

Common Alarms and Events Supported by ONS 15305 and ONS 15302

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Alarms and Events](#)

[Related Information](#)

Introduction

This document explains the most common alarms that ONS 15305 supports. Many of these alarms are also applicable to ONS 15302, except for some differences in default severity for some of the alarms, because the products serve different roles in a network.

For an overview of the default alarm suppression list and persistency for each type of network element (NE), refer to the respective user guides.

Note: Ensure that you enable alarm reporting for modules and ports that are in use, because these parameters are disabled by default.

Note: Most alarm IDs with higher severity than “Warning”, which is an event, are on-off alarms (which are raised and cleared).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ONS 15305 and 15302

Components Used

The information in this document is based on the Cisco ONS 15305 and 15302.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

Alarms and Events

This table describes the alarms and events on Cisco ONS 15305 and 15302:

Reference Number	Object	Default Severity	Alarm Id (Prob Cause)	Description (Prob Cause Q)	Detailed Description	Troubleshooting (or) Comments
1	aiPort	Warning	alarmInp	Alarm condition on alarm-in port	The NEs provide four auxiliary alarm inputs (dry contact alarms) for associated equipment. For example, power module failure, battery condition, and open cabinet door. The operator can set the alarm to be triggered on either open or closed contact.	-
2	au4	Minor	ais	Alarm Indication Signal (AIS)	When an NE detects a defect in the regenerator section (RS) or the multiplexer section (MS) of an incoming link, the payload of that link is invalid. The NE then replaces the payload with an AIS in the forwarding direction. All subsequent NEs detect AU-4 AIS. Note: By	If AIS occurs for AU-4, verify alarm conditions on sections between intermediate nodes on the path.

					default, the alarm is suppressed.	
3	au4	Critical	lop	Loss Of Pointer	AU-4 Loss of Pointer (LOP) occurs when an NE is unable to interpret the AU-4 pointer. This alarm normally indicates that the NE receives concatenated AU-4s when the NE actually expects non-concatenated AU-4s.	Ensure that connected STM-n ports maintain the same structure on both ends.
4	au4	Major	epj	Excessive Ptr Justification	This alarm appears if the number of Pointer justification events (PJE) over a 15-minute period is greater than a threshold that you can configure, or the PJEL (Pointer Justification Event Limit). You can configure the PJEL individually for each AU-4 from 1 to 1024 events. The default configuration is 100 events per interval. PJE, both positive and negative justifications, are counted and measured over a 24-hour interval. Both	This alarm indicates synchronization problems in the network. The likely cause is that the devices operate with different sync-sources. For example, interconnected

						<p>devices that operate in "free running" mode cause this alarm per AU-4 object . The alarm clears when the number of received pointer events is lower than the set threshold within a full 15-minute interval.</p>
5	au 4	Warning	switch Work	SNCP switched to "working"	<p>This event occurs if the traffic switches from "protecting" to "working". Switching criteria depend on SNCP type. In other words, the criteria depend on</p>	-

					whether SNCP is SNC/i or SNC/n. The main difference between the two is that in addition to a switch on AIS/LOP alarms, SNC/n also switches on (non-intrusive) UNEQ/TIM/DEG/EXC alarms.	
6	au 4	Warning	switch Prot	SNCP switched to "protecting"	This event occurs if the traffic switches from "working" to "protecting". Switching criteria depend on SNCP type. In other words, switching depends on whether SNCP is SNC/i or SNC/n. The main difference between the two is that in addition to switch on AIS/LOP alarms, SNC/n also switches on (non-intrusive) UNEQ/TIM/DEG/EXC alarms.	-
7	au 4-4c	Minor	ais	Alarm Indication Signal	When an NE detects a defect in the regenerator section (RS) or the multiplexer section (MS) of an incoming link, the payload of that link is invalid. The NE	If AIS occurs for AU-4-4c, verify alarm conditions on section

					then replaces the payload with an AIS in the forwarding direction. All subsequent NEs detect AU-4-4c AIS. Note: By default, the alarm is suppressed.	ns between intermediate nodes on the path.
8	au 4-4c	Critical	lop	Loss Of Pointer	AU-4-4c Loss of Pointer (LOP) occurs when an NE is unable to interpret the AU-4-4c pointer. This normally indicates that the NE receives non-concatenated AU-4s when the NE expects concatenated AU-4-4cs.	Verify whether connected STM-n ports maintain the same structure on both ends.
9	au 4-4c	Major	epj	Excessive Ptr Justification	Excessive Pointer justification (EPJ) alarm appears if the number of Pointer justification events (PJE) over a 15-minute period is greater than a threshold that you can configure, or the PJEL (Pointer Justification Event Limit). You can configure the PJEL individually for each AU-4-4c	This alarm indicates synchronization problems in the network. The likely cause is that the devices operate with differ

					<p>ent sync-sources. For example, interconnected devices that operate in "free running" mode cause this alarm per AU-4-4c object. The alarm clears when the number of received pointer events is lower than the set threshold within a full 15-minute interval.</p> <p>Note:</p>
				<p>from 1 to 1024 events. 100 events per interval is the default configuration. PJE, both positive and negative justifications, are counted and measured over a 24-hour interval. Both current and past 24-hour interval counters are available.</p>	

						You can experience this alarm after an NE restart. If the network maintains synchronization, this alarm clears in less than 30 minutes.
10	au-4c	Warning	switch Work	SNCP switched to working	This event occurs if the traffic switches from "protecting" to "working". Switching criteria depend on the SNCP type. In other words, switching depends on whether SNCP is SNC/i or SNC/n. The main difference between the two is that in addition to switch on AIS/LOP alarms, SNC/n also switches on (non-	-

					intrusive) UNEQ/TIM/DE G/EXC alarms.	
11	au 4- 4c	War ning	switch Prot	SNCP switch ed to protect ing	This event occurs if the traffic switches from “working” to “protecting”. Switching criteria depend on the SNCP type. In other words, switching depends on whether SNCP is SNC/i or SNC/n. The main difference between the two is that in addition to switch on AIS/LOP alarms, SNC/n also switches on (non- intrusive) UNEQ/TIM/DE G/EXC alarms.	-
12	au xlf	Maj or	lofTx	Loss Of Frame	This alarm appears when an unsupported signal type arrives.	-
13	au xlf	Maj or	los	Loss Of Signal	This alarm appears when the AUX interface has no signal.	-
14	de vic e	Criti cal	ufail	Device main unit failure	This alarm appears if you encounter problems when you try to load FPGA, SPI/Eeprom, Power input, DXC inlet or XBAR on Main card.	Restar t or reboo t the devic e. If the alarm persis ts, replac e the

						device (because the error can be on the main-board).
15	device	Major	temp	High temperature alarm	This alarm appears if the temperature exceeds 450. For ONS 15305, both pair of Fans spin.	Ensure that the combination of equipped modules in the chassis maintains the limit for maximum power consumption. Verify whether the environment that surrounds the device maintains proper ventilation.

16	device	Major	t0Hold Over	T0 in holdover mode	This alarm appears if none of the T0 synchronization candidates is available.	-
17	device	Critical	t0Defect	T0 SETG defect	This alarm appears for defective hardware that impacts the internal T0 clock.	Replace the chassis (because this error is on the main-board).
18	device	Warning	t0Sync Switch	T0 sync switch over	This event occurs when automatic, manual or forced switchover occurs.	-
19	device	Warning	t0QIFailed	T0 sync candidate in fail	This alarm applies to T1/T2/T3 sources member of the T0 synchronization table.	-
20	device	Warning	t0QIDnu	T0 sync candidate rec. DNU	This alarm appears when T0 synchronization candidate receives the "DoNotUse" message.	-
21	device	Critical	t4Squelch	T4 output squelched	This alarm appears when no T4 synchronization candidate has QL equal to or above QL_{min}	-
22	device	Critical	inletFail	DXC inlet	When you power cycle	Restart or

	e			failure	(turn the power on or off at different temperatures) a device, the main card can fail to recover operations after the power on or off, and can remain in an alarm state. In such a state, the device does not carry traffic, and the card reports the "DXC inlet failure alarm."	reboot the device. If the alarm persists, replace the device.
23	device	Critical	inletBit Error	DXC inlet bit error	The DXC inlet bit error alarm appears on the device level to indicate a failure between the two DXC devices on the main-board. The system detects no failures in nominal conditions.	-
24	device	Warning	unknownFlashType	Unknown FLASH-device detected	This alarm appears when the Flash-process discovers an unknown flash type on the main-board.	Restart or reboot the device. If the alarm persists, replace the device.
25	device	Warning	errorNewBank	ERROR in newest bank	This error indicates that the main-board does not start up with the latest	Download the firmware again.

					downloaded firmware.	
26	device	Warning	alarmStormStart	Alarm storm start detected	This alarm indicates number of alarm status changes is too high for the device to report all alarms as traps.	-
27	device	Warning	alarmStormEnd	Alarm storm end detected	This alarm appears when the number of alarm status changes reduces to a level where all alarms show up as traps again.	In a situation where alarm Storm Start appears, the current alarm-list can be wrong before alarm Storm End appears. The list can show alarms that are no longer present, and there can be active alarm

						s that are not in the list. Also, for some alarms, the time-stamp can be wrong. In this situation, the alarm history can also be wrong. Some alarm conditions could have been present and disappeared again, and probably did not appear in the alarm-lists. Also the
--	--	--	--	--	--	---

						time-stamps can be wrong on some alarms or events. After alarm Storm End goes out, the system updates the current-alarm-list, and every alarm from that point in time appears in the alarm-history.
28	device	Warning	rxOverflow HWFault	RX buffer overflow	This alarm indicates an overflow of the receive buffers on the LAN interface.	-
29	device	Warning	txOverflow HWFault	Interport queue overflow	This alarm indicates an interport queue overflow on the LAN interface.	-

30	device	Warning	routeTableOverflow	Routing table overflow	This event occurs when the routing table exceeds 2048 entries.	-
31	device	Warning	endTftp	TFTP session completed	This event occurs on successful completion of a TFTP session.	-
32	device	Warning	abortTftp	TFTP session aborted	This event occurs when the completion of a TFTP session is unsuccessful.	Check TFTP server settings, and retry the transfer.
33	device	Warning	startTftp	TFTP session initiated	This event occurs when a download operation starts from the manager towards the NE. For example, a software upgrade or configuration file restore operation.	-
34	device	Warning	forwardingTableOverflow	Layer II Forward Table overflow	This event indicates that the Unicast Global Forwarding table has reached the maximum limit on the number of MAC addresses. No new addresses are learned until old ones are removed (which can happen	You can configure the Unicast-Global-Forwarding table in the range 20-

					through aging, or when a link goes down, or when the operator removes them).	32767. 8192 entries is the default parameter.
35	device	Warning	vlanDynamicPortAdded	Dynamic VLAN port added	This event shows that the GVRP protocol dynamically adds a port to a VLAN.	-
36	device	Warning	vlanDynamicPortRemoved	Dynamic VLAN port removed	This event shows that the GVRP protocol dynamically removes a port from a VLAN.	-
37	device	Warning	rsPingCompletion	Ping sequence completed	This event signifies the completion of a sequence of ICMP echos (Pings) initiated from the device.	-
38	device	Warning	rllgmpTableOverflow	IGMP table overflow	This alarm indicates that the maximum allowed entries in the IGMP table has been reached.	-
39	device	Warning	rllpFftStnOverflow	IP SFFT overflow	This alarm shows that the table that holds an individual IP address to forward data is full.	-
40	e1Port	Major	lofRx	Loss Of Frame downlink	This alarm appears on E1 in PRA mode, when E1 receives the signal from the network in a	-

					format that E1 does not expect.	
41	e1 Port	Major	lofTx	Loss Of Frame uplink	This alarm appears on E1 in PRA mode, when E1 receives the signal on the PDH port in a format that E1 does not expect.	-
42	e1 Port	Minor	aisRx	AIS received downlink	This alarm appears on E1 in PRA mode, when the network sends a signal with AIS to E1. This event indicates an alarm elsewhere in the network.	-
43	e1 Port	Critical	los	Loss Of Signal	This alarm appears when the E1 port does not receive a PDH signal.	-
44	e1 Port	Warning	loopClosed	Loop closed	This event occurs when you set a test-loop on an E1-port.	-
45	e1 Port	Warning	loopOpened	Loop opened	This event occurs when a test-loop clears on an E1-port.	-
46	e3 T3 Port	Minor	aisRx	AIS received downlink	Not supported.	-
47	e3 T3 Port	Critical	los	Loss Of Signal	This alarm appears when the E3 port does not receive a PDH signal.	-
48	e3	War	loopCl	Loop	This event	-

	T3 Port	Warning	Used	closed	occurs when you set a test-loop on an E3-port.	
49	e3 T3 Port	Warning	loopOpened	loop opened	This event occurs when a test-loop clears on an E3-port.	-
50	eth	Warning	rldot1d StpPort StateForwarding	Bridge port learning to forwarding state transition	This message means that the STP port state for the given port has moved from Learning state to Forwarding state. The port now forwards traffic.	This message indicates a topology change.
51	eth	Warning	rldot1d StpPort StateNotForwarding	Bridge port forwarding to blocking state transition	This message means that the STP port state for the given port has moved from the Forwarding state to the Blocking state. The port no longer forwards traffic.	This message indicates a topology change.
52	fan	Major	fan	Fan failure	This alarm appears on the main-card when temperature rises above 850C. The alarm is specific for each fan. The main-card processes and presents this alarm as "Fan Failure Alarm".	The fan becomes active for a specified time (24 hours) when only two fans run. After the fans are

						active for the specified time, they stop, and the other fans become active. An alarm appears if a fan fails, and the other fans run continuously. You must replace the fan module now in order to protect the remaining fans, which no longer have protection.
53	fan	Critical	diagFail	Diagnostic	This alarm implies incorrect	Replace the

				failure	module identification.	module.
54	fan	Major	inventoryFail	Inventory failure	This alarm indicates that inventory retrieved from the fan module does not match with expected inventory.	Replace the module, even though the module can still be operational.
55	gfp	Minor	plm	GFP payload mismatch	This alarm appears due to a mismatch between expected and received PTI value in the GFP PTI field. Refer to ITU-T G.7041 for details.	Check the configuration at both ends of the path.
56	gfp	Minor	upm	GFP user payload type mismatch	This alarm appears when the received User Payload Identifier (UPI) is different from the expected UPI. This release supports the Frame-Mapped Ethernet UPI. Refer to alarm based on detection of UPI field value in ITU-T G.7041.	Check the configuration at both ends of the path.
57	gfp	Minor	lfd	GFP loss of frame delin.	This alarm appears when the delineation process is not in SYNC state.	-
58	gfp	Minor	exm	GFP ex-header ident.	This alarm appears when the received Extension	The opposite side

				mismatch	Header Identifier (EXI) is different from the expected EXI. This release supports the Null Extension Header EXI. Refer to alarm based on detection of EXI field value in ITU-T G.7041.	port sends unsupported EXI.
59	gfp	Minor	pfm	GFP payload FCS ident. mismatch	This alarm appears when the received Payload FCS Indication (PFI) is different from the expected PFI. Refer to alarm based on detection of PFI field value in ITU-T G.7041.	-
60	lanx	Warning	lanOn	Link Up	This event occurs as you try to connect the Ethernet LAN-port.	-
61	lanx	Warning	lanOff	Link Down	This event occurs as you try to disconnect the Ethernet LAN-port.	-
62	lca	Warning	acMstTimeout	Ack Mst Timeout	This event indicates a Member Status Signal (MST) timeout. When you add a VC-n to the upstream capacity, MST=OK for this VC-n is expected to be received from the opposite end. If the source does not receive an	Check the configuration and cross-connections.

					MST=OK within a reasonable amount of time, the source declares a timeout.	
63	lca s	War ning	rsAckT imeout	RS ACK Timeo ut	This event indicates that an RS-sequence Acknowledge has timed out. When an LCAS source re-sequences the VC-n channels, the LCAS source expects the opposite end to acknowledge this operation through an RS-ACK. If the source does not receive an RS-ACK within a reasonable amount of time, the source declares a timeout.	Look for other alarm s in both ends.
64	lca s	Min or	eosMul tiple	Two or more chan. have EoS	This event occurs when two or more received channels have End of Sequence (EoS). One and only one channel must have EOS. See sqnc alarm.	Look for other alarm s at both ends.
65	lca s	Min or	eosMis sing	No chann el has EoS	None of the received channels has End of Sequence (EoS). One and only one channel must have EOS. See	Look for other alarm s at both ends.

					sqnc alarm.	
66	lca s	Min or	sqNon Cont	Missin g SQ detect ed	This alarm appears when a sequence number is missing. See sqnc alarm.	Chec k for config uratio n mism atch or other alarm s.
67	lca s	Min or	sqMulti ple	Equal SQ for two or more chan	This message appears when two or more channels have the same sequence number. See sqnc alarm.	Chec k for config uratio n mism atch or other alarm s.
68	lca s	Maj or	sqOor	SQ outsid e of range	This alarm occurs when the received sequence number is outside of the valid range (VC-4: 0-6, VC-3: 0-20, VC-12: 0-62). See sqnc alarm.	Chec k for config uratio n mism atch or other alarm s.
69	lca s	Maj or	sqnc	seque nce nbr not consis tent	This alarm appears when one or more of these alarms occur: eosMultiple, eosMissing, sqNonCont, sqOor and sqMultiple.	Chan nels must have uniqu e seque nce numb ers. Chec k the receiv ed seque nce numb ers.

						This alarm can indicate a signaling problem at the opposite port, or cross-connect problems.
70	lca s	Maj or	gidErr	GID differe nt for active chan	This alarm appears when active channels within the same VCGroup receive different Group ID.	Chec k the config uratio n.
71	lca s	Maj or	ctrlOor	CTRL word undefi ned	This alarm indicates the receipt of an illegal or undefined CTRL word value.	Chec k the config uratio n at both ends.
72	lca s	Maj or	lcasCr c	CRC error detect ed	This alarm appears when the Cyclic Redundancy Check (CRC) fails.	Chec k the config uratio n at the other end, and look for other alarm s.
73	lca s	Min or	nonLca s	Non- LCAS source detect ed	This alarm implies that the NE at the other end is not in LCAS mode.	Chec k the config uratio n.

74	lca s	Maj or	plcr	Partial loss capaci ty rx	This alarm appears when the received capacity is less than expected.	Chec k the opera tional- capac ity, VC-n alarm s, and config uratio n para meter s on the oppos ite port.
75	lca s	Criti cal	tlcr	Total loss capaci ty rx	This message indicates that the port receives no traffic.	Chec k for VC-n alarm s and config uratio n para meter s on the oppos ite port.
76	lca s	maj or	plct	Partial loss capaci ty tx	This alarm appears when the send capacity is less than expected.	Chec k the opera tional capac ity. Chec k for config uratio n para meter s on this side, and also

						check the cross-connect status, and alarm status on the opposite port.
77	links	Critical	link	Total loss capacity	This message indicates that no traffic is sent.	Check for configuration parameters on this side, and also check the cross-connect status, and alarm status on the opposite port.
78	module	Critical	modFail	Module failure	This alarm indicates a module failure (power loss on the module).	Restart the module. If the problem persists, replace the module.

						e.
79	module	Critical	diagFail	Diagnostic failure	This alarm appears when you encounter problems when you try to load FPGA, SPI/Eeprom, Power input, DXC inlet or Ethernet switch on service modules.	Restart the module. If the problem persists, replace the module.
80	module	Major	inventoryFail	Inventory failure	Inventory failure occurs when module identification is not correct.	Replace the module.
81	module	Critical	inletFail	DXC inlet failure	When you power cycle (power on/off at different temperatures) a service module, the card can fail to recover operation after the power on/off, and can remain in an alarm state. In such a state the card does not carry traffic. When the card indicates the "DXC inlet failure alarm", the LED of the card is also red. The card recovers normal operation after software reset. This issue occurs in approximately one out of every 20 power cycles.	Restart the module. If the problem persists, replace the module.
82	mo	Criti	inletBit	DXC	Cards with EoS	-

					<p>mappers can experience packet losses. For example, LAN traffic mapped to EoS ports on 8xSTM1+map module, and "DXC inlet bit error alarm" conditions can occur when you expose 8xSTM1+map cards to extreme temperature cycles (-5 to 50C with 2 hours dwell at each extreme temperature, and 1C/min gradients). The packet losses and condition can occur on the 8xSTM1+map card. This only occurs under temperature stress. The frequency with which the issue occurs is an average of 10 packets lost, and less than 100 alarms recorded in a 12 hours cycle. Nominal conditions record no failures.</p>	
83	module	Critical	cardisolated	Card isolated	<p>The 'card isolated' error can occur in these conditions:</p> <ol style="list-style-type: none"> 1. A card 	When a module ends up in

					<p>anomaly occurs while the module is in-service: Module removed (extracted from the chassis). Module failed (power loss on the module). Dxc inlet failure (interface between main-card and the module).</p> <p>Note: If a) or b) or c) occurs on pure SDH/PDH modules, an alarm appears. Card_removed (A) Card_anomaly (B/C) If a) occurs on modules with switch (8xstm1_map/8xfe/2xge/4xfe_map/8xmap) an alarm (card_removed) appears, BUT, in</p>	<p>an "ISOLATED" alarm - state, not caused by physical handling, you must replace the module.</p>
--	--	--	--	--	---	---

					<p>addition the complete device restarts, due to recovery/clean-up handling of the crossbar or switch system. When the device is up again, the card_removed alarm is still present. If b) or c) occurs on modules with switch (8xstm1/8xfe/2xge/4xfe_map/8xmap) an alarm (card_anomaly) appears BUT in addition, the complete device restarts, due to recovery/clean-up handling of the crossbar or switch system.</p>	
--	--	--	--	--	--	--

					<p>When the device is up again, the failed module is marked "ISOLATED".</p> <p>2. On a module (with switch - 8xstm1/8xe/2xge/4xe_map/8xmap) the hot-removal process fails when you shut down the module. Again the system restarts, due to recovery/clean-up handling of the crossbar or switch system. When the device is up again, the failed module is marked "ISOLATED".</p>	
84	module	Critical	cardAnomaly	Card anomaly	See card Isolated.	-
85	module	Critical	hotSwapFailu	Hot swap	This alarm indicates that	Restart the

	e	re	failure	the module cannot be reported to the processor, and Ethernet services will not become operational for the module.	module. If the problem persists, try to insert the module in another slot. If the problem still persists, replace the module. If the module does not fail in different slots, check for issues on the main board (XBAR). Note: In addition, you can experience this condition.
--	---	----	---------	---	--

						ion for 1.x level of software for ONS15305. For more information, refer to the known issues in latest software release note for the respective units.
86	module	Warning	modOos	Module Out Of Service	This event occurs when the module enters the OOS state.	-
87	module	Warning	modOosMaint	Module OOS by maintenance	This event occurs when the module enters the OOS by maintenance state.	-
88	module	Warning	modIns	Module IN Service	This event occurs when the module enters the in-service state.	-
89	module	Warning	unknownFlashType	Unknown FLASH-	This alarm appears when the Flash-process	Restart or reboot the

				device detected	discovers an unknown flash type on the module.	module. If the alarm persists, replace the module.
90	module	Warning	errorNewBank	ERROR in newest bank	This error appears when the module does not start up with the latest downloaded firmware.	Retry download.
91	module	Warning	module Shutdown	Module shutdown	This event occurs when the module enters the Shutdown state.	-
92	module	Warning	module Restart	Module restart	This event occurs when the module enters the Restart state.	-
93	module	Warning	modUnEq	Module Unequipped	This event occurs when the module or slot enters the Unequipped state.	-
94	ms t	Major	exc	BER excessive error rate	This alarm appears if the Bit Error Rate is greater than 1E-5.	Investigate whether there are bit errors for RS sections on the path. For example, a radio

						hop.
95	ms t	Min or	deg	Signal degra de (BER low)	This alarm appears when the Bit Error Rate is greater than the configured threshold. You can configure the threshold for this alarm from 1E-6 to 1E-9. For example, if set to 1E-7 (default), an alarm appears when BER exceeds this threshold. The detection time depends on the threshold. (1E-6 has a short detection-time, 1E-9 has longer detection time).	Investigate whether there are bit errors reported for RS sections on the path. For example, a radio hop. To clear this alarm, improve the BER level by a factor 10.
96	ms t	Min or	csf	Dcc Termin ation Failure	This alarm can occur for a DCC-m (D4-D12) connection, which is active but does not properly terminate at the other end.	Verify whether both ends of the link obtain equal DCC settings.
97	ms t	Min or	ais	Alarm Indicat ion Signal	MS-AIS is the alarm indication signal for the multiplexer section (MS). STM-n ports that are not	If AIS appears in MS, verify alarm condit

					configured often transmit MS-AIS, and a regenerator with no input signal transmits MS-AIS.	ions on regenerator sections on the path, for example, a radio hop. Verify the configuration on the opposite port also.
98	ms t	Min or	rdi	Remote Defect Indication	If an RS alarm (LOS, LOF, TIM, AIS) or MS-AIS appears on an STM-n port, MS-RDI goes out on that port.	Verify alarm conditions on regenerator sections on the path, for example, a radio hop. Also check the configuration on the opposite port.
99	ms t	Critical	mstp	MSP signalling	This problem typically occurs if you have a	Check the MSP

				problem	mismatch in configuration. In other words, this occurs when your configuration is unidirectional on one end and bidirectional on the other end.	configuration.
100	ms t	Warning	switch ToProt	MSP switched to protecting	This event occurs if the traffic switches from "working" to "protecting".	-
101	ms t	Warning	switch ToWork	MSP switched to working	This event occurs if the traffic switches from "protecting" to "working".	-
102	ms t	Warning	mspComTimeOut	MSP command timed out, removed	This event indicates the timeout of an MSP-command that you successfully enter at this end. The timeout occurs due to a "no" from the other end. This alarm only appears when you use bidirectional MSP.	This event does not indicate any malfunction, and can occur as a consequence of the MSP-protocol in different combinations of alarm-state or MSP-commands.
103	ms	War	mspCo	MSP	This event	-

	t	ning	mOver ruled	comm and overrul ed, remov ed	indicates that a user has entered an MSP-command with a higher priority at the other end of the connection. The result is that the MSP-command at this end is removed. This alarm only appears when you use bidirectional MSP.	
104	po we r	Criti cal	pwrInA	Power failure input A	This means power input A is absent.	Chec k power cable or suppl y.
105	po we r	Criti cal	pwrInB	Power failure input B	This means power input B is absent.	Chec k power cable or suppl y.
106	po we r	Criti cal	pwrOut	Power output failure	This indicates that 48VDC / 230VAC power module does not provide internal power (5V).	Repla ce the modul e.
107	po we r	Criti cal	pwrFail	Power modul e out	This alarm appears if the power module is administratively enabled and removed.	-
108	po we r	Criti cal	diagFai l	Diagn ostic failure	This failure occurs due to incorrect module identification.	Repla ce the modul e.
109	po we	Maj or	invento ryFail	Invent ory	This event occurs if the	This condit

	r			failure	correct HW-inventory cannot be retrieved from the power-module.	ion most likely requires a replacement of the module, but can still be operational. If this alarm appears for a slot, independent of module inserted, the alarm indicates problem of the chassis. In this case, replace the device.
110	power	Critical	pwrUIL	230VAC power input low	This alarm appears when an AC module receives less than 195VAC from the 230VAC outlet.	The module disconnects the output voltage

						<p>e and activates an alarm if the output voltage is outside the specified tolerance (Higher than 6V or less than 5V). The module also limits the maximum output current to 11A.</p>
111	power	Critical	pwrUIH	230VAC power input high	<p>This alarm appears when an AC module receives more than 255VAC from the 230VAC outlet.</p>	<p>The module disconnects the output voltage and activates an alarm if the output voltage is outside</p>

						e the specified tolerance (Higher than 6V or less than 5V). The module also limits the maximum output current to 11A.
112	rst	Critical	lof	Loss Of Frame	The loss of frame (LOF) alarm appears when the frame sync is not recognizable, and the out of frame (OOF) alarm persists for 3ms.	Set OOF.
113	rst	Major	exc	BER excessive error rate	This alarm appears if the Bit Error Rate is greater than 1E-5.	Investigate whether there are bit errors reported for other sections in the network between

						intermediate nodes.
114	rst	Minor	degraded	Signal degrade (BER low)	This alarm appears when the Bit Error Rate is greater than the configured threshold. You can configure the threshold for this alarm from 1E-6 to 1E-9. For example, if set to 1E-7 (default), an alarm appears when BER exceeds this threshold. The detection time depends on the threshold. (1E-6 has a short detection-time, 1E-9 has longer detection time).	To clear this alarm, improve the BER level by a factor 10.
115	rst	Critical	timing	Trace Identifier Mismatch	Trace Identifier Mismatch occurs when you have enabled path trace and the "received string" is different from the "expected string". This alarm condition stops traffic.	Verify the configured string at both ends of the physical connection. You do not need to set the Path Trace Identifier

						ier attrib utes, but you can use the tool to check the conne ctivity of compl ex netwo rks. Basic ally, a Path Trace Identif ier is insert ed at the start of a path and extrac ted at the end of a path. When you set Path Trace Trans mitted to a logica l value, (such as, "BON N-3- 21")
--	--	--	--	--	--	--

						you can check whether the other side of the network receives this value. If you enter a value for the Path Trace Expected and enable Path Trace, a TIM alarm appears if the received value is different from the transmitted value.
116	rst	Minor	csf	Dcc Termination Failure	This alarm appears for a DCC-r (D1-D3) connection, which is active but does not properly	Verify whether both ends of the link

					terminate at the other end.	obtain equal DCC settings.
117	rst	Critical	oof	Out Of Frame	The out of frame (OOF) alarm appears when the frame sync is not recognizable. OOF condition results in a loss of frame (LOF) alarm, if persistent in 3ms.	Check whether the framing format configured on the port matches the framing format on the line. Try the other framing format and see if the alarm clears. Open the statistics report (RS) for the port and look for evidence of a bad

						line. Bit errors can indicate a timing problem. If you find evidence of a bad line, isolate the problem. For this, physically loop the ports with a cable at each end of the connection.
118	sdhPort	Critical	los	Loss Of Signal	-	-
119	sdhPort	Minor	orxo	Optical Receiver Overload	This alarm appears on STM-4 and STM-16 when the received signal is too strong (optical Rx-level too high). The maximum allowed level depends on module type and type of optical receiver.	Reduce optical Rx-level to make sure that the traffic remains unaffected.

120	sfp	Warning	sfpRemoved	SFP removed from module	This event indicates that an SFP has been removed at a port.	-
121	sfp	Warning	sfpInserted	SFP inserted in module	This event indicates that an SFP has been inserted at a port.	-
122	slot	Critical	modMismatch	Module mismatch	This alarm appears if the module type that you configure is different from the module you insert.	The alarm clears if you replace the module, or change the expected module (to create a match between expected and installed).
123	slot	Critical	modOut	Module removed	This alarm appears if the module is in the in-service state and is extracted from the slot.	Issue a module shutdown process before you pull out the module.
124	tu12	Minor	ais	Alarm Indicat	When an NE detects a defect	If AIS appe

				ion Signal	on the TU-12 level or any level above TU-12, the TU-12 payload is invalid. The NE then replaces the payload with an AIS in the forwarding direction. All subsequent NEs detect TU-AIS. Note: This alarm is suppressed by default.	ars for an TU- 12, verify alarm condit ions on sectio ns betwe en inter media te nodes on the path.
125	tu1 2	Criti cal	lop	Loss Of Pointe r	This alarm appears when an NE is unable to interpret the TU-12 pointer. This alarm normally indicates that the NE receives TU-3s when the NE actually expects TU-12s.	Verify wheth er conne cted STM- n ports maint ain the same struct ure at both ends.
126	tu1 2	War ning	switch Work	SNCP switch ed to workin g	This event occurs if the traffic switches from "protecting" to "working". Switching criteria include the SNCP type, namely, SNC/i or SNC/n. The main difference between the two is that SNC/n, in addition to a switch on	-

					AIS/LOP alarms, also switches on (non-intrusive) UNEQ/TIM/DEG/EXC alarms.	
127	tu1 2	Warning	switch Prot	SNCP switch ed to protect ing	This event occurs if the traffic switches from “working” to “protecting”. Switching criteria include the SNCP type, namely, SNC/i or SNC/n. The main difference between the two is that SNC/n, in addition to a switch on AIS/LOP alarms, also switches on (non-intrusive) UNEQ/TIM/DEG/EXC alarms.	-
128	tu3	Minor	ais	Alarm Indicat ion Signal	When an NE detects a defect on the TU-3 level or any level above TU-3, the TU-3 payload is invalid. The NE then replaces the payload with an AIS in the forwarding direction. All subsequent NEs detect TU-AIS. Note: This alarm is suppressed by default.	If AIS appears for an TU-3, verify alarm conditions on sections between intermediate nodes on the path.
129	tu3	Critical	lop	Loss Of Pointe r	This alarm appears when an NE is unable to interpret the	Verify whether conne

					TU-3 pointer. This alarm normally indicates that the NE receives TU-12s when the NE actually expects TU-3s.	cted STM-n ports maintain the same structure at both ends.
130	tu3	Warning	switch Work	SNCP switched to working	This event occurs if the traffic switches from "protecting" to "working". Switching criteria include the SNCP type, namely, SNC/i or SNC/n. The main difference between the two is that SNC/n, in addition to a switch on AIS/LOP alarms, also switches on (non-intrusive) UNEQ/TIM/DEG/EXC alarms.	-
131	tu3	Warning	switch Prot	SNCP switched to protecting	This event occurs if the traffic switches from "working" to "protecting". Switching criteria include the SNCP type, namely, SNC/i or SNC/n. The main difference between the two is that SNC/n, in addition to a switch on AIS/LOP alarms, also switches on	-

					(non-intrusive) UNEQ/TIM/DE G/EXC alarms.	
132	vc 12	Maj or	exc	BER exces sive error rate	This alarm appears if the Bit Error Rate is greater than 1E- 5.	Invest igate wheth er bit errors occur for other sectio ns in the netwo rk betwe en inter media te nodes .
133	vc 12	Min or	deg	Signal degra de (BER low)	This alarm appears when the Bit Error Rate is greater than configured threshold. You can configure the threshold for this alarm from 1E-6 to 1E-9. For example, if set to 1E-7 (default), an alarm appears when BER exceeds this threshold. The detection time depends on the threshold. (1E-6 has a short detection-time, 1E-9 has longer detection time).	To clear this alarm , impro ve the BER level by a factor 10. Invest igate wheth er bit errors occur for other sectio ns in the netwo rk betwe en inter media

						te nodes .
134	vc 12	Critical	tim	Trace Identifier Mismatch	<p>This alarm appears when path trace is enabled and the “received string” is different from the “expected string”. This alarm condition stops traffic because AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received Path Trace.</p> <p>Note: For an Ethernet over SDH (EoS) port mapper, Path trace is a global setting for each Group, though you can read the received string for each individual VC.</p>	<p>Verify the configured string at both ends of the VC-12 terminations. You do not have to set the Path Trace Identifier attributes, but you can use the tool to check the connectivity of complex networks. Basically, a Path Trace Identifier is inserted at the</p>

						start of a path and extracted at the end of a path. When you set Path Trace Transmitted to a logical value, (such as, "BON N-3-21") you can easily check whether the other side of the network receives this value. If you enter a value for the Path Trace Expected value and
--	--	--	--	--	--	--

						enable Path Trace, a TIM alarm is triggered if the received value is different from the transmitted value.
135	vc 12	Minor	rdi	Remote Defect Indication	This alarm indicates the presence of an incoming alarm at the point where the VC-12 terminates at the other end. The alarm can be UNEQ, TIM, or SSF.	-
136	vc 12	Minor	ssf	Server Signal Failure	This alarm indicates that an alarm in the device affects the traffic on this VC-12 termination point. For example, a LOS alarm on an STM-n port at the other end of a cross-connect.	-
137	vc 12	Critical	uneq	Unequipped	This alarm means that the VC-12 has no payload. This alarm normally	-

					indicates loss of connectivity for the configured payload. For example, if you enable a 2Mbit (E1) but do not cross-connect the VC, this alarm appears.	
138	vc 12	Critical	plm	Payload Mismatch	The signal label indicates what type of payload the VC-12 carries. The payload label mismatch (PLM) occurs if there is detected a mismatch between an expected and received signal label.	Check the configuration at other end and verify the cross-connections.
139	vc 12 Nim	Major	exc	BER excessive error rate	This alarm appears if the Bit Error Rate is greater than 1E-5 for a KLM-value that is structured as TU-12 and has a non-intrusive monitor active.	Investigate whether bit errors occur for other sections in the network between intermediate nodes.
140	vc 12 Nim	Minor	deg	Signal degrade (BER low)	This alarm appears when the Bit Error Rate is greater than the configured threshold for a KLM-value that	To clear this alarm, improve the BER

					<p>is structured as TU-12 and has a non-intrusive monitor active. You can configure the threshold for this alarm from 1E-6 to 1E-9. For example, if set to 1E-7 (default), an alarm appears when BER exceeds this threshold. The detection time depends on the threshold. (1E-6 has a short detection-time, 1E-9 has longer detection time).</p>	<p>level by a factor 10. Investigate whether bit errors occur for other sections in the network between intermediate nodes.</p>
141	vc 12 Nim	Critical	tim	Trace Identifier Mismatch	<p>This alarm appears when path trace is enabled and the "received string" is different from the "expected string" for a KLM-value that is structured as TU-12 and has a non-intrusive monitor active. This alarm condition does not affect traffic. Note: For an EoS mapper (Ethernet over SDH port), Path trace is a global setting per Group, though you can read the received string for each individual VC.</p>	<p>Verify the configured string in both ends of the VC-12 terminations. You do not have to set the Path Trace Identifier attributes, but you can</p>

						use the tool to check the connectivity of complex networks. Basically, a Path Trace Identifier is inserted at the start of a path and extracted at the end of a path. When you set Path Trace Transmitted to a logical value, (such as, "BONN-3-21") you can easily check whether the
--	--	--	--	--	--	---

						other side of the network receives this value. If you enter a value for the Path Trace Expected value and enable Path Trace, a TIM alarm is triggered if the received value is different from the transmitted value.
142	vc 12 Nim	Critical	uneq	Unequipped	This alarm indicates that an STM-n port does not contain a VC-12 for a KLM-value that is structured as TU-12 and has a non-intrusive	-

					monitor active.	
143	vc 3	Maj or	exc	BER exces sive error rate	This alarm is reported if the Bit Error Rate is greater than 1E-5.	Investigate whether bit errors occur for other sections in the network between intermediate nodes.
144	vc 3	Min or	deg	Signal degra de (BER low)	This alarm appears when the Bit Error Rate is greater than the configured threshold. You can configure the threshold for this alarm from 1E-6 to 1E-9. For example, if set to 1E-7 (default), an alarm appears when BER exceeds this threshold. The detection time depends on the threshold. (1E-6 has a short detection-time, 1E-9 has longer detection time).	To clear this alarm, improve the BER level by a factor 10. Investigate whether bit errors occur for other sections in the network between intermediate nodes.

						.
145	vc 3	Critical	tim	Trace Identifier Mismatch	<p>This alarm appears when path trace is enabled and the "received string" is different from the "expected string". This alarm condition stops traffic because AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received Path Trace.</p> <p>Note: For an EoS mapper (Ethernet over SDH port), Path trace is a global setting for each Group, though you can read the received string for each individual VC.</p>	<p>Verify the configured string in both ends of the VC-3 terminations. You do not have to set the Path Trace Identifier attributes, but you can use the tool to check the connectivity of complex networks. Basically, a Path Trace Identifier is inserted at the start of a path</p>

						and extracted at the end of a path. When you set Path Trace Transmitted to a logical value, (such as "BONN-3-21") you can easily check whether the other side of the network receives this value. If you enter a value for the Path Trace Expected value and enable Path
--	--	--	--	--	--	--

						Trace , a TIM alarm is triggered if the received value is different from the transmitted value.
146	vc 3	Minor	rdi	Remote Defect Indication	This alarm indicates the presence of an incoming alarm at the point where the VC-3 terminates at the other end. The alarm can be UNEQ, TIM, or SSF.	-
147	vc 3	Minor	ssf	Server Signal Failure	This alarm indicates that an alarm in the device affects the traffic on this VC-3 termination point. For example, a LOS-alarm on an STM-n port at the other end of a cross-connect.	-
148	vc 3	Critical	uneq	Unequipped	This alarm indicates loss of connectivity for the configured payload. For example, if you enable a 34Mbit (E3) but do not	-

					cross-connect the VC, this alarm occurs.	
149	vc 3	Critical	plm	Payload Mismatch	The payload label mismatch (PLM) occurs if a mismatch is detected between expected and received signal label.	-
150	vc 3Nim	Major	exc	BER excessive error rate	This alarm appears if the Bit Error Rate is greater than 1E-5 for a K-value that is structured as TU-3 and has a non-intrusive monitor active.	Investigate whether bit errors occur for other sections in the network between intermediate nodes.
151	vc 3Nim	Minor	deg	Signal degrade (BER low)	This alarm appears when the Bit Error Rate is greater than configured threshold for a K-value that is structured as TU-3 and has a non-intrusive monitor active. You can configure the threshold for this alarm from 1E-6 to 1E-9. For example, if set to 1E-7 (default), an alarm is raised	To clear this alarm, improve the BER level by a factor 10. Investigate whether bit errors occur for other

					when BER exceeds this threshold. The detection time depends on the threshold. (1E-6 has a short detection-time, 1E-9 has longer detection time).	sections in the network between intermediate nodes.
152	vc3Nim	Critical	tim	Trace Identifier Mismatch	<p>This alarm appears when path trace is enabled and the "received string" is different from the "expected string" for a K-value that is structured as TU-3 and has a non-intrusive monitor active. This alarm condition does not affect traffic.</p> <p>Note: For an EoS mapper (Ethernet over SDH port), Path trace is a global setting per Group, though you can read the received string for each individual VC.</p>	Verify the configured string in both ends of the VC-3 terminations. You do not have to set the Path Trace Identifier attributes, but you can use the tool to check the connectivity of complex networks. Basic

						ally, a Path Trace Identifier is inserted at the start of a path and extracted at the end of a path. When you set Path Trace Transmitted to a logical value, (for example, "BONN-3-21") you can easily check whether the other side of the network receives this value. If you enter a
--	--	--	--	--	--	--

						value for the Path Trace Expected value and enable Path Trace , a TIM alarm is triggered if the received value is different from the transmitted value.
153	vc3Nim	Critical	uneq	Unequipped	This alarm indicates that an STM-n port does not contain a VC-3 for a K-value that is structured as TU-3 and has a non-intrusive monitor active.	-
154	vc4	Major	exc	BER excessive error rate	This alarm appears if the Bit Error Rate is greater than 1E-5.	Investigate whether bit errors occur for other sections in

						the network between intermediate nodes.
155	vc 4	Minor	degrade	Signal degrade (BER low)	This alarm appears when the Bit Error Rate is greater than configured threshold. You can configure the threshold for this alarm from 1E-6 to 1E-9. For example, if set to 1E-7 (default), an alarm appears when BER exceeds this threshold. The detection time depends on the threshold. (1E-6 has a short detection-time, 1E-9 has longer detection time).	To clear this alarm, improve the BER level by a factor 10. Investigate whether bit errors occur for other sections in the network between intermediate nodes.
156	vc 4	Critical	tim	Trace Identifier Mismatch	This alarm appears when path trace is enabled and the "received string" is different from the "expected string". This alarm condition stops traffic	Verify the configured string in both ends of the VC-4

					<p>because AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received Path Trace.</p> <p>Note: For an EoS mapper (Ethernet over SDH port), Path trace is a global setting for each Group, though you can read the received string for each individual VC.</p>	<p>terminations. You do not have to set the Path Trace Identifier attributes, but you can use the tool to check the connectivity of complex networks. Basically, a Path Trace Identifier is inserted at the start of a path and extracted at the end of a path. When you set Path</p>
--	--	--	--	--	--	---

						Trace Transmitted to a logical value, (for example, "BONN-3-21") you can easily check whether the other side of the network receives this value. If you enter a value for the Path Trace Expected value and enable Path Trace, a TIM alarm is triggered if the received
--	--	--	--	--	--	---

						value is different from the transmitted value.
157	vc 4	Minor	rdi	Remote Defect Indication	This alarm indicates the presence of an incoming alarm at the point where the VC-4 terminates at the other end. The incoming alarm can be UNEQ, TIM, or SSF.	-
158	vc 4	Critical	lom	Loss Of Multiframe	A VC-4 that carries TU-12s has a multiframe indication in the H4 byte. If this multiframe indication is absent, Loss Of Multiframe occurs.	Check the configuration at the other end.
159	vc 4	Minor	ssf	Server Signal Failure	This alarm indicates that an alarm in the device affects the traffic on this VC-4 termination point. For example, a LOS-alarm on an STM-n port at the other end of a cross-connect.	-
160	vc 4	Critical	uneq	Unequipped	This alarm means that the VC-4 has no payload. This alarm normally indicates loss of	Check the configuration at the

					connectivity for configured payload.	other end and verify the cross-connections.
161	vc 4	Critical	plm	Payload Mismatch	The signal label indicates what type of payload the VC-4 carries. The payload label mismatch (PLM) alarm appears in case of a mismatch between expected and received signal label.	Check the configuration at the other end and verify the cross-connections.
162	vc 44 cNim	Major	exc	BER excessive error rate	This alarm appears if the Bit Error Rate is greater than 1E-5 for a C-value that is structured as AU-4-4C and has a non-intrusive monitor active.	Investigate whether bit errors occur for other sections in the network between intermediate nodes.
163	vc 44 cNim	Minor	deg	Signal degrade (BER low)	This alarm appears when the Bit Error Rate is greater than configured threshold for a C-value that is structured as AU-4-4c and has a non-	To clear the alarm, improve the BER level by a

					intrusive monitor active. You can configure the threshold for this alarm from 1E-6 to 1E-9. For example, if set to 1E-7 (default), an alarm appears when BER exceeds this threshold. The detection time depends on the threshold. (1E-6 has a short detection-time, 1E-9 has longer detection time).	factor 10. Investigate whether bit errors occur for other sections in the network between intermediate nodes.
164	vc44cNim	Critical	tim	Trace Identifier Mismatch	This alarm appears when path trace is enabled and the "received string" is different from the "expected string" for a C-value that is structured as AU-4-4c and has a non-intrusive monitor active. This alarm condition does not affect traffic.	When the TIM alarm is present on VC-4-4c level, verify the configured string on both ends of the VC-4-4c terminations. You do not have to set the Path

						<p>Trace Identifier attributes, but you can use the tool to check the connectivity of complex networks. Basically, a Path Trace Identifier is inserted at the start of a path and extracted at the end of a path. When you set Path Trace Transmitted to a logical value, (for example,</p>
--	--	--	--	--	--	---

						<p>"BON N-3-21") you can easily check whether the other side of the network receives this value. If you enter a value for the Path Trace Expected value and enable Path Trace, a TIM alarm is triggered if the received value is different from the transmitted value.</p>
165	vc	Criti	uneq	Unequ	This alarm	-

	44 cNi m	cal		ipped	indicates that an STM-n port does not contain a VC-44c for a C-value that is structured as AU-44c and has a non-intrusive monitor active.	
166	vc 4Ni m	Maj or	exc	BER exces sive error rate	This alarm appears if the Bit Error Rate is greater than 1E-5 for a CB-value that is structured as AU-4 and has a non-intrusive monitor active.	Investigate whether bit errors occur for other sections in the network between intermediate nodes.
167	vc 4Ni m	Min or	deg	Signal degra de (BER low)	This alarm appears when the Bit Error Rate is greater than configured threshold for a CB-value that is structured as AU-4 and has a non-intrusive monitor active. You can configure the threshold for this alarm from 1E-6 to 1E-9. For example, if set to 1E-7 (default), an alarm is raised when BER exceeds this	To clear this alarm, improve the BER level by a factor 10. Investigate whether bit errors occur for other sections in

					threshold. The detection time depends on the threshold. (1E-6 has a short detection-time, 1E-9 has longer detection time).	the network between intermediate nodes.
168	vc4Nim	Critical	tim	Trace Identifier Mismatch	<p>This alarm appears when path trace is enabled and the "received string" is different from the "expected string" for a CB-value that is structured as AU-4 and has a non-intrusive monitor active. This alarm condition does not affect traffic.</p> <p>Note: For an EoS mapper (Ethernet over SDH port), Path trace is a global setting for each Group, though you can read the received string for each individual VC.</p>	<p>When the TIM alarm is present on VC-4 level, verify the configured string in both ends of the VC-4 terminations. You do not have to set the Path Trace Identifier attributes, but you can use the tool to check the connection.</p>

						ctivity of complex networks. Basically, a Path Trace Identifier is inserted at the start of a path and extracted at the end of a path. When you set Path Trace Transmitted to a logical value, (for example, "BONN-3-21") you can easily check whether the other side of the network
--	--	--	--	--	--	--

						receives this value. If you enter a value for the Path Trace Expected value and enable Path Trace, a TIM alarm is triggered if the received value is different from the transmitted value.
169	vc4Nim	Critical	uneq	Unequipped	This alarm indicates that an STM-n port does not contain a VC-4 for a CB-value that is structured as AU-4 and has a non-intrusive monitor active.	-
170	vc at	Critical	lom	Vcat Loss Of	All Vcat VC-ns carry a multiframe	Check the config

				Multiframe	indication to realign all members of a Vcat group in the sink end. If the sink end is unable to interpret the multiframe indication, Vcat Loss Of Multiframe occurs.	uration at the other end and verify the cross-connections.
171	vc at	Maj or	sqm	Seque nce indicat or misma tch	This alarm appears when the received sequence (SQ) number is different from the expected sequence number. This is applicable only in non-LCAS mode.	Check the configuration at the other end and verify the cross-connections.
172	vc at	Maj or	loa	Loss of align. traffic ch	This alarm appears when excessive differential delay between channels prevents channel alignment.	Ensure that the differential delay between the VCAT members is less than the maximum tolerable delay.
173	wa n	Criti cal	wanDe lay	Delay betwe en VC12s	This alarm appears when the differential delay between	-

				above limit	VC-12s exceed ca. 6.5 ms. This alarm is similar to loa , but appears only for WAN ports with proprietary mapping.	
174	wan	Critical	seqFail	Wrong channel sequencing P2P	This alarm appears when the order of the VCs is incorrect. This alarm is similar to sqm , but appears only for WAN ports with proprietary mapping.	Verify the order of VCs that carry Ethernet traffic between two WAN-ports.
175	wan	Major	plc	Partial loss capacity	This alarm appears when the operational status for bandwidth for an EoS mapper is less than what is administratively set. This alarm appears only for ports with bidirectional capacity (proprietary mapping).	-
176	wan	Critical	tlc	Total loss capacity	This alarm appears in the event of absence of traffic on a port due to SDH alarms. This alarm appears only for ports with bidirectional capacity (proprietary	-

					mapping).	
177	warn	Major	plcr	Partial loss capacity rx	This alarm appears when the traffic capacity is less than provisioned in the receive direction on this port due to SDH alarms.	-
178	warn	Critical	tlcr	Total loss capacity rx	This alarm appears when there is no traffic in the receive direction on this port due to SDH alarms.	-
179	warn	Warning	rldot1dStpPortStateForwarding	Bridge port learning to forwarding state transition -	This alarm indicates a move in the STP port state for the given port from the "Learning" state to the "Forwarding" state. The port now forwards traffic.	This alarm indicates a topology change.
180	warn	Warning	rldot1dStpPortStateNotForwarding	Bridge port forwarding to blocking state transition -	This alarm indicates a move in the STP port state for the given port from the "Forwarding" state to the "Blocking" state. The port no longer forwards traffic.	This alarm indicates a topology change.

Related Information

- [Technical Support & Documentation - Cisco Systems](#)