Settings > Software*.
- Il dispositivo carica le impostazioni dal profilo di configurazione “Selezionato”. Vedere la finestra di dialogo *Basic Settings > Load/Save*.

Nota: Durante il riavvio, il dispositivo non trasferisce alcun dato. Durante questo periodo è impossibile accedere al dispositivo attraverso l'interfaccia grafica utente o altri sistemi di gestione.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset MAC address table

Rimuove dalla tabella inoltri gli indirizzi MAC con valore *Switching > Filter for MAC Addresses* all'interno della finestra di dialogo `learned` nella colonna *Status*.

Reset ARP table

Rimuove gli indirizzi impostati dinamicamente dalla tabella ARP.

Vedere la finestra di dialogo *Diagnostics > System > ARP*.

Clear port statistics

Ripristina il contatore per le statistiche della porta su `0`.

Vedere la finestra di dialogo *Basic Settings > Port*, scheda *Statistics*.

Clear management access statistics

Ripristina i contatori delle statistiche dell'accesso alla gestione del dispositivo su `0`.

Vedere la finestra di dialogo *Diagnostics > System > System Information*, tabella `Used Management Ports`.

Reset IGMP snooping data

Rimuove le voci IGMP Snooping e ripristina il contatore nel frame *Information* a `0`.

Vedere la finestra di dialogo *Switching > IGMP Snooping > Global*.

Delete log file

Rimuove gli eventi registrati dal file di registro.

Vedere la finestra di dialogo *Diagnostics > Report > System Log*.

Delete persistent log file

Rimuove i file di registro dalla memoria esterna.

Vedere la finestra di dialogo *Diagnostics > Report > Persistent Logging*.

Clear email notification statistics

Ripristina i contatori nel frame *Information* su `0`.

Vedere la finestra di dialogo *Diagnostics > Email Notification > Global*.

2 Time

Il menu include le seguenti finestre di dialogo:
- Basic Settings
- SNTP
- PTP
- 802.1AS

2.1 Basic Settings

[Time > Basic Settings]

Il dispositivo è equipaggiato con un clock hardware bufferizzato. Questo clock mantiene l'orario corretto se l'alimentazione di tensione diventa inutilizzabile o se si scollega il dispositivo dall'alimentazione di tensione. Dopo l'avvio del dispositivo, l'orario corrente è a disposizione, ad esempio per le voci di registro.

Il clock hardware copre una mancanza di alimentazione di tensione di 3 ore. Il prerequisito è il precedente collegamento dell'alimentazione di tensione del dispositivo in modo continuativo per almeno 5 minuti.

In questa finestra di dialogo è possibile procedere alle impostazioni relative all'orario, indipendentemente dal protocollo di sincronizzazione orario selezionato.

Questa finestra di dialogo include le seguenti schede:
- [Global]
- [Daylight saving time]

[Global]

In questa scheda si specifica l'orario del sistema nel dispositivo e il fuso orario.

Configuration

System time (UTC)

Indica la data e l'ora con riferimento al tempo universale coordinato (UTC).

Set time from PC

Il dispositivo utilizza come system time l'orario del PC.

System time

Indica le attuali data e ora con riferimento all'orario locale: *System time* = *System time (UTC)* + *Local offset [min]* + *Daylight saving time*

Time source

Indica la fonte dell'orario da cui il dispositivo riceve le informazioni orario.

Il dispositivo seleziona automaticamente la fonte dell'orario disponibile con la maggiore precisione possibile.

Possibili valori:

- `local`
  Il clock di sistema del dispositivo.
- `sntp`
  Il client *SNTP* è attivato e il dispositivo è sincronizzato da un server *SNTP*.
- `ptp`
  PTP è attivo e il clock del dispositivo è sincronizzato con un master clock *PTP*.

Local offset [min]

Specifica la differenza tra l'orario locale e *System time (UTC)* in minuti: *Local offset [min]* = *System time* − *System time (UTC)*

Possibili valori:

- `-780..840` (impostazione di default: `60`)

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Daylight saving time]

In questa scheda, si attiva la funzione automatica Ora legale (Daylight saving time). Si specifica l'inizio e la fine dell'ora leale utilizzando un profilo predefinito oppure specificando individualmente queste impostazioni. Durante l'ora legale il dispositivo imposta 1 ora in avanti l'orario locale.

Operation

Daylight saving time

Attiva/disattiva la modalità *Daylight saving time*.

Possibili valori:

- `On`
  La modalità *Daylight saving time* è attivata.
  il dispositivo cambia automaticamente ora legale/ora solare.
- `Off` (impostazione di default)
  La modalità *Daylight saving time* è disattivata.

Gli orari nei quali il dispositivo cambia ora legale/ora solare sono specificati nei frame *Summertime begin* e *Summertime end*.

Profile...

Visualizza la finestra di dialogo *Profile...*. Qui si seleziona un profilo predefinito per l'inizio e la fine dell'ora legale. Questo profilo sovrascrive le impostazioni nei frame *Summertime begin* e *Summertime end*.

Summertime begin

Nei primi 3 campi si specificano il giorno di inizio dell'ora legale e nell'ultimo l'ora.

Quando l'orario nel campo *System time* raggiunge il valore qui inserito, il dispositivo passa all'ora legale.

Week

Specifica la settimana nel mese corrente.

Possibili valori:

- *none* (impostazione di default)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Specifica il giorno della settimana.

Possibili valori:

- *none* (impostazione di default)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Specifica il mese.

Possibili valori:

- *none* (impostazione di default)
- *January*
- *February*
- *March*
- *April*
- *May*
- *June*

- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

System time

Specifica l'ora.

Possibili valori:

- `<HH:MM>` (impostazione di default: `00:00`)

Summertime end

Nei primi 3 campi si specificano il giorno di fine dell'ora legale e nell'ultimo l'ora.

Quando l'orario nel campo *System time* raggiunge il valore qui inserito, il dispositivo passa all'ora solare.

Week

Specifica la settimana nel mese corrente.

Possibili valori:

- *none* (impostazione di default)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Specifica il giorno della settimana.

Possibili valori:

- *none* (impostazione di default)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Specifica il mese.

Possibili valori:
- *none* (impostazione di default)
- *January*
- *February*
- *March*
- *April*
- *May*
- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

System time

Specifica l'ora.

Possibili valori:
- <HH:MM> (impostazione di default: 00:00)

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

2.2 SNTP

[Time > SNTP]

Il Simple Network Time Protocol (SNTP) è una procedura descritta in RFC 4330 per la sincronizzazione orario nella rete.

Il dispositivo consente la sincronizzazione del system time nel dispositivo come un client *SNTP*. Come il server *SNTP*, il dispositivo rende le informazioni orario disponibili ad altri dispositivi.

Il menu include le seguenti finestre di dialogo:
- SNTP Client
- SNTP Server

2.2.1 SNTP Client

[Time > SNTP > Client]

In questa finestra di dialogo si specificano le impostazioni con le quali il dispositivo funziona come un client *SNTP*.

Come un client *SNTP*, il dispositivo ottiene le informazioni orario da entrambi i server *SNTP* e dai server *NTP* e sincronizza il clock locale con l'orario del server orario.

Operation

Operation

Attiva/disattiva la funzione *SNTP Client* del dispositivo.

Possibili valori:

- `On`
  È abilitata la funzione *SNTP Client*.
  Il dispositivo funziona come un client *SNTP*.
- `Off` (impostazione di default)
  È disabilitata la funzione *SNTP Client*.

Configuration

Mode

Specifica se il dispositivo richiede attivamente le informazioni orario da un server *SNTP* conosciuto e configurato nella rete (modalità Unicast) o attende passivamente le informazioni orario da un server casuale *SNTP* server (modalità Broadcast).

Possibili valori:

- `unicast` (impostazione di default)
  Il dispositivo acquisisce le informazioni orario solo dal server *SNTP* configurato. Il dispositivo invia richieste Unicast al server *SNTP* e ne valuta le risposte.
- `broadcast`
  Il dispositivo ottiene le informazioni orario da uno o più server *SNTP* o *NTP*. Il dispositivo valuta i broadcast o i multicast solamente da questi server.

Request interval [s]

Specifica l'intervallo in secondi nel quale il dispositivo richiede le informazioni orario dal server *SNTP*.

Possibili valori:

- `5..3600` (impostazione di default: `30`)

Broadcast recv timeout [s]

Specifica il tempo in secondi durante il quale un client in modalità Client broadcast attende prima di cambiare il valore nel campo da *`syncToRemoteServer`* a *`notSynchronized`* se il client non riceve pacchetti broadcast.

Possibili valori:

- `128..2048` (impostazione di default: `320`)

Disable client after successful sync

Attiva/disattiva la disabilitazione del client *SNTP* dopo che il dispositivo ha completato la sincronizzazione dell'orario.

Possibili valori:

- `selezionato`
  La disabilitazione del client *SNTP* è attiva.
  Il dispositivo disattiva il client *SNTP* dopo aver completato la sincronizzazione dell'orario.
- `non selezionato` (impostazione di default)
  La disabilitazione del client *SNTP* non è attiva.
  Il client *SNTP* rimane attivo dopo il completamento della sincronizzazione orario.

State

State

Visualizza lo stato del client *SNTP*.

Possibili valori:

- *`disabled`*
  Il client *SNTP* è disabilitato.
- *`notSynchronized`*
  Il client *SNTP* non è sincronizzato con nessuno dei server *SNTP* o *NTP*.
- *`synchronizedToRemoteServer`*
  Il client *SNTP* è sincronizzato con un server *SNTP* o *NTP*.

Tabella

Nella tabella si specificano le impostazioni per un massimo di 4 server *SNTP*.

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Possibili valori:

- `1..4`

Il dispositivo assegna automaticamente questo numero.

Quando si elimina una voce della tabella rimane un buco nella numerazione. Quando si crea una nuova voce della tabella, il dispositivo riempie il primo buco.

Dopo l'avvio, il dispositivo invia richieste al server *SNTP* configurato nella prima voce della tabella. Se il server non risponde, il dispositivo invia le richieste al server *SNTP* configurato nella successiva voce della tabella.

Se, nel frattempo, nessuno dei server *SNTP* risponde, il client *SNTP* interrompe la sincronizzazione. Il dispositivo invia ciclicamente richieste ad ogni server *SNTP* finché un server fornisce un orario valido. Il dispositivo si sincronizza con questo server *SNTP*, anche se in un secondo momento è possibile raggiungere gli altri server.

Name

Specifica il nome del server *SNTP*.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 1..32 caratteri

Address

Specifica l'indirizzo IP del server *SNTP*.

Possibili valori:

- Indirizzo IPv4 valido (impostazione di default: `0.0.0.0`)
- Indirizzo IPv6 valido
- Nome host

Destination UDP port

Specifica la porta UDP sulla quale il server *SNTP* prevede le informazioni orario.

Possibili valori:

- `1..65535` (impostazione di default: `123`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Status

Visualizza lo stato del link tra il client *SNTP* e il server *SNTP*.

Possibili valori:

- *`success`*
  Il dispositivo ha completato la sincronizzazione dell'orario con il server *SNTP*.

- *badDateEncoded*
  Le informazioni orario ricevute contengono errori di protocollo - sincronizzazione non riuscita.
- *other*
  - Il valore 0.0.0.0 è inserito per l'indirizzo IP del server *SNTP* - sincronizzazione non riuscita.
    oppure
  - Il client *SNTP* utilizza un server *SNTP* differente.
- *requestTimedOut*
  Il dispositivo non ha ricevuto risposta dal server *SNTP* - sincronizzazione non riuscita.
- *serverKissOfDeath*
  Il server *SNTP* è sovraccarico. Si richiede al dispositivo di sincronizzarsi con un altro server *SNTP*. Se nessun altro server *SNTP* è disponibile, il dispositivo verifica ad intervalli più lunghi di quelli impostati nel campo *Request interval [s]*, se il server è ancora sovraccarico.
- *serverUnsychronized*
  Il server *SNTP* non è sincronizzato con una fonte orario di riferimento né locale né esterna - sincronizzazione non riuscita.
- *versionNotSupported*
  Le versioni *SNTP* sul client e il server sono incompatibili fra di loro - sincronizzazione non riuscita.

Active

Attiva/disattiva il link al server *SNTP*.

Possibili valori:

- selezionato
  Il link al server *SNTP* è attivato.
  Il client *SNTP* ha accesso al server *SNTP*.
- non selezionato (impostazione di default)
  Il link al server *SNTP* è disattivato.
  Il client *SNTP* non ha accesso al server *SNTP*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

2.2.2 SNTP Server

[Time > SNTP > Server]

In questa finestra di dialogo si specificano le impostazioni con le quali il dispositivo funziona come un server *SNTP*.

Il server *SNTP* fornisce il tempo universale coordinato (UTC) senza considerare le differenze di orario.

Se l'impostazione è adeguata, il server *SNTP* funziona in modalità Broadcast. In modalità Broadcast, il server *SNTP* invia automaticamente messaggi broadcast o multicast in base all'intervallo di invio broadcast.

Operation

Operation

Attiva/disattiva la funzione *SNTP Server* del dispositivo.

Possibili valori:

- `On`
  È abilitata la funzione *SNTP Server*.
  Il dispositivo funziona come un server *SNTP*.
- `Off` (impostazione di default)
  È disabilitata la funzione *SNTP Server*.

Tenere presente l'impostazione nella casella di spunta *Disable server at local time source* nel frame *Configuration*.

Configuration

UDP port

Specifica il numero della porta UDP sulla quale il server *SNTP* del dispositivo riceve richieste da altri client.

Possibili valori:

- `1..65535` (impostazione di default: `123`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Broadcast admin mode

Attiva/disattiva la modalità Broadcast.

- `selezionato`
  Il server *SNTP* risponde a richieste da client *SNTP* in modalità Unicast e invia anche pacchetti *SNTP* in modalità Broadcast come broadcast o multicast.
- `non selezionato` (impostazione di default)
  Il server *SNTP* risponde alle richieste dai client *SNTP* nella modalità Unicast.

Broadcast destination address

Specifica l'indirizzo IP al quale il server *SNTP* del dispositivo invia i pacchetti *SNTP* in modalità Broadcast.

Possibili valori:

- Indirizzo IPv4 valido (impostazione di default: `0.0.0.0`)

Sono permessi indirizzi broadcast e multicast.

Broadcast UDP port

Specifica il numero della porta UDP sulla quale il server *SNTP* invia i pacchetti *SNTP* in modalità Broadcast.

Possibili valori:

- `1..65535` (impostazione di default: `123`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Broadcast VLAN ID

Specifica l'ID della VLAN con il quale il server *SNTP* del dispositivo invia i pacchetti *SNTP* in modalità Broadcast.

Possibili valori:

- `0`
  Il server *SNTP* invia i pacchetti dati *SNTP* nella stessa VLAN in cui è possibile l'accesso alla gestione del dispositivo. Vedere la finestra di dialogo *Basic Settings > Network*.
- `1..4042` (impostazione di default: `1`)

Broadcast send interval [s]

Specifica l'intervallo di tempo in cui il server *SNTP* del dispositivo invia i pacchetti broadcast *SNTP*.

Possibili valori:

- `64..1024` (impostazione di default: `128`)

Disable server at local time source

Attiva/disattiva la disabilitazione del server *SNTP* quando il dispositivo è sincronizzato con il clock locale.

Possibili valori:

- `selezionato`
  La disabilitazione del server *SNTP* è attiva.
  Se il dispositivo è sincronizzato con il clock locale, il dispositivo disattiva il server *SNTP*. Il server *SNTP* continua a rispondere a richieste da client *SNTP*. Nel pacchetto *SNTP*, il server *SNTP* informa i client che è sincronizzato localmente.
- `non selezionato` (impostazione di default)
  La disabilitazione del server *SNTP* non è attiva.
  Se il dispositivo è sincronizzato con il clock locale, il server *SNTP* rimane attivo.

State

State

Visualizza lo stato del server *SNTP*.

Possibili valori:

- *disabled*
  Il server *SNTP* è disattivato.
- *notSynchronized*
  Il server *SNTP* non è sincronizzato con una fonte orario di riferimento né locale né esterna.
- *syncToLocal*
  Il server *SNTP* è sincronizzato con il clock hardware del dispositivo.
- *syncToRefclock*
  Il server *SNTP* è sincronizzato con una fonte orario di riferimento esterna, ad esempio PTP.
- *syncToRemoteServer*
  Il server *SNTP* è sincronizzato con un server *SNTP* che, in una cascata, è in posizione superiore rispetto al dispositivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

2.3 PTP

[Time > PTP]

Il menu include le seguenti finestre di dialogo:

- PTP Global
- PTP Boundary Clock
- PTP Transparent Clock

2.3.1 PTP Global

[Time > PTP > Global]

In questa finestra di dialogo si specificano le impostazioni di base per il *PTP* protocollo.

Il Precision Time Protocol (PTP) è una procedura descritta nello standard IEEE 1588-2008 che fornisce ai dispositivi in rete un orario preciso. Il metodo sincronizza i clock nella rete con una precisione di appena 100 ns. Il protocollo utilizza la comunicazione multicast; il carico sulla rete dovuto ai messaggi di sincronizzazione *PTP* è quindi trascurabile.

Il PTP è significativamente più accurato del SNTP. Se nel dispositivo la funzione *SNTP* e la funzione *PTP* sono abilitate contemporaneamente, la funzione *PTP* è prioritaria.

L'algoritmo *Best Master Clock* consente ai dispositivi della rete di determinare quale dispositivo ha l'orario più preciso. I dispositivi utilizzano il dispositivo con l'orario più preciso come fonte orario di riferimento (*Grandmaster*). In seguito, i dispositivi coinvolti si sincronizzano con la fonte orario di riferimento individuata.

Se si desidera trasportare l'orario PTP accuratamente nella rete, si dovrebbe utilizzare solo i dispositivi con supporto hardware per PTP sui percorsi di trasporto.

Il protocollo distingue i seguenti diversi clock:

- *Boundary Clock (BC)*
  Questo clock ha qualsiasi numero di porte PTP e funziona sia come *PTP* master sia come *PTP* slave. Nel suo segmento di rete corrispondente, il clock funziona come Ordinary clock.
  - In stato *PTP* slave, il clock si sincronizza con un *PTP* master che, nella cascata, è in posizione superiore rispetto al dispositivo.
  - In stato *PTP* master, il clock inoltra attraverso la rete le informazioni orario agli *PTP* slave che, nella cascata, sono in posizione superiore rispetto al dispositivo.
- *Transparent Clock (TC)*
  Questo clock ha qualsiasi numero di porte PTP. Diversamente dal *Boundary Clock*, questo clock corregge le informazioni orario prima di inoltrarle, senza sincronizzarsi.

Operation IEEE1588/PTP

Operation IEEE1588/PTP

Abilita/disabilita la funzione *PTP*.

Nel dispositivo è possibile abilitare contemporaneamente la funzione *802.1AS* oppure la funzione *PTP*.

Possibili valori:

- `On`
  È abilitata la funzione *PTP*.
  Il dispositivo sincronizza il suo clock con il PTP.
  Se nel dispositivo la funzione *SNTP* e la funzione *PTP* sono abilitate contemporaneamente, la funzione *PTP* è prioritaria.
- `Off` (impostazione di default)
  È disabilitata la funzione *PTP*.
  Il dispositivo trasmette i messaggi di sincronizzazione *PTP* senza alcuna correzione su tutte le porte.

Configuration IEEE1588/PTP

PTP mode

Specifica la versione di PTP e la modalità del clock locale.

Possibili valori:

- *v2-transparent-clock* (impostazione di default)
- *v2-boundary-clock*

Sync lower bound [ns]

Specifica il valore di soglia inferiore in nanosecondi per la differenza di percorso tra il clock locale e la fonte orario di riferimento (*Grandmaster*). Se la differenza di percorso scende al di sotto di questo valore una volta, il clock locale viene classificato come sincronizzato.

Possibili valori:

- `0..999999999` (impostazione di default: `30`)

Sync upper bound [ns]

Specifica il valore di soglia superiore in nanosecondi per la differenza di percorso tra il clock locale e la fonte orario di riferimento (*Grandmaster*). Se la differenza di percorso supera questo valore una volta, il clock locale viene classificato come non sincronizzato.

Possibili valori:

- `31..1000000000` (impostazione di default: `5000`)

PTP management

Attiva/disattiva la gestione PTP definita negli standard PTP.

Possibili valori:

- `selezionato`
  La gestione PTP è attivata.
- `non selezionato` (impostazione di default)
  La gestione PTP è disattivata.

Status

Is synchronized

Indica se il clock locale è sincronizzato con la fonte orario di riferimento (*Grandmaster*).

Se la differenza di percorso tra il clock locale e la fonte orario di riferimento (*Grandmaster*) scende al di sotto del valore di soglia inferiore di sincronizzazione una volta, il clock locale è sincronizzato. Questo stato resta fino a quando la differenza di percorso non supera il valore di soglia superiore di sincronizzazione.

Le soglie di sincronizzazione devono essere specificate nel frame *Configuration IEEE1588/PTP*.

Max. offset absolute [ns]

Visualizza la differenza di percorso massima in nanosecondi che si è verificata dal momento in cui il clock locale si è sincronizzato con la fonte orario di riferimento (*Grandmaster*).

PTP time

Visualizza il giorno e l'orario in scala di tempo PTP in cui il clock locale si è sincronizzato con la fonte orario di riferimento (*Grandmaster*). Formato: `Mese Giorno, Anno hh:mm:ss AM/PM`

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

2.3.2 PTP Boundary Clock

[Time > PTP > Boundary Clock]

Questo menu consente di configurare la modalità Boundary Clock per il clock locale.

Il menu include le seguenti finestre di dialogo:
- PTP Boundary Clock Global
- PTP Boundary Clock Port

2.3.2.1 PTP Boundary Clock Global

[Time > PTP > Boundary Clock > Global]

In questa finestra di dialogo si inseriscono le impostazioni generali e trasversali alle porte per la modalità *Boundary Clock* del clock locale. Il *Boundary Clock (BC)* funziona in base alla versione 2 PTP (IEEE 1588-2008).

Le impostazioni vengono applicate quando il clock locale funziona come *Boundary Clock (BC)*. A tale fine, nella finestra di dialogo *Time > PTP > Global* nel campo *PTP mode* selezionare il valore `v2-boundary-clock`.

Operation IEEE1588/PTPv2 BC

Priority 1

Specifica la *priorità 1* per il dispositivo.

Possibili valori:

- `0..255` (impostazione di default: `128`)

L'algoritmo *Best Master Clock* valuta prima la *priorità 1* tra i dispositivi coinvolti, in modo da stabilire la fonte orario di riferimento (*Grandmaster*).

Minore è questo valore, maggiori sono le probabilità che il dispositivo diventi la fonte orario di riferimento (*Grandmaster*). Vedere il frame *Grandmaster*.

Priority 2

Specifica la *priorità 2* per il dispositivo.

Possibili valori:

- `0..255` (impostazione di default: `128`)

Se i criteri valutati in precedenza risultano uguali in più dispositivi, l'algoritmo *Best Master Clock* valuta la *priorità 2* dei dispositivi coinvolti.

Minore è questo valore, maggiori sono le probabilità che il dispositivo diventi la fonte orario di riferimento (*Grandmaster*). Vedere il frame *Grandmaster*.

Domain number

Assegna il dispositivo ad un dominio *PTP*.

Possibili valori:

- `0..255` (impostazione di default: `0`)

Il dispositivo trasmette le informazioni orario solo da e verso i dispositivi nello stesso dominio.

Status IEEE1588/PTPv2 BC

Two step

Indica che il clock sta funzionando in modalità Two-Step.

Steps removed

Indica il numero di percorsi di comunicazione attraversati tra il clock locale del dispositivo e la fonte orario di riferimento (*Grandmaster*).

Per uno slave *PTP* il valore `1` significa che il clock è connesso alla fonte orario di riferimento (*Grandmaster*) direttamente, attraverso 1 percorso di comunicazione.

Offset to master [ns]

Indica la differenza misurata (offset) tra il clock locale e la fonte orario di riferimento (*Grandmaster*) in nanosecondi. Il *PTP* slave calcola la differenza dalle informazioni orario ricevute.

In modalità Two-Step, le informazioni orario sono costituite da 2 messaggi di sincronizzazione *PTP* che il *PTP* master invia ciclicamente:

- Il primo messaggio di sincronizzazione (messaggio sync) contiene un valore stimato per l'orario esatto di invio del messaggio.
- Il secondo messaggio di sincronizzazione (messaggio follow-up) contiene l'orario esatto di invio del primo messaggio.

Il *PTP* slave utilizza due messaggi di sincronizzazione *PTP* per calcolare la differenza (offset) rispetto al master e corregge il suo clock di conseguenza. Per fare ciò, il *PTP* slave considera anche il valore *Delay to master [ns]*.

Delay to master [ns]

Indica il ritardo in nanosecondi nella trasmissione dei *PTP* messaggi di sincronizzazione dal *PTP* master al *PTP* slave.

Il *PTP* slave invia un pacchetto "Delay Request" al *PTP* master e determina in questo modo l'orario di invio esatto del pacchetto. Quando riceve il pacchetto, il *PTP* master genera un time stamp e lo reinvia al *PTP* slave con un pacchetto "Delay Response". Il *PTP* slave utilizza i due pacchetti per calcolare il ritardo, considerandolo a partire dalla successiva misurazione di offset.

Il prerequisito è che il valore del meccanismo di ritardo delle porte slave sia specificato su `e2e`.

Grandmaster

Questo frame indica i criteri utilizzati dall'algoritmo *Best Master Clock* per valutare la fonte orario di riferimento (*Grandmaster*).

L'algoritmo valuta prima la *priorità 1* dei dispositivi coinvolti. Il dispositivo con il valore inferiore di *priorità 1* viene selezionato come 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 tutti i criteri sono uguali per diversi dispositivi, il dispositivo fonte orario di riferimento (*Grandmaster*) viene selezionato in base al valore inferiore nel campo *Clock identity*.

Il dispositivo consente di influenzare quale dispositivo della rete viene selezionato come fonte orario di riferimento (*Grandmaster*). Per farlo occorre modificare il valore nel campo *Priority 1* o nel campo *Priority 2* del frame *Operation IEEE1588/PTPv2 BC*.

Priority 1

Indica la *priorità 1* per il dispositivo attualmente selezionato come fonte orario di riferimento (*Grandmaster*).

Clock class

Indica la classe della fonte orario di riferimento (*Grandmaster*). Parametro per l'algoritmo *Best Master Clock*.

Clock accuracy

Indica l'accuratezza stimata della fonte orario di riferimento (*Grandmaster*). Parametro per l'algoritmo *Best Master Clock*.

Clock variance

Indica la variazione della fonte orario di riferimento (*Grandmaster*), detta anche *variazione dell'offset su scala logaritmica*. Parametro per l'algoritmo *Best Master Clock*.

Priority 2

Indica la *priorità 2* per il dispositivo attualmente selezionato come fonte orario di riferimento (*Grandmaster*).

Local time properties

Time source

Specifica la fonte dell'orario da cui il clock locale ottiene le informazioni orario.

Possibili valori:

- `atomicClock`
- `gps`
- `terrestrialRadio`
- `ptp`
- `ntp`
- `handSet`

- *other*
- *internalOscillator* (impostazione di default)

UTC offset [s]

Specifica la differenza tra la scala di tempo *PTP* e l'UTC.

Vedere la casella di spunta *PTP timescale*.

Possibili valori:

- -32768..32767

Nota: L'impostazione di default è il valore valido alla data di creazione del software del dispositivo. È possibile trovare ulteriori informazioni nel "Bulletin C" del Servizio internazionale di Rotazione sella Terra e Sistemi di Servizio (IERS): http://www.iers.org/IERS/EN/Publications/Bulletins/bulletins.html.

UTC offset valid

Specifica se il valore specificato nel campo *UTC offset [s]* è corretto.

Possibili valori:

- selezionato
- non selezionato (impostazione di default)

Time traceable

Indica se il dispositivo ottiene l'orario da un riferimento UTC primario, ad esempio da un server NTP.

Possibili valori:

- selezionato
- non selezionato

Frequency traceable

Indica se il dispositivo ottiene la frequenza da un riferimento UTC primario, ad esempio da un server NTP.

Possibili valori:

- selezionato
- non selezionato

PTP timescale

Indica se il dispositivo utilizza la scala di tempo PTP.

Possibili valori:

- selezionato
- non selezionato

Secondo IEEE 1588, la scala di tempo è il tempo atomico internazionale TAI iniziato il 01/01/1970.

Diversamente dall'UTC, il TAI non utilizza secondi intercalari.

Al 1° luglio 2020, il tempo TAI ha 37 secondi di anticipo rispetto al tempo UTC.

Identities

Il dispositivo indica le identità come sequenze di byte con valori esadecimali.

I codici identificativi (UUID) sono composti come segue:
- Il codice identificativo del dispositivo consiste nell'indirizzo MAC del dispositivo con l'aggiunta dei valori `ff` e `fe` tra il byte 3 e il byte 4.
- L'UUID della porta consiste del codice identificativo del dispositivo seguito da un ID della porta da 16 bit.

Clock identity

Indica il codice identificativo proprio del dispositivo (UUID).

Parent port identity

Indica il codice identificativo della porta (UUID) del dispositivo master direttamente superiore.

Grandmaster identity

Indica il codice identificativo (UUID) del dispositivo fonte orario di riferimento (*Grandmaster*).

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

2.3.2.2 PTP Boundary Clock Port

[Time > PTP > Boundary Clock > Port]

In questa finestra di dialogo si specificano le impostazioni *Boundary Clock (BC)* su ciascuna porta individuale.

Le impostazioni vengono applicate quando il clock locale funziona come *Boundary Clock (BC)*. A tale fine, nella finestra di dialogo *Time > PTP > Global* nel campo *PTP mode* selezionare il valore `v2-boundary-clock`.

Tabella

Port

Visualizza il numero di porta.

PTP enable

Attiva/disattiva la trasmissione del messaggio di sincronizzazione *PTP* sulla porta.

Possibili valori:

- `selezionato` (impostazione di default)
  La trasmissione è attivata. La porta inoltra e riceve i messaggi di sincronizzazione *PTP*.
- `non selezionato`
  La trasmissione è disattivata. La porta blocca i messaggi di sincronizzazione *PTP*.

PTP status

Indica lo stato attuale della porta.

Possibili valori:

- *initializing*
  Fase di inizializzazione
- *faulty*
  Modalità faulty: errore nel protocollo PTP.
- *disabled*
  PTP disabilitato sulla porta.
- *listening*
  La porta del dispositivo è in attesa di messaggi di sincronizzazione *PTP*.
- *pre-master*
  modalità *PTP* pre-master
- *master*
  modalità *PTP* master
- *passive*
  modalità *PTP* passivo
- *uncalibrated*
  modalità *PTP* non calibrato
- *slave*
  modalità *PTP* slave

Sync interval

Specifica l'intervallo in secondi in cui la porta trasmette i messaggi di sincronizzazione *PTP*.

Possibili valori:

- `0.25`
- `0.5`
- `1` (impostazione di default)
- `2`

Delay mechanism

Specifica il meccanismo in base al quale il dispositivo misura il ritardo per la trasmissione dei messaggi di sincronizzazione *PTP*.

Possibili valori:

- *`disabled`*
  La misurazione del ritardo per i messaggi di sincronizzazione *PTP* per i dispositivi PTP collegati non è attiva.
- *`e2e`* (impostazione di default)
  End-to-End: in quanto *PTP* slave, la porta misura il ritardo per i messaggi di sincronizzazione *PTP* verso il *PTP* master.
  Il dispositivo visualizza il valore misurato nella finestra di dialogo *Time > PTP > Boundary Clock >* Global.
- *`p2p`*
  Peer-to-Peer: il dispositivo misura il ritardo per i messaggi di sincronizzazione *PTP* per i dispositivi PTP collegati, a patto che questi dispositivi supportino il P2P.
  Questo meccanismo evita al dispositivo di dover determinare di nuovo il ritardo in caso di riconfigurazione.

P2P delay

Indica il ritardo Peer-to-Peer misurato per i messaggi di sincronizzazione *PTP*.

Il prerequisito è quello di selezionare il valore *`p2p`* nella colonna *Delay mechanism*.

P2P delay interval [s]

Specifica l'intervallo in secondi in cui la porta misura il ritardo Peer-to-Peer.

Il prerequisito è quello di aver selezionato il valore *`p2p`* su questa porta e sulla porta del dispositivo remoto.

Possibili valori:

- `1` (impostazione di default)
- `2`
- `4`
- `8`
- `16`
- `32`

Network protocol

Specifica quale protocollo utilizza la porta per trasmettere i messaggi di sincronizzazione *PTP*.

Possibili valori:

- *IEEE 802.3* (impostazione di default)
- *UDP/IPv4*

Announce interval [s]

Specifica l'intervallo in secondi in cui la porta trasmette i messaggi per il riconoscimento della topologia PTP.

Assegnare lo stesso valore a tutti i dispositivi di un dominio *PTP*.

Possibili valori:

- 1
- 2 (impostazione di default)
- 4
- 8
- 16

Announce timeout

Specifica il numero di intervalli di announcing.

Esempio:

Per l'impostazione di default (*Announce interval [s]* = 2 e *Announce timeout* = 3) il timeout è 3 × 2 s = 6 s.

Possibili valori:

- 2..10 (impostazione di default: 3)
  Assegnare lo stesso valore a tutti i dispositivi di un dominio *PTP*.

E2E delay interval [s]

Indica l'intervallo in secondi in cui la porta misura il ritardo End-to-End:

- Quando la porta funziona come *PTP* master, il dispositivo assegna alla porta il valore 8.
- Quando la porta funziona come *PTP* slave, il valore è specificato dal *PTP* master collegato alla porta.

V1 hardware compatibility

Specifica se la porta adegua la lunghezza dei messaggi di sincronizzazione *PTP* quando nella colonna *Network protocol* si è impostato il valore *udpIpv4*.

È possibile che altri dispositivi nella rete si attendano che la lunghezza dei messaggi di sincronizzazione *PTP* sia uguale a quella dei messaggi PTPv1.

Possibili valori:

- *auto* (impostazione di default)
  Il dispositivo rileva automaticamente se altri dispositivi nella rete si attendono che la lunghezza dei messaggi di sincronizzazione *PTP* sia uguale a quella dei messaggi PTPv1. In questo caso il dispositivo espande la lunghezza dei messaggi di sincronizzazione *PTP* prima di trasmetterli.

- *on*
  Il dispositivo espande la lunghezza dei messaggi di sincronizzazione *PTP* prima di trasmetterli.
- *off*
  Il dispositivo trasmette i messaggi di sincronizzazione *PTP* senza modificare la lunghezza.

Asymmetry

Corregge il valore del ritardo misurato corrotto da percorsi di trasmissione non simmetrici.

Possibili valori:

- `-2000000000..2000000000` (impostazione di default: `0`)

Il valore rappresenta la simmetria del ritardo in nanosecondi.

Un valore di ritardo misurato di y ns corrisponde a una asimmetria di y × 2 ns.

Il valore è positivo se il ritardo dal *PTP* master al *PTP* slave è superiore a quello in direzione opposta.

VLAN

Specifica l'ID VLAN con cui il dispositivo indica i messaggi di sincronizzazione *PTP* su questa porta.

Possibili valori:

- *none* (impostazione di default)
  Il dispositivo trasmette i messaggi di sincronizzazione *PTP* senza tag VLAN.
- `0..4042`
  Specificare le VLAN già impostate nel dispositivo dall'elenco.

Verificare che la porta faccia parte della VLAN.

Vedere la finestra di dialogo *Switching > VLAN > Configuration*.

VLAN priority

Specifica la priorità con cui il dispositivo trasmette i messaggi di sincronizzazione *PTP* indicati con un ID VLAN (Layer 2, IEEE 802.1D).

Possibili valori:

- `0..7` (impostazione di default: `6`)

Se nella colonna *VLAN* si è specificato il valore *none*, il dispositivo ignora la priorità della VLAN.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

2.3.3 PTP Transparent Clock

[Time > PTP > Transparent Clock]

Questo menu consente di configurare la modalità *Transparent Clock* per il clock locale.

Il menu include le seguenti finestre di dialogo:
- PTP Transparent Clock Global
- PTP Transparent Clock Port

2.3.3.1 PTP Transparent Clock Global

[Time > PTP > Transparent Clock > Global]

In questa finestra di dialogo si inseriscono le impostazioni generali e trasversali alle porte per la modalità *Transparent Clock* del clock locale. Il *Transparent Clock (TC)* funziona in base alla versione 2 PTP (IEEE 1588-2008).

Le impostazioni vengono applicate quando il clock locale funziona come *Transparent Clock (TC)*. A tale fine, nella finestra di dialogo *Time > PTP > Global* nel campo *PTP mode* selezionare il valore *v2-transparent-clock*.

Operation IEEE1588/PTPv2 TC

Delay mechanism

Specifica il meccanismo in base al quale il dispositivo misura il ritardo per la trasmissione dei messaggi di sincronizzazione *PTP*.

Possibili valori:

- *e2e* (impostazione di default)
  In quanto *PTP* slave, la porta misura il ritardo per i messaggi di sincronizzazione *PTP* verso il *PTP* master.
  Il dispositivo visualizza il valore misurato nella finestra di dialogo *Time > PTP > Transparent Clock > Global*.
- *p2p*
  Il dispositivo misura il ritardo per i messaggi di sincronizzazione *PTP* per tutti i dispositivi PTP collegati, a patto che il dispositivo supporti il P2P.
  Questo meccanismo evita al dispositivo di dover determinare di nuovo il ritardo in caso di riconfigurazione.
  Se si specifica questo valore, allora il valore *IEEE 802.3* è disponibile solo nel campo *Network protocol*.
- *e2e-optimized*
  Come *e2e*, con le seguenti caratteristiche specifiche:
  - Il dispositivo trasmette le Delay Request dei *PTP* slave solo al *PTP* master, anche se queste richieste sono messaggi multicast. Il dispositivo evita quindi agli altri dispositivi le richieste multicast non necessarie.
  - Se la topologia master-slave cambia, il dispositivo riapprende la porta per il *PTP* master appena riceve un messaggio di sincronizzazione da un altro *PTP* master.
  - Se il dispositivo non conosce un *PTP* master, il dispositivo trasmette le Delay Request alle porte.
- *disabled*
  La misurazione del ritardo è disabilitata sulla porta. Il dispositivo rifiuta i messaggi per la misurazione del ritardo.

Primary domain

Assegna il dispositivo ad un dominio *PTP*.

Possibili valori:

- *0..255* (impostazione di default: *0*)

Il dispositivo trasmette le informazioni orario solo da e verso i dispositivi nello stesso dominio.

Network protocol

Specifica quale protocollo utilizza la porta per trasmettere i messaggi di sincronizzazione *PTP*.

Possibili valori:

- *ieee8023* (impostazione di default)
- *udpIpv4*

Multi domain mode

Attiva/disattiva la correzione dei messaggi di sincronizzazione *PTP* in ogni dominio *PTP*.

Possibili valori:

- `selezionato`
  Il dispositivo corregge i messaggi di sincronizzazione *PTP* in ogni dominio *PTP*.
- `non selezionato` (impostazione di default)
  Il dispositivo corregge i messaggi di sincronizzazione *PTP* solo nel domino primario *PTP*. Vedere il campo *Primary domain*.

VLAN ID

Specifica l'ID VLAN con cui il dispositivo indica i messaggi di sincronizzazione *PTP* su questa porta.

Possibili valori:

- *none* (impostazione di default)
  Il dispositivo trasmette i messaggi di sincronizzazione *PTP* senza tag VLAN.
- `0..4042`
  Specificare le VLAN già impostate nel dispositivo dall'elenco.

VLAN priority

Specifica la priorità con cui il dispositivo trasmette i messaggi di sincronizzazione *PTP* indicati con un ID VLAN (Layer 2, IEEE 802.1D).

Possibili valori:

- `0..7` (impostazione di default: `6`)

Il dispositivo ignora il valore specificato se nel campo *VLAN ID* è specificato il valore *none*.

Local synchronization

Syntonize

Attiva/disattiva la sincronizzazione della frequenza del *Transparent Clock* con il *PTP* master.

Possibili valori:

- `selezionato` (impostazione di default)
  La sincronizzazione della frequenza è attiva.
  Il dispositivo sincronizza la frequenza.
- `non selezionato`
  La sincronizzazione della frequenza non è attiva.
  La frequenza rimane costante.

Synchronize local clock

Attiva/disattiva la sincronizzazione dell'orario di sistema locale.

Possibili valori:

- `selezionato`
  La sincronizzazione è attiva.
  Il dispositivo sincronizza l'orario di sistema locale rispetto all'orario ricevuto via PTP. Il prerequisito è che la casella di spunta *Syntonize* sia selezionata.
- `non selezionato` (impostazione di default)
  La sincronizzazione non è attiva.
  L'orario di sistema locale rimane costante.

Current master

Indica il codice identificativo della porta (UUID) del dispositivo master direttamente superiore con cui il dispositivo sincronizza la sua frequenza.

Se il valore contiene solo zeri è perché:

- È disabilitata la funzione *Syntonize*.
  oppure
- Il dispositivo non riesce a trovare un *PTP* master.

Offset to master [ns]

Indica la differenza misurata (offset) tra il clock locale e il *PTP* master in nanosecondi. Il dispositivo calcola la differenza rispetto alle informazioni orario ricevute.

Il prerequisito è che la funzione *Synchronize local clock* sia abilitata.

Delay to master [ns]

Indica il ritardo in nanosecondi nella trasmissione dei *PTP* messaggi di sincronizzazione dal *PTP* master al *PTP* slave.

Prerequisito:

- È abilitata la funzione *Synchronize local clock*.
- Nel campo *Delay mechanism* il valore `e2e` è selezionato.

Status IEEE1588/PTPv2 TC

Clock identity

Indica il codice identificativo proprio del dispositivo (UUID).

Il dispositivo indica le identità come sequenze di byte con valori esadecimali.

Il codice identificativo del dispositivo consiste nell'indirizzo MAC del dispositivo con l'aggiunta dei valori `ff` e `fe` tra il byte 3 e il byte 4.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

2.3.3.2 PTP Transparent Clock Port

[Time > PTP > Transparent Clock > Port]

In questa finestra di dialogo si specificano le impostazioni *Transparent Clock (TC)* su ciascuna porta individuale.

Le impostazioni vengono applicate quando il clock locale funziona come *Transparent Clock (TC)*. A tale fine, nella finestra di dialogo *Time > PTP > Global* nel campo *PTP mode* selezionare il valore `v2-transparent-clock`.

Tabella

Port

Visualizza il numero di porta.

PTP enable

Attiva/disattiva la trasmissione di messaggi di sincronizzazione *PTP* sulla porta.

Possibili valori:

- `selezionato` (impostazione di default)
  La trasmissione è attiva.
  La porta inoltra e riceve i messaggi di sincronizzazione *PTP*.
- `non selezionato`
  La trasmissione non è attiva.
  La porta blocca i messaggi di sincronizzazione *PTP*.

P2P delay interval [s]

Specifica l'intervallo in secondi in cui la porta misura il ritardo Peer-to-Peer.

Il prerequisito è quello di selezionare il valore `p2p` su questa porta e sulla porta del terminale remoto. Vedere la lista di opzioni *Delay mechanism* nella finestra di dialogo *Time > PTP > Transparent Clock > Global*.

Possibili valori:

- `1` (impostazione di default)
- `2`
- `4`
- `8`
- `16`
- `32`

P2P delay

Indica il ritardo Peer-to-Peer misurato per i messaggi di sincronizzazione *PTP*.

Il prerequisito è che nella lista di opzioni *Delay mechanism* si selezioni il pulsante di opzione `p2p`. Vedere il campo *Delay mechanism* nella finestra di dialogo *Time > PTP > Transparent Clock > Global*.

Asymmetry

Corregge il valore del ritardo misurato corrotto da percorsi di trasmissione non simmetrici.

Possibili valori:

- `-2000000000..2000000000` (impostazione di default: `0`)

Il valore rappresenta la simmetria del ritardo in nanosecondi.

Un valore di ritardo misurato di y ns corrisponde a una asimmetria di y × 2 ns.

Il valore è positivo se il ritardo dal *PTP* master al *PTP* slave è superiore a quello in direzione opposta.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

2.4 802.1AS

[Time > 802.1AS]

Il *802.1AS* protocollo è una procedura descritta nello standard IEEE 802.1AS-2011 che definisce come sincronizzare accuratamente l'orario tra i dispositivi della rete. Quando si utilizza il *802.1AS* protocollo su rete Ethernet è possibile considerarlo un profilo dello standard IEEE 1588-2008.

L'algoritmo *Best Master Clock* consente ai dispositivi della rete di determinare quale dispositivo ha l'orario più preciso. I dispositivi utilizzano il dispositivo con l'orario più preciso come fonte orario di riferimento (*Grandmaster*). In seguito, i dispositivi coinvolti si sincronizzano con la fonte orario di riferimento individuata.

Il *802.1AS* protocollo presenta le seguenti specifiche:

- Nel dispositivo è possibile abilitare sia la funzione *802.1AS* sia la funzione *PTP*.
- Se nel dispositivo la funzione *SNTP* e la funzione *802.1AS* sono abilitate contemporaneamente, la funzione *802.1AS* è prioritaria.
- La funzione *802.1AS* supporta un solo dominio.

Il menu include le seguenti finestre di dialogo:

- 802.1AS Global
- 802.1AS Port
- 802.1AS Statistics

2.4.1 802.1AS Global

[Time > 802.1AS > Global]

In questa finestra di dialogo si specificano le impostazioni di base per il *802.1AS* protocollo.

Operation

Operation

Abilita/disabilita la funzione *802.1AS*.

Possibili valori:

- `On`
  È abilitata la funzione *802.1AS*.
  Il dispositivo sincronizza il suo clock utilizzando il *802.1AS* protocollo.
  Si consideri l'attivazione del *802.1AS* protocollo sulle singole porte.

- `Off` (impostazione di default)
  È disabilitata la funzione *802.1AS*.

Configuration

Priority 1

Specifica la *priorità 1* per il dispositivo.

Possibili valori:

- `0..255` (impostazione di default: `246`)

L'algoritmo *Best Master Clock* valuta prima la *priorità 1* tra i dispositivi coinvolti, in modo da stabilire la fonte orario di riferimento (*Grandmaster*).

Minore è questo valore, maggiori sono le probabilità che il dispositivo sia selezionato come fonte orario di riferimento (*Grandmaster*).

Se si specifica il valore `255`, il dispositivo non viene selezionato come fonte orario di riferimento (*Grandmaster*). Vedere il frame *Grandmaster*.

Priority 2

Specifica la *priorità 2* per il dispositivo.

Possibili valori:

- `0..255` (impostazione di default: `248`)

Se i criteri valutati in precedenza risultano uguali in più dispositivi, l'algoritmo *Best Master Clock* valuta la *priorità 2* dei dispositivi coinvolti.

Minore è questo valore, maggiori sono le probabilità che il dispositivo sia selezionato come fonte orario di riferimento (*Grandmaster*). Vedere il frame *Grandmaster*.

Sync lower bound [ns]

Specifica il valore di soglia inferiore in nanosecondi per la differenza di orario misurata tra il clock locale e la fonte orario di riferimento (*Grandmaster*). Se la differenza di orario misurata scende al di sotto di questo valore una volta, il clock locale viene classificato come sincronizzato.

Possibili valori:

- `0..999999999` (impostazione di default: `30`)

Sync upper bound [ns]

Specifica il valore di soglia superiore in nanosecondi per la differenza di orario misurata tra il clock locale e la fonte orario di riferimento (*Grandmaster*). Se la differenza di orario misurata supera questo valore una volta, il clock locale viene classificato come non sincronizzato.

Possibili valori:

- `31..1000000000` (impostazione di default: `5000`)

UTC offset [s]

Indica la differenza tra la *802.1AS* scala di tempo e l'UTC.

UTC offset valid

Indica se il valore visualizzato nel campo *UTC offset [s]* è corretto.

Possibili valori:

- `selezionato`
- `non selezionato`

Status

Offset to master [ns]

Indica la differenza misurata (offset) tra il clock locale e la fonte orario di riferimento (*Grandmaster*) in nanosecondi. Il dispositivo calcola la differenza rispetto alle informazioni orario ricevute.

Max. offset absolute [ns]

Indica la differenza di orario massima misurata in nanosecondi che si è verificata dal momento in cui il clock locale si è sincronizzato con la fonte orario di riferimento (*Grandmaster*).

Is synchronized

Indica se il clock locale è sincronizzato con la fonte orario di riferimento (*Grandmaster*).

Se la differenza di orario misurata tra il clock locale e la fonte orario di riferimento (*Grandmaster*) scende al di sotto del valore di soglia inferiore di sincronizzazione il clock locale è sincronizzato. Questo stato resta fino a quando la differenza di orario misurata non supera il valore di soglia superiore di sincronizzazione.

Le soglie di sincronizzazione devono essere specificate nel frame *Configuration*.

Steps removed

Indica il numero di percorsi di comunicazione attraversati tra il clock locale del dispositivo e la fonte orario di riferimento (*Grandmaster*).

Per uno slave *802.1AS* il valore `1` significa che il clock è connesso alla fonte orario di riferimento (*Grandmaster*) direttamente, attraverso 1 percorso di comunicazione.

Clock identity

Indica il codice identificativo del clock del dispositivo.

Il dispositivo visualizza il codice identificativo come sequenza di byte con valori esadecimali.

Il codice identificativo del dispositivo consiste nell'indirizzo MAC del dispositivo con l'aggiunta dei valori `ff` e `fe` tra il byte 3 e il byte 4.

Grandmaster

Questo frame indica i criteri utilizzati dall'algoritmo *Best Master Clock* per valutare la fonte orario di riferimento (*Grandmaster*).

L'algoritmo valuta prima la *priorità 1* dei dispositivi coinvolti. Il dispositivo con il valore inferiore di *priorità 1* viene selezionato come 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 tutti i criteri sono uguali per diversi dispositivi, il dispositivo fonte orario di riferimento (*Grandmaster*) viene selezionato in base al valore inferiore nel campo *Clock identity*.

Il dispositivo consente di influenzare quale dispositivo della rete viene selezionato come fonte orario di riferimento (*Grandmaster*). Per farlo occorre modificare il valore nel campo *Priority 1* o nel campo *Priority 2* del frame *Configuration*.

Priority 1

Indica la *priorità 1* per il dispositivo attualmente selezionato come fonte orario di riferimento (*Grandmaster*).

Clock class

Indica la classe della fonte orario di riferimento (*Grandmaster*). Parametro per l'algoritmo *Best Master Clock*.

Clock accuracy

Indica l'accuratezza stimata della fonte orario di riferimento (*Grandmaster*). Parametro per l'algoritmo *Best Master Clock*.

Clock variance

Indica la variazione della fonte orario di riferimento (*Grandmaster*), detta anche *variazione dell'offset su scala logaritmica*. Parametro per l'algoritmo *Best Master Clock*.

Priority 2

Indica la *priorità 2* per il dispositivo attualmente selezionato come fonte orario di riferimento (*Grandmaster*).

Clock identity

Indica il codice identificativo del dispositivo fonte orario di riferimento (*Grandmaster*). Il dispositivo visualizza il codice identificativo come sequenza di byte con valori esadecimali.

Parent

Clock identity

Indica l'identificativo della porta del dispositivo master direttamente superiore. Il dispositivo visualizza il codice identificativo come sequenza di byte con valori esadecimali.

Port

Indica il numero della porta del dispositivo master direttamente superiore.

Cumulative rate ratio [ppm]

Indica la differenza di frequenza misurata del clock locale in parti per milione rispetto alla fonte orario di riferimento (*Grandmaster*).

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

2.4.2 802.1AS Port

[Time > 802.1AS > Port]

In questa finestra di dialogo si specificano le impostazioni *802.1AS* di ciascuna porta individuale.

Tabella

Port

Visualizza il numero di porta.

Active

Attiva/disattiva il protocollo *802.1AS* sulla porta.

Possibili valori:

- `selezionato` (impostazione di default)
  Il protocollo è attivo sulla porta.
  Sulla porta, il dispositivo sincronizza il suo clock utilizzando il protocollo *802.1AS*.
- `non selezionato`
  Il protocollo non è attivo sulla porta.

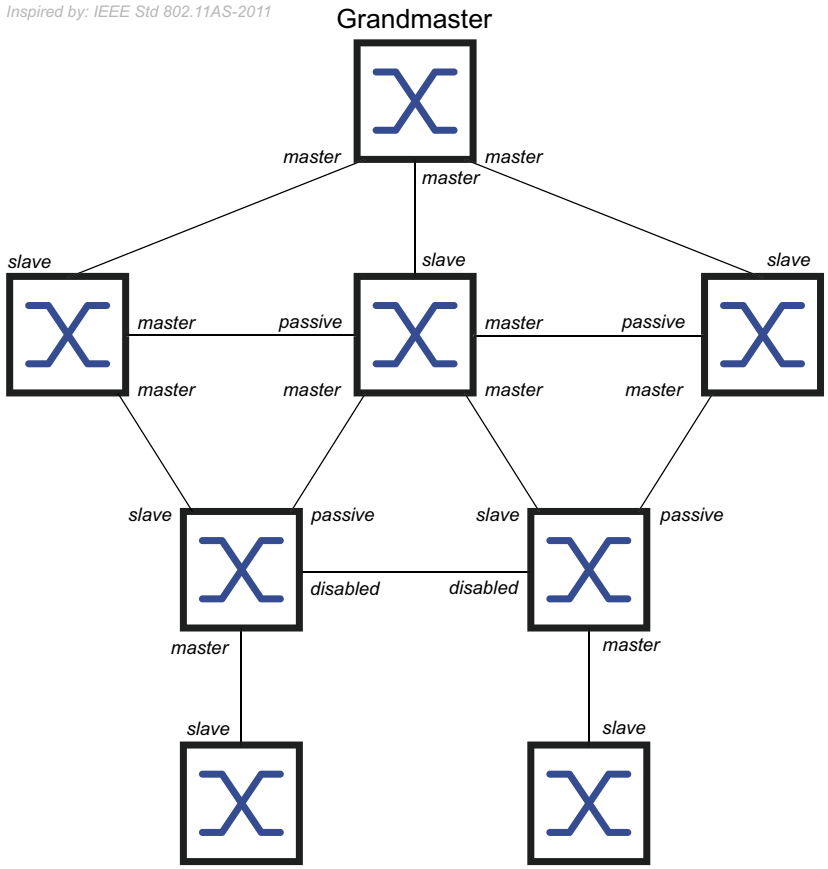
Role

Visualizza il ruolo attuale della porta considerando il protocollo *802.1AS*.

Possibili valori:

- *disabled*
  La porta opera con ruolo *Disabled Port*. La porta non supporta *802.1AS*.
- *master*
  La porta opera con ruolo *Master Port*.

- `passive`
  La porta opera con ruolo *Passive Port*.
- `slave`
  La porta opera con ruolo *Slave Port*.



AS capable

Visualizza se il protocollo *802.1AS* è attivo sulla porta.

Possibili valori:

- `selezionato`
  Il protocollo *802.1AS* è attivo sulla porta. I prerequisiti sono:
  – La porta misura un *Peer delay*, la casella di spunta nella colonna *Measuring delay* è selezionata.
  – Il valore nella colonna *Peer delay [ns]* è inferiore al valore nella colonna *Peer delay threshold [ns]*.
- `non selezionato`
  Il protocollo *802.1AS* non è attivo sulla porta.

Announce interval [s]

Specifica l'intervallo in secondi in cui la porta (con ruolo *Master Port*) trasmette messaggi *Announce* per il riconoscimento della topologia *802.1AS*.

Possibili valori:

- `1..2` (impostazione di default: `1`)
  Assegnare lo stesso valore a tutti i dispositivi di un dominio *802.1AS*.
- `–`
  La porta non trasmette messaggi *Announce*.

Announce timeout

Specifica il numero di *Announce interval [s]* in cui la porta (con ruolo *Slave Port*) attende messaggi *Announce*.

Se il numero di intervalli trascorre senza la ricezione di un messaggio *Announce*, il dispositivo tenta di trovare un nuovo percorso per la fonte orario di riferimento utilizzando l'algoritmo *Best Master Clock*. Se il dispositivo trova una fonte orario di riferimento (*Grandmaster*), assegna il ruolo *Slave Port* alla porta attraverso cui conduce il nuovo percorso. Altrimenti, il dispositivo diventa la fonte orario di riferimento (*Grandmaster*) e assegna il ruolo *Master Port* alle sue porte.

Esempio: nell'impostazione di default (*`Announce interval [s] = 1, Announce timeout = 3`*) il timeout è `3 × 1 s = 3 s`.

Possibili valori:

- `2..10` (impostazione di default: `3`)
  Assegnare lo stesso valore a tutte le porte che appartengono allo stesso domino *802.1AS*.

Sync interval [s]

Specifica l'intervallo in secondi in cui la porta (con ruolo *Master Port*) trasmette i messaggi *Sync* per la sincronizzazione orario.

Possibili valori:

- `0.125` (impostazione di default)
- `0.250`
- `0.5`
- `1`
- `–`
  La porta non trasmette messaggi *Sync*.

Sync timeout

Specifica il numero di *Sync interval [s]* in cui la porta (con ruolo *Slave Port*) attende messaggi *Sync*.

Se il numero di intervalli trascorre senza la ricezione di un messaggio *Sync*, il dispositivo tenta di trovare un nuovo percorso per la fonte orario di riferimento utilizzando l'algoritmo *Best Master Clock*. Se il dispositivo trova una fonte orario di riferimento (*Grandmaster*), assegna il ruolo *Slave Port* alla porta attraverso cui conduce il nuovo percorso. Altrimenti, il dispositivo diventa la fonte orario di riferimento (*Grandmaster*) e assegna il ruolo *Master Port* alle sue porte.

Esempio: nell'impostazione di default (*`Sync interval [s] = 0.125, Sync timeout = 3`*) il timeout è `3 × 0.125 s = 0.375 s`.

Possibili valori:

- `2..10` (impostazione di default: `3`)
  Assegnare lo stesso valore a tutte le porte che appartengono allo stesso domino *802.1AS*.

Peer delay interval [s]

Specifica l'intervallo in secondi in cui la porta (con ruolo *Master Port*, *Passive Port* o *Slave Port*) trasmette un messaggio *Peer delay request* per misurare il *Peer delay*.

Possibili valori:

- `1` (impostazione di default)
- `2`
- `4`
- `8`
- `–`
  La porta non trasmette messaggi *Peer delay request*.

Peer delay timeout

Specifica il numero di *Peer delay interval [s]* in cui la porta (con ruolo *Master Port*, *Passive Port* o *Slave Port*) attende i messaggi *Delay response*.

Se il numero di intervalli trascorre senza la ricezione di un messaggio *Delay response*, il dispositivo assegna il ruolo *Disabled Port* alla porta. La porta non supporta più *802.1AS*.

Possibili valori:

- `2..10` (impostazione di default: `3`)

Peer delay threshold [ns]

Specifica il valore di soglia superiore per il *Peer delay* in nanosecondi. Se il valore nella colonna *Peer delay [ns]* è superiore a questo valore, il dispositivo assegna il ruolo *Disabled Port* alla porta. La porta non supporta più *802.1AS*.

Possibili valori:

- `0..1000000000` (impostazione di default: `10000`)

Measuring delay

Visualizza se la porta misura un *Peer delay*.

Possibili valori:

- `selezionato`
  La porta misura un *Peer delay*. Il valore misurato si trova nella colonna *Peer delay [ns]*.
- `non selezionato`
  La porta non misura un *Peer delay*.

Peer delay [ns]

Visualizza il valore *Peer delay* misurato in nanosecondi. Il prerequisito è che la casella di spunta nella colonna *Measuring delay* sia selezionata.

Neighbor rate ratio [ppm]

Visualizza la differenza di frequenza misurata del clock locale in parti per milione rispetto al clock del dispositivo adiacente.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

2.4.3 802.1AS Statistics

[Time > 802.1AS > Statistics]

Questa finestra di dialogo visualizza le informazioni relative al numero di messaggi ricevuti, inviati o rifiutati sulle porte. La finestra di dialogo visualizza inoltre i contatori che crescono ogni volta che si è verificato un evento di timeout.

Tabella

Port

Visualizza il numero di porta.

Received messages

Visualizza i contatori per i messaggi ricevuti sulle porte:

Sync messages

Visualizza il numero di messaggi *Sync*.

Sync follow-up messages

Visualizza il numero di messaggi *Sync follow-up*.

Delay request messages

Visualizza il numero di messaggi *Peer delay request*.

Delay response messages

Visualizza il numero di messaggi *Peer delay response*.

Delay response follow-up messages

Visualizza il numero di messaggi *Peer delay response follow-up*.

Announce messages

Visualizza il numero di messaggi *Announce*.

Discarded messages

Visualizza il numero di messaggi *Sync* che il dispositivo ha rifiutato su questa porta. Ad esempio, il dispositivo rifiuta un messaggio *Sync* nei casi in cui la porta non riceve un messaggio *Sync follow-up* per un messaggio *Sync* corrispondente.

Sync timeout

Visualizza il numero di volte in cui un evento *Sync timeout* si è verificato sulla porta. Vedere la colonna *Sync timeout* nella finestra di dialogo *Time > 802.1AS > Port*.

Announce timeout

Visualizza il numero di volte in cui un evento *Announce timeout* si è verificato su questa porta. Vedere la colonna *Announce timeout* nella finestra di dialogo *Time > 802.1AS > Port*.

Delay timeout

Visualizza il numero di volte in cui un evento *Peer delay timeout* si è verificato su questa porta. Vedere la colonna *Peer delay timeout* nella finestra di dialogo *Time > 802.1AS > Port*.

Transmitted messages

Visualizza i contatori per i messaggi trasmessi sulle porte:

Sync messages

Visualizza il numero di messaggi *Sync*.

Sync follow-up messages

Visualizza il numero di messaggi *Sync follow-up*.

Delay request messages

Visualizza il numero di messaggi *Peer delay request*.

Delay response messages

Visualizza il numero di messaggi *Peer delay response*.

Delay response follow-up messages

Visualizza il numero di messaggi *Peer delay response follow-up*.

Announce messages

Visualizza il numero di messaggi *Announce*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

3 Device Security

Il menu include le seguenti finestre di dialogo:
- User Management
- Authentication List
- LDAP
- Management Access
- Pre-login Banner

3.1 User Management

[Device Security > User Management]

Se gli utenti accedono con dati di accesso validi, il dispositivo consente loro di accedere alla gestione del dispositivo.

In questa finestra di dialogo si gestiscono gli utenti della gestione utenti locale. Inoltre, qui si specificano le seguenti impostazioni:
- Impostazioni per l'accesso
- Impostazioni per il salvataggio delle password
- Specifica dei criteri per password valide

I metodi che il dispositivo utilizza per l'autenticazione si specificano nella finestra di dialogo*Device Security > Authentication List*.

Configuration

Attraverso questo frame si specificano le impostazioni per l'accesso.

Login attempts

Specifica il numero di tentativi di accesso possibili quando l'utente accede alla gestione del dispositivo utilizzando l'interfaccia grafica utente e la Command Line Interface.

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.

Possibili valori:
- `0..5` (impostazione di default: `0`)

Se l'utente effettua uno o più tentativi di accesso non riusciti, il dispositivo blocca l'accesso per quell'utente.

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

Con il valore `0` si disattiva il blocco. L'utente può effettuare un numero illimitato di tentativi di login.

Login attempts period (min.)

Visualizza il periodo di tempo prima che il dispositivo resetti il contatore nel campo *Login attempts*.

Possibili valori:

- `0..60` (impostazione di default: `0`)

Min. password length

Il dispositivo accetta la password se contiene almeno il numero di caratteri qui specificato.

Il dispositivo verifica la password in base a questa impostazione, indipendentemente dall'impostazione per la casella di spunta *Policy check*.

Possibili valori:

- `1..64` (impostazione di default: `6`)

Password policy

Questo riguardo consente di specificare i criteri per password valide. Il dispositivo verifica ogni nuova password e cambio di password secondo questi criteri.

Le impostazioni hanno effetto sulla colonna *Password*. Il prerequisito è quello di selezionare la casella di spunta nella colonna *Policy check*.

Upper-case characters (min.)

Il dispositivo accetta la password se contiene almeno il numero di maiuscole qui specificato.

Possibili valori:

- `0..16` (impostazione di default: `1`)

Con il valore `0` si disattiva questa impostazione.

Lower-case characters (min.)

Il dispositivo accetta la password se contiene almeno il numero di minuscole qui specificato.

Possibili valori:

- `0..16` (impostazione di default: `1`)

Con il valore `0` si disattiva questa impostazione.

Digits (min.)

Il dispositivo accetta la password se contiene almeno tanti numeri quanti quelli qui specificati.

Possibili valori:

- `0..16` (impostazione di default: `1`)

Con il valore `0` si disattiva questa impostazione.

Special characters (min.)

Il dispositivo accetta la password se contiene almeno il numero di caratteri speciali qui specificato.

Possibili valori:

- `0..16` (impostazione di default: `1`)

Con il valore `0` si disattiva questa impostazione.

Tabella

Per ogni utente è necessario un account utente attivo per avere l'accesso alla gestione del dispositivo. La tabella consente la configurazione e la gestione degli account utente.

Per modificare le impostazioni, fare clic sul parametro desiderato nella tabella e modificare il valore.

User name

Visualizza il nome dell'account utente.

Per creare un nuovo account utente, fare clic sul pulsante  .

Active

Attiva/disattiva l'account utente.

Possibili valori:

- `selezionato`
  L'account utente è attivo. Il dispositivo accetta l'accesso di un utente con questo nome utente.
- `non selezionato` (impostazione di default)
  L'account utente non è attivo. Il dispositivo rifiuta l'accesso di un utente con questo nome utente.

Quando un account utente esiste con il ruolo di accesso *`administrator`*, questo account utente è sempre attivo.

Password

Specifica la password che l'utente applica per accedere alla gestione del dispositivo utilizzando l'interfaccia grafica utente o la Command Line Interface.

Visualizza ***** (asterischi) invece della password con cui l'utente effettua l'accesso. Per modificare la password, fare clic sul campo rilevante.

Quando si specifica la password per la prima volta, il dispositivo utilizza la stessa password nelle colonne *SNMP auth password* e *SNMP encryption password*.

- Il dispositivo consente di specificare diverse password nelle colonne *SNMP auth password* e *SNMP encryption password*.
- Se si modifica la password nella colonna attuale, il dispositivo modifica anche le password per le colonne *SNMP auth password* e *SNMP encryption password*, ma solo se non sono state specificate individualmente in precedenza.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 6..64 caratteri
  Sono consentiti i seguenti caratteri:
  - a..z
  - A..Z
  - 0..9
  - !#$%&'()*+,-./:;<=>?@[\]^_`{}~

La lunghezza minima della password è specificata nel frame *Configuration*. Il dispositivo distingue tra maiuscole e minuscole.

Se la casella di spunta nella colonna *Policy check* è selezionata, il dispositivo verifica la password in base ai criteri specificati nel frame *Password policy*.

Il dispositivo verifica la lunghezza minima della password, anche se la casella di spunta nella colonna *Policy check* è unmarked.

Role

Specifica il ruolo dell'utente che controlla l'accesso dell'utente alle singole funzioni del dispositivo.

Possibili valori:

- *unauthorized*
  L'utente è bloccato e il dispositivo rifiuta l'accesso dell'utente.
  Assegnare questo valore per bloccare temporaneamente l'account utente. Se il dispositivo rileva un errore quando si assegna un altro ruolo, il dispositivo assegna questo ruolo all'account utente.
- *guest* (impostazione di default)
  L'utente è autorizzato a monitorare il dispositivo.
- *auditor*
  L'utente è autorizzato a monitorare il dispositivo e a memorizzare il file di registro nella finestra di dialogo *Diagnostics > Report > Audit Trail*.
- *operator*
  L'utente è autorizzato a monitorare il dispositivo ed a modificare le impostazioni, ad eccezione delle impostazioni di sicurezza per l'accesso al dispositivo.
- *administrator*
  L'utente è autorizzato a monitorare il dispositivo ed a modificare le impostazioni.

Il dispositivo assegna il tipo di servizio trasferito nella risposta di un server RADIUS ad un ruolo utente come seguito indicato:

- Administrative-User: *administrator*
- Login-User: *operator*
- NAS-Prompt-User: *guest*

User locked

Sblocca l'account utente.

Possibili valori:

- selezionato
  L'account utente è bloccato. L'utente non ha accesso alla gestione del dispositivo.
  Se l'utente effettua troppi tentativi di accesso non riusciti, il dispositivo blocca quell'utente.
- non selezionato (in grigio) (impostazione di default)
  L'account utente è sbloccato. L'utente ha accesso alla gestione del dispositivo.

Policy check

Attiva/disattiva la verifica password.

Possibili valori:

- `selezionato`
  La verifica password è attivata.
  Quando si configura o modifica la password, il dispositivo verifica la password in base ai criteri specificati nel frame *Password policy*.
- `non selezionato` (impostazione di default)
  La verifica password è disattivata.

SNMP auth type

Specifica il protocollo di autenticazione che il dispositivo applica per l'accesso utente tramite SNMPv3.

Possibili valori:

- *hmacmd5* (valore di default)
  Per questo account utente, il dispositivo utilizza il protocollo HMACMD5.
- *hmacsha*
  Per questo account utente, il dispositivo utilizza il protocollo HMACSHA.

SNMP auth password

Specifica la password di crittografia che il dispositivo applica per l'accesso utente tramite SNMPv3.

Visualizza ***** (asterischi) invece della password con cui l'utente effettua l'accesso. Per modificare la password, fare clic sul campo rilevante.

Di default, il dispositivo utilizza la stessa password che si specifica nella colonna *Password*.

- Per la colonna attuale il dispositivo consente di specificare una password diversa da quella nella colonna *Password*.
- Se si modifica la password nella colonna *Password*, il dispositivo modifica anche la password per la colonna attuale, ma solo se non è stata specificata individualmente.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 6..64 caratteri
  Sono consentiti i seguenti caratteri:
  - `a..z`
  - `A..Z`
  - `0..9`
  - `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

SNMP encryption type

Specifica il protocollo di crittografia che il dispositivo applica per l'accesso utente tramite SNMPv3.

Possibili valori:

- *none*
  Nessuna crittografia.
- *des* (valore di default)
  Crittografia DES
- *aesCfb128*
  Crittografia AES128

SNMP encryption password

Specifica la password di crittografia che il dispositivo applica per crittografare l'accesso utente tramite SNMPv3.

Visualizza ***** (asterischi) invece della password con cui l'utente effettua l'accesso. Per modificare la password, fare clic sul campo rilevante.

Di default, il dispositivo utilizza la stessa password che si specifica nella colonna *Password*.

- Per la colonna attuale il dispositivo consente di specificare una password diversa da quella nella colonna *Password*.
- Se si modifica la password nella colonna *Password*, il dispositivo modifica anche la password per la colonna attuale, ma solo se non è stata specificata individualmente.

Possibili valori:

▶ Stringa di caratteri ASCII alfanumerici con 6..64 caratteri
Sono consentiti i seguenti caratteri:
– `a..z`
– `A..Z`
– `0..9`
– `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

▶ Nel campo *User name*, si specifica il nome dell'account utente.
Possibili valori:
– Stringa di caratteri ASCII alfanumerici con 1..32 caratteri

3.2 Authentication List

[Device Security > Authentication List]

In questa finestra di dialogo si gestiscono gli elenchi di autenticazione. In un elenco di autenticazione si specifica quale metodo utilizza il dispositivo per l'autenticazione. Inoltre, è possibile assegnare applicazioni predefinite agli elenchi di autenticazione.

Se gli utenti accedono con dati di accesso validi, il dispositivo consente loro di accedere alla gestione del dispositivo. Il dispositivo autentica gli utenti utilizzando i seguenti metodi:
- Gestione utenti del dispositivo
- LDAP
- RADIUS

Attraverso il controllo di accesso basato su porta secondo IEEE 802.1X, se i dispositivi finali connessi accedono con dati di accesso validi, il dispositivo consente loro l'accesso alla rete. Il dispositivo autentica i dispositivi finali utilizzando i seguenti metodi:
- RADIUS
- IAS (server di autenticazione integrato)

Nell'impostazione di default, sono disponibili i seguenti elenchi di autenticazione:
- `defaultDot1x8021AuthList`
- `defaultLoginAuthList`
- `defaultV24AuthList`

Tabella

Nota: Se la tabella non contiene un elenco, l'accesso alla gestione del dispositivo è possibile solo utilizzando la Command Line Interface attraverso l'interfaccia seriale del dispositivo. In questo caso, il dispositivo autentica l'utente utilizzando la gestione utenti locale. Vedere la finestra di dialogo *Device Security > User Management*.

Name

Visualizza il nome dell'elenco.

Per creare un nuovo elenco, fare clic sul pulsante  .

Possibili valori:
- Stringa di caratteri ASCII alfanumerici con 1..32 caratteri

Policy 1
Policy 2
Policy 3
Policy 4
Policy 5

Specifica i criteri d'autenticazione che il dispositivo utilizza per l'accesso, utilizzando l'applicazione specificata nella colonna *Dedicated applications*.

Il dispositivo offre l'opzione di una soluzione fallback. Per questo motivo, si specificano altri criteri in ciascuno dei campi criteri. Se l'autenticazione con i criteri specificati non riesce, il dispositivo può utilizzare il successivo criterio, in funzione dell'ordine dei valori immessi in ogni criterio.

Possibili valori:

- `local` (impostazione di default)
  Il dispositivo autentica gli utenti utilizzando la gestione utenti locale. Vedere la finestra di dialogo *Device Security > User Management*.
  Non è possibile assegnare questo valore all'elenco di autenticazione `defaultDot1x8021AuthList`.
- `radius`
  Il dispositivo autentica gli utenti con un server RADIUS nella rete. Si specifica il server RADIUS nella finestra di dialogo*Network Security > RADIUS > Authentication Server*.
- `reject`
  Il dispositivo accetta o rifiuta l'autenticazione in base a quale criterio si prova per primo. Il seguente elenco contiene gli scenari di autenticazione:
  - Se il primo criterio nell'elenco di autenticazione è `local` e il dispositivo accetta le credenziali di accesso dell'utente, l'accesso dell'utente avviene senza provare altri criteri.
  - Se il primo criterio nell'elenco di autenticazione è `local` e il dispositivo nega le credenziali di accesso dell'utente, l'accesso dell'utente avviene provando gli altri criteri nell'ordine specificato.
  - Se il primo criterio nell'elenco di autenticazione è `radius` o `ldap` e il dispositivo rifiuta un accesso, l'accesso è rifiutato immediatamente senza tentatare di effettuare altri accessi dell'utente con un altro criterio.
    Se non si riceve alcuna risposta dal server RADIUS o LDAP, il dispositivo tenta di autenticare l'utente con il criterio successivo.
  - Se il primo criterio nell'elenco di autenticazione è `reject`, i dispositivi rifiutano immediatamente l'accesso utente senza tentativi con un altro criterio.
  - Verificare che l'elenco di autenticazione `defaultV24AuthList` contenga almeno un criterio diverso da `reject`.
- `ias`
  Il dispositivo autentica i dispositivi finali attraverso l'accesso via 802.1X con il server di autenticazione integrato (IAS). Il server di autenticazione integrato gestisce i dati di accesso in un database separato. Vedere la finestra di dialogo *Network Security > 802.1X Port Authentication > Integrated Authentication Server*.
  È possibile assegnare questo valore solo all'elenco di autenticazione `defaultDot1x8021AuthList`.
- `ldap`
  Il dispositivo autentica gli utenti con i dati di autenticazione e il ruolo di accesso salvati in una posizione centrale. Si specifica il server Active Directory che il dispositivo utilizza nella finestra di dialogo *Network Security > LDAP > Configuration*.

Dedicated applications

Visualizza le applicazioni dedicate. Quando gli utenti accedono al dispositivo con l'applicazione rilevante, il dispositivo utilizza i criteri specificati per l'autenticazione.

Per assegnare un'altra applicazione all'elenco oppure rimuovere l'assegnazione, fare clic sul pulsante ☰ e poi la voce *Allocate applications*. Il dispositivo consente l'assegnazione di ogni applicazione ad un preciso elenco.

Active

Attiva/disattiva l'elenco.

Possibili valori:

- `selezionato`
  L'elenco è attivato. Il dispositivo utilizza i criteri di questo elenco quando gli utenti accedono al dispositivo con l'applicazione rilevante.
- `non selezionato` (impostazione di default)
  L'elenco è disattivato.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Allocate applications

Apre la finestra *Allocate applications*.

- Il campo a sinistra visualizza le applicazioni che possono essere assegnate all'elenco evidenziato.
- Il campo a destra visualizza le applicazioni che sono assegnate all'elenco evidenziato.
- Pulsanti:
  - Sposta ogni voce nel campo destro.
  - Sposta le voci evidenziate dal campo sinistro al campo destro.
  - Sposta le voci evidenziate dal campo destro al campo sinistro.
  - Sposta ogni voce nel campo sinistro.

Nota: Quando si sposta la voce `WebInterface` nel campo di sinistra, si perde la connessione al dispositivo dopo aver fatto clic sul pulsante *Ok*.

3.3 LDAP

[Device Security > LDAP]

Il Lightweight Directory Access Protocol (LDAP) consente l'autenticazione e l'autorizzazine degli utenti da un punto centrale della rete. Un servizio di directory ampiamente utilizzato accessibile attraverso LDAP è Active Directory ®.

Il dispositivo inoltra i dati di accesso dell'utente al server di autenticazione utilizzando il protocollo LDAP. Il server di autenticazione decide se i dati di accesso sono validi e trasferisce le autorizzazioni dell'utente al dispositivo.

In caso di accesso riuscito, il dispositivo salva temporaneamente i dati di accesso nella cache. In questo modo, al successivo accesso dell'utente il processo sarà più rapido. In questo caso non è necessaria un'operazione di ricerca LDAP complessa.

Il menu include le seguenti finestre di dialogo:

- LDAP Configuration
- LDAP Role Mapping

3.3.1 LDAP Configuration

[Device Security > LDAP > Configuration]

Questa finestra di dialogo consente di specificare fino a 4 server di autenticazione. Un server di autenticazione autentica e autorizza gli utenti quando il dispositivo inoltra i dati di accesso al server.

Il dispositivo invia i dati di accesso al primo server di autenticazione. Se questo server non risponde, il dispositivo contatta il server successivo nella tabella.

Operation

Operation

Abilita/disabilita il client *LDAP*.

Se nella finestra di dialogo *Device Security > Authentication List* si specifica il valore `ldap` in una delle righe da *Policy 1* a *Policy 5*, il dispositivo utilizza il client *LDAP*. Prima di questo passaggio, specificare nella finestra di dialogo *Device Security > LDAP > Role Mapping* almeno una mappatura per questo ruolo *administrator*. In questo modo si accede al dispositivo come amministratore in seguito all'accesso tramite LDAP.

Possibili valori:

- *On*
  Il client *LDAP* è abilitato.
- *Off* (impostazione di default)
  Il client *LDAP* è disabilitato.

Configuration

Client cache timeout [min]

Specifica per quanti minuti dopo l'accesso riuscito restano validi i dati di accesso di un utente. Se un utente accede nuovamente entro questo intervallo di tempo, non è necessaria un'operazione di ricerca LDAP complessa. Il processo di accesso è molto più rapido.

Possibili valori:

- `1..1440` (impostazione di default: `10`)

Bind user

Specifica l'ID utente sotto forma del "Distinguished Name" (DN) con cui il dispositivo accede al server LDAP.

Questa informazione è necessaria se il server LDAP richiede un ID utente sotto forma di "Distinguished Name" (DN) per l'accesso. Negli ambienti Active Directory questa informazione non è necessaria.

Il dispositivo accede al server LDAP con l'ID utente per trovare il "Distinguished Name" (DN) per gli utenti che effettuano l'accesso. Il dispositivo esegue la ricerca in base alle impostazioni nei campi *Base DN* e *User name attribute*.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0 .. 64 caratteri

Bind user password

Specifica la password che il dispositivo utilizza con l'ID utente specificato nel campo *Bind user* quando si esegue l'accesso al server LDAP.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0 .. 64 caratteri

Base DN

Specifica il momento in cui si avvia la ricerca nell'albero della directory sotto forma di "Distinguished Name" (DN).

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

User name attribute

Specifica l'attributo LDAP che contiene un nome utente biunivoco. In seguito, l'utente esegue l'accesso utilizzando il nome utente contenuto in questo attributo.

Spesso gli attributi LDAP `userPrincipalName`, `mail`, `sAMAccountName` e `uid` contengono un nome utente unico.

Il dispositivo aggiunge al nome utente la stringa di caratteri specificata nel campo *Default domain* alla seguente condizione:

- Il nome utente contenuto nell'attributo non contiene il carattere @.
- Nel campo *Default domain* è specificato un nome del dominio.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0 .. 64 caratteri
  (Impostazione di default: `userPrincipalName`)

Default domain

Specifica la stringa di caratteri che il dispositivo aggiunge al nome utente dell'utente che esegue l'accesso se il nome utente non contiene il carattere @.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0 .. 64 caratteri

CA certificate

URL

Specifica il percorso e il nome file del certificato.

Il dispositivo accetta i certificati con le seguenti proprietà:

- Formato X.509
- Estensione nome file `.PEM`
- Codifica Base64, compreso tra
  `-----BEGIN CERTIFICATE-----`
  e
  `-----END CERTIFICATE-----`

Per motivi di sicurezza si raccomanda di utilizzare regolarmente un certificato firmato da un'autorità di certificazione.

Il dispositivo rende disponibili le seguenti opzioni per la copia del certificato nel dispositivo:

- Importazione dal PC
  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.
- Importazione da un server FTP
  Se il certificato si trova su un server TFTP, specificare l'URL per il file nella seguente forma:
  `ftp://<Utente>:<Password>@<Indirizzo IP>:<Porta>/<Percorso>/<Nome file>`
- Importazione da un server TFTP
  Se il certificato si trova su un server TFTP, specificare l'URL per il file nella seguente forma:
  `tftp://<Indirizzo IP>/<Percorso>/<Nome file>`
- Importazione da un server SCP o SFTP
  Se la chiave si trova su un server SCP o SFTP, specificare l'URL per il file nella seguente forma:
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`
    Facendo clic sul pulsante *Start*, il dispositivo visualizza la finestra *Credentials*. Qui si inseriscono *User name* e *Password* per accedere al server.
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`

Start

Copia il certificato specificato nel campo *URL* sul dispositivo.

Tabella

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Description

Specifica la descrizione.

Qui è possibile descrivere il server di autenticazione oppure annotare informazioni aggiuntive.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Address

Specifica l'indirizzo IP o il nome DNS del server.

Possibili valori:

- Indirizzo IPv4 (impostazione di default: `0.0.0.0`)
- Indirizzo IPv6
- Nome DNS nel formato `<domain>.<tld>` o `<host>.<domain>.<tld>`
- `_ldap._tcp.<domain>.<tld>`
  Utilizzando questo nome DNS, il dispositivo interroga l'elenco dei server LDAP (record di risorse SRV) dal server DNS.

Se nella riga *Connection security* è specificato un valore diverso da *none* e il certificato contiene solamente nomi DNS del server, si utilizza un nome DNS. Abilita la funzione *Client* nella finestra di dialogo *Advanced > DNS > Client > Global*.

Destination TCP port

Specifica la Porta TCP sulla quale il server prevede le richieste.

Il dispositivo ignora questo valore se nella colonna *Address* è specificato il valore `_ldap._tcp.domain.tld`.

Possibili valori:

- `0..65535` (impostazione di default: `389`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Porte TCP usate di frequente:

- `LDAP: 389`
- `LDAP over SSL: 636`
- `Active Directory Global Catalogue: 3268`
- `Active Directory Global Catalogue SSL: 3269`

Connection security

Specifica il protocollo che crittografa la comunicazione tra il dispositivo e il server di autenticazione.

Possibili valori:

- *none*
  Nessuna crittografia.
  Il dispositivo stabilisce una connessione LDAP al server e trasmette la comunicazione comprese le password in testo non crittografato.

- *ssl*
  Crittografia con SSL.
  Il dispositivo stabilisce una connessione TLS al server e tramite tunnel trasmette la comunicazione LDAP.
- *startTLS* (impostazione di default)
  Crittografia con estensione startTLS.
  Il dispositivo stabilisce una connessione LDAP al server e crittografa la connessione.

Il prerequisito per la comunicazione crittografata è che il dispositivo utilizzi l'orario corretto. Se il certificato contiene solamente i nomi DNS, specificare il nome DNS del server nella riga *Address*. Abilita la funzione *Client* nella finestra di dialogo *Advanced > DNS > Client > Global*.

Se il certificato contiene l'indirizzo IP del server nel campo "Subject Alternative Name" il dispositivo è in grado di verificare l'identità del server senza configurazione DNS.

Server status

Visualizza lo stato della connessione e l'autenticazione con il server di autenticazione.

Possibili valori:

- *ok*
  Il server è raggiungibile.
  Se nella riga *Connection security* è specificato un valore diverso da *none*, il dispositivo ha verficato il certificato del server.
- *unreachable*
  Il server non è raggiungibile.
- *other*
  Il dispositivo non ha ancora stabilito una connessione al server.

Active

Attiva/disattiva l'utilizzo del server.

Possibili valori:

- selezionato
  Il dispositivo utilizza il server.
- non selezionato (impostazione di default)
  Il dispositivo non utilizza il server.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Flush cache

Rimuove i dati di accesso memorizzati nella cache relativi agli utenti che hanno eseguito l'accesso correttamente.

3.3.2 LDAP Role Mapping

[Device Security > LDAP > Role Mapping]

Questa finestra di dialogo consente di creare fino a 64 mappature per assegnare un ruolo agli utenti.

Nella tabella specificare se il dispositivo assegna un ruolo all'utente sulla base di un attributo con un valore specifico o del gruppo di appartenenza.
- Il dispositivo cerca gli attributi e il valore dell'attributo nell'oggetto utente.
- Valutando il “Distinguished Name” (DN) contenuto negli attributi del membro, le verifiche del dispositivo raggruppano l'appartenenza.

Quando un utente esegue l'accesso il dispositivo cerca le seguenti informazioni sul server LDAP.
- Nel progetto utente correlato, il dispositivo cerca gli attributi specificati nelle mappature.
- Negli oggetti gruppo dei gruppi specificati nelle mappature, il dispositivo cerca gli attributi del membro.

Il dispositivo verifica eventuali mappature su questa base.
- L'oggetto utente contiene l'attributo richiesto?
  oppure
- L'utente appartiene al gruppo?

Se il dispositivo non trova una corrispondenza, l'utente non ottiene l'accesso al dispositivo.

Se il dispositivo trova più di una mappatura applicabile a un utente, la decisione è presa dall'impostazione nel campo *Matching policy*. L'utente ottiene il ruolo con autorizzazioni più estese oppure il primo ruolo applicabile nella tabella.

Configuration

Matching policy

Specifica quale ruolo applica il dispositivo se a un utente si applica più di una mappatura.

Possibili valori:
- `highest` (impostazione di default)
  Il dispositivo applica il ruolo con le autorizzazioni più estese.
- `first`
  Il dispositivo applica all'utente la regola con il valore inferiore nella colonna *Index*.

Tabella

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Role

Specifica il ruolo dell'utente che controlla l'accesso dell'utente alle singole funzioni del dispositivo.

Possibili valori:

- `unauthorized`
  L'utente è bloccato e il dispositivo rifiuta l'accesso dell'utente.
  Assegnare questo valore per bloccare temporaneamente l'account utente. Se viene rilevato un errore durante l'assegnazione di un altro ruolo, il dispositivo assegna questo ruolo all'account utente.
- `guest` (impostazione di default)
  L'utente è autorizzato a monitorare il dispositivo.
- `auditor`
  L'utente è autorizzato a monitorare il dispositivo e a memorizzare il file di registro nella finestra di dialogo *Diagnostics > Report > Audit Trail*.
- `operator`
  L'utente è autorizzato a monitorare il dispositivo ed a modificare le impostazioni, ad eccezione delle impostazioni di sicurezza per l'accesso al dispositivo.
- `administrator`
  L'utente è autorizzato a monitorare il dispositivo ed a modificare le impostazioni.

Type

Specifica se un gruppo o un attributo con un valore attributo è configurato nella colonna *Parameter*.

Possibili valori:

- `attribute` (impostazione di default)
  La colonna *Parameter* contiene un attributo con un valore attributo.
- `group`
  La colonna *Parameter* contiene il "Distinguished Name" (DN) di un gruppo.

Parameter

Specifica un gruppo o un attributo con un valore attributo, in base alle impostazioni nella colonna *Type*.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri
  Il dispositivo distingue tra maiuscole e minuscole.
  - Se nella colonna *Type* è specificato il valore `attribute`, si specifica l'attributo sotto forma di `Attribute_name=Attribute_value`.
    Esempio: `l=Germany`
  - Se nella colonna *Type* è specificato il valore `group`, si specifica il "Distinguished Name" (DN) di un gruppo.
    Esempio: `CN=admin-users,OU=Groups,DC=example,DC=com`

Active

Attiva/disattiva la mappatura dei ruoli.

Possibili valori:

- `selezionato` (impostazione di default)
  La mappatura dei ruoli è attiva.
- `non selezionato`
  La mappatura dei ruoli non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

- Nel campo *Index*, si specifica il numero indice.
  Possibili valori:
  - `1..64`

3.4 Management Access

[Device Security > Management Access]

Il menu include le seguenti finestre di dialogo:

- Server
- IP Access Restriction
- Web
- Command Line Interface
- SNMPv1/v2 Community

3.4.1 Server

[Device Security > Management Access > Server]

Questa finestra di dialogo consente la configurazione dei servizi server che abilitano gli utenti o le applicazioni ad accedere alla gestione del dispositivo.

Questa finestra di dialogo include le seguenti schede:
- [Information]
- [SNMP]
- [Telnet]
- [SSH]
- [HTTP]
- [HTTPS]

[Information]

Questa scheda visualizza in una panoramica quali servizi server sono attivati.

Tabella

SNMPv1

Visualizza se è attivo o non attivo il servizio server che autorizza l'accesso al dispositivo, utilizzando Versione SNMP 1. Vedere la scheda *SNMP*.

Possibili valori:
- `selezionato`
  Il servizio server è attivo.
- `non selezionato`
  Il servizio server non è attivo.

SNMPv2

Visualizza se è attivo o non attivo il servizio server che autorizza l'accesso al dispositivo, utilizzando Versione SNMP 2. Vedere la scheda *SNMP*.

Possibili valori:
- `selezionato`
  Il servizio server è attivo.
- `non selezionato`
  Il servizio server non è attivo.

SNMPv3

Visualizza se è attivo o non attivo il servizio server che autorizza l'accesso al dispositivo, utilizzando Versione SNMP 3. Vedere la scheda *SNMP*.

Possibili valori:

- `selezionato`
  Il servizio server è attivo.
- `non selezionato`
  Il servizio server non è attivo.

Telnet server

Visualizza se è attivo o non attivo il servizio server che autorizza l'accesso al dispositivo, utilizzando Telnet. Vedere la scheda *Telnet*.

Possibili valori:

- `selezionato`
  Il servizio server è attivo.
- `non selezionato`
  Il servizio server non è attivo.

SSH server

Visualizza se è attivo o non attivo il servizio server che autorizza l'accesso al dispositivo, utilizzando Secure Shell. Vedere la scheda *SSH*.

Possibili valori:

- `selezionato`
  Il servizio server è attivo.
- `non selezionato`
  Il servizio server non è attivo.

HTTP server

Visualizza se è attivo o non attivo il servizio server che autorizza l'accesso al dispositivo, utilizzando l'interfaccia grafica utente utilizzando HTTP. Vedere la scheda *HTTP*.

Possibili valori:

- `selezionato`
  Il servizio server è attivo.
- `non selezionato`
  Il servizio server non è attivo.

HTTPS server

Visualizza se è attivo o non attivo il servizio server che autorizza l'accesso al dispositivo, utilizzando l'interfaccia grafica utente utilizzando HTTPS. Vedere la scheda *HTTPS*.

Possibili valori:

- `selezionato`
  Il servizio server è attivo.
- `non selezionato`
  Il servizio server non è attivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[SNMP]

Questa scheda consente di specificare le impostazioni per l'agente SNMP del dispositivo e per attivare/disattivare l'accesso al dispositivo con diverse versioni SNMP.

L'agente SNMP consente l'accesso alla gestione del dispositivo con applicazioni basate su SNMP.

Configuration

SNMPv1

Attiva/disattiva l'accesso al dispositivo con versione SNMP 1.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato.
- `non selezionato`
  L'accesso è disattivato.

Si specificano i nomi community nella finestra di dialogo *Device Security > Management Access >* SNMPv1/v2 Community.

SNMPv2

Attiva/disattiva l'accesso al dispositivo con versione SNMP 2.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato.
- `non selezionato`
  L'accesso è disattivato.

Si specificano i nomi community nella finestra di dialogo *Device Security > Management Access >* SNMPv1/v2 Community.

SNMPv3

Attiva/disattiva l'accesso al dispositivo con versione SNMP 3.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato.
- `non selezionato`
  L'accesso è disattivato.

Sistemi per la gestione delle reti come ConneXium Network Manager utilizzano questo protocollo per comunicare con il dispositivo.

UDP port

Specifica il numero della porta UDP sulla quale l'agente SNMP riceve le richieste dai client.

Possibili valori:

- `1..65535` (impostazione di default: `161`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Per attivare l'agente SNMP all'uso della nuova porta dopo una modifica, procedere come di seguito illustrato:

- ☐ Fare clic sul pulsante ☑.
- ☐ Nella finestra di dialogo *Basic Settings > Load/Save*, selezionare il profilo di configurazione attivo.
- ☐ Fare clic sul pulsante 💾 per salvare le attuali modifiche.
- ☐ Riavviare il dispositivo.

SNMPover802

Attiva/disattiva l'accesso al dispositivo tramite SNMP via IEEE-802.

Possibili valori:

- `selezionato`
  L'accesso è attivato.
- `non selezionato` (impostazione di default)
  L'accesso è disattivato.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Telnet]

Questa scheda consente di attivare/disattivare il server Telnet nel dispositivo e di specificarne le impostazioni.

Il server Telnet consente di accedere alla gestione del dispositivo in remoto attraverso la Command Line Interface. Le connessioni Telnet non sono crittografate.

Operation

Telnet server

Attiva/disattiva il server Telnet.

Possibili valori:

- il server Telnet è attivato.
  L'accesso alla gestione del dispositivo è possibile attraverso la Command Line Interface, utilizzando una connessione Telnet non crittografata.
- Il server Telnet è disattivato.

Nota: Se il server *SSH* è disabilitato e si disabilita anche il server *Telnet*, l'accesso alla Command Line Interface è possibile solo attraverso l'interfaccia seriale del dispositivo.

Configuration

TCP port

Specifica il numero della porta TCP sulla quale il dispositivo riceve le richieste Telnet dai client.

Possibili valori:

- `1..65535` (impostazione di default: `23`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Il server si riavvia automaticamente dopo che la porta è modificata. Le connessioni esistenti rimangono attive.

Connections

Visualizza quante connessioni Telnet sono attualmente stabilite con il dispositivo.

Connections (max.)

Specifica il numero massimo di connessioni Telnet al dispositivo che possono essere configurate simultaneamente.

Possibili valori:

- `1..5` (impostazione di default: `5`)

Session timeout [min]

Specifica il timeout in minuti. Dopo che non è stato attivo per questo periodo di tempo, il dispositivo termina la sessione per l'utente registrato.

Una modifica del valore diventa efficace all'accesso successivo dell'utente.

Possibili valori:

- `0`
  Disattiva la funzione. La connessione viene mantenuta in caso di inattività.
- `1..160` (impostazione di default: `5`)

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[SSH]

Questa scheda consente di attivare/disattivare il server SSH nel dispositivo e di specificare le impostazioni necessarie per SSH. Il server funziona con la versione SSH 2.

Il server SSH consente l'accesso alla gestione del dispositivo in remoto attraverso la Command Line Interface. Le connessioni SSH sono crittografate.

Il server SSH si identifica con i client utilizzando la chiave RSA pubblica. Quando si configura per la prima volta la connessione, il programma client mostra all'utente l'impronta digitale della chiave. L'impronta digitale contiene una sequenza di caratteri con codifica Base64 che è semplice da verificare. Quando si rende disponibile questa sequenza di caratteri agli utenti attraverso un canale affidabile, gli utenti hanno l'opzione di confrontare entrambi le impronte digitali. Se le sequenze di caratteri corrispondono, il client è connesso al server corretto.

Il dispositivo consente di creare direttamente nel dispositivo le chiavi private e pubbliche (chiavi host) necessarie per RSA. Altrimenti, è possibile copiare la propria chiave host sul dispositivo in formato PEM.

In alternativa, il dispositivo consente di caricare la chiave RSA (chiave host) da una memoria esterna al riavvio. Si attiva questa funzione nella finestra di dialogo *Basic Settings > External Memory*, colonna *SSH key auto upload*.

Operation

SSH server

Attiva/disattiva il server SSH.

Possibili valori:

- `On` (impostazione di default)
  il server SSH è attivato.
  L'accesso alla gestione del dispositivo è possibile attraverso la Command Line Interface, utilizzando una connessione SSH crittografata.
  È possibile avviare il server solo se è presente una firma RSA nel dispositivo.
- `Off`
  il server SSH è disattivato.
  Quando si disattiva il server SSH, le connessioni esistenti vengono mantenute. Tuttavia, il dispositivo aiuta ad evitare la configurazione di nuove connessioni.

Nota: Se il server *Telnet* è disabilitato e si disabilita anche il server *SSH*, l'accesso alla Command Line Interface è possibile solo attraverso l'interfaccia seriale del dispositivo.

Configuration

TCP port

Specifica il numero della porta TCP sulla quale il dispositivo riceve le richieste SSH dai client.

Possibili valori:

- `1..65535` (impostazione di default: `22`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Il server si riavvia automaticamente dopo che la porta è modificata. Le connessioni esistenti rimangono attive.

Sessions

Visualizza quante connessioni SSH sono attualmente stabilite con il dispositivo.

Sessions (max.)

Specifica il numero massimo di connessioni SSH al dispositivo che possono essere configurate simultaneamente.

Possibili valori:

- `1..5` (impostazione di default: `5`)

Session timeout [min]

Specifica il timeout in minuti. Dopo che l'utente registrato non è stato attivo per questo periodo di tempo, il dispositivo termina la connessione.

Una modifica del valore diventa efficace all'accesso successivo dell'utente.

Possibili valori:

- `0`
  Disattiva la funzione. La connessione viene mantenuta in caso di inattività.
- `1..160` (impostazione di default: `5`)

Fingerprint

L'impronta digitale è una stringa semplice da verificare che identifica in modo univoco la chiave host del server SSH.

Dopo aver importato una nuova chiave host, il dispositivo continua a visualizzare l'impronta digitale esistente finché si riavvia il server.

Fingerprint type

Specifica quale impronta digitale visualizza il campo *RSA fingerprint*.

Possibili valori:

- `md5`
  Il campo *RSA fingerprint* visualizza l'impronta digitale come funzione di hash esadecimale MD5.
- `sha256`
  Il campo *RSA fingerprint* visualizza l'impronta digitale come funzione di hash SHA256 codificata con Base64.

RSA fingerprint

Visualizza l'impronta digitale della chiave host pubblica del server SSH.

Quando si modificano le impostazioni nel campo *Fingerprint type*, subito dopo fare clic sul pulsante e poi sul pulsante per aggiornare la visualizzazione.

Signature

RSA present

Visualizza se una chiave host RSA è presente nel dispositivo.

Possibili valori:

- `selezionato`
  È presente una chiave.
- `non selezionato`
  Nessuna chiave presente.

Create

Genera una chiave host nel dispositivo. Il prerequisito è che il server *SSH* sia disattivato.

Lunghezza della chiave creata:

- 2048 bit (RSA)

Riattivare il server SSH affinché il server SSH utilizzi la chiave host generata.

In alternativa, è possibile copiare la propria chiave host sul dispositivo in formato PEM. Vedere il frame *Key import*.

Delete

Rimuove la chiave host dal dispositivo. Il prerequisito è che il server SSH sia disattivato.

Oper status

Visualizza se il dispositivo sta attualmente generando una chiave host.

È possibile che un altro utente abbia eseguito questa azione.

Possibili valori:

- *rsa*
  Il dispositivo sta attualmente generando una chiave host RSA.
- *none*
  Il dispositivo non genera una chiave host.

Key import

URL

Specifica il percorso e il nome file della propria chiave host RSA.

Il dispositivo accetta la chiave RSA se ha la seguente lunghezza:

- 2048 bit (RSA)

Il dispositivo rende disponibili le seguenti opzioni per la copia della chiave nel dispositivo:

- Importazione dal PC
  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.
- Importazione da un server FTP
  Se la chiave si trova su un server FTP, specificare l'URL per il file nella seguente forma:
  `ftp://<Utente>:<Password>@<Indirizzo IP>:<Porta>/<Nome file>`
- Importazione da un server TFTP
  Se la chiave si trova su un server TFTP, specificare l'URL per il file nella seguente forma:
  `tftp://<Indirizzo IP>/<Percorso>/<Nome file>`
- Importazione da un server SCP o SFTP
  Se la chiave si trova su un server SCP o SFTP, specificare l'URL per il file nella seguente forma:
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`
    Facendo clic sul pulsante *Start*, il dispositivo visualizza la finestra *Credentials*. Qui si inseriscono *User name* e *Password* per accedere al server.
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`

Start

Copia la chiave specificata nel campo *URL* sul dispositivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[HTTP]

Questa scheda consente di attivare/disattivare il protocollo HTTP per il server Web e di specificare le impostazioni necessarie per HTTP.

Il server Web fornisce l'interfaccia grafica utente attraverso una connessione HTTP non crittografata. Per ragioni di sicurezza, disattivare il protocollo HTTP e utilizzare invece il protocollo HTTPS.

Il dispositivo supporta fino a 10 connessioni simultanee utilizzando HTTP o HTTPS.

Nota: In questa scheda è possibile modificare le impostazioni e fare clic sul pulsante ✓, quindi il dispositivo termina la sessione e disconnette ogni connessione aperta. Per continuare a lavorare con l'interfaccia grafica utente, effettuare nuovamente l'accesso.

Operation

HTTP server

Attiva/disattiva il protocollo *HTTP* per il server Web.

Possibili valori:

- *On* (impostazione di default)
  Il protocollo*HTTP* è attivato.
  L'accesso alla gestione del dispositivo è possibile attraverso una connessione *HTTP* non crittografata.
  Se anche il protocollo *HTTPS* è attivato, il dispositivo reindirizza automaticamente la richiesta per una connessione *HTTP* ad una connessione *HTTPS* crittografata.
- *Off*
  Il protocollo *HTTP* è disattivato.
  Quando il protocollo *HTTPS* è abilitato, l'accesso alla gestione del dispositivo è possibile attraverso una connessione *HTTPS* crittografata.

Nota: Se i protocolli *HTTP* e *HTTPS* sono disabilitati, è possibile abilitare il protocollo *HTTP* utilizzando il comando Command Line Interface `http server` per accedere all'interfaccia grafica utente.

Configuration

TCP port

Specifica il numero della porta TCP sulla quale il server Web riceve le richieste HTTP dai client.

Possibili valori:

- `1..65535` (impostazione di default: `80`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[HTTPS]

Questa scheda consente di attivare/disattivare il protocollo HTTP per il server Web e di specificare le impostazioni necessarie per HTTPS.

Il server web fornisce l'interfaccia grafica utente attraverso una connessione HTTP crittografata.

È necessario un certificato digitale per la crittografia della connessione HTTP. Il dispositivo consente di creare in autonomia questo certificato oppure caricare un certificato esistente sul dispositivo.

Il dispositivo supporta fino a 10 connessioni simultanee utilizzando HTTP o HTTPS.

Nota: In questa scheda è possibile modificare le impostazioni e fare clic sul pulsante ✓, quindi il dispositivo termina la sessione e disconnette ogni connessione aperta. Per continuare a lavorare con l'interfaccia grafica utente, effettuare nuovamente l'accesso.

Operation

HTTPS server

Attiva/disattiva il protocollo *HTTPS* per il server Web.

Possibili valori:

- *On* (impostazione di default)
  Il protocollo*HTTPS* è attivato.
  L'accesso alla gestione del dispositivo è possibile attraverso una connessione *HTTPS* crittografata.
  Se non è presente certificato digitale, il dispositivo genera un certificato digitale prima di attivare il protocollo *HTTPS*.
- *Off*
  Il protocollo *HTTPS* è disattivato.
  Quando il protocollo *HTTP* è disabilitato, l'accesso alla gestione del dispositivo è possibile attraverso una connessione *HTTP* non crittografata.

Nota: Se i protocolli *HTTP* e *HTTPS* sono disabilitati, è possibile abilitare il protocollo *HTTPS* utilizzando il comando Command Line Interface `https server` per accedere all'interfaccia grafica utente.

Configuration

TCP port

Specifica il numero della porta TCP sulla quale il server Web riceve le richieste HTTPS dai client.

Possibili valori:

- `1..65535` (impostazione di default: `443`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Fingerprint

L'impronta digitale è una sequenza di numeri esadecimali verificabile in modo semplice che identifica univocamente il certificato digitale del server HTTPS.

Dopo aver importato un nuovo certificato digitale, il dispositivo visualizza l'attuale impronta digitale finché si riavvia il server.

Fingerprint type

Specifica quale impronta digitale visualizza il campo *Fingerprint*.

Possibili valori:

- *sha1*
  Il campo *Fingerprint* visualizza l'impronta digitale SHA1 del certificato.
- *sha256*
  Il campo *Fingerprint* visualizza l'impronta digitale SHA256 del certificato.

Fingerprint

Sequenza di caratteri del certificato digitale utilizzato dal server.

Quando si modificano le impostazioni nel campo *Fingerprint type*, subito dopo fare clic sul pulsante e poi sul pulsante per aggiornare la visualizzazione.

Certificate

Nota: Se il dispositivo utilizza un certificato non firmato da un'autorità di certificazione, il browser web visualizza un messaggio durante il caricamento dell'interfaccia grafica utente. Per continuare, aggiungere una regola di eccezione per il certificato nel browser Web.

Present

Visualizza se il certificato digitale è presente nel dispositivo.

Possibili valori:

- selezionato
  Il certificato è presente.
- non selezionato
  Il certificato è stato rimosso.

Create

Genera un certificato digitale nel dispositivo.

Fino al riavvio, il server Web utilizza il certificato precedente.

Riavviare il server Web affinché il server Web utilizzi il nuovo certificato generato. Il riavvio del server web è possibile solo attraverso la Command Line Interface.

In alternativa, è possibile copiare il proprio certificato sul dispositivo. Vedere il frame *Certificate import*.

Delete

Elimina il certificato digitale.

Fino al riavvio, il server Web utilizza il certificato precedente.

Oper status

Visualizza se il dispositivo sta attualmente generando o eliminando un certificato digitale.

È possibile che un altro utente abbia eseguito l'azione.

Possibili valori:

- *none*
  Il dispositivo non sta attualmente generando o eliminando un certificato.
- *delete*
  Il dispositivo sta attualmente eliminando un certificato.
- *generate*
  Il dispositivo sta attualmente generando un certificato.

Certificate import

URL

Specifica il percorso e il nome file del certificato.

Il dispositivo accetta i certificati con le seguenti proprietà:

- Formato X.509
- Estensione nome file `.PEM`
- Codifica Base64, compreso tra
  - `-----BEGIN PRIVATE KEY-----`
    e
    `-----END PRIVATE KEY-----`
    e anche tra
  - `-----BEGIN CERTIFICATE-----`
    e
    `-----END CERTIFICATE-----`
- Chiave RSA con lunghezza 2048 bit

Il dispositivo rende disponibili le seguenti opzioni per la copia del certificato nel dispositivo:

- Importazione dal PC
  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.
- Importazione da un server FTP
  Se il certificato si trova su un server TFTP, specificare l'URL per il file nella seguente forma:
  `ftp://<Utente>:<Password>@<Indirizzo IP>:<Porta>/<Percorso>/<Nome file>`
- Importazione da un server TFTP
  Se il certificato si trova su un server TFTP, specificare l'URL per il file nella seguente forma:
  `tftp://<Indirizzo IP>/<Percorso>/<Nome file>`
- Importazione da un server SCP o SFTP
  Se la chiave si trova su un server SCP o SFTP, specificare l'URL per il file nella seguente forma:
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`
    Facendo clic sul pulsante *Start*, il dispositivo visualizza la finestra *Credentials*. Qui si inseriscono *User name* e *Password* per accedere al server.
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`

Start

Copia il certificato specificato nel campo *URL* sul dispositivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

3.4.2 IP Access Restriction

[Device Security > Management Access > IP Access Restriction]

Questa finestra di dialogo consente di limitare l'accesso alla gestione del dispositivo a intervalli di indirizzi IP specifici e a selezionate applicazioni basate su IP.

- Se la funzione è disabilitata, l'accesso alla gestione del dispositivo è possibile da qualsiasi indirizzo IP e utilizzando ogni applicazione.
- Se la funzione è attivata, l'accesso è ristretto. L'accesso alla gestione dispositivo è consentito solo alle seguenti condizioni:
  - Almeno una voce della tabella è attivata.
    e
  - L'accesso al dispositivo avviene con un'applicazione consentita da un intervallo di indirizzi IP autorizzato.

Operation

Nota: Prima di attivare la 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.

Operation

Abilita/disabilita la funzione *IP Access Restriction*.

Possibili valori:

- `On`
  È abilitata la funzione *IP Access Restriction*.
  L'accesso alla gestione del dispositivo è limitato.
- `Off` (impostazione di default)
  È disabilitata la funzione *IP Access Restriction*.

Tabella

È possibile definire fino a 16 voci di tabella e attivarle separatamente.

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Quando si elimina una voce della tabella rimane un buco nella numerazione. Quando si crea una nuova voce della tabella, il dispositivo riempie il primo buco.

Possibili valori:

- `1..16`

Address

Specifica l'indirizzo IP della rete da cui si consente l'accesso alla gestione del dispositivo. Specificare l'intervallo di rete nella colonna *Netmask*.

Possibili valori:

- Indirizzo IPv4 valido (impostazione di default: `0.0.0.0`)

Netmask

Specifica l'intervallo della rete indicato nella colonna *Address*.

Possibili valori:

- Netmask valida (impostazione di default: `0.0.0.0`)

HTTP

Attiva/disattiva l'accesso HTTP.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato per l'intervallo di indirizzi IP adiacente.
- `non selezionato`
  L'accesso è disattivato.

HTTPS

Attiva/disattiva l'accesso HTTPS.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato per l'intervallo di indirizzi IP adiacente.
- `non selezionato`
  L'accesso è disattivato.

SNMP

Attiva/disattiva l'accesso SNMP.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato per l'intervallo di indirizzi IP adiacente.
- `non selezionato`
  L'accesso è disattivato.

Telnet

Attiva/disattiva l'accesso Telnet.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato per l'intervallo di indirizzi IP adiacente.
- `non selezionato`
  L'accesso è disattivato.

SSH

Attiva/disattiva l'accesso SSH.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato per l'intervallo di indirizzi IP adiacente.
- `non selezionato`
  L'accesso è disattivato.

IEC61850-MMS

Attiva/disattiva l'accesso al MMS server.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato per l'intervallo di indirizzi IP adiacente.
- `non selezionato`
  L'accesso è disattivato.

Modbus TCP

Attiva/disattiva l'accesso al server *Modbus TCP*.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato per l'intervallo di indirizzi IP adiacente.
- `non selezionato`
  L'accesso è disattivato.

EtherNet/IP

Attiva/disattiva l'accesso al server *EtherNet/IP*.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso è attivato per l'intervallo di indirizzi IP adiacente.
- `non selezionato`
  L'accesso è disattivato.

Active

Attiva/disattiva la voce della tabella.

Possibili valori:

- `selezionato` (impostazione di default)
  La voce della tabella è attivata. Il dispositivo limita l'accesso alla gestione del dispositivo all'intervallo di indirizzi IP adiacente e alle applicazioni basate su IP selezionate.
- `non selezionato`
  La voce della tabella è disattivata.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

3.4.3 Web

[Device Security > Management Access > Web]

In questa finestra di dialogo, si specificano le impostazioni per l'interfaccia grafica utente.

Configuration

Web interface session timeout [min]

Specifica il timeout in minuti. Dopo che non è stato attivo per questo periodo di tempo, il dispositivo termina la sessione per l'utente registrato.

Possibili valori:

- `0..160` (impostazione di default: `5`)

Attraverso il valore `0` si disattiva la funzione e l'utente rimane registrato quando non attivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

3.4.4 Command Line Interface

[Device Security > Management Access > CLI]

In questa finestra di dialogo, si specificano le impostazioni per la Command Line Interface. Informazioni dettagliate in merito alla Command Line Interface sono riportate nel manuale di riferimento “Command Line Interface”.

Questa finestra di dialogo include le seguenti schede:
- [Global]
- [Login banner]

[Global]

Questa scheda consente di modificare la richiesta nella Command Line Interface e di specificare la chiusura automatica di sessioni attraverso l'interfaccia seriale in caso di inattività.

Il dispositivo ha le seguenti interfacce seriali.
- Interfaccia USB-C

Configuration

Login prompt

Specifica la stringa di caratteri visualizzata dal dispositivo nella Command Line Interface all'avvio di ogni riga di comando.

Possibili valori:
- Stringa di caratteri ASCII con 0 .. 128 caratteri (`0x20..0x7E`) inclusi i caratteri spazio
  Caratteri jolly
  - `%d` Data
  - `%i` Indirizzo IP
  - `%m` Indirizzo MAC
  - `%p` Nome del prodotto
  - `%t` Orario

  Impostazione di default: `(MCSESM-E)`

Le modifiche a questa impostazione hanno efficacia immediata nella sessione della Command Line Interface attiva.

Serial interface timeout [min]

Specifica l'orario in minuto dopo il quale il dispositivo chiude automaticamente la sessione di un utente inattivo con accesso effettuato nell'interfaccia a riga di comando (CLI).

Possibili valori:
- `0..160` (impostazione di default: `5`)
  Attraverso il valore `0` si disattiva la funzione e l'utente rimane registrato quando non attivo.

Una modifica del valore diventa efficace all'accesso successivo dell'utente.

Per il server *Telnet* e il server *SSH*, si specifica il timeout nella finestra di dialogo *Device Security* > Management Access > *Server*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Login banner]

In questa scheda si sostituisce la schermata iniziale della Command Line Interface con un proprio testo.

Nell'impostazione di default, la schermata iniziale visualizza le informazioni sul dispositivo, quali la versione software e le impostazioni dispositivo. Attraverso la funzione in questa scheda, si disattivano queste informazioni e si sostituiscono con un testo personalizzato.

Per visualizzare il proprio testo nella Command Line Interface e nell'interfaccia grafica utente prima di accedere si utilizza la finestra di dialogo *Device Security* > *Pre-login Banner*.

Operation

Operation

Abilita/disabilita la funzione *Login banner*.

Possibili valori:

- `On`
  È abilitata la funzione *Login banner*.
  Il dispositivo visualizza le informazioni di testo specificate nel campo *Banner text* per gli utenti che accedono al dispositivo con la Command Line Interface.
- `Off` (impostazione di default)
  È disabilitata la funzione *Login banner*.
  La schermata iniziale visualizza le informazioni sul dispositivo. Le informazioni di testo nel campo *Banner text* vengono mantenute.

Banner text

Banner text

Specifica la stringa di caratteri che il dispositivo visualizza nell'interfaccia a riga di comando all'avvio di ogni sessione.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..1024 caratteri (`0x20..0x7E`) inclusi i caratteri spazio

- `<Scheda>`
- `<Interruzione di riga>`

Remaining characters

Visualizza quanti caratteri rimangono nel campo *Banner text* per le informazioni di testo.

Possibili valori:

- `1024..0`

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

3.4.5 SNMPv1/v2 Community

[Device Security > Management Access > SNMPv1/v2 Community]

In questa finestra di dialogo si specifica il nome della community per applicazioni SNMPv1/v2.

Le applicazioni inviano richieste tramite SNMPv1/v2 con un nome comunità nell'header pacchetto dati SNMP. In base al nome della community, l'applicazione ottiene l'autorizzazione in lettura o l'autorizzazione in lettura e scritta per il dispositivo.

Si attiva l'accesso al dispositivo tramite SNMPv1/v2 nella finestra di dialogo *Device Security > Management Access > Server*.

Tabella

Community

Visualizza l'autorizzazione per applicazioni SNMPv1/v2 al dispositivo:

- `Write`
  Per richieste con il nome della community immesso, l'applicazione riceve l'autorizzazione in lettura e scrittura per il dispositivo.
- `Read`
  Per richieste con il nome della community immesso, l'applicazione riceve l'autorizzazione in lettura per il dispositivo.

Name

Specifica il nome della community per l'autorizzazione adiacente.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..32 caratteri
  `admin` (impostazione di default per autorizzazioni in lettura e scrittura)
  `user` (impostazione di default per autorizzazioni in lettura)

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

3.5 Pre-login Banner

[Device Security > Pre-login Banner]

Questa finestra di dialogo consente la visualizzazione di un saluto o di un testo informativo per gli utenti prima che effettuino l'accesso.

Gli utenti visualizzano questo testo nella finestra di dialogo di accesso dell'interfaccia grafica utente e della Command Line Interface. Gli utenti che effettuano l'accesso con SSH visualizzano il testo prima o durante l'accesso, indipendentemente dal client utilizzato.

Per visualizzare solo il testo nella Command Line Interface, utilizzare le impostazioni nella finestra di dialogo *Device Security > Management Access > CLI*.

Operation

Operation

Abilita/disabilita la funzione *Pre-login Banner*.

Utilizzando la funzione *Pre-login Banner*, il dispositivo visualizza un saluto o un testo informativo nella finestra di dialogo di accesso dell'interfaccia grafica utente e dell'interfaccia a riga di comando.

Possibili valori:

- *On*
  È abilitata la funzione *Pre-login Banner*.
  Il dispositivo visualizza il testo specificato nel campo *Banner text* nella finestra di dialogo di accesso.
- *Off* (impostazione di default)
  È disabilitata la funzione *Pre-login Banner*.
  Il dispositivo non visualizza un testo nella finestra di dialogo di accesso. Se si inserisce un testo nel campo *Banner text*, questo testo viene memorizzato nel dispositivo.

Banner text

Banner text

Specifica il testo informativo che il dispositivo visualizza nella finestra di dialogo di accesso dell'interfaccia grafica utente e della Command Line Interface.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..512 caratteri (`0x20..0x7E`) inclusi i caratteri spazio
- `<Scheda>`
- `<Interruzione di riga>`

Remaining characters

Visualizza quanti caratteri rimangono nel campo *Banner text*.

Possibili valori:

- 512..0

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4 Network Security

Il menu include le seguenti finestre di dialogo:

- Network Security Overview
- Port Security
- 802.1X Port Authentication
- RADIUS
- DoS
- DHCP Snooping
- IP Source Guard
- Dynamic ARP Inspection
- ACL

4.1 Network Security Overview

[Network Security > Overview]

Questa finestra di dialogo visualizza le regole di sicurezza della rete utilizzate nel dispositivo.

Parametro

Port/VLAN

Specifica se il dispositivo visualizza regole basate su VLAN e/o su porta.

Possibili valori:

- `All` (impostazione di default)
  Il dispositivo visualizza le regole basate su VLAN e su porta specificate dall'utente.
- `Porta: <Numero di porta>`
  Il dispositivo visualizza regole basate su porta per una porta specifica. Questa selezione è disponibile se l'utente ha specificato una o più regole per questa porta.
- `VLAN: <ID VLAN>`
  Il dispositivo visualizza regole basate su VLAN per una VLAN specifica. Questa selezione è disponibile se l'utente ha specificato una o più regole per questa VLAN.

ACL

Visualizza le regole *ACL* nella panoramica.

Nella finestra di dialogo *Network Security > ACL* si modificano le regole *ACL*.

All

Seleziona le caselle di spunta vicine. Il dispositivo visualizza le regole correlate nella panoramica.

None

Deseleziona le caselle di spunta vicine. Il dispositivo non visualizza regole nella panoramica.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.2 Port Security

[Network Security > Port Security]

Il dispositivo consente solo di trasmettere pacchetti dati dal mittente desiderato su una porta. Se questa funzione è attivata, il dispositivo verifica il VLAN-ID e l'indirizzo MAC o il VLAN-ID e l'indirizzo IP del mittente prima della trasmissione di un pacchetto dati. Il dispositivo scarta i pacchetti dati di altri mittenti e registra questo evento.

Il dispositivo offre inoltre la funzione di verifica dell'indirizzo IP del mittente prima della trasmissione di un pacchetto dati.

Nota: Se nel frame *Mode* è selezionato il pulsante di opzione *IP*, la funzione *Port Security* opera indirettamente sul Layer 2. Quando si configura un indirizzo IP consentito, il dispositivo recupera l'indirizzo MAC attualmente associato con l'indirizzo IP. Il dispositivo utilizza una richiesta ARP e salva internamente l'indirizzo MAC associato. Il prerequisito per specificare un indirizzo IP consentito è che il dispositivo collegato sia raggiungibile e risponda alle richieste ARP.

Se un dispositivo collegato invia pacchetti dati con un indirizzo IP consentito ma con un indirizzo MAC diverso da quello associato, il dispositivo rifiuta i relativi pacchetti dati. Se si sostituisce il dispositivo collegato e si utilizza lo stesso indirizzo IP utilizzato in precedenza, specificare nuovamente l'indirizzo IP come consentito. In seguito a questo passaggio il dispositivo utilizza il nuovo indirizzo MAC associato.

Se la funzione *Auto-Disable* è attivata, il dispositivo disattiva la porta. Questa restrizione rende gli attacchi di spoofing MAC più difficili. La funzione *Auto-Disable* attiva nuovamente in automatico la porta rilevante se non si superano più i parametri.

In questa finestra di dialogo, una finestra *Wizard* aiuta l'utente a connettere le porte con una o più fonti desiderate. Nel dispositivo, questi indirizzi sono noti come *Static entries (x/y)*. Per visualizzare gli indirizzi statici specificati, evidenziare la porta rilevante e fare clic sul pulsante  .

Per semplificare il processo di configurazione, il dispositivo consente la registrazione automatica dei mittenti desiderati. Il dispositivo “apprende” i mittenti valutando i pacchetti dati ricevuti. Nel dispositivo, questi indirizzi sono noti come *Dynamic entries*. Se si raggiunge un limite superiore definito dall'utente (*Dynamic limit*), il dispositivo arresta “l'apprendimento” sulla porta rilevante e trasmette solo i pacchetti dati dei mittenti già registrati. Adattando il limite superiore al numero di mittenti previsti si rendono più difficili gli attacchi di flooding MAC.

Nota: Attraverso la registrazione automatica delle *Dynamic entries*, il dispositivo scarta sempre il 1° pacchetto dati da mittenti sconosciuti. Utilizzando il 1° pacchetto dati, il dispositivo verifica il raggiungimento del limite superiore. Il dispositivo registra il mittente finché si raggiunge il limite superiore. Poi, il dispositivo trasmette pacchetti dati che riceve sulla porta rilevante da questo mittente.

Operation

Operation

Abilita/disabilita la funzione *Port Security*.

Possibili valori:

- `On`
  È abilitata la funzione *Port Security*.
  Il dispositivo verifica l'ID VLAN e l'indirizzo MAC sorgente prima della trasmissione di un pacchetto dati.
  Il dispositivo trasmette un pacchetto dati ricevuto solo se l'ID VLAN e l'indirizzo MAC sorgente del pacchetto dati sono consentiti sulla porta corrispondente. Per rendere efficace questa impostazione, attivare anche la verifica dell'indirizzo sorgente sulle porte coinvolte.
- `Off` (impostazione di default)
  È disabilitata la funzione *Port Security*.
  Il dispositivo trasmette ogni pacchetto dati ricevuto senza verificare l'indirizzo sorgente.

Nota: Se nel frame *Mode* è selezionato il pulsante di opzione *MAC*, il dispositivo confronta l'indirizzo MAC sorgente con gli indirizzi MAC sorgente consentiti. Se il pulsante di opzione *IP* è selezionato, il dispositivo confronta l'indirizzo MAC sorgente con gli indirizzi MAC associati agli indirizzi IP sorgente consentiti.

Configuration

Auto-disable

Attiva/disattiva la funzione *Auto-Disable* per *Port Security*.

Possibili valori:

- `selezionato`
  La funzione *Auto-Disable* per *Port Security* è attiva.
  Selezionare anche la casella di spunta nella colonna *Auto-disable* per le porte rilevanti.
- `non selezionato` (impostazione di default)
  La funzione *Auto-Disable* per *Port Security* non è attiva.

Mode

Mode

Specifica se la funzione *Port Security* utilizza gli indirizzi MAC consentiti o gli indirizzi IP consentiti per verificare un pacchetto ricevuto.

Possibili valori:

- *MAC* (Impostazione di default)
  La funzione *Port Security* utilizza gli indirizzi MAC sorgente consentiti.
  Il dispositivo confronta l'ID VLAN e l'indirizzo MAC sorgente con gli indirizzi MAC sorgente consentiti prima della trasmissione di un pacchetto dati.
- *IP*
  La funzione *Port Security* utilizza gli indirizzi IP sorgente consentiti.
  Il dispositivo confronta l'ID VLAN e l'indirizzo MAC sorgente con gli indirizzi MAC sorgente associati agli indirizzi IP sorgente consentiti prima della trasmissione di un pacchetto dati.

Tabella

Port

Visualizza il numero di porta.

Active

Attiva/disattiva la verifica dell'indirizzo sorgente sulla porta.

Possibili valori:

- `selezionato`
  Il dispositivo verifica ogni pacchetto dati ricevuto sulla porta e lo trasmette solo se l'indirizzo sorgente del pacchetto dati è consentito. Abilitare anche la funzione *Port Security* nel frame *Operation*.
- `non selezionato` (impostazione di default)
  Il dispositivo trasmette ogni pacchetto dati ricevuto sulla porta senza verificare l'indirizzo sorgente.

Nota: Se si utilizza il dispositivo come partecipante attivo all'interno di un *MRP* Ring o di *HIPER Ring*, si raccomanda di deselezionare la casella di spunta per le Ring port.

Nota: Se si utilizza il dispositivo come partecipante attivo di un *Ring/Network Coupling* o *RCP*, si raccomanda di deselezionare la casella di spunta per le porte di collegamento coinvolte.

Auto-disable

Attiva/disattiva la funzione *Auto-Disable* per i parametri che la funzione *Port Security* monitora sulla porta.

Possibili valori:

- `selezionato` (impostazione di default)
  La funzione *Auto-Disable* è attiva sulla porta.
  Il prerequisito è quello di selezionare la casella di spunta *Auto-disable* nel frame *Configuration*.
  - Se la porta registra gli indirizzi MAC sorgente che non sono consentiti o più indirizzi MAC rispetto a quelli specificati nella colonna *Dynamic limit*, il dispositivo disattiva la porta. Il LED “Stato del link” per la porta lampeggia 3 volte per periodo.
  - La finestra di dialogo *Diagnostics > Ports > Auto-Disable* visualizza quali porte sono attualmente disabilitate a causa del superamento dei parametri.
  - La funzione *Auto-Disable* riattiva automaticamente la porta. Per fare ciò, nella finestra di dialogo *Diagnostics > Ports > Auto-Disable*, si specifica un periodo di attesa per la porta interessata nella colonna *Reset timer [s]*.
- `non selezionato`
  La funzione *Auto-Disable* sulla porta non è attiva.

Send trap

Attiva/disattiva l'invio di trap SNMP se il dispositivo rifiuta un pacchetto dati da un mittente indesiderato sulla porta.

Possibili valori:

- `selezionato`
  L'invio di trap SNMP è attivo.
  Se il dispositivo scarta i pacchetti dati da un mittente non consentito sulla porta, il dispositivo invia un trap SNMP.
- `non selezionato` (impostazione di default)
  L'invio di trap SNMP non è attivo.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Trap interval [s]

Specifica il tempo di ritardo in secondi per il quale il dispositivo attende dopo l'invio di un trap SNMP prima dell'invio del successivo trap SNMP.

Possibili valori:

- `0..3600` (impostazione di default: `0`)

Il valore `0` disattiva il tempo di ritardo.

Dynamic limit

Specifica il limite superiore per il numero di fonti registrate automaticamente (*Dynamic entries*). Raggiunto il limite superiore, il dispositivo smette di “apprendere” su questa porta.

Adattare il valore al numero di fonti previsti.

Se la porta registra più mittenti rispetto a quelli qui specificati, la porta disattiva la funzione *Auto-Disable*. Il prerequisito è quello di selezionare la casella di spunta nella colonna *Auto-disable* e la casella di spunta *Auto-disable* nel frame *Configuration*.

Possibili valori:

- `0`
  Disattiva la registrazione automatica delle fonti su questa porta.
- `1..600` (impostazione di default: `600`)

Static limit

Specifica il limite superiore per il numero di fonti connesse alla porta (*Static entries (x/y)*). La finestra *Wizard*, finestra di dialogo *MAC addresses*, aiuta l'utente a collegare la porta con una o più fonti desiderate.

Possibili valori:

- `0..64` (impostazione di default: `64`)

Il valore `0` aiuta ad evitare che l'utente connetta una fonte alla porta.

Dynamic entries

Visualizza il numero di mittenti che il dispositivo ha stabilito automaticamente.

Vedere la finestra *Wizard*, finestra di dialogo *MAC addresses*, campo *Dynamic entries*.

Se si seleziona il valore *IP* nel frame *Mode*, la colonna *Dynamic entries* mostra il valore `0`.

Static MAC entries

Visualizza il numero di mittenti collegati alla porta.

Vedere la finestra *Wizard*, finestra di dialogo *MAC addresses*, campo *Static entries (x/y)*.

Static IP entries

Mostra il numero di indirizzi IP consentiti sulla porta.

Vedere la finestra *Wizard*, finestra di dialogo *IP addresses*, campo *Static entries (x/y)*.

Last violating VLAN ID/MAC

Visualizza il VLAN-ID e l'indirizzo MAC di un mittente indesiderato i cui pacchetti dati sono stati scartati per ultimi dal dispositivo su questa porta.

Sent traps

Visualizza il numero di pacchetti dati scartati su questa porta che hanno determinato l'invio di un trap SNMP da parte del dispositivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Port security (Wizard)]

La finestra *Wizard* aiuta l'utente a connettere le porte con una o più fonti desiderate. Dopo aver specificato le impostazioni, fare clic sul pulsante *Finish*.

Nota: Il dispositivo salva le fonti connesse con la porta finché si disattiva il controllo sorgente sulla porta rilevante o nel frame *Operation*.

Dopo aver chiuso la finestra *Wizard*, fare clic sul pulsante per salvare le impostazioni.

[Port security (Wizard) – Select port]

Port

Specifica la porta che si assegna al mittente nella fase successiva.

[Port security (Wizard) – MAC addresses]

VLAN ID

Specifica l'ID VLAN sorgente fonte desiderata.

Possibili valori:

- `1..4042`

Per trasferire il VLAN-ID e l'indirizzo MAC al campo *Static entries (x/y)*, fare clic sul pulsante *Add*.

MAC address

Specifica l'indirizzo MAC sorgente desiderata.

Possibili valori:

- Indirizzo MAC unicast valido
  Specificare il valore separato dai due punti, per esempio `00:11:22:33:44:55`.

Per trasferire il VLAN-ID e l'indirizzo MAC al campo *Static entries (x/y)*, fare clic sul pulsante *Add*.

Add

Trasferisce i valori specificati nei campi *VLAN ID* e *MAC address* al campo *Static entries (x/y)*.

Static entries (x/y)

Visualizza il VLAN-ID e l'indirizzo MAC dei mittenti desiderati connessi con la porta.

Il dispositivo utilizza questo campo per visualizzare il numero di mittenti connessi alla porta e il limite superiore. Specificare il limite superiore per il numero di voci in tabella, campo *Static limit*.

Nota: Non è possibile assegnare un indirizzo MAC assegnato a questa porta ad una qualsiasi altra porta.

Remove

Rimuove le voci evidenziate nel campo *Static entries (x/y)*.

Sposta le voci evidenziate nel campo *Dynamic entries* al campo *Static entries (x/y)*.

Sposta ogni voce dal campo *Dynamic entries* al campo *Static entries (x/y)*.

Se il campo *Dynamic entries* contiene più voci di quelle consentite nel campo *Static entries (x/y)*, il dispositivo sposta le prime voci fino a raggiungere il limite superiore.

Dynamic entries

Visualizza in ordine ascendente il VLAN-ID e l'indirizzo MAC dei mittenti registrati automaticamente su questa porta. Il dispositivo trasmette pacchetti dati da questi mittenti quando riceve i pacchetti dati su questa porta.

I prerequisiti affinché il dispositivo visualizzi gli indirizzi MAC sono:

- È abilitata la funzione *Port Security*. Vedere il frame *Operation*.
- Il dispositivo verifica tutti i pacchetti dati ricevuti sulla porta. La casella di spunta nella colonna *Active* è selezionata.

Specificare il limite superiore per il numero di voci in tabella, campo *Dynamic limit*.

I pulsanti  e  consentono il trasferimento di voci da questo campo al campo *Static entries (x/y)*. In questo modo si connettono i mittenti rilevanti alla porta.

[Port security (Wizard) – IP addresses]

VLAN ID

Specifica l'ID VLAN sorgente fonte desiderata.

Possibili valori:

▶ `1..4042`

Nota: Assegnare il VLAN-ID della VLAN di gestione.

Per trasferire il *VLAN ID* e il *IP address* al campo *Static entries (x/y)*, fare clic sul pulsante *Add*.

IP address

Specifica l'indirizzo IP sorgente desiderata.

Possibili valori:

▶ Indirizzo IPv4 valido

Per trasferire il *VLAN ID* e il *IP address* al campo *Static entries (x/y)*, fare clic sul pulsante *Add*.

Add

Trasferisce i valori specificati nei campi *VLAN ID* e *IP address* al campo *Static entries (x/y)*.

Static entries (x/y)

Visualizza il VLAN-ID e l'indirizzo IP dei mittenti desiderati connessi con la porta.

Il dispositivo utilizza questo campo per visualizzare il numero di mittenti connessi alla porta e il limite superiore. È possibile specificare un numero massimo di `10` indirizzi IP.

Remove

Rimuove le voci evidenziate nel campo *Static entries (x/y)*.

4.3 802.1X Port Authentication

[Network Security > 802.1X Port Authentication]

Attraverso il controllo di accesso basato su porta secondo IEEE 802.1X, il dispositivo monitora l'accesso alla rete dai dispositivi finali connessi. Il dispositivo (autenticatore) consente ad un dispositivo finale (supplicant) l'accesso alla rete se accede con dati di accesso validi. L'autenticatore e i dispositivi finali comunicano tramite il protocollo di autenticazione EAPOL (Extensible Authentication Protocol over LAN).

Il dispositivo supporta i seguenti metodi di autenticazione dei dispositivi finali:

- `radius`
  Un server RADIUS nella rete autentica i dispositivi finali.
- `ias`
  Il server di autenticazione integrato (IAS) implementato nel dispositivo autentica i dispositivi finali. Rispetto a RADIUS, IAS offre solo funzioni di base.

Il menu include le seguenti finestre di dialogo:

- 802.1X Global
- 802.1X Port Configuration
- 802.1X Port Clients
- 802.1X EAPOL Port Statistics
- 802.1X Port Authentication History
- 802.1X Integrated Authentication Server

4.3.1 802.1X Global

[Network Security > 802.1X Port Authentication > Global]

Attraverso questa finestra di dialogo si specificano le impostazioni di base per il controllo di accesso basato su porta.

Operation

Operation

Abilita/disabilita la funzione *802.1X Port Authentication*.

Possibili valori:

- `On`
  È abilitata la funzione *802.1X Port Authentication*.
  Il dispositivo verifica l'accesso alla rete da dispositivi finali connessi.
  Il controllo di accesso basato su porta è attivato.
- `Off` (impostazione di default)
  È disabilitata la funzione *802.1X Port Authentication*.
  Il controllo di accesso basato su porta è disattivato.

Configuration

VLAN assignment

Attiva/disattiva l'assegnazione della porta rilevante ad una VLAN. Grazie a questa funzione si forniscono servizi selezionati al dispositivo finale connesso in questa VLAN.

Possibili valori:

- `selezionato`
  L'assegnazione è attiva.
  Se il dispositivo finale completa la sua autenticazione, il dispositivo assegna alla porta rilevante il VLAN-ID trasferito dal server di autenticazione RADIUS.
- `non selezionato` (impostazione di default)
  L'assegnazione non è attiva.
  La porta rilevante è assegnata alla VLAN specificata nella finestra di dialogo *Network Security* > 802.1X Port Authentication > *Port Configuration*, riga *Assigned VLAN ID*.

Dynamic VLAN creation

Attiva/disattiva la creazione automatica della VLAN assegnata dal server di autenticazione RADIUS se la VLAN non esiste.

Possibili valori:

- `selezionato`
  La creazione automatica della VLAN è attiva.
  Il dispositivo crea la VLAN se non esiste.
- `non selezionato` (impostazione di default)
  La creazione automatica della VLAN non è attiva.
  Se la VLAN assegnata non esiste, la porta rimane assegnata alla VLAN originale.

Monitor mode

Attiva/disattiva la modalità Controllo.

Possibili valori:

- `selezionato`
  La modalità Controllo è attiva.
  Il dispositivo monitora l'autenticazione e aiuta nella diagnosi degli errori riconosciuti. Se un dispositivo finale non ha completato correttamente l'accesso, il dispositivo consente al dispositivo finale la rete.
- `non selezionato` (impostazione di default)
  La modalità Controllo non è attiva.

MAC authentication bypass format options

Group size

Specifica le dimensioni del gruppo di indirizzi MAC. Il dispositivo divide l'indirizzo MAC per l'autenticazione in gruppi. Le dimensioni dei gruppi sono specificate in mezzi byte, ciascuno dei quali è rappresentato da un carattere.

Possibili valori:

- *1*
  Il dispositivo divide l'indirizzo MAC in 12 gruppi da un carattere.
  Esempio: `A:A:B:B:C:C:D:D:E:E:F:F`
- *2*
  Il dispositivo divide l'indirizzo MAC in 6 gruppi da 2 caratteri.
  Esempio: `AA:BB:CC:DD:EE:FF`
- *4*
  Il dispositivo divide l'indirizzo MAC in 3 gruppi da 4 caratteri.
  Esempio: `AABB:CCDD:EEFF`
- *12* (impostazione di default)
  Il dispositivo formatta l'indirizzo MAC come un gruppo di 12 caratteri.
  Esempio: `AABBCCDDEEFF`

Group separator

Specifica il carattere che separa i gruppi.

Possibili valori:

- *-*
  trattino
- *:*
  due punti
- *.*
  punto

Upper or lower case

Specifica se il dispositivo formatta i dati di autenticazione in lettere minuscole o maiuscole.

Possibili valori:

- *lower-case*
- *upper-case*

Password

Specifica la password opzionale per i client che utilizzano il bypass di autenticazione.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0 .. 64 caratteri
  Dopo l'inserimento, il campo mostra ***** (asterisco) invece della password.
- <vuoto>
  Il dispositivo utilizza il nome utente del client anche come password.

Information

Monitor mode clients

Visuali a quanti dispositivi finali il dispositivo ha consentito accesso alla rete anche senza completamento corretto dell'accesso.

Il prerequisito è quello di attivare la funzione *Monitor mode*. Vedere il frame *Configuration*.

Non monitor mode clients

Visualizza il numero di dispositivi finali ai quali il dispositivo ha consentito accesso alle rete dopo il completamento dell'accesso.

Policy 1

Visualizza il metodo che il dispositivo attualmente utilizza per autenticare i dispositivi finali tramite IEEE 802.1X.

Specificare il metodo utilizzato nella finestra di dialogo *Device Security > Authentication List*.

- ☐ Per autenticare i dispositivi finali attraverso un server RADIUS, si assegna la policy `radius` all'elenco `8021x`.
- ☐ Per autenticare i dispositivi finali attraverso il server di autenticazione integrato (IAS), si assegna la policy `ias` all'elenco `8021x`.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.3.2 802.1X Port Configuration

[Network Security > 802.1X Port Authentication > Port Configuration]

Attraverso questa finestra di dialogo si specificano le impostazioni di accesso per ogni porta.

Quando più dispositivi finali sono connessi a una porta, il dispositivo ne consente l'autenticazione individualmente (autenticazione multi-client). In tal caso, il dispositivo consente ai dispositivi finali collegati di accedere alla rete. In caso contrario, il dispositivo blocca l'accesso ai dispositivi finali non autenticati, o ai dispositivi finali la cui autenticazione è scaduta.

Tabella

Port

Visualizza il numero di porta.

Port initialization

Attiva/disattiva l'inizializzazione della porta per attivare il controllo di accesso sulla porta oppure ripristina il suo stato iniziale. Utilizzare questa funzione solo su porte in cui la colonna *Port control* contiene il valore `auto` o `multiClient`.

Possibili valori:

- `selezionato`
  L'inizializzazione della porta è attiva.
  Quando l'inizializzazione è completa, il dispositivo cambia nuovamente il valore in `non selezionato`.
- `non selezionato` (impostazione di default)
  L'inizializzazione della porta non è attiva.
  Il dispositivo mantiene l'attuale stato della porta.

Port reauthentication

Attiva/disattiva la richiesta unica di ri-autenticazione.

Utilizzare questa funzione solo su porte in cui la colonna *Port control* contiene il valore `auto` o `multiClient`.

Inoltre, il dispositivo consente di richiedere a intervalli regolari al dispositivo finale di effettuare nuovamente l'accesso. Vedere la colonna *Periodic reauthentication*.

Possibili valori:

- `selezionato`
  La richiesta di ri-autenticazione unica è attiva.
  Il dispositivo richiede al dispositivo finale di effettuare nuovamente l'accesso. Dopodiché, il dispositivo cambia nuovamente il valore in `non selezionato`.
- `non selezionato` (impostazione di default)
  La richiesta di ri-autenticazione unica non è attiva.
  Il dispositivo mantiene il dispositivo finale con accesso effettuato.

Authentication activity

Visualizza lo stato attuale dell'autenticatore (`Authenticator PAE state`).

Possibili valori:

- *initialize*
- *disconnected*
- *connecting*
- *authenticating*
- *authenticated*
- *aborting*
- *held*
- *forceAuth*
- *forceUnauth*

Backend authentication state

Visualizza lo stato attuale del link al server di autenticazione (`Backend Authentication state`).

Possibili valori:

- *request*
- *response*
- *success*
- *fail*
- *timeout*
- *idle*
- *initialize*

Authentication state

Visualizza lo stato attuale dell'autenticazione sulla porta (`Controlled Port Status`).

Possibili valori:

- *authorized*
  Il dispositivo finale ha completato l'accesso.
- *unauthorized*
  Il dispositivo finale non ha effettuato l'accesso.

Users (max.)

Specifica il limite superiore per il numero di dispositivi finali che il dispositivo autentica simultaneamente su questa porta. Questo limite superiore si applica solamente a porte in cui la colonna *Port control* contiene il valore `multiClient`.

Possibili valori:

- `1..16` (impostazione di default: `16`)

Port control

Specifica come il dispositivo consente l'accesso alla rete (`Port control mode`).

Possibili valori:

- *`forceUnauthorized`*
  Il dispositivo blocca l'accesso alla rete. Utilizzare questa impostazione se un dispositivo finale è connesso alla porta che non ottiene accesso alla rete.
- *`auto`*
  Il dispositivo consente l'accesso alla rete se il dispositivo finale ha completato l'accesso. Utilizzare questa impostazione se un dispositivo finale è connesso alla porta che effettua l'accesso sull'autenticatore.

Nota: Se altri dispositivi finali sono connessi alla stessa porta, questi ottengono l'accesso alla rete senza ulteriore autenticazione.

- *`forceAuthorized`* (impostazione di default)
  Se i dispositivi finali non supportano IEEE 802.1X, il dispositivo consente l'accesso alla rete. Utilizzare questa impostazione se un dispositivo finale è connesso alla porta che ottiene l'accesso alla rete senza effettuare l'accesso.
- *`multiClient`*
  Il dispositivo garantisce l'accesso alla rete se il dispositivo finale completa l'accesso.
  Se il dispositivo finale non invia alcun pacchetto dati EAPOL, il dispositivo garantisce o nega l'accesso alla rete individualmente a seconda dell'indirizzo MAC del dispositivo finale. Vedere la colonna *MAC authorized bypass*.
  Si utilizza questa impostazione se più dispositivi finali sono connessi alla porta o se la funzione *MAC authorized bypass* è necessaria.

Quiet period [s]

Specifica il periodo di tempo in secondi in cui l'autenticatore non accetta più accessi dal dispositivo finale dopo un tentativo di accesso non riuscito (*Quiet period [s]*).

Possibili valori:

- `0..65535` (impostazione di default: `60`)

Transmit period [s]

Specifica il periodo in secondi trascorso il quale l'autenticatore richiede al dispositivo finale di accedere nuovamente. Terminato il periodo di attesa, il dispositivo invia un pacchetto dati EAP request/identity al dispositivo finale.

Possibili valori:

- `1..65535` (impostazione di default: `30`)

Supplicant timeout period [s]

Specifica il periodo in secondi per il quale l'autenticatore attende che il dispositivo finale effettui l'accesso.

Possibili valori:

- `1..65535` (impostazione di default: `30`)

Server timeout [s]

Specifica il periodo in secondi per il quale l'autenticatore attende la risposta dal server di autenticazione.

Possibili valori:

- `1..65535` (impostazione di default: `30`)

Requests (max.)

Specifica quante volte l'autenticatore richiede al dispositivo finale di accedere finché è scaduto il tempo specificato nella colonna *Supplicant timeout period [s]*. Il dispositivo invia un pacchetto dati EAP request/identity al dispositivo finale il numero di volte qui specificato.

Possibili valori:

- `0..10` (impostazione di default: `2`)

Assigned VLAN ID

Visualizza l'ID della VLAN che l'autenticatore ha assegnato alla porta. Questo valore è relativo solamente a porte in cui la colonna *Port control* contiene il valore `auto`.

Possibili valori:

- `0..4042` (impostazione di default: `0`)

Il VLAN-ID assegnato dall'autenticatore alle porte si trova nella finestra di dialogo *Network Security* > 802.1X Port Authentication > *Port Clients*.

Per le porte in cui la colonna *Port control* contiene il valore `multiClient`, il dispositivo assegna la tag VLAN in base all'indirizzo MAC del dispositivo finale durante la ricezione dei pacchetti dati senza una tag VLAN.

Assignment reason

Visualizza la ragione dell'assegnazione del VLAN-ID. Questo valore è relativo solamente a porte in cui la colonna *Port control* contiene il valore `auto`.

Possibili valori:

- `notAssigned` (impostazione di default)
- `radius`
- `guestVlan`
- `unauthenticatedVlan`

Il VLAN-ID assegnato dall'autenticatore alle porte per un supplicant si trova nella finestra di dialogo *Network Security > 802.1X Port Authentication > Port Clients*.

Reauthentication period [s]

Specifica il periodo in secondi trascorso il quale l'autenticatore richiedea intervalli regolari al dispositivo finale di accedere nuovamente.

Possibili valori:

- `1..65535` (impostazione di default: `3600`)

Periodic reauthentication

Attiva/disattiva le richieste periodiche di ri-autenticazione.

Possibili valori:

- `selezionato`
  Le richieste periodiche di ri-autenticazione sono attive.
  Il dispositivo richiede a intervalli regolari al dispositivo finale di effettuare nuovamente l'accesso. Specificare questo periodo di tempo nella colonna *Reauthentication period [s]*.
  Se l'autenticatore aveva assegnato l'ID di una VLAN voce, di una Unauthenticated VLAN oppure di una Guest VLAN al dispositivo finale, questa impostazione diventa inefficace.
- `non selezionato` (impostazione di default)
  Le richieste periodiche di ri-autenticazione non sono attive.
  Il dispositivo mantiene il dispositivo finale con accesso effettuato.

Guest VLAN ID

Specifica l'ID della VLAN che l'autenticatore assegna alla porta se il dispositivo finale non effettua l'accesso durante il periodo di tempo specificato nella colonna *Guest VLAN period*. Questo valore si applica solamente alle porte in cui la colonna *Port control* contiene il valore `auto` o `multiClient`.

Attraverso questa funzione si consente a dispositivi finali senza supporto IEEE 802.1X l'accesso a selezionati servizi nella rete.

Possibili valori:

- `0` (impostazione di default)
  L'autenticatore non assegna una Guest VLAN alla porta.
  Quando si abilita l'autenticazione basata su MAC nella colonna *MAC authorized bypass*, il dispositivo imposta automaticamente il valore su `0`.
- `1..4042`

Nota: La funzione *MAC authorized bypass* e la funzione *Guest VLAN ID* non si possono utilizzare contemporaneamente.

Guest VLAN period

Specifica il periodo in secondi per il quale l'autenticatore attende i pacchetti dati EAPOL dopo che il dispositivo finale è connesso. Se questo periodo termia, l'autenticatore consente al dispositivo finale l'accesso alla rete e assegna la porta alla Guest VLAN specificata nella colonna *Guest VLAN ID*.

Possibili valori:

- `1..300` (impostazione di default: `90`)

Unauthenticated VLAN ID

Specifica l'ID della VLAN che l'autenticatore assegna alla porta se il dispositivo finale non completa correttamente l'accesso. Questo valore è relativo solamente a porte in cui la colonna *Port control* contiene il valore *`auto`*.

Attraverso questa funzione si consente a dispositivi finali senza dati di accesso validi l'accesso a selezionati servizi nella rete.

Possibili valori:

- `0..4042` (impostazione di default: `0`)

L'effetto del valore `0` è quello che l'autenticatore non assegna una Unauthenticated VLAN alla porta.

Nota: Assegnare alla porta una VLAN configurata staticamente nel dispositivo.

MAC authorized bypass

Attiva/disattiva l'autenticazione basata su MAC.

Questa funzione consente l'autenticazione di dispositivi finali senza supporto IEEE 802.1X sulla base del loro indirizzo MAC.

Possibili valori:

- `selezionato`
  L'autenticazione basata su MAC è attiva.
  Il dispositivo invia l'indirizzo MAC del dispositivo finale al server di autenticazione RADIUS. Il dispositivo assegna il supplicante tramite il suo indirizzo MAC alla VLAN corrispondente come se l'autenticazione fosse eseguita direttamente attraverso IEEE 802.1X.
- `non selezionato` (impostazione di default)
  L'autenticazione basata su MAC non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.3.3 802.1X Port Clients

[Network Security > 802.1X Port Authentication > Port Clients]

Questa finestra di dialogo visualizza informazioni sui dispositivi finali connessi.

Tabella

Port

Visualizza il numero di porta.

User name

Visualizza il nome utente con cui il dispositivo finale ha effettuato l'accesso.

MAC address

Visualizza l'indirizzo MAC del dispositivo finale.

Assigned VLAN ID

Visualizza il VLAN-ID che l'autenticatore assegna alla porta dopo il completamento dell'autenticazione del dispositivo finale.

Se per la porta nella finestra di dialogo *Network Security > 802.1X Port Authentication > Port Configuration*, colonna *Port control*, il valore `multiClient` è specificato, il dispositivo assegna la tag VLAN in base all'indirizzo MAC del dispositivo finale durante la ricezione dei pacchetti dati senza una tag VLAN.

Assignment reason

Visualizza la ragione dell'assegnazione della VLAN.

Possibili valori:

- `default`
- `radius`
- `unauthenticatedVlan`
- `guestVlan`
- `monitorVlan`
- `invalid`

Il campo visualizza solamente un valore valido se il client è autenticato.

Session timeout

Visualizza il tempo rimanente in secondi fino alla scadenza dell'accesso del dispositivo finale. Questo valore si applica solamente se per la porta nella finestra di dialogo *Network Security > 802.1X Port Authentication > Port Configuration*, colonna *Port control*, è specificato il valore `auto` o `multiClient`.

Il server di autenticazione assegna il periodo di timeout al dispositivo tramite RADIUS. Il valore `0` indica che il server di autenticazione non ha assegnato un timeout.

Termination action

Visualizza l'azione eseguita dal dispositivo quando è scaduto l'accesso.

Possibili valori:

- *default*
- *reauthenticate*

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.3.4 802.1X EAPOL Port Statistics

[Network Security > 802.1X Port Authentication > Statistics]

Questa finestra di dialogo visualizza quali pacchetti dati EAPOL ha inviato e ricevuto il dispositivo finale per l'autenticazione dei dispositivi finali.

Tabella

Port

Visualizza il numero di porta.

Received packets

Visualizza il numero di pacchetti dati EAPOL che il dispositivo ha ricevuto sulla porta.

Transmitted packets

Visualizza il numero totale di pacchetti dati EAPOL che il dispositivo ha inviato sulla porta.

Start packets

Visualizza il numero di pacchetti dati di avvio EAPOL che il dispositivo ha ricevuto sulla porta.

Logoff packets

Visualizza il numero di pacchetti dati di fine sessione EAPOL che il dispositivo ha ricevuto sulla porta.

Response/ID packets

Visualizza il numero di pacchetti dati EAP response/identity che il dispositivo ha ricevuto sulla porta.

Response packets

Visualizza il numero di pacchetti dati EAP response che il dispositivo ha ricevuto sulla porta (senza pacchetti dati EAP response/identity).

Request/ID packets

Visualizza il numero di pacchetti dati EAP request/identity che il dispositivo ha ricevuto sulla porta.

Request packets

Visualizza il numero di pacchetti dati EAP request che il dispositivo ha ricevuto sulla porta (senza pacchetti dati EAP request/identity).

Invalid packets

Visualizza il numero di pacchetti dati EAPOL con un tipo di frame sconosciuto che il dispositivo ha ricevuto sulla porta.

Received error packets

Visualizza il numero di pacchetti dati EAPOL con un campo lunghezza del corpo pacchetto non valido che il dispositivo ha ricevuto sulla porta.

Packet version

Visualizza il numero di versione protocollo del pacchetto dati EAPOL che il dispositivo ha ricevuto sulla porta.

Source of last received packet

Visualizza l'indirizzo MAC del mittente dei pacchetti dati EAPOL che il dispositivo ha ricevuto per ultimi sulla porta.

Il valore `00:00:00:00:00:00` indica che la porta non ha ricevuto ancora pacchetti dati EAPOL.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.3.5 802.1X Port Authentication History

[Network Security > 802.1X Port Authentication > Port Authentication History]

Il dispositivo registra il processo di autenticazione dei dispositivi finali che sono connessi alle sue porte. Questa finestra di dialogo visualizza le informazioni registrate durante l'autenticazione.

Tabella

Port

Visualizza il numero di porta.

Authentification time stamp

Visualizza l'orario in cui l'autenticatore ha autenticato il dispositivo finale.

Result age

Visualizza da quando questa voce è stata inserita in tabella.

MAC address

Visualizza l'indirizzo MAC del dispositivo finale.

VLAN ID

Visualizza l'ID della VLAN che è stato assegnato al dispositivo finale prima dell'accesso.

Authentication status

Visualizza lo stato dell'autenticazione sulla porta.

Possibili valori:

- *success*
  L'autenticazione è stata completata.
- *failure*
  L'autenticazione non è riuscita.

Access status

Visualizza se il dispositivo consente al dispositivo finale l'accesso alla rete.

Possibili valori:

- *granted*
  Il dispositivo consente al dispositivo finale l'accesso alla rete.
- *denied*
  Il dispositivo nega al dispositivo finale l'accesso alla rete.

Assigned VLAN ID

Visualizza l'ID della VLAN che l'autenticatore ha assegnato alla porta.

Assignment type

Visualizza il tipo della VLAN che l'autenticatore ha assegnato alla porta.

Possibili valori:

- *default*
- *radius*
- *unauthenticatedVlan*
- *guestVlan*
- *monitorVlan*
- *notAssigned*

Assignment reason

Visualizza la ragione dell'assegnazione del VLAN-ID e del tipo di VLAN.

802.1X Port Authentication History

Port

Semplifica la tabella e visualizza solo le voci relative alla porta selezionata qui. In questo modo è più semplice prendere nota della tabella e ordinarla in base alle esigenze.

Possibili valori:

- `all`
  La tabella visualizza le voci per ogni porta.
- `<Numero di porta>`
  La tabella visualizza le voci che riguardano la porta selezionata qui.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.3.6 802.1X Integrated Authentication Server

[Network Security > 802.1X Port Authentication > Integrated Authentication Server]

Il server di autenticazione integrato (IAS) consente l'autenticazione dei dispositivi finali utilizzando IEEE 802.1X. Rispetto a RADIUS, IAS ha una gamma di funzioni molto limitata. L'autenticazione si basa sullo sul nome utente e sulla password.

In questa finestra di dialogo si gestiscono i dati di accesso dei dispositivi finali. Il dispositivo consente la configurazione di fino a 100 set di dati di accesso.

Per autenticare i dispositivi finali attraverso il server di autenticazione integrato, nella finestra di dialogo *Device Security > Authentication List* si assegna la policy `ias` all'elenco 8021x.

Tabella

User name

Visualizza il nome utente del dispositivo finale.

Per creare un nuovo utente, fare clic sul pulsante .

Password

Specifica la password di autenticazione dell'utente.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0 .. 64 caratteri

Il dispositivo distingue tra maiuscole e minuscole.

Active

Attiva/disattiva i dati di accesso.

Possibili valori:

- `selezionato`
  I dati di accesso sono attivi. Per un dispositivo finale esiste l'opzione di accesso attraverso IEEE 802.1X, utilizzando questi dati di accesso.
- `non selezionato` (impostazione di default)
  I dati di accesso non sono attivi.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.4 RADIUS

[Network Security > RADIUS]

Attraverso queste impostazioni di fornitura, il dispositivo autentica gli utenti sulla base della gestione locale degli utenti. Tuttavia, man mano la rete aumenta le sue dimensioni, diventa più difficile mantenere coerenti i dati di accesso degli utenti su tutti i dispositivi.

RADIUS (Remote Authentication Dial-In User Service) consente l'autenticazione e l'autorizzazione degli utenti da un punto centrale della rete. Un server RADIUS esegue qui le seguenti attività:

- Authentication (autenticazione)
  Il server di autenticazione autentica gli utenti quando il cliente RADIUS nel punto di accesso inoltra i dati di accesso degli utenti al server.
- Authorization (autorizzazione)
  Il server di autenticazione consente agli utenti con accesso effettuato l'autorizzazione per selezionati servizi, assegnando diversi parametri per il dispositivo finale rilevante al client RADIUS nel punto di accesso.
- Accounting
  Il server di accounting registra il traffico dati che si è verificato durante l'autenticazione porta secondo IEEE 802.1X. In questo modo l'utente è abilitato a stabilire successivamente quali servizi gli utenti hanno utilizzato e in quale misura.

Assegnando la policy `radius` ad una applicazione nella finestra di dialogo *Device Security > Authentication List*, il dispositivo funziona con il ruolo del client RADIUS. Il dispositivo inoltra i dati di accesso dell'utente al server di autenticazione primario. Il server di autenticazione decide se i dati di accesso sono validi e trasferisce le autorizzazioni dell'utente al dispositivo.

Come di seguito illustrato, il dispositivo assegna il tipo di servizio trasferito nella risposta di un server RADIUS ad un ruolo utente che esiste nel dispositivo:

- `Administrative-User`: *`administrator`*
- `Login-User`: *`operator`*
- `NAS-Prompt-User`: *`guest`*

Inoltre, il dispositivo consente l'autenticazione di dispositivi finali con IEEE 802.1X attraverso un server di autenticazione. Allo scopo, assegnare la policy `radius` all'elenco `8021x` nella finestra di dialogo *Device Security > Authentication List*.

Il menu include le seguenti finestre di dialogo:

- RADIUS Global
- RADIUS Authentication Server
- RADIUS Accounting Server
- RADIUS Authentication Statistics
- RADIUS Accounting Statistics

4.4.1 RADIUS Global

[Network Security > RADIUS > Global]

Attraverso questa finestra di dialogo si specificano le impostazioni di base per RADIUS.

RADIUS configuration

Retransmits (max.)

Specifica quante volte il dispositivo ritrasmette una richiesta senza risposta al server di autenticazione prima che il dispositivo invii la richiesta ad un altro server di autenticazione.

Possibili valori:

- `1..15` (impostazione di default: `4`)

Timeout [s]

Specifica quanto secondi il dispositivo attende per una risposta dopo una richiesta ad un server di autenticazione prima che ritrasmetta la richiesta.

Possibili valori:

- `1..30` (impostazione di default: `5`)

Accounting

Attiva/disattiva l'accounting.

Possibili valori:

- `selezionato`
  L'accounting è attivo.
  Il dispositivo invia il traffico dati a un server di accounting specificato nella finestra di dialogo *Network Security > RADIUS > Accounting Server*.
- `non selezionato` (impostazione di default)
  L'accounting non è attivo.

NAS IP address (attribute 4)

Specifica l'indirizzo IP che il dispositivo trasferisce al server di autenticazione come attributo 4. Specifica l'indirizzo IP del dispositivo o di un altro indirizzo disponibile.

Nota: Il dispositivo include solo l'attributo 4 se il pacchetto è stato attivato dalla richiesta di autenticazione *802.1X* di un dispositivo finale (supplicant).

Possibili valori:

- Indirizzo IPv4 valido (impostazione di default: `0.0.0.0`)

In molti casi, è presente un firewall tra il dispositivo e il server di autenticazione. Nella Network Address Translation (NAT), il firewall cambia l'indirizzo IP originale e il server di autenticazione riceve l'indirizzo IP tradotto del dispositivo.

Il dispositivo trasferisce l'indirizzo IP invariato in questo campo nell'ambito della Network Address Translation (NAT).

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Cancella i dati statistici nella finestra di dialogo *Network Security > RADIUS > Authentication Statistics* e nella finestra di dialogo *Network Security > RADIUS > Accounting Statistics*.

4.4.2 RADIUS Authentication Server

[Network Security > RADIUS > Authentication Server]

Attraverso questa finestra di dialogo si specificano fino ad 8 server di autenticazione. Un server di autenticazione autentica e autorizza gli utenti quando il dispositivo inoltra i dati di accesso al server.

Il dispositivo invia i dati di accesso al server di autenticazione primario specificato. Se il server non risponde, il dispositivo contatta il server di autenticazione specificato che si trova nella posizione più alta in tabella. Se anche questo server non risponde, il dispositivo contatta il server successivo in tabella.

Tabella

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Name

Visualizza il nome del server.

Per modificare il valore, fare clic sul campo rilevante.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 1..32 caratteri
  (Impostazione di default: `Default-RADIUS-Server`)

Address

Specifica l'indirizzo IP del server.

Possibili valori:

- Indirizzo IPv4 valido

Destination UDP port

Specifica il numero della porta UDP sulla quale il server riceve richieste.

Possibili valori:

- `0..65535` (impostazione di default: `1812`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Secret

Visualizza ****** (asterischi) quando si specifica una password tramite cui il dispositivo accede al server. Per modificare la password, fare clic sul campo rilevante.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 1..64 caratteri

Si riceve la password dall'amministratore del server di autenticazione.

Primary server

Specifica il server di autenticazione come primario o secondario.

Possibili valori:

- `selezionato`
  Il server è specificato come il server di autenticazione primario. Il dispositivo invia i dati di accesso per l'autenticazione degli utenti a questo server di autenticazione.
  Se si attivano più server, il dispositivo specifica l'ultimo server attivato come server di autenticazione primario.
- `non selezionato` (impostazione di default)
  Il server è il server di autenticazione secondario. Se il dispositivo non riceve risposta dal server di autenticazione primario, il dispositivo invia i dati di accesso al server di autenticazione secondario.

Active

Attiva/disattiva il link al server.

Il dispositivo utilizza il server se nella finestra di dialogo *Device Security > Authentication List* si specifica il valore `radius` in una delle righe da *Policy 1* a *Policy 5*.

Possibili valori:

- `selezionato` (impostazione di default)
  Il link è attivo. Il dispositivo invia i dati di accesso per l'autenticazione degli utenti a questo server se le suddette precondizioni sono soddisfatte.
- `non selezionato`
  Il link non è attivo. Il dispositivo non invia dati di accesso a questo server.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

- Nel campo *Index*, si specifica il numero indice.
- Nel campo *Address*, si specifica l'indirizzo IP del server.

4.4.3 RADIUS Accounting Server

[Network Security > RADIUS > Accounting Server]

Attraverso questa finestra di dialogo si specificano fino ad 8 server di accounting. Un server di accounting registra il traffico dati che si è verificato durante l'autenticazione porta secondo IEEE 802.1X. Il prerequisito è quello di attivare nel menu *Network Security > RADIUS > Global* la funzione *Accounting*.

Il dispositivo invia il traffico dati al primo server di accounting raggiungibile. Se il server di accounting non risponde, il dispositivo contatta il server successivo in tabella.

Tabella

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Possibili valori:

- `1..8`

Name

Visualizza il nome del server.

Per modificare il valore, fare clic sul campo rilevante.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 1..32 caratteri
  (Impostazione di default: `Default-RADIUS-Server`)

Address

Specifica l'indirizzo IP del server.

Possibili valori:

- Indirizzo IPv4 valido

Destination UDP port

Specifica il numero della porta UDP sulla quale il server riceve richieste.

Possibili valori:

- `0..65535` (impostazione di default: `1813`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Secret

Visualizza ****** (asterischi) quando si specifica una password tramite cui il dispositivo accede al server. Per modificare la password, fare clic sul campo rilevante.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 1..16 caratteri

Si riceve la password dall'amministratore del server di autenticazione.

Active

Attiva/disattiva il link al server.

Possibili valori:

- `selezionato` (impostazione di default)
  Il link è attivo. Il dispositivo invia il traffico dati a questo server se le suddette precondizioni sono soddisfatte.
- `non selezionato`
  Il link non è attivo. Il dispositivo non invia traffico dati a questo server.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

- Nel campo *Index*, si specifica il numero indice.
- Nel campo *Address*, si specifica l'indirizzo IP del server.

4.4.4 RADIUS Authentication Statistics

[Network Security > RADIUS > Authentication Statistics]

Questa finestra di dialogo visualizza informazioni sulla comunicazione tra il dispositivo e il server di autenticazione. La tabella visualizza le informazioni per ogni server in una riga separata.

Per cancellare i dati statistici, nella finestra di dialogo *Network Security > RADIUS > Global* fare clic sul pulsante ☰ e sulla voce *Reset*.

Tabella

Name

Visualizza il nome del server.

Address

Specifica l'indirizzo IP del server.

Round trip time

Visualizza l'intervallo di tempo in centesimi di secondo tra l'ultima risposta ricevuta dal server (Access Reply/Access Challenge) e il corrispondente pacchetto dati inviato.

Access requests

Visualizza il numero di pacchetti dati di accesso che il dispositivo ha inviato al server. Questo valore non tiene in considerazione le ripetizioni.

Retransmitted access-request packets

Visualizza il numero di pacchetti dati di accesso che il dispositivo ha ritrasmesso al server.

Access accepts

Visualizza il numero di pacchetti dati Access Accept che il dispositivo ha ricevuto dal server.

Access rejects

Visualizza il numero di pacchetti dati Access Reject che il dispositivo ha ricevuto dal server.

Access challenges

Visualizza il numero di pacchetti dati Access Challenge che il dispositivo ha ricevuto dal server.

Malformed access responses

Visualizza il numero di pacchetti dati Access Response malformati che il dispositivo ha ricevuto dal server (inclusi i pacchetti dati con una lunghezza non valida).

Bad authenticators

Visualizza il numero di pacchetti dati Access Response con un autenticatore non valido che il dispositivo ha ricevuto dal server.

Pending requests

Visualizza il numero di pacchetti dati Access Request che il dispositivo ha inviato al server e per i quali non ha ancora ricevuto risposta dal server.

Timeouts

Visualizza quante volte non si è ricevuta risposta dal server prima che scadesse il tempo di attesa specificato.

Unknown types

Visualizza il numero di pacchetti dati con un tipo di dati sconosciuto che il dispositivo ha ricevuto dal server sulla porta di autenticazione.

Packets dropped

Visualizza il numero di pacchetti dati che il dispositivo ha ricevuto dal server sulla porta di autenticazione e poi li ha scartati.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.4.5 RADIUS Accounting Statistics

[Network Security > RADIUS > Accounting Statistics]

Questa finestra di dialogo visualizza informazioni sulla comunicazione tra il dispositivo e il server di accounting. La tabella visualizza le informazioni per ogni server in una riga separata.

Per cancellare i dati statistici, nella finestra di dialogo *Network Security > RADIUS > Global* fare clic sul pulsante ☰ e sulla voce *Reset*.

Tabella

Name

Visualizza il nome del server.

Address

Specifica l'indirizzo IP del server.

Round trip time

Visualizza l'intervallo di tempo in centesimi di secondo tra l'ultima risposta ricevuta dal server (Accounting Response) e il corrispondente pacchetto dati inviato (Accounting Request).

Accounting-request packets

Visualizza il numero di pacchetti dati Accounting Request che il dispositivo ha inviato al server. Questo valore non tiene in considerazione le ripetizioni.

Retransmitted accounting-request packets

Visualizza il numero di pacchetti dati Accounting Request che il dispositivo ha ritrasmesso al server.

Received packets

Visualizza il numero di pacchetti dati Accounting Response che il dispositivo ha ricevuto dal server.

Malformed packets

Visualizza il numero di pacchetti dati Accounting Response malformati che il dispositivo ha ricevuto dal server (inclusi i pacchetti dati con una lunghezza non valida).

Bad authenticators

Visualizza il numero di pacchetti dati Accounting Response con un autenticatore non valido che il dispositivo ha ricevuto dal server.

Pending requests

Visualizza il numero di pacchetti dati Accounting Request che il dispositivo ha inviato al server e per i quali non ha ancora ricevuto risposta dal server.

Timeouts

Visualizza quante volte non si è ricevuta risposta dal server prima che scadesse il tempo di attesa specificato.

Unknown types

Visualizza il numero di pacchetti dati con un tipo di dati sconosciuto che il dispositivo ha ricevuto dal server sulla porta di accounting.

Packets dropped

Visualizza il numero di pacchetti dati che il dispositivo ha ricevuto dal server sulla porta di accounting e poi li ha scartati.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.5 DoS

[Network Security > DoS]

Denial of Service (DoS) è un cyber attacco che ha l'obbiettivo di arrestare specifici servizi o dispositivi. In questa finestra di dialogo è possibile configurare diversi filtri che aiutino a proteggere il dispositivo stesso e altri dispositivi nella rete da attacchi DoS.

Il menu include le seguenti finestre di dialogo:
- DoS Global

4.5.1 DoS Global

[Network Security > DoS > Global]

In questa finestra di dialogo si specificano le impostazioni DoS per i protocolli TCP/UDP, IP e ICMP.

TCP/UDP

Uno scanner utilizza scansioni porta per preparare attacchi alla rete. Lo scanner utilizza diverse tecniche per determinare quali dispositivi sono in funzione e quali le porte aperte. Attraverso questo frame si attivano filtri per tecniche di scansione specifiche.

Il dispositivo supporta il rilevamento dei seguenti tipi di scansione:
- Scansioni null
- Scansioni Xmas
- Scansioni SYN/FIN
- Attacchi offset TCP
- Attacchi SYN TCP
- Attacchi porta L4
- Scansioni Minimal Header

Null Scan filter

Attiva/disattiva il filtro scansioni null.

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.

Possibili valori:
- `selezionato`
  Il filtro è attivo.
- `non selezionato` (impostazione di default)
  Il filtro non è attivo.

Xmas filter

Attiva/disattiva 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 simultaneamente.
- Il numero di sequenza TCP è 0.

Possibili valori:
- `selezionato`
  Il filtro è attivo.
- `non selezionato` (impostazione di default)
  Il filtro non è attivo.

SYN/FIN filter

Attiva/disattiva il filtro SYN/FIN.

Il dispositivo rileva i pacchetti dati in ingresso con flag TCP *SYN* e *FIN* impostati simultaneamente e li rifiuta.

Possibili valori:

- `selezionato`
  Il filtro è attivo.
- `non selezionato` (impostazione di default)
  Il filtro non è attivo.

TCP Offset protection

Attiva/disattiva la protezione offset TCP.

La protezione offset TCP rileva pacchetti dati TCP in ingresso il cui campo offset frammenti dell'header IP corrisponde a 1 e li scarta.

La protezione offset TCP accetta pacchetti UDP E ICMP il cui campo offset frammenti dell'header IP corrisponde a 1.

Possibili valori:

- `selezionato`
  La protezione è attiva.
- `non selezionato` (impostazione di default)
  La protezione non è attiva.

TCP SYN protection

Attiva/disattiva la protezione SYN TCP.

La protezione TCP SYN rileva pacchetti dati in ingresso con il flag TCP SYN impostato e una porta di origine L4 <1024, e li scarta.

Possibili valori:

- `selezionato`
  La protezione è attiva.
- `non selezionato` (impostazione di default)
  La protezione non è attiva.

L4 Port protection

Attiva/disattiva la protezione porta L4.

La protezione porta L4 rileva pacchetti dati TCP e UDP in ingresso il cui numero porta di origine e di destinazione coincidono e li scarta.

Possibili valori:

- `selezionato`
  La protezione è attiva.
- `non selezionato` (impostazione di default)
  La protezione non è attiva.

IP

Attraverso questo frame si attiva o disattiva il filtro attacco land. Tramite il metodo di attacco land, la stazione di attacco invia pacchetti dati i cui indirizzi sorgente e di destinazione sono identici a quelli del destinatario. Attivando questo filtro, il dispositivo rileva i pacchetti dati con indirizzo sorgente e di destinazione identici e scarta questi pacchetti dati.

Land Attack filter

Attiva/disattiva il filtro attacco land.

Il filtro attacco land rileva i pacchetti dati IP in ingresso il cui indirizzo IP sorgente e di destinazione sono identici e li scarta.

Possibili valori:

- `selezionato`
  Il filtro è attivo.
- `non selezionato` (impostazione di default)
  Il filtro non è attivo.

ICMP

Questa finestra di dialogo fornisce le opzioni filtro per i seguenti parametri ICMP:
- Pacchetti dati frammentati
- Pacchetti ICMP a partire da una specifica dimensione
- Ping broadcast

Filter fragmented packets

Attiva/disattiva il filtro per pacchetti ICMP frammentati.

Il filtro rileva pacchetti ICMP frammentati e li scarta.

Possibili valori:

- `selezionato`
  Il filtro è attivo.
- `non selezionato` (impostazione di default)
  Il filtro non è attivo.

Filter by packet size

Attiva/disattiva il filtro per pacchetti ICMP in ingresso.

Il filtro rileva pacchetti ICMP la cui dimensione payload è superiore alla dimensione specificata nel campo *Allowed payload size [byte]* e li scarta.

Possibili valori:

- `selezionato`
  Il filtro è attivo.
- `non selezionato` (impostazione di default)
  Il filtro non è attivo.

Allowed payload size [byte]

Specifica la dimensione payload massima consentita dei pacchetti ICMP in byte.

Selezionare la casella di spunta *Filter by packet size* se si desidera che il dispositivo scarti i pacchetti dati in ingresso la cui dimensione payload eccede la dimensione massima consentita per pacchetti ICMP.

Possibili valori:

- `0..1472` (impostazione di default: `512`)

Drop broadcast ping

Attiva/disattiva il filtro per ping broadcast. I ping broadcast sono una ben nota prova di attacchi smurf.

Possibili valori:

- `selezionato`
  Il filtro è attivo.
  Il dispositivo rileva ping broadcast e li scarta.
- `non selezionato` (impostazione di default)
  Il filtro non è attivo.

Information

Packets dropped

Visualizza il numero di pacchetti dati che il dispositivo ha scartato.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.6 DHCP Snooping

[Network Security > DHCP Snooping]

DHCP Snooping è una funzione che supporta la sicurezza della rete. DHCP Snooping monitora i pacchetti DHCP tra il client DHCP e il server DHCP e funge da firewall tra gli host non protetti e i server DHCP protetti.

In questa finestra di dialogo si configurano e monitorano le seguenti proprietà del dispositivo:

- Validare i pacchetti DHCP da fonti non trusted e scartare i pacchetti non validi.
- Limitare il traffico di dati DHCP da fonti trusted e non trusted.
- Configurare e aggiornare il database di binding di DHCP Snooping. Questo database contiene l'indirizzo MAC, l'indirizzo IP, la VLAN e la porta dei client DHCP alle porte non trusted.
- Validare le richieste successive da host non trusted sulla base del database di binding di DHCP Snooping.

È possibile attivare DHCP Snooping globalmente e per una VLAN specifica. Specificare lo stato di sicurezza (trusted o non trusted) sulle porte individuali. Verificare che il servizio DHCP sia raggiungibile attraverso porte trusted. Per DHCP Snooping si configurano tipicamente le porte utente/client come non trusted e le porte uplink come trusted.

Il menu include le seguenti finestre di dialogo:

- DHCP Snooping Global
- DHCP Snooping Configuration
- DHCP Snooping Statistics
- DHCP Snooping Bindings

4.6.1 DHCP Snooping Global

[Network Security > DHCP Snooping > Global]

Questa finestra di dialogo consente di configuarare i parametri DHCP Snooping globali per il dispositivo:

- Attiva/disattiva *DHCP Snooping* globalmente.
- Attiva/disattiva *Auto-Disable* globalmente.
- Abilita/disabilita la verifica dell'indirizzo MAC sorgente.
- Configurare il nome, la posizione di memoria e l'intervallo di memorizzazione per il database di binding.

Operation

Operation

Abilita/disabilita globalmente la funzione DHCP Snooping.

Possibili valori:

- `On`
- `Off` (impostazione di default)

Configuration

Verify MAC

Attiva/disattiva la verifica dell'indirizzo MAC sorgente nel pacchetto Ethernet.

Possibili valori:

- `selezionato`
  La verifica dell'indirizzo MAC sorgente è attiva.
  Il dispositivo confronta l'indirizzo MAC sorgente con l'indirizzo MAC del client nel pacchetto DHCP ricevuto.
- `non selezionato` (impostazione di default)
  La verifica dell'indirizzo MAC sorgente non è attiva.

Auto-disable

Attiva/disattiva la funzione *Auto-Disable* per *DHCP Snooping*.

Possibili valori:

- `selezionato`
  La funzione *Auto-Disable* per *DHCP Snooping* è attiva.
  Selezionare anche la casella di spunta nella colonna *Auto-disable* nella scheda *Port* nella finestra di dialogo *Network Security > DHCP Snooping > Configuration* per le porte coinvolte.
- `non selezionato` (impostazione di default)
  La funzione *Auto-Disable* per *DHCP Snooping* non è attiva.

Binding database

Remote file name

Specifica il nome del file in cui il dispositivo salva il database di binding di DHCP Snooping.

Nota:

Il dispositivo salva solo i binding dinamici nel database di binding persistente. Il dispositivo salva i binding statici nel profilo di configurazione.

Remote IP address

Specifica l'indirizzo IP remoto su cui il dispositivo salva il database di binding persistente di DHCP Snooping. Con il valore `0.0.0.0` il dispositivo salva il database di binding localmente.

Possibili valori:

- Indirizzo IPv4 valido
- `0.0.0.0` (impostazione di default)
  Il dispositivo salva il database di binding di DHCP Snooping localmente.

Store interval [s]

Specifica il ritardo in secondi dopo il quale il dispositivo salva il database di binding di DHCP Snooping quando il dispositivo identifica una modifica nel database.

Possibili valori:

- `15..86400` (impostazione di default: `300`)

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.6.2 DHCP Snooping Configuration

[Network Security > DHCP Snooping > Configuration]

Questa finestra di dialogo consente di configurare DHCP Snooping per le porte individuali e per le VLAN individuali.

Questa finestra di dialogo include le seguenti schede:
- [Port]
- [VLAN ID]

[Port]

In questa scheda si configura la funzione *DHCP Snooping* per le porte individuali.
- Configurare una porta come trusted/non trusted.
- Attivare/disattivare la registrazione di pacchetti non validi per le porte individuali.
- Limitare il numero di pacchetti DHCP.
- Disattivare una porta automaticamente se il traffico di dati DHCP supera il limite specificato.

Tabella

Port

Visualizza il numero di porta.

Trust

Attiva/disattiva lo stato di sicurezza (trusted, non trusted) della porta.

Quando questa funzione è attiva, la porta è configurata come trusted. Tipicamente, la porta trusted è stata collegata a un server DHCP.

Quando questa funzione non è attiva, la porta è configurata come non trusted.

Possibili valori:
- `selezionato`
  La porta è specificata come trusted. DHCP Snooping inoltra i pacchetti client ammissibili attraverso le porte trusted.
- `non selezionato` (impostazione di default)
  La porta è configurata come non trusted. Sulle porte non trusted il dispositivo confronta la porta ricevente con la porta client nel database di binding.

Log

Attiva/disattiva la registrazione di pacchetti non validi che il dispositivo determina su questa porta.

Possibili valori:
- `selezionato`
  La registrazione dei pacchetti non validi è attiva.
- `non selezionato` (impostazione di default)
  La registrazione dei pacchetti non validi non è attiva.

Rate limit

Specifica il numero massimo di pacchetti DHCP per intervallo di burst per questa porta. Se il numero di pacchetti DHCP in ingresso è attualmente superiore al limite specificato in un intervallo di burst, il dispositivo rifiuta gli ulteriori pacchetti DHCP in ingresso.

Possibili valori:

- `-1` (impostazione di default)
  Disattiva la limitazione del numero di pacchetti DHCP per intervallo di burst su questa porta.
- `0..150`pacchetti per intervallo
  Limita il numero massimo di pacchetti DHCP per intervallo di burst per questa porta.

Specificare l'intervallo di burst nella colonna *Burst interval*.

Se si attiva la funzione di disabilitazione automatica, il dispositiva disabilita anche la porta. La funzione di disabilitazione automatica si trova nella colonna *Auto-disable*.

Burst interval

Specifica la durata dell'intervallo di burst in secondi su questa porta. L'intervallo di brust è rilevante per la funzione di limitazione del carico.

Specificare il numero massimo di pacchetti DHCP per intervallo di burst nella colonna *Rate limit*.

Possibili valori:

- `1..15` (impostazione di default: `1`)

Auto-disable

Attiva/disattiva la funzione *Auto-Disable* per i parametri che la funzione *DHCP Snooping* monitora sulla porta.

Possibili valori:

- `selezionato` (impostazione di default)
  La funzione *Auto-Disable* è attiva sulla porta.
  Il prerequisito è che nella finestra di dialogo *Network Security > DHCP Snooping > Global* sia selezionata la casella di spunta *Auto-disable* nel frame *Configuration*.
  - Se la porta riceve più pacchetti DHCP di quanto specificato nel campo *Rate limit* nel tempo specificato nella colonna *Burst interval*, il dispositivo disabilita la porta. Il LED “Stato del link” per la porta lampeggia 3 volte per periodo.
  - La finestra di dialogo *Diagnostics > Ports > Auto-Disable* visualizza quali porte sono attualmente disabilitate a causa del superamento dei parametri.
  - La funzione *Auto-Disable* riattiva automaticamente la porta. Per fare ciò, nella finestra di dialogo *Diagnostics > Ports > Auto-Disable*, si specifica un periodo di attesa per la porta interessata nella colonna *Reset timer [s]*.
- `non selezionato`
  La funzione *Auto-Disable* sulla porta non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[VLAN ID]

In questa scheda si configura la funzione *DHCP Snooping* per le VLAN individuali.

Tabella

VLAN ID

Visualizza l'ID VLAN a cui fa riferimento la voce della tabella.

Active

Attiva/disattiva la funzione *DHCP Snooping* in questa VLAN.

La funzione *DHCP Snooping* inoltra i messaggi del client DHCP validi alle porte trusted nelle VLAN senza la funzione *Routing*.

Possibili valori:

- `selezionato`
  La funzione *DHCP Snooping* è attiva in questa VLAN.
- `non selezionato` (impostazione di default)
  La funzione *DHCP Snooping* non è attiva in questa VLAN.
  Il dispositivo inoltra i pacchetti DHCP in base alle impostazioni di switching senza monitorare i pacchetti. Il database di binding resta invariato.

Nota: Per abilitare DHCP Snooping per una porta, abilitare la funzione *DHCP Snooping* globalmente nella finestra di dialogo *Network Security > DHCP Snooping > Global*. Verificare di assegnare la porta a una VLAN in cui sia abilitato DHCP Snooping.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.6.3 DHCP Snooping Statistics

[Network Security > DHCP Snooping > Statistics]

Con DHCP Snooping, il dispositivo registra gli errori rilevati e genera statistiche. In questa finestra di dialogo si monitorano le statistiche del DHCP Snooping per ciascuna porta.

Il dispositivo registra i seguenti dati:
- Errori rilevati nella validazione dell'indirizzo MAC del client DHCP
- Messaggi del client DHCP con una porta errata rilevata
- Messaggi del server DHCP verso porte non trusted

Tabella

Port

Visualizza il numero di porta.

MAC verify failures

Visualizza il numero di discrepanze tra l'indirizzo MAC del client DHCP nel campo CHADDR del pacchetto dati DHCP e l'indirizzo sorgente nel pacchetto Ethernet.

Invalid client messages

Visualizza il numero di messaggi del client DHCP in ingresso ricevuti sulla porta per i quali il dispositivo attende il client su un'altra porta in base al database di binding di DHCP Snooping.

Invalid server messages

Visualizza il numero di messaggi del server DHCP che il dispositivo ha ricevuto sulla porta non trusted.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Resetta l'intera tabella.

4.6.4 DHCP Snooping Bindings

[Network Security > DHCP Snooping > Bindings]

DHCP Snooping utilizza i messaggi DHCP per configurare e aggiornare il database di binding.
- Binding statici
  Il dispositivo consente di immettere nel database fino a 256 binding statici di DHCP Snooping.
- Binding dinamici
  Il database di binding dinamico contiene i dati per i client solo sulle porte non trusted.

Questo menu consente di specificare le impostazioni per i binding statici e dinamici.
- Configurare nuovi binding statici e impostarli su attivo/inattivo.
- Visualizzare, attivare/disattivare o cancellare i binding statici che sono stati configurati.

Tabella

MAC address

Specifica l'indirizzo MAC nella voce di tabella che si associa a un *IP address* e un *VLAN ID*.

Possibili valori:
- Indirizzo MAC unicast valido
  Specificare il valore separato dai due punti, per esempio `00:11:22:33:44:55`.

IP address

Specifica l'indirizzo IP per il binding statico di DHCP Snooping.

Possibili valori:
- Indirizzo IPv4 unicast valido inferiore a `224.x.x.x` e al di fuori dell'intervallo `127.0.0.0/8` (impostazione di default: `0.0.0.0`)

VLAN ID

Specifica l'ID della VLAN a cui si applica la voce della tabella.

Possibili valori:
- `<ID delle VLAN configurate>`

Port

Specifica la porta per il binding statico di DHCP Snooping.

Possibili valori:
- Porte disponibili

Remaining binding time

Visualizza il tempo rimanente per il binding dinamico di DHCP Snooping.

Active

Attiva/disattiva il binding statico specificato di DHCP Snooping.

Possibili valori:

- `selezionato`
  Il binding statico di DHCP Snooping è attivo.
- `non selezionato` (impostazione di default)
  Il binding statico di DHCP Snooping non è attivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

Nel campo *MAC address*, specificare l'indirizzo MAC da assegnare a un indirizzo IP e un ID VLAN.

Rimuove la voce tabella evidenziata.

Il prerequisito è che la casella di spunta nella colonna *Active* non sia selezionata.

Inoltre, il dispositivo rimuove i binding dinamici di questa porta creati con la funzione *IP Source Guard*.

4.7 IP Source Guard

[Network Security > IP Source Guard]

IP Source Guard (IPSG) è una funzione che supporta la sicurezza della rete. La funzione filtra i pacchetti dati IP in base all'ID sorgente (indirizzo IP sorgente o indirizzo MAC sorgente) dell'utente. IPSG supporta la protezione della rete da attacchi di spoofing attraverso indirizzi IP/MAC.

IPSG e DHCP Snooping
IP Source Guard opera in combinazione alla funzione *DHCP Snooping* della porta.

DHCP Snooping rifiuta i pacchetti dati IP sulle porte non trusted, ad eccezione dei messaggi DHCP. Quando il dispositivo riceve le risposte DHCP e il database di binding di DHCP Snooping è configurato, il dispositivo crea un elenco di controllo accessi VLAN (VACL) per ciascuna porta contenente gli ID sorgente degli utenti.

Configurare i parametri della funzione *DHCP Snooping* per le porte individuali e le VLAN individuali nella finestra di dialogo *Network Security > DHCP Snooping > Configuration*.

IPSG e sicurezza porte
IP Source Guard collabora con la funzione *Port Security*. Vedere la finestra di dialogo *Network Security > Port Security*. Se richiesto, IPSG informa la funzione *Port Security* della richiesta se un indirizzo MAC appartiene a un binding valido.
- Se IPSG è disattivato sulla porta di ingresso, IPSG identifica il pacchetto dati come valido.
- Se IPSG è attivato sulla porta di ingresso, IPSG verifica l'indirizzo MAC utilizzando il database di binding. Se l'indirizzo MAC è inserito nel database di binding, IPSG identifica il pacchetto dati come valido, altrimenti come non valido.

La funzione *Port Security* gestisce la successiva elaborazione dei pacchetti dati non validi. Specificare le impostazioni della funzione *Port Security* nella finestra di dialogo *Network Security > Port Security*.

Nota: Affinché il dispositivo verifichi l'indirizzo IP e l'indirizzo MAC dei pacchetti dati ricevuti sulla porta, abilitare la funzione *Verify MAC*.

Affinché il dispositivo verifichi l'ID VLAN e l'indirizzo MAC sorgente prima di inoltrare il pacchetto dati, abilitare anche la funzione *Port Security*. Vedere la finestra di dialogo *Network Security > Port Security*.

Il menu include le seguenti finestre di dialogo:
- IP Source Guard Port
- IP Source Guard Bindings

4.7.1 IP Source Guard Port

[Network Security > IP Source Guard > Port]

Questa finestra di dialogo consente di visualizzare e configurare le seguenti proprietà del dispositivo per ciascuna porta:

- Includere/escludere gli indirizzi MAC sorgente nel filtro.
- Attivare/disattivare la funzione *IP Source Guard*.

Tabella

Port

Visualizza il numero di porta.

Verify MAC

Attiva/disattiva il filtro in base all'indirizzo MAC sorgente se la funzione *IP Source Guard* è attiva. Il dispositivo applica questo filtro in aggiunta al filtro basato sull'indirizzo IP sorgente.

Possibili valori:

- `selezionato`
  Il filtro basato sull'indirizzo MAC sorgente è attivo.
  Per attivare questa funzione, selezionare la casella di spunta *Active*.
- `non selezionato` (impostazione di default)
  Il filtro basato sull'indirizzo MAC sorgente non è attivo.
  Per disattivare questa funzione, deselezionare anche la casella di spunta *Active*.

Active

Attiva/disattiva la funzione *IP Source Guard* sulla porta.

Possibili valori:

- `selezionato`
  La funzione *IP Source Guard* è attiva.
  Abilitare anche la funzione *DHCP Snooping* nella finestra di dialogo *Network Security > DHCP Snooping > Global*.
- `non selezionato` (impostazione di default)
  La funzione *IP Source Guard* non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.7.2 IP Source Guard Bindings

[Network Security > IP Source Guard > Bindings]

Questa finestra di dialogo visualizza i binding statici e dinamici dell'IP Source Guard.

- Il dispositivo apprende i binding dinamici attraverso DHCP Snooping. Vedere la finestra di dialogo *Network Security > DHCP Snooping > Configuration*.
- I binding statici sono i binding di IP Source Guard configurati manualmente dall'utente. La finestra di dialogo consente di modificare i binding statici.

Tabella

MAC address

Visualizza l'indirizzo MAC del binding.

IP address

Visualizza l'indirizzo IP del binding.

VLAN ID

Visualizza l'ID VLAN del binding.

Port

Visualizza il numero della porta del binding.

Hardware status

Visualizza lo stato dell'hardware del binding.

Il dispositivo applica il binding all'hardware solo se le impostazioni sono corrette. Prima di applicare il binding statico di IPSG all'hardware, il dispositivo verifica i seguenti prerequisiti:

- La casella di spunta *Active* è selezionata.
- La funzione *IP Source Guard* sulla porta è attiva, nella finestra di dialogo *Network Security > IP Source Guard > Port* la casella di spunta *Active* è selezionata.

Possibili valori:

- `selezionato`
  Il binding è attivo, il dispositivo applica il binding all'hardware.
- `non selezionato`
  Il binding non è attivo.

Active

Attiva/disattiva il binding statico di IPSG specificato tra l'indirizzo MAC specificato e l'indirizzo IP specificato per la VLAN specificata sulla porta specificata.

Possibili valori:

- `selezionato`
  Il binding statico di IPSG è attivo.
- `non selezionato` (impostazione di default)
  Il binding statico di IPSG non è attivo.

Nota: Per rendere efficace il binding statico, attivare la funzione *IP Source Guard* sulla porta corrispondente. Nella finestra di dialogo *Network Security > IP Source Guard > Port* selezionare la casella di spunta *Active*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

- Nel campo *MAC address* specificare l'indirizzo MAC per il binding statico.
- Nel campo *IP address* specificare l'indirizzo IP per il binding statico.
- Nel campo *VLAN ID* specificare l'ID VLAN.
- Nel campo *Port* specificare l'ID della VLAN.

Rimuove la voce tabella evidenziata.

Il prerequisito è che la casella di spunta nella colonna *Active* non sia selezionata.

4.8 Dynamic ARP Inspection

[Network Security > Dynamic ARP Inspection]

Dynamic ARP Inspection è una funzione che supporta la sicurezza della rete. Questa funzione analizza i pacchetti ARP, li registra e rifiuta i pacchetti ARP non validi e ostili.

La funzione *Dynamic ARP Inspection* aitua a evitare una serie di attacchi man in the middle. Con questo tipo di attacchi, una stazione ostile si inserisce per ascoltare il traffico di dati di altri utenti invadendo la cache ARP dei vicini ignari. La stazione ostile invia richieste ARP e risposte ARP e immette l'indirizzo IP di un altro utente per il suo indirizzo MAC nel rapporto indirizzo IP-MAC (binding).

Utilizzando le seguenti misure, la funzione *Dynamic ARP Inspection* contribuisce a garantire che il dispositivo inoltri solo richieste e risposte ARP valide.

- Ascolto di richieste e risposte ARP su porte non trusted.
- Verifica che i pacchetti determinati abbiano un rapporto di indirizzo da IP a MAC valido (binding) prima che il dispositivo aggiorni la cache ARP locale e prima che il dispositivo inoltri i pacchetti all'indirizzo di destinazione correlato.
- Rifiuto di pacchetti ARP non validi.

Il dispositivo consente di specificare fino a 100 elenchi di controllo accesso ARP attivi (elenchi di accesso). È possibile attivare fino a 20 regole per ciascun elenco di controllo accessi ARP.

Il menu include le seguenti finestre di dialogo:

- Dynamic ARP Inspection Global
- Dynamic ARP Inspection Configuration
- Dynamic ARP Inspection ARP Rules
- Dynamic ARP Inspection Statistics

4.8.1 Dynamic ARP Inspection Global

[Network Security > Dynamic ARP Inspection > Global]

Configuration

Verify source MAC

Attiva/disattiva la verifica dell'indirizzo MAC sorgente. Il dispositivo esegue la verifica sia nelle richieste ARP sia nelle risposte ARP.

Possibili valori:

- `selezionato`
  La verifica dell'indirizzo MAC sorgente è attiva.
  Il dispositivo verifica l'indirizzo MAC sorgente dei pacchetti ARP ricevuti.
  - Il dispositivo trasmette i pacchetti ARP con un indirizzo MAC sorgente valido all'indirizzo di destinazione correlato e aggiorna la cache ARP locale.
  - Il dispositivo rifiuta i pacchetti ARP con un indirizzo MAC sorgente non valido.
- `non selezionato` (impostazione di default)
  La verifica dell'indirizzo MAC sorgente non è attiva.

Verify destination MAC

Attiva/disattiva la verifica dell'indirizzo MAC di destinazione. Il dispositivo esegue la verifica nelle risposte ARP.

Possibili valori:

- `selezionato`
  La verifica dell'indirizzo MAC di destinazione è attiva.
  Il dispositivo verifica l'indirizzo MAC di destinazione dei pacchetti ARP in ingresso.
  - Il dispositivo trasmette i pacchetti ARP con un indirizzo MAC di destinazione valido all'indirizzo di destinazione correlato e aggiorna la cache ARP locale.
  - Il dispositivo rifiuta i pacchetti ARP con un indirizzo MAC di desitnazione non valido.
- `non selezionato` (impostazione di default)
  La verifica dell'indirizzo MAC di destinazione dei pacchetti ARP in ingresso non è attiva.

Verify IP address

Attiva/disattiva la verifica dell'indirizzo IP.

Nelle richieste ARP, il dispositivo verifica l'indirizzo IP sorgente. Nelle risposte ARP, il dispositivo verifica l'indirizzo IP di destinazione e sorgente.

Il dispositivo definisce non validi i seguenti indirizzi IP

- `0.0.0.0`
- Indirizzi broadcast `255.255.255.255`
- Indirizzi multicast `224.0.0.0/4` (Classe D)
- Indirizzi di Classe E `240.0.0.0/4` (riservati per finalità successive)
- Indirizzi loopback nell'intervallo `127.0.0.0/8`.

Possibili valori:

- `selezionato`
  La verifica dell'indirizzo IP è attiva.
  Il dispositivo verifica l'indirizzo IP dei pacchetti ARP in ingresso. Il dispositivo trasmette i pacchetti ARP con un indirizzo IP valido all'indirizzo di destinazione correlato e aggiorna la cache ARP locale. Il dispositivo rifiuta i pacchetti ARP con un indirizzo IP non valido.
- `non selezionato` (impostazione di default)
  La verifica dell'indirizzo IP non è attiva.

Auto-disable

Attiva/disattiva la funzione *Auto-Disable* per *Dynamic ARP Inspection*.

Possibili valori:

- `selezionato`
  La funzione *Auto-Disable* per *Dynamic ARP Inspection* è attiva.
  Selezionare anche la casella di spunta nella colonna *Port* nella scheda *Auto-disable* nella finestra di dialogo *Network Security > Dynamic ARP Inspection > Configuration* per le porte coinvolte.
- `non selezionato` (impostazione di default)
  La funzione *Auto-Disable* per *Dynamic ARP Inspection* non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.8.2 Dynamic ARP Inspection Configuration

[Network Security > Dynamic ARP Inspection > Configuration]

Questa finestra di dialogo include le seguenti schede:
- [Port]
- [VLAN ID]

[Port]

Tabella

Port

Visualizza il numero di porta.

Trust

Attiva/disattiva il monitoraggio del pacchetti ARP sulle porte non trusted.

Possibili valori:
- `selezionato`
  Il monitoraggio è attivo.
  Il dispositivo monitora i pacchetti ARP sulle porte non trusted.
  Il dispositivo inoltra immediatamente i pacchetti ARP sulle porte trusted.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Rate limit

Specifica il numero massimo di pacchetti ARP per intervallo su questa porta. Se il numero di pacchetti ARP in ingresso è attualmente superiore al limite specificato in un intervallo di burst, il dispositivo rifiuta gli ulteriori pacchetti ARP in ingresso. Specificare l'intervallo di burst nella colonna *Burst interval*.

Opzionalmente, il dispositivo disattiva anche la porta se si attiva la funzione di disabilitazione automatica. Si abilita/disabilita la funzione *Auto-Disable* nella colonna *Auto-disable*.

Possibili valori:
- `-1` (impostazione di default)
  Disattiva la limitazione del numero di pacchetti ARP per intervallo di burst su questa porta.
- `0..300`pacchetti per intervallo
  Limita il numero massimo di pacchetti ARP per intervallo di burst per questa porta.

Burst interval

Specifica la durata dell'intervallo di burst in secondi su questa porta. L'intervallo di brust è rilevante per la funzione di limitazione del carico.

Specificare il numero massimo di pacchetti ARP per intervallo di burst nella colonna *Rate limit*.

Possibili valori:

- `1..15` (impostazione di default: `1`)

Auto-disable

Attiva/disattiva la funzione *Auto-Disable* per i parametri che la funzione *Dynamic ARP Inspection* monitora sulla porta.

Possibili valori:

- `selezionato` (impostazione di default)
  La funzione *Auto-Disable* è attiva sulla porta.
  Il prerequisito è che nella finestra di dialogo *Network Security > Dynamic ARP Inspection > Global* sia selezionata la casella di spunta *Auto-disable* nel frame *Configuration*.
  - Se la porta riceve più pacchetti ARP di quanto specificato nel campo *Rate limit* nel tempo specificato nella colonna *Burst interval*, il dispositivo disabilita la porta. Il LED “Stato del link” per la porta lampeggia 3 volte per periodo.
  - La finestra di dialogo *Diagnostics > Ports > Auto-Disable* visualizza quali porte sono attualmente disabilitate a causa del superamento dei parametri.
  - La funzione *Auto-Disable* riattiva automaticamente la porta. Per fare ciò, nella finestra di dialogo *Diagnostics > Ports > Auto-Disable*, si specifica un periodo di attesa per la porta interessata nella colonna *Reset timer [s]*.
- `non selezionato`
  La funzione *Auto-Disable* sulla porta non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[VLAN ID]

Tabella

VLAN ID

Visualizza l'ID VLAN a cui fa riferimento la voce della tabella.

Log

Attiva/disattiva la registrazione di pacchetti ARP non validi che il dispositivo determina in questa VLAN. Se il dispositivo rileva un errore durante la verifica dell'indirizzo IP, MAC sorgente o MAC di destinazione, o nel verificare il rapporto dell'indirizzo da IP a MAC (binding), il dispositivo individua un pacchetto ARP come non valido.

Possibili valori:

- `selezionato`
  La registrazione dei pacchetti non validi è attiva.
  Il dispositivo registra i pacchetti ARP non validi.
- `non selezionato` (impostazione di default)
  La registrazione dei pacchetti non validi non è attiva.

Binding check

Attiva/disattiva la verifica dei pacchetti ARP in ingresso che il dispositivo riceve sulle porte non trusted e sulle VLAN per cui è attiva la funzione *Dynamic ARP Inspection*. Per questi pacchetti ARP il dispositivo verifica l'elenco di controllo accessi ARP e il rapporto DHCP Snooping (binding).

Possibili valori:

- `selezionato` (impostazione di default)
  La verifica del binding dei pacchetti ARP è attiva.
- `non selezionato`
  La verifica del binding dei pacchetti ARP non è attiva.

ACL strict

Attiva/disattiva la verifica strict dei pacchetti ARP in ingresso sulla base delle regole specificate dell'elenco di controllo accessi ARP.

Possibili valori:

- `selezionato`
  La verifica strict è attiva.
  Il dispositivo verifica i pacchetti ARP in ingresso in base alla regola dell'elenco di controllo accessi ARP specificata nella colonna *ARP ACL*.
- `non selezionato` (impostazione di default)
  La verifica strict non è attiva.
  Il dispositivo verifica i pacchetti ARP in ingresso in base alla regola dell'elenco di controllo accessi ARP specificata nella colonna *ARP ACL* e, in seguito, in base alle voci nel database di DHCP Snooping.

ARP ACL

Specifica l'elenco di controllo accessi ARP utilizzato dal dispositivo.

Possibili valori:

- `<nome regola>`
  È possibile creare e modificare le regole nella finestra di dialogo *Network Security > Dynamic ARP Inspection > ARP Rules*.

Active

Attiva/disattiva la funzione *Dynamic ARP Inspection* in questa VLAN.

Possibili valori:

- `selezionato`
  La funzione *Dynamic ARP Inspection* è attiva in questa VLAN.
- `non selezionato` (impostazione di default)
  La funzione *Dynamic ARP Inspection* non è attiva in questa VLAN.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

4.8.3 Dynamic ARP Inspection ARP Rules

[Network Security > Dynamic ARP Inspection > ARP Rules]

Questa finestra di dialogo consente di specificare le regole per controllare e filtrare i pacchetti ARP.

Tabella

Name

Visualizza il nome della regola ARP.

Source IP address

Specifica l'indirizzo sorgente dei pacchetti dati IP a cui il dispositivo applica la regola.

Possibili valori:

- Indirizzo IPv4 valido
  Il dispositivo applica la regola ai pacchetti dati IP con l'indirizzo sorgente specificato.

Source MAC address

Specifica l'indirizzo sorgente dei pacchetti dati MAC a cui il dispositivo applica la regola.

Possibili valori:

- Indirizzo MAC valido
  Il dispositivo applica la regola ai pacchetti dati MAC con l'indirizzo sorgente specificato.

Active

Attiva/disattiva la regola *ARP*.

Possibili valori:

- `selezionato` (impostazione di default)
  La regola è attiva.
- `non selezionato`
  La regola non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

- Nel campo *Name*, specificare il nome della regola ARP.
- Nel campo *Source IP address*, specificare l'indirizzo IP sorgente della regola ARP.
- Nel campo *Source MAC address*, si specifica l'indirizzo MAC fonte della regola ARP.

4.8.4 Dynamic ARP Inspection Statistics

[Network Security > Dynamic ARP Inspection > Statistics]

Questa finestra visualizza una panoramica del numero di pacchetti ARP rifiutati e inoltrati.

Tabella

VLAN ID

Visualizza l'ID VLAN a cui fa riferimento la voce della tabella.

Packets forwarded

Visualizza il numero di pacchetti ARP che il dispositivo inoltra dopo averli controllati utilizzando la funzione *Dynamic ARP Inspection*.

Packets dropped

Visualizza il numero di pacchetti ARP che il dispositivo rifiuta dopo averli controllati utilizzando la funzione *Dynamic ARP Inspection*.

DHCP drops

Visualizza il numero di pacchetti ARP che il dispositivo rifiuta dopo averli controllati utilizzando il rapporto di DHCP Snooping (binding).

DHCP permits

Visualizza il numero di pacchetti ARP che il dispositivo inoltra dopo averli controllati utilizzando il rapporto di DHCP Snooping (binding).

ACL drops

Visualizza il numero di pacchetti ARP che il dispositivo rifiuta dopo averli controllati utilizzando le regole dell'elenco di controllo accessi ARP.

ACL permits

Visualizza il numero di pacchetti ARP che il dispositivo inoltra dopo averli controllati utilizzando le regole dell'elenco di controllo accessi ARP.

Bad source MAC

Visualizza il numero di pacchetti ARP che il dispositivo rifiuta dopo che la funzione *Dynamic ARP Inspection* ha rilevato un errore nell'indirizzo MAC sorgente.

Bad destination MAC

Visualizza il numero di pacchetti ARP che il dispositivo rifiuta dopo che la funzione *Dynamic ARP Inspection* ha rilevato un errore nell'indirizzo MAC di destinazione.

Invalid IP address

Visualizza il numero di pacchetti ARP che il dispositivo rifiuta dopo che la funzione *Dynamic ARP Inspection* ha rilevato un errore nell'indirizzo IP.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Resetta l'intera tabella.

4.9 ACL

[Network Security > ACL]

In questo menu si specificano le impostazioni per gli elenchi di controllo accesso (Access Control Lists, ACL). Gli elenchi di controllo accesso contengono regole che il dispositivo applica in successione al flusso di dati sulle sue porte o VLAN.

Se un pacchetto dati è conforme ai criteri di una o più regole, il dispositivo esegue l'azione specificata nella prima regola che si applica al flusso di dati. Il dispositivo ignora le regole che seguono. Possibili azioni comprendono:
- *permit*: il dispositivo trasmette il pacchetto dati a una porta o ad una VLAN.
- *deny*: il dispositivo scarta i pacchetti dati

Nell'impostazione di default, il dispositivo inoltra ogni pacchetto dati. Assegnato un elenco di controllo accessi ad un'interfaccia o VLAN, non vi sono modifiche a questo comportamento. Alla fine di un elenco di controllo accessi, il dispositivo inserisce una regola implicita Deny-All. Di conseguenza, il dispositivo scarta i pacchetti dati che non soddisfano nessuna delle regole. Se si desidera un comportamento differente, aggiungere una regola “permesso” alla fine dell'elenco di controllo accessi.

Procedere come di seguito illustrato per configurare gli elenchi di controllo accesso e le regole:
- ☐ Creare una regola e specificare le impostazioni della regola. Vedere la finestra di dialogo *Network Security > ACL > IPv4 Rule* o la finestra di dialogo *Network Security > ACL > MAC Rule*.
- ☐ Assegnare l'elenco di controllo accessi alle porte e alle VLAN del dispositivo. Vedere la finestra di dialogo *Network Security > ACL > Assignment*.

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

4.9.1 ACL IPv4 Rule

[Network Security > ACL > IPv4 Rule]

In questa finestra di dialogo, si specificano le regole che il dispositivo applica ai pacchetti dati IP.

Un elenco di controllo accessi (gruppo) contiene una o più regole. Il dispositivo applica le regole di un elenco di controllo accessi in successione, iniziando con la regola con il valore più basso nella colonna *Index*.

Il dispositivo consente di inserire filtri secondo i seguenti criteri:
- Indirizzo IP sorgente o di destinazione di un pacchetto dati
- Tipo di protocollo di trasmissione
- Porta sorgente o di destinazione di un pacchetto dati

Tabella

Group name

Visualizza il nome dell'elenco di controllo accessi. L'elenco di controllo accessi contiene le regole.

Index

Visualizza il numero della regola all'interno dell'elenco di controllo accessi.

Se l'elenco di controllo accessi contiene regole multiple, il dispositivo elabora prima la regola con il valore più basso.

Match every packet

Specifica a quale pacchetto dati IP il dispositivo applica la regola.

Possibili valori:
- `selezionato` (impostazione di default)
  Il dispositivo applica la regola ad ogni pacchetto dati IP.
- `non selezionato`
  Il dispositivo applica la regola ai pacchetti dati IP in funzione del valore nei campi *Source IP address*, *Destination IP address* e *Protocol*.

Source IP address

Specifica l'indirizzo sorgente dei pacchetti dati IP a cui il dispositivo applica la regola.

Possibili valori:
- `?.?.?.?` (impostazione di default)
  Il dispositivo applica la regola ai pacchetti dati IP con qualsiasi indirizzo sorgente.

- Indirizzo IPv4 valido
  Il dispositivo applica la regola ai pacchetti dati IP con l'indirizzo sorgente specificato.
  Si utilizza il carattere `?` come un carattere jolly.
  Ad esempio `192.?.?.32`: il dispositivo applica la regola a pacchetti dati IP il cui indirizzo sorgente inizia con `192.` e finisce con `.32`.
- Indirizzo IPv4 valido/bitmask
  Il dispositivo applica la regola ai pacchetti dati IP con l'indirizzo sorgente specificato. Attraverso il bitmask inverso si specifica l'intervallo di indirizzi con un'accuratezza a livello di bit.
  Ad esempio `192.168.1.0/0.0.0.127`: il dispositivo applica la regola a pacchetti dati IP con un indirizzo sorgente nell'intervallo da `192.168.1.0` a `….127`.

Destination IP address

Specifica l'indirizzo di destinazione dei pacchetti dati IP a cui il dispositivo applica la regola.

Possibili valori:

- `?.?.?.?` (impostazione di default)
  Il dispositivo applica la regola ai pacchetti dati con qualsiasi indirizzo di destinazione.
- Indirizzo IPv4 valido
  Il dispositivo applica la regola ai pacchetti dati con l'indirizzo di destinazione specificato.
  Si utilizza il carattere `?` come un carattere jolly.
  Ad esempio `192.?.?.32`: il dispositivo applica la regola a pacchetti dati IP il cui indirizzo sorgente inizia con `192.` e finisce con `.32`.
- Indirizzo IPv4 valido/bitmask
  Il dispositivo applica la regola ai pacchetti dati con l'indirizzo di destinazione specificato. Attraverso il bitmask inverso si specifica l'intervallo di indirizzi con un'accuratezza a livello di bit.
  Ad esempio `192.168.1.0/0.0.0.127`: il dispositivo applica la regola a pacchetti dati IP con un indirizzo di destinazione nell'intervallo da `192.168.1.0` a `….127`.

Protocol

Specifica il tipo di protocollo dei pacchetti dati IP a cui il dispositivo applica la regola.

Possibili valori:

- `any` (impostazione di default)
  Il dispositivo applica la regola ad ogni pacchetto dati IP senza considerare il tipo di protocollo.
- `icmp`
- `igmp`
- `ip-in-ip`
- `tcp`
- `udp`
- `ip`

Source TCP/UDP port

Specifica la porta di origine dei pacchetti dati IP a cui il dispositivo applica la regola. Il prerequisito è quello di specificare nella colonna *Protocol* il valore `TCP` o `UDP`.

Possibili valori:

- `any` (impostazione di default)
  Il dispositivo applica la regola ad ogni pacchetto dati IP senza considerare la porta di origine.
- `1..65535`
  Il dispositivo applica la regola solo ai pacchetti dati IP contenenti la porta di origine specificata.

Destination TCP/UDP port

Specifica la porta di destinazione dei pacchetti dati IP a cui il dispositivo applica la regola. Il prerequisito è quello di specificare nella colonna *Protocol* il valore `TCP` o `UDP`.

Possibili valori:

- `any` (impostazione di default)
  Il dispositivo applica la regola ad ogni pacchetto dati IP senza considerare la porta di destinazione.
- `1..65535`
  Il dispositivo applica la regola solo ai pacchetti dati IP contenenti la porta di destinazione specificata.

Action

Specifica come il dispositivo elabora i pacchetti dati IP ricevuti quando il dispositivo applica la regola.

Possibili valori:

- *permit* (impostazione di default)
  Il dispositivo trasmette i pacchetti dati IP.
- *deny*
  Il dispositivo scarta i pacchetti dati IP.

Log

Attiva/disattiva la registrazione nel file di registro. Vedere la finestra di dialogo *Diagnostics > Report > System Log*.

Possibili valori:

- `selezionato`
  La registrazione è attivata.
  Il prerequisito è quello di assegnare l'elenco di controllo accessi nella finestra di dialogo *Network Security > ACL > Assignment* ad una VLAN oppure a una porta.
  Il dispositivo registra nel file di registro, ad un intervallo di 30 s, quante volte applica la regola di rifiuto a pacchetti dati IP.
- `non selezionato` (impostazione di default)
  La registrazione è disattivata.

Il dispositivo consente l'attivazione di questa funzione per un massimo di 128 regole di rifiuto.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

- Nel campo *Group name*, si specifica il nome dell'elenco di controllo accessi a cui appartiene la regola.
- Nel campo *Index*, si specifica il numero della regola all'interno dell'elenco di controllo accessi. Se l'elenco di controllo accessi contiene regole multiple, il dispositivo elabora prima la regola con il valore più basso.

4.9.2 ACL MAC Rule

[Network Security > ACL > MAC Rule]

In questa finestra di dialogo, si specificano le regole che il dispositivo applica ai pacchetti dati MAC.

Un elenco di controllo accessi (gruppo) contiene una o più regole. Il dispositivo applica le regole di un elenco di controllo accessi in successione, iniziando con la regola con il valore più basso nella colonna *Index*.

Il dispositivo consente di inserire filtri per l'indirizzo MAC sorgente o di destinazione di un pacchetto dati.

Tabella

Group name

Visualizza il nome dell'elenco di controllo accessi. L'elenco di controllo accessi contiene le regole.

Index

Visualizza il numero della regola all'interno dell'elenco di controllo accessi.

Se l'elenco di controllo accessi contiene regole multiple, il dispositivo elabora prima la regola con il valore più basso.

Match every packet

Specifica a quale pacchetto dati MAC il dispositivo applica la regola.

Possibili valori:

- `selezionato` (impostazione di default)
  Il dispositivo applica la regola ad ogni pacchetto dati MAC.
- `non selezionato`
  Il dispositivo applica la regola ai pacchetti dati MAC in funzione del valore nei campi *Source MAC address* e *Destination MAC address*.

Source MAC address

Specifica l'indirizzo sorgente dei pacchetti dati MAC a cui il dispositivo applica la regola.

Possibili valori:

- `??:??:??:??:??:??` (impostazione di default)
  Il dispositivo applica la regola ai pacchetti dati MAC con qualsiasi indirizzo sorgente.
- Indirizzo MAC valido
  Il dispositivo applica la regola ai pacchetti dati MAC con l'indirizzo sorgente specificato.
  Si utilizza il carattere `?` come un carattere jolly.
  Ad esempio `00:11:??:??:??:??`: il dispositivo applica la regola a pacchetti dati MAC il cui indirizzo sorgente inizia con `00:11`.
- Indirizzo MAC valido/bitmask
  Il dispositivo applica la regola ai pacchetti dati MAC con l'indirizzo sorgente specificato. Attraverso il bitmask si specifica l'intervallo di indirizzi con un'accuratezza a livello di bit.
  Ad esempio `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: il dispositivo applica la regola a pacchetti dati MAC con un indirizzo sorgente nell'intervallo da `00:11:22:33:44:54` a `…:57`.

Destination MAC address

Specifica l'indirizzo di destinazione dei pacchetti dati MAC a cui il dispositivo applica la regola.

Possibili valori:

- `??:??:??:??:??:??` (impostazione di default)
  Il dispositivo applica la regola ai pacchetti dati MAC con qualsiasi indirizzo di destinazione.
- Indirizzo MAC valido
  Il dispositivo applica la regola ai pacchetti dati MAC con l'indirizzo di destinazione specificato.
  Si utilizza il carattere `?` come un carattere jolly.
  Ad esempio `00:11:??:??:??:??`: il dispositivo applica la regola a pacchetti dati MAC il cui indirizzo di destinazione inizia con `00:11`.
- Indirizzo MAC valido/bitmask
  Il dispositivo applica la regola ai pacchetti dati MAC con l'indirizzo sorgente specificato. Attraverso il bitmask si specifica l'intervallo di indirizzi con un'accuratezza a livello di bit.
  Ad esempio `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: il dispositivo applica la regola a pacchetti dati MAC con un indirizzo di destinazione nell'intervallo da `00:11:22:33:44:54` a `…:57`.

Action

Specifica come il dispositivo elabora i pacchetti dati MAC ricevuti quando il dispositivo applica la regola.

Possibili valori:

- *permit* (impostazione di default)
  Il dispositivo trasmette i pacchetti dati MAC.
- *deny*
  Il dispositivo scarta i pacchetti dati MAC.

Log

Attiva/disattiva la registrazione nel file di registro. Vedere la finestra di dialogo *Diagnostics > Report >* System Log.

Possibili valori:

- `selezionato`
  La registrazione è attivata.
  Il prerequisito è quello di assegnare l'elenco di controllo accessi nella finestra di dialogo *Network Security > ACL > Assignment* ad una VLAN oppure a una porta.
  Il dispositivo registra nel file di registro, ad un intervallo di 30 s, quante volte applica la regola di rifiuto a pacchetti dati MAC.
- `non selezionato` (impostazione di default)
  La registrazione è disattivata.

Il dispositivo consente l'attivazione di questa funzione per un massimo di 128 regole di rifiuto.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

- Nel campo *Group name*, si specifica il nome dell'elenco di controllo accessi a cui appartiene la regola.
- Nel campo *Index*, si specifica il numero della regola all'interno dell'elenco di controllo accessi. Se l'elenco di controllo accessi contiene regole multiple, il dispositivo elabora prima la regola con il valore più basso.

4.9.3 ACL Assignment

[Network Security > ACL > Assignment]

Attraverso questa finestra di dialogo si assegnano uno o più elenchi di controllo accesso alle porte e VLAN del dispositivo. Assegnando una priorità si specifica la sequenza di elaborazione, a condizione di assegnare uno o più elenchi di controllo accesso alle porte e alle VLAN.

Il dispositivo applica le regole in successione, ovvero nella sequenza specificata dall'indice regole. Si specifica la priorità di un gruppo nella colonna *Priority*. Più è basso il numero, più è alta la priorità. In questo processo, il dispositivo applica le regole con una priorità alta prima delle regole con una priorità bassa.

L'assegnazione di elenchi di controllo accesso a porte e VLAN determina i seguenti tipi differenti di ACL:
- ACL IPv4 basati su porta
- ACL MAC basati su porta
- ACL IPv4 basati su VLAN
- ACL MAC basati su VLAN

Il dispositivo consente di applicare l'elenco di controllo accessi ai pacchetti dati ricevuti (`inbound`).

Nota: Prima di attivare la funzione, verificare che almeno una voce attiva nella tabella consenta l'accesso. In caso contrario, il link al dispositivo termina se si modifica l'impostazione. L'accesso alla gestione del dispositivo è possibile solo utilizzando la CLI attraverso l'interfaccia seriale del dispositivo.

Tabella

Group name

Visualizza il nome dell'elenco di controllo accessi. L'elenco di controllo accessi contiene le regole.

Type

Visualizza se l'elenco di controllo accessi contiene regole MAC o regole IPv4.

Possibili valori:
- *mac*
  L'elenco di controllo accessi contiene regole MAC.
- *ip*
  L'elenco di controllo accessi contiene regole IPv4.

Nella finestra di dialogo *Network Security > ACL > IPv4 Rule* si modificano gli elenchi di controllo accesso con regole IPv4. Nella finestra di dialogo *Network Security > ACL > MAC Rule* si modificano gli elenchi di controllo accesso con regole MAC.

Port

Visualizza la porta alla quale è assegnato l'elenco di controllo accessi. Il campo rimane vuoto quando l'elenco di controllo accessi è assegnato alla VLAN.

VLAN ID

Visualizza la VLAN alla quale è assegnato l'elenco di controllo accessi. Il campo rimane vuoto quando l'elenco di controllo accessi è assegnato a una porta.

Direction

Visualizza che il dispositivo applica l'elenco di controllo accessi ai pacchetti dati ricevuti.

Priority

Visualizza la priorità dell'elenco di controllo accessi.

Utilizzando la priorità, si specifica la sequenza con la quale il dispositivo applica gli elenchi di controllo accesso al flusso di dati. Il dispositivo applica le regole in ordine ascendente iniziando dalla priorità `1`.

Possibili valori:

- `1..4294967295`

Se si assegna un elenco di controllo accessi a una porta ed a una VLAN con la stessa priorità, il dispositivo applica le regole innanzitutto alla porta.

Active

Visualizza se l'elenco di controllo accessi sulla porta o sulla VLAN è attiva.

Possibili valori:

- `selezionato` (impostazione di default)
  L'elenco di controllo accessi è attivo.
- `non selezionato`
  L'elenco di controllo accessi non è attivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra di dialogo *Create* per assegnare una regola a una porta oppure ad una VLAN.

- Nel campo *Port/VLAN*, si specifica la porta o il VLAN-ID.
- Nel campo *Priority*, si specifica l'indirizzo MAC fonte della regola ARP.
- Nel campo *Direction*, si specificano i pacchetti dati a cui il dispositivo applica la regola.
- Nel campo *Group name*, si specifica quale regola il dispositivo assegna alla porta o alla VLAN.

5 Switching

Il menu include le seguenti finestre di dialogo:
- Switching Global
- Rate Limiter
- Filter for MAC Addresses
- IGMP Snooping
- Time-Sensitive Networking
- MRP-IEEE
- GARP
- QoS/Priority
- VLAN
- L2-Redundancy

5.1 Switching Global

[Switching > Global]

Questa finestra di dialogo consente di specificare le seguenti impostazioni:
- Modificare l'Aging time della tabella indirizzi
- Abilitare il controllo di flusso nel dispositivo

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, per esempio, quando il dispositivo riceve dati su una porta Gigabit e li inoltra a una porta con una larghezza di banda inferiore. Il dispositivo rifiuta i pacchetti dati in eccesso.

Il meccanismo di controllo di flusso descritto nella norma tecnica IEEE 802.3 contribuisce a garantire che nessun pacchetto dati vada 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 connessi 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.

Poi i dispositivi connessi non inviano più alcun pacchetto dati per tutto il tempo necessario alla segnalazione. Sulle porte uplink, ciò può eventualmente causare interruzioni indesiderate dell'invio nel segmento di rete di livello superiore (“wandering backpressure”).

Configuration

MAC address

Mostra l'indirizzo MAC del dispositivo.

Aging time [s]

Specifica l'aging time in secondi.

Possibili valori:

- `10..500000` (impostazione di default: `30`)

Il dispositivo monitora l'età degli indirizzi MAC unicast appresi. Il dispositivo cancella le voci degli indirizzi che superano una particolare età (aging time) dalla sua tabella indirizzi.

La tabella indirizzi si trova nella finestra di dialogo *Switching > Filter for MAC Addresses*.

Flow control

Attiva/disattiva il controllo di flusso nel dispositivo.

Possibili valori:

- `selezionato`
  Il controllo di flusso è attivo nel dispositivo.
  Attivare ulteriormente il controllo di flusso sulle porte richieste. Vedere finestra di dialogo *Basic Settings > Port*, scheda *Configuration*, casella di spunta nella colonna *Flow control*.
- `non selezionato` (impostazione di default)
  Il controllo di flusso non è attivo nel dispositivo.

Se si utilizza una funzionalità di ridondanza, disattivare il controllo di flusso sulle porte interessate. Se il controllo di flusso e la funzionalità di ridondanza sono attive contemporaneamente, è possibile che la funzionalità di ridondanza operi in modo diverso dal previsto.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.2 Rate Limiter

[Switching > Rate Limiter]

Il dispositivo consente di limitare il traffico sulle porte al fine di contribuire a fornire un funzionamento stabile persino con un ampio volume di traffico. Se il traffico su una porta supera il valore di traffico inserito, il dispositivo rifiuta il traffico in eccesso su tale porta.

La funzione di limitatore del carico funziona solo sul Layer 2 ed è utilizzata per limitare gli effetti delle tempeste di pacchetti dati che inondano il dispositivo (generalmente i Broadcast).

La funzione di limitatore del carico ignora le informazioni del protocollo ai livelli superiori, come l'IP o il TCP.

Questa finestra di dialogo include le seguenti schede:
- [Ingress]
- [Egress]

[Ingress]

In questa scheda si abilita la funzione *Rate Limiter*. Questo valore di soglia specifica la massima quantità di traffico ricevuta dalla porta. Se il traffico su questa porta supera il valore di soglia, il dispositivo rifiuta il traffico in eccesso su questa porta.

Tabella

Port

Visualizza il numero di porta.

Threshold unit

Specifica l'unità per il valore di soglia:

Possibili valori:
- *percent* (impostazione di default)
  Specifica il valore di soglia come percentuale della velocità di trasmissione dati della porta.
- *pps*
  Specifica il valore di soglia nei pacchetti dati al secondo.

Broadcast mode

Attiva/disattiva la funzione di limitatore del carico per i pacchetti dati del broadcast ricevuti.

Possibili valori:
- `selezionato`
- `non selezionato` (impostazione di default)

Se il valore di soglia è superato, il dispositivo rifiuta i pacchetti dati del broadcast in eccesso su questa porta.

Broadcast threshold

Specifica il valore di soglia dei broadcast ricevuti su questa porta.

Possibili valori:

- `0..14880000` (impostazione di default: `0`)
  Il valore `0` disattiva la funzione di limitatore del carico su questa porta.
  - Se si seleziona il valore *`percent`* nella colonna *Threshold unit*, immettere un valore percentuale da `1` a `100`.
  - Se si seleziona il valore *`pps`* nella colonna *Threshold unit*, inserire un valore assoluto per la velocità di trasmissione dati.

Known multicast mode

Attiva/disattiva la funzione di limitatore del carico per i pacchetti dati multicast noti ricevuti.

Possibili valori:

- `selezionato`
- `non selezionato` (impostazione di default)

Se il valore di soglia è superato, il dispositivo rifiuta i pacchetti dati multicast in eccesso su questa porta.

Known multicast threshold

Specifica il valore di soglia per i multicast ricevuti su questa porta.

Possibili valori:

- `0..14880000` (impostazione di default: `0`)
  Il valore `0` disattiva la funzione di limitatore del carico su questa porta.
  - Se si seleziona il valore *`percent`* nella colonna *Threshold unit*, immettere un valore percentuale da `0` a `100`.
  - Se si seleziona il valore *`pps`* nella colonna *Threshold unit*, inserire un valore assoluto per la velocità di trasmissione dati.

Unknown frame mode

Attiva/disattiva la funzione di limitatore del carico per i pacchetti dati unicast e multicast ricevuti con un indirizzo di destinazione sconosciuto.

Possibili valori:

- `selezionato`
- `non selezionato` (impostazione di default)

Se il valore di soglia è superato, il dispositivo rifiuta i pacchetti dati unicast in eccesso su questa porta.

Unknown frame threshold

Specifica il valore di soglia degli unicast ricevuti su questa porta con un indirizzo di destinazione sconosciuto.

Possibili valori:

- `0..14880000` (impostazione di default: `0`)
  Il valore `0` disattiva la funzione di limitatore del carico su questa porta.
  - ☐ Se si seleziona il valore *`percent`* nella *Threshold unit*, immettere un valore percentuale da `0` a `100`.
  - ☐ Se si seleziona il valore *`pps`* nella colonna *Threshold unit*, inserire un valore assoluto per la velocità di trasmissione dati.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Egress]

In questa scheda si specifica la velocità di trasmissione in uscita sulla porta.

Tabella

Port

Visualizza il numero di porta.

Bandwidth [%]

Specifica la velocità di trasmissione in uscita.

Possibili valori:

- `0` (impostazione di default)
  La limitazione della larghezza di banda è disabilitata.
- `1..100`
  La limitazione della larghezza di banda è abilitata.
  Questo valore specifica la percentuale della velocità generale di connessione per la porta con incrementi dell'1%.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.3 Filter for MAC Addresses

[Switching > Filter for MAC Addresses]

Questa finestra di dialogo consente di visualizzare e modificare i filtri degli indirizzi per la tabella indirizzi. I filtri degli indirizzi specificano il metodo di inoltro dei pacchetti dati nel dispositivo in base all'indirizzo MAC di destinazione.

Ciascuna riga nella tabella rappresenta un filtro. Il dispositivo configura automaticamente i filtri. Il dispositivo consente di configurare ulteriori filtri manualmente.

Il dispositivo trasmette i pacchetti dati come segue:

- Quando la tabella comprende una voce per l'indirizzo di destinazione di un pacchetto dati, il dispositivo trasmette il pacchetto dati dalla porta di ricezione alla porta specificata nella voce della tabella.
- In assenza di voce della tabella per l'indirizzo di destinazione, il dispositivo trasmette il pacchetto dati dalla porta di ricezione a ogni altra porta.

Tabella

Per cancellare gli indirizzi MAC appresi dalla tabella indirizzi, fare clic sul pulsante *Reset MAC address table* della finestra di dialogo *Basic Settings > Restart*.

Address

Mostra l'indirizzo MAC di destinazione a cui si applica la voce della tabella.

VLAN ID

Mostra l'ID della VLAN a cui si applica la voce della tabella.

Il dispositivo apprende gli indirizzi MAC per ciascuna VLAN separatamente (apprendimento VLAN indipendente).

Status

Mostra il metodo di configurazione del filtro degli indirizzi utilizzato dal dispositivo.

Possibili valori:

- `learned`
  Filtro dell'indirizzo configurato automaticamente dal dispositivo in base ai pacchetti dati ricevuti.
- `permanent`
  Filtro dell'indirizzo configurato manualmente. Il filtro dell'indirizzo rimane configurato in modo permanente.
- `IGMP`
  Filtro dell'indirizzo configurato automaticamente da IGMP Snooping.
- `mgmt`
  Indirizzo MAC del dispositivo. Il filtro dell'indirizzo è protetto dalle modifiche.
- `MRP-MMRP`
  Filtro dell'indirizzo Multicast configurato automaticamente da MMRP.
- `GMRP`
  Filtro dell'indirizzo Multicast configurato automaticamente da GMRP.

<Numero di portar>

Mostra il metodo di trasmissione dei pacchetti dati utilizzato dalla porta corrispondente, che li indirizza all'indirizzo di destinazione adiacente.

Possibili valori:

- `-`
  La porta non trasmette alcun pacchetto dati all'indirizzo di destinazione.
- `learned`
  La porta trasmette i pacchetti dati all'indirizzo di destinazione. Il dispositivo ha creato il filtro automaticamente, in base ai pacchetti dati ricevuti.
- `IGMP learned`
  La porta trasmette i pacchetti dati all'indirizzo di destinazione. Il dispositivo ha creato il filtro automaticamente in base all'IGMP.
- `unicast static`
  La porta trasmette i pacchetti dati all'indirizzo di destinazione. Un utente ha creato il filtro.
- `multicast static`
  La porta trasmette i pacchetti dati all'indirizzo di destinazione. Un utente ha creato il filtro.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

- Nel campo *Address* si specifica l'indirizzo MAC di destinazione.
- Nel campo *VLAN ID* specificare l'ID della VLAN.
- Nel campo *Port* si specifica la porta.
  - Selezionare una porta se l'indirizzo MAC di destinazione è un indirizzo unicast.
  - Selezionare una o più porte se l'indirizzo MAC di destinazione è un indirizzo multicast.
  - Non selezionare alcuna porta per creare un filtro discard. Il dispositivo rifiuta i pacchetti con indirizzo MAC di destinazione specificato nella voce della tabella.

Reset MAC address table

Rimuove dalla tabella inoltri gli indirizzi MAC con valore `learned` nella colonna *Status*.

5.4 IGMP Snooping

[Switching > IGMP Snooping]

L'Internet Group Management Protocol (IGMP) è un protocollo per la gestione dinamica dei gruppi Multicast. Il protocollo descrive la distribuzione dei pacchetti dati Multicast tra router e dispositivi finali sul Layer 3.

Il dispositivo consente di utilizzare la funzione IGMP Snooping anche per avvalersi dei meccanismi IGMP sul Layer 2.

- Senza IGMP Snooping, il dispositivo trasmette i pacchetti dati Multicast a ogni porta.
- Con la funzione IGMP Snooping attivata, il dispositivo trasmette i pacchetti dati Multicast solo alle porte a cui si connettono i destinatari Multicast. Ciò riduce il carico di rete. Il dispositivo valuta i pacchetti dati IGMP trasmessi sul Layer 3 e utilizza le informazioni sul Layer 2.

Attivare la funzione IGMP Snooping solo quando si verificano le seguenti condizioni:

- Nella rete vi è un router Multicast che crea query IGMP (query periodiche).
- I dispositivi che partecipano all'IGMP Snooping inoltrano le query IGMP.

Il dispositivo connette i report IGMP alle voci nella sua tabella indirizzi. Quando un destinatario multicast si unisce a un gruppo multicast, il dispositivo crea una voce della tabella per questa porta nella finestra di dialogo*Switching > Filter for MAC Addresses*. Quando il destinatario multicast abbandona il gruppo multicast, il dispositivo rimuove la voce della tabella.

Il menu include le seguenti finestre di dialogo:

- IGMP Snooping Global
- IGMP Snooping Configuration
- IGMP Snooping Enhancements
- IGMP Snooping Querier
- IGMP Snooping Multicasts

5.4.1 IGMP Snooping Global

[Switching > IGMP Snooping > Global]

Questa finestra di dialogo consente di abilitare il protocollo *IGMP Snooping* nel dispositivo e di configurarlo, inoltre, per ciascuna porta e VLAN.

Operation

Operation

Abilita/disabilita la funzione *IGMP Snooping* nel dispositivo.

Possibili valori:

- `On`
  La funzione *IGMP Snooping* è abilitata nel dispositivo secondo la RFC 4541 (Considerazioni per Internet Group Management Protocol (IGMP) e Multicast Listener Discovery (MLD) switch di Snooping).
- `Off` (impostazione di default)
  La funzione *IGMP Snooping* è disabilitata nel dispositivo.
  Il dispositivo trasmette il report e la query ricevuta e lascia i pacchetti dati senza valutarli. I pacchetti dati ricevuti con un indirizzo di destinazione Multicast sono trasmessi dal dispositivo a ogni porta.

Information

Multicast control packets processed

Mostra il numero di pacchetti dati di controllo Multicast elaborati.

Questa statistica comprende i seguenti tipi di pacchetti:

- Report IGMP
- Query IGMP versione V1
- Query IGMP versione V2
- Query IGMP versione V3
- Query IGMP con una versione errata
- Pacchetti PIM o DVMRP

Il dispositivo utilizza i pacchetti dati di controllo Multicast per creare la tabella indirizzi per la trasmissione dei pacchetti dati Multicast.

Possibili valori:

- `0..2`^{31}`-1`

Per ripristinare le voci IGMP Snooping, compreso il contatore per i pacchetti dati di controllo multicast elaborati, si utilizza il pulsante *Reset IGMP snooping data* nella finestra di dialogo *Basic Settings* > Restart o il comando `clear igmp-snooping`.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset IGMP snooping counters

Rimuove le voci IGMP Snooping e ripristina il contatore nel frame *Information* a `0`.

5.4.2 IGMP Snooping Configuration

[Switching > IGMP Snooping > Configuration]

Questa finestra di dialogo consente di abilitare la funzione *IGMP Snooping* nel dispositivo e di configurarla, inoltre, per ciascuna porta e VLAN.

Questa finestra di dialogo include le seguenti schede:
- [VLAN ID]
- [Port]

[VLAN ID]

In questa scheda, si configura la funzione *IGMP Snooping* per ciascuna VLAN.

Tabella

VLAN ID

Mostra l'ID della VLAN a cui si applica la voce della tabella.

Active

Attiva/disattiva la funzione *IGMP Snooping* per questa VLAN.

Il prerequisito è che la funzione *IGMP Snooping* sia abilitata globalmente.

Possibili valori:
- `selezionato`
  IGMP Snooping è attivato per questa VLAN. La VLAN si è unita al flusso di dati Multicast.
- `non selezionato` (impostazione di default)
  IGMP Snooping è disattivato per questa VLAN. La VLAN ha lasciato il flusso di dati Multicast.

Group membership interval

Specifica il tempo in secondi in cui una VLAN di un gruppo Multicast dinamico rimane inserita nella tabella indirizzi quando il dispositivo non riceve più alcun pacchetto dati report dalla VLAN.

Specificare un valore maggiore del valore nella colonna *Max. response time*.

Possibili valori:
- `2..3600` (impostazione di default: `260`)

Max. response time

Specifica il tempo in secondi in cui i membri di un gruppo multicast rispondono a un pacchetto dati query. Per la loro risposta, i membri specificano un tempo casuale all'interno del “Response Time”. In questo modo, si contribuisce a evitare che i membri del gruppo multicast rispondano alla query contemporaneamente.

Specificare un valore inferiore al valore nella colonna *Group membership interval*.

Possibili valori:

- `1..25` (impostazione di default: `10`)

Fast leave admin mode

Attiva/disattiva la funzione Fast Leave per questa VLAN.

Possibili valori:

- `selezionato`
  Quando la funzione Fast Leave è attiva e il dispositivo riceve un messaggio IGMP Leave da un gruppo multicast, il dispositivo rimuove immediatamente la voce dalla propria tabella indirizzi.
- `non selezionato` (impostazione di default)
  Quando la funzione Fast Leave non è attiva, il dispositivo prima invia query basate sul MAC ai membri del gruppo multicast e rimuove una voce quando una VLAN non invia più messaggi di report.

MRP expiration time

Scadenza attuale del router Multicast. Specifica il tempo in secondi in cui i dispositivi aspettano una query su questa porta appartenente a una VLAN. Quando la porta non riceve un pacchetto dati query, il dispositivo rimuove la porta dall'elenco delle porte con router multicast connessi.

È possibile configurare questo parametro solo se la porta appartiene a una VLAN esistente.

Possibili valori:

- `0`
  timeout illimitato - nessuna scadenza
- `1..3600` (impostazione di default: `260`)

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Port]

In questa scheda si configura la funzione *IGMP Snooping* per ciascuna porta.

Tabella

Port

Visualizza il numero di porta.

Active

Attiva/disattiva la funzione *IGMP Snooping* per questa porta.

Il prerequisito è che la funzione *IGMP Snooping* sia abilitata globalmente.

Possibili valori:

- `selezionato`
  IGMP Snooping è attivo su questa porta. Il dispositivo comprende la porta nel flusso di dati multicast.
- `non selezionato` (impostazione di default)
  IGMP Snooping non è attivo su questa porta. La porta ha lasciato il flusso di dati multicast.

Group membership interval

Specifica il tempo in secondi in cui una porta di un gruppo multicast dinamico rimane inserita nella tabella indirizzi quando il dispositivo non riceve più alcun pacchetto dati report dalla porta.

Possibili valori:

- `2..3600` (impostazione di default: `260`)

Specificare il valore maggiore del valore nella colonna *Max. response time*.

Max. response time

Specifica il tempo in secondi in cui i membri di un gruppo multicast rispondono a un pacchetto dati query. Per la loro risposta, i membri specificano un tempo casuale all'interno del “Response Time”. In questo modo, si contribuisce a evitare che i membri del gruppo multicast rispondano alla query contemporaneamente.

Possibili valori:

- `1..25` (impostazione di default: `10`)

Specificare un valore inferiore al valore nella colonna *Group membership interval*.

MRP expiration time

Specifica la scadenza attuale del router Multicast. La scadenza MRP è il tempo in secondi che il dispositivo aspetta per ricevere un pacchetto query su questa porta. Quando la porta non riceve un pacchetto dati query, il dispositivo rimuove la porta dall'elenco delle porte con router multicast connessi.

Possibili valori:

- `0`
  timeout illimitato - nessuna scadenza
- `1..3600` (impostazione di default: `260`)

Fast leave admin mode

Attiva/disattiva la funzione Fast Leave per questa porta.

Possibili valori:

- `selezionato`
  Quando la funzione Fast Leave è attiva e il dispositivo riceve un messaggio IGMP Leave da un gruppo multicast, il dispositivo rimuove immediatamente la voce dalla propria tabella indirizzi.
- `non selezionato` (impostazione di default)
  Quando la funzione Fast Leave non è attiva, il dispositivo prima invia query basate sul MAC ai membri del gruppo multicast e rimuove una voce quando una porta non invia più messaggi di report.

Static query port

Attiva/disattiva la modalità *Static query port*.

Possibili valori:

- `selezionato`
  La modalità *Static query port* è attiva.
  La porta è una porta query statica nelle VLAN configurate.
  Se si utilizza la funzione *Redundant Coupling Protocol* e il dispositivo agisce da slave, non attivare la modalità *Static query port* per le porte sulla rete secondaria/sull'anello secondario.
- `non selezionato` (impostazione di default)
  La modalità *Static query port* non è attiva.
  La porta non è una porta query statica. Il dispositivo trasmette messaggi di report IGMP alla porta solo se riceve query IGMP.

VLAN IDs

Mostra l'ID delle VLAN a cui si applica la voce della tabella.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.4.3 IGMP Snooping Enhancements

[Switching > IGMP Snooping > Snooping Enhancements]

Questa finestra di dialogo consente di selezionare una porta per un VLAN-ID e di configurare la porta.

Tabella

VLAN ID

Mostra l'ID della VLAN a cui si applica la voce della tabella.

<Numero di portar>

Mostra per ogni configurazione VLAN nel dispositivo se la porta interessata è una porta query. Inoltre, il campo mostra se il dispositivo trasmette a questa porta ogni flusso Multicast presente nella VLAN.

Possibili valori:

- `-`
  La porta non è una porta query in questa VLAN.
- `L`= Learned
  Il dispositivo ha rilevato una porta come porta query in quanto la porta ha ricevuto query IGMP in questa VLAN. La porta non è una porta query configurata staticamente.
- `A`= Automatic
  La porta ha rilevato la porta come una porta query. Il prerequisito è che la porta sia configurata come *`Learn by LLDP`*.
- `S`= Static (impostazione manuale)
  Un utente ha specificato la porta come una porta query statica. Il dispositivo trasmette report IGMP solo alle porte su cui ha precedentemente ricevuto query IGMP, e alle porte query configurate staticamente.
  Per assegnare questo valore, eseguire i seguenti passaggi:
  - ☐ Aprire la finestra *Wizard*.
  - ☐ Nella finestra di dialogo *Configuration* selezionare la casella di spunta *`Static`*.
- `P`= Learn by LLDP (impostazione manuale)
  Un utente ha specificato la porta come *`Learn by LLDP`*.
  Con il Link Layer Discovery Protocol (LLDP), il dispositivo rileva Schneider Electric dispositivi connessi direttamente alla porta. Il dispositivo indica le porte query rilevate con `A`.
  Per assegnare questo valore, eseguire i seguenti passaggi:
  - ☐ Aprire la finestra *Wizard*.
  - ☐ Nella finestra di dialogo *Configuration* selezionare la casella di spunta *`Learn by LLDP`*.
- `F`= Forward All (impostazione manuale)
  Un utente ha specificato la porta di modo che il dispositivo trasmetta ogni flusso Multicast ricevuto nella VLAN a questa porta. Utilizzare queste impostazioni a fini diagnostici, per esempio.
  Per assegnare questo valore, eseguire i seguenti passaggi:
  - ☐ Aprire la finestra *Wizard*.
  - ☐ Nella finestra di dialogo *Configuration* selezionare la casella di spunta *`Forward all`*.

Display categories

Ottimizza la chiarezza del display. La tabella sottolinea le celle contenenti il valore specificato. Ciò aiuta ad analizzare e ordinare la tabella in base alle proprie esigenze.

- *Learned (L)*
  La tabella mostra le celle contenenti il valore `L` ed eventualmente ulteriori valori. Con le celle contenenti solo valori diversi da `L` , la tabella mostra l'icona “-”.
- *Static (S)*
  La tabella mostra le celle contenenti il valore `S` ed eventualmente ulteriori valori. Con le celle contenenti solo valori diversi da `S` , la tabella mostra l'icona “-”.
- *Automatic (A)*
  La tabella mostra le celle contenenti il valore `A` ed eventualmente ulteriori valori. Con le celle contenenti solo valori diversi da `A` , la tabella mostra l'icona “-”.
- *Learned by LLDP (P)*
  La tabella mostra le celle contenenti il valore `P` ed eventualmente ulteriori valori. Con le celle contenenti solo valori diversi da `P` , la tabella mostra l'icona “-”.
- *Forward all (F)*
  La tabella mostra le celle contenenti il valore `F` ed eventualmente ulteriori valori. Con le celle contenenti solo valori diversi da `F` , la tabella mostra l'icona “-”.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Wizard* che aiuta a selezionare e configurare le porte.

[Selection VLAN/Port (Wizard)]

Nella finestra di dialogo *Selection VLAN/Port* assegnare un ID VLAN alla porta.

Nella finestra di dialogo *Configuration* specificare le impostazioni per la porta.

Dopo aver chiuso la finestra *Wizard*, fare clic sul pulsante  per salvare le impostazioni.

[Selection VLAN/Port (Wizard) – Selection VLAN/Port]

VLAN ID

Selezionare l'ID della VLAN.

Possibili valori:

- `1..4042`

Port

Selezionare la porta.

Possibili valori:

- `<Numero di porta>`

[Selection VLAN/Port (Wizard) – Configuration]

VLAN ID

Mostra l'ID della VLAN selezionata.

Port

Mostra il numero della porta selezionata.

Static

Specifica la porta come porta query statica nelle VLAN configurate. Il dispositivo trasmette messaggi di report IGMP alle porte su cui riceve le query IGMP. Ciò consente inoltre di trasmettere messaggi di report IGMP ad altre porte selezionate (abilita) o a dispositivi connessi Schneider Electric (`Automatic`).

Learn by LLDP

Specifica la porta come *`Learn by LLDP`*. Consente al dispositivo di rilevare direttamente i dispositivi Schneider Electric connessi utilizzando l'LLDP e di acquisire le relative porte come porta query.

Forward all

Specifica la porta come *`Forward all`*. Con l'impostazione *`Forward all`*, il dispositivo trasmette a questa porta tutti i pacchetti dati con un indirizzo Multicast nel campo dell'indirizzo di destinazione.

5.4.4 IGMP Snooping Querier

[Switching > IGMP Snooping > Querier]

Il dispositivo consente di inviare un flusso Multicast solo a quelle porte a cui il destinatario Multicast è connesso.

Per stabilire a quali porte sono connessi i destinatari Multicast, il dispositivo invia pacchetti dati query alle porte a un intervallo definibile. Quando un destinatario Multicast è connesso, si unisce al flusso Multicast rispondendo al dispositivo con un pacchetto dati report.

Questa finestra di dialogo consente di configurare globalmente le impostazioni per la Snooping Querier e per le VLAN configurate.

Operation

Operation

Abilita/disabilita la funzione IGMP Querier nel dispositivo globalmente.

Possibili valori:

- *On*
- *Off* (impostazione di default)

Configuration

In questo frame si specificano le impostazioni per l'IGMP Snooping Querier per i pacchetti dati query generali.

Protocol version

Specifica la versione IGMP dei pacchetti dati query generali.

Possibili valori:

- 1
  IGMP v1
- 2 (impostazione di default)
  IGMP v2
- 3
  IGMP v3

Query interval [s]

Specifica il tempo in secondi dopo il quale il dispositivo genera pacchetti dati query generali alla ricezione dei pacchetti dati query dal router Multicast.

Possibili valori:

- `1..1800` (impostazione di default: `60`)

Expiry interval [s]

Specifica il tempo in secondi dopo il quale un querier attivo torna dallo stato passivo allo stato attivo nel caso in cui non abbia ricevuto alcun pacchetto query per un tempo superiore a quello qui specificato.

Possibili valori:

- `60..300` (impostazione di default: `125`)

Tabella

Nella tabella si specificano le impostazioni Snooping Querier per le VLAN configurate.

VLAN ID

Mostra l'ID della VLAN a cui si applica la voce della tabella.

Active

Attiva/disattiva la funzione IGMP Snooping Querier per questa VLAN.

Possibili valori:

- `selezionato`
  La funzione IGMP Snooping Querier è attiva per questa VLAN.
- `non selezionato` (impostazione di default)
  La funzione IGMP Snooping Querier non è attiva per questa VLAN.

Current state

Mostra se la Snooping Querier è attiva per questa VLAN.

Possibili valori:

- `selezionato`
  La Snooping Querier è attiva per questa VLAN.
- `non selezionato`
  La Snooping Querier non è attiva per questa VLAN.

Address

Specifica l'indirizzo IP che il dispositivo aggiunge come indirizzo sorgente nei pacchetti dati query generali generati. Si utilizza l'indirizzo del router multicast.

Possibili valori:

- Indirizzo IPv4 valido (impostazione di default: `0.0.0.0`)

Protocol version

Mostra la versione del protocollo IGMP dei pacchetti dati query generali.

Possibili valori:

- `1`
  IGMP v1
- `2`
  IGMP v2
- `3`
  IGMP v3

Max. response time

Mostra il tempo in secondi in cui i membri di un gruppo Multicast rispondono a un pacchetto dati query. Per la loro risposta, i membri specificano un tempo casuale all'interno del “Response Time”. Ciò impedisce che i membri del gruppo multicast rispondano alla query contemporaneamente.

Last querier address

Mostra l'indirizzo IP del router Multicast dal quale è stata inviata l'ultima query IGMP ricevuta.

Last querier version

Mostra la versione IGMP che il router Multicast ha utilizzato durante l'invio dell'ultima query IGMP ricevuta in questa VLAN.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.4.5 IGMP Snooping Multicasts

[Switching > IGMP Snooping > Multicasts]

Il dispositivo consente di specificare il metodo di trasmissione dei pacchetti dati con indirizzi Multicast sconosciuti: o il dispositivo rifiuta questi pacchetti dati, inondando con essi ogni porta, o li trasmette solo alle porte che precedentemente hanno ricevuto i pacchetti query.

Il dispositivo consente anche la trasmissione di pacchetti dati con indirizzi Multicast noti alle porte query.

Configuration

Unknown multicasts

Specifica come il dispositivo trasmette i pacchetti dati con indirizzi Multicast sconosciuti.

Possibili valori:

- *discard*
  Il dispositivo rifiuta i pacchetti dati con un indirizzo Multicast MAC/IP sconosciuto.
- *flood* (impostazione di default)
  Il dispositivo inoltra i pacchetti dati con un indirizzo multicast MAC/IP sconosciuto a tutte le porte.

Tabella

Nella tabella si specificano le impostazioni per i Multicast conosciuti per le VLAN configurate.

VLAN ID

Mostra l'ID della VLAN a cui si applica la voce della tabella.

Known multicasts

Specifica come il dispositivo trasmette i pacchetti dati con indirizzi Multicast noti.

Possibili valori:

- *send to query and registered ports*
  Il dispositivo inoltra i pacchetti dati con un indirizzo Multicast MAC/IP sconosciuto alle porte query e alle porte registrate.
- *send to registered ports* (impostazione di default)
  Il dispositivo inoltra i pacchetti dati con un indirizzo Multicast MAC/IP sconosciuto alle porte registrate.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.5 Time-Sensitive Networking

[Switching > TSN]

Il menu include le seguenti finestre di dialogo:

- TSN Configuration
- TSN Gate Control List

5.5.1 TSN Configuration

[Switching > TSN > Configuration]

In questa finestra si abilita la funzione *TSN* e si specificano le impostazioni sensibili al fattore tempo.

Il dispositivo supporta l'accodamento sensibile al fattore tempo definito in IEEE 802.1 Qbv. Questa funzionalità *TSN* consente alle porte che supportano TSN di trasmettere pacchetti dati di tutte le classi di traffico programmate relativamente a un ciclo definito nel Gate Control List. Il tag VLAN di un pacchetto Ethernet, o la priorità della porta in caso di pacchetto non taggato, contiene la priorità.

La funzionalità contribuisce a evitare latenza e perdite dovute a congestione per flussi di dati riservati. La sincronizzazione percisa dei cicli e degli stati del gate utilizzando IEEE1588 (PTP) consente una comunicazione priva di congestioni e a bassa latenza. Il prerequisito è che tutti i dispositivi della rete supportino IEEE 802.1 Qbv.

Nota: Diversamente dalla Command Line Interface, le impostazioni si confermano immediatamente facendo clic sul pulsante ☑.

Operation

Operation

Abilita/disabilita la funzione *TSN* nel dispositivo.

Possibili valori:

- *On*
  La funzione *TSN* è abilitata globalmente.
  Il dispositivo elabora i link local frame sulle porte che supportano TSN con la priorità della classe di traffico`6`. Di conseguenza, nella fase di inoltro i link local frame concorrono con altri pacchetti dati con livello di priorità uguale o superiore. Questa funzione interessa i seguenti tipi di frame:
  - RSTP
  - LLDP
  - IEEE 802.1AS
  - PTP Peer Delay
- *Off* (impostazione di default)
  La funzione *TSN* è disabilitata globalmente.
  Finché la funzione *TSN* è attiva su una porta, la porta utilizza i gate aperti `0,1,2,3,4,5,6,7`. Le impostazioni sono preconfigurate dal produttore.

Base time

Date
Time
[ns]

Specifica l'orario in cui il ciclo inizia relativamente all'ora UTC.

Il dispositivo converte il valore in scala di tempo PTP direttamente, senza considerare i secondi intercalari.

Possibili valori:

- `MM/GG/AA`
  Mese/Giorno/Anno
  (in base alle preferenze della lingua del browser dell'utente)
- `hh:mm:ss`
  Ora:Minuto:Secondo
- `0..999999999`
  Specifica l'offset di nanosecondi.

Nota: Se si specifica il tempo base nel futuro, il ciclo inizia tanti secondi prima quanti indicati nel campo *UTC offset [s]*. Vedere la finestra di dialogo *Time > PTP > Boundary Clock > Global*.

Configuration

Cycle time [ns]

Specifica la durata di un ciclo in nanosecondi.

Possibili valori:

- `50000..10000000` (impostazione di default: `1000000`)
  50 µs .. 10 ms

Tabella

Port

Visualizza il numero di porta.

Active

Attiva/disattiva la funzione *TSN* sulla porta.

Possibili valori:

- `selezionato`
  La funzione *TSN* è attiva sulla porta.
  Se si specifica il tempo base nel futuro, il ciclo inizia all'orario specificato nel frame *Base time*.
  Il prerequisito è che la funzione *PTP* sia abilitata e il dispositivo sia sincronizzato.
  Finché la funzione *TSN* è abilitata globalmente, la porta utilizza il ciclo specificato nella finestra di dialogo *Switching > TSN > Gate Control List > Configured*.
- `non selezionato` (impostazione di default)
  La funzione *TSN* non è attiva sulla porta.
  Finché la funzione *TSN* è abilitata globalmente, la porta utilizza i gate aperti `0,1,2,3,4,5,6,7`.

Port state

Visualizza lo stato del ciclo sulla porta.

Possibili valori:

- *running*
  Il ciclo è in corso.
  La porta utilizza il ciclo specificato nella finestra di dialogo *Switching > TSN > Gate Control List >* Configured.
- *waitForTimeSync*
  Il ciclo non è ancora iniziato.
  Il clock del dispositivo non è sincronizzato.
  Verificare la impostazioni *PTP*.
- *pending*
  Il ciclo non è ancora iniziato.
  Il tempo base è specificato nel futuro.
- *disabled*
  Il ciclo non è in corso.
  La funzione *TSN* non è attiva sulla porta.
  – Verificare le impostazioni nel frame *Operation*.
  – Verificare le impostazioni nella colonna *Active*.
  La porta utilizza gli stati del gate specificati nella colonna *Default gate states*.
- *error*
  Il ciclo non è in corso.
  È stato rilevato un errore.

Time of last activation

Visualizza la data e l'orario in cui le impostazioni orarie si sono attivate l'ultima volta.

Questa valore riguarda l'ora PTP.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.5.2 TSN Gate Control List

[Switching > TSN > Gate Control List]

Il menu include le seguenti finestre di dialogo:

- TSN Configured Gate Control List
- TSN Current Gate Control List

5.5.2.1 TSN Configured Gate Control List

[Switching > TSN > Gate Control List > Configured]

In questa finestra di dialogo si specificano le finestre temporali del ciclo per le porte che supportano TSN. Aggiungendo una voce di tabella si specificano i gate aperti e la durata della finestra temporale.

Nota: Diversamente dalla Command Line Interface, le impostazioni si confermano immediatamente facendo clic sul pulsante ☑.

Questa finestra di dialogo include le seguenti schede:
- Una scheda per ogni porta che supporta TSN.
  Il numero di porte che supportano TSN dipende dal dispositivo.

[<Numero di portar>]

Configuration

Status

Visualizza il template assegnato al Gate Control List.

Possibili valori:
- `-`
  Template assente. Nessuna voce è assegnata al Gate Control List.
- *`default 2 time slots`*
  Template con 3 voci:
  - La prima voce è la classe di traffico `7`.
  - La seconda voce è la classe di traffico da `6` a `0`.
  - La terza voce è una banda di guardia.
- *`default 3 time slots`*
  Template con 5 voci:
  - La prima voce è la classe di traffico `7`.
  - La seconda voce è una banda di guardia.
  - La terza voce è la classe di traffico `6`.
  - La quarta voce è la classe di traffico da `5` a `0`.
  - La quinta voce è una banda di guardia.
- <`any other template name`>
  Il template è stato assegnato utilizzando la Command Line Interface.

Template

Apre la finestra *Template* per assegnare un template differente al Gate Control List. Quando si seleziona un template differente e si fa clic sul pulsante *Ok*, il dispositivo sostiuisce le voci nella tabella.

Nell'elenco a discesa selezionare uno dei seguenti template:
- *`default 2 time slots`*
- *`default 3 time slots`*

Il dispositivo consente di assegnare template aggiuntivi utilizzando la Command Line Interface.

Delete

Rimuove il template assegnato al Gate Control List. In seguito, al Gate Control List non vengono assegnate ulteriori voci.

Tabella

Index

Visualizza il numero di indice della voce nel Gate Control List, che specifica l'ordine cronologico delle finestre temporali.

Gate states

Specifica i gate aperti nel caso in cui la funzione *TSN* sia attiva sulla porta.

- I pacchetti dati con classe di traffico assegnata a un gate selezionato sono selezionati per la trasmissione. Stato gate: OPEN.
- I pacchetti dati con classe di traffico assegnata a un gate non selezionato non sono selezionati per la trasmissione. Stato gate: CLOSED.

Possibili valori:

- `-` (impostazione di default)
  Nessun gate selezionato.
  Il dispositivo non apre nessun gate sulla porta durante l'elaborazione della finestra temporale.
  Nell'elenco a discesa deselezionare tutti i gate.
- `0..7`
  Il dispositivo apre i gate selezionati sulla porta durante l'elaborazione della finestra temporale.
  Nell'elenco a discesa selezionare uno o più gate.
  Assegnare le priorità della VLAN a una classe di traffico nella finestra di dialogo *Switching > QoS/ Priority > 802.1D/p Mapping*.

Interval [ns]

Specifica la durata della finestra temporale in nanosecondi.

Possibili valori:

- `1000..10000000`

Quando si specifica la durata delle finestre temporali considerare le seguenti condizioni:

- Una finestra temporale singola
  - Confermare che una finestra temporale è sufficientemente lunga per consentire alla porta di trasmettere il pacchetto dati più lungo previsto.
  - Confermare che una finestra temporale è inferiore o pari alla durata del ciclo.
- La somma delle finestre temporali specificata
  - Si raccomanda che la somma delle finestre temporali sia pari alla durata del ciclo.
  - Se la somma supera la durata del ciclo, le finestre temporali che si sovrappongono vengono rifiutate e il ciclo si riavvia.
  - Se la somma è inferiore alla durata del ciclo, l'intervallo dell'ultima finestra temporale viene esteso in modo da adeguarsi al ciclo.

Nota: Le divergenze tra le finestre temporali specificate e la durata del ciclo non sono evidenziate nella finestra di dialogo *Switching > TSN > Gate Control List > Current*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.5.2.2 TSN Current Gate Control List

[Switching > TSN > Gate Control List > Current]

In questa finestra di dialogo si monitorano le impostazioni attuali del ciclo per le porte che supportano TSN. Ogni voce di tabella rappresenta una finestra temporale specificata.

Se l'orario in cui inizia il ciclo (*Base time*) è nel futuro, i valori visualizzati sono differenti dai valori specificati nella finestra di dialogo *Switching > TSN > Gate Control List > Configured*.

Nella finestra di dialogo *Switching > TSN > Configuration*, la colonna *Port state* visualizza se il ciclo è in corso su una porta.

Questa finestra di dialogo include le seguenti schede:
- Una scheda per ogni porta che supporta TSN.
  Il numero di porte che supportano TSN dipende dal dispositivo.

[<Numero di portar>]

Tabella

Index

Visualizza il numero di indice della voce nel Gate Control List, che specifica l'ordine cronologico delle finestre temporali.

Gate states

Visualizza i gate aperti nel caso in cui la funzione *TSN* sia attiva sulla porta.

Interval [ns]

Visualizza la durata della finestra temporale in nanosecondi.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.6 MRP-IEEE

[Switching > MRP-IEEE]

L'emendamento IEEE 802.1ak alla norma tecnica IEEE 802.1Q ha introdotto il Multiple Registration Protocol (MRP) per sostituire il Generic Attribute Registration Protocol (GARP). La IEEE ha inoltre modificato e sostituito le applicazioni GARP, GARP Multicast Registration Protocol (GMRP) e GARP VLAN Registration Protocol (GVRP). Il Multiple MAC Registration Protocol (MMRP) e il Multiple VLAN Registration Protocol (MVRP) sostituiscono questi protocolli.

MRP-IEEE aiuta a limitare il traffico alle aree richieste della LAN. Per limitare il traffico, le applicazioni MRP-IEEE distribuiscono i valori degli attributi ai dispositivi MRP-IEEE partecipanti attraverso una LAN che registra e cancella l'appartenenza a un gruppo multicast e gli identificatori VLAN.

La registrazione dei partecipanti del gruppo consente di riservare risorse per il traffico specifico che attraversa una LAN. La definizione dei requisiti delle risorse regola il livello di traffico, permettendo ai dispositivi di determinare le risorse necessarie e provvede alla manutenzione dinamica delle risorse assegnate.

Il menu include le seguenti finestre di dialogo:
- MRP-IEEE Configuration
- MRP-IEEE Multiple MAC Registration Protocol
- MRP-IEEE Multiple VLAN Registration Protocol

5.6.1 MRP-IEEE Configuration

[Switching > MRP-IEEE > Configuration]

Questa finestra di dialogo consente di impostare i vari timer MRP. Mantenendo un rapporto tra i vari valori del timer, il protocollo funziona in modo efficiente e con minore probabilità di ritiri di attributi non necessari e di nuove registrazioni. I valori predefiniti del timer mantengono tali relazioni in maniera efficace.

Quando si riconfigurano i timer, mantenere le seguenti relazioni:
- Per consentire una nuova registrazione dopo un evento Leave o LeaveAll, anche in caso di messaggio perso, specificare il LeaveTime a: `≥ (2x JoinTime) + 60`.
- Per ridurre al minimo il volume di traffico di ricongiungimento generato a seguito di un evento LeaveAll, specificare il valore del timer LeaveAll maggiore del valore LeaveTime.

Tabella

Port

Visualizza il numero di porta.

Join time [1/100s]

Specifica il timer Join che controlla l'intervallo tra le opportunità di trasmissione applicate alla macchina di stato richiedente.

Possibili valori:
- `10..100` (impostazione di default: `20`)

Leave time [1/100s]

Specifica il timer Leave che controlla il periodo che la macchina di stato del Registrar attende nello stato Leave (LV) prima di passare allo stato Empty (MT).

Possibili valori:
- `20..600` (impostazione di default: `60`)

Leave all time [1/100s]

Specifica il timer LeaveAll che controlla la frequenza con cui la macchina di stato LeaveAll genera le PDU LeaveAll.

Possibili valori:
- `200..6000` (impostazione di default: `1000`)

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.6.2 MRP-IEEE Multiple MAC Registration Protocol

[Switching > MRP-IEEE > MMRP]

Il Multiple MAC Registration Protocol (MMRP) consente la registrazione e la cancellazione delle informazioni degli indirizzi MAC individuali e dei gruppi di appartenenza da dispositivi finali e switch MAC con switch situati nella stessa LAN. Gli switch all'interno della LAN diffondono le informazioni attraverso switch che supportano servizi di filtraggio esteso. Utilizzando le informazioni dell'indirizzo MAC, l'MMRP consente di limitare il traffico multicast alle aree richieste di una rete di Layer 2.

Per un esempio di come funziona l'MMRP, si consideri una telecamera di sicurezza montata su un traliccio che si affaccia su un edificio. La telecamera invia pacchetti multicast su una LAN. Vi sono 2 dispositivi finali installati per la sorveglianza in luoghi separati. Si registrano gli indirizzi MAC della telecamera e dei 2 dispositivi finali nello stesso gruppo multicast. Si specificano successivamente le impostazioni dell'MMRP sulle porte per inviare i pacchetti del gruppo multicast ai 2 dispositivi finali.

Questa finestra di dialogo include le seguenti schede:
- [Configuration]
- [Service requirement]
- [Statistics]

[Configuration]

In questa scheda si selezionano i partecipanti attivi della porta MMRP e si imposta il dispositivo per trasmettere eventi periodici. La finestra di dialogo consente inoltre di abilitare la trasmissione dell'indirizzo MAC registrato VLAN.

Vi è una macchina di stato periodica per ciascuna porta, che trasmette regolarmente eventi periodici alle macchine di stato richiedenti associate alle porte attive. Gli eventi periodici comprendono informazioni che indicano lo stato dei dispositivi associati alla porta attiva.

Operation

Operation

Abilita/disabilita la funzione *MMRP* globale nel dispositivo. Il dispositivo partecipa agli scambi di messaggi MMRP.

Possibili valori:
- *On*
  Il dispositivo è un partecipante normale agli scambi di messaggi MMRP.
- *Off* (impostazione di default)
  Il dispositivo ignora i messaggi MMRP.

Configuration

Periodic state machine

Abilita/disabilita la macchina di stato periodica globale nel dispositivo.

Possibili valori:

- *On*
  Con *Operation* MMRP abilitato globalmente, il dispositivo trasmette messaggi MMRP a intervalli di un secondo sulle porte partecipanti all'MMRP.
- *Off* (impostazione di default)
  Disabilita la macchina di stato periodica nel dispositivo.

Tabella

Port

Visualizza il numero di porta.

Active

Attiva/disattiva la partecipazione MMRP della porta.

Possibili valori:

- selezionato (impostazione di default)
  Con l'MMRP abilitato globalmente e su questa porta, il dispositivo invia e riceve messaggi MMRP su questa porta.
- non selezionato
  Disabilita la partecipazione MMRP della porta.

Restricted group registration

Attiva/disattiva la restrizione della registrazione degli indirizzi MAC dinamici utilizzando MMRP sulla porta.

Possibili valori:

- selezionato
  Se è abilitato e vi è una voce del filtro statico per l'indirizzo MAC sulla VLAN interessata, il dispositivo registra in maniera dinamica gli attributi dell'indirizzo MAC.
- non selezionato (impostazione di default)
  Attiva/disattiva la restrizione della registrazione degli indirizzi MAC dinamici utilizzando MMRP sulla porta.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Service requirement]

Questa scheda comprende parametri di inoltro per ciascuna VLAN attiva, che specificano le porte su cui si applica l'inoltro multicast. Il dispositivo consente di configurare le porte VLAN in maniera statica come *Forward all* o Forbidden. Si configura in maniera statica il requisito del servizio MMRP Forbidden solo attraverso l'interfaccia grafica utente o la Command line interface (CLI).

Una porta è configurata solo come ForwardAll o Forbidden.

Tabella

VLAN ID

Mostra l'ID della VLAN.

<Numero di portar>

Specifica la gestione dei requisiti del servizio per la porta.

Possibili valori:

- FA
  Specifica le impostazioni del traffico ForwardAll sulla porta. Il dispositivo inoltra il traffico destinato agli indirizzi MAC multicast registrati MMRP sulla VLAN. Il dispositivo inoltra il traffico alle porte configurate in maniera dinamica dall'MMRP o alle porte configurate dall'amministratore in maniera statica come porte ForwardAll.
- F
  Specifica le impostazioni del traffico Forbidden sulla porta. Il dispositivo blocca i requisiti dinamici di servizio ForwardAll MMRP. Con le richieste ForwardAll bloccate su questa porta in questa VLAN, il dispositivo blocca il traffico destinato agli indirizzi MAC multicast registrati MMRP su questa porta. Inoltre, il dispositivo blocca la richiesta di servizio MMRP per la modifica di questo valore su questa porta.
- \- (impostazione di default)
  Disabilita le funzioni di inoltro su questa porta.
- Learned
  Mostra i valori impostati dalle richieste di servizio MMRP.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Statistics]

I dispositivi su uno scambio LAN Multiple MAC Registration Protocol Data Units (MMRPDU) manterranno lo stato dei dispositivi su una porta MMRP attiva. Questa scheda consente di monitorare le statistiche del traffico MMRP per ciascuna porta.

Information

Transmitted MMRP PDU

Mostra il numero di MMRPDU trasmesse nel dispositivo.

Received MMRP PDU

Mostra il numero di MMRPDU ricevute nel dispositivo.

Received bad header PDU

Mostra il numero di MMRPDU ricevute con una intestazione errata nel dispositivo.

Received bad format PDU

Mostra il numero di MMRPDU con un campo dei dati errato non trasmesse nel dispositivo.

Transmission failed

Mostra il numero di MMRPDU non trasmesse nel dispositivo.

Tabella

Port

Visualizza il numero di porta.

Transmitted MMRP PDU

Mostra il numero di MMRPDU trasmesse sulla porta.

Received MMRP PDU

Mostra il numero di MMRPDU ricevute sulla porta.

Received bad header PDU

Mostra il numero di MMRPDU con un'intestazione errata ricevute sulla porta.

Received bad format PDU

Mostra il numero di MMRPDU con un campo dei dati errato non trasmesse sulla porta.

Transmission failed

Mostra il numero di MMRPDU non trasmesse sulla porta.

Last received MAC address

Mostra l'indirizzo MAC più recente da cui la porta ha ricevuto MMRPPDU.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Ripristina i contatori statistici della porta e i valori nella colonna *Last received MAC address*.

5.6.3 MRP-IEEE Multiple VLAN Registration Protocol

[Switching > MRP-IEEE > MVRP]

Il Multiple VLAN Registration Protocol (MVRP) fornisce un meccanismo che consente di distribuire le informazioni VLAN e di configurare le VLAN in modo dinamico. Per esempio, quando si configura una VLAN su una porta MVRP attiva, il dispositivo distribuisce le informazioni VLAN ad altri dispositivi abilitati MVRP. Utilizzando le informazioni ricevute, un dispositivo abilitato MVRP crea in maniera dinamica i trunk VLAN su altri dispositivi abilitati MVRP in base alle proprie esigenze.

Questa finestra di dialogo include le seguenti schede:
- [Configuration]
- [Statistics]

[Configuration]

In questa scheda si selezionano i partecipanti attivi della porta MVRP e si imposta il dispositivo per trasmettere eventi periodici.

Vi è una macchina di stato periodica per ciascuna porta, che trasmette regolarmente eventi periodici alle macchine di stato richiedenti associate alle porte attive. Gli eventi periodici comprendono informazioni che indicano lo stato delle VLAN associate alla porta attiva. Utilizzando gli eventi periodici, gli switch abilitati MVRP mantengono le VLAN in maniera dinamica.

Operation

Operation

Abilita/disabilita il Controllo Amministrativo globale del Richiedente che specifica se la macchina di stato richiedente partecipa agli scambi di messaggi MMRP.

Possibili valori:

- *On*
  Partecipante normale. La macchina di stato richiedente partecipa agli scambi di messaggi MMRP.
- *Off* (impostazione di default)
  Non partecipante. La macchina di stato richiedente ignora i messaggi MMRP.

Configuration

Periodic state machine

Abilita/disabilita la macchina di stato periodica nel dispositivo.

Possibili valori:

- *On*
  La macchina di stato periodica è abilitata.
  Con *Operation* MVRP abilitato globalmente, il dispositivo trasmette gli eventi periodici MVRP, a intervalli di 1 secondo, sulle porte partecipanti MVRP.
- *Off* (impostazione di default)
  La macchina di stato periodica è disabilitata.
  Disabilita la macchina di stato periodica nel dispositivo.

Tabella

Port

Visualizza il numero di porta.

Active

Attiva/disattiva la partecipazione MVRP della porta.

Possibili valori:

- selezionato (impostazione di default)
  Con MVRP abilitato globalmente e su questa porta, il dispositivo distribuisce le informazioni di appartenenza VLAN ai dispositivi sensibili a MVRP connessi a questa porta.
- non selezionato
  Disabilita la partecipazione MVRP della porta.

Restricted VLAN registration

Attiva/disattiva la funzione *Restricted VLAN registration* su questa porta.

Possibili valori:

- selezionato
  Se abilitato e vi è una voce di registrazione VLAN statica, il dispositivo consente di creare una VLAN dinamica per questa voce.
- non selezionato (impostazione di default)
  Disabilita la funzione *Restricted VLAN registration* su questa porta.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Statistics]

I dispositivi su uno scambio LAN Multiple VLAN Registration Protocol Data Units (MVRPDU) manterranno lo stato delle VLAN sulle porte attive. Questa scheda consente di monitorare il traffico MVRP.

Information

Transmitted MVRP PDU

Mostra il numero di MVRPDU trasmesse nel dispositivo.

Received MVRP PDU

Mostra il numero di MVRPDU ricevute nel dispositivo.

Received bad header PDU

Mostra il numero di MVRPDU ricevute con un'intestazione errata nel dispositivo.

Received bad format PDU

Mostra il numero di MVRPDU con un campo dei dati errato bloccato dal dispositivo.

Transmission failed

Mostra il numero di guasti rilevati durante l'aggiunta di un messaggio all'interno della coda MVRP.

Message queue failures

Mostra il numero di MVRPDU bloccate dal dispositivo.

Tabella

Port

Visualizza il numero di porta.

Transmitted MVRP PDU

Mostra il numero di MVRPDU trasmesse sulla porta.

Received MVRP PDU

Mostra il numero di MVRPDU ricevute sulla porta.

Received bad header PDU

Mostra il numero di MVRPDU con un'intestazione errata ricevute dal dispositivo sulla porta.

Received bad format PDU

Mostra il numero di MVRPDU con un campo dei dati errato bloccato dal dispositivo sulla porta.

Transmission failed

Mostra il numero di MVRPDU bloccate dal dispositivo sulla porta.

Registrations failed

Mostra il numero di tentativi di registrazione non riusciti sulla porta.

Last received MAC address

Mostra l'ultimo indirizzo MAC da cui la porta ha ricevuto le MMRPDU.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Ripristina i contatori statistici della porta e i valori nella colonna *Last received MAC address*.

5.7 GARP

[Switching > GARP]

Il Generic Attribute Registration Protocol (GARP) è definito dallo IEEE per fornire un quadro generico di modo che gli switch possano registrare e cancellare i valori degli attributi, come gli identificatori VLAN e l'appartenenza a gruppi multicast.

Quando un attributo per un partecipante è registrato o cancellato in base al GARP, il partecipante è modificato secondo le regole specifiche. I partecipanti sono un insieme di dispositivi finali e dispositivi di rete raggiungibili. L'insieme definito dei partecipanti in un dato momento, insieme ai loro attributi, è l'albero di raggiungibilità per il sottoinsieme della topologia della 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.

Nota: Prima di abilitare la funzione *GMRP*, verificare che la funzione *MMRP* sia disabilitata.

Il menu include le seguenti finestre di dialogo:
- GMRP
- GVRP

5.7.1 GMRP

[Switching > GARP > GMRP]

Il GARP Multicast Registration Protocol (GMRP) è un Generic Attribute Registration Protocol (GARP) che fornisce un meccanismo che consente ai dispositivi di rete e ai dispositivi finali di registrare in maniera dinamica l'appartenenza al gruppo. I dispositivi registrano le informazioni di appartenenza al gruppo con i dispositivi connessi allo stesso segmento LAN. GARP consente inoltre ai dispositivi di distribuire le informazioni tra i dispositivi di rete che supportano servizi di filtraggio estesi.

Il GMRP e il GARP sono protocolli standard del settore definiti dalla IEEE 802.1P.

Operation

Operation

Abilita/disabilita la funzione *GMRP* globale nel dispositivo. Il dispositivo partecipa agli scambi di messaggi GMRP.

Possibili valori:

- *On*
  GMRP è abilitato.
- *Off* (impostazione di default)
  Il dispositivo ignora i messaggi GMRP.

Multicasts

Unknown multicasts

Abilita/disabilita i dati multicast sconosciuti da diffondere o rifiutare.

Possibili valori:

- *discard*
  Il dispositivo rifiuta i dati multicast sconosciuti.
- *flood* (impostazione di default)
  Il dispositivo inoltra dati multicast sconosciuti a ogni porta.

Tabella

Port

Visualizza il numero di porta.

GMRP active

Attiva/disattiva la partecipazione *GMRP* della porta.

Il prerequisito è che la funzione *GMRP* sia abilitata globalmente.

Possibili valori:

- `selezionato` (impostazione di default)
  La partecipazione *GMRP* della porta è attiva.
- `non selezionato`
  La partecipazione *GMRP* della porte non è attiva.

Service requirement

Specifica le porte su cui si applica l'inoltro multicast.

Possibili valori:

- *`Forward all unregistered groups`* (impostazione di default)
  Il dispositivo inoltra i dati destinati agli indirizzi MAC multicast registrati *GMRP* sulla VLAN. Il dispositivo inoltra i dati ai gruppi non registrati.
- *`Forward all groups`*
  Il dispositivo inoltra i dati destinati a ogni gruppo, registrato e non registrato.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.7.2 GVRP

[Switching > GARP > GVRP]

Il GARP VLAN Registration Protocol (GVRP) o Generic VLAN Registration Protocol è un protocollo che semplifica il controllo delle Virtual Local Area Network (VLAN) all'interno di una rete più grande. Il GVRP è un protocollo di rete di Layer 2, utilizzato per configurare automaticamente i dispositivi in una rete VLAN.

Il GVRP è un'applicazione GARP che fornisce potatura VLAN conforme alla IEEE 802.1Q e crea VLAN dinamiche su porte trunk 802.1Q. Con il GVRP, il dispositivo scambia le informazioni di configurazione della VLAN con altri dispositivi GVRP. Di conseguenza, il dispositivo riduce il traffico unicast sconosciuto e broadcast non necessario. Lo scambio delle informazioni di configurazione VLAN consente inoltre la gestione e la creazione dinamiche delle VLAN connesse attraverso porte trunk 802.1Q.

Operation

Operation

Abilita/disabilita la funzione *GVRP* globalmente nel dispositivo. Il dispositivo partecipa agli scambi di messaggi *GVRP*. Se la funzione è disabilitata, il dispositivo ignora i messaggi *GVRP*.

Possibili valori:

- `On`
  È abilitata la funzione *GVRP*.
- `Off` (impostazione di default)
  È disabilitata la funzione *GVRP*.

Tabella

Port

Visualizza il numero di porta.

GVRP active

Attiva/disattiva la partecipazione *GVRP* della porta.

Il prerequisito è che la funzione *GVRP* sia abilitata globalmente.

Possibili valori:

- `selezionato` (impostazione di default)
  La partecipazione *GVRP* della porta è attiva.
- `non selezionato`
  La partecipazione *GVRP* della porte non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.8 QoS/Priority

[Switching > QoS/Priority]

Le reti di comunicazione trasmettono in contemporanea un certo numero di applicazioni dotate di requisiti diversi in relazione a disponibilità, larghezza di banda e periodi di latenza.

La QoS (Quality of Service) è una procedura definita nella IEEE 802.1D. È utilizzata per distribuire risorse nella rete. È pertanto possibile fornire una larghezza di banda minima per le applicazioni necessarie. Il prerequisito è che i dispositivi finali e i dispositivi nella rete supportino la trasmissione dati prioritaria. I pacchetti dati con elevata priorità sono preferiti quando trasmessi dai dispositivi nella rete. Si trasferiscono pacchetti dati con priorità inferiore in assenza di pacchetti dati con priorità superiore da trasmettere.

Il dispositivo fornisce le seguenti opzioni di impostazione:
- Si specifica come il dispositivo valuti le informazioni di priorizzazione/QoS per pacchetti dati in entrata.
- Per i pacchetti in uscita, si specificano le informazioni di priorizzazione/QoS che il dispositivo scrive nel pacchetto dati (per esempio la priorità per i pacchetti di gestione, priorità della porta).

Nota: Se si utilizzano le funzioni in questo menù, disabilitare il controllo di flusso. Il controllo di flusso non è attivo se nella finestra di dialogo *Switching > Global*, frame *Configuration* la casella di spunta *Flow control* è `non selezionata`.

Il menu include le seguenti finestre di dialogo:
- QoS/Priority Global
- QoS/Priority Port Configuration
- 802.1D/p Mapping
- IP DSCP Mapping
- Queue Management

5.8.1 QoS/Priority Global

[Switching > QoS/Priority > Global]

Il dispositivo consente di mantenere l'accesso alla gestione del dispositivo, anche in situazioni di forte utilizzo. In questa finestra di dialogo si specificano le impostazioni di priorità/QoS richieste.

Configuration

VLAN priority for management packets

Specifica la priorità della VLAN per l'invio dei pacchetti dati di gestione. A seconda della priorità della VLAN il dispositivo assegna il pacchetto dati a una classe di traffico specifica e pertanto a una coda di priorità specifica della porta.

Possibili valori:

- `0..7` (impostazione di default: `0`)

Nella finestra di dialogo *Switching > QoS/Priority > 802.1D/p Mapping*, si assegna una classe di traffico a ogni priorità della VLAN.

IP DSCP value for management packets

Specifica il valore IP DSCP per l'invio dei pacchetti dati di gestione. A seconda del valore IP DSCP, il dispositivo assegna il pacchetto dati a una classe di traffico specifica e pertanto a una coda di priorità specifica della porta.

Possibili valori:

- *`0 (be/cs0)..63`* (impostazione di default: *`0 (be/cs0)`*)

Alcuni valori nell'elenco dispongono inoltre di una parola chiave DSCP, per esempio *`0 (be/cs0)`*, *`10 (af11)`* e *`46 (ef)`*. Tali valori sono compatibili con il modello IP Precedence.

Nella finestra di dialogo *Switching > QoS/Priority > IP DSCP Mapping* si assegna una classe di traffico a ogni valore IP DSCP.

Queues per port

Mostra il numero delle code di priorità per porta.

Il dispositivo dispone di 8 code di priorità per porta. Si assegna ogni coda di priorità a una classe di traffico specifica (classe di traffico secondo la IEEE 802.1D).

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.8.2 QoS/Priority Port Configuration

[Switching > QoS/Priority > Port Configuration]

In questa finestra di dialogo, si specifica, per ogni porta, come il dispositivo elabori i pacchetti dati ricevuti in base alle loro informazioni di priorità/QoS.

Tabella

Port

Visualizza il numero di porta.

Port priority

Specifica quali informazioni di priorità della VLAN vengono scritte dal dispositivo all'interno del pacchetto dati se il pacchetto dati non comprende alcuna informazione di priorità. In seguito, il dispositivo trasmette il pacchetto dati in base al valore specificato nella colonna *Trust mode*.

Possibili valori:

- `0..7` (impostazione di default: `0`)

Trust mode

Specifica come il dispositivo gestisce un pacchetto dati ricevuto se il pacchetto dati comprende informazioni di priorità/QoS.

Possibili valori:

- *untrusted*
  Il dispositivo trasmette il pacchetto dati in base alla priorità specificata nella colonna *Port priority*.
  Il dispositivo ignora le informazioni di priorità comprese nel pacchetto dati.
  Nella finestra di dialogo *Switching > QoS/Priority > 802.1D/p Mapping*, si assegna una classe di traffico a ogni priorità della VLAN.
- *trustDot1p* (impostazione di default)
  Il dispositivo trasmette il pacchetto dati in base alle informazioni di priorità nel tag VLAN.
  Nella finestra di dialogo *Switching > QoS/Priority > 802.1D/p Mapping*, si assegna una classe di traffico a ogni priorità della VLAN.
- *trustIpDscp*
  - Se il pacchetto dati è un pacchetto IP, allora:
    Il dispositivo trasmette il pacchetto dati in base al valore IP DSCP compreso nel pacchetto dati.
    Nella finestra di dialogo *Switching > QoS/Priority > IP DSCP Mapping* si assegna una classe di traffico a ogni valore IP DSCP.
  - Se il pacchetto dati non è un pacchetto IP, allora:
    Il dispositivo trasmette il pacchetto dati in base alla priorità specificata nella colonna *Port priority*.
    Nella finestra di dialogo *Switching > QoS/Priority > 802.1D/p Mapping*, si assegna una classe di traffico a ogni priorità della VLAN.

Untrusted traffic class

Mostra la classe di traffico assegnata alle informazioni di priorità della VLAN specificate nella colonna *Port priority*. Nella finestra di dialogo *Switching > QoS/Priority > 802.1D/p Mapping*, si assegna una classe di traffico a ogni priorità della VLAN.

Possibili valori:

- `0..7`

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.8.3 802.1D/p Mapping

[Switching > QoS/Priority > 802.1D/p Mapping]

Il dispositivo trasmette pacchetti dati con un tag VLAN in base alle informazioni di priorità/QoS comprese con una priorità superiore o inferiore.

In questa finestra di dialogo, si assegna una classe di traffico a ogni priorità VLAN. Si assegnano le classi di traffico alle code di priorità delle porte.

Tabella

VLAN priority

Mostra la priorità della VLAN.

Traffic class

Specifica la classe di traffico assegnata alla priorità della VLAN.

Possibili valori:

- `0..7`
  `0` assegnata alla coda di priorità con la priorità più bassa.
  `7` assegnata alla coda di priorità con la priorità più alta.

Nota: Tra le altre cose, i meccanismi di ridondanza utilizzano la classe di traffico più alta. Di conseguenza, selezionare un'altra classe di traffico per i dati di applicazione.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Assegnazione di default della priorità della VLAN alle classi di traffico

Priorità VLAN	Classe di traffico	Descrizione del contenuto secondo la IEEE 802.1D
`0`	2	`Best Effort` Dati normali senza priorizzazione
`1`	0	`Background` Dati non sensibili al fattore tempo e servizi di background
`2`	1	`Standard` Dati normali
`3`	3	`Excellent Effort` Dati fondamentali
`4`	4	`Controlled Load` Dati sensibili al fattore tempo con elevata priorità

Priorità VLAN	Classe di traffico	Descrizione del contenuto secondo la IEEE 802.1D
5	5	Video Trasmissione video con ritardi e jitter inferiori a 100 ms
6	6	Voice Trasmissione vocale con ritardi e jitter inferiori a 10 millise-condi
7	7	Network Control Dati per la gestione della rete e meccanismi di ridondanza.

5.8.4 IP DSCP Mapping

[Switching > QoS/Priority > IP DSCP Mapping]

Il dispositivo trasmette i pacchetti dati IP secondo il valore DSCP compreso nel pacchetto dati con una priorità superiore o inferiore.

In questa finestra di dialogo si assegna una classe di traffico a ogni valore DSCP. Si assegnano le classi di traffico alle code di priorità delle porte.

Tabella

DSCP value

Mostra il valore DSCP.

Traffic class

Specifica la classe di traffico assegnata al valore DSCP.

Possibili valori:

- `0..7`
  `0` assegnata alla coda di priorità con la priorità più bassa.
  `7` assegnata alla coda di priorità con la priorità più alta.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Assegnazione di default dei valori DSCP alle classi di traffico

Valore DSCP	Nome DSCP	Classe di traffico
0	Best Effort /CS0	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4

Valore DSCP	Nome DSCP	Classe di traffico
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

5.8.5 Queue Management

[Switching > QoS/Priority > Queue Management]

Questa finestra di dialogo consente di abilitare e disabilitare la funzione *Strict priority* per le classi di traffico. Quando si disabilita la funzione *Strict priority*, il dispositivo elabora le code di priorità delle porte con “Weighted Fair Queuing”.

Vi è inoltre la possibilità di assegnare una larghezza di banda minima a ogni classe di traffico utilizzata dal dispositivo per elaborare le code di priorità con “Weighted Fair Queuing”.

Tabella

Traffic class

Mostra la classe di traffico.

Strict priority

Attiva/disattiva l'elaborazione della coda di priorità della porta con *Strict priority* per questa classe di traffico.

Possibili valori:

- `selezionato` (impostazione di default)
  L'elaborazione della coda di priorità della porta con *Strict priority* è attiva.
  - La porta inoltra solo i pacchetti dati presenti nella coda di priorità con la priorità più alta. Quando questa coda di priorità è vuota, la porta inoltra i pacchetti dati presenti nella coda di priorità con la priorità inferiore successiva.
  - La porta inoltra i pacchetti dati con una classe di traffico inferiore dopo che le code di priorità con una priorità superiore sono vuote. In situazioni sfavorevoli, la porta non invia questi pacchetti dati.
  - Quando si seleziona questa impostazione per una classe di traffico, il dispositivo abilita inoltre la funzione per le classi di traffico con una priorità superiore.
  - Utilizzare questa impostazione per applicazioni quali il VoIP o per video che richiedano il minor ritardo possibile.
- `non selezionato`
  L'elaborazione della coda di priorità della porta con *Strict priority* non è attiva. Il dispositivo utilizza “Weighted Fair Queuing”/“Weighted Round Robin” (WRR) per elaborare la coda di priorità della porta.
  - Il dispositivo assegna una larghezza di banda minima a ciascuna classe di traffico.
  - Anche in condizioni elevato carico di rete la porta trasmette pacchetti dati con una classe di traffico ridotta.
  - Quando si seleziona questa impostazione per una classe di traffico, il dispositivo disabilita inoltre la funzione per le classi di traffico con una priorità inferiore.

Min. bandwidth [%]

Specifica la larghezza di banda minima per questa classe di traffico quando il dispositivo elabora le code di priorità delle porte con “Weighted Fair Queuing”.

Possibili valori:

- `0..100` (impostazione di default: `0` = il dispositivo non riserva alcuna larghezza di banda per questa classe di traffico)

Il valore specificato in percentuale si riferisce alla larghezza di banda disponibile sulla porta. Quando si disabilita la funzione *Strict priority* per ogni classe di traffico, la larghezza di banda massima è disponibile sulla porta per “Weighted Fair Queuing”.

Il totale massimo delle larghezze di banda assegnate è pari al 100 %.

Max. bandwidth [%]

Specifica lo shaping rate a cui la classe di traffico trasmette i pacchetti (Queue Shaping).

Possibili valori:

- `0` (impostazione di default)
  Il dispositivo non riserva alcuna larghezza di banda per questa classe di traffico.
- `1..100`
  Il dispositivo si riserva la larghezza di banda specifica per questa classe di traffico. Il valore specificato in percentuale si riferisce alla larghezza di banda massima disponibile su questa porta.

Per esempio, l'utilizzo dello shaping della coda consente di limitare la velocità di una coda di priorità strict-high. La limitazione di una coda di priorità strict-high consente al dispositivo di elaborare anche code a bassa priorità. Per utilizzare lo shaping della coda, impostare la massima larghezza di banda per una coda particolare.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.9 VLAN

[Switching > VLAN]

Con la VLAN(Virtual Local Area Network) si distribuisce il traffico dati nella rete fisica alle sottoreti logiche. Ciò garantisce i seguenti vantaggi:

- Flessibilità elevata
  - Con la VLAN si distribuisce il traffico dati alle reti logiche nell'infrastruttura esistente. Senza VLAN sarebbe necessario avere ulteriori dispositivi e complicati cablaggi.
  - Con la VLAN si specificano i segmenti di rete a prescindere dalla posizione dei singoli dispositivi finali.

- Portata migliorata
  - Nelle VLAN è possibile trasferire i pacchetti dati in base alla priorità.
    Quando la priorità è alta, il dispositivo trasferisce i dati di una VLAN preferenzialmente, per esempio per le applicazioni sensibili al fattore tempo come le telefonate VoIP.
  - Quando i pacchetti dati e i broadcast sono distribuiti in segmenti di rete ridotti invece che in reti intere, il carico di rete è notevolmente ridotto.
- Sicurezza aumentata
  La distribuzione del traffico dati tra le singole reti logiche complica l'accesso indesiderato e rafforza il sistema contro attacchi come il MAC Flooding o il MAC Spoofing.

I dispositivi supportano VLAN “taggate” basate sui pacchetti secondo la norma tecnica IEEE 802.1Q. Il tagging VLAN nel pacchetto dati indica la VLAN a cui appartiene il pacchetto dati.

Il dispositivo trasmette i pacchetti dati taggati di una VLAN solo sulle porte assegnate alla stessa VLAN. Ciò riduce il carico di rete.

Il dispositivo apprende gli indirizzi MAC per ciascuna VLAN separatamente (apprendimento VLAN indipendente).

Il dispositivo dà priorità al flusso di dati ricevuto nella sequenza seguente:
- Voice VLAN
- VLAN basata su porta

Il menu include le seguenti finestre di dialogo:
- VLAN Global
- VLAN Configuration
- VLAN Port
- VLAN Voice

5.9.1 VLAN Global

[Switching > VLAN > Global]

Questa finestra di dialogo consente di vedere i parametri VLAN generali per il dispositivo.

Configuration

Max. VLAN ID

Massimo ID assegnabile a una VLAN.

Vedere la finestra di dialogo *Switching > VLAN > Configuration*.

VLANs (max.)

Mostra il numero massimo di VLAN possibile.

Vedere la finestra di dialogo *Switching > VLAN > Configuration*.

VLANs

Numero delle VLAN attualmente configurate nel dispositivo.

Vedere la finestra di dialogo *Switching > VLAN > Configuration*.

L'ID VLAN 1 è costantemente presente nel dispositivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Clear...

Ripristina le impostazioni VLAN del dispositivo sull'impostazione di default.

Si noti che, cambiando il VLAN-ID per la gestione del dispositivo nella finestra di dialogo *Basic Settings > Network*, si perderà la connessione al dispositivo.

5.9.2 VLAN Configuration

[Switching > VLAN > Configuration]

In questa finestra di dialogo si gestiscono le VLAN. Per configurare una VLAN creare un'ulteriore riga nella tabella. In essa si specifica, per ciascuna porta, se trasmette pacchetti dati della VLAN corrispondente e se i pacchetti dati comprendono un tag VLAN.

Si distingue tra le seguenti VLAN:
- L'utente configura le VLAN statiche.
- Il dispositivo configura automaticamente le VLAN dinamiche e le rimuove se i prerequisiti non valgono più.
  Per le seguenti funzioni, il dispositivo crea VLAN dinamiche:
  - *MRP*: se si assegna una VLAN inesistente alle porte ring, il dispositivo crea questa VLAN.
  - *MVRP*: il dispositivo crea una VLAN basata sui messaggi dei dispositivi adiacenti.

Tabella

VLAN ID

ID della VLAN.

Il dispositivo supporta fino a 128°VLAN in configurazione simultanea.

Possibili valori:
- `1..4042`

Status

Mostra il metodo di configurazione della VLAN.

Possibili valori:
- *`other`*
  VLAN `1`
  oppure
  Configurazione della VLAN attraverso la funzione *802.1X Port Authentication*. Vedere la finestra di dialogo *Network Security > 802.1X Port Authentication*.
- *`permanent`*
  VLAN configurata dall'utente.
  oppure
  Configurazione della VLAN attraverso la funzione *MRP*. Vedere la finestra di dialogo *Switching* > L2-Redundancy > *MRP*.
  Se si salvano le modifiche nella memoria non volatile, le VLAN con queste impostazioni rimangono configurate dopo un riavvio.
- *`dynamicMvrp`*
  Configurazione della VLAN attraverso la funzione *MVRP*. Vedere la finestra di dialogo *Switching > MRP-IEEE > MVRP*.
  Le VLAN con questa impostazione sono protette da scrittura. Il dispositivo rimuove una VLAN dalla tabella non appena l'ultima porta abbandona la VLAN.

Creation time

Mostra l'orario di creazione della VLAN.

Il campo mostra la marca temporale per l'orario di funzionamento (tempo di attività del sistema).

Name

Specifica il nome della VLAN.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 1..32 caratteri

<Numero di portar>

Specifica se la porta corrispondente trasmette i pacchetti dati della VLAN e se i pacchetti dati comprendono un tag VLAN.

Possibili valori:

- `-` (impostazione di default)
  La porta non fa parte della VLAN e non trasmette pacchetti dati della VLAN.
- `T` = Tagged
  La porta fa parte della VLAN e trasmette pacchetti dati con un tag VLAN. Si utilizzano queste impostazioni per le porte Uplink, per esempio.
- `LT` = Tagged Learned
  La porta fa parte della VLAN e trasmette pacchetti dati con un tag VLAN.
  Il dispositivo ha creato la voce in maniera automatica in base alla funzione *GVRP* o *MVRP*.
- `F` = Forbidden
  La porta non fa parte della VLAN e non trasmette pacchetti dati di questa VLAN.
  Inoltre, il dispositivo contribuisce a impedire che la porta entri a far parte della VLAN attraverso la funzione *MVRP*.
- `U` = Untagged (impostazione di default per VLAN1)
  La porta fa parte della VLAN e trasmette i pacchetti dati senza un tag VLAN. Utilizzare questa impostazione se il dispositivo connesso non valuta alcun tag VLAN per esempio sulle porte dispositivi finali.
- `LU` = Untagged Learned
  La porta fa parte della VLAN e trasmette i pacchetti dati senza un tag VLAN.
  Il dispositivo ha creato la voce in maniera automatica in base alla funzione *GVRP* o *MVRP*.

Nota: Verificare che la porta a cui si collega la network management station faccia parte della VLAN in cui il dispositivo trasmette i dati di gestione. Nelle impostazioni di default, il dispositivo trasmette i dati di gestione sulla VLAN1. Altrimenti, il collegamento al dispositivo termina quando si trasferiscono le modifiche al dispositivo. L'accesso alla gestione del dispositivo è possibile solo utilizzando la Command Line Interface attraverso l'interfaccia seriale.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

Nel campo *VLAN ID* specificare l'ID della VLAN.

5.9.3 VLAN Port

[Switching > VLAN > Port]

In questa finestra di dialogo si specifica in che modo il dispositivo gestisce i pacchetti dati ricevuti che non dispongono di un tag VLAN o quelli il cui tag VLAN differisce dal VLAN-ID della porta.

Questa finestra di dialogo consente di assegnare una VLAN alle porte e pertanto di specificare il Port VLAN-ID.

Inoltre, si specifica il metodo di trasmissione dei pacchetti dati da parte del dispositivo per ciascuna porta e si verifica una delle seguenti situazioni:
- La porta riceve pacchetti dati senza un tagging VLAN.
- La porta riceve pacchetti dati con informazioni di priorità VLAN (VLAN-ID `0`, taggati per priorità).
- Il tagging VLAN del pacchetto dati differisce dal VLAN-ID della porta.

Tabella

Port

Visualizza il numero di porta.

Port-VLAN ID

Specifica l'ID della VLAN che il dispositivo assegna ai pacchetti dati senza un tag VLAN.

Prerequisiti:
- Nella colonna *Acceptable packet types*, specificare il valore `admitAll`.

Possibili valori:
- L'ID di una VLAN configurata (impostazione di default: `1`)

Se si utilizza la funzione *MRP* e non si è assegnata una VLAN alle porte ring, si specifica qui il valore `1` per le porte ring. Altrimenti, il dispositivo assegna automaticamente il valore alle porte ring.

Acceptable packet types

Specifica se la porta trasmette o rifiuta i pacchetti dati ricevuti senza un tag VLAN.

Possibili valori:
- `admitAll` (impostazione di default)
  La porta accetta pacchetti dati con e senza un tag VLAN.
- `admitOnlyVlanTagged`
  La porta accetta solo pacchetti dati taggati con un VLAN-ID ≥ `1`.

Ingress filtering

Attiva/disattiva il filtraggio in ingresso.

Possibili valori:

- `selezionato`
  Il filtraggio in ingresso è attivo.
  Il dispositivo confronta il VLAN-ID nel pacchetto dati con le VLAN di cui il dispositivo fa parte. Vedere la finestra di dialogo *Switching > VLAN > Configuration*. Se il VLAN-ID nel pacchetto dati corrisponde a una di queste VLAN, la porta trasmette il pacchetto dati. Altrimenti, il dispositivo rifiuta il pacchetto dati.
- `non selezionato` (impostazione di default)
  Il filtraggio in ingresso non è attivo.
  Il dispositivo trasmette i pacchetti dati ricevuti senza confrontare il VLAN-ID. Di conseguenza, la porta trasmette anche i pacchetti dati con un VLAN-ID di cui la porta non fa parte.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.9.4 VLAN Voice

[Switching > VLAN > Voice]

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 della Voice VLAN è la salvaguardia della qualità del traffico vocale quando il traffico dati sulla porta è elevato.

Il dispositivo rileva i telefoni VoIP utilizzando il Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED). Il dispositivo aggiunge poi la porta adatta all'insieme di membri della Voice VLAN configurata. L'insieme di membri è taggato o non taggato. Il tagging dipende dalla modalità dell'interfaccia Voice VLAN (VLAN-ID, Dot1p, nessuna, non taggata).

Un altro vantaggio della funzione Voice VLAN è che il telefono VoIP ottiene dal dispositivo un VLAN-ID o informazioni di priorità tramite LLDP-MED. Di conseguenza, il telefono VoIP invia dati vocali taggati come prioritari o non taggati. Ciò dipende dalla modalità dell'interfaccia Voice VLAN configurata. Si attiva la Voice VLAN sulla porta che si sta collegando al telefono VoIP.

Operation

Operation

Abilita/disabilita la funzione *VLAN Voice* del dispositivo globalmente.

Possibili valori:

- *On*
- *Off* (impostazione di default)

Tabella

Port

Visualizza il numero di porta.

Voice VLAN mode

Specifica se la porta trasmette o rifiuta i pacchetti dati ricevuti senza tagging Voice VLAN o con un'informazione di priorità della Voice VLAN.

Possibili valori:

- *disabled* (impostazione di default)
  Disattiva la funzione *VLAN Voice* per la voce di questa tabella.
- *none*
  Consente al telefono IP di utilizzare la propria configurazione per l'invio di traffico vocale non taggato.
- *vlan/dot1p-priority*
  La porta filtra i pacchetti dati sulla Voice VLAN utilizzando la VLAN e i tag di priorità dot1p.
- *untagged*
  La porta filtra pacchetti dati senza un tag Voice VLAN.

- *vlan*
  La porta filtra pacchetti dati della Voice VLAN utilizzando il tag VLAN.
- *dot1p-priority*
  La porta filtra pacchetti dati della Voice VLAN utilizzando i tag di priorità dot1p. Se si seleziona questo valore, si specifica ulteriormente un valore adeguato nella colonna *Priority*.

Data priority mode

Specifica la modalità trust per il traffico dati sulla porta in questione.

Il dispositivo utilizza questa modalità per il traffico dati sulla Voice VLAN quando rileva un telefono VoIP e un PC e quando tali dispositivi utilizzano lo stesso cavo per la trasmissione e la ricezione dei dati.

Possibili valori:

- *trust* (impostazione di default)
  Se il traffico vocale è presente sull'interfaccia, il traffico dati utilizza la priorità normale con questa impostazione.
- *untrust*
  Se il traffico vocale è presente e la *Voice VLAN mode* è impostata su *dot1p-priority*, i dati hanno la priorità 0. Se l'interfaccia trasmette solo dati, i dati hanno la priorità normale.

Status

Mostra lo stato della Voice VLAN sulla porta.

Possibili valori:

- selezionato
  La Voice VLAN è abilitata.
- non selezionato
  La Voice VLAN è disabilitata.

VLAN ID

Specifica l'ID della VLAN a cui si applica la voce della tabella.

Per inoltrare il traffico a questo VLAN-ID utilizzando questo filtro, selezionare il valore *vlan* nella colonna *Voice VLAN mode*.

Possibili valori:

- 0..4042

Priority

Specifica la priorità della Voice VLAN della porta.

Prerequisiti:

- Nella colonna *Voice VLAN mode*, specificare il valore *dot1p-priority*.

Possibili valori:

- *0..7*
- *none*
  Disattiva la priorità della Voice VLAN della porta.

Bypass authentication

Attiva la modalità di autenticazione della Voice VLAN.

Se si disattiva la funzione e si imposta il valore `dot1p-priority` nella colonna *Voice VLAN mode*, i dispositivi vocali richiedono un'autenticazione.

Possibili valori:

- `selezionato` (impostazione di default)
  Se è stata attivata la funzione nella finestra di dialogo *Network Security > 802.1X Port Authentication > Global*, impostare il parametro *Port control* per questa porta sul valore `multi-Client` prima di attivare questa funzione. Il parametro *Port control* si trova nella finestra di dialogo *Network Security > 802.1X Port Authentication > Global*.
- `non selezionato`

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.10 L2-Redundancy

[Switching > L2-Redundancy]

Il menu include le seguenti finestre di dialogo:

- MRP
- HIPER Ring
- Spanning Tree
- Link Aggregation
- Link Backup
- FuseNet

5.10.1 MRP

[Switching > L2-Redundancy > MRP]

⚠ 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 collegare le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione dell'anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Il Media Redundancy Protocol (MRP) è un protocollo che consente di configurare strutture di rete ad anello ad alta disponibilità. Un MRP ring con Schneider Electric dispositivi è composto da max 100 dispositivi che supportano il protocollo MRP conformemente alla IEC 62439.

In caso di una sezione non funzionante, la struttura dell'anello di un MRP ring cambia e torna a essere una struttura lineare. È possibile configurare il massimo tempo di ripristino.

La funzione Ring Manager del dispositivo chiude le estremità di un backbone in una struttura lineare formando un anello ridondante.

Nota: La *Spanning Tree* e la ridondanza ad anello hanno effetto l'una sull'altra. Disattivare il protocollo *Spanning Tree* per le porte connesse all'MRP ring. Vedere la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*.

Quando si lavora con pacchetti Ethernet sovradimensionati (il valore nella colonna *MTU* per le porte è > `1518`, vedi la finestra di dialogo *Basic Settings > Port*), il tempo di commutazione della riconfigurazione dell'MRP ring dipende dai seguenti parametri:
- Larghezza di banda della linea dell'anello
- Dimensioni dei pacchetti Ethernet
- Numero di dispositivi nell'anello

Impostare un tempo di ripristino sufficientemente ampio per contribuire a evitare ritardi nei pacchetti MRP dovuti a latenze nei dispositivi. La formula per calcolare il tempo di commutazione si trova nella IEC 62439-2, sezione 9.5.

Operation

Operation

Abilita/disabilita la funzione *MRP*.

Dopo aver configurato i parametri per l'MRP ring, abilitare la funzione qui.

Possibili valori:

- *On*
  È abilitata la funzione *MRP*.
  Dopo aver configurato i dispositivi nell'MRP ring, la ridondanza è attiva.
- *Off* (impostazione di default)
  È disabilitata la funzione *MRP*.

Ring port 1/Ring port 2

Port

Specifica il numero della porta che funziona come porta dell'anello.

Possibili valori:

- <Numero di porta>
  Numero della porta dell'anello

Operation

Mostra il modo operativo della porta dell'anello.

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.

Fixed backup

Attiva/disattiva la funzione della porta di backup per la *Ring port 2*.

Nota: La commutazione alla porta primaria può superare il massimo tempo di ripristino dell'anello.

Possibili valori:

- selezionato
  La funzione di backup *Ring port 2* è attiva. Quando l'anello è chiuso, il Ring Manager torna alla porta dell'anello primaria.
- non selezionato (impostazione di default)
  La funzione di backup *Ring port 2* non è attiva. Quando l'anello è chiuso, il Ring Manager continua a inviare dati alla porta dell'anello secondaria.

Configuration

Ring manager

Abilita/disabilita la funzione *Ring manager*.

Se vi è un dispositivo a ciascuna estremità della linea, si attiva questa funzione.

Possibili valori:

- *On*
  È abilitata la funzione *Ring manager*.
  Il dispositivo funziona come un Ring Manager.
- *Off* (impostazione di default)
  È disabilitata la funzione *Ring manager*.
  Il dispositivo funziona come ring client.

Advanced mode

Attiva/disattiva la modalità avanzata per tempi di ripristino rapidi.

Possibili valori:

- `selezionato` (impostazione di default)
  Modalità avanzata attiva.
  I dispositivi Schneider Electric compatibili con l'MRP supportano questa modalità.
- `non selezionato`
  Modalità avanzata non attiva.
  Selezionare queste impostazioni se un altro dispositivo nell'anello non supporta questa modalità.

Ring recovery

Specifica il massimo tempo di ripristino in millisecondi per la riconfigurazione dell'anello. Queste impostazioni sono efficaci se il dispositivo funziona come un Ring Manager.

Possibili valori:

- *500ms*
- *200ms* (impostazione di default)

Tempi di commutazione inferiori richiedono tempi di risposta maggiori per ogni singolo dispositivo nell'anello. Utilizzare valori inferiori a *500ms* se gli altri dispositivi nell'anello supportano anche questo tempo di ripristino inferiore.

Quando si lavora con pacchetti Ethernet sovradimensionati, il numero di dispositivi nell'anello è limitato. Si noti che il tempo di commutazione dipende da diversi parametri. Vedere la descrizione fornita sopra.

VLAN ID

Specifica l'ID della VLAN che si assegna alle porte ring.

Possibili valori:

- `0` (impostazione di default)
  Nessuna VLAN assegnata.
  Assegnare alle porte ring il valore *Switching > VLAN > Configuration* per VLAN`1` nella finestra di dialogo `U`.
- `1..4042`
  VLAN assegnata.
  Se si assegna una VLAN inesistente alle porte ring, il dispositivo crea questa VLAN. Nella finestra di dialogo *Switching > VLAN > Configuration*, il dispositivo crea una voce nella tabella per la VLAN e assegna il valore `T` alle porte ring.

Information

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 è presente un altro dispositivo che funziona come Ring Manager.
  Abilita 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 diversa porta invece che con una porta dell'anello. Il dispositivo riceve solo pacchetti dati di test su una Ring port.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Delete ring configuration

Disabilita la funzionalità di ridondanza e ripristina le impostazioni nella finestra di dialogo sulle impostazioni di default.

5.10.2 HIPER Ring

[Switching > L2-Redundancy > 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 collegare le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione dell'anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Il principio della ridondanza ad anello HIPER consente la costruzione di reti ad anello ad alta disponibilità. Questo dispositivo fornisce un client dell'HIPER ring. Questa funzione consente di espandere un HIPER ring esistente o di sostituire un dispositivo che partecipa già in qualità di client in un HIPER ring.

Un HIPER ring comprende un Ring Manager (RM) che controlla l'anello. L'RM invia pacchetti watchdog nell'anello sulle porte primarie e secondarie. Quando l'RM riceve i pacchetti watchdog su entrambe le porte, la porta primaria rimane in stato di inoltro e la porta secondaria rimane in stato di rifiuto.

Il dispositivo funziona solo nella modalità ring client. Ciò significa che il dispositivo è in grado di riconoscere e inoltrare i pacchetti watchdog sulle porte ring e che può anche inoltrare la modifica dello stato di connessione all'RM, per esempio, pacchetti LinkDown e LinkUp.

Il dispositivo supporta solo porte Fast Ethernet e Gigabit Ethernet come porte ring. Inoltre, il dispositivo supporta solo HIPER ring nella VLAN `1`.

Nota: La *Spanning Tree* e la ridondanza ad anello hanno effetto l'una sull'altra. Disattivare il protocollo *Spanning Tree* per le porte connesse all'HIPER ring. Vedere la finestra di dialogo *Switching* > L2-Redundancy > *Spanning Tree* > *Port*.

Nota: Configurare i dispositivi dell'HIPER ring individualmente. Prima di eseguire il collegamento ridondante, completare la configurazione di tutti i dispositivi dell'HIPER ring. In questo modo si contribuisce a evitare la formazione di loop durante la configurazione.

Operation

Operation

Abilita/disabilita il client *HIPER Ring*.

Possibili valori:

- `On`
  Il client *HIPER Ring* è abilitato.
- `Off` (impostazione di default)
  Il client *HIPER Ring* è disabilitato.

Ring port 1/Ring port 2

Port

Specifica il numero di porta della porta dell'anello primaria/secondaria.

Possibili valori:

- `-` (impostazione di default)
  Nessuna porta dell'anello primaria/secondaria selezionata.
- `<Numero di porta>`
  Numero della porta dell'anello

State

Mostra lo stato della porta dell'anello primaria/secondaria.

Possibili valori:

- *`not-available`*
  Il client *HIPER Ring* è disabilitato.
  oppure
  Nessuna porta dell'anello primaria o secondaria selezionata.
- *`active`*
  La porta dell'anello è abilitata e funziona in maniera logica.
- *`inactive`*
  La porta dell'anello non è attiva in maniera logica.
  Non appena il collegamento si interrompe su una porta dell'anello, il dispositivo invia un pacchetto LinkDown al Ring Manager sull'altra porta dell'anello.

Information

Mode

Mostra la capacità del dispositivo di funzionare nella modalità client dell'anello.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.10.3 Spanning Tree

[Switching > L2-Redundancy > Spanning Tree]

⚠ 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.

Lo Spanning Tree Protocol (STP) è un protocollo che disattiva i percorsi ridondanti di una rete al fine di contribuire a evitare la formazione di loop. Se un componente di rete diventa inutilizzabile lungo il percorso, il dispositivo calcola la nuova topologia e attiva nuovamente questi percorsi.

Lo Rapid Spanning Tree Protocol (RSTP) abilita il passaggio rapido a una topologia ricalcolata senza interrompere i collegamenti esistenti. L'RSTP ottiene tempi medi di riconfigurazione inferiori a un secondo. Quando si utilizza l'RSTP in un anello contenente tra i 10 e i 20 dispositivi, è possibile ottenere tempi di riconfigurazione nell'ordine dei millisecondi.

Nota: Quando si collega il dispositivo alla rete attraverso twisted pair SFP invece che attraverso le normali porte twisted pair, la riconfigurazione della rete richiede più tempo.

Il menu include le seguenti finestre di dialogo:
- Spanning Tree Global
- Spanning Tree Dual RSTP (MCSESM-E)
- Spanning Tree Port

5.10.3.1 Spanning Tree Global

[Switching > L2-Redundancy > Spanning Tree > Global]

In questa finestra di dialogo si abilita/disabilita la funzione *Spanning Tree* e si specificano le impostazioni dello switch.

Operation

Operation

Abilita/disabilita la funzione Spanning Tree nel dispositivo.

Possibili valori:

- *On* (impostazione di default)
- *Off*
  Il dispositivo si comporta in maniera trasparente. Il dispositivo inonda le porte con i pacchetti dati Spanning Tree ricevuti come i pacchetti dati multicast.

Variant

Variant

Mostra il protocollo utilizzato per la funzione *Spanning Tree*:

Possibili valori:

- *rstp*
  Il protocollo RSTP è attivo.
  Con l'RSTP (IEEE 802.1Q-2005), la funzione *Spanning Tree* opera per il layer fisico sottostante.

Traps

Send trap

Attiva/disattiva l'invio delle SNMP trap per gli eventi seguenti:

- Un altro switch assume il ruolo di root switch.
- Le modifiche della topologia. Una porta modifica la sua *Port state* da *forwarding* a *discarding* o da *discarding* a *forwarding*.

Possibili valori:

- selezionato
  L'invio di trap SNMP è attivo.
- non selezionato (impostazione di default)
  L'invio di trap SNMP non è attivo.

Bridge configuration

Bridge ID

Mostra lo switch ID del dispositivo.

Il dispositivo con il valore numerico switch ID più basso assume il ruolo di root switch nella rete.

Possibili valori:

- `<Priorità Switch> / <Indirizzo MAC>`
  Valore nel campo *Priority* / indirizzo MAC del dispositivo

Priority

Specifica la priorità dello switch del dispositivo.

Possibili valori:

- `0..61440` a passi di 4096 (impostazione di default: `32768`)

Per rendere questo dispositivo il root switch, assegnare al dispositivo il valore di priorità numerico più basso nella rete.

Hello time [s]

Specifica il tempo in secondi tra l'invio di due messaggi di configurazione (pacchetti dati Hello).

Possibili valori:

- `1..2` (impostazione di default: `2`)

Se il dispositivo assume il ruolo di root switch, gli altri dispositivi nella rete utilizzano il valore qui specificato.

Altrimenti, il dispositivo utilizza il valore specificato dal root switch. Vedere il frame *Root information*.

Per via dell'interazione con il parametro *Tx holds*, si consiglia di non modificare l'impostazione di default.

Forward delay [s]

Specifica il tempo di ritardo in secondi per la modifica dello stato.

Possibili valori:

- `4..30` (impostazione di default: `15`)

Se il dispositivo assume il ruolo di root switch, gli altri dispositivi nella rete utilizzano il valore qui specificato.

Altrimenti, il dispositivo utilizza il valore specificato dal root switch. Vedere il frame *Root information*.

Nel protocollo RSTP, gli switch negoziano una modifica dello stato senza un ritardo specificato.

Il protocollo *Spanning Tree* utilizza il parametro per posticipare la modifica dello stato tra gli stati *disabled*, *discarding*, *learning*, *forwarding*.

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.

Max age

Specifica la lunghezza massima del ramo consentita, per esempio, il numero di dispositivi fino al root switch.

Possibili valori:

- `6..40` (impostazione di default: `20`)

Se il dispositivo assume il ruolo di root switch, gli altri dispositivi nella rete utilizzano il valore qui specificato.

Altrimenti, il dispositivo utilizza il valore specificato dal root switch. Vedere il frame *Root information*.

Il protocollo *Spanning Tree* utilizza il parametro per specificare la validità delle STP-BPDU in secondi.

Tx holds

Limita la velocità massima di trasmissione per l'invio di BPDU.

Possibili valori:

- `1..40` (impostazione di default: `10`)

Quando il dispositivo invia una BPDU, il dispositivo incrementa il valore di un contatore su questa porta.

Se il contatore raggiunge il valore qui specificato, la porta smette di inviare BPDU. Da un lato, questo riduce il carico generato dall'RSTP e, dall'altro, quando il dispositivo non riceve BPDU, si può verificare un'interruzione della comunicazione.

Il dispositivo riduce il valore del contatore di `1` al secondo. Nel secondo seguente, il dispositivo invia un massimo di `1` nuove BPDU.

BPDU guard

Attiva/disattiva la funzione BPDU Guard nel dispositivo.

Con questa funzione, il dispositivo aiuta a proteggere la rete da configurazioni errate, attacchi tramite STP-BPDU, e modifiche indesiderate della topologia.

Possibili valori:

- `selezionato`
  La *BPDU guard* è attiva.
  - Il dispositivo applica la funzione a porte edge specificate manualmente. Per queste porte, nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, scheda *CIST*, la casella di spunta nella colonna *Admin edge port* è selezionata.
  - Se una porta edge riceve una STP-BPDU, il dispositivo disabilita la porta. Per questa porta, nella finestra di dialogo *Basic Settings > Port*, scheda *Configuration*, la casella di spunta nella colonna *Port on* è `non selezionata`.
- `non selezionato` (impostazione di default)
  La *BPDU guard* non è attiva.

Per ripristinare lo stato della porta sul valore `forwarding`, si procede come segue:

- ☐ Se la porta riceve ancora BPDU, allora:
  - Nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, scheda *CIST*, deselezionare la casella di spunta nella colonna *Admin edge port*.
    oppure
  - Nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*, deselezionare la casella di spunta *BPDU guard*.
- ☐ Per abilitare nuovamente la porta si utilizza la funzione *Auto-Disable*. In alternativa, procedere come segue:
  - Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
  - Contrassegnare la casella di spunta nella colonna *Port on*.

BPDU filter (all admin edge ports)

Attiva/disattiva il filtro STP-BPDU su ogni porta edge specificata manualmente. Per queste porte, nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, scheda *CIST*, la casella di spunta nella colonna *Admin edge port* è selezionata.

Possibili valori:

- `selezionato`
  Il filtro BPDU è attivo su ogni porta edge.
  La funzione non utilizza queste porte nelle operazioni *Spanning Tree*.
  - Il dispositivo non invia STP-BPDU su queste porte.
  - Il dispositivo scarta ogni STP-BPDU ricevuta su queste porte.
- `non selezionato` (impostazione di default)
  Il filtro BPDU globale non è attivo.
  È possibile attivare esplicitamente il filtro BPDU per porte singole. Vedere la colonna *Port BPDU filter* nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*.

Auto-disable

Attiva/disattiva la funzione *Auto-Disable* per i parametri monitorati dalla *BPDU guard* sulla porta.

Possibili valori:

- `selezionato`
  La funzione *Auto-Disable* per la *BPDU guard* è attiva.
  - Quando la porta riceve una STP-BPDU, il dispositivo disabilita una porta edge. Il LED “Stato del link” per la porta lampeggia 3 volte per periodo.
  - La finestra di dialogo *Diagnostics > Ports > Auto-Disable* visualizza quali porte sono attualmente disabilitate a causa del superamento dei parametri.
  - La funzione *Auto-Disable* riattiva automaticamente la porta. Per fare ciò, nella finestra di dialogo *Diagnostics > Ports > Auto-Disable*, si specifica un periodo di attesa per la porta interessata nella colonna *Reset timer [s]*.
- `non selezionato` (impostazione di default)
  La funzione *Auto-Disable* per la *BPDU guard* non è attiva.

Root information

Bridge ID

Mostra lo switch ID del root switch corrente.

Possibili valori:

- `<Priorità Switch> / <Indirizzo MAC>`

Priority

Mostra la priorità dello switch del root switch attuale.

Possibili valori:

- `0..61440` a passi di 4096

Hello time [s]

Mostra il tempo in secondi specificato dal root switch tra l'invio di due messaggi di configurazione (pacchetti dati Hello).

Possibili valori:

- `1..2`

Il dispositivo utilizza questo valore specificato. Vedere il frame *Bridge configuration*.

Forward delay [s]

Specifica il tempo di ritardo in secondi impostato dal root switch per le modifiche dello stato.

Possibili valori:

- `4..30`

Il dispositivo utilizza questo valore specificato. Vedere il frame *Bridge configuration*.

Nel protocollo RSTP, gli switch negoziano una modifica dello stato senza un ritardo specificato.

Il protocollo *Spanning Tree* utilizza il parametro per posticipare la modifica dello stato tra gli stati *disabled*, *discarding*, *learning*, *forwarding*.

Max age

Specifica la lunghezza massima consentita del ramo impostata dal root switch, per esempio, il numero di dispositivi fino al root switch.

Possibili valori:

- `6..40` (impostazione di default: `20`)

Il protocollo *Spanning Tree* utilizza il parametro per specificare la validità delle STP-BPDU in secondi.

Topology information

Bridge is root

Mostra se il dispositivo ricopre attualmente il ruolo di root switch.

Possibili valori:

- `selezionato`
  Il dispositivo ricopre attualmente il ruolo di root switch.
- `non selezionato`
  Un altro dispositivo ricopre attualmente il ruolo di root switch.

Root port

Mostra il numero della porta da cui il percorso corrente conduce al root switch.

Se il dispositivo assume il ruolo di root switch, il campo mostra il valore `no Port`.

Root path cost

Mostra il costo del percorso per il percorso che conduce dalla porta root del dispositivo al root switch della rete di Layer 2.

Possibili valori:

- `0..200000000`
  Se il valore `0` è specificato, il dispositivo assume il ruolo di root switch.

Topology changes

Mostra quante volte il dispositivo ha impostato una porta nello stato *`forwarding`* tramite la funzione *Spanning Tree* dall'avvio dell'istanza *Spanning Tree*.

Time since topology change

Mostra il tempo trascorso dall'ultima modifica della topologia.

Possibili valori:

- `<giorni, ore:minuti:secondi>`

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.10.3.2 Spanning Tree Dual RSTP (MCSESM-E)

[Switching > L2-Redundancy > Spanning Tree > Dual RSTP]

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per contribuire a evitare la formazione di loop durante la fase di configurazione, configurare individualmente ciascun dispositivo della configurazione *RCP* e *Dual RSTP*. Prima di collegare le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione dell'anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

In questa finestra di dialogo, si specificano le impostazioni di switch corrispondenti alla seconda istanza *Spanning Tree*.

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 2 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.

Specificare le impostazioni della funzione *RCP* nella finestra di dialogo *Switching > L2-Redundancy > FuseNet > RCP*.

Operation

Operation

Visualizza se la funzione *Dual RSTP* è abilitata/disabilitata nel dispositivo.

Possibili valori:

- *On*
  La funzione *Dual RSTP* è abilitata nel dispositivo.
  Il dispositivo abilita autonomamente la funzione *Dual RSTP* se sono soddisfatti i seguenti prerequisiti:
  - Nella finestra di dialogo *Switching > L2-Redundancy > FuseNet > RCP* sono state specificate le porte per le impostazioni *Primary ring/network* e *Secondary ring/network*.
  - Nella finestra di dialogo *Switching > L2-Redundancy > FuseNet > RCP*, riquadro *Operation* si è abilitata la funzione *RCP*.
  - Nella finestra di dialogo *Spanning Tree Global*, frame *Operation*, si è abilitata la funzione *Spanning Tree*.
  - Non c'è un protocollo di ridondanza configurato nell'anello secondario.
- *Off* (impostazione di default)
  La funzione *Dual RSTP* è disabilitata nel dispositivo.

Traps

Send trap

Attiva/disattiva l'invio delle SNMP trap per gli eventi seguenti:

- Un altro switch assume il ruolo di root switch.
- Le modifiche della topologia. Una porta modifica la sua *Port state* da *forwarding* a *discarding* o da *discarding* a *forwarding*.

Possibili valori:

- `selezionato` (impostazione di default)
  L'invio di trap SNMP è attivo.
- `non selezionato`
  L'invio di trap SNMP non è attivo.

Bridge configuration

Bridge ID

Mostra lo switch ID del dispositivo.

Il dispositivo con il valore numerico switch ID più basso assume il ruolo di root switch nella rete.

Possibili valori:

- `<Priorità Switch> / <Indirizzo MAC>`
  Valore nel campo *Priority* / indirizzo MAC del dispositivo

Priority

Specifica la priorità dello switch del dispositivo.

Possibili valori:

- `0..61440` a passi di 4096 (impostazione di default: `32768`)

Per rendere questo dispositivo il root switch, assegnare al dispositivo il valore di priorità numerico più basso nella rete.

Hello time [s]

Specifica il tempo in secondi tra l'invio di due messaggi di configurazione (pacchetti dati Hello).

Possibili valori:

- `1..2` (impostazione di default: `2`)

Se il dispositivo assume il ruolo di root switch, gli altri dispositivi nella rete utilizzano il valore qui specificato.

Altrimenti, il dispositivo utilizza il valore specificato dal root switch. Vedere il frame *Root information*.

Per via dell'interazione con il parametro *Tx holds*, si consiglia di non modificare l'impostazione di default.

Forward delay [s]

Specifica il tempo di ritardo in secondi per la modifica dello stato.

Possibili valori:

- `4..30` (impostazione di default: `15`)

Se il dispositivo assume il ruolo di root switch, gli altri dispositivi nella rete utilizzano il valore qui specificato. Altrimenti, il dispositivo utilizza il valore specificato dal root switch. Vedere il frame *Root information*.

Nel protocollo RSTP, gli switch negoziano una modifica dello stato senza un ritardo specificato.

Il protocollo *Spanning Tree* utilizza il parametro per posticipare la modifica dello stato tra gli stati `disabled`, `discarding`, `learning`, `forwarding`.

I parametri *Forward delay [s]* e *Max age* hanno le seguenti relazioni:

Forward delay [s] ≥ (*Max age*/2) + 1

Max age

Specifica il numero massimo di dispositivi consentito nel percorso fino al root switch.

Possibili valori:

- `6..40` (impostazione di default: `20`)

Se il dispositivo assume il ruolo di root switch, gli altri dispositivi nella rete utilizzano il valore qui specificato. Altrimenti, il dispositivo utilizza il valore specificato dal root switch. Vedere il frame *Root information*.

Tx holds

Limita la velocità massima di trasmissione per l'invio di BPDU.

Possibili valori:

- `1..40` (impostazione di default: `10`)

Quando il dispositivo invia una BPDU, il dispositivo incrementa il valore di un contatore su questa porta.

Quando il contatore raggiunge il valore qui specificato, la porta smette di inviare BPDU. Da un lato, questo riduce il carico generato dall'RSTP e, dall'altro, quando il dispositivo non riceve BPDU, si può verificare un'interruzione della comunicazione.

Il dispositivo riduce il valore del contatore di `1` al secondo. Nel secondo seguente, il dispositivo invia un massimo di `1` nuove BPDU.

BPDU guard

Attiva/disattiva la funzione BPDU Guard nel dispositivo.

Con questa funzione, il dispositivo aiuta a proteggere la rete da configurazioni errate, attacchi tramite STP-BPDU, e modifiche indesiderate della topologia.

Possibili valori:

- `selezionato`
  La *BPDU guard* è attiva.
  - Il dispositivo applica la funzione a porte edge specificate manualmente. Per queste porte, nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, scheda *CIST*, la casella di spunta nella colonna *Admin edge port* è selezionata.
  - Se una porta edge riceve una STP-BPDU, il dispositivo disabilita la porta. Per questa porta, nella finestra di dialogo *Basic Settings > Port*, scheda *Configuration*, la casella di spunta nella colonna *Port on* è `non selezionata`.
- `non selezionato` (impostazione di default)
  La *BPDU guard* non è attiva.

Per ripristinare lo stato della porta sul valore *`forwarding`*, si procede come segue:

- ☐ Se la porta riceve ancora BPDU:
  - Nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, scheda *CIST*, deselezionare la casella di spunta nella colonna *Admin edge port*.
    oppure
  - Nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*, deselezionare la casella di spunta *BPDU guard*.
- ☐ Per abilitare nuovamente la porta, procedere come segue:
  - Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
  - Contrassegnare la casella di spunta nella colonna *Port on*.

BPDU filter (all admin edge ports)

Attiva/disattiva il filtro STP-BPDU su ogni porta edge specificata manualmente. Per queste porte, nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*, scheda *CIST*, la casella di spunta nella colonna *Admin edge port* è selezionata.

Possibili valori:

- `selezionato`
  Il filtro BPDU è attivo su ogni porta edge.
  La funzione non utilizza queste porte nelle operazioni *Spanning Tree*.
  - Il dispositivo non invia STP-BPDU su queste porte.
  - Il dispositivo scarta ogni STP-BPDU ricevuta su queste porte.
- `non selezionato` (impostazione di default)
  Il filtro BPDU globale non è attivo.
  È possibile attivare esplicitamente il filtro BPDU per porte singole. Vedere la colonna *Port BPDU filter* nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*.

Root information

Root ID

Mostra lo switch ID del root switch corrente.

Possibili valori:

- `<Priorità Switch> / <Indirizzo MAC>`

Priority

Mostra la priorità dello switch del root switch attuale.

Possibili valori:

- `0..61440` a passi di 4096

Hello time [s]

Mostra il tempo in secondi specificato dal root switch tra l'invio di due messaggi di configurazione (pacchetti dati Hello).

Possibili valori:

- `1..2`

Il dispositivo utilizza questo valore specificato. Vedere il frame *Bridge configuration*.

Forward delay [s]

Specifica il tempo di ritardo in secondi impostato dal root switch per le modifiche dello stato.

Possibili valori:

- `4..30`

Il dispositivo utilizza questo valore specificato. Vedere il frame *Bridge configuration*.

Nel protocollo RSTP, gli switch negoziano una modifica dello stato senza un ritardo specificato.

Il protocollo *Spanning Tree* utilizza il parametro per posticipare la modifica dello stato tra gli stati *disabled*, *discarding*, *learning*, *forwarding*.

Max age

Specifica la lunghezza massima consentita del ramo impostata dal root switch, per esempio, il numero di dispositivi fino al root switch.

Possibili valori:

- `6..40` (impostazione di default: `20`)

Il protocollo *Spanning Tree* utilizza il parametro per specificare la validità delle STP-BPDU in secondi.

Topology information

Bridge is root

Mostra se il dispositivo ricopre attualmente il ruolo di root switch.

Possibili valori:

- `selezionato`
  Il dispositivo ricopre attualmente il ruolo di root switch.
- `non selezionato`
  Un altro dispositivo ricopre attualmente il ruolo di root switch.

Root port

Mostra il numero della porta da cui il percorso corrente conduce al root switch.

Se il dispositivo assume il ruolo di root switch, il campo mostra il valore `no Port`.

Root path cost

Mostra il costo del percorso per il percorso che conduce dalla porta root del dispositivo al root switch della rete di Layer 2.

Possibili valori:

- `0..200000000`
  Se il valore `0` è specificato, il dispositivo assume il ruolo di root switch.

Topology changes

Mostra quante volte il dispositivo ha impostato una porta nello stato *`forwarding`* tramite la funzione *Spanning Tree* dall'avvio dell'istanza *Spanning Tree*.

Time since topology change

Mostra il tempo trascorso dall'ultima modifica della topologia.

Possibili valori:

- `<giorni, ore:minuti:secondi>`

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.10.3.3 Spanning Tree Port

[Switching > L2-Redundancy > Spanning Tree > Port]

In questa finestra di dialogo si attiva la funzione Spanning Tree sulle porte, si specificano le porte edge, e si specificano le impostazioni per varie funzioni di protezione.

Questa finestra di dialogo include le seguenti schede:
- [CIST]
- [Guards]

[CIST]

In questa scheda è possibile attivare la funzione Spanning Tree sulle porte individualmente, specificare le impostazioni per le porte edge e visualizzare i valori correnti. L'abbreviazione CIST sta per Common and Internal Spanning Tree.

Nota: Disattivare la funzione *Spanning Tree* sulle porte che partecipano ad altri protocolli di ridondanza di Layer 2. Altrimenti, è possibile che i protocolli di ridondanza operino in maniera diversa dal previsto. Ciò può causare la formazione di loop.

Tabella

Port

Visualizza il numero di porta.

STP active

Attiva/disattiva la funzione Spanning Tree sulla porta.

Possibili valori:
- `selezionato` (impostazione di default)
  La funzione *Spanning Tree* è attiva sulla porta.
- `non selezionato`
  La funzione *Spanning Tree* non è attiva sulla porta.
  Se la funzione *Spanning Tree* è abilitata nel dispositivo e non attiva sulla porta, la porta non invia STP-BPDU e scarta ogni STP-BPDU ricevuta.

Port state

Mostra lo stato della trasmissione sulla porta.

Possibili valori:
- *discarding*
  La porta è bloccata e inoltra solo STP-BPDU.
- *learning*
  La porta è bloccata ma acquisisce gli indirizzi MAC dei pacchetti dati ricevuti.
- *forwarding*
  La porta inoltra i pacchetti dati.

- *disabled*
  La porta non è attiva. Vedere la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
- *manualFwd*
  La funzione *Spanning Tree* è disabilitata sulla porta. La porta inoltra STP-BPDU.
- *notParticipate*
  La porta non partecipa all'STP.

Port role

Mostra il ruolo attuale della porta nel CIST.

Possibili valori:

- *root*
  Porta con il percorso più conveniente verso il root switch:
- *alternate*
  Porta con il percorso alternativo verso il root switch (attualmente in blocco).
- *designated*
  Porta per il lato del tree allontanato dal root switch (attualmente in blocco).
- *backup*
  La porta riceve STP-BPDU dal proprio dispositivo.
- *disabled*
  La porta non è attiva. Vedere la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.

Port path cost

Specifica i costi del percorso della porta.

Possibili valori:

- `0..200000000` (impostazione di default: `0`)

Quando il valore è `0`, il dispositivo calcola automaticamente i costi del percorso in base alla velocità di trasmissione della porta.

Port priority

Specifica la priorità della porta.

Possibili valori:

- `16..240` a passi di 16 (impostazione di default: `128`)

Questo valore rappresenta i primi 4 bit dell'ID porta.

Received bridge ID

Mostra lo switch ID del dispositivo da cui questa porta ha ricevuto una STP-BPDU l'ultima volta.

Possibili valori:

- Per porte con ruolo *designated*, il dispositivo mostra le informazioni per l'ultima STP-BPDU ricevuta dalla porta. Ciò facilita la diagnosi di eventuali problemi STP nella rete.
- Per i ruoli delle porte *alternate*, *backup*, *master*, e *root*, in stato stazionario (topologia statica) queste informazioni sono identiche alle informazioni del ruolo della porta *designated*.
- Nel caso in cui una porta non disponga di collegamento o non abbia ancora ricevuto nessuna STP-BDPU, il dispositivo mostra i valori che la porta può inviare con il ruolo *designated*.

Received port ID

Mostra l'ID porta del dispositivo da cui questa porta ha ricevuto una STP-BPDU l'ultima volta.

Possibili valori:

- Per porte con ruolo `designated`, il dispositivo mostra le informazioni per l'ultima STP-BPDU ricevuta dalla porta. Ciò facilita la diagnosi di eventuali problemi STP nella rete.
- Per i ruoli delle porte `alternate`, `backup`, `master`, e `root`, in stato stazionario (topologia statica) queste informazioni sono identiche alle informazioni del ruolo della porta `designated`.
- Nel caso in cui una porta non disponga di collegamento o non abbia ancora ricevuto nessuna STP-BDPU, il dispositivo mostra i valori che la porta può inviare con il ruolo `designated`.

Received path cost

Mostra il costo del percorso dello switch di livello superiore dalla sua porta root al root switch.

Possibili valori:

- Per porte con ruolo `designated`, il dispositivo mostra le informazioni per l'ultima STP-BPDU ricevuta dalla porta. Ciò facilita la diagnosi di eventuali problemi STP nella rete.
- Per i ruoli delle porte `alternate`, `backup`, `master`, e `root`, in stato stazionario (topologia statica) queste informazioni sono identiche alle informazioni del ruolo della porta `designated`.
- Nel caso in cui una porta non disponga di collegamento o non abbia ancora ricevuto nessuna STP-BDPU, il dispositivo mostra i valori che la porta può inviare con il ruolo `designated`.

Admin edge port

Attiva/disattiva la modalità *Admin edge port*. Se la porta è connessa a un dispositivo finale, utilizzare la modalità *Admin edge port*. Queste impostazioni consentono la modifica più rapida della porta edge allo stato di inoltro dopo il linkup e pertanto una più rapida accessibilità al dispositivo finale.

Possibili valori:

- `selezionato`
  La modalità *Admin edge port* è attiva.
  La porta è connessa a un dispositivo finale.
  - Dopo aver impostato il collegamento, la porta passa allo stato `forwarding` senza passare allo stato `learning`, prima.
  - Se la porta riceve una STP-BPDU e la funzione BPDU Guard è attiva, il dispositivo disattiva la porta. Vedere la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- `non selezionato` (impostazione di default)
  La modalità *Admin edge port* non è attiva.
  La porta è collegata a un altro STP switch.
  Dopo aver impostato il collegamento, la porta passa allo stato `learning` prima di passare allo stato `forwarding`, se applicabile.

Auto edge port

Attiva/disattiva il rilevamento automatico dell'eventuale connessione di un dispositivo finale alla porta. Il prerequisito è che la casella di spunta nella colonna *Admin edge port* sia `non selezionata`.

Possibili valori:

- `selezionato` (impostazione di default)
  Il rilevamento automatico è attivo.
  Dopo l'installazione del collegamento e dopo 1.5 × *Hello time [s]*, il dispositivo imposta la porta allo stato *`forwarding`* (impostazione di default 1.5 × 2 s) se la porta non ha ricevuto alcuna STP-BPDU in questo periodo.
- `non selezionato`
  Rilevamento automatico non attivo.
  Dopo l'installazione del collegamento, e dopo l'impostazione della porta allo stato *`forwarding`* da parte del dispositivo *Max age*.
  (impostazione di default: 20 s)

Oper edge port

Mostra se un dispositivo finale o un STP switch è connesso alla porta.

Possibili valori:

- `selezionato`
  Un dispositivo finale è connesso alla porta. La porta non riceve alcuna STP-BPDU.
- `non selezionato`
  Un STP switch è connesso alla porta. La porta riceve STP-BPDU.

Oper PointToPoint

Mostra se la porta è collegata a un dispositivo STP attraverso un collegamento diretto full-duplex.

Possibili valori:

- `selezionato`
  La porta è collegata direttamente a un dispositivo STP attraverso un collegamento full-duplex. La comunicazione diretta decentralizzata tra 2 switch favorisce brevi intervalli di riconfigurazione.
- `non selezionato`
  La porta è collegata in un altro modo, per esempio attraverso un collegamento half-duplex o attraverso un hub.

Port BPDU filter

Attiva/disattiva esplicitamente il filtraggio di STP-BPDU sulla porta.

Il prerequisito è che la porta sia una porta edge specificata manualmente. Per queste porte, la casella di spunta nella colonna *Admin edge port* è selezionata.

Possibili valori:

- `selezionato`
  Il filtro BPDU è attivo sulla porta.
  La funzione esclude la porta da operazioni *Spanning Tree*.
  – Il dispositivo non invia STP-BPDU alla porta.
  – Il dispositivo scarta ogni STP-BPDU ricevuta sulla porta.
- `non selezionato` (impostazione di default)
  Il filtro BPDU non è attivo sulla porta.
  È possibile attivare globalmente il filtro BPDU per ogni porta edge. Vedere la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*, frame *Bridge configuration*.
  Se la casella di spunta *BPDU filter (all admin edge ports)* è selezionata, il filtro BPDU è ancora attivo sulla porta.

BPDU filter status

Mostra se il filtro BPDU è attivo sulla porta.

Possibili valori:

- `selezionato`
  Il filtro BPDU è attivo sulla porta come conseguenza delle seguenti impostazioni:
  – La casella di spunta nella colonna *Port BPDU filter* è selezionata.
  e/o
  – La casella di spunta nella colonna *BPDU filter (all admin edge ports)* è selezionata. Vedere la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*, frame *Bridge configuration*.
- `non selezionato`
  Il filtro BPDU non è attivo sulla porta.

BPDU flood

Attiva/disattiva la modalità *BPDU flood* sulla porta anche se la funzione *Spanning Tree* non è attiva sulla porta. Il dispositivo inonda con le STP-BPDU ricevute sulla porta le porte per cui la funzione *Spanning Tree* non è attiva e la modalità *BPDU flood* è attiva.

Possibili valori:

- `selezionato`
  La modalità *BPDU flood* è attiva.
- `non selezionato` (impostazione di default)
  La modalità *BPDU flood* non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Guards]

Questa scheda consente di specificare le impostazioni per varie funzioni di protezione sulle porte.

Tabella

Port

Visualizza il numero di porta.

Root guard

Attiva/disattiva il monitoraggio delle STP-BPDU sulla porta. Il prerequisito è che la funzione *Loop guard* non sia attiva.

Con queste impostazioni il dispositivo contribuisce a proteggere la rete da configurazioni errate o attacchi tramite STP-BPDU che tentano di modificare la topologia. Queste impostazioni sono rilevanti solo per le porte con ruolo STP `designated`.

Possibili valori:

- `selezionato`
  Il monitoraggio delle STP-BPDU è attivo.
  - Se la porta riceve una STP-BPDU con migliori informazioni di percorso verso il root switch, il dispositivo la rifiuta e imposta lo status della porta sul valore `discarding` invece di `root`.
  - In assenza di STP-BPDU con migliori informazioni di percorso verso il root switch, il dispositivo ripristina lo stato della porta dopo 2 × *Hello time [s]*.
- `non selezionato` (impostazione di default)
  Il monitoraggio delle STP-BPDU non è attivo.

TCN guard

Attiva/disattiva il monitoraggio delle “Topology Change Notifications” sulla porta. Con queste impostazioni il dispositivo contribuisce a proteggere la rete da attacchi tramite STP-BPDU che tentano di modificare la topologia.

Possibili valori:

- `selezionato`
  Il monitoraggio delle “Topology Change Notifications” è abilitato.
  - La porta ignora la bandiera di modifica della topologia nelle STP-BPDU ricevute.
  - Se la BPDU ricevuta comprende altre informazioni che causano una modifica della topologia, il dispositivo elabora la BPDU anche se il TCN Guard è abilitato.
    Esempio: il dispositivo riceve informazioni di percorso migliori per il root switch.
- `non selezionato` (impostazione di default)
  Il monitoraggio delle “Topology Change Notifications” è disabilitato.
  Se il dispositivo riceve delle STP-BPDU con un flag di modifica della topologia, il dispositivo cancella la tabella indirizzi della porta e inoltra le Topology Change Notifications.

Loop guard

Attiva/disattiva il monitoraggio della formazione dei loop sulla porta. Il prerequisito è che la funzione *Root guard* non sia attiva.

Con queste impostazioni il dispositivo contribuisce a prevenire la formazione di loop se la porta non riceve più alcuna STP-BPDU. Utilizzare queste impostazioni solo per le porte con ruolo STP `alternate`, `backup` o `root`.

Possibili valori:

- `selezionato`
  Il monitoraggio della formazione di loop è attivo. Ciò contribuisce a prevenire la formazione di loop, per esempio, se si disabilita la funzione Spanning Tree sul dispositivo remoto o se il collegamento è interrotto solo in ricezione.
  - Se la porta non riceve alcuna STP-BPDU per un po' di tempo, il dispositivo imposta lo stato della porta sul valore *`discarding`* e seleziona la casella di spunta nella colonna *Loop state*.
  - Se la porta riceve nuovamente STP-BPDU, il dispositivo imposta lo stato della porta su un valore conforme a *Port role* e deseleziona la casella di spunta nella colonna *Loop state*.
- `non selezionato` (impostazione di default)
  Il monitoraggio della formazione di loop non è attivo.
  Se la porta non riceve alcuna STP-BPDU per un po' di tempo, il dispositivo imposta lo stato della porta sul valore *`forwarding`*.

Loop state

Mostra se lo stato del loop della porta è incoerente.

Possibili valori:

- `selezionato`
  Lo stato del loop della porta è incoerente:
  - La porta non riceve alcuna STP-BPDU e la funzione *Loop guard* è abilitata.
  - Il dispositivo imposta lo stato della porta sul valore *`discarding`*. Il dispositivo contribuisce pertanto a prevenire qualsiasi eventuale loop.
- `non selezionato`
  Lo stato del loop della porta è coerente. La porta riceve STP-BPDU.

Trans. into loop

Visualizza quante volte lo stato del loop della porta è diventato incoerente (casella di spunta selezionata nella colonna *Loop state*).

Trans. out of loop

Visualizza quante volte lo stato del loop della porta è diventato incoerente (casella di spunta non selezionata nella colonna *Loop state*).

BPDU guard effect

Mostra se la porta ha ricevuto una STP-BPDU come porta edge.

Prerequisito:

- La porta è una porta edge specificata manualmente. Nella finestra di dialogo *Port*, la casella di spunta per questa porta nella colonna *Admin edge port* è `selezionata`.
- Nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*, la funzione BPDU Guard è attiva.

Possibili valori:

- `selezionato`
  La porta è una porta edge e ha ricevuto una STP-BPDU.
  Il dispositivo disattiva la porta. Per questa porta, nella finestra di dialogo *Basic Settings > Port*, scheda *Configuration*, la casella di spunta nella colonna *Port on* è `non selezionata`.
- `non selezionato`
  La porta è una porta edge e non ha ricevuto alcuna STP-BPDU, o la porta non è una porta edge.

Per ripristinare lo stato della porta sul valore `forwarding`, si procede come segue:

- ☐ Se la porta riceve ancora BPDU, allora:
  - Nella scheda *CIST*, deselezionare la casella di spunta nella colonna *Admin edge port*.
    oppure
  - Nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*, deselezionare la casella di spunta *BPDU guard*.
- ☐ Per attivare la porta, procedere come segue:
  - Aprire la finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.
  - Contrassegnare la casella di spunta nella colonna *Port on*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.10.4 Link Aggregation

[Switching > L2-Redundancy > 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.

La funzione *Link Aggregation* consente di aggregare collegamenti paralleli multipli. Il prerequisito è che i collegamenti abbiano la stessa velocità e siano full duplex. I vantaggi in confronto ai collegamenti tradizionali utilizzando una linea singola sono una disponibilità maggiore e una larghezza di banda di trasmissione superiore.

Il Link Aggregation Control Protocol (LACP) consente di monitorare lo stato di connessione continuo a pacchetti sulle porte fisiche. Il LACP contribuisce anche a garantire che i partner di collegamento soddisfino i prerequisiti di aggregazione.

Se il lato remoto non supporta il Link Aggregation Control Protocol (LACP), è possibile utilizzare la funzione *Static link aggregation*. In questo caso il dispositivo aggrega i collegamenti basati sul collegamento, velocità di collegamento e impostazioni duplex.

Tabella

Trunk port

Mostra il numero dell'interfaccia LAG.

Name

Specifica il nome dell'interfaccia LAG.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 1..15 caratteri

Link/Status

Mostra il modo operativo corrente dell'interfaccia LAG e delle porte fisiche.

Possibili valori:

- `up` (riga `lag/…`)
  L'interfaccia LAG è operativa.
  I prerequisiti sono:
  - La funzione *Static link aggregation* è attiva sull'interfaccia LAG.
    oppure
  - Il LACP è attivo sulle porte fisiche assegnate all'interfaccia LAG, vedere la colonna *LACP active*.
    e
    La chiave specificata per l'interfaccia LAG nella colonna *LACP admin key* corrisponde alle chiavi specificate per le porte fisiche nella colonna *LACP port actor admin key*.
    e
    Il numero di porte fisiche operative assegnate all'interfaccia LAG è maggiore o uguale al valore specificato nella colonna *Active ports (min.)*.
- `up`
  La porta fisica è operativa.
- `down` (riga `lag/…`)
  L'interfaccia LAG non è attiva.
- `down`
  La porta è fisica è disabilitata.
  oppure
  Nessun cavo collegato o collegamento attivo.

Active

Attiva/disattiva l'interfaccia LAG.

Possibili valori:

- `selezionato` (impostazione di default)
  L'interfaccia LAG è attiva.
  Si consideri che i seguenti protocolli non funzionano correttamente sulle porte fisiche se si attiva l'interfaccia LAG:
  - *PTP*
  - *802.1AS*
- `non selezionato`
  L'interfaccia LAG non è attiva.

STP active

Attiva/disattiva il protocollo *Spanning Tree* su questa interfaccia LAG. Il prerequisito è che si abiliti la funzione *Spanning Tree* globalmente nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*.

È inoltre possibile attivare/disattivare il protocollo *Spanning Tree* sulle interfacce LAG nella finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Port*.

Possibili valori:

- `selezionato` (impostazione di default)
  Il protocollo *Spanning Tree* è attivo su questa interfaccia LAG.
- `non selezionato`
  Il protocollo *Spanning Tree* non è attivo su questa interfaccia LAG.

Static link aggregation

Attiva/disattiva la funzione *Static link aggregation* sull'interfaccia LAG. Il dispositivo aggrega le porte fisiche assegnate all'interfaccia LAG, anche se il sito remoto non supporta il LACP.

Possibili valori:

- `selezionato`
  La funzione *Static link aggregation* è attiva sull'interfaccia LAG. Il dispositivo aggrega una porta fisica assegnata all'interfaccia LAG non appena la porta fisica ottiene un collegamento. Il dispositivo non invia LACPDU e rifiuta le LACPDU ricevute.
- `non selezionato` (impostazione di default)
  La funzione *Static link aggregation* non è attiva su questa interfaccia LAG. Se il collegamento è stato negoziato con successo utilizzando il LACP, il dispositivo aggrega una porta fisica assegnata all'interfaccia LAG.

MTU

Specifica le dimensioni massime consentite dei pacchetti Ethernet sull'interfaccia LAG in byte. Nessuna delle etichette VLAN presenti è presa in considerazione.

Queste impostazioni consentono di aumentare le dimensioni dei pacchetti Ethernet per applicazioni specifiche.

Possibili valori:

- `1518..9720` (impostazione di default: `1518`)
  Con il valore `1518`, l'interfaccia LAG trasmette i pacchetti Ethernet fino alle seguenti dimensioni:
  - 1518 byte senza tag VLAN
    (1514 byte + 4°byte CRC)
  - 1522 byte con tag VLAN
    (1518 byte + 4 byte CRC)

Active ports (min.)

Specifica il numero minimo di porte fisiche attive necessarie per far sì che l'interfaccia LAG rimanga attiva. Se il numero di porte fisiche attive è inferiore al valore specificato, il dispositivo disattiva l'interfaccia LAG.

Se nel dispositivo è attiva una funzionalità di ridondanza come *Spanning Tree* o *MRP* via LAG, si utilizza tale funzionalità per costringere il dispositivo a passare automaticamente alla linea ridondante.

Possibili valori:

- `1` (impostazione di default)
- `2`
- In base all'hardware:
  `4`
  `8`
  `32`

Type

Mostra se l'interfaccia LAG è basata sulla funzione *Static link aggregation* o sul LACP.

Possibili valori:

- *`static`*
  L'interfaccia LAG è basata sulla funzione *Static link aggregation*.
- *`dynamic`*
  L'interfaccia LAG è basata sul LACP.

Send trap (Link up/down)

Attiva/disattiva l'invio di SNMP trap quando il dispositivo rileva un cambiamento nello stato link up/down per questa interfaccia.

Possibili valori:

- `selezionato` (impostazione di default)
  L'invio di trap SNMP è attivo.
  Se il dispositivo rileva un cambiamento dello stato link up/down, il dispositivo invia una SNMP trap.
- `non selezionato`
  L'invio di trap SNMP non è attivo.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

LACP admin key

Specifica la chiave dell'interfaccia LAG. Il dispositivo utilizza tale chiave per identificare le porte aggregabili all'interfaccia LAG.

Possibili valori:

- `0..65535`
  Si specifica il valore corrispondente per le porte fisiche nella colonna *LACP port actor admin key*.

Port

Mostra il numero delle porte fisiche assegnate all'interfaccia LAG.

Aggregation port status

Mostra se l'interfaccia LAG aggrega la porta fisica.

Possibili valori:

- *active*
  L'interfaccia LAG aggrega la porta fisica.
- *inactive*
  L'interfaccia LAG non aggrega la porta fisica.

LACP active

Attiva/disattiva il LACP sulla porta fisica.

Possibili valori:

- `selezionato` (impostazione di default)
  IlLACP è attivo sulla porta fisica.
- `non selezionato`
  Il LACP non è attivo sulla porta fisica.

LACP port actor admin key

Specifica la chiave della porta fisica. Il dispositivo utilizza tale chiave per identificare le porte aggregabili all'interfaccia LAG.

Possibili valori:

- `0`
  Il dispositivo ignora la chiave su questa porta fisica quando decide di aggregare la porta nell'interfaccia LAG.
- `1..65535`
  Se questo valore corrisponde al valore dell'interfaccia LAG specificato nella colonna *LACP admin key*, il dispositivo aggrega solo questa porta fisica all'interfaccia LAG.

LACP actor admin state

Specifica i valori di stato dell'attore trasmessi dall'interfaccia LAG nelle LACPDU. Ciò consente di controllare i parametri LACPDU.

Il dispositivo consente di combinare i valori. Nell'elenco a discesa, selezionare uno o più valori.

Possibili valori:

- *ACT*
  (Stato `LACP_Activity`)
  Quando è selezionato, il collegamento trasmette ciclicamente LACPDU, altrimenti le trasmette quando richiesto.
- *STO*
  (Stato `LACP_Timeout`)
  Quando è selezionato, il collegamento trasmette ciclicamente LACPDU utilizzando il timeout breve, le trasmette altrimenti utilizzando il timeout lungo.
- *AGG*
  (Stato `Aggregation`)
  Quando è selezionato, il dispositivo interpreta il collegamento come candidato all'aggregazione, altrimenti lo interpreta come collegamento individuale.

Per ulteriori informazioni sui valori, vedere la norma tecnica IEEE 802.1AX-2014.

LACP actor oper state

Mostra i valori di stato dell'attore trasmessi dall'interfaccia LAG nelle LACPDU.

Possibili valori:

- *ACT*
  (Stato `LACP_Activity`)
  Quando è visibile, il collegamento trasmette ciclicamente le LACPDU, altrimenti le trasmette quando richiesto.
- *STO*
  (Stato `LACP_Timeout`)
  Quando è visibile, il collegamento trasmette ciclicamente le LACPDU utilizzando il timeout breve, le trasmette altrimenti utilizzando il timeout lungo.
- *AGG*
  (Stato `Aggregation`)
  Quando è visibile, il dispositivo interpreta il collegamento come candidato per l'aggregazione, altrimenti lo interpreta come collegamento individuale.
- *SYN*
  (Stato `Synchronization`)
  Quando è visibile, il dispositivo interpreta il collegamento come `IN_SYNC`, altrimenti lo interpreta come `OUT_OF_SYNC`.
- *COL*
  (Stato `Collecting`)
  Quando è visibile, la raccolta di frame in ingresso è abilitata su questo collegamento, altrimenti è disabilitata.
- *DST*
  (Stato `Distributing`)
  Quando è visibile, la distribuzione di frame in uscita è abilitata su questo collegamento, altrimenti è disabilitata.
- *DFT*
  (Stato `Defaulted`)
  Quando è visibile, il collegamento utilizza informazioni operative di default specificate dall'amministrazione per il Partner. Altrimenti, il collegamento utilizza le informazioni operative ricevute da una LACPDU.
- *EXP*
  (Stato `Expired`)
  Quando è visibile, il destinatario del collegamento è in stato `EXPIRED`:

LACP partner oper SysID

Mostra l'indirizzo MAC del dispositivo remoto connesso a questa porta fisica.

L'interfaccia LAG ha ricevuto queste informazioni in una LACPDU proveniente dal partner.

LACP partner oper port

Mostra il numero della porta del dispositivo remoto connesso a questa porta fisica.

L'interfaccia LAG ha ricevuto queste informazioni in una LACPDU proveniente dal partner.

LACP partner oper port state

Mostra i valori di stato del partner ricevuti dall'interfaccia LAG nelle LACPDU.

Possibili valori:

- *ACT*
- *STO*
- *AGG*
- *SYN*
- *COL*
- *DST*
- *DFT*
- *EXP*

Per ulteriori informazioni sui valori, vedere la descrizione della colonna *LACP actor oper state* e la norma tecnica IEEE 802.1AX-2014.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce dell'interfaccia LAG alla tabella o assegnare una porta fisica a un'interfaccia LAG.

- Nell'elenco a discesa *Trunk port* si seleziona il numero dell'interfaccia LAG.
- Nell'elenco a discesa *Port* si seleziona il numero di una porta fisica da assegnare all'interfaccia LAG.

Dopo aver creato un'interfaccia LAG, il dispositivo aggiunge l'interfaccia LAG alla tabella nella finestra di dialogo *Basic Settings > Port*, scheda *Statistics*.

5.10.5 Link Backup

[Switching > L2-Redundancy > Link Backup]

⚠ 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.

Con il Link Backup, si configurano coppie di collegamenti ridondanti. Ciascuna coppia dispone di una porta primaria e di una porta di backup. La porta primaria inoltra il traffico finché il dispositivo non rileva un errore. Se il dispositivo rileva un errore sulla porta primaria, la funzione di Link Backup trasferisce il traffico sulla porta di backup.

Questa finestra di dialogo consente di impostare un opzione di fail back. Se si abilita la funzione di fail back e la porta primaria torna al funzionamento normale, il dispositivo prima blocca il traffico sulla porta di backup e poi inoltra il traffico sulla porta primaria. Questo processo contribuisce a proteggere il dispositivo dal causare loop nella rete.

Operation

Operation

Abilita/disabilità la funzione Link Backup globalmente nel dispositivo.

Possibili valori:

- *On*
  Abilita la funzione Link Backup.
- *Off* (impostazione di default)
  Disabilita la funzione Link Backup.

Tabella

Primary port

Mostra la porta primaria della coppia di interfacce. Quando si abilita la funzione Link Backup, questa porta è responsabile per l'inoltro del traffico.

Possibili valori:

- Porte fisiche

Backup port

Mostra la porta di backup su cui il dispositivo inoltra il traffico se rileva un errore sulla porta primaria.

Possibili valori:

- Porte fisiche a eccezione della porta impostata come porta primaria.

Description

Specifica la coppia di Link Backup. Inserire un nome per identificare la coppia di Backup.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Primary port status

Mostra lo stato della porta primaria per questa coppia di Link Backup.

Possibili valori:

- *forwarding*
  Il collegamento è attivo, nessun arresto, e inoltra traffico.
- *blocking*
  Il collegamento è attivo, nessun arresto, e blocca traffico.
- *down*
  La porta ha il collegamento interrotto, il cavo scollegato, o è disabilitata nel software, spegnimento.
- *unknown*
  La funzione di Link Backup è disabilitata globalmente, o la coppia di porte è inattiva. Di conseguenza, il dispositivo ignora le impostazioni della coppia di porte.

Backup port status

Mostra lo stato della porta di backup per questa coppia di Link Backup.

Possibili valori:

- *forwarding*
  Il collegamento è attivo, nessun arresto, e inoltra traffico.
- *blocking*
  Il collegamento è attivo, nessun arresto, e blocca traffico.
- *down*
  La porta ha il collegamento interrotto, il cavo scollegato, o è disabilitata nel software, spegnimento.
- *unknown*
  La funzione di Link Backup è disabilitata globalmente, o la coppia di porte è inattiva. Di conseguenza, il dispositivo ignora le impostazioni della coppia di porte.

Fail back

Attiva/disattiva il fail back automatico.

Possibili valori:

- `selezionato` (impostazione di default)
  Il fail back automatico è attivo.
  Alla scadenza del timer di ritardo, la porta di backup cambia in *`blocking`* e la porta primaria cambia in *`forwarding`*.
- `non selezionato`
  Il fail back automatico non è attivo.
  La porta di backup continua a inoltrare il traffico anche dopo che la porta primaria ha ristabilito un collegamento o dopo che si è modificato manualmente lo stato di amministrazione della porta primaria da `shutdown` a `no shutdown`.

Fail back delay [s]

Specifica il tempo di ritardo in secondi che il dispositivo attende dopo che la porta primaria ristabilisce un collegamento. Inoltre, questo timer si applica anche quando si imposta manualmente lo stato di amministrazione della porta primaria da `shutdown` a `no shutdown`. Alla scadenza del timer di ritardo, la porta di backup cambia in *`blocking`* e la porta primaria cambia in *`forwarding`*.

Possibili valori:

- `0..3600` (impostazione di default: `30`)
  Quando impostata a `0`, immediatamente dopo che la porta primaria ristabilisce un collegamento, la porta di backup cambia in *`blocking`* e la porta primaria cambia in *`forwarding`*. Inoltre, immediatamente dopo aver impostato manualmente lo stato di amministrazione da `shutdown` a `no shutdown`, la porta di backup cambia in *`blocking`* e la porta primaria cambia in *`forwarding`*.

Active

Attiva/disattiva la configurazione della coppia di Link Backup.

Possibili valori:

- `selezionato`
  La coppia di Link Backup è attiva. Il dispositivo rileva il collegamento e lo stato dell'amministrazione e inoltra il traffico in conformità alla configurazione della coppia.
- `non selezionato` (impostazione di default)
  La coppia di Link Backup non è attiva. Le porte inoltrano il traffico in conformità alla commutazione standard.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Create

Primary port

Specifica la porta primaria della coppia dell'interfaccia di backup. Durante il funzionamento normale, questa porta è responsabile dell'inoltro del traffico.

Possibili valori:

- Porte fisiche

Backup port

Specifica la porta di backup a cui il dispositivo trasferisce il traffico se rileva un errore sulla porta primaria.

Possibili valori:

- Porte fisiche a eccezione della porta impostata come porta primaria.

5.10.6 FuseNet

[Switching > L2-Redundancy > FuseNet]

I protocolli *FuseNet* consentono di collegare gli anelli che funzionano con uno dei seguenti protocolli di ridondanza:

- MRP
- HIPER Ring
- RSTP

Nota: Se si utilizza il protocollo *Ring/Network Coupling* per collegare reti, verificare che le reti contengano solo Schneider Electric dispositivi.

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*

– nessun protocollo di collegamento idoneo

1) con *MRP* configurate su VLAN diverse

Il menu include le seguenti finestre di dialogo:

- Sub Ring
- Ring/Network Coupling
- Redundant Coupling Protocol (MCSESM-E)

5.10.6.1 Sub Ring

[Switching > L2-Redundancy > FuseNet > Sub 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 *Sub Ring*. Prima di collegare le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione dell'anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Questa finestra di dialogo consente di impostare il dispositivo come un subring manager.

La funzione *Sub Ring* consente di collegare facilmente i segmenti di rete ad anelli di ridondanza esistenti. Il subring manager (SRM) collega un subring a un anello esistente (base ring).

Nel subring è possibile utilizzare qualsiasi dispositivo che supporti MRP come partecipanti all'anello. Tali dispositivi non richiedono una funzione di subring manager.

Quando si configurano subring, è necessario ricordare le seguenti regole:
- Il dispositivo supporta *Link Aggregation* nel subring.
- Nessun spanning tree sulle porte subring
- Stesso *MRP domain* sui dispositivi all'interno di un subring
- VLAN diverse per base ring e subring

Specificare le impostazioni della VLAN come segue:
- VLAN `X` per base ring
  - sulle porte ring dei partecipanti al base ring
  - sulle porte del base ring del subring manager
- VLAN `Y` per subring
  - sulle porte ring dei partecipanti al subring
  - sulle porte subring del subring manager

Nota: Per contribuire a evitare la formazione di loop, chiudere solo la linea ridondante quando le impostazioni sono specificate in ogni dispositivo partecipante nell'anello.

Operation

Operation

Abilita/disabilita la funzione *Sub Ring*.

Possibili valori:

- `On`
  È abilitata la funzione *Sub Ring*.
- `Off` (impostazione di default)
  È disabilitata la funzione *Sub Ring*.

Information

Table entries (max.)

Mostra il numero massimo di subring supportati dal dispositivo.

Tabella

Sub ring ID

Specifica l'identificatore unico di questo subring.

Possibili valori:

- `1..8`

Name

Specifica il nome opzionale del subring.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Active

Attiva/disattiva il subring.

Attivare il subring quando la configurazione di ogni dispositivo subring è completa. Chiudere il subring solo dopo aver attivato la funzione *Sub Ring*.

Possibili valori:

- `selezionato`
  Il subring è attivo.
- `non selezionato` (impostazione di default)
  Il subring non è attivo.

Configuration status

Mostra il modo operativo della configurazione subring.

Possibili valori:

- *`noError`*
  Il dispositivo rileva una configurazione subring accettabile.
- *`ringPortLinkError`*
  - La porta dell'anello non dispone di alcun collegamento.
  - Una delle linee subring è connessa a un'altra porta del dispositivo. Ma la linea subring non è connessa a una delle porte ring del dispositivo.
- *`multipleSRM`*
  Il subring manager riceve pacchetti da più di un subring manager nel subring.
- *`noPartnerManager`*
  Il subring manager riceve il proprio frame.
- *`concurrentVLAN`*
  Il protocollo MRP nel base ring utilizza la VLAN del dominio del subring manager.

- *concurrentPort*
  Un altro protocollo di ridondanza utilizza la porta dell'anello del dominio subring manager.
- *concurrentRedundancy*
  Il dominio subring manager non è attivo per via di un altro protocollo di ridondanza più attivo.
- *trunkMember*
  La porta dell'anello del dominio subring manager fa parte di un collegamento *Link Aggregation*.
- *sharedVLAN*
  Il dominio subring manager è inattivo perché la VLAN condivisa è attiva e anche l'anello principale utilizza il protocollo MRP.

Redundancy available

Mostra il modo operativo della ridondanza ad anello nel subring.

Possibili valori:

- *redGuaranteed*
  La riserva di ridondanza è disponibile.
- *redNotGuaranteed*
  Perdita della riserva di ridondanza.

Port

Specifica la porta che collega il dispositivo al subring.

Possibili valori:

- <Numero di porta>

SRM mode

Mostra la modalità corrente del subring manager.

Un subring dispone di 2 manager che collegano simultaneamente il subring al base ring. Finché il subring è fisicamente chiuso, un manager blocca la sua porta subring.

Possibili valori:

- *manager* (impostazione di default)
  La porta subring inoltra i pacchetti dati.
  Quando questo valore è impostato su entrambi i dispositivi che collegano il subring al base ring, il dispositivo con l'indirizzo MAC superiore funziona come *redundantManager*.
- *redundantManager*
  La porta subring è bloccata mentre il subring è fisicamente chiuso. Se il subring è interrotto, la porta subring trasmette i pacchetti dati.
  Quando questo valore è impostato su entrambi i dispositivi che collegano il subring al base ring, il dispositivo con l'indirizzo MAC superiore funziona come *redundantManager*.
- *singleManager*
  Utilizzare questo valore quando il subring è connesso al base ring attraverso un solo dispositivo. Il prerequisito è che vi siano 2 istanze del subring nella tabella. Assegnare questo valore a entrambe le istanze. La porta subring dell'istanza con il numero della porta superiore è bloccata mentre il subring è fisicamente chiuso.

SRM status

Mostra la modalità corrente del subring manager.

Possibili valori:

- *manager*
  La porta subring inoltra i pacchetti dati.
- *redundantManager*
  La porta subring è bloccata mentre il subring è fisicamente chiuso. Se il subring è interrotto, la porta subring trasmette i pacchetti dati.
- *singleManager*
  Il subring è connesso al base ring attraverso un solo dispositivo. La porta subring dell'istanza con il numero della porta superiore è bloccata mentre il subring è fisicamente chiuso.
- *disabled*
  Il subring non è attivo.

Port status

Mostra lo stato di connessione della porta subring.

Possibili valori:

- *forwarding*
  La porta sta passando i frame in base al comportamento di inoltro della IEEE 802.1D.
- *disabled*
  La porta sta scartando ogni frame.
- *blocked*
  La porta sta scartando ogni frame a eccezione dei seguenti casi:
  - La porta passa i frame utilizzati dal protocollo dell'anello selezionato, specificato per passare porte bloccate.
  - La porta passa i frame provenienti da altri protocolli specificati per passare porte bloccate.
- *not-connected*
  Il collegamento della porta non è attivo.

VLAN

Specifica la VLAN a cui questo subring è assegnato. Se nei VLAN-ID inseriti non vi è alcuna VLAN, il dispositivo la crea automaticamente.

Possibili valori:

- VLAN configurate disponibili (impostazione di default: `0`)
  Se non si desidera utilizzare una VLAN separata per questo subring, lasciare la voce su 0.

Partner MAC

Mostra l'indirizzo MAC del subring manager all'altra estremità del subring.

MRP domain

Specifica il dominio MRP del subring manager. Assegnare lo stesso nome del dominio MRP a tutti i membri di un subring. Se si utilizzano solo Schneider Electric dispositivi, utilizzare il valore predefinito per il dominio MRP; altrimenti regolare tale valore, se necessario. In presenza di più subring, la funzione consente di utilizzare lo stesso nome di dominio MRP per i subring.

Possibili valori:

- Nomi di dominio MRP consentiti (impostazione di default: `255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255`)

Protocol

Specifica il protocollo.

Possibili valori:

- *`iec-62439-mrp`*

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

5.10.6.2 Ring/Network Coupling

[Switching > L2-Redundancy > FuseNet > 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 collegare le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione dell'anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Utilizzare la funzione *Ring/Network Coupling* per collegare in maniera ridondante un HIPER ring, un MRP ring, o un Fast HIPER ring esistente a un'altra rete o a un altro anello. Verificare che i partner di collegamento siano dispositivi Schneider Electric.

Nota: Con un collegamento con due switch, verificare di aver configurato l'HIPER ring, l'MRP ring, o il Fast HIPER ring prima di configurare la funzione *Ring/Network Coupling*.

Nella finestra di dialogo *Ring/Network Coupling* è possibile eseguire le seguenti operazioni:
- mostrare una panoramica degli *Ring/Network Coupling* esistenti.
- configurare un *Ring/Network Coupling*
- creare un nuovo *Ring/Network Coupling*
- cancellare *Ring/Network Coupling*
- abilitare/disabilitare *Ring/Network Coupling*

Quando si configurano le porte di collegamento, specificare le seguenti impostazioni nella finestra di dialogo *Basic Settings > 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	–
Optical	100 Mbit/s	selezionato	non selezionato	*100 Mbit/s FDX*
Optical	1 Gbit/s	selezionato	selezionato	–
Ottico	2.5 Gbit/s	selezionato	–	*2.5 Gbit/s FDX*

Nota: I modi operativi della porta attualmente disponibili dipendono dalla configurazione del dispositivo.

Se si sono configurate delle VLAN prendere nota della configurazione delle VLAN delle porte di collegamento e di collegamento partner. Nella configurazione *Ring/Network Coupling*, selezionare i seguenti valori per le porte di collegamento e di collegamento partner:
- `VLAN ID 1` e *Ingress filtering* disabilitate nella tabella porte
- Appartenenza VLAN `T` nella tabella *VLAN Configuration*.

A prescindere dalle impostazioni VLAN il dispositivo invia i frame di collegamento dell'anello con `VLAN ID 1` e priorità `7`. Verificare che il dispositivo invii i frame VLAN1 taggati nell'anello locale e nella rete connessa. L'etichettatura dei frame VLAN mantiene la priorità dei frame di collegamento dell'anello.

La funzione *Ring/Network Coupling* agisce con i pacchetti di test. I dispositivi inviano i propri pacchetti di test con tag VLAN, compreso l'ID VLAN `1` e la massima priorità VLAN `7`. Se la porta di inoltro fa parte della VLAN `1` e trasmette i pacchetti dati senza un tag VLAN, il dispositivo invia anche questi pacchetti di test.

Operation

Operation

Abilita/disabilita la funzione *Ring/Network Coupling*.

Possibili valori:

- `On`
  È abilitata la funzione *Ring/Network Coupling*.
- `Off` (impostazione di default)
  È disabilitata la funzione *Ring/Network Coupling*.

Mode

Type

Specifica il metodo utilizzato per collegare le reti tra loro.

Possibili valori:

- `one-switch coupling`
  Consente di specificare le impostazioni della porta nei frame *Coupling port* e *Partner coupling port*.
- `two-switch coupling, master`
  Consente di specificare le impostazioni della porta nel frame *Coupling port*.
- `two-switch coupling, slave`
  Consente di specificare le impostazioni della porta nel frame *Coupling port*.
- `two-switch coupling with control line, master`
  Consente di specificare le impostazioni della porta nei frame *Coupling port* e *Control port*.
- `two-switch coupling with control line, slave`
  Consente di specificare le impostazioni della porta nei frame *Coupling port* e *Control port*.

Coupling port

Port

Specifica la porta alla quale si collega il collegamento ridondante.

Possibili valori:

- `-`
  Nessuna porta selezionata.
- `<Numero di porta>`

Se sono state configurate anche le porte ring, specificare le porte ring e di collegamento su porte diverse.

Per contribuire a prevenire la formazione di loop continui, il dispositivo disabilita la porta di collegamento nei seguenti casi:

- disabilitazione della funzione
- modifica della configurazione durante il funzionamento dei collegamenti sulle porte

Quando il dispositivo ha disabilitato la porta di collegamento, la casella di spunta *Port on* è non selezionata nella finestra di dialogo *Basic Settings > Port*, scheda *Configuration*.

State

Mostra lo stato della porta selezionata.

Possibili valori:

- *active*
  La porta è attiva.
- *standby*
  La porta è in modalità stand-by.
- *not-connected*
  La porta non è connessa.
- *not-applicable*
  La porta è incompatibile con la modalità di controllo configurata.

Partner coupling port

Port

Specifica la porta alla quale si collega la porta partner.

Possibili valori:

- `-`
  Nessuna porta selezionata.
- `<Numero di porta>`

Se sono state configurate anche le porte ring, specificare le porte ring e di collegamento su porte diverse.

State

Mostra lo stato della porta selezionata.

Possibili valori:

- *active*
  La porta è attiva.
- *standby*
  La porta è in modalità stand-by.
- *not-connected*
  La porta non è connessa.
- *not-applicable*
  La porta è incompatibile con la modalità di controllo configurata.

IP address

Mostra l'indirizzo IP del partner, quando i dispositivi sono connessi.

Il prerequisito è che si selezioni un metodo di collegamento con due switch e si abiliti il partner nella rete.

Control port

Port

Mostra la porta alla quale si collega la linea di controllo.

Possibili valori:

- -
  Nessuna porta selezionata.
- <Numero di porta>

State

Mostra lo stato della porta selezionata.

Possibili valori:

- *active*
  La porta è attiva.
- *standby*
  La porta è in modalità stand-by.
- *not-connected*
  La porta non è connessa.
- *not-applicable*
  La porta è incompatibile con la modalità di controllo configurata.

Configuration

Redundancy mode

Specifica se il dispositivo risponde a un guasto rilevato nella rete o nell'anello remoto.

Possibili valori:

- *redundant ring/network coupling*
  La linea principale o la linea ridondante è attiva. Entrambe le linee non sono attive contemporaneamente. Se il dispositivo rileva che il collegamento tra i dispositivi nella rete connessa non è attivo, il dispositivo di standby mantiene la porta ridondante nella modalità standby.
- *extended redundancy*
  La linea principale e la linea ridondante sono attive contemporaneamente. Se il dispositivo rileva un problema nella connessione tra i dispositivi nella rete connessa, il dispositivo di standby inoltra i dati alla porta ridondante. Con l'impostazione è possibile mantenere continuità nella rete remota.

Nota: Durante l'intervallo di riconfigurazione si possono verificare duplicazioni di pacchetti. Di conseguenza, se l'applicazione è in grado di rilevare duplicazioni di pacchetti, è possibile selezionare questa impostazione.

Coupling mode

Specifica la modalità di accoppiamento a una specifica tipologia di rete.

Possibili valori:

- *ring coupling*
  Il dispositivo collega anelli ridondanti. Il dispositivo consente di collegare gli anelli che utilizzano i seguenti protocolli di ridondanza:
  - HIPER ring
  - Fast HIPER ring
  - MRP ring
- *network coupling*
  Il dispositivo collega i segmenti di rete. La funzione consente di collegare reti bus e mesh tra loro.

Information

Redundancy available

Mostra se la ridondanza è disponibile.

Quando un componente dell'anello non funziona, la linea ridondante assume la sua funzione.

Possibili valori:

- *redGuaranteed*
  La ridondanza è disponibile.
- *redNotGuaranteed*
  La ridondanza non è disponibile.

Configuration failure

La funzione non è stata configurata correttamente o la connessione alla porta dell'anello non è disponibile.

Possibili valori:

- *noError*
- *slaveCouplingLinkError*
  La linea di collegamento non è collegata alla porta di collegamento del dispositivo slave. Invece, la linea di collegamento è collegata a un'altra porta del dispositivo slave.
- *slaveControlLinkError*
  La porta di controllo del dispositivo slave non dispone di collegamento dati.
- *masterControlLinkError*
  La linea di controllo non è collegata alla porta di controllo del dispositivo master. Invece, la linea di controllo è collegata a un'altra porta del dispositivo master.
- *twoSlaves*
  La linea di controllo collega due dispositivi slave.
- *localPartnerLinkError*
  La linea di collegamento partner non è collegata alla porta di collegamento partner del dispositivo slave. Invece, la linea di collegamento partner è collegata a un'altra porta del dispositivo slave in modalità *one-switch coupling*.
- *localInvalidCouplingPort*
  In modalità *one-switch coupling*, la linea di collegamento non è collegata sullo stesso dispositivo della linea partner. Invece, la linea di collegamento è collegata a un altro dispositivo.
- *couplingPortNotAvailable*
  La porta di collegamento non è disponibile in quanto il modulo a cui si riferisce la porta non è disponibile o la porta non esiste su questo modulo.
- *controlPortNotAvailable*
  La porta di controllo non è disponibile in quanto il modulo a cui si riferisce la porta non è disponibile o la porta non esiste su questo modulo.
- *partnerPortNotAvailable*
  La porta di collegamento partner non è disponibile in quanto il modulo a cui si riferisce la porta non è disponibile o la porta non esiste su questo modulo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Disabilita la funzionalità di ridondanza e ripristina i parametri nella finestra di dialogo alle impostazioni di default.

5.10.6.3 Redundant Coupling Protocol (MCSESM-E)

[Switching > L2-Redundancy > FuseNet > 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 collegare le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione dell'anello.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

⚠ AVVERTENZA

PERICOLO DI LOOP

- Configurare ciascun dispositivo della configurazione *RCP* e *Dual RSTP* individualmente. Prima di collegare le linee ridondanti, completare la configurazione degli altri dispositivi della configurazione dell'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.

Una topologia ad anello offre tempi di transizione ridotti con un impiego minimo di risorse. Tuttavia, il collegamento di questi anelli in maniera ridondante a una rete di livello superiore rappresenta più di una sfida.

Quando si desidera utilizzare un protocollo standard come l'MRP per la ridondanza ad anello e l'RSTP per collegare gli anelli tra loro, la *Redundant Coupling Protocol* contribuisce a fornire delle opzioni.

Non utilizzare i seguenti protocolli di ridondanza sulle porte dell'anello primario *RCP* e degli anelli secondari *RCP*:

- *Sub Ring*
- *Ring/Network Coupling*

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*. Le impostazioni della funzione *Dual RSTP* si specificano nella finestra di dialogo *Switching > L2-Redundancy*.

Se si configura la funzione *RCP* in una rete e la configurazione non è completata, è possibile che i dispositivi scolleghino temporaneamente l'anello secondario e l'anello primario. In tal caso, la gestione del dispositivo degli switch *RCP* non è raggiungibile dall'anello secondario. Durante questa fase di configurazione, collegare la propria stazione di gestione all'anello primario.

Operation

Operation

Abilita/disabilita la funzione *RCP*.

Possibili valori:

- `On`
  È abilitata la funzione *RCP*.
- `Off` (impostazione di default)
  È disabilitata la funzione *RCP*.

Primary ring/network / Secondary ring/network

Se il dispositivo funziona come slave (il valore nel campo *Role* è `slave`), non attivare la modalità *Static query port* per le porte sull'anello/rete secondario/a.

Inner port

Specifica il numero della porta interna nell'anello secondario/primario. La porta è connessa direttamente allo switch del partner.

Possibili valori:

- `-` (impostazione di default)
  Nessuna porta selezionata.
- `<Numero di porta>`

Outer port

Specifica il numero della porta esterna nell'anello primario/secondario.

Possibili valori:

- `-` (impostazione di default)
  Nessuna porta selezionata.
- `<Numero di porta>`

Primary Ring protocol/Secondary Ring protocol

Visualizza il protocollo attivo sulla porta di collegamento ridontante nei dispositivi dell'anello primario/secondario.

Coupler configuration

Role

Specifica il ruolo del dispositivo locale.

Possibili valori:

- `master`
  Il dispositivo funziona come master.
- `slave`
  Il dispositivo funziona come slave.
- `single`
  Il dispositivo collega 2 reti RSTP con un'istanza *Dual RSTP* utilizzando uno switch.
- `auto` (impostazione di default)
  Il dispositivo seleziona automaticamente il proprio ruolo come *master* o *slave*.

Current role

Mostra il ruolo attuale del dispositivo locale. Il valore può essere diverso dal ruolo configurato:

- Se si sono configurati entrambi gli switch partner come `auto`, lo switch partner che collega attualmente le istanze assume il ruolo di `master`. L'altro switch partner assume il ruolo di `slave`.
- Se entrambi gli switch partner sono configurati come `master` o `slave`, lo switch partner con l'indirizzo MAC di base inferiore assume il ruolo di `master`.
  L'altro switch partner assume il ruolo di `slave`.
- Se il protocollo è avviato e risulta impossibile trovare lo switch partner per uno switch nel ruolo configurato `master`, `slave` o `auto`, lo switch imposta il proprio ruolo su `listening`.
- Se il dispositivo rileva un problema di configurazione, per esempio, se le porte ring interne sono connesse trasversalmente, il dispositivo imposta il proprio ruolo su `error`.

Timeout [ms]

Specifica il massimo intervallo di tempo, in millisecondi, durante il quale il dispositivo slave aspetta i pacchetti di test provenienti dal dispositivo master sulle porte esterne, prima che il dispositivo slave assuma il controllo del collegamento. Questo vale solo nello stato in cui entrambe le porte interne del dispositivo slave abbiano perso il collegamento al dispositivo master.

Configurare il timeout di modo che sia più lungo della più lunga interruzione prevedibile per il protocollo di ridondanza dell'istanza più rapida. Altrimenti potrebbero formarsi dei loop.

Possibili valori:

- `5..60000` (impostazione di default: `45`)

Partner MAC address

Mostra l'indirizzo MAC di base del dispositivo partner.

Partner IP address

Mostra l'indirizzo IP del dispositivo partner.

Coupling state

Mostra lo stato di connessione del dispositivo locale.

Possibili valori:

- *forwarding*
  Lo stato di connessione della porta è “inoltro”.
- *blocking*
  Lo stato di connessione della porta è “blocco”.

Redundancy state

Mostra se la ridondanza è disponibile.

Per una configurazione master-slave, entrambi gli switch mostrano questa informazione.

Possibili valori:

- *redAvailable*
  La ridondanza è disponibile.
- *redNotAvailable*
  La ridondanza non è disponibile.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6 Diagnostics

Il menu include le seguenti finestre di dialogo:

- Status Configuration
- System
- Email Notification
- Syslog
- Ports
- Loop Protection
- LLDP
- Report

6.1 Status Configuration

[Diagnostics > Status Configuration]

Il menu include le seguenti finestre di dialogo:

- Device Status
- Security Status
- Signal Contact
- MAC Notification
- Alarms (Traps)

6.1.1 Device Status

[Diagnostics > Status Configuration > Device Status]

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 frame *Device status*. Il dispositivo determina questo stato sulla base dei singoli risultati del monitoraggio.

Il dispositivo visualizza gli errori rilevati nella scheda *Status* e anche nella finestra di dialogo *Basic Settings > System*, frame *Device Status*.

Questa finestra di dialogo include le seguenti schede:
- [Global]
- [Port]
- [Status]

[Global]

Device status

Device status

Visualizza lo stato attuale del dispositivo. Il dispositivo determina lo stato sulla base dei singoli parametri monitorati.

Possibili valori:

- `error`
  Il dispositivo visualizza questo valore per indicare un errore rilevato in uno dei parametri monitorati.
- `ok`

Traps

Send trap

Attiva/disattiva l'invio di trap SNMP se il dispositivo rileva una modifica in una funzione monitorata.

Possibili valori:

- `selezionato` (impostazione di default)
  L'invio di trap SNMP è attivo.
  Se il dispositivo rileva una modifica nelle funzioni monitorate, il dispositivo invia una trap SNMP.
- `non selezionato`
  L'invio di trap SNMP non è attivo.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Tabella

Temperature

Attiva/disattiva il monitoraggio della temperatura nel dispositivo.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Se la temperatura eccede o è inferiore al limite specificato, nel frame *Device status* il valore cambia in `error`.
- `non selezionato`
  Il monitoraggio non è attivo.

Si specificano le soglie di temperatura nella finestra di dialogo *Basic Settings > System*, campo *Upper temp. limit [°C]* e il campo *Lower temp. limit [°C]* .

Ring redundancy

Attiva/disattiva il monitoraggio della ridondanza ad anello.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Nel frame *Device status*, il valore 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.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Connection errors

Attiva/disattiva il monitoraggio dello stato del link della porta/interfaccia.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Se il link si interrompe su una porta/interfaccia monitorata, nel frame*Device status* il valore cambia in `error`.
  Nella scheda *Port*, è possibile selezionare le porte/interfacce da monitorare singolarmente.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

External memory removal

Attiva/disattiva il monitoraggio della memoria esterna attiva.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Rimuovendo la memoria esterna attiva dal dispositivo, nel frame *Device status* il valore cambia in `error`.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

External memory not in sync

Attiva/disattiva il monitoraggio del profilo di configurazione nel dispositivo e nella memoria esterna.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Nel frame *Device status*, il valore 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.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Power supply

Attiva/disattiva il monitoraggio dell'alimentatore.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Se il dispositivo presenta un errore di alimentazione di tensione rilevato, nel frame*Device status* il valore cambia in `error`.
- `non selezionato`
  Il monitoraggio non è attivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Port]

Tabella

Port

Visualizza il numero di porta.

Propagate connection error

Attiva/disattiva il monitoraggio del link sulla porta/interfaccia.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Se il link si interrompe sulla porta/interfaccia selezionata, nel frame*Device status* il valore cambia in *`error`*.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Questa impostazione viene applicata quando si seleziona la casella di spunta *Connection errors* nella scheda *Global*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Status]

Tabella

Timestamp

Visualizza la data e l'ora dell'evento nel formato, `mese giorno, anno hh:mm:ss AM/PM`.

Cause

Visualizza l'evento che ha causato la trap SNMP.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.1.2 Security Status

[Diagnostics > Status Configuration > Security Status]

La finestra di dialogo fornisce una panoramica dello stato delle impostazioni rilevanti per la sicurezza nel dispositivo.

Il dispositivo visualizza il suo stato attuale come `error` o `ok` nel frame *Security status*. Il dispositivo determina questo stato sulla base dei singoli risultati del monitoraggio.

Il dispositivo visualizza gli errori rilevati nella scheda *Status* e anche nella finestra di dialogo *Basic Settings > System*, frame *Security status*.

Questa finestra di dialogo include le seguenti schede:
- [Global]
- [Port]
- [Status]

[Global]

Security status

Security status

Visualizza l'attuale stato delle impostazioni rilevanti per la sicurezza nel dispositivo. Il dispositivo determina lo stato sulla base dei singoli parametri monitorati.

Possibili valori:

- `error`
  Il dispositivo visualizza questo valore per indicare un errore rilevato in uno dei parametri monitorati.
- `ok`

Traps

Send trap

Attiva/disattiva l'invio di trap SNMP se il dispositivo rileva una modifica in una funzione monitorata.

Possibili valori:

- `selezionato`
  L'invio di trap SNMP è attivo.
  Se il dispositivo rileva una modifica nelle funzioni monitorate, il dispositivo invia una trap SNMP.
- `non selezionato` (impostazione di default)
  L'invio di trap SNMP non è attivo.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Tabella

Password default settings unchanged

Attiva/disattiva il monitoraggio della password per gli account utente `user` e `admin` configurati localmente.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Se la password ha l'impostazione di default per gli account utente `user` o `admin`, nel frame *Security status* il valore cambia in *`error`*.
- `non selezionato`
  Il monitoraggio non è attivo.

Impostare la password nella finestra di dialogo *Device Security > User Management*.

Min. password length < 8

Attiva/disattiva il monitoraggio del criterio *Min. password length*.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Se il valore per il criterio *Min. password length* è inferiore a `8`, nel frame *Security status* il valore cambia in *`error`*.
- `non selezionato`
  Il monitoraggio non è attivo.

Specificare il criterio *Min. password length* nella finestra di dialogo *Device Security > User Management* nel frame *Configuration*.

Password policy settings deactivated

Attiva/disattiva il monitoraggio delle impostazioni dei criteri per la password.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Se il valore per almeno uno dei seguenti criteri è inferiore a `1`, nel frame *Security status* il valore cambia in *`error`*.
  - *Upper-case characters (min.)*
  - *Lower-case characters (min.)*
  - *Digits (min.)*
  - *Special characters (min.)*
- `non selezionato`
  Il monitoraggio non è attivo.

Specificare le impostazioni dei criteri nella finestra di dialogo *Device Security > User Management*, nel frame *Password policy*.

User account password policy check deactivated

Attiva/disattiva il monitoraggio della funzione *Policy check*.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Se la funzione *Policy check* è inattiva per almeno un account utente, nel frame *Security status* il valore cambia in `error`.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Attivare la funzione *Policy check* nella finestra di dialogo *Device Security > User Management*.

Telnet server active

Attiva/disattiva il monitoraggio del server Telnet.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Abilitando il server Telnet, nel frame *Security status* il valore cambia in `error`.
- `non selezionato`
  Il monitoraggio non è attivo.

Abilitare/disabilitare il server Telnet nella finestra di dialogo *Device Security > Management Access > Server*, scheda *Telnet*.

HTTP server active

Attiva/disattiva il monitoraggio del server HTTP.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Abilitando il server HTTP, nel frame *Security status* il valore cambia in `error`.
- `non selezionato`
  Il monitoraggio non è attivo.

Abilitare/disabilitare il server HTTP nella finestra di dialogo *Device Security > Management Access > Server*, scheda *HTTP*.

SNMP unencrypted

Attiva/disattiva il monitoraggio del server SNMP.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Se si applica almeno una delle seguenti condizioni, nel frame *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*, nella colonna *SNMP encryption type*.
- `non selezionato`
  Il monitoraggio non è attivo.

Specificare le impostazioni dell'agente SNMP nella finestra di dialogo *Device Security > Management Access > Server*, scheda *SNMP*.

Access to system monitor with serial interface possible

Attiva/disattiva il monitoraggio del monitor di sistema.

Se il monitor di sistema è attivato, è possibile modificare il monitor di sistema attraverso una connessione seriale.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Attivando il monitor di sistema, nel frame *Security status* il valore cambia in `error`.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Attivare/disattivare il monitor di sistema nella finestra di dialogo *Diagnostics > System > Selftest*.

Saving the configuration profile on the external memory possible

Attiva/disattiva il monitoraggio del profilo di configurazione nella memoria esterna.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Se si attiva il salvataggio del profilo di configurazione nella memoria esterna, nel frame *Security status* il valore cambia in `error`.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Attivare/disattivare il salvataggio del profilo di configurazione nella memoria esterna nella finestra di dialogo *Basic Settings > External Memory*.

Link interrupted on enabled device ports

Attiva/disattiva il monitoraggio del link sulle porte attive..

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Se il link si interrompe su una porta attiva, nel frame *Security status* il valore cambia in `error`.
  Nella scheda *Port*, è possibile selezionare le porte da monitorare singolarmente.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Access with Ethernet Switch Configurator possible

Attiva/disattiva il monitoraggio della funzione Ethernet Switch Configurator.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Abilitando la funzione Ethernet Switch Configurator, nel frame *Security status* il valore cambia in `error`.
- `non selezionato`
  Il monitoraggio non è attivo.

Si abilita/disabilita la funzione Ethernet Switch Configurator nella finestra di dialogo *Basic Settings* > Network.

Load unencrypted config from external memory

Attiva/disattiva il monitoraggio di caricamento di profili di configurazione non crittografati dalla memoria esterna.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Se le impostazioni consentono al dispositivo di caricare un profilo di configurazione non crittografato dalla memoria esterna, nel frame *Security status* il valore cambia in `error`.
  Se sono soddisfatte le seguenti precondizioni, il frame *Security status* nella finestra di dialogo *Basic Settings* > *System* visualizza un allarme.
  - Il profilo di configurazione memorizzato nella memoria esterna non è crittografato.
    e
  - La colonna *Config priority* nella finestra di dialogo *Basic Settings* > *External Memory* ha il valore `first`.
- `non selezionato`
  Il monitoraggio non è attivo.

IEC61850-MMS active

Attiva/disattiva il monitoraggio della funzione *IEC61850-MMS*.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Abilitando la funzione *IEC61850-MMS*, nel frame *Security status* il valore cambia in `error`.
- `non selezionato`
  Il monitoraggio non è attivo.

Si abilita/disabilita la funzione *IEC61850-MMS* nella finestra di dialogo *Industrial Protocols > IEC61850-MMS*, frame *Operation*.

Self-signed HTTPS certificate present

Attiva/disattiva il monitoraggio del certificato HTTPS.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Se il server HTTPS utilizza un certificato digitale creato autonomamente, nel frame *Security status* il valore cambia in `error`.
- `non selezionato`
  Il monitoraggio non è attivo.

Modbus TCP active

Attiva/disattiva il monitoraggio della funzione *Modbus TCP*.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Abilitando la funzione *Modbus TCP*, nel frame *Security status* il valore cambia in `error`.
- `non selezionato`
  Il monitoraggio non è attivo.

Si abilita/disabilita la funzione *Modbus TCP* nella finestra di dialogo *Advanced > Industrial Protocols >* Modbus TCP, frame *Operation*.

EtherNet/IP active

Attiva/disattiva il monitoraggio della funzione *EtherNet/IP*.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Abilitando la funzione *EtherNet/IP*, nel frame *Security status* il valore cambia in `error`.
- `non selezionato`
  Il monitoraggio non è attivo.

Si abilita/disabilita la funzione *EtherNet/IP* nella finestra di dialogo *Advanced > Industrial Protocols >* EtherNet/IP, frame *Operation*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Port]

Tabella

Port

Visualizza il numero di porta.

Link interrupted on enabled device ports

Attiva/disattiva il monitoraggio del link sulle porte attive..

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Se la porta è abilitata (finestra di dialogo *Basic Settings > Port*, scheda *Configuration*, la casella di spunta*Port on* è `selezionato`) e il link non è attivo sulla porta, nel frame *Security status* il valore cambia in *error*.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Questa impostazione viene applicata quando si seleziona la casella di spunta *Link interrupted on enabled device ports* nella finestra di dialogo *Diagnostics > Status Configuration > Security Status*, scheda *Global*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Status]

Tabella

Timestamp

Visualizza la data e l'ora dell'evento nel formato, `mese giorno, anno hh:mm:ss AM/PM`.

Cause

Visualizza l'evento che ha causato la trap SNMP.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.1.3 Signal Contact

[Diagnostics > Status Configuration > Signal Contact]

Il contatto di segnalazione è un contatto relay privo di potenziale. Pertanto il dispositivo consente l'effettuazione di una diagnosi remota. Il dispositivo utilizza il contatto relay per segnalare il verificarsi di eventi attraverso l'apertura del contatto relay e interrompendo il circuito chiuso.

Nota: Il dispositivo può contenere diversi contatti di segnalazione. Ogni contatto contiene le stesse funzioni di monitoraggio. Diversi contatti consentono di raggruppare diverse funzioni, fornendo flessibilità e monitoraggio di sistema.

Il menu include le seguenti finestre di dialogo:
- Signal Contact 1 / Signal Contact 2

6.1.3.1 Signal Contact 1 / Signal Contact 2

[Diagnostics > Status Configuration > Signal Contact > Signal Contact 1]

In questa finestra di dialogo si specificano le condizioni di attivazione del contatto di segnalazione.

Il contatto di segnalazione offre le seguenti opzioni:
- Monitoraggio del corretto funzionamento del dispositivo.
- Segnalazione dello stato del dispositivo.
- Segnalazione dello stato di sicurezza del dispositivo.
- Controllo dei dispositivi esterni impostando manualmente i contatti di segnalazione.

Il dispositivo visualizza gli errori rilevati nella scheda *Status* e anche nella finestra di dialogo *Basic Settings > System*, frame *Signal contact status*.

Questa finestra di dialogo include le seguenti schede:
- [Global]
- [Port]
- [Status]

[Global]

Configuration

Mode

Specifica quali eventi il contatto di segnalazione indica.

Possibili valori:

- `Manual setting` (impostazione di default per *Signal Contact 2* se presente)
  Utilizzare questa impostazione per aprire o chiudere manualmente il contatto di segnalazione, ad esempio per accendere o spegnere un dispositivo remoto. Vedere la lista di opzioni *Contact*.
- `Monitoring correct operation` (impostazione di default)
  Utilizzando questa impostazione il contatto di segnalazione indica lo stato dei parametri specificato nella tabella qui di seguito.
- `Device status`
  Utilizzando questa impostazione il contatto di segnalazione indica lo stato dei parametri monitorati nella finestra di dialogo *Diagnostics > Status Configuration > Device Status*. Inoltre, è possibile leggere lo stato nel frame *Signal contact 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*. Inoltre, è possibile leggere lo stato nel frame *Signal contact 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*. Inoltre, è possibile leggere lo stato nel frame *Signal contact status*.

Contact

Attiva/disattiva manualmente il contatto di segnalazione. Il prerequisito è che nell'elenco a discesa *Mode* sia selezionata la voce `Manual setting`.

Possibili valori:

- `open`
  Il contatto di segnalazione è aperto.
- `close`
  Il contatto di segnalazione è chiuso.

Signal contact status

Signal contact status

Visualizza lo stato attuale del contatto di segnalazione.

Possibili valori:

- `Opened (error)`
  Il contatto di segnalazione è aperto. Il circuito è interrotto.
- `Closed (ok)`
  Il contatto di segnalazione è chiuso. Il circuito è chiuso.

Trap configuration

Send trap

Attiva/disattiva l'invio di trap SNMP se il dispositivo rileva una modifica in una funzione monitorata.

Possibili valori:

- `selezionato`
  L'invio di trap SNMP è attivo.
  Se il dispositivo rileva una modifica nelle funzioni monitorate, il dispositivo invia una trap SNMP.
- `non selezionato` (impostazione di default)
  L'invio di trap SNMP non è attivo.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Monitoring correct operation

Nella tabella si specificano i parametri che il dispositivo monitora. Il dispositivo segnala il verificarsi di un evento aprendo il contatto di segnalazione.

Connection errors

Attiva/disattiva il monitoraggio dello stato del link della porta/interfaccia.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Se il link si interrompe su una porta/interfaccia monitorata, il contatto di segnalazione si apre.
  Nella scheda *Port*, è possibile selezionare le porte/interfacce da monitorare singolarmente.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Temperature

Attiva/disattiva il monitoraggio della temperatura nel dispositivo.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Se la temperatura eccede / è inferiore ai valori soglia, il contatto di segnalazione si apre.
- `non selezionato`
  Il monitoraggio non è attivo.

Si specificano le soglie di temperatura nella finestra di dialogo *Basic Settings > System*, campo *Upper temp. limit [°C]* e il campo *Lower temp. limit [°C]* .

Ring redundancy

Attiva/disattiva il monitoraggio della ridondanza ad anello.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  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.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

External memory removed

Attiva/disattiva il monitoraggio della memoria esterna attiva.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Rimuovendo la memoria esterna attiva dal dispositivo, il contatto di segnalazione si apre.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

External memory not in sync with NVM

Attiva/disattiva il monitoraggio del profilo di configurazione nel dispositivo e nella memoria esterna.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  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.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Ethernet loops

Attiva/disattiva il monitoraggio di loop Ethernet di Layer 2. Le impostazioni della funzione *Loop Protection* si specificano nella finestra di dialogo *Diagnostics > Loop Protection*.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Se il dispositivo rileva un loop Ethernet, il contatto di segnalazione si apre.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Power supply

Attiva/disattiva il monitoraggio dell'alimentatore.

Possibili valori:

- `selezionato` (impostazione di default)
  Il monitoraggio è attivo.
  Se il dispositivo presenta un errore di alimentazione di tensione rilevato, il contatto di segnalazione si apre.
- `non selezionato`
  Il monitoraggio non è attivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Port]

Tabella

Port

Visualizza il numero di porta.

Propagate connection error

Attiva/disattiva il monitoraggio del link sulla porta/interfaccia.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  Se il link si interrompe sulla porta/interfaccia selezionata, il contatto di segnalazione si apre.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Questa impostazione viene applicata quando si seleziona la casella di spunta *Connection errors* nella scheda *Global*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Status]

Tabella

Timestamp

Visualizza la data e l'ora dell'evento nel formato, `mese giorno, anno hh:mm:ss AM/PM`.

Cause

Visualizza l'evento che ha causato la trap SNMP.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.1.4 MAC Notification

[Diagnostics > Status Configuration > MAC Notification]

Il dispositivo consente di tracciare le modifiche nella rete utilizzando l'indirizzo MAC dei dispositivi nella rete. Il dispositivo salva la combinazione di porta e indirizzo MAC nella relativa tabella di indirizzi MAC. Se il dispositivo (dis)apprende l'indirizzo MAC di un dispositivo (dis)connesso, il dispositivo invia una trap SNMP.

Questa funzione è pensata per le porte alle quali si connettono dispositivi finali e quindi l'indirizzo MAC modifica in modo non frequente.

Operation

Operation

Abilita/disabilita la funzione *MAC Notification* nel dispositivo.

Possibili valori:

- `On`
  È abilitata la funzione *MAC Notification*.
- `Off` (impostazione di default)
  È disabilitata la funzione *MAC Notification*.

Configuration

Interval [s]

Specifica l'intervallo di invio in secondi. Se il dispositivo (dis)apprende l'indirizzo MAC di un dispositivo (dis)connesso, il dispositivo invia una trap SNMP trascorso questo periodo di tempo.

Possibili valori:

- `0..2147483647` (impostazione di default: `30`)

Prima di inviare una trap SNMP, il dispositivo registra fino a 20°indirizzi MAC. Se il dispositivo rileva un numero elevato di modifiche, il dispositivo invia la trap SNMP prima che termini l'intervallo di invio.

Tabella

Port

Visualizza il numero di porta.

Active

Attiva/disattiva la funzione *MAC Notification* sulla porta.

Possibili valori:

- `selezionato`
  La funzione *MAC Notification* è attiva sulla porta.
  Il dispositivo invia una trap SNMP in caso di uno dei seguenti eventi:
  - Il dispositivo apprende l'indirizzo MAC di un dispositivo nuovo connesso.
  - Il dispositivo disapprende l'indirizzo MAC di un dispositivo disconnesso.
- `non selezionato` (impostazione di default)
  La funzione *MAC Notification* non è attiva sulla porta.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Last MAC address

Visualizza l'indirizzo MAC del dispositivo connesso per ultimo o disconnesso dalla porta.

Il dispositivo rileva gli indirizzi MAC dei dispositivi che sono connessi come di seguito indicato:

- Connessione diretta alla porta
- Connessione alla porta attraverso altri dispositivi nella rete

Last MAC status

Visualizza lo stato del valore *Last MAC address* su questa porta.

Possibili valori:

- `added`
  Il dispositivo ha rilevato che un altro dispositivo era connesso alla porta.
- `removed`
  Il dispositivo ha rilevato che il dispositivo è stato rimosso dalla porta.
- `other`
  Il dispositivo non ha rilevato uno stato.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.1.5 Alarms (Traps)

[Diagnostics > Status Configuration > Alarms (Traps)]

Il dispositivo consente di inviare una trap SNMP come una reazione a specifici eventi. In questa finestra di dialogo, si specificano le destinazioni delle trap a cui il dispositivo invia le trap SNMP.

Gli eventi per i quali il dispositivo attiva una trap SNMP si specificano, ad esempio, nelle seguenti finestre di dialogo:
- Nella finestra di dialogo *Diagnostics > Status Configuration > Device Status*
- Nella finestra di dialogo *Diagnostics > Status Configuration > Security Status*
- Nella finestra di dialogo *Diagnostics > Status Configuration > MAC Notification*

Operation

Operation

Abilitare/disabilitare l'invio di trap SNMP alle destinazioni trap.

Possibili valori:
- `On` (impostazione di default)
  L'invio di trap SNMP è abilitato.
- `Off`
  L'invio di trap SNMP è disabilitato.

Tabella

Name

Specifica il nome della destinazione trap.

Possibili valori:
- Stringa di caratteri ASCII alfanumerici con 1..32 caratteri

Address

Specifica l'indirizzo IP e il numero di porta della destinazione trap.

Possibili valori:
- `<Indirizzo IPv4 valido>: <numero di porta>`

Active

Attiva/disattiva l'invio di trap SNMP a questa destinazioni trap.

Possibili valori:
- `selezionato` (impostazione di default)
  L'invio di trap SNMP a questa destinazione trap è attiva.
- `non selezionato`
  L'invio di trap SNMP a questa destinazione trap non è attivo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Apre la finestra *Create* per aggiungere una nuova voce alla tabella.

- Nel campo *Name*, si specifica un nome per la destinazione trap.
- Nel campo *Address* si specifica l'indirizzo IP e il numero di porta della destinazione trap. Scegliendo di non inserire un numero di porta, il dispositivo aggiunge automaticamente il numero di porta `162`.

6.2 System

[Diagnostics > System]

Il menu include le seguenti finestre di dialogo:

- System Information
- Hardware State
- IP Address Conflict Detection
- ARP
- Selftest

6.2.1 System Information

[Diagnostics > System > System Information]

Questa finestra di dialogo visualizza l'attuale condizione di funzionamento dei singoli componenti nel dispositivo. I valori visualizzati sono uno snapshot; rappresentano la condizione di funzionamento nel momento in cui la finestra di dialogo è stata caricata sulla pagina.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Save system information

Apre la pagina HTML in una nuova finestra o scheda del browser Web. È possibile salvare la pagina HTML sul PC utilizzando il comando del browser Web corretto.

6.2.2 Hardware State

[Diagnostics > System > Hardware State]

Questa finestra di dialogo fornisce le informazioni sulla distribuzione e lo stato della flash memory del dispositivo.

Information

Uptime

Visualizza il tempo di funzionamento totale del dispositivo dalla data di consegna.

Possibili valori:

▶ `..d ..h ..m ..s`
Giorno(i) Ora(e) Minuto(i) Secondo(i)

Tabella

Flash region

Visualizza il nome della rispettiva area di memoria.

Description

Visualizza una descrizione della destinazione d'uso dell'area di memoria.

Flash sectors

Visualizza quanti settori sono assegnati all'area di memoria.

Sector erase operations

Visualizza quante volte il dispositivo ha sovrascritto i settori dell'area di memoria.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.2.3 IP Address Conflict Detection

[Diagnostics > System > IP Address Conflict Detection]

Utilizzando la funzione *IP Address Conflict Detection*, il dispositivo verifica che il suo indirizzo IP sia univoco nella rete. Allo scopo il dispositivo analizza i pacchetti ARP ricevuti.

In questa finestra di dialogo si specifica la procedura con la quale i dispositivo rileva conflitti tra indirizzi e ne specifica le impostazioni.

Il dispositivo visualizza i conflitti tra indirizzi rilevati nella tabella.

Quando il dispositivo rileva un conflitto tra indirizzi, il LED di stato del dispositivo lampeggia di rosso per 4 volte.

Operation

Operation

Abilita/disabilita la funzione *IP Address Conflict Detection*.

Possibili valori:

- `On` (impostazione di default)
  È abilitata la funzione *IP Address Conflict Detection*.
  Il dispositivo verifica che il suo indirizzo IP sia univoco nella rete.
- `Off`
  È disabilitata la funzione *IP Address Conflict Detection*.

Configuration

Detection mode

Specifica la procedura con la quale il dispositivo riconosce conflitti tra indirizzi.

Possibili valori:

- `active and passive` (impostazione di default)
  Il dispositivo utilizza il rilevamento attivo e passivo di conflitti tra indirizzi.

- *active*
  Rilevamento attivo di conflitti tra indirizzi. Il dispositivo consente attivamente di evitare la comunicazione con un indirizzo IP che esiste già in rete. Il rilevamento di conflitti tra indirizzi inizia non appena si connette il dispositivo alle rete oppure si modificano i rispettivi parametri IP.
  - Il dispositivo invia 4 pacchetti di dati di probe ARP all'intervallo specificato nel campo *Detection delay [ms]*. Se il dispositivo riceve una risposta a questi pacchetti di dati, sussiste un conflitto tra indirizzi.
  - Se il dispositivo non rileva un conflitto tra indirizzi, invia 2 pacchetti di dati ARP gratuiti come un annuncio. Il dispositivo invia anche questi pacchetti di dati quando il rilevamento conflitti tra indirizzi è disabilitato.
  - Se l'indirizzo IP esiste già nella rete, il dispositivo ritorna ai parametri IP utilizzati in precedenza (se possibile).
    Se il dispositivo riceve i parametri IP da un server DHCP, rinvia un messaggio DHCPDECLINE al server DHCP.
  - Terminato il periodo di tempo specificato nel campo *Release delay [s]*, il dispositivo verifica se esiste ancora il conflitto tra indirizzi. Quando il dispositivo rileva 10 conflitti tra indirizzi in sequenza, il dispositivo allunga il tempo di attesa per la verifica successiva a 60 s.
  - Quando il dispositivo risolve il conflitto tra indirizzi, la gestione dispositivi ritorna alla rete.
- *passive*
  Rilevamento passivo di conflitti tra indirizzi. Il dispositivo analizza il traffico dati nella rete. Se un altro dispositivo nella rete sta utilizzando lo stesso indirizzo IP, il dispositivo “difende” inizialmente il suo indirizzo IP. Il dispositivo interrompe l'invio se l'altro dispositivo continua a inviare con lo stesso indirizzo IP.
  - Come “difesa” il dispositivo invia pacchetti di dati ARP gratuiti. Il dispositivo ripete questa procedura per il numero di volte specificato nel campo *Address protections*.
  - Se l'altro dispositivo continua a inviare con lo stesso indirizzo IP, dopo il periodo di tempo specificato nel campo *Release delay [s]*, il dispositivo verifica periodicamente se esiste ancora il conflitto tra indirizzi.
  - Quando il dispositivo risolve il conflitto tra indirizzi, la gestione dispositivi ritorna alla rete.

Send periodic ARP probes

Attiva/disattiva il rilevamento periodico di conflitti tra indirizzi.

Possibili valori:

- selezionato (impostazione di default)
  Il rilevamento periodico di conflitti tra indirizzi è attivo.
  - Il dispositivo invia periodicamente un pacchetto di dati di probe ARP ogni 90 -150 secondi e attende per il periodo di tempo specificato nel campo *Detection delay [ms]* per una risposta.
  - Se il dispositivo rileva un conflitto tra indirizzi, il dispositivo attiva la modalità di rilevamento passivo. Se la funzione *Send trap* è attiva, il dispositivo invia una trap SNMP.
- non selezionato
  Il rilevamento periodico di conflitti tra indirizzi non è attivo.

Detection delay [ms]

Specifica il periodo in millisecondi per cui il dispositivo attende una risposta dopo l'invio di un pacchetto di dati ARP.

Possibili valori:

- `20..500` (impostazione di default: `200`)

Release delay [s]

Specifica il periodo in secondi dopo il quale il dispositivo verifica nuovamente se esiste ancora il conflitto tra indirizzi.

Possibili valori:

- `3..3600` (impostazione di default: `15`)

Address protections

Specifica quante volte il dispositivo invia pacchetti di dati ARP gratuiti nella modalità di rilevamento passivo per “difendere” il suo indirizzo IP.

Possibili valori:

- `0..100` (impostazione di default: `3`)

Protection interval [ms]

Specifica il periodo di tempo in millisecondi dopo il quale il dispositivo invia nuovamente pacchetti di dati ARP gratuiti in modalità di rilevamento passivo per “difendere” il suo indirizzo IP.

Possibili valori:

- `20..5000` (impostazione di default: `200`)

Send trap

Attiva/disattiva l'invio di trap SNMP quando il dispositivo rileva un conflitto tra indirizzi.

Possibili valori:

- `selezionato`
  L'invio di trap SNMP è attivo.
  Se il dispositivo rileva un conflitto tra indirizzi, il dispositivo invia una trap SNMP.
- `non selezionato` (impostazione di default)
  L'invio di trap SNMP non è attivo.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Information

Conflict detected

Visualizza se attualmente esiste un conflitto tra indirizzi.

Possibili valori:

- `selezionato`
  Il dispositivo rileva un conflitto tra indirizzi.
- `non selezionato`
  Il dispositivo non rileva un conflitto tra indirizzi.

Tabella

Timestamp

Visualizza l'orario in cui il dispositivo rileva un conflitto tra indirizzi.

Port

Visualizza il numero della porta su cui il dispositivo ha rilevato il conflitto tra indirizzi.

IP address

Visualizza l'indirizzo IP che causa il conflitto tra indirizzi.

MAC address

Visualizza l'indirizzo MAC del dispositivo con cui esiste il conflitto tra indirizzi.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.2.4 ARP

[Diagnostics > System > ARP]

Questa finestra di dialogo visualizza gli indirizzi MAC e IP dei dispositivi adiacenti connessi alla gestione dispositivo.

Il dispositivo può visualizzare sia indirizzi IPv4 sia indirizzi IPv6. Per il protocollo IPv6 gli indirizzi dei dispositivi adiacenti vengono ottenuti utilizzando il protocollo Neighbor Discovery Protocol (NDP).

Tabella

Port

Visualizza il numero di porta.

IP address

Visualizza l'indirizzo IPv4o l'indirizzo IPv6 di un dispositivo adiacente.

MAC address

Visualizza l'indirizzo MAC di un dispositivo adiacente.

Last updated

Visualizza il tempo in secondi da quando le attuali impostazioni della voce sono state registrate nella tabella ARP.

Type

Visualizza il tipo della voce.

Possibili valori:

- `static`
  Voce statica. Quando la tabella ARP è rimossa, il dispositivo mantiene la voce statica.
- `dynamic`
  Voce dinamica. Quando viene superato*Aging time [s]* e il dispositivo non riceve dati da questo dispositivo durante questo periodo di tempo, il dispositivo rimuove la voce dinamica.
- `local`
  indirizzo IP e indirizzo MAC della gestione dispositivi.

Active

Visualizza che la tabella ARP contiene l'assegnazione dell'indirizzo IP/MAC come una voce attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset ARP table

Rimuove gli indirizzi impostati dinamicamente dalla tabella ARP.

6.2.5 Selftest

[Diagnostics > System > Selftest]

Questa finestra di dialogo consente le seguenti operazioni:
- Attivare/disattivare il RAM test quando il dispositivo viene avviato.
- Abilitare/disabilitare l'opzione di inserimento del monitor di sistema all'avvio del sistema.
- Specificare come il dispositivo si comporta in caso di un errore rilevato.

Configuration

Se il dispositivo non rileva profili di configurazione leggibili al riavvio, le seguenti impostazioni bloccano permanentemente l'accesso al dispositivo.
- La casella di spunta *SysMon1 is available* è impostata su `non selezionato`.
- La casella di spunta *Load default config on error* è impostata su `non selezionato`.

Questo è ad esempio il caso se 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.

RAM test

Attiva/disattiva la verifica della memoria RAM durante il riavvio.

Possibili valori:
- `selezionato` (impostazione di default)
  La verifica della memoria RAM è attivata. Durante il riavvio, il dispositivo verifica la memoria RAM.
- `non selezionato`
  La verifica della memoria RAM è disattivata. Questa condizione accorcia il tempo di avvio del dispositivo.

SysMon1 is available

Attiva/disattiva l'accesso al monitor di sistema durante il riavvio.

Possibili valori:
- `selezionato` (impostazione di default)
  Il dispositivo consente di aprire il monitor di sistema durante il riavvio.
- `non selezionato`
  Il dispositivo si avvia senza l'opzione di apertura del monitor di sistema.

Tra le altre cose, il monitor di sistema consente l'aggiornamento del software del dispositivo e l'eliminazione dei profili di configurazione salvati.

Load default config on error

Attiva/disattiva il caricamento delle impostazioni di default se il dispositivo non rileva profili di configurazione leggibili al riavvio.

Possibili valori:

- `selezionato` (impostazione di default)
  Il dispositivo carica le impostazioni di default.
- `non selezionato`
  Il dispositivo interrompe il riavvio e si arresta. L'accesso alla gestione del dispositivo è possibile solo utilizzando la Command Line Interface attraverso l'interfaccia seriale.
  Per ottenere nuovamente l'accesso al dispositivo attraverso la rete, aprire il monitor di sistema e ripristinare le impostazioni. Al riavvio, Il dispositivo carica le impostazioni di default.

Tabella

In questa tabella, si specifica come il dispositivo si comporta in caso di un errore rilevato.

Cause

Cause di errori rilevati alle quali il dispositivo reagisce.

Possibili valori:

- `task`
  Il dispositivo rileva errore nell'applicazione eseguita, ad esempio se un'attività finisce oppure non è disponibile.
- `resource`
  Il dispositivo rileva errori nelle risorse disponibili, ad esempio se la memoria disponibile si sta esaurendo.
- `software`
  Il dispositivo rileva errori software, ad esempio errori nel controllo di coerenza.
- `hardware`
  Il dispositivo rileva errori hardware, ad esempio nel chipset.

Action

Specifica come il dispositivo si comporta se si verifica un evento adiacente.

Possibili valori:

- `reboot` (impostazione di default)
  Il dispositivo attiva un riavvio.
- `logOnly`
  Il dispositivo registra l'errore rilevato nel file di registrato. Vedere la finestra di dialogo *Diagnostics > Report > System Log*.
- `sendTrap`
  Il dispositivo invia una trap SNMP.
  Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.3 Email Notification

[Diagnostics > Email Notification]

Il dispositive consente di informare tramite e-mail destinatari multipli sugli eventi che si sono verificati.

Il dispositivo invia le e-mail immediatamente o periodicamente, in base alla gravità dell'evento. Solitamente per gli eventi molto gravi si imposta l'invio immediato.

È possibile specificare destinatari multipli a cui il dispositivo invia le e-mail immediatamente o periodicamente.

Il menu include le seguenti finestre di dialogo:
- Email Notification Global
- Email Notification Recipients
- Email Notification Mail Server

6.3.1 Email Notification Global

[Diagnostics > Email Notification > Global]

In questa finestra di dialogo si specificano le impostazioni del mittente. Inoltre, si specifica per quali livelli di gravità degli eventi il dispositivo invia le e-mail immediatamente o periodicamente.

Operation

Operation

Abilita/disabilità l'invio di e-mail:

Possibili valori:

- *On*
  L'invio delle e-mail è abilitato.
- *Off* (impostazione di default)
  L'invio delle e-mail è disabilitato.

Certificate

Il dispositivo può inviare messaggi a un server attraverso reti non protette. Per contribuire a bloccare un attacco man in the middle, richiedere all'autorità di certificazione la creazione di un certificato per il server. Configurare il server per utilizzare il certificato. Trasferire il certificato sul dispositivo.

Se si specificano le impostazioni per i server e-mail, utilizzare l'indirizzo IP o il nome DNS indicati nel certificato come `Common Name` o `Subject Alternative Name`. Altrimenti la convalida del certificato non avverrà correttamente.

URL

Specifica il percorso e il nome file del certificato.

Il dispositivo accetta i certificati con le seguenti proprietà:

- Formato X.509
- Estensione nome file `.PEM`
- Codifica Base64, compreso tra
  `-----BEGIN CERTIFICATE-----`
  e
  `-----END CERTIFICATE-----`

Per motivi di sicurezza si raccomanda di utilizzare regolarmente un certificato firmato da un'autorità di certificazione.

Il dispositivo rende disponibili le seguenti opzioni per la copia del certificato nel dispositivo:

- Importazione dal PC
  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.

- Importazione da un server FTP
  Se il certificato si trova su un server TFTP, specificare l'URL per il file nella seguente forma:
  `ftp://<Utente>:<Password>@<Indirizzo IP>:<Porta>/<Percorso>/<Nome file>`
- Importazione da un server TFTP
  Se il certificato si trova su un server TFTP, specificare l'URL per il file nella seguente forma:
  `tftp://<Indirizzo IP>/<Percorso>/<Nome file>`
- Importazione da un server SCP o SFTP
  Se il certificato si trova su un server SCP o SFTP, specificare l'URL per il file nella seguente forma:
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`
    Facendo clic sul pulsante *Start*, il dispositivo visualizza la finestra *Credentials*. Qui si inseriscono *User name* e *Password* per accedere al server.
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`

Start

Copia il certificato specificato nel campo *URL* sul dispositivo.

Sender

Address

Specifica l'indirizzo e-mail del dispositivo.

Il dispositivo invia le e-mail utilizzando questo indirizzo e-mail come mittente.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Notification immediate

Qui è possibile specificare le impostazioni per le e-mail che il dispositivo invia immediatamente.

Severity

Specifica il livello minimo di gravità degli eventi per cui il dispositivo invia un'e-mail immediatamente. Se si verifica un evento con questo livello di gravità o più urgente, il dispositivo invia un'e-mail ai destinatari.

Possibili valori:

- *emergency*
- *alert* (impostazione di default)
- *critical*
- *error*
- *warning*
- *notice*
- *informational*
- *debug*

Subject

Specifica l'oggetto dell'e-mail.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Notification periodic

Qui è possibile specificare le impostazioni per le e-mail che il dispositivo invia periodicamente.

Severity

Specifica il livello minimo di gravità degli eventi per cui il dispositivo invia un'e-mail periodicamente. Se si verifica un evento con questo livello di gravità o più urgente, il dispositivo registra l'evento nel buffer. Il dispositivo invia il contenuto del buffer periodicamente o quando il buffer è pieno.

Se si verifica un evento con livello di gravità inferiore, il dispositivo non registra l'evento nel buffer.

Possibili valori:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (impostazione di default)
- *notice*
- *informational*
- *debug*

Subject

Specifica l'oggetto dell'e-mail.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Sending interval [min]

Specifica l'intervallo di invio in minuti.

Se il dispositivo ha registrato almeno un evento, allo scadere del tempo il dispositivo invia un'e-mail contenente il file di registro.

Possibili valori:

- `30..1440` (impostazione di default: `30`)

Send

Invia immediatamente un'e-mail con il contenuto del buffer e lo svuota.

Information

Sent messages

Visualizza quante volte il dispositivo ha correttamente inviato un'e-mail al server di posta.

Undeliverable messages

Visualizza quante volte il dispositivo ha tentato di inviare un'e-mail al server di posta senza successo.

Time of the last messages sent

Visualizza il giorno e l'orario in cui il dispositivo ha inviato l'ultima e-mail al server di posta.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Clear email notification statistics

Ripristina i contatori nel frame *Information* su `0`.

Significato dei livelli di gravità evento

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

6.3.2 Email Notification Recipients

[Diagnostics > Email Notification > Recipients]

In questa finestra di dialogo si specificano i destinatari a cui il dispositivo invia le e-mail. Il dispositivo consente di specificare fino a 10 destinatari.

Tabella

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Notification type

Specifica se il dispositivo invia le e-mail a questo destinatario immediatamente o periodicamente.

Possibili valori:

- *immediate*
  Il dispositivo invia le e-mail a questo destinatario immediatamente.
- *periodic*
  Il dispositivo invia le e-mail a questo destinatario periodicamente.

Address

Specifica l'indirizzo e-mail del destinatario.

Possibili valori:

- Indirizzo e-mail valido con fino a 255 caratteri

Active

Attiva/disattiva l'attività di informazione del destinatario.

Possibili valori:

- `selezionato` (impostazione di default)
  L'attività di informazione del destinatario è attiva.
- `non selezionato`
  L'attività di informazione del destinatario non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.3.3 Email Notification Mail Server

[Diagnostics > Email Notification > Mail Server]

In questa finestra di dialogo si specificano le impostazioni per i server di posta. Il dispositivo supporta le connessioni al server di posta crittografate e non crittografate.

Tabella

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Description

Specifica il nome del server.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

IP address

Specifica l'indirizzo IP o il nome DNS del server.

Possibili valori:

- Indirizzo IPv4 valido (impostazione di default: `0.0.0.0`)
- Nome DNS nel formato `domain.tld` o `host.domain.tld`
  Se si specifica un nome DNS si abilita anche la funzione *Client* nella finestra di dialogo *Advanced > DNS > Client > Global*.
  Se si stabilisce una connesione crittografata utilizzando il certificato, verificare che il nome DNS sia uguale al nome del server DNS indicato nel certificato.

Destination TCP port

Specifica la porta TCP del server.

Possibili valori:

- `1..65535` (impostazione di default: `25`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Porte TCP usate di frequente:

- SMTP `25`
- Message Submission `587`

Encryption

Specifica il protocollo che crittografa la connessione tra il dispositivo e il server di posta.

Possibili valori:

- `none` (impostazione di default)
  Il dispositivo stabilisce una connessione non crittografata al server.
- `tlsv1`
  Il dispositivo stabilisce una connessione crittografata al server utilizzando l'estensione startTLS.

User name

Specifica il nome utente dell'account che il dispositivo utilizza per l'autenticazione sul server di posta.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Password

Specifica la password dell'account che il dispositivo utilizza per l'autenticazione sul server di posta.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Timeout [s]

Specifica il tempo in secondi dopo il quale il dispositivo invia nuovamente un'e-mail. Il prerequisito è che il dispositivo non sia riuscito a inviare l'e-mail completa a causa di un errore di connessione.

Possibili valori:

- `1..15` (impostazione di default: `3`)

Active

Attiva/disattiva l'utilizzo del server di posta.

Possibili valori:

- `selezionato`
  Il server di posta è attivo.
  Il dispositivo invia e-mail a questo server di posta.
- `non selezionato` (impostazione di default)
  Il server di posta non è attivo.
  Il dispositivo non invia e-mail a questo server di posta.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Connection test

Apre la finestra di dialogo *Connection test* per l'invio di un'e-mail di prova.

Se le impostazioni del server di posta sono corrette, i destinatari selezionati ricevono un'e-mail di prova.

- Nel campo *Recipient*, specificare a quali destinatari il dispositivo invia l'e-mail di prova:
  - *immediate*
    Il dispositivo invia l'e-mail di prova ai destinatari a cui il dispositivo invia le e-mail immediatamente.
  - *periodic*
    Il dispositivo invia l'e-mail di prova ai destinatari a cui il dispositivo invia le e-mail periodicamente.
- Nel campo *Message text*, specificare il testo dell'e-mail di prova.

6.4 Syslog

[Diagnostics > Syslog]

Il dispositivo consente di segnalare eventi selezionati, indipendentemente dalla gravità dell'evento, a diversi server syslog. In questa finestra di dialogo, si specificano le impostazioni per questa funzione e si gestiscono fino a 8 server syslog.

Operation

Operation

Abilita/disabilita l'invio di eventi ai server syslog.

Possibili valori:

- *On*
  L'invio di eventi è abilitato.
  Il dispositivo invia gli eventi specificati nella tabella ai server syslog specificati.
- *Off* (impostazione di default)
  L'invio di eventi è disabilitato.

Certificate

Il dispositivo può inviare messaggi a un server attraverso reti non protette. Per contribuire a bloccare un attacco man in the middle, richiedere all'autorità di certificazione la creazione di un certificato per il server. Configurare il server per utilizzare il certificato. Trasferire il certificato sul dispositivo.

Se si specificano i parametri sul server, verificare che siano specificati l'indirizzo IP e il nome DNS indicati come `Common Name` o `Subject Alternative Name` nel certificato. Altrimenti la convalida del certificato non avverrà correttamente.

Nota: Per abilitare le modifiche dopo il caricamento di un nuovo certificato, riavviare la funzione *Syslog*.

URL

Specifica il percorso e il nome file del certificato.

Il dispositivo accetta i certificati con le seguenti proprietà:

- Formato X.509
- Estensione nome file `.PEM`
- Codifica Base64, compreso tra
  `-----BEGIN CERTIFICATE-----`
  e
  `-----END CERTIFICATE-----`

Per motivi di sicurezza si raccomanda di utilizzare regolarmente un certificato firmato da un'autorità di certificazione.

Il dispositivo rende disponibili le seguenti opzioni per la copia del certificato nel dispositivo:

- Importazione dal PC

  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.
- Importazione da un server FTP
  Se il certificato si trova su un server TFTP, specificare l'URL per il file nella seguente forma:
  `ftp://<Utente>:<Password>@<Indirizzo IP>:<Porta>/<Percorso>/<Nome file>`
- Importazione da un server TFTP
  Se il certificato si trova su un server TFTP, specificare l'URL per il file nella seguente forma:
  `tftp://<Indirizzo IP>/<Percorso>/<Nome file>`
- Importazione da un server SCP o SFTP
  Se il certificato si trova su un server SCP o SFTP, specificare l'URL per il file nella seguente forma:
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`
    Facendo clic sul pulsante *Start*, il dispositivo visualizza la finestra *Credentials*. Qui si inseriscono *User name* e *Password* per accedere al server.
  - `scp://` o `sftp://<Indirizzo IP>/<Percorso>/<Nome file>`

Start

Copia il certificato specificato nel campo *URL* sul dispositivo.

Tabella

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Quando si elimina una voce della tabella rimane un buco nella numerazione. Quando si crea una nuova voce della tabella, il dispositivo riempie il primo buco.

Possibili valori:

- `1..8`

IP address

Specifica l'indirizzo IP del server syslog.

Possibili valori:

- Indirizzo IPv4 valido (impostazione di default: `0.0.0.0`)
- Indirizzo IPv6 valido
- Nome host

Destination UDP port

Specifica la porta TCP o UDP sulla quale il server syslog attende le voci di registro.

Possibili valori:

- `1..65535` (impostazione di default: `514`)

Transport type

Visualizza il tipo di trasporto che il dispositivo utilizza per inviare gli eventi al server syslog.

Possibili valori:

- `udp`(impostazione di default)
  Il dispositivo invia gli eventi attraverso la porta UDP specificata nella colonna *Destination UDP port*.
- `tls`
  Il dispositivo invia gli eventi attraverso TLS sulla TCP specificata nella colonna *Destination UDP port*.

Min. severity

Specifica la minima gravità degli eventi. Il dispositivo invia una voce di registro per eventi di questa gravità e di maggiore urgenza al server syslog.

Possibili valori:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (impostazione di default)
- `notice`
- `informational`
- `debug`

Type

Specifica il tipo di voce di registro trasmessa dal dispositivo.

Possibili valori:

- `systemlog` (impostazione di default)
- `audittrail`

Active

Attiva/disattiva la trasmissione di eventi al server syslog.

- `selezionato`
  Il dispositivo invia eventi al server syslog.
- `non selezionato` (impostazione di default)
  La trasmissione di eventi al server syslog è disattivata.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.5 Ports

[Diagnostics > Ports]

Il menu include le seguenti finestre di dialogo:

- SFP
- TP cable diagnosis
- Port Monitor
- Auto-Disable
- Port Mirroring

6.5.1 SFP

[Diagnostics > Ports > SFP]

La finestra di dialogo consente di esaminare i ricetrasmettitori SFP attualmente connessi al dispositivo e le rispettive proprietà.

Tabella

La tabella visualizza valori validi se il dispositivo è equipaggiato con ricetrasmettitori SFP.

Port

Visualizza il numero di porta.

Module type

Tipo del ricetrasmettitore SFP, ad esempio M-SFP-SX/LC.

Serial number

Visualizza il numero di serie del ricetrasmettitore SFP.

Connector type

Visualizza il tipo di connettore.

Supported

Visualizza se il dispositivo supporta il ricetrasmettitore SFP.

Temperature [°C]

La temperatura di funzionamento del ricetrasmettitore SFP in gradi Celsius.

Tx power [mW]

La potenza di trasmissione del ricetrasmettitore SFP in mW.

Rx power [mW]

La potenza di ricezione del ricetrasmettitore SFP in mW.

Tx power [dBm]

La potenza di trasmissione del ricetrasmettitore SFP in dBm.

Rx power [dBm]

La potenza di ricezione del ricetrasmettitore SFP in dBm.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.5.2 TP cable diagnosis

[Diagnostics > Ports > TP cable diagnosis]

Questa funzione consente di sottoporre a test i cavi collegati a un'interfaccia per un cortocircuito o un circuito aperto. La tabella mostra lo stato dei cavi e la lunghezza stimata. Il dispositivo visualizza, inoltre, i singoli doppini collegati alla porta. Quando il dispositivo rileva un cortocircuito o un circuito aperto nel cavo, visualizza anche la distanza stimata al problema.

Per ricevere risultati affidabili utilizzare la funzione *TP cable diagnosis* perdoppino intrecciato con lunghezza minima di 3 metri.

Nota: Questo test interrompe il traffico sulla porta.

Information

Port

Visualizza il numero di porta.

Status

Stato del Tester dei cavi virtuali

Possibili valori:

- *active*
  Il test dei cavi è in corso.
  Per avviare il test, fare clic sul pulsante ☰ e poi sulla voce *Start cable diagnosis...*. Questa azione apre la finestra di dialogo *Select port*.
- *success*
  Il dispositivo visualizza questa voce dopo aver effettuato correttamente un test.
- *failure*
  Il dispositivo visualizza questa voce dopo un'interruzione nel test.
- *uninitialized*
  Il dispositivo visualizza questa voce mentre si trova in modalità standby.

Tabella

Cable pair

Visualizza il doppino a cui fa riferimento la voce. Il dispositivo utilizza il primo indice PHY supportato per visualizzare i valori.

Result

Mostra i risultati del test del cavo.

Possibili valori:

- *normal*
  Il cavo funziona correttamente.

- *open*
  Nel cavo è presente una rottura che provoca un'interruzione.
- *short*
  I fili nel cavo entrano in contatto tra loro provocando un cortocircuito.
- *unknown*
  Il dispositivo visualizza questo valore per doppini non sottoposti a test.

Il dispositivo visualizza valori diversi da quelli previsti nei seguenti casi:

- Se alla porta non è collegato alcun cavo, il dispositivo mostra il valore *unknown* invece di *open*.
- Se la porta è disattivata, il dispositivo mostra il valore *short*.

Min. length

Mostra la lunghezza minima stimata del cavo in metri.

Se la lunghezza del cavo non è nota o se nel frame *Information* il campo *Status* mostra il valore *active*, *failure* oppure *uninitialized*, il dispositivo visualizza il valore 0.

Max. length

Mostra la lunghezza massima stimata del cavo in metri.

Se la lunghezza del cavo non è nota o se nel frame *Information* il campo *Status* mostra il valore *active*, *failure* oppure *uninitialized*, il dispositivo visualizza il valore 0.

Distance [m]

Mostra la distanza stimata in metri da un'estremità all'altra del cavo oppure fino a un'interruzione nel cavo.

Se la lunghezza del cavo non è nota o se nel frame *Information* il campo *Status* mostra il valore *active*, *failure* oppure *uninitialized*, il dispositivo visualizza il valore 0.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Start cable diagnosis...

Apre la finestra di dialogo *Select port*.

Nella lista a discesa *Port*, si seleziona la porta da sottoporre a test. Utilizzare unicamente per le porte in rame.

Per avviare il test dei cavi nella porta selezionata, fare clic sul pulsante *Ok*.

6.5.3 Port Monitor

[Diagnostics > Ports > Port Monitor]

La funzione *Port Monitor* monitora l'aderenza ai parametri specificati sulle porte. Se la funzione *Port Monitor* rileva che i parametri vengono superati, il dispositivo esegue un'azione.

Per applicare la funzione *Port Monitor*, eseguire i seguenti passaggi:
- Scheda *Global*
  - Abilita la funzione *Operation* nel frame *Port Monitor*.
  - Per ogni porta, attivare quei parametri per i quasi si desidera il monitoraggio tramite la funzione *Port Monitor*.
- Schede *Link flap*, *CRC/Fragments* e *Overload detection*
  - Specificare i valori soglia per i parametri di ogni porta.
- Scheda *Link speed/Duplex mode detection*
  - Attiva le combinazioni consentite di velocità e modalità duplex per ogni porta.
- Scheda *Global*
  - Per ogni porta specifica un'azione che il dispositivo esegue se la funzione *Port Monitor* rileva il superamento dei parametri.
- Scheda *Auto-disable*
  - Spuntare la casella di spunta *Auto-disable* per i parametri monitorati se si è specificata l'azione `auto-disable` almeno una volta.

Questa finestra di dialogo include le seguenti schede:
- [Global]
- [Auto-disable]
- [Link flap]
- [CRC/Fragments]
- [Overload detection]
- [Link speed/Duplex mode detection]

[Global]

In questa scheda, si abilita la funzione *Port Monitor* e si specificano i parametri che la funzione *Port Monitor* sta monitorando. Inoltre, specifica l'azione che il dispositivo esegue se la funzione *Port Monitor* rileva il superamento dei parametri.

Operation

Operation

Abilita/disabilita la funzione *Port Monitor* globalmente.

Possibili valori:
- `On`
  È abilitata la funzione *Port Monitor*.
- `Off` (impostazione di default)
  È disabilitata la funzione *Port Monitor*.

Tabella

Port

Visualizza il numero di porta.

Link flap on

Attiva/disattiva il monitoraggio dei link flap sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  - La funzione *Port Monitor* monitora i link flap a sulla porta.
  - Se il dispositivo rileva troppi link flap, il dispositivo esegue l'azione specificata nella colonna *Action*.
  - Nella scheda *Link flap*, si specificano i parametri da monitorare.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

CRC/Fragments on

Attiva/disattiva il monitoraggio di errori CRC/frammenti rilevati sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  - La funzione *Port Monitor* monitora gli errori CRC/frammenti rilevati sulla porta.
  - Se il dispositivo rileva troppi errori CRC/frammenti, il dispositivo esegue l'azione specificata nella colonna *Action*.
  - Nella scheda *CRC/Fragments*, si specificano i parametri da monitorare.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Duplex mismatch detection active

Attiva/disattiva il monitoraggio delle mancate corrispondenze duplex sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  - La funzione *Port Monitor* monitora le mancate corrispondenze sulla porta.
  - Se il dispositivo rileva una mancata corrispondenza duplex, il dispositivo esegue l'azione specificata nella colonna *Action*.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Overload detection on

Attiva/disattiva il rilevamento sovraccarico sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  - La funzione *Port Monitor* monitora il caricamento dati sulla porta.
  - Se il dispositivo rileva un sovraccarico dati sulla porta, il dispositivo esegue l'azione specificata nella colonna *Action*.
  - Nella scheda *Overload detection*, si specificano i parametri da monitorare.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Link speed/Duplex mode detection on

Attiva/disattiva il monitoraggio della velocità link e della modalità duplex sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio è attivo.
  - La funzione *Port Monitor* monitora la velocità link e la modalità duplex sulla porta.
  - Se il dispositivo rileva una combinazione non permessa di velocità link e modalità duplex, il dispositivo esegue l'azione specificata nella colonna *Action*.
  - Nella scheda *Link speed/Duplex mode detection*, si specificano i parametri da monitorare.
- `non selezionato` (impostazione di default)
  Il monitoraggio non è attivo.

Active condition

Visualizza il parametro monitorato che comporta l'azione sulla porta.

Possibili valori:

- `-`
  Nessuno parametro monitorato.
  Il dispositivo non effettua alcuna azione.
- *`Link flap`*
  Troppe modifiche del link durante il periodo osservato.
- *`CRC/Fragments`*
  Troppi errori CRC/frammenti durante il periodo osservato.
- *`Duplex mismatch`*
  Rilevata mancata corrispondenza duplex.
- *`Overload detection`*
  Sovraccarico rilevato durante il periodo osservato.
- *`Link speed/Duplex mode detection`*
  Combinazione inammissibile di velocità e modalità duplex rilevata.

Action

Specifica l'azione che il dispositivo esegue se la funzione *Port Monitor* rileva il superamento dei parametri.

Possibili valori:

- `disable port`
  Il dispositivo disabilita la porta e invia una trap SNMP.
  Il LED “Stato del link” per la porta lampeggia 3 volte per periodo.
  - Per riabilitare la porta, evidenziare la porta e fare clic sul pulsante ☰ e poi sulla voce *Reset*.
  - Se non si superano più i parametri, la funzione *Auto-Disable* abilita nuovamente la porta rilevante dopo un periodo di attesa specificato. Il prerequisito è quello di avere selezionata la casella di spunta per il parametro monitorato nella scheda *Auto-disable*.
- `send trap`
  Il dispositivo invia una trap SNMP.
  Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.
- `auto-disable` (impostazione di default)
  Il dispositivo disabilita la porta e invia una trap SNMP.
  Il LED “Stato del link” per la porta lampeggia 3 volte per periodo.
  Il prerequisito è quello di avere selezionata la casella di spunta per il parametro monitorato nella scheda *Auto-disable*.
  - La finestra di dialogo *Diagnostics > Ports > Auto-Disable* visualizza quali porte sono attualmente disabilitate a causa del superamento dei parametri.
  - La funzione *Auto-Disable* riattiva automaticamente la porta. Per fare ciò, nella finestra di dialogo *Diagnostics > Ports > Auto-Disable*, si specifica un periodo di attesa per la porta interessata nella colonna *Reset timer [s]*.

Port status

Visualizza il modo operativo della porta.

Possibili valori:

- `up`
  La porta è abilitata.
- `down`
  La porta è disabilitata.
- `notPresent`
  Porta fisica non disponibile.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Abilita nuovamente la porta evidenziata nella tabella e resetta il relativo contatore su `0`. Ciò influenza i contatori nelle seguenti finestre di dialogo:

- Finestra di dialogo *Diagnostics > Ports > Port Monitor*
  - Scheda *Link flap*
  - Scheda *CRC/Fragments*
  - Scheda *Overload detection*
- Finestra di dialogo *Diagnostics > Ports > Auto-Disable*

[Auto-disable]

In questa scheda, si attiva la funzione *Auto-Disable* per i parametri monitorati tramite la funzione *Port Monitor*.

Tabella

Reason

Visualizza i parametri monitorati tramite la funzione *Port Monitor*.

Segna la casella di spunta adiacente in modo che la funzione *Port Monitor* esegue l'azione `auto-disable` se rileva il superamento dei parametri monitorati.

Auto-disable

Attiva/disattiva la funzione *Auto-Disable* per i parametri adiacenti.

Possibili valori:

- `selezionato`
  La funzione *Auto-Disable* per i parametri adiacenti è attiva.
  In caso di superamento dei parametri adiacenti e se il valore `auto-disable` è specificato nella colonna *Action*, il dispositivo esegue la funzione *Auto-Disable*.
- `non selezionato` (impostazione di default)
  La funzione *Auto-Disable* sulla porta non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Abilita nuovamente la porta evidenziata nella tabella e resetta il relativo contatore su `0`. Ciò influenza i contatori nelle seguenti finestre di dialogo:

- Finestra di dialogo *Diagnostics > Ports > Port Monitor*
  - Scheda *Link flap*
  - Scheda *CRC/Fragments*
  - Scheda *Overload detection*
- Finestra di dialogo *Diagnostics > Ports > Auto-Disable*

[Link flap]

In questa scheda, si specificano individualmente per ogni porta le seguenti impostazioni:

- Il numero di modifiche del link.
- Il periodo durante il quale la funzione *Port Monitor* monitora un parametro per rilevare le discrepanze.

Si visualizzano inoltre quante modifiche del link la funzione *Port Monitor* ha rilevato finora.

La funzione *Port Monitor* monitora quelle porte per le quali la casella di spunta nella colonna *Link flap on* è contrassegnata nella scheda *Global*.

Tabella

Port

Visualizza il numero di porta.

Sampling interval [s]

Specifica in secondi il periodo durante il quale la funzione *Port Monitor* monitora un parametro per rilevare le discrepanze.

Possibili valori:

- `1..180` (impostazione di default: `10`)

Link flaps

Specifica il numero di modifiche del link.

Se la funzione *Port Monitor* rileva questo numero di modifiche del link nel periodo monitorato, il dispositivo effettua l'azione specificata.

Possibili valori:

- `1..100` (impostazione di default: `5`)

Last sampling interval

Visualizza il numero di errori che il dispositivo ha rilevato durante il periodo trascorso.

Total

Visualizza il numero totale di errori che il dispositivo ha rilevato da quando la porta è stata abilitata.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Abilita nuovamente la porta evidenziata nella tabella e resetta il relativo contatore su `0`. Ciò influenza i contatori nelle seguenti finestre di dialogo:

- Finestra di dialogo *Diagnostics > Ports > Port Monitor*
  - Scheda *Link flap*
  - Scheda *CRC/Fragments*
  - Scheda *Overload detection*
- Finestra di dialogo *Diagnostics > Ports > Auto-Disable*

[CRC/Fragments]

In questa scheda, si specificano individualmente per ogni porta le seguenti impostazioni:
- La percentuale di errori frammenti rilevati.
- Il periodo durante il quale la funzione *Port Monitor* monitora un parametro per rilevare le discrepanze.

Inoltre, si visualizza la percentuale di errori frammenti che il dispositivo ha rilevato finora.

La funzione *Port Monitor* monitora quelle porte per le quali la casella di spunta nella colonna *CRC/Fragments on* è contrassegnata nella scheda *Global*.

Tabella

Port

Visualizza il numero di porta.

Sampling interval [s]

Specifica in secondi il periodo durante il quale la funzione *Port Monitor* monitora un parametro per rilevare le discrepanze.

Possibili valori:
- `5..180` (impostazione di default: `10`)

CRC/Fragments count [ppm]

Specifica la percentuale di errori frammenti rilevati (in parti per milioni).

Se la funzione *Port Monitor* rileva questa percentuale di errori frammenti nel periodo monitorato, il dispositivo esegue l'azione specificata.

Possibili valori:
- `1..1000000` (impostazione di default: `1000`)

Last active interval [ppm]

Visualizza la percentuale di errori frammenti che il dispositivo ha rilevato durante il periodo trascorso.

Total [ppm]

Visualizza la percentuale di errori frammenti che il dispositivo ha rilevato da quando la porta è stata abilitata.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Abilita nuovamente la porta evidenziata nella tabella e resetta il relativo contatore su `0`. Ciò influenza i contatori nelle seguenti finestre di dialogo:

- Finestra di dialogo *Diagnostics > Ports > Port Monitor*
  - Scheda *Link flap*
  - Scheda *CRC/Fragments*
  - Scheda *Overload detection*
- Finestra di dialogo *Diagnostics > Ports > Auto-Disable*

[Overload detection]

In questa scheda, si specificano individualmente per ogni porta le seguenti impostazioni:

- I valori di soglia di caricamento.
- Il periodo durante il quale la funzione *Port Monitor* monitora un parametro per rilevare le discrepanze.

Inoltre, si visualizza il numero di pacchetti di dati che il dispositivo ha rilevato finora.

La funzione *Port Monitor* monitora quelle porte per le quali la casella di spunta nella colonna *Overload detection on* è contrassegnata nella scheda *Global*.

La funzione *Port Monitor* non monitora porte che fanno parte di un gruppo di aggregazione link.

Tabella

Port

Visualizza il numero di porta.

Traffic type

Specifica il tipo di pacchetti di dati che il dispositivo considera durante il monitoraggio del carico sulla porta.

Possibili valori:

- `all`
  La funzione *Port Monitor* monitora pacchetti broadcast, multicast e unicast.
- `bc` (impostazione di default)
  La funzione *Port Monitor* monitora solo pacchetti broadcast.
- `bc-mc`
  La funzione *Port Monitor* monitora solo pacchetti broadcast e multicast.

Threshold type

Specifica l'unità della velocità dati.

Possibili valori:

- `pps` (impostazione di default)
  pacchetti al secondo
- `kbps`
  kbit al secondo
  Il prerequisito è quello che il valore nella colonna *Traffic type* = `all`.

Lower threshold

Specifica il valore di soglia inferiore per la velocità dati.

La funzione *Auto-Disable* abilita nuovamente la porta solo quando il carico sulla porta è inferiore al valore qui specificato.

Possibili valori:

- `0..10000000` (impostazione di default: `0`)

Upper threshold

Specifica il valore di soglia superiore per la velocità dati.

Se la funzione *Port Monitor* rileva questo carico nel periodo monitorato, il dispositivo esegue l'azione specificata.

Possibili valori:

- `0..10000000` (impostazione di default: `0)`)

Interval [s]

Specifica in secondi il periodo durante il quale la funzione *Port Monitor* osserva un parametro per rilevare il superamento di un parametro.

Possibili valori:

- `1..20` (impostazione di default: `1`)

Packets

Visualizza il numero di pacchetti broadcast, multicast e unicast che il dispositivo ha rilevato durante il periodo trascorso.

Broadcast packets

Visualizza il numero di pacchetti broadcast che il dispositivo ha rilevato durante il periodo trascorso.

Multicast packets

Visualizza il numero di pacchetti multicast che il dispositivo ha rilevato durante il periodo trascorso.

Kbit/s

Visualizza la velocità dati in Kbit che il dispositivo ha rilevato durante il periodo trascorso.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Abilita nuovamente la porta evidenziata nella tabella e resetta il relativo contatore su `0`. Ciò influenza i contatori nelle seguenti finestre di dialogo:

- Finestra di dialogo *Diagnostics > Ports > Port Monitor*
  - Scheda *Link flap*
  - Scheda *CRC/Fragments*
  - Scheda *Overload detection*
- Finestra di dialogo *Diagnostics > Ports > Auto-Disable*

[Link speed/Duplex mode detection]

In questa scheda, si attivano le combinazioni consentite di velocità e modalità duplex per ogni porta.

La funzione *Port Monitor* monitora quelle porte per le quali la casella di spunta nella colonna *Link speed/Duplex mode detection on* è contrassegnata nella scheda *Global*.

La funzione *Port Monitor* monitora solo le porte fisiche abilitate.

Tabella

Port

Visualizza il numero di porta.

10 Mbit/s HDX

Attiva/disattiva il monitoraggio porte per accettare una combinazione half-duplex e velocità dati di 10 Mbit/s sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio porte tiene in considerazione la combinazione di velocità e duplex.
- `non selezionato`
  Se il monitoraggio porte rileva la combinazione velocità e duplex sulla porta, il dispositivo esegue l'azione specificata nella scheda *Global*.

10 Mbit/s FDX

Attiva/disattiva il monitoraggio porte per accettare una combinazione full-duplex e velocità dati di 10 Mbit/s sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio porte tiene in considerazione la combinazione di velocità e duplex.
- `non selezionato`
  Se il monitoraggio porte rileva la combinazione velocità e duplex sulla porta, il dispositivo esegue l'azione specificata nella scheda *Global*.

100 Mbit/s HDX

Attiva/disattiva il monitoraggio porte per accettare una combinazione half-duplex e velocità dati pari a 100 Mbit/s sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio porte tiene in considerazione la combinazione di velocità e duplex.
- `non selezionato`
  Se il monitoraggio porte rileva la combinazione velocità e duplex sulla porta, il dispositivo esegue l'azione specificata nella scheda *Global*.

100 Mbit/s FDX

Attiva/disattiva il monitoraggio porte per accettare una combinazione full-duplex e velocità dati pari a 100 Mbit/s sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio porte tiene in considerazione la combinazione di velocità e duplex.
- `non selezionato`
  Se il monitoraggio porte rileva la combinazione velocità e duplex sulla porta, il dispositivo esegue l'azione specificata nella scheda *Global*.

1,000 Mbit/s FDX

Attiva/disattiva il monitoraggio porte per accettare una combinazione full-duplex e velocità dati di 1 Gbit/s sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio porte tiene in considerazione la combinazione di velocità e duplex.
- `non selezionato`
  Se il monitoraggio porte rileva la combinazione velocità e duplex sulla porta, il dispositivo esegue l'azione specificata nella scheda *Global*.

2.5 Gbit/s FDX

Attiva/disattiva il monitoraggio porte per accettare una combinazione full-duplex e velocità dati pari a 2,5 Gbit/s sulla porta.

Possibili valori:

- `selezionato`
  Il monitoraggio porte tiene in considerazione la combinazione di velocità e duplex.
- `non selezionato`
  Se il monitoraggio porte rileva la combinazione velocità e duplex sulla porta, il dispositivo esegue l'azione specificata nella scheda *Global*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Abilita nuovamente la porta evidenziata nella tabella e resetta il relativo contatore su `0`. Ciò influenza i contatori nelle seguenti finestre di dialogo:

- Finestra di dialogo *Diagnostics > Ports > Port Monitor*
  - Scheda *Link flap*
  - Scheda *CRC/Fragments*
  - Scheda *Overload detection*
- Finestra di dialogo *Diagnostics > Ports > Auto-Disable*

6.5.4 Auto-Disable

[Diagnostics > Ports > Auto-Disable]

La funzione *Auto-Disable* consente la disabilitazione automatica delle porte monitorate e le abilita nuovamente in base alle esigenze.

Ad esempio, la funzione *Port Monitor* e le funzioni selezionate nel menu *Network Security* utilizzano la funzione *Auto-Disable* per disabilitare le porte in caso di superamento dei parametri.

Se non si superano più i parametri, la funzione *Auto-Disable* abilita nuovamente la porta rilevante dopo un periodo di attesa specificato.

Questa finestra di dialogo include le seguenti schede:
- [Port]
- [Status]

[Port]

Questa scheda visualizza quali porte sono attualmente disabilitate a causa del superamento di parametri. Se non si verifica più superamento dei parametri e si specifica un periodo di attesa nella colonna *Reset timer [s]*, la funzione *Auto-Disable* abilita automaticamente di nuovo la porta rilevante.

Tabella

Port

Visualizza il numero di porta.

Reset timer [s]

Specifica il periodo di attesa in secondi dopo il quale la funzione *Auto-Disable* abilita nuovamente la porta.

Possibili valori:
- `0` (impostazione di default)
  Il timer non è attivo. La porta rimane disabilitata.
- `30..4294967295`
  Se non si superano più i parametri, la funzione *Auto-Disable* abilita nuovamente la porta dopo un periodo di attesa qui specificato.

Error time

Visualizza quando il dispositivo disabilita la porta a causa del superamento dei parametri.

Remaining time [s]

Visualizza il tempo rimanente in secondi fino a quando la funzione *Auto-Disable* abilita di nuovo la porta.

Component

Visualizza il componente software nel dispositivo che ha disabilitato la porta.

Possibili valori:

- `PORT_MON`
  Port Monitor
  Vedere la finestra di dialogo *Diagnostics > Ports > Port Monitor*.
- `PORT_ML`
  Port Security
  Vedere la finestra di dialogo *Network Security > Port Security*.
- `DHCP_SNP`
  DHCP Snooping
  Vedere la finestra di dialogo *Network Security > DHCP Snooping*.
- `DOT1S`
  BPDU guard
  Vedere la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- `DAI`
  Dynamic ARP Inspection
  Vedere la finestra di dialogo *Network Security > Dynamic ARP Inspection*.

Reason

Visualizza il parametro monitorato che comporta la disabilitazione sulla porta.

Possibili valori:

- `none`
  Nessuno parametro monitorato.
  La porta è abilitata.
- `link-flap`
  Troppe modifiche del link. Vedere la finestra di dialogo *Diagnostics > Ports > Port Monitor*, scheda *Link flap*.
- `crc-error`
  Troppi errori CRC/frammenti rilevati. Vedere la finestra di dialogo *Diagnostics > Ports > Port Monitor*, scheda *CRC/Fragments*.
- `duplex-mismatch`
  Rilevata mancata corrispondenza duplex. Vedere la finestra di dialogo *Diagnostics > Ports > Port Monitor*, scheda *Global*.
- `dhcp-snooping`
  Troppi pacchetti DHCP da fonti non trusted. Vedere la finestra di dialogo *Network Security* > DHCP Snooping > *Configuration*, scheda *Port*.
- `arp-rate`
  Troppi pacchetti ARP da fonti non trusted. Vedere la finestra di dialogo *Network Security* > Dynamic ARP Inspection > *Configuration*, scheda *Port*.
- `bpdu-rate`
  STP-BPDUs ricevute. Vedere la finestra di dialogo *Switching > L2-Redundancy > Spanning Tree* > Global.
- `mac-based-port-security`
  Troppi pacchetti di dati da mittenti indesiderati. Vedere la finestra di dialogo *Network Security* > Port Security.
- `overload-detection`
  Sovraccarico. Vedere la finestra di dialogo *Diagnostics > Ports > Port Monitor*, scheda *Overload detection*.

- `speed-duplex`
  Combinazione inammissibile di velocità e modalità duplex rilevata. Vedere la finestra di dialogo *Diagnostics > Ports > Port Monitor*, scheda *Link speed/Duplex mode detection*.
- `Loop protection`
  Rilevato un loop di rete di Layer 2 sulla porta. Vedere la finestra di dialogo *Diagnostics > Loop Protection*, colonna *Loop detected*.

Active

Visualizza se la porta è attualmente disabilitata a causa del superamento dei parametri.

Possibili valori:

- `selezionato`
  La porta è attualmente disabilitata.
- `non selezionato`
  La porta è abilitata.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[Status]

Questa scheda visualizza i parametri monitorati per i quali la funzione *Auto-Disable* è attivata.

Tabella

Reason

Visualizza i parametri che il dispositivo monitora.

Contrassegnare la casella di spunta adiacente in modo che la funzione *Auto-Disable* disabilita e, quando applicabile, abilita nuovamente la porta in caso di superamento dei parametri monitorati.

Category

Visualizza la funzione a cui il parametro adiacente appartiene.

Possibili valori:

- `port-monitor`
  Il parametro appartiene alle funzioni nel menu *Diagnostics > Port > Port Monitor*.
- `network-security`
  Il parametro appartiene alle funzioni nel menu *Network Security*.
- `l2-redundancy`
  Il parametro appartiene alle funzioni nel menu *Switching > L2-Redundancy*.

Auto-disable

Visualizza se la funzione *Auto-Disable* è attivata/disattivata per il parametro adiacente.

Possibili valori:

- `selezionato`
  La funzione *Auto-Disable* per i parametri adiacenti è attiva.
  La funzione *Auto-Disable* disabilita e, quando applicabile, abilita nuovamente la porta in caso di superamento dei parametri monitorati.
- `non selezionato` (impostazione di default)
  La funzione *Auto-Disable* sulla porta non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Abilita nuovamente la porta evidenziata nella tabella e resetta il relativo contatore su `0`. Ciò influenza i contatori nelle seguenti finestre di dialogo:

- Finestra di dialogo *Diagnostics > Ports > Port Monitor*
  - Scheda *Link flap*
  - Scheda *CRC/Fragments*
  - Scheda *Overload detection*
- Finestra di dialogo *Diagnostics > Ports > Auto-Disable*

6.5.5 Port Mirroring

[Diagnostics > Ports > Port Mirroring]

La funzione *Port Mirroring* consente di copiare i pacchetti di dati ricevuti e inviati da porte selezionate ad una porta di destinazione. È possibile visualizzare ed elaborare il flusso di dati utilizzando un analizzatore o una sonda RMON, connesso/a alla porta di destinazione. I pacchetti di dati rimangono non modificati sulla porta di origine.

Nota: Per consentire l'accesso alla gestione del dispositivo utilizzando la porta di destinazione, contrassegnare la casella di spunta *Allow management* nel frame *Destination port* prima di abilitare la funzione *Port Mirroring*.

Operation

Operation

Abilita/disabilita la funzione *Port Mirroring*.

Possibili valori:

- `On`
  È abilitata la funzione *Port Mirroring*.
  Il dispositivo copia i pacchetti di dati dalle porte di origine selezionate alla porta di destinazione.
- `Off` (impostazione di default)
  È disabilitata la funzione *Port Mirroring*.

Destination port

Primary port

Specifica la porta di destinazione.

Le porte adatte sono quelle porte che non sono utilizzate per i seguenti scopi:

- Porta di origine
- Protocolli di ridondanza L2

Possibili valori:

- `no Port` (impostazione di default)
  Nessuna porta di destinazione selezionata.
- `<Numero di porta>`
  Numero della porta di destinazione. Il dispositivo copia i pacchetti di dati dalle porte di origine a questa porta.

Sulla porta di destinazione, il dispositivo aggiunge un tag VLAN ai pacchetti di dati che la porta di origine trasmette. La porta di destinazione trasmette i pacchetti di dati non modificati che la porta di origine riceve.

Nota: La porta di destinazione necessita di una larghezza di banda sufficiente per assorbire il flusso di dati. Se il flusso di dati copiato è superiore alla larghezza di banda della porta di destinazione, il dispositivo elimina i pacchetti di dati sulla porta di destinazione.

Secondary port

Specifica una seconda porta di destinazione. Il prerequisito è che sia configurata una porta primaria.

Possibili valori:

- `no Port` (impostazione di default)
  Nessuna porta di destinazione selezionata.
- `<Numero di porta>`
  Numero della porta di destinazione. Il dispositivo copia i pacchetti di dati dalle porte di origine a questa porta.

Allow management

Attiva/disattiva l'accesso alla gestione del dispositivo utilizzando la porta di destinazione.

Possibili valori:

- `selezionato`
  L'accesso alla gestione del dispositivo utilizzando la porta di destinazione è attivo.
  Il dispositivo consente agli utenti l'accesso alla gestione dispositivo utilizzando la porta di destinazione senza interrompere la sessione *Port Mirroring* attiva.
  - 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 utilizzando la porta di destinazione prevede che la porta di destinazione non faccia parte della VLAN della gestione del dispositivo.
- `non selezionato` (impostazione di default)
  L'accesso alla gestione del dispositivo utilizzando la porta di destinazione non è attivo.
  Il dispositivo non consente l'accesso alla gestione del dispositivo utilizzando la porta di destinazione.

Tabella

Source port

Specifica il numero di porta.

Possibili valori:

- `<Numero di porta>`

Enabled

Attiva/disattiva la copia dei pacchetti di dati da questa porta di origine alla porta di destinazione.

Possibili valori:

- `selezionato`
  La copia dei pacchetti di dati è attiva.
  La porta è specificata come una porta di origine.
- `non selezionato` (impostazione di default)
  La copia dei pacchetti di dati non è attiva.
- (Visualizzazione in grigio)
  Non è possibile copiare i pacchetti di dati per questa porta.
  Possibili cause:
  - La porta è già specificata come una porta di destinazione.
  - La porta è una porta logica, non una porta fisica.

Nota: Il dispositivo consente l'attivazione di ogni porta fisica come porta di origine ad eccezione della porta di destinazione.

Type

Specifica quali pacchetti di dati il dispositivo copia sulla porta di destinazione.

Sulla porta di destinazione, il dispositivo aggiunge un tag VLAN ai pacchetti di dati che la porta di origine trasmette. La porta di destinazione trasmette i pacchetti di dati non modificati che la porta di origine riceve.

Possibili valori:

- `none` (impostazione di default)
  Nessun pacchetto di dati.
- `tx`
  Pacchetti di dati che la porta di origine trasmette.
- `rx`
  Pacchetti di dati che la porta di origine riceve.
- `txrx`
  Pacchetti di dati che la porta di origine trasmette e riceve.

Nota: Con l'impostazione `txrx` il dispositivo copia i pacchetti di dati trasmessi e ricevuti. Le porte di destinazione necessitano almeno di una larghezza di banda che corrisponde alla somma dei canali di invio e ricezione delle porte di origine. Ad esempio, per porte simili, la porta di destinazione è al 100 % di capacità quando i canali di invio e ricezione di una porta di origine sono rispettivamente al 50 % di capacità.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset config

Resetta le impostazioni nella finestra di dialogo alle impostazioni di default e trasferisce le modifiche alla memoria volatile del dispositivo (*RAM*).

6.6 LLDP

[Diagnostics > LLDP]

Il dispositivo consente di raccogliere informazioni sui dispositivi adiacenti. Per questo motivo, il dispositivo utilizza il Link Layer Discovery Protocol (LLDP). Grazie a queste informazioni, una network management station è in grado di mappare la struttura della rete.

Questo menu consente la configurazione del rilevamento della topologia e la visualizzazione delle informazioni ricevute in forma tabellare.

Il menu include le seguenti finestre di dialogo:

- LLDP Configuration
- LLDP Topology Discovery

6.6.1 LLDP Configuration

[Diagnostics > LLDP > Configuration]

Questa finestra di dialogo consente la configurazione del riconoscimento della topologia per ogni porta.

Operation

Operation

Abilita/disabilita la funzione *LLDP*.

Possibili valori:

- `On` (impostazione di default)
  È abilitata la funzione *LLDP*.
  Il riconoscimento della topologia utilizzando LLDP è attiva nel dispositivo.
- `Off`
  È disabilitata la funzione *LLDP*.

Configuration

Transmit interval [s]

Specifica l'intervallo in secondi nel quale il dispositivo trasmette pacchetti di dati LLDP.

Possibili valori:

- `5..32768` (impostazione di default: `30`)

Transmit interval multiplier

Specifica il fattore per determinare il valore di durata per i pacchetti di dati LLDP.

Possibili valori:

- `2..10` (impostazione di default: `4`)

Il valore di durata codificato nell'intestazione di LLDP risulta dalla moltiplica di questo valore con il valore nel campo *Transmit interval [s]*.

Reinit delay [s]

Specifica il ritardo in secondi per la reinizializzazione di una porta.

Possibili valori:

- `1..10` (impostazione di default: `2`)

Se nella colonna *Operation* è specificato il valore `Off`, il dispositivo tenta di reinizializzare la porta dopo che è trascorso il periodo di tempo qui specificato.

Transmit delay [s]

Specifica il ritardo in secondi per trasmettere i pacchetti di dati LLDP successivi dopo l'effettuazione di modifiche nella configurazione del dispositivo.

Possibili valori:

- `1..8192` (impostazione di default: `2`)

Il valore raccomandato è compreso tra un minimo di `1` e un massimo di un quarto del valore nel campo *Transmit interval [s]*.

Notification interval [s]

Specifica l'intervallo in secondi per la trasmissione di notifiche LLDP.

Possibili valori:

- `5..3600` (impostazione di default: `5`)

Dopo la trasmissione di una trap di notifica, il dispositivo attende un minimo del tempo specificato qui prima di trasmettere la trap di notifica successiva.

Tabella

Port

Visualizza il numero di porta.

Operation

Specifica se la porta trasmette e riceve pacchetti di dati LLDP.

Possibili valori:

- *`transmit`*
  La porta trasmette pacchetti di dati LLDP ma non salva informazioni relative ai dispositivi adiacenti.
- *`receive`*
  La porta riceve pacchetti di dati LLDP ma non trasmette informazioni ai dispositivi adiacenti.
- *`receive and transmit`* (impostazione di default)
  La porta trasmette pacchetti di dati LLDP e salva informazioni relative ai dispositivi adiacenti.
- *`disabled`*
  La porta non trasmette pacchetti di dati LLDP e non salva informazioni relative ai dispositivi adiacenti.

Notification

Attiva/disattiva le notifiche LLDP sulla porta.

Possibili valori:

- `selezionato`
  Le notifiche LLDP sono attive sulla porta.
- `non selezionato` (impostazione di default)
  Le notifiche LLDP non sono attive sulla porta.

Transmit port description

Attiva/disattiva la trasmissione di un TLV (Type Length Value) con la descrizione della porta.

Possibili valori:

- `selezionato` (impostazione di default)
  La trasmissione del TLV è attiva.
  Il dispositivo trasmette il TLV con la descrizione della porta.
- `non selezionato`
  La trasmissione del TLV non è attiva.
  Il dispositivo non trasmette un TLV con la descrizione della porta.

Transmit system name

Attiva/disattiva la trasmissione di un TLV (Type Length Value) con il nome dispositivo.

Possibili valori:

- `selezionato` (impostazione di default)
  La trasmissione del TLV è attiva.
  Il dispositivo trasmette il TLV con il nome dispositivo.
- `non selezionato`
  La trasmissione del TLV non è attiva.
  Il dispositivo non trasmette un TLV con il nome dispositivo.

Transmit system description

Attiva/disattiva la trasmissione del TLV (Type Length Value) con la descrizione del sistema.

Possibili valori:

- `selezionato` (impostazione di default)
  La trasmissione del TLV è attiva.
  Il dispositivo trasmette il TLV con la descrizione del sistema.
- `non selezionato`
  La trasmissione del TLV non è attiva.
  Il dispositivo non trasmette un TLV con la descrizione del sistema.

Transmit system capabilities

Attiva/disattiva la trasmissione del TLV (Type Length Value) con le capacità del sistema.

Possibili valori:

- `selezionato` (impostazione di default)
  La trasmissione del TLV è attiva.
  Il dispositivo trasmette il TLV con le capacità del sistema.
- `non selezionato`
  La trasmissione del TLV non è attiva.
  Il dispositivo non trasmette un TLV con le capacità del sistema.

Neighbors (max.)

Limita il numero di dispositivi adiacenti da registrare per questa porta.

Possibili valori:

- `1..50` (impostazione di default: `10`)

FDB mode

Specifica quale funzione il dispositivo utilizza per registrare i dispositivi adiacenti su questa porta.

Possibili valori:

- `lldpOnly`
  Il dispositivo utilizza solo pacchetti di dati LLDP per registrare i dispositivi adiacenti su questa porta.
- `macOnly`
  Il dispositivo utilizza indirizzi MAC appresi per registrare i dispositivi adiacenti su questa porta. Il dispositivo utilizza l'indirizzo MAC so se non vi sono altre voci nella tabella indirizzi (FDB, Forwarding Database) per questa porta.
- `both`
  Il dispositivo utilizza pacchetti di dati LLDP e indirizzi MAC appresi per registrare i dispositivi adiacenti su questa porta.
- `autoDetect` (impostazione di default)
  Se il dispositivo riceve pacchetti di dati LLDP su questa porta, il dispositivo funziona nello stesso modo come con l'impostazione `lldpOnly`. Altrimenti il dispositivo funziona nello stesso modo come con l'impostazione `macOnly`.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.6.2 LLDP Topology Discovery

[Diagnostics > LLDP > Topology Discovery]

I dispositivi nelle reti inviano notifiche sotto forma di pacchetti che sono noti anche come “LLDPDU” (unità dati LLDP). I dati inviati e ricevuti tramite LLDPDU sono utili per diversi motivi. Pertanto il dispositivo rileva quali dispositivi nella rete sono adiacenti e attraverso quali porte sono connessi.

La finestra di dialogo consente la visualizzazione della rete e il rilevamento dei dispositivi connessi insieme alle specifiche funzionalità.

Questa finestra di dialogo include le seguenti schede:
- [LLDP]
- [LLDP-MED]

[LLDP]

Questa scheda visualizza le informazioni LLDP raccolte per i dispositivi adiacenti. Grazie a queste informazioni, una network management station è in grado di mappare la struttura della rete.

Se a una porta sono collegati sia dispositivi con la funzione di riconoscimento della topologia sia dispositivi senza funzione di riconoscimento della topologia, la tabella Topologia nasconde i dispositivi senza la funzione di riconoscimento della topologia.

Se sono connessi solo dispositivi senza riconoscimento della topologia attivo, la tabella contiene per questa porta una riga riferita a tutti i dispositivi. La ria contiene il numero di dispositivi connessi.

La tabella di indirizzi del Forwarding Database (FDB) contiene indirizzi MAC dei dispositivi che la tabella topologia contiene per chiarezza.

Quando si utilizza una porta per collegare diversi dispositivi, ad esempio tramite un hub, la tabella contiene una riga per ogni dispositivo collegato.

Tabella

Port

Visualizza il numero di porta.

Neighbor identifier

Visualizza l'ID del modulo di base del dispositivo adiacente. Questo può corrispondere, ad esempio, all'indirizzo MAC di base del dispositivo adiacente.

FDB

Visualizza se il dispositivo connesso ha il supporto LLDP attivo.

Possibili valori:

- `selezionato`
  Il dispositivo connesso non ha supporto LLDP attivo.
  Il dispositivo utilizza le informazioni dalla tabella indirizzi (FDB, Forwarding Database)
- `non selezionato` (impostazione di default)
  Il dispositivo connetto ha supporto LLDP attivo.

Neighbor IP address

Visualizza l'indirizzo IP con il quale è possibile l'accesso alla gestione del dispositivo adiacente.

Neighbor port description

Visualizza una descrizione per la porta del dispositivo adiacente.

Neighbor system name

Visualizza il nome del dispositivo del dispositivo adiacente.

Neighbor system description

Visualizza una descrizione per il dispositivo adiacente.

Port ID

Visualizza l'ID della porta attraverso cui il dispositivo adiacente è connesso al dispositivo.

Autonegotiation supported

Visualizza se la porta del dispositivo adiacente supporta la negoziazione automatica.

Autonegotiation

Visualizza se la negoziazione automatica è abilitata sulla porta del dispositivo adiacente.

PoE supported

Visualizza se la porta del dispositivo adiacente supporta Power over Ethernet (PoE).

PoE enabled

Visualizza se Power over Ethernet (PoE) è abilitata sulla porta del dispositivo adiacente.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[LLDP-MED]

LLDP per Media Endpoint Devices (LLDP-MED) è un'estensione di LLDP che funziona tra i dispositivi endpoint e dispositivi di rete. Fornisce specificamente il supporto per applicazioni VoIP. In questa regola di supporto, fornisce un set di annunci comuni, Type Length Value (TLV), messaggi. Il dispositivo utilizzai i TLV per il riconoscimento delle capacità, quali criteri di rete, Power over Ethernet, gestione magazzino e informazioni di posizione.

Tabella

Port

Visualizza il numero di porta.

Device class

Visualizza la classe del dispositivo del dispositivo connesso in remoto.

- Un valore `notDefined` indica che il dispositivo ha capacità non coperte da nessuna delle classi*LLDP-MED*.
- Un valore di `endpointClass1..3` indica che il dispositivo ha capacità di “classe endpoint 1 .. 3”.
- Un valore `networkConnectivity` indica che il dispositivo ha capacità di dispositivo di connettività di rete.

VLAN ID

Visualizza l'estensione dell'identificativo VLAN per il sistema remoto connesso a questa porta, come definito in IEEE 802.3.

- Il dispositivo utilizza un valore da `1` a `4042` per specificare un VLAN ID valido per la porta.
- Il dispositivo visualizza il valore `0` per pacchetti contrassegnati con priorità. Questo significa che solo la priorità 802.1D è significativa e il dispositivo utilizza L'ID VLAN della porta d'ingresso.

Priority

Visualizza il valore della priorità 802.1D associato al sistema remoto connesso con la porta.

DSCP

Visualizza il valore del Differentiated Service Code Point (DSCP) associato al sistema remoto connesso con la porta.

Unknown bit status

Visualizza lo stato bit sconosciuto del traffico in ingresso.

- Un valore `true` indica che il criterio di rete per il tipo di applicazione specifica è attualmente sconosciuto. In questo caso, l'ID VLAN ignora la priorità Layer 2 e il valore del campo *DSCP*.
- Un valore `false` indica un criterio di rete specificato.

Tagged bit status

Visualizza lo stato bit contrassegnato.

- Un valore `true` indica che l'applicazione utilizza una VLAN contrassegnata.
- Un valore `false` indica che per la specifica applicazione il dispositivo utilizza una trasmissione VLAN non contrassegnata. In questo caso, il dispositivo ignora entrambi i campi ID VLAN e priorità Layer 2. Tuttavia, il valore DSCP è rilevante.

Hardware revision

Visualizza la stringa di revisione hardware specifica del rivenditore come annunciato dall'endpoint remoto.

Firmware revision

Visualizza la stringa di revisione firmware specifica del rivenditore come annunciato dall'endpoint remoto.

Software revision

Visualizza la stringa di revisione software specifica del rivenditore come annunciato dall'endpoint remoto.

Serial number

Visualizza il numero di serie specifico del rivenditore come annunciato dall'endpoint remoto.

Manufacturer name

Visualizza il nome del produttore specifico del rivenditore come annunciato dall'endpoint remoto.

Model name

Visualizza il nome del modello specifico del rivenditore come annunciato dall'endpoint remoto.

Asset ID

Visualizza l'identificatore asset-tracking specifico del rivenditore come annunciato dall'endpoint remoto.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

6.7 Loop Protection

[Diagnostics > Loop Protection]

La funzione *Loop Protection* aiuta 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.

Per 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.

Nelle reti di tipo ridondante si attivano generalmente protocolli di ridondanza. Tipicamente si disabilita la funzione *Spanning Tree* sulle porte coinvolte in altri protocolli di ridondanza. I protocolli di ridondanza contribuiscono già a evitare i loop.

Operation

Operation

Abilita/disabilita la funzione *Loop Protection*.

Possibili valori:

▶ `On`
È abilitata la funzione *Loop Protection*.
– Sulle porte attive e passive il dispositivo valuta i pacchetti di *rilevazione loop* ricevuti.
Sulle porte attive il dispositivo invia i pacchetti di *rilevazione loop* a intervalli regolari in base a quanto specificato nel campo *Transmit interval*.
Il prerequisito è che la funzione *Loop Protection* sia attiva sulla porta.
– Il dispositivo consente di monitorare i loop Ethernet con il contatto di segnalazione. Per il parametro vedere la finestra di dialogo *Diagnostics > Status Configuration > Signal Contact >* Signal Contact 1, casella di spunta *Ethernet loops*.

▶ `Off` (impostazione di default)
È disabilitata la funzione *Loop Protection*.
Il dispositivo non invia pacchetti di *rilevazione loop* né valuta i pacchetti di *rilevazione loop* ricevuti.

Global

Transmit interval

Specifica l'intervallo in secondi nel quale il dispositivo invia i pacchetti di *rilevazione loop* se la funzione *Loop Protection* è attiva sulla porta.

Possibili valori:

- `1..10`

Receive threshold

Specifica il valore soglia per il numero di pacchetti di *rilevazione loop* ricevuti consecutivamente. Se il numero raggiunge o supera questa soglia, il dispositivo esegue l'azione specificata nella colonna *Action*.

Possibili valori:

- `1..50`

Configuration

Auto-disable

Attiva/disattiva la funzione *Auto-Disable* per *Loop Protection*.

Possibili valori:

- `selezionato`
  La funzione *Auto-Disable* per *Loop Protection* è attiva.
  Il prerequisito per disabilitare la porta è che l'azione *auto-disable* o *all* sia specificata nella colonna *Action*.
  Il dispositivo consente di specificare l'intervallo di attesa in secondi dopo il quale la funzione *Auto-Disable* abilita nuovamente la porta. A tale scopo, nella finestra di dialogo *Diagnostics* > Ports > *Auto-Disable* specificare il periodo di attesa nella colonna *Reset timer [s]*.
- `non selezionato` (impostazione di default)
  La funzione *Auto-Disable* per *Loop Protection* non è attiva.

Tabella

Port

Visualizza il numero di porta.

Active

Attiva/disattiva la funzione *Loop Protection* sulla porta.

Possibili valori:

- `selezionato`
  La funzione *Loop Protection* è attiva sulla porta.
  Attivare la funzione solo sulle porte che non fanno parte di un percorso di rete ridondante. Questa azione contribuisce a evitare l'arresto dei percorsi di rete ridondanti.
  Se il dispositivo riceve un pacchetto di *rilevazione loop* su questa porta, inviato da un'altra porta sullo stesso dispositivo, il dispositivo esegue l'azione specificata nella colonna *Action*.
- `non selezionato` (impostazione di default)
  La funzione *Loop Protection* non è attiva sulla porta. La porta non invia pacchetti di *rilevazione loop* né valuta i pacchetti di *rilevazione loop* ricevuti.

Mode

Specifica il comportamento della funzione *Loop Protection* sulla porta.

Possibili valori:

- *active*
  Il dispositivo invia pacchetti di *rilevazione loop* e valuta i pacchetti di *rilevazione loop* ricevuti.
- *passive*
  Il dispositivo valuta i pacchetti di *rilevazione loop* ricevuti.

Action

Specifica l'azione che il dispositivo esegue quando rileva un loop di rete di Layer 2 su questa porta.

Possibili valori:

- *trap*
  Il dispositivo invia una trap.
- *auto-disable*
  Il dispositivo disabilita la porta utilizzando la funzione *Auto-Disable*.
  Il prerequisito per disabilitare la porta è che la casella di spunta *Auto-disable* nel frame *Configuration* sia selezionata.
- *all*
  Il dispositivo invia una trap. In seguito, il dispositivo disabilita la porta utilizzando la funzione *Auto-Disable*.
  Il prerequisito per disabilitare la porta è che la casella di spunta *Auto-disable* nel frame *Configuration* sia selezionata.

VLAN ID

Specifica la VLAN in cui il dispositivo invia i pacchetti di *rilevazione loop*.

Possibili valori:

- `0` (impostazione di default)
  Il dispositivo invia i pacchetti di *rilevazione loop* senza un tag VLAN.
- `1..4042`
  Il dispositivo invia i pacchetti di *rilevazione loop* nella VLAN specificata. Il prerequisito è che la VLAN sia già configurata e che la porta faccia parte della VLAN. Vedere la finestra di dialogo *Switching > VLAN > Port*.

Loop detected

Visualizza se il dispositivo ha rilevato un loop di rete di Layer 2 sulla porta.

Possibili valori:

- *yes*
  Il dispositivo ha rilevato un loop di rete di Layer 2 sulla porta.
  Dopo la conclusione del loop e la riabilitazione della porta, il dispositivo ripristina il valore su *no*.
- *no*
  Il dispositivo non ha rilevato un loop di rete di Layer 2 sulla porta.

Loop count

Visualizza il numero di loop che il dispositivo ha rilevato sulla porta dall'ultimo ripristino delle statistiche della porta o dall'ultimo riavvio del dispositivo.

Last loop time

Visualizza l'orario in cui il dispositivo ha rilevato l'ultimo loop sulla porta.

Il prerequisito per la corretta valutazione del valore è che l'orario di sistema del dispositivo sia sincronizzato con il corretto orario di riferimento. Vedere la finestra di dialogo *Time > Basic Settings*.

Sent frames

Visualizza il numero di pacchetti di *rilevazione loop* inviati sulla porta dall'ultimo ripristino delle statistiche della porta o dall'ultimo riavvio del dispositivo.

Received frames

Visualizza il numero di pacchetti di *rilevazione loop* inviati e ricevuti sulla porta dall'ultimo ripristino delle statistiche della porta o dall'ultimo riavvio del dispositivo.

Discarded frames

Visualizza il numero di pacchetti di *rilevazione loop* rifiutati sulla porta.

Esempi di motivi per il rifiuto dei pacchetti:

- Il dispositivo rileva pacchetti con formato errato.
- Il dispositivo rileva pacchetti con marcature temporali scadute (pacchetti ricevuti più di 5 secondi dopo l'invio).
- Il dispositivo ha ricevuto un pacchetto dati con informazioni VLAN inattese.
- Il dispositivo rileva pacchetti ricevuti su una porta disabilitata.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Clear port statistics

Ripristina i valori nelle seguenti colonne:

- *Loop count*
- *Sent frames*
- *Received frames*

6.8 Report

[Diagnostics > Report]

Il menu include le seguenti finestre di dialogo:

- Report Global
- Persistent Logging
- System Log
- Audit Trail

6.8.1 Report Global

[Diagnostics > Report > Global]

Il dispositivo consente la registrazione di specifici eventi utilizzando i seguenti output:
- sulla console
- su uno o più server syslog
- su una connessione alla Command Line Interface configurata utilizzando SSH
- su una connessione alla Command Line Interface configurata utilizzando Telnet

In questa finestra di dialogo si specificano le impostazioni necessarie. Assegnando il livello di gravità, si specifica quali eventi registra il dispositivo.

La finestra di dialogo consente il salvataggio di un archivio ZIP con informazioni di sistema sul PC.

Console logging

Operation

Abilita/disabilita la funzione *Console logging*.

Possibili valori:
- `On`
  È abilitata la funzione *Console logging*.
  Il dispositivo registra gli eventi sulla console.
- `Off` (impostazione di default)
  È disabilitata la funzione *Console logging*.

Severity

Specifica la minima gravità per gli eventi. Il dispositivo registra gli eventi con questa gravità e con gravità più urgenti.

Il dispositivo emette i messaggi sull'interfaccia seriale.

Possibili valori:
- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (impostazione di default)
- `notice`
- `informational`
- `debug`

Buffered logging

Il dispositivo bufferizza gli eventi registrati in 2 area di archiviazione, in modo da conservare le voci di registro di eventi urgenti.

Questa finestra di dialogo consente di specificare la gravità minima per eventi che il dispositivo bufferizza nell'area di archiviazione con una priorità superiore.

Severity

Specifica la minima gravità per gli eventi. Il dispositivo bufferizza le voci di registro per eventi di questa gravità e di maggiore urgenza nell'area di archiviazione con una priorità superiore.

Possibili valori:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (impostazione di default)
- `notice`
- `informational`
- `debug`

SNMP logging

Quando si abilita la registrazione di richieste SNMP, il dispositivo invia queste richieste sotto forma di eventi con il livello di gravità predefinito `notice` all'elenco dei server syslog. Il livello di gravità minimo predefinito per una voce di server syslog è `critical`.

Per inviare richieste SNMP a un server syslog sono disponibili diverse opzioni per modificare le impostazioni predefinite. Selezionare le impostazioni che meglio rispondono alle proprie esigenze.

- ☐ Impostare su `warning` o `error` il livello di gravità per cui il dispositivo crea richieste SNMP sotto forma di eventi. Modificare il livello di gravità minimo per una voce di syslog per uno o più server syslog impostandolo sullo stesso valore.
  Inoltre, al riguardo è possibile creare una voce di server syslog.
- ☐ Impostare solo la gravità per le richieste SNMP su `critical` o superiore. Il dispositivo invia ai server syslog richieste SNMP sotto forma di eventi con il livello di gravità `critical` o superiore.
- ☐ Impostare solo la gravità minima per una o più voci di server syslog su `notice` o inferiore. È possibile che il dispositivo invii molti eventi ai server syslog.

Log SNMP get request

Abilita/disabilita la registrazione di SNMP Get requests.

Possibili valori:

- *On*
  La registrazione è abilitata.
  Il dispositivo registra SNMP Get requests sotto forma di eventi nel syslog.
  Nella lista a discesa *Severity get request*, si seleziona il livello di gravità di questo evento.
- *Off* (impostazione di default)
  La registrazione è disabilitata.

Log SNMP set request

Abilita/disabilita la registrazione di SNMP Set requests.

Possibili valori:

- *On*
  La registrazione è abilitata.
  Il dispositivo registra SNMP Set requests sotto forma di eventi nel syslog.
  Nella lista a discesa *Severity set request*, si seleziona il livello di gravità di questo evento.
- *Off* (impostazione di default)
  La registrazione è disabilitata.

Severity get request

Specifica la gravità dell'evento che il dispositivo registra per SNMP Get requests.

Possibili valori:

- emergency
- alert
- critical
- error
- warning
- notice (impostazione di default)
- informational
- debug

Severity set request

Specifica la gravità dell'evento che il dispositivo registra per SNMP Set requests.

Possibili valori:

- emergency
- alert
- critical
- error
- warning
- notice (impostazione di default)
- informational
- debug

CLI logging

Operation

Abilita/disabilita la funzione *CLI logging*.

Possibili valori:

- `On`
  È abilitata la funzione *CLI logging*.
  Il dispositivo registra ogni comando ricevuto utilizzando la Command Line Interface.
- `Off` (impostazione di default)
  È disabilitata la funzione *CLI logging*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Download support information

Genera un archivio ZIP che il browser Web consente di scaricare dal dispositivo.

L'archivio ZIP contiene informazioni di sistema relative al dispositivo. Si trova una spiegazione dei file contenuti nell'archivio ZIP nella seguente sezione.

Informazioni di supporto: file contenuti nell'archivio ZIP

Nome file	Formato	Commenti
`audittrail.html`	HTML	Contiene le registrazioni cronologiche degli eventi di sistema e le modifiche utenti salvate in Audit Trail.
`defaultconfig.xml`	XML	Contiene il profilo di configurazione con le impostazioni di default.
`script`	TEXT	Contiene l'uscita del comando `show running-config script`.
`runningconfig.xml`	XML	Contiene il profilo di configurazione con le attuali impostazioni di funzionamento.
`supportinfo.html`	TEXT	Contiene le informazioni di supporto interne per il dispositivo.
`systeminfo.html`	HTML	Contiene le informazioni sulle attuali impostazioni e parametri di funzionamento.
`systemlog.html`	HTML	Contiene gli eventi registrati nel file di registro. Vedere la finestra di dialogo *Diagnostics > Report > System Log*.

Significato dei livelli di gravità evento

Livello di gravità	Significato
`emergency`	Il dispositivo non è pronto per il funzionamento
`alert`	È richiesto l'intervento immediato dell'utente
`critical`	Stato critico

Livello di gravità	Significato
`error`	Stato di errore
`warning`	Avvertenza
`notice`	Stato normale, significativo
`informational`	Messaggio informale
`debug`	Messaggio di debug

6.8.2 Persistent Logging

[Diagnostics > Report > Persistent Logging]

Il dispositivo consente di salvare le voci di registro in modo permanente in un file nella memoria esterna. Pertanto, anche dopo il riavvio del dispositivo, si ha accesso alle voci di registro.

In questa finestra di dialogo si limita la dimensione del file di registro e si specifica il livello di gravità minimo per gli eventi da salvare. Quando il file di registro raggiunge la dimensione specificata, il dispositivo archivia questo file e salva le seguenti voci di registro in un file creato nuovo.

Nella tabella il dispositivo visualizza i file di registro archiviati nella memoria esterna. Non appena si raggiunge il numero massimo specificato di file, il dispositivo elimina il file più vecchio e rinomina i file rimanenti. In questo modo si garantisce sufficiente spazio nella memoria esterna.

Nota: Verificare che sia connessa una memoria esterna. Per verificare se è connessa una memoria esterna, vedere la colonna *Status* nella finestra di dialogo *Basic Settings > External Memory*. Raccomandiamo di monitorare la connessione della memoria esterna utilizzando la funzione *Device Status*, vedere il parametro *External memory removal* nella finestra di dialogo *Diagnostics > Status Configuration > Device Status*.

Operation

Operation

Abilita/disabilita la funzione *Persistent Logging*.

Attivare questa funzione solo se la memoria esterna è disponibile nel dispositivo.

Possibili valori:

- *On* (impostazione di default)
  È abilitata la funzione *Persistent Logging*.
  Il dispositivo salva le voci di registro in un file nella memoria esterna.
- *Off*
  È disabilitata la funzione *Persistent Logging*.

Configuration

Max. file size [kbyte]

Specifica la dimensione massima del file di registro in KByte. Quando il file di registro raggiunge la dimensione specificata, il dispositivo archivia questo file e salva le seguenti voci di registro in un file creato nuovo.

Possibili valori:

- `0..4096` (impostazione di default: `1024`)

Il valore `0` disattiva il salvataggio delle voci di registro nel file di registro.

Files (max.)

Specifica il numero di file di registro che il dispositivo mantiene nella memoria esterna.

Non appena si raggiunge il numero massimo specificato di file, il dispositivo elimina il file più vecchio e rinomina i file rimanenti.

Possibili valori:

- `0..25` (impostazione di default: `4`)

Il valore `0` disattiva il salvataggio delle voci di registro nel file di registro.

Severity

Specifica la minima gravità degli eventi. Il dispositivo salva la voce di registro per eventi di questa gravità e di maggiore urgenza nel file di registro nella memoria esterna.

Possibili valori:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (impostazione di default)
- `notice`
- `informational`
- `debug`

Log file target

Specifica il dispositivo di memoria esterno per l'accesso.

Possibili valori:

- `usb`
  Memoria USB esterna (EAM)

Tabella

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Possibili valori:

- `1..25`

Il dispositivo assegna automaticamente questo numero.

File name

Visualizza il nome del file di registro nella memoria esterna.

Possibili valori:

- `messages`
- `messages.X`

File size [byte]

Visualizza la dimensione del file di registro in byte nella memoria esterna.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Delete persistent log file

Rimuove i file di registro dalla memoria esterna.

6.8.3 System Log

[Diagnostics > Report > System Log]

Il dispositivo registra gli eventi interni al dispositivo in un file di registro (System Log).

La finestra di dialogo visualizza il file di registro (System Log). La finestra di dialogo consente di salvare il file di registro nel formato HTML sul proprio PC.

Per ricercare nel file di registro termini di ricerca, utilizzare il funzione di ricerca del proprio browser Web.

Il file di registro viene mantenuto finché si effettua un riavvio nel dispositivo. Dopo il riavvio il dispositivo crea nuovamente il file.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Save log file

Apre la pagina HTML in una nuova finestra o scheda del browser Web. È possibile salvare la pagina HTML sul PC utilizzando il comando del browser Web corretto.

Delete log file

Rimuove gli eventi registrati dal file di registro.

6.8.4 Audit Trail

[Diagnostics > Report > Audit Trail]

La finestra di dialogo visualizza il file di registro (Audit Trail). La finestra di dialogo consente di salvare il file di registro come file HTML sul proprio PC.

Per ricercare nel file di registro termini di ricerca, utilizzare il funzione di ricerca del proprio browser Web.

Il dispositivo registra eventi di sistema e azioni in scrittura degli utenti nel dispositivo. In questo modo è possibile tenere traccia di CHI modifica CHE COSA nel dispositivo e QUANDO. Il prerequisito è che al proprio account utente sia assegnato il ruolo `auditor` o `administrator`.

Il dispositivo registra le seguenti azioni degli utenti, tra le quali:
- Un accesso utente con Command Line Interface (locale o remoto)
- Una disconnessione utente manuale
- Una disconnessione automatica di un utente nella Command Line Interface dopo uno specifico periodo di inattività.
- Riavvio del dispositivo
- Blocco di un account utente dovuto a troppi tentativi di accesso non riusciti
- Blocco dell'accesso alla gestione del dispositivo dovuto a tentativi di accesso non riusciti
- Comandi eseguiti nella Command Line Interface, a eccezione dei comandi `show`
- Modifiche delle variabili di configurazione
- Modifiche dell'orario di sistema
- Operazioni di trasferimento di file, compresi gli aggiornamenti firmware
- Modifiche della configurazione tramite Ethernet Switch Configurator
- Aggiornamenti firmware e configurazione automatica del dispositivo attraverso la memoria esterna
- Apertura e chiusura di SNMP tramite un tunnel HTTPS

Il dispositivo non registra password. Le voci registrate sono protette in scrittura e rimangono memorizzate nel dispositivo dopo un riavvio.

Durante il riavvio, l'accesso al monitor del sistema è possibile utilizzando le impostazioni di default del dispositivo. Se un aggressore riesce ad accedere fisicamente al dispositivo, è in grado di resettare le impostazioni del dispositivo ai valori di default utilizzando il monitor del sistema. Successivamente, il dispositivo e il file di registro sono accessibili utilizzando la password standard.

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Adottare misure adeguate per limitare l'accesso fisico al dispositivo. Altrimenti disattivare l'accesso al monitor del sistema. Vedere la finestra di dialogo *Diagnostics > System > Selftest*, casella di spunta *SysMon1 is available*.

Il mancato rispetto di queste istruzioni può causare morte, lesioni gravi o danni all'apparecchiatura.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Save audit trail file

Apre la pagina HTML in una nuova finestra o scheda del browser Web. È possibile salvare la pagina HTML sul PC utilizzando il comando del browser Web corretto.

7 Advanced

Il menu include le seguenti finestre di dialogo:

- DHCP L2 Relay
- DHCP Server
- DNS
- Industrial Protocols
- Digital IO Module
- Command Line Interface

7.1 DHCP L2 Relay

[Advanced > DHCP L2 Relay]

Nel pannello anteriore del dispositivo è visualizzato il seguente messaggio di pericolo:

⚠ AVVERTENZA

FUNZIONAMENTO IMPREVISTO

Non cambiare le posizioni dei cavi se la DHCP Option 82 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* L2 per aggiungere informazioni del client DHCP. I *relay agent* L3 e i server DHCP richiedono le informazioni del client DHCP per assegnare un indirizzo IP e una configurazione a un client.

Quando è attivo, il relay aggiunge le informazioni di *Option 82* configurate in questa finestra di dialogo ai pacchetti prima di inoltrare richieste DHCP dai client al server. I campi *Option 82* forniscono informazioni univoche sul client e sul relay. Questo identificatore univoco consiste in un *ID circuito* per il client e in un *ID remoto* per il relay.

Oltre ai campi del tipo, della lunghezza e del multicast, l'*ID circuito* include l'ID VLAN, il numero dell'unità, il numero di slot e il numero di porta per il client connesso.

L'*ID remoto* consiste in un campo del tipo e della lunghezza oltre a un indirizzo MAC, all'indirizzo IP, all'identificatore del client oppure a una descrizione del dispositivo definita dall'utente. Un identificatore client è il nome di sistema definito dall'utente per il dispositivo.

Per il protocollo DHCPv6 il dispositivo utilizza 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:

- Messaggi *relay Forward*
  Il *relay agent* inoltra i messaggi *relay forward* contenenti informazioni uniche del client. Le informazioni del client comprendono indirizzo peer, ovvero l'indirizzo link-local IPv6 del client e l'informazione *ID di Interfaccia*. L'informazione *ID di Interfaccia* , detta anche *Option 18*, fornisce le informazioni di identificazione dell'interfaccia su cui è stata inviata la richiesta del client.
- Messaggi *Relay Reply*
  Il server DHCPv6 invia messaggi *Relay reply*. Il *relay agent* valida i messaggi in modo da includere le informazioni all'interno del messaggio *relay forward* iniziale. Se l'informazione è valida il *relay agent* inoltra il pacchetto al client.

Il menu include le seguenti finestre di dialogo:

- DHCP L2 Relay Configuration
- DHCP L2 Relay Statistics

7.1.1 DHCP L2 Relay Configuration

[Advanced > DHCP L2 Relay > Configuration]

Questa finestra di dialogo consente di attivare la funzione relay su un'interfaccia e sulla VLAN. Quando si attiva questa funzione su una porta, il dispositivo inoltra le informazioni di *Option 82* oppure scarta le informazioni sulle porte non trusted. Il dispositivo, inoltre, consente di specificare l'identificatore remoto.

L'informazione *Option 82* è specifica della funzione L2 del relay DHCPv4. Per la funzione L2 del relay DHCPv6 l'informazione *Option 18* viene utilizzata nello scambio del pacchetto tra il client e il server DHCPv6. Il dispositivo scarta i pacchetti DHCPv6 ricevuti sulle porte non contenenti le informazioni di *Option 18*.

Questa finestra di dialogo include le seguenti schede:
- [Interface]
- [VLAN ID]

Operation

Operation

Abilita/disabilita la funzione del relay DHCP L2 del dispositivo a livello globale.

Quando questa funzione è abilitata le funzioni L2 del relay DHCPv4 L2 e L2 del relay DHCPv6 possono operare nel dispositivo contemporaneamente.

Possibili valori:

- `On`
  Abilita la funzione *DHCP L2 Relay* nel dispositivo.
- `Off` (impostazione di default)
  Disabilita la funzione *DHCP L2 Relay* nel dispositivo.

[Interface]

Tabella

Port

Visualizza il numero di porta.

Active

Attiva/disattiva la funzione *DHCP L2 Relay* sulla porta.

Il prerequisito è quello di attivare la funzione a livello globale.

Possibili valori:

- `selezionato`
  La funzione *DHCP L2 Relay* è attiva.
- `non selezionato` (impostazione di default)
  La funzione *DHCP L2 Relay* non è attiva.

Trusted port

Attiva/disattiva la modalità *DHCP L2 Relay* protetta per la porta corrispondente.

Possibili valori:

- `selezionato`
  Il dispositivo accetta i pacchetti DHCPv4 con le informazioni di *Option 82*.
  Il dispositivo accetta i pacchetti DHCPv6 con le informazioni di *Option 18*.
- `non selezionato` (impostazione di default)
  Il dispositivo scarta i pacchetti DHCPv4 ricevuti sulle porte non protette contenenti le informazioni di *Option 82*.
  Il dispositivo scarta i pacchetti DHCPv6 ricevuti sulle porte non contenenti le informazioni di *Option 18*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

[VLAN ID]

Tabella

VLAN ID

VLAN a cui fa riferimento la voce della tabella.

Active

Attiva/disattiva la funzione *DHCP L2 Relay* sulla VLAN.

Il prerequisito è quello di attivare la funzione a livello globale.

Possibili valori:

- `selezionato`
  La funzione *DHCP L2 Relay* è attiva.
- `non selezionato` (impostazione di default)
  La funzione *DHCP L2 Relay* non è attiva.

Circuit ID

Attiva o disattiva l'aggiunta dell'*ID circuito* alle informazioni di *Option 82*.

Possibili valori:

- `selezionato` (impostazione di default)
  Abilita l'*ID circuito* e l'*ID remoto* da inviare insieme.
- `non selezionato`
  Il dispositivo invia solo l'*ID remoto*.

Remote ID type

Specifica i componenti dell'*ID remoto* per questa VLAN.

Possibili valori:

- `ip`
  Specifica l'indirizzo IP del dispositivo come *ID remoto*.
- `mac` (impostazione di default)
  Specifica l'indirizzo MAC del dispositivo come *ID remoto*.
- `client-id`
  Specifica il nome di sistema del dispositivo come *ID remoto*.
- `other`
  Quando si utilizza questo valore, inserire nella colonna *Remote ID* le informazioni definite dall'utente.

Remote ID

Mostra l'*ID remoto* della VLAN.

Quando si inserisce il valore `other` nella colonna *Remote ID type*, specificare l'identificatore.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

7.1.2 DHCP L2 Relay Statistics

[Advanced > DHCP L2 Relay > Statistics]

Questo dispositivo monitora il traffico sulle porte e visualizza i risultati in formato tabulare.

Questa tabella è suddivisa in varie categorie per agevolare l'analisi del traffico.

Le opzioni del relay DHCPv6 non sono riportate nella tabella delle statistiche.

Tabella

Port

Visualizza il numero di porta.

Untrusted server messages with Option 82

Mostra il numero di messaggi del server DHCP ricevuti con le informazioni di *Option 82* sull'interfaccia non trusted.

Untrusted client messages with Option 82

Mostra il numero di messaggi del client DHCP ricevuti con le informazioni di *Option 82* sull'interfaccia non trusted.

Trusted server messages without Option 82

Mostra il numero di messaggi del server DHCP ricevuti senza le informazioni di *Option 82* sull'interfaccia trusted.

Trusted client messages without Option 82

Mostra il numero di messaggi del client DHCP ricevuti senza le informazioni di *Option 82* sull'interfaccia trusted.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Reset

Resetta l'intera tabella.

7.2 DHCP Server

[Advanced > DHCP Server]

Con il server DHCP si gestisce un database di indirizzi IP disponibili e informazioni di configurazione. Se il dispositivo riceve una richiesta da un client, il server DHCP server valida la rete client DHCP e poi assegna il lease di un indirizzo IP. Quando è attivato, il server DHCP assegna anche informazioni di configurazione adatte per quel client. Le informazioni di configurazione specificano, ad esempio, quale indirizzo IP, server DNS e la route predefinita un client utilizza.

Il server DHCP assegna un indirizzo IP a un client per un intervallo definito dall'utente. Il client DHCP è responsabile per il rinnovo dell'indirizzo IP prima del termine dell'intervallo. Se il client DHCP non riesce a rinnovare l'indirizzo, l'indirizzo ritorna al pool per la riassegnazione.

Il menu include le seguenti finestre di dialogo:

- DHCP Server Global
- DHCP Server Pool
- DHCP Server Lease Table

7.2.1 DHCP Server Global

[Advanced > DHCP Server > Global]

Attiva la funzione a livello globale o di porta in base ai requisiti.

Operation

Operation

Abilita/disabilita la funzione del server DHCP del dispositivo a livello globale.

Possibili valori:

- `On`
- `Off` (impostazione di default)

Configuration

IP Probe

Attiva/disattiva la ricerca degli indirizzi IP unici. Prima di assegnare un indirizzo IP, il server usa una richiesta *ICMP Echo* per controllare se questo indirizzo IP è già in uso sulla rete.

Possibili valori:

- `selezionato` (impostazione di default)
  La funzione *IP Probe* è attiva.
- `non selezionato`
  La funzione *IP Probe* non è attiva.

Tabella

Port

Visualizza il numero di porta.

DHCP server active

Attiva/disattiva la funzione del server DHCP su questa porta.

Il prerequisito è quello di attivare la funzione a livello globale.

Possibili valori:

- `selezionato` (impostazione di default)
  La funzione del server DHCP è attiva.
- `non selezionato`
  La funzione del server DHCP non è attiva.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

7.2.2 DHCP Server Pool

[Advanced > DHCP Server > Pool]

Assegnare un indirizzo IP a un dispositivo finale oppure ad uno switch connesso a una porta o incluso in una VLAN.

Il server DHCP fornisce pool di indirizzi IP da cui assegna indirizzi IP ai client. Un pool è composto da un elenco di voci. Definire una voce come statica per un indirizzo IP specifico oppure come dinamica per un intervallo di indirizzi IP. Il dispositivo contiene un massimo di 128 pool. I pool contengono complessivamente un massimo di 1000 voci.

Con l'assegnazione statica, il server DHCP assegna un 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. Si applica questo indirizzo IP a ogni porta oppure a una porta specifica del dispositivo. Per l'assegnazione statica, immettere un indirizzo IP per l'assegnazione nel campo *IP address* e lasciare la colonna *Last IP address* vuoto. Inserire 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 dispositivo con un ID hardware noto, il server DHCP assegna l'indirizzo statico.

Con un'assegnazione dinamica, quando un client DHCP entra in contatto su una porta, il server DHCP assegna un indirizzo IP disponibile da un pool per questa porta. Con l'assegnazione dinamica, creare un pool per le porte assegnando un intervallo di indirizzi IP. Specificare il primo e l'ultimo indirizzo IP per l'intervallo di indirizzi IP. Lasciare i campi *MAC address*, *Client ID*, *Remote ID* e *Circuit ID* vuoti. È possibile creare più voci pool. In questo modo è possibile creare un intervallo di indirizzi IP che contiene dei buchi.

Questa finestra di dialogo visualizza le diverse informazioni che sono necessarie per assegnare un indirizzo IP ad una porta oppure ad una VLAN. Utilizzare il pulsante  per aggiungere una voce. Il dispositivo aggiunge una voce scrivibile e leggibile.

Tabella

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Active

Attiva/disattiva la funzione del server DHCP su questa porta.

Possibili valori:

- `selezionato`
  La funzione del server DHCP è attiva.
- `non selezionato` (impostazione di default)
  La funzione del server DHCP non è attiva.

IP address

Specifica l'indirizzo IP per l'assegnazione statica dell'indirizzo IP. Quando si utilizza l'assegnazione dinamica dell'indirizzo IP, questo valore specifica l'inizio dell'intervallo di indirizzi IP.

Possibili valori:

- Indirizzo IPv4 valido

Last IP address

Quando si utilizza l'assegnazione dinamica dell'indirizzo IP, questo valore specifica la fine dell'intervallo di indirizzi IP.

Possibili valori:

- Indirizzo IPv4 valido

Port

Visualizza il numero di porta.

VLAN ID

Visualizza la VLAN a cui fa riferimento la voce della tabella.

Un valore pari a `1` corrisponde alla VLAN di gestione del dispositivo predefinita.

Possibili valori:

- `1..4042`

MAC address

Specifica l'indirizzo MAC del dispositivo che assegna il lease dell'indirizzo IP.

Possibili valori:

- Indirizzo MAC unicast valido
  Specificare il valore separato dai due punti, per esempio `00:11:22:33:44:55`.
- `-`
  Per l'assegnazione dell'indirizzo IP, il server ignora questa variabile.

DHCP relay

Specifica l'indirizzo IP del DHCP relay attraverso la quale i client trasmettono le loro richieste al server DHCP. Quando il server DHCP riceve la richiesta del client attraverso un altro DHCP relay, ignora questa richiesta.

Possibili valori:

- Indirizzo IPv4 valido
  Indirizzo IP del DHCP relay.
- `-`
  Tra il client e il server DHCP nessun DHCP relay.

Client ID

Specifica l'identificazione del dispositivo client che assegna il lease dell'indirizzo IP.

Possibili valori:

- 1 .. 80 byte (formato `XX XX .. XX`)
- `-`
  Per l'assegnazione dell'indirizzo IP, il server ignora questa variabile.

Remote ID

Specifica l'identificazione del dispositivo remoto che assegna il lease dell'indirizzo IP.

Possibili valori:

- 1 .. 80 byte (formato `XX XX .. XX`)
- `-`
  Per l'assegnazione dell'indirizzo IP, il server ignora questa variabile.

Circuit ID

Specifica l'ID circuito del dispositivo che assegna il lease dell'indirizzo IP.

Possibili valori:

- 1 .. 80 byte (formato `XX XX .. XX`)
- `-`
  Per l'assegnazione dell'indirizzo IP, il server ignora questa variabile.

Schneider Electric device

Attiva/disattiva Schneider Electric multicast.

Se il dispositivo in questo intervallo di indirizzi IP si utilizza solo per dispositivi Schneider Electric, attivare questa funzione.

Possibili valori:

- `selezionato`
  In questo intervallo di indirizzi IP, il dispositivo si utilizza solo per Schneider Electric dispositivi. Schneider Electric multicast sono attivati.
- `non selezionato` (impostazione di default)
  In questo intervallo di indirizzi IP, il dispositivo si utilizza per i dispositivi di produttori diversi. Schneider Electric multicast sono disattivati.

Configuration URL

Specifica il protocollo da utilizzare oltre al nome e al percorso del file di configurazione.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0.. 70 caratteri
  Esempio: `tftp://192.9.200.1/cfg/config.xml`

Lasciando questo campo vuoto, il dispositivo lascia questo campo opzione vuoto nel messaggio DHCP.

Lease time [s]

Specifica l'intervallo di lease in secondi.

Possibili valori:

- `60..220752000` (impostazione di default: `86400`)
- `4294967295`
  Utilizzare questo valore per assegnazioni illimitate nel tempo e per assegnazioni tramite BOOTP.

Default gateway

Specifica l'indirizzo IP del gateway di default.

Un valore pari a `0.0.0.0` non consente di allegare il campo opzione nel messaggio DHCP.

Possibili valori:

- Indirizzo IPv4 valido

Netmask

Specifica la maschera di rete a cui appartiene il client.

Un valore pari a `0.0.0.0` non consente di allegare il campo opzione nel messaggio DHCP.

Possibili valori:

- Maschera di rete IPv4 valida

WINS server

Specifica l'indirizzo IP del Windows Internet Name Server che converte i nomi NetBIOS.

Un valore pari a `0.0.0.0` non consente di allegare il campo opzione nel messaggio DHCP.

Possibili valori:

- Indirizzo IPv4 valido

DNS server

Specifica l'indirizzo IP del server DNS.

Un valore pari a `0.0.0.0` non consente di allegare il campo opzione nel messaggio DHCP.

Possibili valori:

- Indirizzo IPv4 valido

Hostname

Specifica il nome host.

Lasciando questo campo vuoto, il dispositivo lascia questo campo opzione vuoto nel messaggio DHCP.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0 .. 64 caratteri

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

7.2.3 DHCP Server Lease Table

[Advanced > DHCP Server > Lease Table]

Questa finestra di dialogo visualizza lo stato dei lease di indirizzi IP in base alle porte.

Tabella

Port

Visualizza il numero di porta a cui attualmente si assegna il lease dell'indirizzo.

IP address

Visualizza l'indirizzo IP assegnato in lease a cui fa riferimento la voce.

Status

Visualizza la fase di lease.

In base allo standard per operazioni DHCP, vi sono 4 fasi per il lease di un indirizzo IP: Discovery, Offer, Request e Acknowledgement.

Possibili valori:

- `bootp`
  Un client DHCP sta provando a individuare un server DHCP per l'assegnazione dell'indirizzo IP.
- `offering`
  Il server DHCP sta validando l'adeguatezza dell'indirizzo IP per il client.
- `requesting`
  Un client DHCP sta acquisendo l'indirizzo IP offerto.
- `bound`
  Il server DHCP ha assegnato il lease dell'indirizzo IP ad un client.
- `renewing`
  Il client DHCP sta richiedendo un estensione per il lease.
- `rebinding`
  Il server DHCP sta assegnando l'indirizzo IP al client dopo aver completato un rinnovo.
- `declined`
  Il server DHCP ha negato la richiesta per l'indirizzo IP.
- `released`
  L'indirizzo IP è disponibile per altri client.

Remaining lifetime

Visualizza il tempo rimanente per l'indirizzo IP oggetto del lease.

Leased MAC address

Visualizza l'indirizzo MAC del dispositivo che assegna il lease dell'indirizzo IP.

Gateway

Specifica l'indirizzo IP del gateway del dispositivo che assegna il lease dell'indirizzo IP.

Client ID

Specifica l'identificatore client del dispositivo che assegna il lease dell'indirizzo IP.

Remote ID

Visualizza l'identificatore remoto del dispositivo che assegna il lease dell'indirizzo IP.

Circuit ID

Visualizza l'ID circuito del dispositivo che assegna il lease dell'indirizzo IP.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

7.3 DNS

[Advanced > DNS]

Il menu include le seguenti finestre di dialogo:
- DNS Client

7.3.1 DNS Client

[Advanced > DNS > Client]

Il DNS (Domain Name System) è un servizio della rete che traduce i nomi host in indirizzi IP. Questa risoluzione del nome consente di contattare altri dispositivi utilizzando i nomi dell'host invece degli indirizzi IP.

La funzione *Client* consente al dispositivo di inviare richieste a un server DNS per tradurre i nomi host in indirizzi IP.

Il menu include le seguenti finestre di dialogo:
- DNS Client Global
- DNS Client Current
- DNS Client Static
- DNS Client Static Hosts

7.3.1.1 DNS Client Global

[Advanced > DNS > Client > Global]

In questa finestra di dialogo si abilitano la funzione *Client* e la funzione *Cache*.

Operation

Operation

Abilita/disabilita la funzione *Client*.

Possibili valori:

- *On*
  È abilitata la funzione *Client*.
  Il dispositivo invia richieste a un server DNS per tradurre i nomi host in indirizzi IP.
- *Off* (impostazione di default)
  È disabilitata la funzione *Client*.

Cache

Cache

Abilita/disabilita la funzione *Cache*.

Possibili valori:

- *On* (impostazione di default)
  È abilitata la funzione *Cache*.
  Il dispositivo salva temporaneamente fino a 128 risposte del server DNS (nome host e indirizzo IP corrispondente) nella cache. Quando la cache contiene una voce corrispondente, il nome host di una nuova richiesta del dispositivo si risolve. Ciò rende superfluo l'invio di una nuova richiesta al server DNS.
- *Off*
  È disabilitata la funzione *Cache*.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Flush cache

Rimuove tutte le voci dalla cache DNS.

7.3.1.2 DNS Client Current

[Advanced > DNS > Client > Current]

Questa finestra di dialogo visualizza a quali server DNS il dispositivo invia le richieste per tradurre i nomi host in indirizzi IP.

Tabella

Index

Visualizza il numero di serie del server DNS.

Address

Visualizza l'indirizzo IP del server DNS. Il dispositivo inoltra le richieste per tradurre i nomi host in indirizzi IP al server DNS con questo indirizzo IP.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

7.3.1.3 DNS Client Static

[Advanced > DNS > Client > Static]

Questa finestra di dialogo consente di specificare i server DNS a cui il dispositivo inoltra le richieste per tradurre i nomi host in indirizzi IP.

Il dispositivo consente di specificare fino a 4 indirizzi IP o di trasferire gli indirizzi IP da un server DHCP.

Configuration

Configuration source

Specifica l'origine da cui il dispositivo ottiene l'indirizzo IP dei server DNS a cui invia le richieste.

Possibili valori:

- `user`
  Il dispositivo utilizza gli indirizzi IP specificati nella tabella.
- `mgmt-dhcp` (impostazione di default)
  Il dispositivo utilizza gli indirizzi IP che il server DHCP fornisce al dispositivo.

Domain name

Specifica il nome del dominio secondo RCF 1034 che il dispositivo aggiunge ai nomi host privi di suffisso di dominio.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

Request timeout [s]

Specifica l'intervallo temporale in secondi per inviare nuovamente una richiesta al server.

Possibili valori:

- `0`
  Disattiva la funzione. Il dispositivo non invia nuovamente una richiesta al server.
- `1..3600` (impostazione di default: `3`)

Request retransmits

Specifica quante volte il dispositivo ritrasmette una richiesta.

Il prerequisito è che nel campo *Request timeout [s]* sia specificato un valore `0`.

Possibili valori:

- `0..100` (impostazione di default: `2`)

Tabella

Index

Visualizza il numero di serie del server DNS.

Il dispositivo consente di specificare fino a 4 server DNS.

Address

Specifica l'indirizzo IP del server DNS.

Possibili valori:

- Indirizzo IPv4 valido (impostazione di default: `0.0.0.0`)
- Indirizzo IPv6 valido

Active

Attiva/disattiva la voce della tabella.

Il dispositivo invia le richieste al server DNS configurato nella prima voce attiva della tabella. Quanto il dispositivo non riceve una risposta da questo server invia le richieste al server DNS configurato nella successiva voce attiva della tabella.

Possibili valori:

- `selezionato`
  Il client DNS invia le richieste a questo server DNS.
  Prerequisiti:
  - ☐ Abilitare la funzione client DNS nella finestra di dialogo *Advanced > DNS > Global*.
  - ☐ Selezionare nel frame *Configuration*, elenco a discesa *Configuration source* il valore `user`.
- `non selezionato` (impostazione di default)
  Il dispositivo non invia richieste a questo server DNS.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

7.3.1.4 DNS Client Static Hosts

[Advanced > DNS > Client > Static Hosts]

Questa finestra di dialogo consente di specificare fino a 64 nomi host da collegare con un indirizzo IP ciascuno. Quando si richiede la traduzione di nomi host in indirizzi IP il dispositivo cerca una voce corrispondente in questa tabella. Il dispositivo inoltra la richiesta quando non trova una voce corrispondente.

Tabella

Index

Visualizza il numero di indice a cui fa riferimento la voce della tabella.

Possibili valori:

- `1..64`

Name

Specifica il nome host.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..255 caratteri

IP address

Specifica l'indirizzo IP a cui è raggiungibile l'host.

Possibili valori:

- Indirizzo IPv4 valido

Active

Attiva/disattiva la voce della tabella.

Possibili valori:

- `selezionato`
  Il dispositivo risolve una richiesta di nome host per questa voce.
- `non selezionato`
  Dopo la ricezione di una richiesta per questo nome host, il dispositivo invia una richiesta a uno dei server dei nomi configurati per la risoluzione.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

7.4 Industrial Protocols

[Advanced > Industrial Protocols]

Il menu include le seguenti finestre di dialogo:

- IEC61850-MMS
- Modbus TCP
- EtherNet/IP

7.4.1 IEC61850-MMS

[Advanced > Industrial Protocols > IEC61850-MMS]

Lo IEC61850-MMS è un protocollo standardizzato di comunicazione industriale dell'International Electrotechnical Commission (IEC). Per esempio, l'apparecchiatura di switching automatica utilizza questo protocollo durante la comunicazione con l'apparecchiatura della centrale elettrica.

Il protocollo orientato al pacchetto definisce un linguaggio di comunicazione uniforme basato sul protocollo di trasporto, TCP/IP. Il protocollo utilizza un server Manufacturing Messaging Specification (MMS) per la comunicazione client-server. Il protocollo include funzioni per SCADA, dispositivi elettronici intelligenti (IED) e per i sistemi di controllo della rete.

Nota: 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.

Attivare l'accesso in scrittura solo se si sono adottate misure ulteriori (per esempio Firewall, VPN, etc.) per ridurre possibili accessi non autorizzati.

Questa finestra di dialogo consente di specificare le seguenti impostazioni del server MMS:
- Attiva/disattiva il server MMS.
- Attiva/disattiva l'accesso in scrittura al server MMS.
- La porta TCP del server MMS.
- Il numero massimo di sessioni del server MMS.

Operation

Operation

Abilita/disabilita il server *IEC61850-MMS*.

Possibili valori:

- `On`
  Il server *IEC61850-MMS* è abilitato.
- `Off` (impostazione di default)
  Il server *IEC61850-MMS* è disattivato.
  Le IEC61850 MIB restano accessibili.

Configuration

Write access

Attiva/disattiva l'accesso in scrittura al server MMS.

Possibili valori:

- `selezionato`
  L'accesso in scrittura al server MMS è attivato. Queste impostazioni consentono di modificare le impostazioni del dispositivo utilizzando il protocollo IEC 61850 MMS.
- `non selezionato` (impostazione di default)
  L'accesso in scrittura al server MMS è disattivato. Il server MMS è accessibile in sola lettura.

Technical key

Specifica il nome IED.

Il nome IED è ammissibile indipendentemente dal nome del sistema.

Possibili valori:

- Stringa di caratteri ASCII alfanumerici con 0..32 caratteri
  Sono consentiti i seguenti caratteri:
  - `_`
  - `0..9`
  - `a..z`
  - `A..Z` (impostazione di default: `KEY`)

Per far sì che il server MMS utilizzi il nome IED, fare clic sul pulsante e riavviare il server MMS. La connessione ai client connessi viene successivamente interrotta.

TCP port

Specifica la porta TCP per l'accesso al server MMS.

Possibili valori:

- `1..65535` (impostazione di default: `102`)
  Eccezione: la porta `2222` è riservata per funzioni interne.

Nota: Il server si riavvia automaticamente dopo la modifica della porta. Durante il processo, il dispositivo interrompe le connessioni aperte al server.

Sessions (max.)

Specifica il numero massimo di connessioni del server MMS.

Possibili valori:

- `1..15` (impostazione di default: `5`)

Information

Status

Mostra lo stato attuale del server *IEC61850-MMS*.

Possibili valori:

- *unavailable*
- *starting*
- *running*
- *stopping*
- *halted*
- *error*

Active sessions

Mostra il numero di connessioni del server MMS attive.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Download ICD file

Copia il file ICD sul PC dell'utente.

7.4.2 Modbus TCP

[Advanced > Industrial Protocols > Modbus TCP]

Modbus TCP è un protocollo utilizzato per l'integrazione del sistema Supervisory Control and Data Acquisition (SCADA). *Modbus TCP* è un protocollo vendor-neutral utilizzato per monitorare e controllare apparecchiatura di automazione industriale come Programmable Logic Controllers (PLC), sensori e contatori.

Questa finestra di dialogo consente di specificare i parametri del protocollo. Per monitorare e controllare i parametri del dispositivo sono necessari un software di interfaccia uomo-macchina (HMI) e una tabella di mappatura della memoria. Fare riferimento alle tabelle della sezione "Configurazione" del manuale utente per conoscere gli oggetti supportati e la mappatura della memoria.

Questa finestra di dialogo consente di abilitare la funzione, attivare l'accesso in scrittura, controllare quale porta TCP è interrogata dall'interfaccia uomo-macchina (HMI) per i dati. È inoltre possibile specificare il numero di sessioni apribili simultaneamente.

Nota: L'attivazione dell'accesso in scrittura *Modbus TCP* può causare un inevitabile rischio per la sicurezza, in quanto il protocollo non autentica l'accesso dell'utente.

Per contribuire a minimizzare gli inevitabili rischi per la sicurezza, specificare l'intervallo di indirizzi IP presente nella finestra di dialogo *Device Security > Management Access*. Inserire solo gli indirizzi IP assegnati ai propri dispositivi prima di abilitare la funzione. Inoltre, l'impostazione di default per l'attivazione della funzione di monitoraggio nella finestra di dialogo *Diagnostics > Status Configuration > Security Status*, scheda *Global*, è attiva.

Operation

Operation

Abilita/disabilita il server *Modbus TCP* nel dispositivo.

Possibili valori:

- *On*
  Il server *Modbus TCP* è abilitato.
- *Off* (impostazione di default)
  Il server *Modbus TCP* è disattivato.

Configuration

Write access

Attiva/disattiva l'accesso in scrittura ai parametri *Modbus TCP*.

Nota: L'attivazione dell'accesso in scrittura *Modbus TCP* può causare un inevitabile rischio per la sicurezza, in quanto il protocollo non autentica l'accesso dell'utente.

Possibili valori:

- `selezionato` (impostazione di default)
  L'accesso in scrittura/lettura del server *Modbus TCP* è attivo. Questo consente di modificare la configurazione del dispositivo utilizzando il protocollo *Modbus TCP*.
- `non selezionato`
  L'accesso in sola lettura al server *Modbus TCP* è attivo.

TCP port

Specifica il numero di porta TCP utilizzato dal server *Modbus TCP* per la comunicazione.

Possibili valori:

- `<TCP Port number>` (impostazione di default: `502`)
  La specifica `0` non è consentita.

Sessions (max.)

Specifica il numero massimo di sessioni simultanee mantenute dal server *Modbus TCP*.

Possibili valori:

- `1..5` (impostazione di default: `5`)

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

7.4.3 EtherNet/IP

[Advanced > Industrial Protocols > EtherNet/IP]

Questa finestra di dialogo consente di specificare le impostazioni *EtherNet/IP*: Sono disponibili le seguenti opzioni:
- Abilita/disabilita la funzione *EtherNet/IP* nel dispositivo.
- Specifica la VLAN che inoltra esclusivamente i pacchetti *EtherNet/IP*.
- Attiva/disattiva la capacità di lettura/scrittura del protocollo *EtherNet/IP*.
- Scarica il file Electronic Data Sheet (EDS) dal dispositivo.

Operation

Operation

Abilita/disabilita la funzione *EtherNet/IP* nel dispositivo.

Possibili valori:

- `On`
  È abilitata la funzione *EtherNet/IP*.
- `Off` (impostazione di default)
  È disabilitata la funzione *EtherNet/IP*.

VLAN Configuration

Vantaggi di impostare una VLAN:
- Flooding ridotto di pacchetti *EtherNet/IP*. Il dispositivo inoltra i pacchetti *EtherNet/IP* nella VLAN assegnata.
- Migliore sicurezza di rete e privacy.

VLAN ID

Specifica una VLAN in cui il dispositivo inoltra i pacchetti *EtherNet/IP*.

Possibili valori:

- `mgmt` (impostazione di default)
  Il dispositivo inoltra i pacchetti *EtherNet/IP* nella VLAN in cui è disponibile l'accesso alla gestione del dispositivo attraverso la rete. Questa VLAN si specifica nella finestra di dialogo *Basic Settings > Network > Global*, frame *Management interface*, campo *VLAN ID*.
- `1..4042`
  Selezionare una voce nell'elenco a discesa. Il dispositivo inoltra i pacchetti *EtherNet/IP* in questa VLAN.
  Prerequisiti:
  - La VLAN è già impostata nel dispositivo.
    Vedere la finestra di dialogo *Switching > VLAN > Configuration*.
  - La porta tramite cui il dispositivo inoltra i pacchetti *EtherNet/IP* fa parte della VLAN assegnata e trasmette i pacchetti di dati con una tag VLAN.
    Vedere la finestra di dialogo *Switching > VLAN > Configuration*.
  - È abilitata la funzione *IP Access Restriction*.
    Vedere la finestra di dialogo *Device Security > Management Access > IP Access Restriction*.

Configuration

Write access

Attiva/disattiva la capacità di lettura/scrittura del protocollo *EtherNet/IP*.

Possibili valori:

- `selezionato`
  Il protocollo *EtherNet/IP* accetta le richieste set/get.
- `non selezionato` (impostazione di default)
  La protocollo *EtherNet/IP* accetta solo le richieste get.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Download EDS file

Copia le seguenti informazioni in un file zip sul PC:

- Electronic Data Sheet (EDS) con le informazioni relative al dispositivo
- icona del dispositivo

7.5 Digital IO Module

[Advanced > Digital IO Module]

Gli ingressi digitali consentono l'acquisizione e l'inoltro dei segnali da sensori digitali. Le uscite digitali consentono l'applicazione del segnale, inoltrato dagli ingressi, agli attuatori. La tensione di uscita 24 VDC consente l'utilizzo degli attuatori come spie d'indicazione.

Il dispositivo trasmette segnali sensore in tutta la rete per attivare gli attuatori adatti. Il modulo acquisisce i segnali attraverso le connessioni degli ingressi e li inoltra alle uscite. Sulla base della posizione degli attuatori, il dispositivo inoltra i segnali alle uscite che si trovano sullo stesso modulo, su un modulo diverso all'interno dello stesso dispositivo oppure su un altro dispositivo.

Quando il dispositivo esegue il mapping dalle porte di ingresso digitale alle porte di uscita digitale, sussiste una relazione 1:N. Il dispositivo esegue il mirroring del flusso di dati di una porta di ingresso digitale a un numero qualsiasi di porte di uscita digitale.

Quando il dispositivo esegue il mapping dalle porte di uscita digitale alle porte di ingresso digitale, sussiste una relazione 1:1. Una porta di uscita digitale esegue il mirroring del flusso di dati di una porta di ingresso digitale.

Questa finestra di dialogo include le seguenti schede:
- [IO input]

[IO input]

Questa scheda consente di:
- Attivare/disattivare la richiesta degli ingressi digitali a livello globale
- Configurare l'intervallo in cui il dispositivo richiede i valori degli ingressi digitali
- Attivare/disattivare la registrazione di un evento
- Attivare/disattivare l'invio di SNMP traps

Operation

Operation

Consentire/non consentire le richieste cicliche dagli ingressi digitali (IO Input)

Possibili valori:
- *On*
  Consente la richiesta dei valori di ingresso.
- *Off* (impostazione di default)

Configuration

Refresh interval [ms]

Specifica l'intervallo in millisecondi cui il dispositivo richiede i valori dagli ingressi digitali.

Possibili valori:

- `1000..10000` (impostazione di default: `1000`)

Tabella

Input ID

Visualizza il numero di slot del modulo (x) e il numero di ingresso digitale (i) che si applica a questa voce.

Annotazione: `x.i`

Possibili valori:

- x =`0..7`
  Il valore `0` corrisponde all'unità principale (MU).
- i =`1..4`

Value

Specifica il livello di ingresso digitale.

Possibili valori:

- `low`
  La tensione di ingresso dell'ingresso digitale è 0 V.
- `high`
  La tensione di ingresso dell'ingresso digitale è +24 VDC.
- `not-available`
  La tensione di ingresso dell'ingresso digitale ha un valore diverso da 0 V o +24 VDC. Verificare che il modulo sia presente e in posizione corretta.

Log event

Attiva/disattiva la registrazione nel file di registro. Vedere la finestra di dialogo *Diagnostics > Report >* System Log.

Possibili valori:

- `selezionato`
  La registrazione è attivata.
  Il dispositivo verifica lo stato degli ingressi digitali in base all'intervallo di tempo specificato nel frame *Configuration*, campo *Refresh interval [ms]*.
  Quando si verificano modifiche negli ingressi digitali, il dispositivo registra una voce nel file di registro System Log.
- `non selezionato` (impostazione di default)
  La registrazione è disattivata.

Send trap

Attiva/disattiva l'invio di trap SNMP quando il dispositivo rileva una modifica negli ingressi digitali.

Il dispositivo verifica lo stato degli ingressi digitali in base all'intervallo di tempo specificato nel frame *Configuration*, campo *Refresh interval [ms]*.

Possibili valori:

- `selezionato`
  L'invio di trap SNMP è attivo.
  Se il dispositivo rileva modifiche negli ingressi digitali, il dispositivo invia una trap SNMP.
- `non selezionato` (impostazione di default)
  L'invio di trap SNMP non è attivo.

Il prerequisito per l'invio di trap SNMP è quello di abilitare la funzione nella finestra di dialogo *Diagnostics > Status Configuration > Alarms (Traps)* e specificare almeno una destinazione trap.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

7.6 Command Line Interface

[Advanced > CLI]

Questa finestra di dialogo consente l'accesso al dispositivo utilizzando l'interfaccia a riga di comando.

I prerequisiti sono:
- ☐ Nel dispositivo, abilitare il server SSH nella finestra di dialogo *Device Security > Management Access > Server*, scheda *SSH*.
- ☐ Sulla propria stazione di lavoro, installare un'applicazione client che supporta SSH, che registra un gestore di URL che inizia con `ssh://` nel sistema operativo.

Pulsanti

La descrizione dei pulsanti standard è disponibile nella sezione “Pulsanti” a pagina 17.

Open SSH connection

Apre l'applicazione client che supporta SSH.

Facendo clic sul pulsante, l'applicazione Web accetta l'URL del dispositivo che inizia con `ssh://` e il nome utente dell'utente attualmente registrato.

Se il browser Web individua un'applicazione client che supporta SSH, il client che supporta SSH stabilisce una connessione con il dispositivo utilizzando il protocollo SSH.

A Indice

P

R