

HOW TO

Opzioni di diagnostica su Scalance X

SIEMENS

Contents

Opzioni di diagnostica su Scalance X	3
Utilizzo CPU e RAM	3
Definizione di eventi	4
Log Table	5
Gestione dei Faults	5
Segnalazione eventi tramite Syslog	9
Segnalazione eventi tramite SMTP	10
Segnalazione eventi tramite SNMP	12
Statistiche e RMON	13
Diagnostica dei collegamenti cablati	16
Identificazione Loop di rete	19

Opzioni di diagnostica su Scalance X

L'obiettivo di questa è quello di quidare l'utente nell'utilizzo di alcune funzionalità di diagnostica della famiglia di dispositivi Scalance X.

La guida è valida per i seguenti dispositivi in vendita alla data attuale (10/22) dotati di un firmware aggiornato alla versione 4.3.1:

- **SCALANCE XB-200**
- **SCALANCE XC-200**
- SCALANCE XF-200BA
- **SCALANCE XP-200**
- SCALANCE XR-300WG

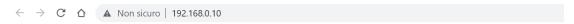
Per la stesura di questa guida, sono stati presi come riferimento due dispositivi delle famiglie XB e XC. Tuttavia, la validità dei procedimenti sequiti è comunque garantita sugli altri dispositivi della famiglia SCALANCE X.

Per ulteriori informazioni e chiarimenti, si rimanda il lettore alla lettura del manuale ufficiale visualizzabile al sequente link:

https://cache.industry.siemens.com/dl/files/818/109799818/att 1088476/v1/PH SCALANCE-XB-200-XC-200-XF-200BA-XP-200-XR-300WG-WBM 76.pdf.

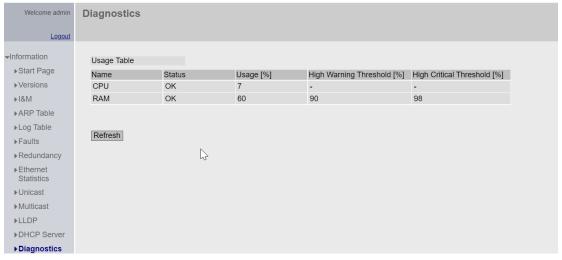
Utilizzo CPU e RAM

Navigando sul percorso "Information/Diagnostics", è possibile avere informazioni circa l'uso della CPU e della RAM, tenendo in considerazione anche eventuali soglie, di tipo Warning o più grave nel caso di Critical.



SIEMENS

192.168.0.10/SCALANCE XB208



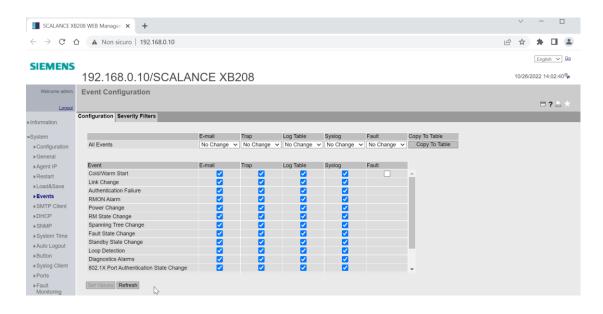
Definizione di eventi

La diagnostica su dispositivi SCALANCE avviene sotto diversi punti di vista per rispondere a diverse esigenze. A tal proposito, gli utenti hanno la possibilità di configurare come il dispositivo deve reagire a diversi eventi al quale può andare incontro.

Per configurarlo, navigare su "System/Events" e nella Tab "Configuration" sarà possibile associare all'evento desiderato, elencato nella colonna "Events", diverse possibilità di notifica:

- E-mail: si utilizza il protocollo SMTP, definendo quindi un SMTP Server e abilitando la funzione SMTP Client (vedere capitolo "Segnalazione eventi tramite SMTP").
- Trap: segnala l'evento sfruttando il protocollo SNMP, se configurato (vedere capitolo "Segnalazione eventi tramite SNMP").
- Log Table: il device registra un'entrata nella tabella di Log, visualizzabile da "Information/Log Table" (Vedere capitolo "Log Table").
- Syslog: se il dispositivo viene configurato come Syslog client e vi è un server Syslog al quale trasferire i dati (vedere capitolo "Segnalazione eventi tramite Syslog").
- Fault: il dispositivo segnala un errore come Fault tramite l'apposito LED (vedere capitolo "Gestione dei Faults").

Scelte le opzioni desiderate, confermare cliccando su Set Values.

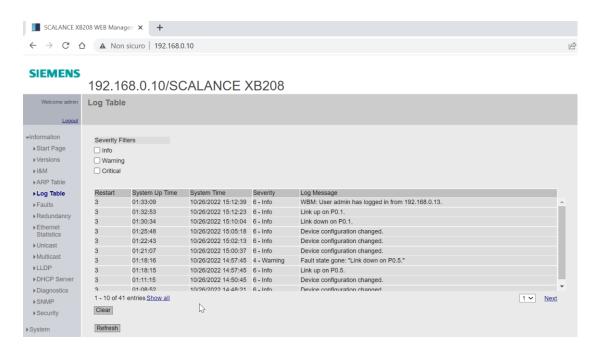


È inoltre possibile, dalla tab "Severity Filters" impostare il livello di soglia (Info, Warning e Critical) per le l'invio delle notifiche relative agli eventi precedentemente selezionati.



Log Table

È possibile visualizzare gli eventi scelti dall'utente ("System/Events"), insieme ad altri prestabiliti dal sistema, seguendo il percorso "Information/Log Table".



Le uniche opzioni modificabili sono i Severity Filters, che permettono di visualizzare soltanto gli eventi del livello di gravità di interesse.

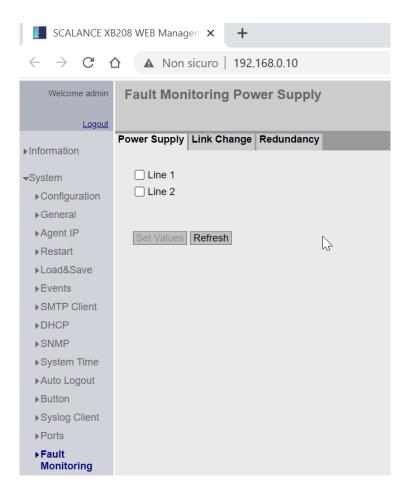
Il contenuto della log table è mantenuto anche quando il dispositivo è spento e può essere azzerato o aggiornato cliccando rispettivamente sul tasto "Clear" o "Refresh".

Gestione dei Faults

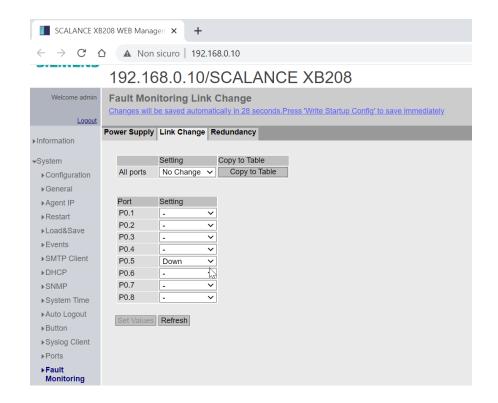
È possibile gestire i motivi per cui la spia di Fault nel dispositivo segnali un problema illuminandosi di rosso.

Dal menu "System", basta selezionare "Fault Monitoring". Nella Tab sono mostrati i tre sottomenù che corrispondono ai motivi per cui la condizione di Fault può essere attivata o disattivata:

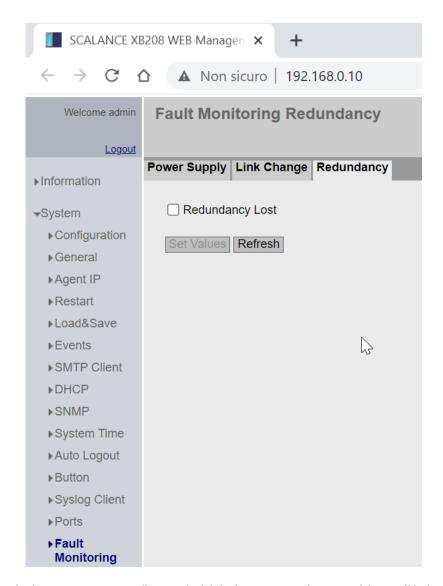
Power Supply: nel caso di doppia alimentazione, posso selezionare quale delle due linee, se staccata, sarà la causa del Fault del dispositivo.



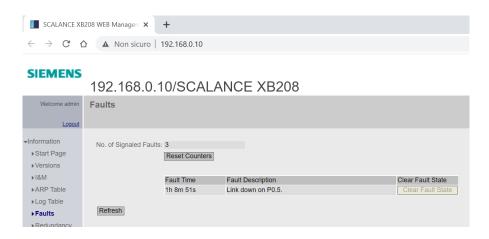
Link Change: posso selezionare in che stato una rispettiva porta debba trovarsi per far andare in Fault il device. Per farlo basta selezionare la porta d'interesse e scegliere per quale stato (Up o Down) il sistema debba andare in Fault.



Redundancy: nel caso il dispositivo abbia attivo un sistema di ridondanza, cliccando sulla voce "Redundancy Lost" il sistema andrà immediatamente in Fault qualora la ridondanza andasse perduta.



Se si desidera capire la presenza o meno di un Fault del device, senza ovviamente visionare il led sull'hardware e desiderando qualche informazione in più circa la causa, è possibile, attraverso il percorso "Information/Faults", visualizzare lo storico dei Fault precedentemente avvenuti.



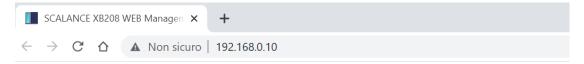
Il device, oltre a mostrare una chiarificazione del motivo del Fault, tiene il conto di Fault avvenuti e della loro durata.

Segnalazione eventi tramite Syslog

Syslog è un protocollo che, in accordo con RFC 3164, viene usato per trasferire messaggi di testo piccoli, non criptati attraverso protocollo UDP nella rete. Ovviamente richiede un Server Syslog da interrogare all'interno della rete.

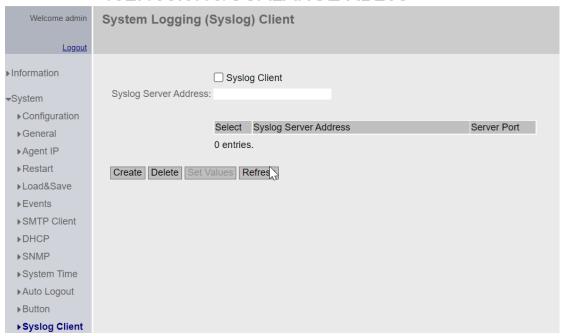
Per attivare il protocollo, basterà seguire questi step:

- Digitare l'indirizzo IP del Server Syslog
- Cliccare su "Create" per creare una riga all'interno della tabella

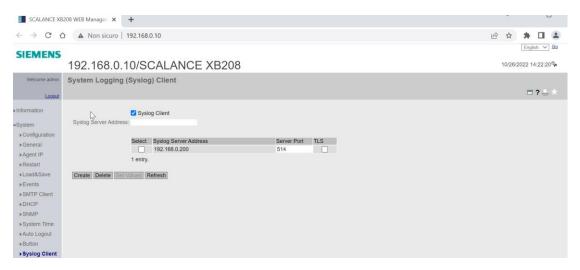


SIEMENS

192.168.0.10/SCALANCE XB208



Impostare la porta UDP del Server ed eventualmente spuntare la voce "TLS" se si desidera una comunicazione criptata con il server.



- Spuntare la voce "Syslog Client"
- Terminare cliccano su "Set Values".

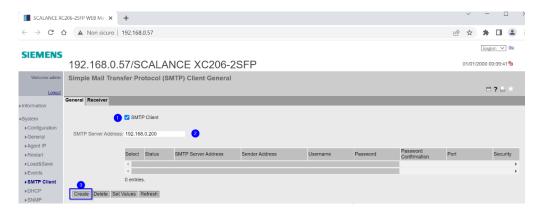
Segnalazione eventi tramite SMTP

La famiglia Scalance X offre la possibilità di inviare automaticamente una e-mail nel caso di eventi specifici, a cui viene spuntata la voce "E-mail" in "System/Events".

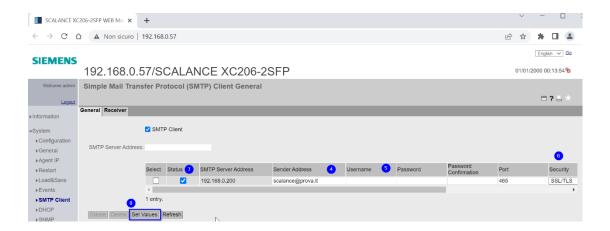
La e-mail conterrà le informazioni nel dispositivo che la invia, una descrizione testuale riguardo la causa ed una marca temporale.

Per configurare questa funzionalità basterà seguire il percorso "System/SMTP Client" e nella tab "General":

- 1. Abilitare la spunta "SMTP Client".
- Digitare l'indirizzo IP del server SMTP alla voce "SMTP Server Address".
- 3. Cliccare sul pulsante "Create" per generare una nuova riga nella tabella.



- 4. Inserire il nome nel dispositivo che verrà incluso nella e-mail per "Sender Email Address".
- 5. Inserire il nome utente e la password nel caso il server SMTP richieda di effettuare il log in.
- 6. Sotto la voce "Security" specificare se la comunicazione deve essere criptata o meno.
- 7. Abilitare la riga per il server SMTP desiderato.
- Salvare le scelte cliccando sul pulsante "Set Values".



A questo punto occorre specificare chi deve ricevere la e-mail quando l'evento si verifica. Per farlo, recarsi alla Tab "Receiver" e:

1. Selezionare il server SMTP richiesto.

▶General

▶Agent IP

▶Restart ▶Load&Save

▶ Events ▶SMTP Client

- 2. Inserire l'indirizzo e-mail del destinatario SMTP.
- 3. Cliccare sul pulsante "Create" per generare una nuova riga nella tabella.



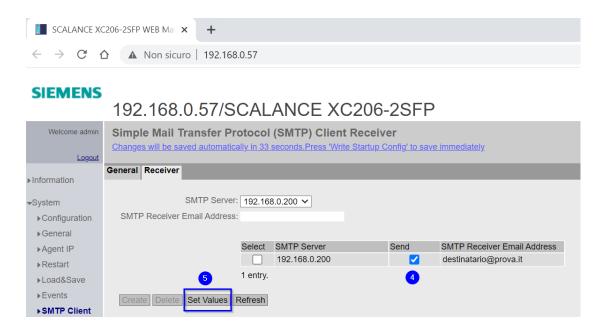
Select SMTP Server Send SMTP Receiver Email Address

Attivare l'opzione "Send" per la riga corrispondente.

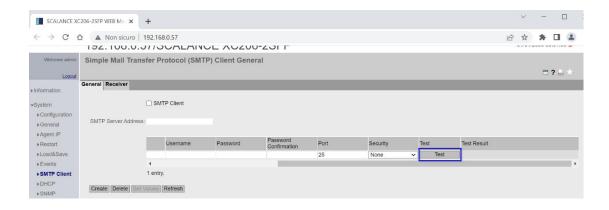
Create Delete Refresh

Confermare le impostazioni tramite il tasto "Set Values".

0 entries.



Se si desidera testare il corretto invio delle e-mail, basterà recarsi nella Tab "General" e cliccare sul tasto "Test". A questo punto il dispositivo manderà una e-mail ad ogni destinatario configurato e il risultato in formato testo sarà disponibile sotto la voce "Test Result" nella tabella.



Segnalazione eventi tramite SNMP

Per la configurazione del protocollo SNMP, si faccia riferimento al precedente How To "Configurazione SNMP" che, nonostante sia stato realizzato per la famiglia SCALANCE W, mantiene la sua validità anche per la famiglia degli SCALANCE X.

La quida è visualizzabile e scaricabile al seguente link:

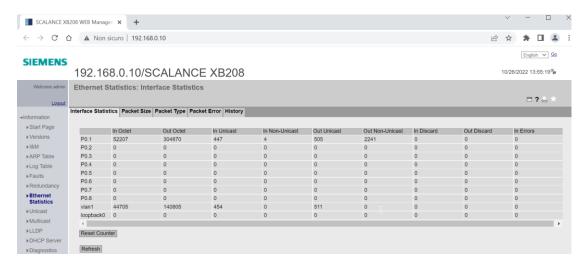
https://assets.new.siemens.com/siemens/assets/api/uuid:8ddf7802-057a-4dbe-8a09-53974def5f3a/configurazione-snmp.pdf

Statistiche e RMON

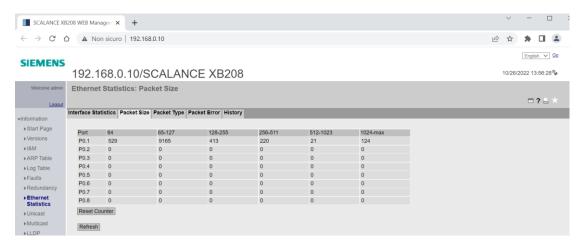
La famiglia di dispositivi Scalance X raccoglie dati di diversa natura e mostra diverse statistiche per l'utente, navigando al percorso "Information/ Ethernet Statistics".

Le informazioni in questa schermata sono solo visualizzabili e, agendo sulla Tab, è possibile scegliere diverse opzioni:

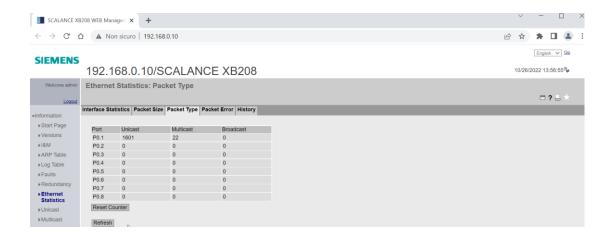
"Interface Statistics": La tabella mostra il numero di bytes ricevuti e inviati, il numero di frames, Unicast e non, ricevuti e inviati, il numero di frames scartati ed infine il numero di tutti i possibili pacchetti errorati. Questi dati vengono forniti per ciascuna porta e per le interfacce VLAN.



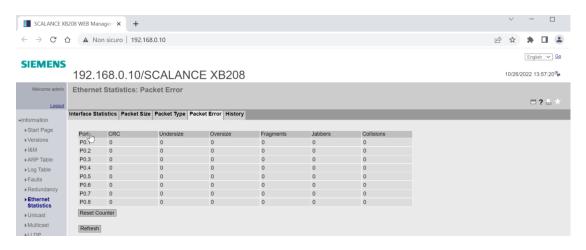
"Packet Size": questa schermata mostra il numero di pacchetti ricevuti e inviati, per ciascuna lunghezza (divisa in gruppi di bytes), su ogni porta. I valori mostrati vengono trasferiti grazie al protocollo RMON, di cui parleremo successivamente.



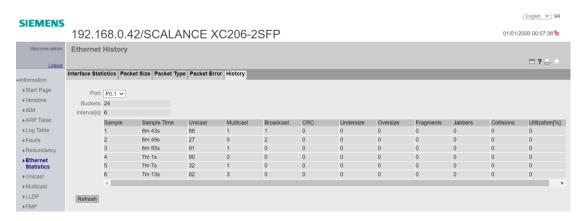
"Packet Type": questa pagina mostra il numero di pacchetti di ciascun tipo (Unicast, Multicast e Broadcast) vengono ricevuti e inviati su ciascuna porta. Anche questi valori vengono trasferiti attravero RMON.



"Packet Error": la pagina mostra il numero di pacchetti difettosi ricevuti per ciascuna porta. I pacchetti vengono suddivisi per il tipo di errore, tra cui un negativo controllo CRC, pacchetti identificati come "undersize" se hanno una lunghezza minore di 64 bytes, come "oversize" se troppo lunghi, come "Fragments" nel caso di pacchetti undersize che non hanno superto il controllo CRC. Inoltre, viene mostrato, sotto la categoria "Jabbers", il numero di pacchetti taggati per una VLAN specifica con un incorretto controllo CRC scartati perché troppo lunghi e il numero di collisioni identificate.



"History": questa pagina mostra i campioni raccolti per la porta selezionata, con le corrispondenti informazioni per le statistiche raccolte tramite RMON. Le informazioni mostrate sono le stesse che abbiamo visto precedentemente, con l'aggiunta della voce "Utilization" che mostra l'utilizzo della porta durante un campionamento.

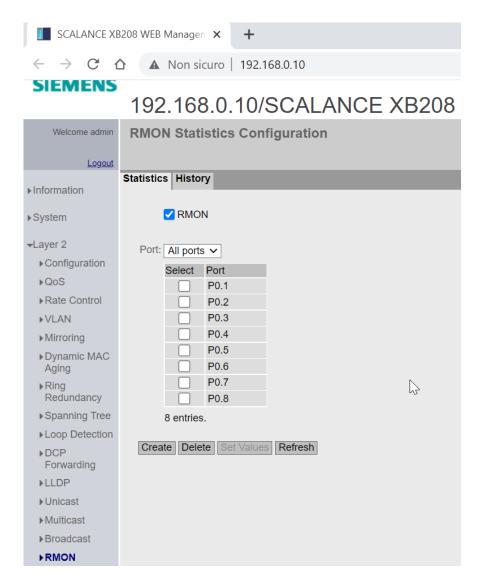


Per ciascuna tab mostrata, è possibile resettare il conteggio tramite il comando "Reset Counter" oppure riaggiornare il conteggio cliccando su "Reset".

N.B.: i menu Tab "Packet Size", "Packet Type", "Packet Error" e "History" mostrano valori che vengono trasferiti attraverso Remote Network Monitoring (RMON), una funzione che va abilitata separatamente, come spiegato nel prossimo capitolo.

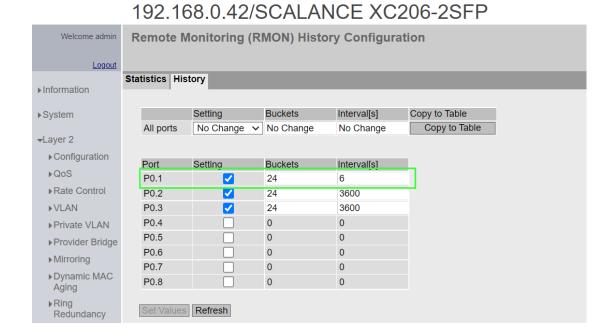
RMON

Seguendo il percorso "Layer 2/RMON", si giungerà alla pagina "Statistics". Qui è possibile spuntare la voce "RMON", la quale, se abilitata, permette di collezionare dati di diagnostica sul dispositivo, prepararli e renderli visibili usando SNMP da una stazione di monitoraggio della rete che supporta anch'essa RMON. Una volta attivata la funzione RMON, e confermando la scelta cliccando su "Set Values", sarà possibile scegliere se attivare tale funzione su una singola porta, su un gruppo di porte creato agendo sui tasti "Create" /" Delete", o so tutte le porti disponibili.



N.B.: se la spunta "RMON" viene disabilitata, le statistiche visualizzabili da "information/Ethernet Statistics" non vengono riaggiornate, ma mantenute nel loro ultimo

Dalla Tab "History" è possibile specificare se i campioni delle statistiche vengono salvati o meno per la corrispondente porta. Inoltre, possono essere impostati il numero di dati in entrata da salvare e con quale intervallo i campioni vanno raccolti:



Diagnostica dei collegamenti cablati

I dispositivi SCALANCE offrono una funzione di diagnostica dei cavi di collegamento disponibile al percorso "System/Port Diagnostic".

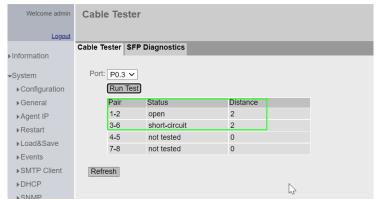
Selezionando la porta dove è connesso il cavo in rame dal menù a tendina e cliccando su "Run Test" si avvierà il test e il dispositivo sarà in grado di analizzare lo stato delle varie coppie del cavo fornendo, in caso di cavo guasto, la distanza del punto di guasto.

Un esempio di cavo tranciato a una distanza di 2m è il seguente:

SIEMENS

SIEMENS

192.168.0.42/SCALANCE XC206-2SFP



Mentre in caso di cavo funzionante:



Attenzione: durante l'esecuzione del test sul cavo, la comunicazione dati viene temporaneamente interrotta!

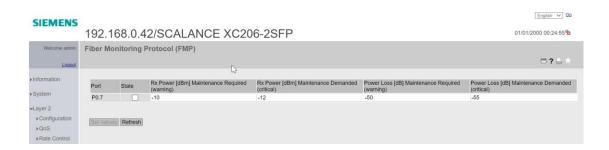
Per i dispositivi SCALANCE X che permettono l'utilizzo della fibra (Scalance X- SFP o Scalance X-C dotati di porte combo), è possibile eseguire ugualmente una diagnostica seguendo lo stesso percorso

SCALANCE XC206-2SFP WEB Mar × + → C 🛕 Non sicuro | 192.168.0.57 Cable Tester | SFP Diagnostics ▶ Information Port: P0.7 ~ System Name: SIEMENS ▶ Configuration Model: SFP992-1 ▶ General Revision: 1 ▶Agent IP Serial: IF0068J7100046 ▶Restart ▶Load&Save Nominal Bit Rate[MBit/s]: 1300 ▶Events Max, Link (single mode)[m]: -▶SMTP Client Max. Link (50.0/125um)[m]: 550 ▶DHCP Max. Link (62.5/125um)[m]: 270 ▶SNMP ▶System Time Temperature[°C]: 38.75 -40.0 ▶ Auto Logout Voltage[V]: 3.29 3.0 3.60 ▶Button Current[mA]: 3.5 0.10 15.0 ▶Syslog Client Rx Power[uW]: 0.0 15.8 631.0 ▶Ports Rx Power[dBm]: --18.0 -2.0 ▶Fault Monitoring Tx Power[uW]: 188.0 89.1 501.2 Tx Power[dBm]: -7.1 ▶PROFINET ▶EtherNet/IP Refresh ▶PLUG ▶Ping ▶DCP Discovery

"System/Port Diagnostics" e cliccando sulla Tab "SFP", dove compariranno diverse informazioni circa il ricetrasmettitore:

N.B.: se c'è connessione dati tramite la fibra, questa verrà interrotta brevemente ed è probabile che per ripristinarla sia necessario riconnettere i cavi manualmente.

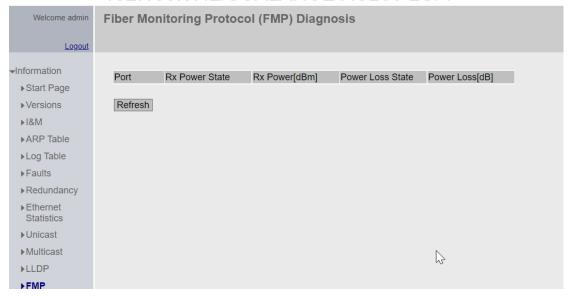
Se si desidera monitorare il traffico di rete scambiato tramite fibra ottica, basterà seguire "Layer 2/FMP", dove è possibile impostare dei parametri di controllo del traffico, come ad esempio il valore di deterioramento della potenza e quelli di perdita di potenza che stabiliscono le condizioni di warning e critical.



Oltre all'impostazione dei valori che definiscono le condizioni di warning e critical, è possibile visualizzare i valori correnti del deterioramento della potenza e della perdita di potenza al percorso "Information/FMP":

SIEMENS

192.168.0.42/SCALANCE XC206-2SFP



Identificazione Loop di rete

Una funzione utile per identificare una condizione di loop all'interno della rete è raggiungibile seguendo il percorso "Layer2/Loop Detection" e spuntando la voce "Loop Detection".

Sarà possibile selezionare per quali porte la funzione sarà attivata, ed in particolare, queste porte invieranno dei frame che, se tornati al dispositivo, dimostrano una condizione di loop.

È possibile spuntare la voce "VLAN Loop Detection" per far utilizzare al dispositivo le informazioni VLAN per la porta corrispondente.

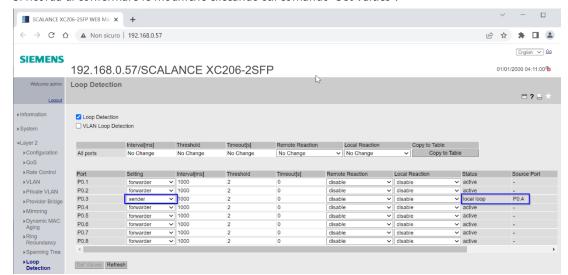
N.B.: per l'attivazione del Loop Detection non possono essere selezione porte di anello, porte in Standby e porte destinate all'interconnessione MRP!

Nella tabella è possibile impostare, per ciascuna porta:

"Setting": Il modo in cui la porta gestisce i loop detection frames, se il dispositivo deve inviare i frames ("Sender"), se deve semplicemente inoltrarli ("Forwarder") o bloccarli ("blocked")

N.B.: è consigliato configurare come "sender" soltanto switch individuali, per esempio ai punti di diramazione dell'anello di ridondanza, e gli altri come "Forwarder" per evitare di creare carico addizionale nella rete dovuto ai loop detection frames

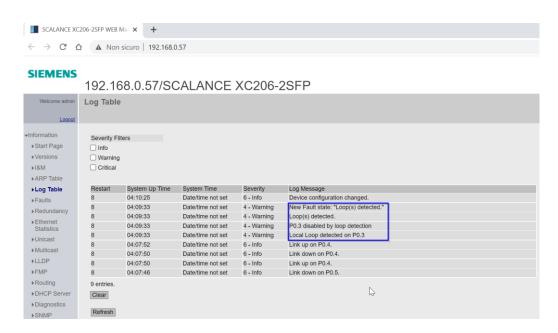
- "Interval": l'intervallo di tempo in millisecondi per l'invio dei frames
- Threshold: numero di frames ricevuti dopo il quale scatta la condizione di Loop.
- Timeouts: i secondi dopo il quale il dispositivo cambia automaticamente lo stato al quale era prima del loop. Se impostato a "0", la porta deve essere abilitata manualmente tramite il bottone "Reset".
- Remote/Local Reaction: a queste voci è possibile scegliere come far reagire la porta nel caso di loop ed in particolare se bloccare la porta tramite la voce "Disable" oppure non eseguire nessuna azione tramite "No Action". La differenza tra loop locale o remoto dipende se il frame di ritorno si manifesta su una porta diversa da quella d'invio o sulla stessa rispettivamente.



Si ricorda di confermare le modifiche cliccando sul comando "Set Values".

Nell'immagine soprastante è mostrato il messaggio mostrato in condizione di loop: scelta la porta 3 come "sender" dei loop detection frame e avendo collegato un cavo di rete dalla porta 3 alla porta 4 dello stesso switch, il dispositivo rileva il loop locale (in quanto i frames arrivano su una porta diversa da quelli di invio) e comunica quale porta è la fonte del loop, ovvero la porta 4 sotto la voce "Source Port" in tabella.

Avendo inserito "Loop Detection" tra gli eventi che desidero registrare nella Log Table del mio dispositivo, attraverso il percorso "System/Events", basterà seguire il percorso "Information/Log Table" per visualizzare la condizione di Loop registrata:



Come si può notare, oltre ad aver segnalato la condizione di loop, il dispositivo reagisce a tale condizione bloccando la porta 3, poiché è stato impostata la voce "disabled" all'interno della tabella nella colonna "Local Reaction" al percorso "Layer 2/Loop Detection".

Con riserva di modifiche e salvo errori.

Il presente documento contiene solo descrizioni generali o informazioni su caratteristiche non sempre applicabili, nella forma descritta, al caso concreto o che possono cambiare a seguito di un ulteriore sviluppo dei prodotti. Le caratteristiche desiderate sono vincolanti solo se espressamente concordate all'atto di stipula del contratto.

Tutte le denominazioni dei prodotti possono essere marchi oppure denominazioni di prodotti della Siemens AG o di altre ditte fornitrici, il cui utilizzo da parte di terzi per propri scopi può violare il diritto dei proprietari.