

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 guidare 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 seguiti 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 seguente 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.

 $\leftrightarrow \rightarrow$  C  $\triangle$  Non sicuro | 192.168.0.10

#### SIEMENS

	192.168.0	.10/SCAL	ANCE XB	208		
Welcome admin	Diagnostics					
Logout						
-Information	Usage Table					
▶Start Page	Name	Status	Usage [%]	High Warning Threshold [%]	High Critical Threshold [%]	
▶Versions	CPU	ОК	7	-	-	
▶I&M	RAM	ОК	60	90	98	
►ARP Table						
▶Log Table						
▶ Faults	Refresh					
▶Redundancy		€J				
▶ Ethernet Statistics						
►Unicast						
►Multicast						
▶LLDP						
►DHCP Server						
▶Diagnostics						

### 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.

	1208 WEB Managerry × +								$\sim$	-		]
JCALARCE AD	200 Web Managen X											
$\leftrightarrow$ $\rightarrow$ C (	A Non sicuro   192.168.0.10							Ê	☆	*		-
SIEMENS										Englis	h V	Go
SILITILITS	192.168.0.10/SCALAN	VCE XB2	208						10/26/2	022 14	:02:40	)@
Welcome admin	Event Configuration											
Logout											? 📑	
	Configuration Severity Filters											
▶ Inionnauon												
-System		E-mail	Trap	Log Table	Syslog	Fault	Copy To Table					
▶Configuration	All Events	No Change 🗸	No Change 🗸	No Change 🗸	No Change 🗸	No Change 🗸	Copy To Table					
▶General												
▶Agent IP	Event	E-mail	Trap	Log Table	Syslog	Fault						
> Pectart	Cold/Warm Start	<b>~</b>	· · ·	Z	Z							
Presidit	Link Change											
▶Load&Save	Authentication Failure	<b>Z</b>	<b>~</b>	<b>~</b>	<b>Z</b>							
►Events	RMON Alarm	<b>~</b>	<b>~</b>	<b>~</b>	<b>~</b>							
▶SMTP Client	Power Change	<b>~</b>	<b>~</b>	<b>~</b>	<b>~</b>							
▶DHCP	RM State Change	<b>Z</b>	<b>~</b>	<b>~</b>	<b>~</b>							
▶SNMP	Spanning Tree Change	<b>~</b>	<b>~</b>	<b>~</b>	<b>~</b>							
System Time	Fault State Change	<b>~</b>	<b>~</b>	2	<b>~</b>							
»Auto Logout	Standby State Change	<b>~</b>	<b>~</b>	<b>~</b>	<b>~</b>							
- Dutter	Loop Detection	Image: A start and a start	<b>~</b>	Image: A start and a start	<b>~</b>							
▶ Button	Diagnostics Alarms	<b>~</b>	<b>~</b>	Image: A start and a start	<b>~</b>							
Syslog Client	802.1X Port Authentication State Change	Image: A state of the state	Image: A state of the state	Image: A start and a start	<b>~</b>		*					
▶Ports												
Fault Monitoring	Set Values Refresh											

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.

SCALANCE XE	3208 WEB Manageri × +					$\checkmark$	-	
$\leftrightarrow$ $\rightarrow$ C (	▲ Non sicuro   192.1	68.0.10				Ê 1	*	
CIEMENIC							Engl	ish 🗸 <u>Go</u>
SIEMENS	192.168.0.10/	SCALANC	E XB208			10/2	:6/2022 1	4:03:07 <b>%</b>
Welcome admin	Event Severity Filters							
Logout								? 🗄 🖈
Information	Configuration Severity Filters							
-system	Client Type	Severity	1					
▶Configuration	E-mail	Info ~	]					
▶General	Log Table	Info ~						
Agent IP	Syslog							
▶Restart	Set Values Refresh							
▶Load&Save								
. Encoder								

### Log Table

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

SCALANCE XB	208 WEB Mana	gen × +					
$\leftrightarrow$ $\rightarrow$ C (	A Non	sicuro   192.168.0	.10				Ė
SIEMENS	192.16	68.0.10/SC	CALANCE >	(B208			
Welcome admin	Log Table						
Logout							
<ul> <li>✓Information</li> <li>◆Start Page</li> <li>◆Versions</li> <li>◆I&amp;M</li> <li>◆ARP Table</li> </ul>	Severity Fil Info Warning Critical	ters					
NLog Table	Restart	System Up Time	System Time	Severity	Log Message		
> Eculto	3	01:33:09	10/26/2022 15:12:39	6 - Info	WBM: User admin has logged in from 192.168.0.13.		
Faults	3	01:32:53	10/26/2022 15:12:23	6 - Info	Link up on P0.1.		
▶Redundancy	3	01:30:34	10/26/2022 15:10:04	6 - Info	Link down on P0.1.		
► Ethernet Statistics	3	01:25:48	10/26/2022 15:05:18	6 - Info	Device configuration changed.		
Statistics	3	01:22:43	10/26/2022 15:02:13	6 - Info	Device configuration changed.		
▶ Unicast	3	01:21:07	10/26/2022 15:00:37	6 - Info	Device configuration changed.		
▶Multicast	3	01:18:16	10/26/2022 14:57:45	4 - Warning	Fault state gone: "Link down on P0.5."		
▶LLDP	3	01:18:15	10/26/2022 14:57:45	6 - Info	Link up on P0.5.		
DHCP Server	3	01:11:15	10/26/2022 14:50:45	6 - Info	Device configuration changed.		
▶Diagnostics	3	01-08-52	10/26/2022 14-48-21	6 - Info	Device configuration changed		
▶ SNMP	1 - 10 of 41	entries Show all				1 ❤ <u>Ne</u>	<u>xt</u>
▶Security	Clear		2				
▶System	Refresh						

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.

SCALANCE X	B208 WEB Managen 🗙 🕂
$\leftrightarrow$ $\rightarrow$ C t	▲ Non sicuro   192.168.0.10
Welcome admin	Fault Monitoring Power Supply
Logout	
►Information	Power Supply Link Change Redundancy
∽Svstem	Line 1
Configuration	Line 2
▶ General	
►Agent IP	Set Values Refresh
▶Restart	
▶Load&Save	
▶Events	
▶SMTP Client	
▶DHCP	
▶SNMP	
▶System Time	
►Auto Logout	
▶Button	
▶Syslog Client	
▶ Ports	
Fault Monitoring	

• 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.

SCALANCE XE	3208 WEB Manag	gen × +
$\leftrightarrow$ $\rightarrow$ C (	A Non	sicuro   192.168.0.10
	192.16	8.0.10/SCALANCE XB208
Welcome admin	Fault Mon	itoring Link Change
	Changes will I	be saved automatically in 28 seconds.Press 'Write Startup Config' to save immediately
Logout		
▶ Information	Power Supply	Link Change Redundancy
Finiornation		
-System		Setting Copy to Table
▶Configuration	All ports	No Change 🗸 Copy to Table
▶General		
▶Agent IP	Port	Setting
▶Restart	P0.1	· · ·
▶Load&Save	P0.2	- v
> Events	P0.3	· · ·
	P0.4	· •
► SM I P Client	P0.5	Down V
▶DHCP	P0.6	<u> </u>
▶SNMP	P0.7	· · ·
▶System Time	P0.8	· · ·
►Auto Logout	Sot Values	Pofresh
▶Button	loct values	Renden
▶Syslog Client		
▶Ports		
Fault Monitoring		

• 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.

SCALANCE XE	3208 WEB Managen 🗙 🕂
$\leftrightarrow$ $\rightarrow$ C (	A Non sicuro   192.168.0.10
Welcome admin	Fault Monitoring Redundancy
Logout	
▶ Information	Power Supply Link Change Redundancy
<b>⊸</b> System	Redundancy Lost
▶Configuration	Cat Values Defrach
▶General	Set values Reliesn
▶Agent IP	
▶Restart	
▶Load&Save	
▶Events	$\searrow$
▶SMTP Client	
▶DHCP	
▶SNMP	
▶System Time	
►Auto Logout	
▶Button	
Syslog Client	
▶Ports	
Fault Monitoring	

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.

SCALANCE XB	208 WEB Managen 🗙	+		
$\leftrightarrow$ $\rightarrow$ C C	A Non sicuro	192.168.0.10		
SIEMENS	192.168.0.1	0/SCALA	NCE XB208	
Welcome admin	Faults			
Logout				
<ul> <li>Information</li> <li>▶Start Page</li> <li>▶Versions</li> </ul>	No. of Signaled Faults:	3 Reset Counters		
▶I&M ▶ARP Table		Fault Time 1h 8m 51s	Fault Description Link down on P0.5.	Clear Fault State Clear Fault State
►Log Table ►Faults ►Redundancy	Refresh			

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:

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



#### SIEMENS

#### 192.168.0.10/SCALANCE XB208

Welcome admin	System Logging (S	yslog) Client		
<u>Logout</u>				
►Information ←System	C Syslog Server Address:	] Syslog Client		
►Configuration ►General	s	Select Syslog Server Ad	dress	Server Port
►Agent IP	C	entries.		
▶Restart	Create Delete Set Val	ues Refres		
►Load&Save Events				
▶SMTP Client				
▶DHCP				
▶SNMP				
►System Time				
►Auto Logout				
▶Button				
►Syslog Client				

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

SCALANCE XB	B208 WEB Managerr × +	· ⊔
$\leftrightarrow$ $\rightarrow$ C (	A Non sicuro   192.168.0.10	ic 🛧 🛪 🗖 😩
SIEMENS	192.168.0.10/SCALANCE XB208	English ✓ 92 10/26/2022 14:22:20%
Logout	System Logging (Sysiog) Client	<b>- ?</b> = *
Information  System  Configuration  General  Agent IP  Restart  Restart  Events  SMTP Citents  SMTP Citent  SMMP  System Time  Auto Logout  Button  Sugott	Syslog Server Address: Select Syslog Server Address Server Port TLS 1 192,168.0.200 514 1 entry: Create Delete SerValues Refresh	

- 4. Spuntare la voce "Syslog Client"
- 5. 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".
- 2. Digitare l'indirizzo IP del server SMTP alla voce "SMTP Server Address".
- 3. Cliccare sul pulsante "Create" per generare una nuova riga nella tabella.

SCALANCE XC	206-2SFP WEB Mar 🗙	+							~	- 0	]
$\leftrightarrow$ $\rightarrow$ C (	△ 🔺 Non sicuro   192.168.0.57									* 🗉	
										<u>Go</u>	
	192.100.0.	5115	GALAI	NCE AC200-2	SFF				0110112		
Welcome admin	Simple Mail Tran	isfer Pro	otocol (SI	MTP) Client General							
Logout										<b>?</b> -	
. Information	General Receiver										
Information											
-System	•	SMTI	P Client								
▶Configuration		- 400 400	0.000	•							
▶General	SMTP Server Addres	IS: 192.168	1.0.200	<b>4</b>							
▶Agent IP		_				_		Bassword			_
▶Restart		Select	Status	SMTP Server Address	Sender Address	Username	Password	Confirmation	Port	Secur	ity
▶Load&Save		€.									•
▶Events											•
► SMTP Client	3	0 entries	8.								
▶ DHCP	Create Delete Se	t Values F	Refresh								
▶SNMP											

- 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.
- 8. Salvare le scelte cliccando sul pulsante "Set Values".

r											~	_		
SCALANCE XC	206-2SFP WEB Mar 🗙	+									Ť			
$\leftrightarrow$ $\rightarrow$ C (	A Non sicuro	192.168	0.57								6 \$	*		)
SIEMENS												Engli	ish 🗸 Go	
5121112113	192.168.0.	57/S	CALA	NCE XC206-	2SFP						01/01/	2000 0	0:13:54 🔁	
Welcome admin	Simple Mail Tran	sfer Pro	otocol (SI	ITP) Client General	l .									
Logout												-	? 🛎 🖈	
	General Receiver													
Information		_	_			_	_	_	_				_	
→System		🗹 SMTI	P Client											
Configuration														
▶General	SMTP Server Addres	s:												
► Agent IP													6	
▶Restart		Select	Status 7	SMTP Server Address	Sender Address	4	Username	5	Password	Password Confirmation	Port		Security	E.
▶Load&Save				192.168.0.200	scalance@prova.it						465		SSL/TLS	
▶Events		•											-	•
▶SMTP Client	•	1 entry.												
*DHCP	<u>e</u>													
. 01110	Create Delete Set	Values F	Refresh	N										

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

← → C ☆ ▲ Non sicuro | 192.168.0.57

SCALANCE XC206-2SFP WEB Mar × +

#### SIEMENS

	192.168.0.57/SCALANCE XC206-2SFP											
Welcome admin	Simple Mail Transfer Pro	otocol (SMTP) Clien	t Receiver									
Logout												
Information	General Receiver											
Finiornation												
-System	SMTP Server:	192.168.0.200 🗸 🕛										
►Configuration	SMTP Receiver Email Address:	destinatario@prova.it	]2									
▶General												
▶Agent IP		Select SMTP Server	Send	SMTP Receiver Email Address								
▶Restart	3	0 entries.										
▶Load&Save	Create Delete Pofresh											
▶Events	Create Delete Refresh											
▶ SMTP Client												

- 4. Attivare l'opzione "Send" per la riga corrispondente.
- 5. Confermare le impostazioni tramite il tasto "Set Values".

SCALANCE X	206-2SFP WEB Ma × +
$\leftrightarrow$ $\rightarrow$ C (	A Non sicuro   192.168.0.57
SIEMENS	192.168.0.57/SCALANCE XC206-2SFP
Welcome admin <u>Logout</u>	Simple Mail Transfer Protocol (SMTP) Client Receiver Changes will be saved automatically in 33 seconds.Press 'Write Startup Config' to save immediately.
▶ Information	General Receiver
<ul> <li>System</li> <li>▶ Configuration</li> <li>▶ General</li> </ul>	SMTP Server: 192.168.0.200 V SMTP Receiver Email Address:
▶Agent IP	Select SMTP Server Send SMTP Receiver Email Address
▶Restart	192.168.0.200 destinatario@prova.it
▶Load&Save	5 1 entry. 4
▶Events	Create Delete Set Values Refresh
►SMTP Client	

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.

SCALANCE XC	206-2SFP WEB Ma 🗙	+							~	-		
$\leftrightarrow$ $\rightarrow$ C C	Non sicuro   1	92.168.0.57							6 \$	*		0
	132.100.0.0	NOUNLAN	UL AUZU	0-201 F					01101			
Welcome admin	Simple Mail Trans	er Protocol (SM1	P) Client Gene	eral								
Logout											? 🛎 🖈	
	General Receiver											
Information												
-System	1	SMTP Client										
► Configuration												
General	SMTP Server Address:											
▶Agent IP				Descent								
Restart		Username	Password	Confirmation	Port	Security	Test	Test Result				
▶Load&Save					25	None	✓ Test					
▶Events		4										۲
▶ SMTP Client		1 entry.										
▶ DHCP	Croate Dalata Sala	Bofrach										
▶ SNMP	Cicate Delete Set V	rides										

### 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 guida 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.

SCALANCE XB	208 WEB Manag	err × +								~ -	- [	1
$\rightarrow$ C (	A Non	sicuro   192.1	68.0.10						Ŕ	* 1		-
										E	nglish 🗸	G
EMENS	192.16	8.0.10/	SCALANC	E XB208						10/26/2022	2 13:55:19	P
Welcome admin	Ethernet S	statistics: In	terface Statistic	s								
Looput											<b>?</b> .	
Logists	Interface Statis	tics Packet Si	ze Packet Type Pac	ket Error History								
mation										_	_	Ĩ
art Page		In Octet	Out Octet	In Unicast	In Non-Unicast	Out Unicast	Out Non-Unicast	In Discard	Out Discard	In Err	ors	
rsions	P0.1	52207	304870	447	4	505	2241	0	0	0		
N	P0.2	0	0	0	0	0	0	0	0	0		
P Table	P0.3	0	0	0	0	0	0	0	0	0		
Table	P0.4	0	0	0	0	0	0	0	0	0		
ilts	P0.5	0	0	0	0	0	0	0	0	0		
dundancy	P0.6	0	0	0	0	0	0	0	0	0		
undancy	P0.7	0	0	0	0	0	0	0	0	0		
tistics	P0.8	0	0	0	0	0	0	0	0	0		
icast	vlan1	44705	140805	454	0	511	0	0	0	0		
liteest	loopback0	0	0	0	0	0	0	0	0	0		
anucasi	•											
UP	Reset Cour	nter										
HCP Server												
agnostics	Refresh											

• "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.

SCALANCE XE	3208 WEB Mar	nagen × +								$\vee$	-		
$\leftrightarrow$ $\rightarrow$ C f	A No	on sicuro   192	2.168.0.10						Ê	☆	*		9
SIEMENS	192.1	68.0.10	)/SCALAN(	CE XB208	3					10/26/2	Englisi	56:28¶	2
Welcome admin	Etherne	t Statistics:	Packet Size								<b>=</b> 1	<b>?</b> ≞ ★	
-Information	Interface Sta	atistics Packet	Size Packet Type Pa	acket Error History									
▶Start Page	Port	64	65-127	128-255	256-511	512-1023	1024-max						
▶Versions	P0.1	529	9165	413	220	21	124						
▶1&M	P0.2	0	0	0	0	0	0						
♦ARP Table	P0.3	0	0	0	0	0	0						
Log Table	P0.4	0	0	0	0	0	0						
Faults	P0.5	0	0	0	0	0	0						
▶Redundancy	P0.6	0	0	0	0	0	0						
► Ethernet Statistics	P0.7 P0.8	0	0	0	0	0	0						
▶Unicast	Reset Co	ounter											
▶Multicast	Defrech	1											
▶LLDP	Kellesii	1											

• "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.

SCALANCE XE	3208 WEB Mar	nagen × +		
$\leftrightarrow$ $\rightarrow$ C (	A No	on sicuro   192	.168.0.10	
SIEWIENS	192.1	68.0.10	SCALANC	CE XB208
Welcome admin	Etherne	t Statistics: I	Packet Type	
Logout				
	Interface Sta	atistics Packet S	Size Packet Type Pa	cket Error History
-Information				
▶ Start Page	-			
	Port	Unicast	Multicast	Broadcast
▶ Versions	Port P0.1	Unicast 1601	Multicast 22	Broadcast 0
≽Versions ≽I&M	Port P0.1 P0.2	Unicast 1601 0	Multicast 22 0	Broadcast 0 0
<ul> <li>Versions</li> <li>I&amp;M</li> <li>ARP Table</li> </ul>	Port P0.1 P0.2 P0.3	Unicast 1601 0 0	Multicast 22 0 0	Broadcast 0 0 0
<ul> <li>Versions</li> <li>I&amp;M</li> <li>ARP Table</li> <li>Log Table</li> </ul>	Port P0.1 P0.2 P0.3 P0.4	Unicast 1601 0 0 0	Multicast 22 0 0 0 0	Broadcast 0 0 0 0
<ul> <li>Versions</li> <li>►I&amp;M</li> <li>►ARP Table</li> <li>►Log Table</li> <li>►Faults</li> </ul>	Port P0.1 P0.2 P0.3 P0.4 P0.5	Unicast 1601 0 0 0 0 0	Multicast 22 0 0 0 0 0	Broadcast 0 0 0 0 0 0
Versions I&M ARP Table Log Table Faults Perfundancy	Port P0.1 P0.2 P0.3 P0.4 P0.5 P0.6	Unicast 1601 0 0 0 0 0 0 0	Multicast 22 0 0 0 0 0 0 0	Broadcast 0 0 0 0 0 0 0
	Port P0.1 P0.2 P0.3 P0.4 P0.5 P0.6 P0.7	Unicast 1601 0 0 0 0 0 0 0 0	Multicast 22 0 0 0 0 0 0 0 0 0	Broadcast 0 0 0 0 0 0 0 0 0 0 0 0 0
<ul> <li>Versions</li> <li>I&amp;M</li> <li>ARP Table</li> <li>Log Table</li> <li>Faults</li> <li>Redundancy</li> <li>Ethernet Statistics</li> </ul>	Port P0.1 P0.2 P0.3 P0.4 P0.5 P0.6 P0.7 P0.8	Unicast 1601 0 0 0 0 0 0 0 0 0 0 0	Multicast 22 0 0 0 0 0 0 0 0 0 0 0 0	Broadcast 0 0 0 0 0 0 0 0 0 0 0 0 0
<ul> <li>Versions</li> <li>I&amp;M</li> <li>ARP Table</li> <li>Log Table</li> <li>Faults</li> <li>Redundancy</li> <li>Ethernet Statistics</li> <li>Unicast</li> </ul>	Port P0.1 P0.2 P0.3 P0.4 P0.5 P0.6 P0.7 P0.8 Reset C	Unicast 1601 0 0 0 0 0 0 0 0 0 0 0 0 0	Multicast 22 0 0 0 0 0 0 0 0 0	Broadcast 0 0 0 0 0 0 0 0 0 0 0 0 0

• "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.

SCALANCE XE	208 WEB Man	agen × +							$\sim$	-	
$\leftrightarrow$ $\rightarrow$ C (	A No	n sicuro   19	2.168.0.10					Ê	☆	*	
SIEMENS	192.1	68.0.10	)/SCALANC	CE XB208	}				10/26/2	Englis	<u>sh ∨ Go</u> 3:57:20%
Welcome admin	Ethernet	t Statistics:	Packet Error								?≞★
-Information	Interface Sta	tistics Packet	Size Packet Type Pa	cket Error History							
Istart Page	Porte	CRC	Undersize	Quercize	Fragments	Inhhere	Collisions				
▶Versions	PO.	0	0	0	0	0	0				
▶18.M	P0.2	0	0	0	0	0	0				
♦ARP Table	P0.3	0	0	0	0	0	0				
Log Table	P0.4	0	0	0	0	0	0				
Faults	P0.5	0	0	0	0	0	0				
▶Redundancy	P0.6	0	0	0	0	0	0				
► Ethernet Statistics	P0.7 P0.8	0	0	0	0	0	0				
▶Unicast	Reset Co	ounter									
▶Multicast	Defrech	1									
NUDP	Kellesii	J									

 "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.

SIEMENS													English 🗸 😡	
SIEWIENS	192.1	68.0.4	2/SCALA	NCE X	C206-2	SFP						01/01/20	000 00:07:36	
Welcome admin	Ethernet	History												
Logout													🗆 <b>?</b> 🛎 🖈	
-Information	Interface Stat	tistics Pack	et Size Packet Typ	Packet Err	or History									
Start Page	Port	P0.1 ¥												
▶Versions	Buckets:	24												
▶1&M	Interval[s]:	6												
▶ARP Table		Sample	Sample Time	Unicast	Multicast	Broadcast	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions	Utilization[%]	
Log Table		1	6m 43s	88	1	1	0	0	0	0	0	0	0	
▶Faults		2	6m 49s	27	0	2	0	0	0	0	0	0	0	
▶Redundancy		3	6m 55s	91	1	0	0	0	0	0	0	0	0	
►Ethernet		4	7m 1s	90	0	0	0	0	0	0	0	0	0	
Statistics		5	7m 7s	32	1	0	0	0	0	0	0	0	0	
▶Unicast		6	7m 13s	82	3	0	0	0	0	0	0	0	0	
▶Multicast														۲
▶LLDP	Refresh													
<b>NEMP</b>														

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" *I*" Delete", o so tutte le porti disponibili.

SCALANCE XB	208 WEB Managen × +
$\leftrightarrow$ $\rightarrow$ C (	A Non sicuro   192.168.0.10
SIEMENS	192.168.0.10/SCALANCE XB208
Welcome admin	RMON Statistics Configuration
Logout	
►Information	Statistics History
▶System	Z RMON
←Layer 2	Port: All ports x
▶Configuration	Select Port
▶QoS	
▶Rate Control	P0.2
▶VLAN	<b>P</b> 0.3
► Mirroring	<b>P</b> 0.4
▶Dynamic MAC Aging	P0.5 P0.6
▶Ring Redundancy	P0.7
▶Spanning Tree	8 entries.
►Loop Detection	
►DCP Forwarding	Create Delete Set Values Refresh
▶LLDP	
►Unicast	
▶Multicast	
▶Broadcast	
►RMON	

63

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

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:

#### SIEMENS

	192.168.0.42/SCALANCE XC206-2SFP												
Welcome admin	Remote N	Ionitoring (R	MON) Histo	ory Configura	tion								
Logout													
▶ Information	Statistics His	Statistics History											
▶System		Setting	Buckets	Interval[s]	Copy to Table								
	All ports	No Change 🗸	No Change	No Change	Copy to Table								
►Configuration	Dent	O a thin a	Duchata	late a selfel									
▶QoS	Port	Setting	Buckets	Intervalisi	-								
- Data Control	P0.1		24	6									
Rate Control	P0.2		24	3600									
▶VLAN	P0.3	Image: A start and a start and a start a st	24	3600									
Private VLAN	P0.4		0	0									
▶Provider Bridge	P0.5		0	0									
Mirroring	P0.6		0	0									
- Dumonala MAO	P0.7		0	0									
►Dynamic MAC Aging	P0.8		0	0									
▶Ring Redundancy	Set Values	Refresh											

### 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						
	192	.168	.0.42/SCAL	ANCE	XC20	6-2SFP
Malaama admin	Cable	Tester				
weicome aumin	Cable	e lester				
Logout						
	Cable Te	ster SFF	Diagnostics			
Information						
-System	Port:	P0.3 🗸				
► Configuration		Run Test	)			
▶General		Pair	Status	Distance		
▶Agent IP		1-2	open	2		
▶Restart		3-6	short-circuit	2		
N Loads Save		4-5	not tested	0		
FLOAUQSave		7-8	not tested	0		
▶Events						
►SMTP Client	Refre	esh				
▶DHCP					N	
▶ SNMP					43	

Mentre in caso di cavo funzionante:

SCALANCE XE	3208 WEB	Managen 3	× +		
$\leftarrow$ $\rightarrow$ C (		Non sicu	ro   192.168.0.10		
Logout					
►Information	Cable Te	ster			
-System	Port:	P0.1 ➤			
Configuration		Run Test			
▶General		Pair	Status	Distance	
▶Agent IP		1-2	ОК	unknown	
▶Restart		3-6	ОК	unknown	
▶Load&Save		4-5	not tested	0	
▶Events		7-8	not tested	0	
▶SMTP Client	Refre	esh			
▶DHCP					
▶SNMP					
▶Svstem Time					
►Auto Logout					
▶Button					
▶Svslog Client					
▶Ports					
Fault Monitoring					
▶PROFINET					
▶EtherNet/IP					
▶Ping					
►DCP Discovery					
▶Port Diagnostics					

#### 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

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

SCALANCE X	C206-2SFP WEB Mar × +			
$\leftarrow \rightarrow $ C $+$	△ A Non sicuro   192.168.0.57			
Logout	Cable Tester SFP Diagnostics			
►Information				
-System	Port: P0.7 V			
▶Configuration	Name: SIEMENS			
▶ General	Model: SFP992-1			
▶Agent IP	Revision: 1			
▶Restart	Serial: IF0068J7100046			
▶Load&Save				
►Events	Nominal Bit Rate[MBIt/s]: 1300			
▶SMTP Client	Max. Link (single mode)[m]: -			
▶ DHCP	Max. Link (50.0/125um)[m]: 550			
▶SNMP	Max. Link (62.3/1230m)[m]: 270			
▶System Time	Current	Low	High	
►Auto Logout	Temperature[°C]: 38.75	-40.0	110.0	
▶Button	Voltage[V]: 3.29	3.0	3.60	
▶Svslog Client	Current[mA]: 3.5	0.10	15.0	
▶Ports	Rx Power[uW]: 0.0	15.8	631.0	
▶ Foult	Rx Power[dBm]: -	-18.0	-2.0	
Monitoring	Tx Power[uW]: 188.0	89.1	501.2	
▶PROFINET	Tx Power[dBm]: -7.1	-10.5	-3.0	
▶EtherNet/IP	Defeat			
▶PLUG	Reliesh			
▶Ping				
►DCP Discovery				
▶Port Diagnostics				

### 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.

						English 🗸 🖸
SIEMIENS	192.1	68.0.4	2/SCALANCE XC20	6-2SFP		01/01/2000 00:24:55
Welcome admin	Fiber Mo	onitoring	Protocol (FMP)			
Logout			N			□?≞★
. Information			6			
▶ Information	Port	State	Rx Power [dBm] Maintenance Required (warning)	Rx Power [dBm] Maintenance Demanded (critical)	Power Loss [dB] Maintenance Required (warning)	Power Loss [dB] Maintenance Demanded (critical)
▶System	P0.7		-10	-12	-50	-55
-Layer 2						
▶Configuration	Set Value	Refresh				
▶QoS						
▶Rate Control						

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										
	192.10	68.0.42/S	CALANCE	E XC206-2	SFP					
Welcome admin	Fiber Monitoring Protocol (FMP) Diagnosis									
Logout										
Logour										
-Information	Port	Rx Power State	Rx Power[dBm]	Power Loss State	Power Loss[dB]					
▶Start Page			naci onor[abiii]							
▶Versions	Refresh									
▶I&M										
►ARP Table										
▶Log Table										
Faults										
▶Redundancy										
▶ Ethernet Statistics										
▶Unicast										
▶Multicast					N					
▶LLDP					N2					
►FMP										

### 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 con	mando "Set Values".
---	---------------------

SCALANCE XC	206-2SFP WEB Mar 🗙	+							$\sim$	-	
$\leftrightarrow$ $\rightarrow$ C $\triangle$	A Non sicuro	192.168.0.57						Ŕ	☆	* 1	<b>a</b>
SIEMENS 192.168.0.57/SCALANCE XC206-2SFP											
Welcome admin	Loop Detection				13					□?	= <b>*</b>
<ul><li>► Information</li><li>► System</li></ul>	✓ Loop Detection ○ VLAN Loop Dete	ction									
-Layer 2		Interval[ms]	Threshold	Timeout[s]	Remote Reaction	Local Reaction	Copy to Table				
►Configuration	All ports	No Change	No Change	No Change	No Change	V No Change	<ul> <li>Copy to Ta</li> </ul>	ble			
▶QoS											
Rate Control	Port	Setting	Interval[ms]	Threshold	Timeout[s]	Remote Reaction	Local Reaction	Status		ource P	ort
▶VLAN	P0.1	forwarder V	1000	2	0	disable	✓ disable	✓ active		001001	
▶ Private VLAN	P0.2	forwarder 🗸	1000	2	0	disable	✓ disable	✓ active			
Provider Bridge	P0.3	sender 🗸	1000	2	0	disable	✓ disable	<ul> <li>local loop</li> </ul>	F	P0.4	
Mirroring	P0.4	forwarder 🗸	1000	2	0	disable	✓ disable	✓ active		_	
Finitioning	P0.5	forwarder 🗸	1000	2	0	disable	✓ disable	✓ active			
Dynamic MAC Aging	P0.6	forwarder 🗸	1000	2	0	disable	✓ disable	✓ active			
⊾Ring	P0.7	forwarder V	1000	2	0	disable	✓ disable	✓ active			
Redundancy	P0.8	forwarder v	1000	2	0	disable	✓ disable	✓ active	-		
▶Spanning Tree	4										+
►Loop Detection	Set Values Refres	h									

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:

SCALANCE XC	206-2SFP WEB	Mai × +				
$\leftrightarrow$ $\rightarrow$ C (	A Non	sicuro   192.168.0	.57			
SIEMENS	192.16	68.0.57/SC	CALANCE	XC206-2	2SFP	
Welcome admin	Log Table	•				
Logout						
<ul> <li>✓Information</li> <li>◆Start Page</li> <li>◆Versions</li> <li>►I&amp;M</li> <li>◆ARP Table</li> </ul>	Severity Fil Info Warning Critical	lters				
▶Log Table	Restart	System Up Time	System Time	Severity	Log Message	
Faults	8	04:10:25	Date/time not set	6 - Info	Device configuration changed.	
▶Redundancy	8	04:09:33	Date/time not set	4 - Warning	New Fault state: "Loop(s) detected."	
▶ Ethernet	8	04:09:33	Date/time not set	4 - Warning	Loop(s) detected.	
Statistics	8	04:09:33	Date/time not set	4 - Warning	P0.3 disabled by loop detection	
▶Unicast	8	04:09:33	Date/time not set	4 - Warning	Local Loop detected on P0.3	
▶Multicast	8	04:07:52	Date/time not set	6 Info	Link down on P0.4.	
▶LLDP	8	04:07:50	Date/time not set	6 - Info	Link up on P0.4	
▶FMP	8	04:07:46	Date/time not set	6 - Info	Link down on P0.5.	
▶Routing	9 entries.					
▶DHCP Server	Clear				<i>b</i> <sup>2</sup>	
▶Diagnostics ▶SNMP	Refresh					

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.