CHAPTER 10

Signaling Troubleshooting

Revised: July 22, 2009, OL-8000-32

Introduction

This chapter provides the information needed to monitor and troubleshoot Signaling events and alarms. This chapter is divided into the following sections:

- Signaling Events and Alarms – Provides a brief overview of each Signaling event and alarm.
- Monitoring Signaling Events – Provides the information needed to monitor and correct Signaling events.
- Troubleshooting Signaling Alarms – Provides the information needed to troubleshoot and correct Signaling alarms.

Caution The use of the **UNIX ifconfig down** command on any signaling interface to test or troubleshoot network or interface failures of the Cisco BTS 10200 Softswitch Signaling Interface may lead to undesirable consequences or conditions.

Note The following billing records are created when a call is rejected due to overload conditions:
• SS7 termination cause code 42
• Cable signaling stop event cause code “resource unavailable”
Calls rejected by the signaling adapter will not generate a billing record.

Signaling Events and Alarms

This section provides a brief overview of the Signaling events and alarms for the Cisco BTS 10200 Softswitch in numerical order. Table 10-1 lists all signaling events and alarms by severity.

Note Click the Signaling message number in Table 10-1 to display information about the event or alarm.

Table 10-1 Signaling Events and Alarms by Severity

CRITICAL	MAJOR	MINOR	WARNING	INFO
SIGNALING (12)	SIGNALING (7)	SIGNALING (10)	SIGNALING (4)	SIGNALING (1)
SIGNALING (64)	SIGNALING (8)	SIGNALING (14)	SIGNALING (6)	SIGNALING (42)
SIGNALING (65)	SIGNALING (9)	SIGNALING (15)	SIGNALING (25)	SIGNALING (43)
SIGNALING (69)	SIGNALING (11)	SIGNALING (16)	SIGNALING (26)	SIGNALING (44)
SIGNALING (75)	SIGNALING (13)	SIGNALING (17)	SIGNALING (27)	SIGNALING (45)
SIGNALING (80)	SIGNALING (23)	SIGNALING (18)	SIGNALING (28)	SIGNALING (46)
SIGNALING (81)	SIGNALING (59)	SIGNALING (19)	SIGNALING (29)	SIGNALING (49)
SIGNALING (82)	SIGNALING (63)	SIGNALING (20)	SIGNALING (30)	SIGNALING (50)
SIGNALING (83)	SIGNALING (66)	SIGNALING (21)	SIGNALING (31)	SIGNALING (51)
SIGNALING (84)	SIGNALING (68)	SIGNALING (22)	SIGNALING (32)	SIGNALING (52)
SIGNALING (107)	SIGNALING (79)	SIGNALING (24)	SIGNALING (33)	SIGNALING (53)
SIGNALING (110)	SIGNALING (85)	SIGNALING (36)	SIGNALING (34)	SIGNALING (54)
SIGNALING (119)	SIGNALING (86)	SIGNALING (40)	SIGNALING (60)	SIGNALING (55)
SIGNALING (120)	SIGNALING (87)	SIGNALING (78)	SIGNALING (70)	SIGNALING (57)
SIGNALING (142)	SIGNALING (88)	SIGNALING (92)	SIGNALING (71)	SIGNALING (58)
SIGNALING (144)	SIGNALING (89)	SIGNALING (93)	SIGNALING (72)	SIGNALING (61)
	SIGNALING (90)	SIGNALING (94)	SIGNALING (73)	SIGNALING (62)
	SIGNALING (91)	SIGNALING (95)	SIGNALING (74)	SIGNALING (76)
	SIGNALING (108)	SIGNALING (96)	SIGNALING (115)	SIGNALING (77)
	SIGNALING (109)	SIGNALING (97)	SIGNALING (132)	SIGNALING (104)
	SIGNALING (113)	SIGNALING (98)	SIGNALING (141)	SIGNALING (105)
	SIGNALING (114)	SIGNALING (99)	SIGNALING (146)	SIGNALING (133)
	SIGNALING (116)	SIGNALING (100)	SIGNALING (147)	SIGNALING (134)
	SIGNALING (121)	SIGNALING (101)	SIGNALING (148)	SIGNALING (135)
	SIGNALING (122)	SIGNALING (102)	SIGNALING (166)	SIGNALING (136)
	SIGNALING (125)	SIGNALING (103)	SIGNALING (167)	SIGNALING (137)
	SIGNALING (126)	SIGNALING (106)		SIGNALING (139)
	SIGNALING (127)	SIGNALING (111)		SIGNALING (140)
		SIGNALING (112)		SIGNALING (152)

Table 10-1 Signaling Events and Alarms by Severity (continued)

CRITICAL	MAJOR	MINOR	WARNING	INFO
		SIGNALING (117)		
		SIGNALING (118)		
		SIGNALING (124)		
		SIGNALING (138)		
		SIGNALING (143)		
		SIGNALING (145)		
		SIGNALING (150)		
		SIGNALING (151)		

SIGNALING (1)

For additional information, refer to the "Test Report - Signaling (1)" section on page 10-82.

DESCRIPTION	Test Report
SEVERITY	Information (INFO)
THRESHOLD	10000
THROTTLE	0

Note SIGNALING (2) and SIGNALING (3) are not used.

SIGNALING (4)

To monitor and correct the cause of the event, refer to the "Invalid Message Received - Signaling (4)" section on page 10-82.

DESCRIPTION	Invalid Message Received
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Endpoint Name - STRING [40] Message Type - STRING [40]
PRIMARY CAUSE	Issued when a signaling adapter has received an invalid message from the specified endpoint.
PRIMARY ACTION	Monitor the associated signaling link to see if there is an interruption of service on the link.
SECONDARY ACTION	If there is a communication problem, restart the link.
TERNARY ACTION	Verify that the version of the protocol used by the device at the endpoint is consistent with the version expected by the call agent.
SUBSEQUENT ACTION	If there is a mismatch, then either the endpoint or call agent must be re-provisioned.

Note SIGNALING (5) is not used.

SIGNALING (6)

To monitor and correct the cause of the event, refer to the "Database Module Function Call Failure - Signaling (6)" section on page 10-82.

DESCRIPTION	Database Module Function Call Failure
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Endpoint Name - STRING [40] Return Code - FOUR_BYTES Function Name - STRING [64] Calling Function - STRING [64] Index - FOUR_BYTES
PRIMARY CAUSE	A signaling adapter has detected an error while accessing a database interface.
PRIMARY ACTION	If the database that the adapter attempted to access is not available, restart the associated process.
SECONDARY ACTION	If an incompatible versions of the signaling adapter process and the database processes are present on the system, correct the error and restart the processes.

SIGNALING (7)

To troubleshoot and correct the cause of the alarm, refer to the "Socket Failure - Signaling (7)" section on page 10-111.

DESCRIPTION	Socket Failure
SEVERITY	MAJOR
THRESHOLD	30
THROTTLE	0
DATAWORDS	Reason Text - STRING [30]
PRIMARY CAUSE	Issued when there is a failure in creating/binding to the User Datagram Protocol (UDP) socket.
PRIMARY ACTION	Verify there is no conflict in port assignment with other processes in the system and ensure no previous instance of the same process is still running.
SECONDARY CAUSE	Software logic problem.
SECONDARY ACTION	Contact Cisco Support. (Contact Cisco Technical Assistance Center (TAC).)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (8)

To troubleshoot and correct the cause of the alarm, refer to the "Session Initiation Protocol Message Receive Failure - Signaling (8)" section on page 10-111.

DESCRIPTION	Session Initiation Protocol Message Receive Failure
SEVERITY	MAJOR
THRESHOLD	30
THROTTLE	0
DATAWORDS	Reason Text - STRING [50]
PRIMARY CAUSE	Operating system level network errors or invalid network configuration.
PRIMARY ACTION	Have your network administrator resolve network errors. Contact Cisco TAC if you need assistance. Manually clear alarm. Restart this call agent instance using the platform start command.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (9)

To troubleshoot and correct the cause of the alarm, refer to the "Timeout on Internet Protocol Address - Signaling (9)" section on page 10-112.

DESCRIPTION	Timeout on Internet Protocol Address
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	MGW/Term Name - STRING [80] Gateway Type - STRING [32] Possible Cause - STRING [32]
PRIMARY CAUSE	Issued when opticall is unable to communicate with a gateway.
PRIMARY ACTION	Verify that the gateway is both configured for service and that it has been set in service.
SECONDARY ACTION	Attempt to ping the gateway using the Internet Protocol (IP) address from the event report. If the ping is not successful, then diagnose the issue that prevents the address from being reached.
TERNARY ACTION	Use the status media gateway (MGW) identification (ID) = xxx, where xxx is the IP address given in the event report. If the status is not in service (INS), then use control mgw command to put it in service.

SIGNALING (10)

To troubleshoot and correct the cause of the alarm, refer to the "Failed to Send Complete Session Initiation Protocol Message - Signaling (10)" section on page 10-112.

DESCRIPTION	Failed to Send Complete Session Initiation Protocol Message
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Destination Address - STRING [64]
PRIMARY CAUSE	Notifies the user that the Session Initiation Protocol (SIP) stack failed to send an SIP message due to it exceeding the maximum length of a UDP packet.
PRIMARY ACTION	If encountered in normal network operations, the message should be captured on passive testing equipment and sent to Cisco TAC for evaluation.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (11)

To troubleshoot and correct the cause of the alarm, refer to the "Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)" section on page 10-112.

DESCRIPTION	Failed to Allocate Session Initiation Protocol Control Block
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Size - TWO_BYTES Detail - STRING [80]
PRIMARY CAUSE	Issued when there is not enough memory to allocate a SIP call control block.
PRIMARY ACTION	Increase the SIP call control block (CCB) count specified in mem.cfg file.
SECONDARY ACTION	Restart call agent to take effect.

SIGNALING (12)

To troubleshoot and correct the cause of the alarm, refer to the "Feature Server is not Up or is not Responding to Call Agent - Signaling (12)" section on page 10-113.

DESCRIPTION	Feature Server is not Up or is not Responding to Call Agent
SEVERITY	CRITICAL
THRESHOLD	30
THROTTLE	0
DATAWORDS	Domain Name of FS - STRING [65] Feature Server ID - STRING [20]
PRIMARY CAUSE	Feature server platform is down or is not operating properly.
PRIMARY ACTION	Restart the applicable feature server.

SIGNALING (13)

To troubleshoot and correct the cause of the alarm, refer to the "Signaling System 7 Signaling Link Down - Signaling (13)" section on page 10-114.

DESCRIPTION	Signaling System 7 Signaling Link Down
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link_Number - ONE_BYTE Link_Name - STRING [25]
PRIMARY CAUSE	Signaling System 7 (SS7) trunk group may be out-of-service (OOS).
PRIMARY ACTION	Use control ss7-trunk-grp to place the trunk group in service (INS).
SECONDARY CAUSE	The local Ulticom stack may be down.
SECONDARY ACTION	Run the Ulticom stack again.
TERNARY CAUSE	SS7 link may be disconnected or faulty.
TERNARY ACTION	Check the Ulticom local configuration.
SUBSEQUENT CAUSE	Remote SS7 signaling site may be down or incorrectly configured.
SUBSEQUENT ACTION	Check the Ulticom remote configuration.

SIGNALING (14)

To troubleshoot and correct the cause of the alarm, refer to the "Link is Remotely Inhibited - Signaling (14)" section on page 10-115.

DESCRIPTION	Link is Remotely Inhibited
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link - ONE_BYTE Link Name - STRING [8]
PRIMARY CAUSE	Issued when the specified Signaling System 7 (SS7) link is inhibited at the remote end.
PRIMARY ACTION	Monitor events at the network level for any related to the specified SS7 link. Restorative actions needs to be taken on the remote end.

SIGNALING (15)

To troubleshoot and correct the cause of the alarm, refer to the "Link is Locally Inhibited - Signaling (15)" section on page 10-115.

DESCRIPTION	Link is Locally Inhibited
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link No - ONE_BYTE Link Name - STRING [8]
PRIMARY CAUSE	Issued when the specified SS7 link is inhibited at the local end.
PRIMARY ACTION	Verify that the SS7 signaling adapter process is running and that the SS7 interface card(s) are in service.
SECONDARY ACTION	If a component is found to be non-operational, restore it to service.

SIGNALING (16)

To troubleshoot and correct the cause of the alarm, refer to the "Link is Congested - Signaling (16)" section on page 10-115.

DESCRIPTION	Link is Congested
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link No - ONE_BYTE
PRIMARY CAUSE	Issued when the specified SS7 link is experiencing congestion.
PRIMARY ACTION	Monitor event reports at the network level to determine if the traffic load on the specified SS7 link is too high on the local end, or if the remote end is lagging in processing the traffic.
SECONDARY ACTION	Verify that the SS7 link has not degraded in quality.
TERNARY ACTION	Verify that the traffic load has not become unbalanced if multiple SS7 links are used.
SUBSEQUENT ACTION	Verify that local SS7 signaling adapter process is running normally.

SIGNALING (17)

To troubleshoot and correct the cause of the alarm, refer to the "Link: Local Processor Outage - Signaling (17)" section on page 10-115.

DESCRIPTION	Link: Local Processor Outage
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link No - ONE_BYTE Link Name - STRING [8]
PRIMARY CAUSE	Issued when the specified SS7 link has experienced a processor outage.
PRIMARY ACTION	Monitor the system for maintenance event reports associated with the signaling adapter or underlying platform instance that support the specified SS7 link. Verify that the process and or platform are restarted and returned to service.

SIGNALING (18)

To troubleshoot and correct the cause of the alarm, refer to the "Link: Remote Processor Outage - Signaling (18)" section on page 10-115.

DESCRIPTION	Link: Remote Processor Outage
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link No - ONE_BYTE Link Name - STRING [8]
PRIMARY CAUSE	Issued when the specified SS7 link has experienced a processor outage.
PRIMARY ACTION	Monitor the network level event reports for any events associated with the processing complex used by the specified SS7 link. Verify that the SS7 link is returned to service.

SIGNALING (19)

To troubleshoot and correct the cause of the alarm, refer to the "Link Set Inaccessible - Signaling (19)" section on page 10-115.

DESCRIPTION	Link Set Inaccessible
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link Set No - ONE_BYTE Link Set Name - STRING [8]
PRIMARY CAUSE	Issued when the specified SS7 link set is inaccessible.
PRIMARY ACTION	If the SS7 signaling adapter is not running normally and the associated call agent platform is not active, return them to service.

SIGNALING (20)

To troubleshoot and correct the cause of the alarm, refer to the "Link Set Congestion - Signaling (20)" section on page 10-116.

DESCRIPTION	Link Set Congestion
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link Set No - ONE_BYTE Link Set Name - STRING [8] Congestion Level - ONE_BYTE
PRIMARY CAUSE	Issued when the specified SS7 link set is experiencing congestion.
PRIMARY ACTION	Monitor event reports at the network level to determine if the traffic load on the specified SS7 link set is too high on the local end, or if the remote end is lagging in processing the traffic.
SECONDARY ACTION	Verify that the SS7 link set has not degraded in quality.
TERNARY ACTION	Verify that the traffic load has not become unbalanced if multiple SS7 link sets are used.
SUBSEQUENT ACTION	Verify that local SS7 signaling adapter process is running normally.

SIGNALING (21)

To troubleshoot and correct the cause of the alarm, refer to the "Route Set Failure - Signaling (21)" section on page 10-116.

DESCRIPTION	Route Set Failure
SEVERITY	MAJOR
THRESHOLD	200
THROTTLE	0
DATAWORDS	Route Set No - TWO_BYTES Route Set Name - STRING [8]
PRIMARY CAUSE	Issued when the specified route set has experienced a failure.
PRIMARY ACTION	Verify that the processing complex supporting the route set is functional.
SECONDARY ACTION	Monitor event reports at the network level to determine the failing component and verify its restoral to service.

SIGNALING (22)

To troubleshoot and correct the cause of the alarm, refer to the "Route Set Congested - Signaling (22)" section on page 10-116.

DESCRIPTION	Route Set Congested
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Route Set No - TWO_BYTES Route Set Name - STRING [8] Congestion Level - ONE_BYTE
PRIMARY CAUSE	Issued when the specified route set is experiencing congestion.
PRIMARY ACTION	Monitor event reports at the network level to determine if the traffic load on the specified SS7 link set is too high on the local end, or if the remote end is lagging in processing the traffic.
SECONDARY ACTION	Verify that the SS7 link set has not degraded in quality.
TERNARY ACTION	Verify that the traffic load has not become unbalanced if multiple SS7 link sets are used.
SUBSEQUENT ACTION	Verify that local SS7 signaling adapter process is running normally.

SIGNALING (23)

To troubleshoot and correct the cause of the alarm, refer to the "Destination Point Code Unavailable - Signaling (23)" section on page 10-117.

DESCRIPTION	Destination Point Code Unavailable
SEVERITY	MAJOR
THRESHOLD	200
THROTTLE	0
DATAWORDS	DPC - STRING [12]
PRIMARY CAUSE	Issued when the specified destination point code (DPC) is not available. This is usually caused by one of the following: 1) A failure in the affected DPC. 2) An unavailable route between the Cisco BTS 10200 Softswitch and the affected DPC.
PRIMARY ACTION	Verify that alternate routing has been assigned for traffic destined to the affected DPC.

SIGNALING (24)

To troubleshoot and correct the cause of the alarm, refer to the "Destination Point Code Congested - Signaling (24)" section on page 10-118.

DESCRIPTION	Destination Point Code Congested
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	DPC - STRING [12] DPC Type - ONE_BYTE Congestion Level - ONE_BYTE
PRIMARY CAUSE	Issued when the specified destination point code is congested.
PRIMARY ACTION	Monitor event reports at the network level to determine if the traffic load to the specified DPC is too high on the local end, or if the remote end is lagging in processing the traffic.

SIGNALING (25)

To monitor and correct the cause of the event, refer to the "Unanswered Blocking - Signaling (25)" section on page 10-85.

DESCRIPTION	Unanswered Blocking
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a blocking (BLO) message was not acknowledged before the timer 13 (T13) expired for the associated circuit identification code (CIC).
PRIMARY ACTION	Verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active.
SECONDARY ACTION	Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available.
TERNARY ACTION	Verify that the T13 timer is set to an appropriate level.
SUBSEQUENT ACTION	Verify that the SS7 link is not congested.

SIGNALING (26)

To monitor and correct the cause of the event, refer to the "Unanswered Unblocking Message - Signaling (26)" section on page 10-85.

DESCRIPTION	Unanswered Unblocking Message
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a unblocking message (UBL) message was not acknowledged before the timer 15 (T15) expired for the associated CIC.
PRIMARY ACTION	Verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active.
SECONDARY ACTION	Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available.
TERNARY ACTION	Verify that the T13 timer is set to an appropriate level.
SUBSEQUENT ACTION	Verify that the SS7 link is not congested.

SIGNALING (27)

To monitor and correct the cause of the event, refer to the "Unanswered Circuit Group Blocking - Signaling (27)" section on page 10-86.

DESCRIPTION	Unanswered Circuit Group Blocking
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a circuit group blocking (CGB) message was not acknowledged before the timer 19 (T19) expired for the associated CIC.
PRIMARY ACTION	Verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active.
SECONDARY ACTION	Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available.
TERNARY ACTION	Verify that the T13 timer is set to an appropriate level.
SUBSEQUENT ACTION	Verify that the SS7 link is not congested.

SIGNALING (28)

To monitor and correct the cause of the event, refer to the "Unanswered Circuit Group Unblocking - Signaling (28)" section on page 10-86.

DESCRIPTION	Unanswered Circuit Group Unblocking
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a circuit group unblocking (CGU) message was not acknowledged before the timer 21 (T21) expired for the associated CIC.
PRIMARY ACTION	Verify that the SS7 signaling adapter processes is running normally.
SECONDARY ACTION	Verify that the call agent platform is active.
TERNARY ACTION	Verify that the SS7 interface hardware is in service.
SUBSEQUENT ACTION	Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

SIGNALING (29)

To monitor and correct the cause of the event, refer to the "Unanswered Circuit Query Message - Signaling (29)" section on page 10-86.

DESCRIPTION	Unanswered Circuit Query Message
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a circuit query message (CQM) message was not acknowledged before the timer 28 (T28) expired for the associated CIC.
PRIMARY ACTION	Verify that the SS7 signaling adapter processes is running normally.
SECONDARY ACTION	Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service.
TERNARY ACTION	Verify that the associated SS7 signaling link is available.
SUBSEQUENT ACTION	Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

SIGNALING (30)

To monitor and correct the cause of the event, refer to the "Unanswered Circuit Validation Test - Signaling (30)" section on page 10-86.

DESCRIPTION	Unanswered Circuit Validation Test
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a circuit validation test (CVT) message was not acknowledged before the Tcvt expired for the associated CIC.
PRIMARY ACTION	Verify that the SS7 signaling adapter processes is running normally.
SECONDARY ACTION	Verify that the call agent platform is active.
TERNARY ACTION	Verify that the SS7 interface hardware is in service.
SUBSEQUENT ACTION	Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

SIGNALING (31)

To monitor and correct the cause of the event, refer to the "Unanswered Reset Circuit - Signaling (31)" section on page 10-86.

DESCRIPTION	Unanswered Reset Circuit
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a reset circuit (RSC) message was not acknowledged before the timer 17 (T17) expired for the associated CIC.
PRIMARY ACTION	Verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active.
SECONDARY ACTION	Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available.
TERNARY ACTION	Verify that the T13 timer is set to an appropriate level.
SUBSEQUENT ACTION	Verify that the SS7 link is not congested.

SIGNALING (32)

To monitor and correct the cause of the event, refer to the "Unanswered Group Reset - Signaling (32)" section on page 10-87.

DESCRIPTION	Unanswered Group Reset
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a group reset (GRS) message was not acknowledged before the timer 23 (T23) expired for the associated CIC.
PRIMARY ACTION	Verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active.
SECONDARY ACTION	Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available.
TERNARY ACTION	Verify that the T13 timer is set to an appropriate level.
SUBSEQUENT ACTION	Verify that the SS7 link is not congested.

SIGNALING (33)

To monitor and correct the cause of the event, refer to the "Unanswered Release - Signaling (33)" section on page 10-87.

DESCRIPTION	Unanswered Release
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a release (REL) message was not acknowledged before the timer 5 (T5) expired for the associated CIC.
PRIMARY ACTION	Verify that the SS7 signaling adapter processes is running normally.
SECONDARY ACTION	Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service.
TERNARY ACTION	Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level.
SUBSEQUENT ACTION	Verify that the SS7 link is not congested.

SIGNALING (34)

To monitor and correct the cause of the event, refer to the "Unanswered Continuity Check Request - Signaling (34)" section on page 10-87.

DESCRIPTION	Unanswered Continuity Check Request
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when an loop prevention acknowledgement (LPA) message was not acknowledged before the timer continuity check request (T_{CCR}) expired for the associated CIC.
PRIMARY ACTION	Verify that the SS7 signaling adapter processes is running normally.
SECONDARY ACTION	Verify that the call agent platform is active.
TERNARY ACTION	Verify that the SS7 interface hardware is in service.
SUBSEQUENT ACTION	Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Note SIGNALING (35) is not used.

SIGNALING (36)

To troubleshoot and correct the cause of the alarm, refer to the "Trunk Locally Blocked - Signaling (36)" section on page 10-118. For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x."

DESCRIPTION	Trunk Locally Blocked
SEVERITY	MINOR
THRESHOLD	500
THROTTLE	0
DATAWORDS	CIC Number - STRING [40] TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20] MGW-EP-NAME - STRING [64] MGW-TSAP-ADDR - STRING [80] Reason - STRING [80]
PRIMARY CAUSE	Issued when a BLO or CGB message was sent on the specified CIC.
PRIMARY ACTION	For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x."

Note SIGNALING (37) through SIGNALING (39) are not used.

SIGNALING (40)

To troubleshoot and correct the cause of the alarm, refer to the "Trunk Remotely Blocked - Signaling (40)" section on page 10-118.

DESCRIPTION	Trunk Remotely Blocked
SEVERITY	MAJOR
THRESHOLD	500
THROTTLE	0
DATAWORDS	CIC Number - STRING [40] TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20] MGW-EP-NAME - STRING [64] MGW-TSAP-ADDR - STRING [80]
PRIMARY CAUSE	Issued when a BLO or CGB message was received on the specified CIC if it is SS7 trunk. Issued when SERVICE OOS message is received for Integrated Services Digital Network (ISDN) trunks. Issued when Reverse Make Busy (rbz) signal received for channel-associated signaling (CAS) operator trunk.
PRIMARY ACTION	No action required. Can manually recover from this condition locally by controlling effected trunks to unequipped (UEQP) state and back INS.

Note SIGNALING (41) is not used.

SIGNALING (42)

For additional information, refer to the "Continuity Testing Message Received on the Specified Circuit Identification Code - Signaling (42)" section on page 10-88.

DESCRIPTION	Continuity Testing Message Received on the Specified Circuit Identification Code
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a continuity testing (COT) message was received on the specified CIC.
PRIMARY ACTION	No action required.

SIGNALING (43)

For additional information, refer to the "Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code - Signaling (43)" section on page 10-88.

DESCRIPTION	Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a release complete (RLC) message was received in response to a RSC message on the specified CIC.
PRIMARY ACTION	No action required.

SIGNALING (44)

For additional information, refer to the "Continuity Recheck is Performed on Specified Circuit Identification Code - Signaling (44)" section on page 10-88.

DESCRIPTION	Continuity Recheck is Performed on Specified Circuit Identification Code
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a continuity recheck was performed on the specified CIC.
PRIMARY ACTION	No action required.

SIGNALING (45)

For additional information, refer to the "Circuit is UNEQUIPPED on Remote Side - Signaling (45)" section on page 10-88.

DESCRIPTION	Circuit is UNEQUIPPED on Remote Side
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when an unequipped circuit has been detected on the remote side.
PRIMARY ACTION	Monitor the event reports at the network level to verify if an existing circuit was unequipped causing a status mismatch with the local end.

SIGNALING (46)

For additional information, refer to the "Specified Circuit Identification Code is Invalid for the Operation - Signaling (46)" section on page 10-88.

DESCRIPTION	Specified Circuit Identification Code is Invalid for the Operation
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when an invalid operation was performed on the specified CIC.
PRIMARY ACTION	Verify that the SS7 provisioning tables are properly configured at the circuit level.

Note SIGNALING (47) and SIGNALING (48) are not used.

SIGNALING (49)

For additional information, refer to the "A General Processing Error Encountered - Signaling (49)" section on page 10-88.

DESCRIPTION	A General Processing Error Encountered
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a general SS7 processing error occurred due to all resources being busy or an invalid event occurring.
PRIMARY ACTION	Verify the status of the signaling adapter process and the SS7 signaling interface to verify proper operation.

SIGNALING (50)

For additional information, refer to the "Unexpected Message for the Call State is Received: Clear Call - Signaling (50)" section on page 10-89.

DESCRIPTION	Unexpected Message for the Call State is Received: Clear Call
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when an unexpected message was received for the current call state.
PRIMARY ACTION	The call is cleared. Verify the status of the signaling adapter process and the SS7 signaling interface to verify proper operation.

SIGNALING (51)

For additional information, refer to the "Set Trunk State as Remotely Unequipped - Signaling (51)" section on page 10-89.

DESCRIPTION	Set Trunk State as Remotely Unequipped
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when the specified CIC is marked at remotely unequipped due to the CQM response indicating that it is unequipped at the far end.
PRIMARY ACTION	Equip the trunk circuit at the far end.

SIGNALING (52)

For additional information, refer to the "Set Trunk State as NOT Remotely Blocked - Signaling (52)" section on page 10-89.

DESCRIPTION	Set Trunk State as NOT Remotely Blocked
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when the specified CIC is marked as not remotely blocked due to the CQM response indicating that it is not remotely blocked at the far end.
PRIMARY ACTION	No action required.

SIGNALING (53)

For additional information, refer to the "Set Trunk State as Remotely Blocked - Signaling (53)" section on page 10-89.

DESCRIPTION	Set Trunk State as Remotely Blocked
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when the specified CIC is marked as remotely blocked due to the CQM response indicating that it is remotely blocked at the far end.
PRIMARY ACTION	Clear the blocking situation at the far end based on network level event reports.

SIGNALING (54)

For additional information, refer to the "Circuit Validation Test Aborted - Signaling (54)" section on page 10-89.

DESCRIPTION	Circuit Validation Test Aborted
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when the circuit specified failed a validation test due to an internal failure.
PRIMARY ACTION	Verify the SS7 signaling adapter process and SS7 interface is operating normally.

SIGNALING (55)

For additional information, refer to the "Circuit Validation Successful - Signaling (55)" section on page 10-89.

DESCRIPTION	Circuit Validation Successful
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when the specified circuit was successfully validated.
PRIMARY ACTION	No action required.

Note SIGNALING (56) is not used.

SIGNALING (57)

For additional information, refer to the "Continuity Recheck Failed - Signaling (57)" section on page 10-90.

DESCRIPTION	Continuity Recheck Failed
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a continuity recheck of the specified CIC failed.
PRIMARY ACTION	Verify the SS7 signaling adapter process and SS7 interface is operating normally.

SIGNALING (58)

For additional information, refer to the "Continuity Recheck Successful - Signaling (58)" section on page 10-90.

DESCRIPTION	Continuity Recheck Successful
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a continuity recheck of the specified CIC was successful.
PRIMARY ACTION	No action required.

SIGNALING (59)

To troubleshoot and correct the cause of the alarm, refer to the "Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)" section on page 10-118.

DESCRIPTION	Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES Media Gateway Name - STRING [65] Media Gateway Index - FOUR_BYTES Service Status - FOUR_BYTES
PRIMARY CAUSE	Issued when the specified ISDN trunk group's status was changed due to a media gateway operation.
PRIMARY ACTION	Monitor the event reports at the network level to determine which media gateway caused the status change of the trunk group.
SECONDARY ACTION	Verify that the gateway is reconfigured properly to support the usage of the trunk group.

SIGNALING (60)

To monitor and correct the cause of the event, refer to the "Integrated Services Digital Network STATUS Message Containing Error Indication Received - Signaling (60)" section on page 10-90.

DESCRIPTION	Integrated Services Digital Network STATUS Message Containing Error Indication Received
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Name - STRING [40] Termination Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES Cause Value - ONE_BYTE Call State - ONE_BYTE
PRIMARY CAUSE	Issued when an ISDN status message was received containing an error indication for the specified termination.
PRIMARY ACTION	If the specified termination is not operating normally, place it in service state.

SIGNALING (61)

For additional information, refer to the "Trunk Operational State Changed by Service Message - Signaling (61)" section on page 10-90.

DESCRIPTION	Trunk Operational State Changed by Service Message
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Name - STRING [40] Termination Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES Service Status - FOUR_BYTES
PRIMARY CAUSE	Issued when the specified trunk group's operational status was changed via a service message from the specified gateway.
PRIMARY ACTION	Monitor the event reports at the network level to verify that the specified gateway and terminations are operating normally.

SIGNALING (62)

For additional information, refer to the "Received Integrated Services Digital Network RESTART Message - Signaling (62)" section on page 10-91.

DESCRIPTION	Received Integrated Services Digital Network RESTART Message
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Name - STRING [40] Termination Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES Flag - FOUR_BYTES
PRIMARY CAUSE	Issued when an ISDN restart message was received from the specified gateway.
PRIMARY ACTION	Monitor the event reports at the network level to verify that the specified gateway and terminations are operating normally.

SIGNALING (63)

To troubleshoot and correct the cause of the alarm, refer to the "Media Gateway/Termination Faulty - Signaling (63)" section on page 10-119.

DESCRIPTION	Media Gateway/Termination Faulty
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Fully Qualified Name - STRING [80] Type of Gateway - STRING [32] Reason for Failure - STRING [80]
PRIMARY CAUSE	Issued when a media gateway or termination has gone faulty due to the detection of an unknown endpoint, unknown package type, and unknown event, a hardware failure, or a general call agent error.
PRIMARY ACTION	Verify the proper operation of the media gateway specified. Place the termination out-of-service and then back into service from the call agent.

SIGNALING (64)

To troubleshoot and correct the cause of the alarm, refer to the "Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)" section on page 10-119.

DESCRIPTION	Media Gateway Adapter Running out of Shared Memory Pools
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Issued when the Media Gateway Control Protocol (MGCP) signaling adapter was unable to allocate data store for an inter-process communication (IPC) message due to a lack of resources.
PRIMARY ACTION	Call Cisco TAC technologies for assistance. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (65)

To troubleshoot and correct the cause of the alarm, refer to the "Media Gateway Adapter Running out of Heap Memory - Signaling (65)" section on page 10-119.

DESCRIPTION	Media Gateway Adapter Running out of Heap Memory
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Issued when the MGCP signaling adapter was unable to allocate data store for an IPC message from the heap due to a lack of resources.
PRIMARY ACTION	Call Cisco TAC Technologies for assistance. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (66)

To troubleshoot and correct the cause of the alarm, refer to the "Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)" section on page 10-119.

DESCRIPTION	Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Fully Qualified Name - STRING [80] Reason - STRING [80] Detailed Reason - STRING [80]
PRIMARY CAUSE	Issued when a call agent internal error has occurred causing the restart of the MGCP signaling adapter.
PRIMARY ACTION	Send log files to Cisco TAC for analysis and corrective action. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Note SIGNALING (67) is not used.

SIGNALING (68)

To troubleshoot and correct the cause of the alarm, refer to the "Media Gateway Endpoints are out of Service at Gateway - Signaling (68)" section on page 10-119.

DESCRIPTION	Media Gateway Endpoints are out of Service at Gateway
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Fully Qualified Name - STRING [80] Type of MGW- STRING [32] Failure Cause - STRING [80] Subscriber Info - STRING [80] ICMP Ping Status - STRING [80]
PRIMARY CAUSE	This could have been caused by (1) The media gateway has been administratively taken OOS using command in gateway (GW). (2) The endpoint is alarmed/OOS state.
PRIMARY ACTION	Bring the Media gateway has been administratively taken INS using command in GW. Fix the endpoint alarms.

SIGNALING (69)

To troubleshoot and correct the cause of the alarm, refer to the "Call Agent and Feature Server Communication Message Timeout - Signaling (69)" section on page 10-120.

DESCRIPTION	Call Agent and Feature Server Communication Message Timeout
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Configured CA Name - STRING [70]
PRIMARY CAUSE	Call Agent (CA) - Feature Server (FS) communication failure due to wrong system configuration; -OR- CA or FS is down.
PRIMARY ACTION	Check the configuration related to CA-FS communication. FS table entries, CA entry.

SIGNALING (70)

To monitor and correct the cause of the event, refer to the "Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication - Signaling (70)" section on page 10-92.

DESCRIPTION	Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES
PRIMARY CAUSE	The ISDN signaling adapter is unable to restore a D-channel due to incorrect backhaul provisioning at the media gateway or call agent.
PRIMARY ACTION	Ensure the provisioning of the backhaul port is correct at both the call agent and media gateway.

SIGNALING (71)

To monitor and correct the cause of the event, refer to the "Integrated Services Digital Network Unable to Establish D-channel - Signaling (71)" section on page 10-92.

DESCRIPTION	Integrated Services Digital Network Unable to Establish D-channel
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES
PRIMARY CAUSE	The ISDN signaling adapter is unable to establish a D-channel due to layer 1 parameters not being provisioned correctly or improper provisioning of the network or user side.
PRIMARY ACTION	Verify the correct provisioning at the media gateway.

SIGNALING (72)

To monitor and correct the cause of the event, refer to the "Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time - Signaling (72)" section on page 10-92.

DESCRIPTION	Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES
PRIMARY CAUSE	The ISDN signaling adapter has lost calls due to a D-channel being down as a result of a media gateway power loss or a loss of connection between the private branch exchange (PBX) and media gateway.
PRIMARY ACTION	Resupply power to the media gateway and verify that the connection between the PBX and media gateway is intact.

SIGNALING (73)

To monitor and correct the cause of the event, refer to the "Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired - Signaling (73)" section on page 10-93.

DESCRIPTION	Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Name - STRING [40] Termination Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES Restart Class - FOUR_BYTES
PRIMARY CAUSE	The ISDN signaling adapter was unable to send a RESTART message due to the expiration of the RESTART timer.
PRIMARY ACTION	Verify that the RESTART timer is set to an appropriate level.

SIGNALING (74)

To monitor and correct the cause of the event, refer to the "Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired - Signaling (74)" section on page 10-93.

DESCRIPTION	Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Name - STRING [40] Termination Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES Service Status - FOUR_BYTES
PRIMARY CAUSE	The ISDN signaling adapter was unable to send a SERVICE message due to the expiration of the SERVICE timer.
PRIMARY ACTION	Ensure that the RESTART timer is set to an appropriate level.

SIGNALING (75)

To troubleshoot and correct the cause of the alarm, refer to the "Signaling System 7 Stack not Ready - Signaling (75)" section on page 10-120.

DESCRIPTION	Signaling System 7 Stack not Ready
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	LogicalName - STRING [64]
PRIMARY CAUSE	SS7 stack not configured properly.
PRIMARY ACTION	Check SS7 stack configuration.
SECONDARY CAUSE	SS7 stack not ready.
SECONDARY ACTION	Check SS7 stack status. Do platform "**start -i omni**" to bring up SS7 stack.

SIGNALING (76)

For additional information, refer to the "Timeout on Remote Instance - Signaling (76)" section on page 10-93.

DESCRIPTION	Timeout on Remote Instance
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Port Number - TWO_BYTES Hostname - STRING [64]
PRIMARY CAUSE	Communication between call agent and remote instance is faulty.
PRIMARY ACTION	No action needed.

SIGNALING (77)

For additional information, refer to the "Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling - Signaling (77)" section on page 10-93.

DESCRIPTION	Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES
PRIMARY CAUSE	Manually switched the D-channels using the command line interface (CLI).
PRIMARY ACTION	Verify operator action.
SECONDARY CAUSE	Lost active D-channel.
SECONDARY ACTION	Verify that gateway is operational and connection to PBX is good.

SIGNALING (78)

To troubleshoot and correct the cause of the alarm, refer to the "Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)" section on page 10-120.

DESCRIPTION	Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES Trunk Group Idx - FOUR_BYTES IS Primary D Channel - FOUR_BYTES
PRIMARY CAUSE	One of the ISDN D-channels in primary rate interface (PRI) is down.
PRIMARY ACTION	Check gateway power, and gateway connection to PBX.

SIGNALING (79)

To troubleshoot and correct the cause of the alarm, refer to the "Media Gateway Unreachable - Signaling (79)" section on page 10-120. For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x."

DESCRIPTION	Media Gateway Unreachable
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Entity Name - STRING [40] General Context - STRING [40] Specific Context - STRING [40] Failure Context - STRING [40]
PRIMARY CAUSE	MGCP signaling interop error has occurred.
PRIMARY ACTION	Notify customer support or refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x". (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (80)

To troubleshoot and correct the cause of the alarm, refer to the "Out of Bounds, Memory/Socket Error - Signaling (80)" section on page 10-120.

DESCRIPTION	Out of Bounds, Memory/Socket Error
SEVERITY	CRITICAL
DATAWORDS	Process Name - STRING [40] Description - STRING [40] Extra Info - STRING [40]
PRIMARY CAUSE	Out of heap memory.
PRIMARY ACTION	Notify customer support. Increase random access memory (RAM). (Contact Cisco TAC.)
SECONDARY CAUSE	Out of IPC pool memory.
SECONDARY ACTION	Resize IPC pool size in the platform configuration file.
TERNARY CAUSE	Socket error has occurred. Inappropriate/already bound socket is in use.
TERNARY ACTION	Check UDP port supplied with media gateway adapter (MGA) command-line for validity and prior use.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (81)

To troubleshoot and correct the cause of the alarm, refer to the "Insufficient Heap Memory - Signaling (81) (H.323)" section on page 10-121.

DESCRIPTION	Insufficient Heap Memory
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32]
PRIMARY CAUSE	Issued when the H.323 Protocol (H323) signaling adapter is unable to allocate memory from the system.
PRIMARY ACTION	Call CISCO TAC for assistance. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (82)

To troubleshoot and correct the cause of the alarm, refer to the "Insufficient Shared Memory Pools - Signaling (82) (H.323)" section on page 10-121.

DESCRIPTION	Insufficient Shared Memory Pools
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32]
PRIMARY CAUSE	Issued when H323 signaling adapter was unable to allocate storage.
PRIMARY ACTION	Call Cisco TAC for corrective action. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (83)

To troubleshoot and correct the cause of the alarm, refer to the "Error While Binding to Socket - Signaling (83)" section on page 10-121.

DESCRIPTION	Error While Binding to Socket
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Socket ID - FOUR_BYTES Local TSAP Address - STRING [32] Reason - STRING [128]

SIGNALING (84)

To troubleshoot and correct the cause of the alarm, refer to the "Reached Maximum Socket Limit - Signaling (84) (H.323)" section on page 10-121.

DESCRIPTION	Reached Maximum Socket Limit
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Active Sockets - FOUR_BYTES
PRIMARY CAUSE	The configuration setting of an H.323 signaling adapter (H3A) parameter in platform.cfg file is wrong.
PRIMARY ACTION	Reconfigure platform.cfg file and restart the H3A process.

SIGNALING (85)

To troubleshoot and correct the cause of the alarm, refer to the "Initialization Failure - Signaling (85)" section on page 10-121.

DESCRIPTION	Initialization Failure
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Reason - STRING [128]
PRIMARY CAUSE	Process initialization failure has occurred.
PRIMARY ACTION	Check Dataword 2 (Reason) for the failure cause and take action accordingly.

SIGNALING (86)

To troubleshoot and correct the cause of the alarm, refer to the "Remote H323 Gateway is not Reachable - Signaling (86) (H.323)" section on page 10-121.

DESCRIPTION	Remote H323 Gateway is not Reachable
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Remote GW TSAP Addr - STRING [32]
PRIMARY CAUSE	Loss of communication with a remote gateway has occurred.
PRIMARY ACTION	Perform standard connectivity tests - both physical checks and IP tests. Also, ensure that the gateway is not out of service.

SIGNALING (87)

To troubleshoot and correct the cause of the alarm, refer to the "H323 Message Parsing Error - Signaling (87) (H.323)" section on page 10-122.

DESCRIPTION	H323 Message Parsing Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Remote GW TSAP Addr - STRING [32]
PRIMARY CAUSE	Unable to successfully parse an incoming H323 message.
PRIMARY ACTION	This is a result of either a software bug or bad message being received - a message with a valid message type but an invalid field within the message. Snoop the message from the endpoint and verify it's content or call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (88)

To troubleshoot and correct the cause of the alarm, refer to the "H323 Message Encoding Error - Signaling (88) (H.323)" section on page 10-122.

DESCRIPTION	H323 Message Encoding Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Reason - STRING [128]
PRIMARY CAUSE	Unable to encode an H323 message for sending.
PRIMARY ACTION	This is indicative a software bug. Contact Cisco TAC.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (89)

To troubleshoot and correct the cause of the alarm, refer to the "Gatekeeper not Available/Reachable - Signaling (89)" section on page 10-122.

DESCRIPTION	Gatekeeper not Available/Reachable
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Gatekeeper ID - STRING [32] GK TSAP Addr - STRING [32]
PRIMARY CAUSE	Gatekeeper is not available or is unreachable.
PRIMARY ACTION	Check network connectivity. Check to ensure gatekeeper (GK) is reachable by trying to ping GK IP address. If reachable, then check to ensure that GK is configured up. This is a result of either a software bug or bad message being received - a message with a valid message type but an invalid field within the message. Snoop the message from the endpoint and verify its content or call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (90)

To troubleshoot and correct the cause of the alarm, refer to the "Alternate Gatekeeper is not Responding - Signaling (90)" section on page 10-122.

DESCRIPTION	Alternate Gatekeeper is not Responding
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Gatekeeper ID - STRING [32] GK TSAP Addr - STRING [32]
PRIMARY CAUSE	Alternate gatekeeper is not responding.
PRIMARY ACTION	Check network connectivity. Check to ensure the alternate GK is reachable by trying to ping the alternate GK IP address. If reachable, then check to ensure that alternate GK is configured up. This is a result of either a software bug or bad message being received - a message with a valid message type but an invalid field within the message. Snoop the message from the endpoint and verify its content or call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (91)

To troubleshoot and correct the cause of the alarm, refer to the "Endpoint Security Violation - Signaling (91) (H.323)" section on page 10-123.

DESCRIPTION	Endpoint Security Violation
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Gatekeeper ID - STRING [32] GK TSAP Addr - STRING [32]
PRIMARY CAUSE	An H323 security violation has occurred.
PRIMARY ACTION	The password on the Cisco BTS 10200 Softswitch and/or gatekeeper is wrong - the H323 gateway (H323GW) table may not be provisioned properly OR there is a time synchronization problem between the Cisco BTS 10200 Softswitch and/or gatekeeper and the Network Time Protocol (NTP) server. Ensure both the Cisco BTS 10200 Softswitch and gatekeeper are pointing to the same NTP server.

SIGNALING (92)

To troubleshoot and correct the cause of the alarm, refer to the "Invalid Call Identifier - Signaling (92)" section on page 10-123.

DESCRIPTION	Invalid Call Identifier
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Remote GW TSAP Addr - STRING [32] Call ID - EIGHT_BYTES
PRIMARY CAUSE	The call ID was invalid or changed mid-call.
PRIMARY ACTION	This is a software problem on the Cisco BTS 10200 Softswitch or endpoint. Call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (93)

To troubleshoot and correct the cause of the alarm, refer to the "Invalid Call Reference Value - Signaling (93)" section on page 10-123.

DESCRIPTION	Invalid Call Reference Value
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Remote GW TSAP Addr - STRING [32] Call ID - EIGHT_BYTES Call Ref Value - EIGHT_BYTES
PRIMARY CAUSE	The call ID was invalid or changed mid-call.
PRIMARY ACTION	This is a software problem on the Cisco BTS 10200 Softswitch or endpoint. Call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (94)

To troubleshoot and correct the cause of the alarm, refer to the "Invalid Conference Identifier - Signaling (94)" section on page 10-123.

DESCRIPTION	Invalid Conference Identifier
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Reason - STRING [32] Remote GW Port - TWO_BYTES Call ID - EIGHT_BYTES Conference ID - EIGHT_BYTES
PRIMARY CAUSE	The call ID was invalid or changed mid-call.
PRIMARY ACTION	This is a software problem on the Cisco BTS 10200 Softswitch or endpoint. Call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (95)

To troubleshoot and correct the cause of the alarm, refer to the "Invalid Message from the Network - Signaling (95)" section on page 10-123.

DESCRIPTION	Invalid Message from the Network
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Remote GW TSAP Addr - STRING [32] Call ID - EIGHT_BYTES Conf ID - EIGHT_BYTES Call Ref Value - EIGHT_BYTES
PRIMARY CAUSE	Unsupported or invalid message type received from network.
PRIMARY ACTION	Call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (96)

To troubleshoot and correct the cause of the alarm, refer to the "Internal Call Processing Error - Signaling (96)" section on page 10-124.

DESCRIPTION	Internal Call Processing Error
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES Reason - STRING [128]
PRIMARY CAUSE	A software error has occurred.
PRIMARY ACTION	Call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (97)

To troubleshoot and correct the cause of the alarm, refer to the "Insufficient Information to Complete Call - Signaling (97)" section on page 10-124.

DESCRIPTION	Insufficient Information to Complete Call
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES Conf ID - EIGHT_BYTES Call Ref Value - EIGHT_BYTES
PRIMARY CAUSE	Not enough initial call setup information was received to establish the call.
PRIMARY ACTION	Call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (98)

To troubleshoot and correct the cause of the alarm, refer to the "H323 Protocol Inconsistencies - Signaling (98) (H.323)" section on page 10-124.

DESCRIPTION	H323 Protocol Inconsistencies
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES Reason - STRING [128]
PRIMARY CAUSE	The H323 endpoint and Cisco BTS 10200 Softswitch are running different protocol versions.
PRIMARY ACTION	This is only an issue where the endpoint is running a higher version of the H323 protocol than the Cisco BTS 10200 Softswitch. Call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (99)

To troubleshoot and correct the cause of the alarm, refer to the "Abnormal Call Clearing - Signaling (99)" section on page 10-124.

DESCRIPTION	Abnormal Call Clearing
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES Reason - STRING [128]
PRIMARY CAUSE	Unsupported or invalid message type received from network.
PRIMARY ACTION	Call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (100)

To troubleshoot and correct the cause of the alarm, refer to the "Codec Negotiation Failed - Signaling (100)" section on page 10-124.

DESCRIPTION	Codec Negotiation Failed
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES Reason - STRING [128]
PRIMARY CAUSE	Codec negotiation failed.
PRIMARY ACTION	Find a compatible set of codec settings for both sides, re-provision the endpoints of the call and try the call again.

SIGNALING (101)

To troubleshoot and correct the cause of the alarm, refer to the "Per Call Security Violation - Signaling (101)" section on page 10-124.

DESCRIPTION	Per Call Security Violation
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES Gatekeeper ID - STRING [32]
PRIMARY CAUSE	This is a future trap definition.
PRIMARY ACTION	None

SIGNALING (102)

To troubleshoot and correct the cause of the alarm, refer to the "H323 Network Congested - Signaling (102) (H.323)" section on page 10-125.

DESCRIPTION	H323 Network Congested
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Gatekeeper ID - STRING [32]
PRIMARY CAUSE	The H323 application processes has depleted it's resources. no more calls can be completed.
PRIMARY ACTION	The high water mark has been reached - all new call requests are rejected until the low water mark is reached. Reprovision the water marks or check the network for overload. Also verify that alternate routes have been provisioned on the Cisco BTS 10200 Softswitch.

SIGNALING (103)

To troubleshoot and correct the cause of the alarm, refer to the "Aggregation Connection Down - Signaling (103)" section on page 10-125.

DESCRIPTION	Aggregation Connection Down
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	AGGR-ID - STRING [16]
PRIMARY CAUSE	Transmission Control Protocol (TCP) connection is down.
PRIMARY ACTION	Check the associated cabling and perform PINGs to test the connectivity.

SIGNALING (104)

For additional information, refer to the "Aggregation Unable To Establish Connection - Signaling (104)" section on page 10-97.

DESCRIPTION	Aggregation Unable To Establish Connection
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	AGGR-ID - STRING [16]
PRIMARY CAUSE	TCP connection establish failure.
PRIMARY ACTION	Check the IP connectivity of CA and cable modem termination system (CMTS).

SIGNALING (105)

For additional information, refer to the "Aggregation Gate Set Failed - Signaling (105)" section on page 10-98.

DESCRIPTION	Aggregation Gate Set Failed
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	AGGR-ID - STRING [16] Error-Code - TWO_BYTES Sub-Error-Code - TWO_BYTES
PRIMARY CAUSE	Gate set acknowledgement never came from CMTS.
PRIMARY ACTION	None

SIGNALING (106)

To troubleshoot and correct the cause of the alarm, refer to the "Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)" section on page 10-125.

DESCRIPTION	Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Delivery function (DF) server not responding.
PRIMARY ACTION	Check the encryption key or IP connectivity to DF.

SIGNALING (107)

To troubleshoot and correct the cause of the alarm, refer to the "Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)" section on page 10-125.

DESCRIPTION	Logical Internet Protocol Addresses not Mapped Correctly
SEVERITY	CRITICAL
THRESHOLD	30
THROTTLE	0
DATAWORDS	Contact Domain Name - STRING [128] Number of IP Addresses Resolved - FOUR_BYTES Number of Virtual IP Addresses - FOUR_BYTES
PRIMARY CAUSE	Contact name in the configuration file not configured in domain name system (DNS).
PRIMARY ACTION	Verify name in DNS matches name in platform.cfg and opticall.cfg files.
SECONDARY CAUSE	Contact could not be resolved to an IP address on the host.
SECONDARY ACTION	Verify DNS resolves to IP addresses reserved for process on the Cisco BTS 10200 Softswitch.
TERNARY CAUSE	IP address manager not running.
TERNARY ACTION	Verify Internet Protocol Manager (IPM) process is running and check for alarms from IPM.
SUBSEQUENT CAUSE	Mis-configuration during installation or manual changes made after installation.
SUBSEQUENT ACTION	Contact Cisco TAC for support.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (108)

To troubleshoot and correct the cause of the alarm, refer to the "Simplex Only Operational Mode - Signaling (108)" section on page 10-126.

DESCRIPTION	Simplex Only Operational Mode
SEVERITY	MAJOR
THRESHOLD	30
THROTTLE	0
DATAWORDS	Host Domain Name - STRING [128]
PRIMARY CAUSE	The hostname parameter specified in platform.cfg file instead of -contact parameter.
PRIMARY ACTION	Cisco BTS 10200 Softswitch is configured as a SIMPLEX system.
SECONDARY CAUSE	SIP adapter (SIA) host and contact parameters are the same in the platform.cfg file. SIA is configured for use on a simplex system.
SECONDARY ACTION	If this is a duplex installation, regardless of current operational state, contact Cisco TAC. If this is a simplex installation only, this alarm can be turned off.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (109)

To troubleshoot and correct the cause of the alarm, refer to the "Stream Control Transmission Protocol Association Failure - Signaling (109)" section on page 10-126.

DESCRIPTION	Stream Control Transmission Protocol Association Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	SCTP Association ID - STRING [17]
PRIMARY CAUSE	Ethernet cables on signaling gateway process (SGP) are unplugged or severed.
PRIMARY ACTION	Plug Ethernet cables in or fix severed connection.
SECONDARY CAUSE	SGP is not operational.
SECONDARY ACTION	Check SGP alarms to determine why it is not operating properly.

SIGNALING (110)

To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Group Is Out-of-Service - Signaling (110)" section on page 10-130.

DESCRIPTION	Signaling Gateway Group is Out-of-Service
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	SG Group ID - STRING [17]
PRIMARY CAUSE	All Stream Control Transmission Protocol (SCTP) associations between CA and SGs are out-of-service.
PRIMARY ACTION	Make sure all Ethernet connections on the CA and SGs are plugged in. Also make sure all associated IP routers are operational.
SECONDARY CAUSE	The MTP3 user adapter (M3UA) layer is down between the CA and SGs.
SECONDARY ACTION	Use Cisco Snooper application to determine why the M3UA layer is down.

SIGNALING (111)

To troubleshoot and correct the cause of the alarm, refer to the "Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)" section on page 10-130.

DESCRIPTION	Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	SCTP Association ID - STRING [17] Destination IP Address - STRING [11]
PRIMARY CAUSE	Single Ethernet connection on CA or SGP is unplugged or severed.
PRIMARY ACTION	Plug in all Ethernet connections or repair if severed.
SECONDARY CAUSE	SCTP communication problem - protocol timeout.
SECONDARY ACTION	Use Cisco Snooper application to determine why SCTP association is degraded.

SIGNALING (112)

To troubleshoot and correct the cause of the alarm, refer to the "Stream Control Transmission Protocol Association Configuration Error - Signaling (112)" section on page 10-130.

DESCRIPTION	Stream Control Transmission Protocol Association Configuration Error
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	SCTP Association ID - STRING [17]
PRIMARY CAUSE	Destination IP address is invalid.
PRIMARY ACTION	Input new destination IP address - see log for additional details.
SECONDARY CAUSE	Local IP address is invalid.
SECONDARY ACTION	Input new local IP address information.
TERNARY CAUSE	IP Routing Table is not configured properly.
TERNARY ACTION	Have the system administrator configure IP routing table.

SIGNALING (113)

To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Failure - Signaling (113)" section on page 10-131.

DESCRIPTION	Signaling Gateway Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Signaling Gateway ID - STRING [17]
PRIMARY CAUSE	All associated signaling gateway processes are out-of-service.
PRIMARY ACTION	Determine why each associated SGP is out-of-service (see SGP alarm definition).

SIGNALING (114)

To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Process Is Out-of-Service - Signaling (114)" section on page 10-131.

DESCRIPTION	Signaling Gateway Process is Out-of-Service
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Signaling Gateway - STRING [17]
PRIMARY CAUSE	All SCTP associations between the SGP and the CA are out-of-service.
PRIMARY ACTION	See SCTP association alarm definition to determine how to rectify the problem.
SECONDARY CAUSE	The M3UA layer is down between the CA and SGP.
SECONDARY ACTION	Use Cisco snooper utility to determine why M3UA layer is down. Also see log for additional information.

SIGNALING (115)

To monitor and correct the cause of the event, refer to the "Invalid Routing Context Received - Signaling (115)" section on page 10-100.

DESCRIPTION	Invalid Routing Context Received
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Invalid Routing Cont - FOUR_BYTES SG from Which the In - STRING [17]
PRIMARY CAUSE	Routing context was configured improperly on CA or signaling gateway (SG).
PRIMARY ACTION	Reconfigure routing context on CA or SG so that they match in both places.

SIGNALING (116)

To troubleshoot and correct the cause of the alarm, refer to the "Destination Point Code User Part Unavailable - Signaling (116)" section on page 10-132.

DESCRIPTION	Destination Point Code User Part Unavailable
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	DPC ID - STRING [17]
PRIMARY CAUSE	SGP sent a destination user part unavailable (DUPU) M3UA message to CA indicating that a User Part is unavailable on at a DPC.
PRIMARY ACTION	Contact SS7 Network Administrator to report the User Part Unavailable problem of the DPC so communication can be restored.

SIGNALING (117)

To troubleshoot and correct the cause of the alarm, refer to the "Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)" section on page 10-132.

DESCRIPTION	Circuit Validation Test Message Received for an Unequipped Circuit Identification Code
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC - TWO_BYTES TGN-ID - EIGHT_BYTES DPC - STRING [13]
PRIMARY CAUSE	CIC is not provisioned
PRIMARY ACTION	Provision CIC.

SIGNALING (118)

To troubleshoot and correct the cause of the alarm, refer to the "Circuit Verification Response Received with Failed Indication - Signaling (118)" section on page 10-132.

DESCRIPTION	Circuit Verification Response Received with Failed Indication
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC - TWO_BYTES TGN-ID - EIGHT_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	CIC mismatch.
PRIMARY ACTION	Perform internal test such as checking that the CIC is assigned to a circuit between the sending and the receiving switch.

SIGNALING (119)

To troubleshoot and correct the cause of the alarm, refer to the "Signaling System 7 Adapter Process Faulty - Signaling (119)" section on page 10-132.

DESCRIPTION	Signaling System 7 Adapter Process Faulty
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Reason - STRING [36]
PRIMARY CAUSE	OMNI or S7A exception.
PRIMARY ACTION	Check OMNI process. The S7A will restart itself if S7A maximum restart is not exceeded.

SIGNALING (120)

To troubleshoot and correct the cause of the alarm, refer to the "Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)" section on page 10-132.

DESCRIPTION	Signaling System 7 Module/Signaling System 7 Adapter Faulty
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Reason - STRING [36]
PRIMARY CAUSE	OMNI failure.
PRIMARY ACTION	Check OMNI status; failover will occur in a duplex configuration.

SIGNALING (121)

To troubleshoot and correct the cause of the alarm, refer to the "Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)" section on page 10-133.

DESCRIPTION	Message Transfer Part 3 User Adapter Cannot Go Standby
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Platform ID - STRING [17]
PRIMARY CAUSE	No INACTIVE acknowledge (ACK) messages received from any SG or SCTP Associations are probably down.
PRIMARY ACTION	Investigate other alarms to see if SGs are down or SCTP associations are down. Take corrective action according to those alarms.

SIGNALING (122)

To troubleshoot and correct the cause of the alarm, refer to the "Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)" section on page 10-133.

DESCRIPTION	Message Transfer Part 3 User Adapter Cannot Go Active
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Platform ID - STRING [17]
PRIMARY CAUSE	No ACTIVE acknowledgement messages received from any SG or SCTP associations are probably down.
PRIMARY ACTION	Investigate other alarms to see if SGs are down or SCTP associations are down. Take corrective action according to those alarms.

Note SIGNALING (123) is not used.

SIGNALING (124)

To troubleshoot and correct the cause of the alarm, refer to the "Remote Subsystem is Out Of Service - Signaling (124)" section on page 10-133.

DESCRIPTION	Remote Subsystem is Out Of Service
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Destination Point Co - STRING [20] Remote Subsystem Num - TWO_BYTES
PRIMARY CAUSE	Link loss or the remote subsystem out of service.
PRIMARY ACTION	Check links. Check remote location, if possible.

SIGNALING (125)

To troubleshoot and correct the cause of the alarm, refer to the "Signaling Connection Control Part Routing Error - Signaling (125)" section on page 10-133.

DESCRIPTION	Signaling Connection Control Part Routing Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Signaling connection control part (SCCP) route invalid or not available.
PRIMARY ACTION	Provision the right SCCP route.

SIGNALING (126)

To troubleshoot and correct the cause of the alarm, refer to the "Signaling Connection Control Part Binding Failure - Signaling (126)" section on page 10-134.

DESCRIPTION	Signaling Connection Control Part Binding Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local Point Code - STRING [20] Local Subsystem Numb - ONE_BYTE
PRIMARY CAUSE	Trillium stack binding failure.
PRIMARY ACTION	Re-initialize the TCAP signaling adapter (TSA) process or remove the subsystem from the Element Management System (EMS) table and add it again.

SIGNALING (127)

To troubleshoot and correct the cause of the alarm, refer to the "Transaction Capabilities Application Part Binding Failure - Signaling (127)" section on page 10-134.

DESCRIPTION	Transaction Capabilities Application Part Binding Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Trillium stack binding failure.
PRIMARY ACTION	Re-initialize the TSA process or remove the subsystem from the EMS table and add it again.

Note SIGNALING (128) through SIGNALING (131) are not used.

SIGNALING (132)

To monitor and correct the cause of the event, refer to the "Transaction Capabilities Application Part Reaches the Provisioned Resource Limit - Signaling (132)" section on page 10-102.

DESCRIPTION	Transaction Capabilities Application Part Reaches the Provisioned Resource Limit
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Dialogue/Invoke ID - FOUR_BYTES
PRIMARY CAUSE	Transaction Capabilities Application Part (TCAP) runs out of all the pre-configured dialogue IDs or invoke IDs.

SIGNALING (133)

For additional information, refer to the "Unable to Decode Generic Transport Descriptor Message - Signaling (133)" section on page 10-102.

DESCRIPTION	Unable to Decode Generic Transport Descriptor Message
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Endpoint Name - STRING [40] GTD Content Type - STRING [40]
PRIMARY CAUSE	Issued when the generic transport descriptor (GTD) parser failed to decode a GTD message received from the specified endpoint.
PRIMARY ACTION	Verify that the version of the GTD protocol used by the device at the remote endpoint is consistent with the version expected by the call agent.
SECONDARY ACTION	Examine the associated signaling link to see if there is any interruption of the supplementary services on the link.

SIGNALING (134)

For additional information, refer to the "Signaling System 7 Message Encoding Failure - Signaling (134)" section on page 10-103.

DESCRIPTION	Signaling System 7 Message Encoding Failure
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Error in ISDN user part (ISUP) stack or signaling adapter interface (SAI) message.
PRIMARY ACTION	Capture SS7 trace of circuit for examination by support personnel. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (135)

For additional information, refer to the "Signaling System 7 Message Decoding Failure - Signaling (135)" section on page 10-103.

DESCRIPTION	Signaling System 7 Message Decoding Failure
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Error in ISUP stack or SAI message.
PRIMARY ACTION	Capture SS7 trace of circuit for examination by support personnel. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (136)

For additional information, refer to the "Signaling System 7 Message Invalid Received - Signaling (136)" section on page 10-103.

DESCRIPTION	Signaling System 7 Message Invalid Received
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Invalid message was received from line in ISUP stack.
PRIMARY ACTION	Capture SS7 trace of circuit for examination by support personnel.
SECONDARY CAUSE	Invalid message was received from line in ISUP stack.
SECONDARY ACTION	Verify the signal switching point (SSP) sending the message to the CA is correctly configured.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (137)

For additional information, refer to the "Signaling System 7 Confusion Message Received - Signaling (137)" section on page 10-103.

DESCRIPTION	Signaling System 7 Confusion Message Received
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	An ISUP message or parameter received was not recognized or understood.
PRIMARY ACTION	Check the log for more information (including confusion (CFN) diagnostic output). Capture SS7 trace of affected circuits. If diagnostic data indicates messages/parameters that must be supported are being dropped, refer the captured data to support along with a description of the call scenario. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (138)

To monitor and correct the cause of the event, refer to the "Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138)" section on page 10-103.

DESCRIPTION	Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Number of SIP Connections Open - FOUR_BYTES SIP Connection Alarm Threshold - FOUR_BYTES Open SIP Connection Limit - FOUR_BYTES
PRIMARY CAUSE	Call failure/feature unavailable.
PRIMARY ACTION	System configuration and traffic load have caused the number of open connections to approach the engineered limit. This limit will need to be increased to allow for more connections. Please contact Cisco support. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (139)

For additional information, refer to the "Signaling System 7 Trunk was Found to be in Erroneous State - Signaling (139) (SS7)" section on page 10-104.

DESCRIPTION	Signaling System 7 Trunk was Found to be in Erroneous State
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20] Near-End State - STRING [64] Far-End State - STRING [64] Resolution Action - STRING [64]
PRIMARY CAUSE	Discrepancy between local and remote trunk states.
PRIMARY ACTION	Automatic corrective action enforced when using American National Standards Institute (ANSI) ISUP.

SIGNALING (140)

For additional information, refer to the "Unanswered Information Message - Signaling (140)" section on page 10-104.

DESCRIPTION	Unanswered Information Message
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Far-end switch is not responding to information (INF) message with an information request (INR) message.
PRIMARY ACTION	Verify that far-end switch can correctly respond to an INF message.

SIGNALING (141)

To monitor and correct the cause of the event, refer to the "Address not Resolved by Domain Name System Server - Signaling (141)" section on page 10-104.

DESCRIPTION	Address not Resolved by Domain Name System Server
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	TSAP_Address/Hostname - STRING [256]
PRIMARY CAUSE	The transport service access point (TSAP) address/hostname is not defined in DNS.
PRIMARY ACTION	Add entry for TSAP address to DNS server, or fix Cisco BTS 10200 Softswitch provisioning.

SIGNALING (142)

To troubleshoot and correct the cause of the alarm, refer to the "Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)" section on page 10-134.

DESCRIPTION	Session Initiation Protocol Trunk Operationally Out-of-Service
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group Description - STRING [16] Trunk TSAP Address - STRING [65]
PRIMARY CAUSE	Issued when Cisco BTS 10200 Softswitch is unable to communicate with a remote SIP party (Call-Agent or Proxy) over a SIP or SIP-T trunk.
PRIMARY ACTION	Verify DNS resolution exists, if TSAP address of the remote entity is a domain name. Verify the remote entity is reachable by Internet Control Message Protocol (ICMP) ping, using the Trunk TSAP address from the Event Report. If the same alarm is reported on all the softswitch trunk groups, then verify that the network connection is operational.
SECONDARY CAUSE	Remote SIP party is not operational.
SECONDARY ACTION	If the ping is not successful, then diagnose the issue that prevents the TSAP address from being reached. Verify the SIP application is running on the remote host and listening on the port specified in the TSAP address.

SIGNALING (143)

To troubleshoot and correct the cause of the alarm, refer to the "Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)" section on page 10-134.

DESCRIPTION	Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [65] Interface IP Address - STRING [65]
PRIMARY CAUSE	Hardware problem has occurred.
PRIMARY ACTION	Check the link interfaces.

SIGNALING (144)

To troubleshoot and correct the cause of the alarm, refer to the "All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)" section on page 10-134.

DESCRIPTION	All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [65] Interface IP Address - STRING [65]
PRIMARY CAUSE	Hardware problem has occurred.
PRIMARY ACTION	Check the link interfaces.

SIGNALING (145)

To troubleshoot and correct the cause of the alarm, refer to the "One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)" section on page 10-135.

DESCRIPTION	One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [65] Interface IP Address - STRING [65]
PRIMARY CAUSE	Hardware problem has occurred.
PRIMARY ACTION	Check the link interfaces.

SIGNALING (146)

To monitor and correct the cause of the event, refer to the "All Retransmission Attempts of Session Initiation Protocol Request or Response Failed - Signaling (146)" section on page 10-105.

DESCRIPTION	All Retransmission Attempts of Session Initiation Protocol Request or Response Failed
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	SIP Request Type - STRING [15] Sender IP - STRING [20]
PRIMARY CAUSE	SIP request: All retransmission attempts for a SIP request failed for DNS or IP address of request uniform resource identifier (URI). SIP response: All retransmission attempts for a SIP response failed for received socket IP address of request and DNS (or IP address) of via header.
PRIMARY ACTION	Ensure if DNS server is up and running for host name resolution and provisioned properly to resolve to correct order of IP addresses. Ensure that previous hop network component is alive and in healthy state for failures related to SIP responses.

SIGNALING (147)

To monitor and correct the cause of the event, refer to the "Domain Name System Service Addresses Exhausted - Signaling (147)" section on page 10-105.

DESCRIPTION	Domain Name System Service Addresses Exhausted
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	SRV Hostname - STRING [256]
PRIMARY CAUSE	DNS service (SRV) hostname resolution to IP address exhausted.
PRIMARY ACTION	Add entry to SRV in DNS server. Fix Cisco BTS 10200 Softswitch provisioning.

SIGNALING (148)

To monitor and correct the cause of the event, refer to the "Softswitch Audit Released Stale Memory - Signaling (148)" section on page 10-106.

DESCRIPTION	Softswitch Audit Released Stale Memory
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Stale Memory Release Info - STRING [128]
PRIMARY CAUSE	Loss of communication with originating or terminating side.
PRIMARY ACTION	Check if adjacent network element is up and having proper communication link with the BTS 10200 Softswitch.
SECONDARY CAUSE	Adjacent network device protocol error.
SECONDARY ACTION	Check the adjacent network device protocol compatibility.
TERNARY CAUSE	An internal software error has occurred.
TERNARY ACTION	Contact BTS 10200 engineer. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Note SIGNALING (149) is not used.

SIGNALING (150)

To troubleshoot and correct the cause of the alarm, refer to the "Stream Control Transmission Protocol Association Congested - Signaling (150)" section on page 10-135.

DESCRIPTION	Stream Control Transmission Protocol Association Congested
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	SCTP Association ID - STRING [17] Congestion Level - ONE_BYTE
PRIMARY CAUSE	Network is congested.
PRIMARY ACTION	Clean off the network congestion caused by routing or switching issues.
SECONDARY CAUSE	Central processing unit (CPU) is throttled.
SECONDARY ACTION	May need upgrade to a more powerful platform or offload some traffic.

SIGNALING (151)

To troubleshoot and correct the cause of the alarm, refer to the "Termination Permanent Error Code Received - Signaling (151)" section on page 10-135.

DESCRIPTION	Termination Permanent Error Code Received
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	End Point /Termination - STRING [54] Media Gateway - STRING [54] MGCP Message Type - STRING [54]
PRIMARY CAUSE	Fault in the gateway device.
PRIMARY ACTION	Maintenance required on the gateway or termination.

SIGNALING (152)

For additional information, refer to the "Termination Transient Error Received - Signaling (152)" section on page 10-106.

DESCRIPTION	Termination Transient Error Received
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Entity Name - STRING [40] General Context - STRING [40] Specific Context - STRING [40] Failure Context - STRING [40]
PRIMARY CAUSE	MGCP signaling interop errors have occurred.
PRIMARY ACTION	Notify customer support. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Note SIGNALING (153) through SIGNALING (165) are not used.

SIGNALING (166)

To monitor and correct the cause of the event, refer to the "No Routing Keys are Active - Signal (166)" section on page 106.

DESCRIPTION	No Routing Keys are Active
SEVERITY	WARNING
THRESHOLD	0
THROTTLE	0
PRIMARY CAUSE	Routing keys not controlled into ACTIVE state.
PRIMARY ACTION	Control routing keys to ACTIVE state.
SECONDARY CAUSE	The ITP provisioning is incorrect.
SECONDARY ACTION	Check the ITP provisioning.

SIGNALING (167)

To monitor and correct the cause of the event, refer to the "No Signaling Gateways are Active – Signaling (167)" section on page 107.

DESCRIPTION	No Signaling Gateways are Active
SEVERITY	WARNING
THRESHOLD	0
THROTTLE	0
PRIMARY CAUSE	A communication problem between ITP and the Cisco BTS 10200 Softswitch.
PRIMARY ACTION	Check the communication path between the Cisco BTS 10200 Softswitch and the ITP.

Monitoring Signaling Events

This section provides the information needed to monitor and correct Signaling events. Table 10-2 lists all Signaling events in numerical order and provides cross reference to each subsection in this section.

Table 10-2 Cisco BTS 10200 Softswitch Signaling Events

Event Type	Event Name	Event Severity
SIGNALING(1)	Test Report - Signaling (1)	INFO
SIGNALING(4)	Invalid Message Received - Signaling (4)	WARNING
SIGNALING(6)	Database Module Function Call Failure - Signaling (6)	WARNING
SIGNALING(7)	Socket Failure - Signaling (7)	MAJOR
SIGNALING(8)	Session Initiation Protocol Message Receive Failure - Signaling (8)	MAJOR
SIGNALING(9)	Timeout on Internet Protocol Address - Signaling (9)	MAJOR
SIGNALING(10)	Failed to Send Complete Session Initiation Protocol Message - Signaling (10)	MINOR
SIGNALING(11)	Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)	MAJOR
SIGNALING(12)	Feature Server is not Up or is not Responding to Call Agent - Signaling (12)	CRITICAL
SIGNALING(13)	Signaling System 7 Signaling Link Down - Signaling (13)	MAJOR
SIGNALING(14)	Link is Remotely Inhibited - Signaling (14)	MINOR
SIGNALING(15)	Link is Locally Inhibited - Signaling (15)	MINOR
SIGNALING(16)	Link is Congested - Signaling (16)	MINOR
SIGNALING(17)	Link: Local Processor Outage - Signaling (17)	MINOR
SIGNALING(18)	Link: Remote Processor Outage - Signaling (18)	MINOR
SIGNALING(19)	Link Set Inaccessible - Signaling (19)	MAJOR
SIGNALING(20)	Link Set Congestion - Signaling (20)	MAJOR
SIGNALING(21)	Route Set Failure - Signaling (21)	MAJOR
SIGNALING(22)	Route Set Congested - Signaling (22)	MINOR
SIGNALING(23)	Destination Point Code Unavailable - Signaling (23)	MAJOR
SIGNALING(24)	Destination Point Code Congested - Signaling (24)	MINOR
SIGNALING(25)	Unanswered Blocking - Signaling (25)	WARNING
SIGNALING(26)	Unanswered Unblocking Message - Signaling (26)	WARNING
SIGNALING(27)	Unanswered Circuit Group Blocking - Signaling (27)	WARNING
SIGNALING(28)	Unanswered Circuit Group Unblocking - Signaling (28)	WARNING
SIGNALING(29)	Unanswered Circuit Query Message - Signaling (29)	WARNING
SIGNALING(30)	Unanswered Circuit Validation Test - Signaling (30)	WARNING
SIGNALING(31)	Unanswered Reset Circuit - Signaling (31)	WARNING
SIGNALING(32)	Unanswered Group Reset - Signaling (32)	WARNING
SIGNALING(33)	Unanswered Release - Signaling (33)	WARNING
SIGNALING(34)	Unanswered Continuity Check Request - Signaling (34)	WARNING
SIGNALING(36)	Trunk Locally Blocked - Signaling (36)	MINOR

Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)

Event Type	Event Name	Event Severity
SIGNALING(40)	Trunk Remotely Blocked - Signaling (40)	MAJOR
SIGNALING(42)	Continuity Testing Message Received on the Specified Circuit Identification Code - Signaling (42)	INFO
SIGNALING(43)	Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code - Signaling (43)	INFO
SIGNALING(44)	Continuity Recheck is Performed on Specified Circuit Identification Code - Signaling (44)	INFO
SIGNALING(45)	Circuit is UNEQUIPPED on Remote Side - Signaling (45)	INFO
SIGNALING(46)	Specified Circuit Identification Code is Invalid for the Operation - Signaling (46)	INFO
SIGNALING(49)	A General Processing Error Encountered - Signaling (49)	INFO
SIGNALING(50)	Unexpected Message for the Call State is Received: Clear Call - Signaling (50)	INFO
SIGNALING(51)	Set Trunk State as Remotely Unequipped - Signaling (51)	INFO
SIGNALING(52)	Set Trunk State as NOT Remotely Blocked - Signaling (52)	INFO
SIGNALING(53)	Set Trunk State as Remotely Blocked - Signaling (53)	INFO
SIGNALING(54)	Circuit Validation Test Aborted - Signaling (54)	INFO
SIGNALING(55)	Circuit Validation Successful - Signaling (55)	INFO
SIGNALING(57)	Continuity Recheck Failed - Signaling (57)	INFO
SIGNALING(58)	Continuity Recheck Successful - Signaling (58)	INFO
SIGNALING(59)	Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)	MAJOR
SIGNALING(60)	Integrated Services Digital Network STATUS Message Containing Error Indication Received - Signaling (60)	WARNING
SIGNALING(61)	Trunk Operational State Changed by Service Message - Signaling (61)	INFO
SIGNALING(62)	Received Integrated Services Digital Network RESTART Message - Signaling (62)	INFO
SIGNALING(63)	Media Gateway/Termination Faulty - Signaling (63)	MAJOR
SIGNALING(64)	Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)	CRITICAL
SIGNALING(65)	Media Gateway Adapter Running out of Heap Memory - Signaling (65)	CRITICAL
SIGNALING(66)	Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)	MAJOR
SIGNALING(68)	Media Gateway Endpoints are out of Service at Gateway - Signaling (68)	MAJOR
SIGNALING(69)	Call Agent and Feature Server Communication Message Timeout - Signaling (69)	CRITICAL
SIGNALING(70)	Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication - Signaling (70)	WARNING
SIGNALING(71)	Integrated Services Digital Network Unable to Establish D-channel - Signaling (71)	WARNING
SIGNALING(72)	Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time - Signaling (72)	WARNING
SIGNALING(73)	Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired - Signaling (73)	WARNING

Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)

Event Type	Event Name	Event Severity
SIGNALING(74)	Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired - Signaling (74)	WARNING
SIGNALING(75)	Signaling System 7 Stack not Ready - Signaling (75)	CRITICAL
SIGNALING(76)	Timeout on Remote Instance - Signaling (76)	INFO
SIGNALING(77)	Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling - Signaling (77)	INFO
SIGNALING(78)	Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)	MINOR
SIGNALING(79)	Media Gateway Unreachable - Signaling (79)	MAJOR
SIGNALING(80)	Out of Bounds, Memory/Socket Error - Signaling (80)	CRITICAL
SIGNALING(81)	Insufficient Heap Memory - Signaling (81) (H.323)	CRITICAL
SIGNALING(82)	Insufficient Shared Memory Pools - Signaling (82) (H.323)	CRITICAL
SIGNALING(83)	Error While Binding to Socket - Signaling (83)	CRITICAL
SIGNALING(84)	Reached Maximum Socket Limit - Signaling (84) (H.323)	CRITICAL
SIGNALING(85)	Initialization Failure - Signaling (85)	CRITICAL
SIGNALING(86)	Remote H323 Gateway is not Reachable - Signaling (86) (H.323)	MAJOR
SIGNALING(87)	H323 Message Parsing Error - Signaling (87) (H.323)	MAJOR
SIGNALING(88)	H323 Message Encoding Error - Signaling (88) (H.323)	MAJOR
SIGNALING(89)	Gatekeeper not Available/Reachable - Signaling (89)	MAJOR
SIGNALING(90)	Alternate Gatekeeper is not Responding - Signaling (90)	MAJOR
SIGNALING(91)	Endpoint Security Violation - Signaling (91) (H.323)	MAJOR
SIGNALING(92)	Invalid Call Identifier - Signaling (92)	MINOR
SIGNALING(93)	Invalid Call Reference Value - Signaling (93)	MINOR
SIGNALING(94)	Invalid Conference Identifier - Signaling (94)	MINOR
SIGNALING(95)	Invalid Message from the Network - Signaling (95)	MINOR
SIGNALING(96)	Internal Call Processing Error - Signaling (96)	MINOR
SIGNALING(97)	Insufficient Information to Complete Call - Signaling (97)	MINOR
SIGNALING(98)	H323 Protocol Inconsistencies - Signaling (98) (H.323)	MINOR
SIGNALING(99)	Abnormal Call Clearing - Signaling (99)	MINOR
SIGNALING(100)	Codec Negotiation Failed - Signaling (100)	MINOR
SIGNALING(101)	Per Call Security Violation - Signaling (101)	MINOR
SIGNALING(102)	H323 Network Congested - Signaling (102) (H.323)	MINOR
SIGNALING(103)	Aggregation Connection Down - Signaling (103)	MAJOR
SIGNALING(104)	Aggregation Unable To Establish Connection - Signaling (104)	INFO
SIGNALING(105)	Aggregation Gate Set Failed - Signaling (105)	INFO
SIGNALING(106)	Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)	MINOR

Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)

Event Type	Event Name	Event Severity
SIGNALING(107)	Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)	CRITICAL
SIGNALING(108)	Simplex Only Operational Mode - Signaling (108)	MAJOR
SIGNALING(109)	Stream Control Transmission Protocol Association Failure - Signaling (109)	MAJOR
SIGNALING(110)	Signaling Gateway Group is Out-of-Service - Signaling (110)	CRITICAL
SIGNALING(111)	Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)	MAJOR
SIGNALING(112)	Stream Control Transmission Protocol Association Configuration Error - Signaling (112)	MINOR
SIGNALING(113)	Signaling Gateway Failure - Signaling (113)	MAJOR
SIGNALING(114)	Signaling Gateway Process is Out-of-Service - Signaling (114)	MAJOR
SIGNALING(115)	Invalid Routing Context Received - Signaling (115)	WARNING
SIGNALING(116)	Destination Point Code User Part Unavailable - Signaling (116)	MAJOR
SIGNALING(117)	Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)	MINOR
SIGNALING(118)	Circuit Verification Response Received with Failed Indication - Signaling (118)	MINOR
SIGNALING(119)	Signaling System 7 Adapter Process Faulty - Signaling (119)	CRITICAL
SIGNALING(120)	Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)	CRITICAL
SIGNALING(121)	Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)	MAJOR
SIGNALING(122)	Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)	MAJOR
SIGNALING(124)	Remote Subsystem is out of Service - Signaling (124)	MINOR
SIGNALING(125)	Signaling Connection Control Part Routing Error - Signaling (125)	MAJOR
SIGNALING(126)	Signaling Connection Control Binding Failure - Signaling (126)	MAJOR
SIGNALING(127)	Transaction Capabilities Application Part Binding Failure - Signaling (127)	MAJOR
SIGNALING(132)	Transaction Capabilities Application Part Reaches the Provisioned Resource Limit - Signaling (132)	WARNING
SIGNALING(133)	Unable to Decode Generic Transport Descriptor Message - Signaling (133)	INFO
SIGNALING(134)	Signaling System 7 Message Encoding Failure - Signaling (134)	INFO
SIGNALING(135)	Signaling System 7 Message Decoding Failure - Signaling (135)	INFO
SIGNALING(136)	Signaling System 7 Message Invalid Received - Signaling (136)	INFO
SIGNALING(137)	Signaling System 7 Confusion Message Received - Signaling (137)	INFO
SIGNALING(138)	Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138)	WARNING
SIGNALING(139)	Signaling System 7 Trunk was Found to be in Erroneous State - Signaling (139) (SS7)	INFO
SIGNALING(140)	Unanswered Information Message - Signaling (140)	INFO
SIGNALING(141)	Address not Resolved by Domain Name System Server - Signaling (141)	WARNING
SIGNALING(142)	Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)	CRITICAL
SIGNALING(143)	Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)	MINOR

Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)

Event Type	Event Name	Event Severity
SIGNALING(144)	All Internet Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)	CRITICAL
SIGNALING(145)	One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)	MINOR
SIGNALING(146)	All Retransmission Attempts of Session Initiation Protocol Request or Response Failed - Signaling (146)	WARNING
SIGNALING(147)	Domain Name System Service Addresses Exhausted - Signaling (147)	WARNING
SIGNALING(148)	Softswitch Audit Released Stale Memory - Signaling (148)	WARNING
SIGNALING(150)	Stream Control Transmission Protocol Association Congested - Signaling (150)	MINOR
SIGNALING(151)	Termination Permanent Error Code Received - Signaling (151)	MINOR
SIGNALING(152)	Termination Transient Error Received - Signaling (152)	INFO
SIGNALING(166)	No Routing Keys are Active - Signal (166)	WARNING
SIGNALING(167)	No Signaling Gateways are Active – Signaling (167)	WARNING

Test Report - Signaling (1)

The Test Report event is for testing the signaling event category. The event is informational and no further action is required.

Invalid Message Received - Signaling (4)

The Invalid Message Received event serves as a warning that an invalid message has been received. The primary cause of the event is that a signaling adapter has received an invalid message from the specified endpoint. To correct the primary cause of the event, monitor the associated signaling link to see if there is an interruption of service on the link. If there is a communication problem, restart the link. Verify that the version of the protocol used by the device at the endpoint is consistent with the version expected by the call agent. If there is a mismatch, then either the endpoint or call agent must be re-provisioned.

Database Module Function Call Failure - Signaling (6)

The Database Module Function Call Failure event serves as a warning that a database module function call has failed. The primary cause of the event is that a signaling adapter has detected an error while accessing a database interface. To correct the primary cause of the event, restart the associated process if the database that the adapter attempted to access is not available. If incompatible versions of the signaling adapter process and the database processes are present on the system, correct the error and restart the processes.

Socket Failure - Signaling (7)

The Socket Failure alarm (major) indicates that there is a failure in creating/binding to the UDP socket. To troubleshoot and correct the cause of the Socket Failure alarm, refer to the "Socket Failure - Signaling (7)" section on page 10-111.

Session Initiation Protocol Message Receive Failure - Signaling (8)

The Session Initiation Protocol Message Receive Failure alarm (major) indicates that a SIP message receive has failed. To troubleshoot and correct the cause of the Session Initiation Protocol Message Receive Failure alarm, refer to the "Session Initiation Protocol Message Receive Failure - Signaling (8)" section on page 10-111.

Timeout on Internet Protocol Address - Signaling (9)

The Timeout on Internet Protocol Address alarm (major) indicates that an IP address has timed out. To troubleshoot and correct the cause of the Timeout on Internet Protocol Address alarm, refer to the "Timeout on Internet Protocol Address - Signaling (9)" section on page 10-112.

Failed to Send Complete Session Initiation Protocol Message - Signaling (10)

The Failed to Send Complete Session Initiation Protocol Message alarm (minor) indicates that a SIP message failure has occurred. To troubleshoot and correct the cause of the Failed to Send Complete Session Initiation Protocol Message alarm, refer to the "Failed to Send Complete Session Initiation Protocol Message - Signaling (10)" section on page 10-112.

Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)

The Failed to Allocate Session Initiation Protocol Control Block alarm (major) indicates that a SIP control block allocation failed. To troubleshoot and correct the cause of the Failed to Allocate Session Initiation Protocol Control Block alarm, refer to the "Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)" section on page 10-112.

Feature Server is not Up or is not Responding to Call Agent - Signaling (12)

The Feature Server is not Up or is not Responding to Call Agent alarm (critical) indicates that the feature server is not up or is not responding to the call agent server. To troubleshoot and correct the cause of the Feature Server is not Up or is not Responding to Call Agent alarm, refer to the "Feature Server is not Up or is not Responding to Call Agent - Signaling (12)" section on page 10-113.

Signaling System 7 Signaling Link Down - Signaling (13)

The Signaling System 7 Signaling Link Down alarm (major) indicates the SS7 signaling link is down. To troubleshoot and correct the cause of the Signaling System 7 Signaling Link Down alarm, refer to the "Signaling System 7 Signaling Link Down - Signaling (13)" section on page 10-114.

Link is Remotely Inhibited - Signaling (14)

The Link is Remotely Inhibited alarm (minor) indicates that the SS7 link is inhibited at the remote end. To troubleshoot and correct the cause of the Link is Remotely Inhibited alarm, refer to the "Link is Remotely Inhibited - Signaling (14)" section on page 10-115.

Link is Locally Inhibited - Signaling (15)

The Link is Locally Inhibited alarm (minor) indicates that the SS7 link is inhibited at the local end. To troubleshoot and correct the cause of the Link is Locally Inhibited alarm, refer to the "Link is Locally Inhibited - Signaling (15)" section on page 10-115.

Link is Congested - Signaling (16)

The Link is Congested alarm (minor) indicates that the SS7 link is congested. To troubleshoot and correct the cause of the Link is Congested alarm, refer to the "Link is Congested - Signaling (16)" section on page 10-115.

Link: Local Processor Outage - Signaling (17)

The Link: Local Processor Outage alarm (minor) indicates that the SS7 link has experienced a local processor outage. To troubleshoot and correct the cause of the Link: Local Processor Outage alarm, refer to the "Link: Local Processor Outage - Signaling (17)" section on page 10-115.

Link: Remote Processor Outage - Signaling (18)

The Link: Remote Processor Outage alarm (minor) indicates that the SS7 link has experienced a remote processor outage. To troubleshoot and correct the cause of the Link: Remote Processor Outage alarm, refer to the "Link: Remote Processor Outage - Signaling (18)" section on page 10-115.

Link Set Inaccessible - Signaling (19)

The Link Set Inaccessible alarm (major) indicates that the specified SS7 link in inaccessible. To troubleshoot and correct the cause of the Link Set Inaccessible alarm, refer to the "Link Set Inaccessible - Signaling (19)" section on page 10-115.

Link Set Congestion - Signaling (20)

The Link Set Congestion alarm (major) indicates that the specified SS7 link set is congested. To troubleshoot and correct the cause of the Link Set Congestion alarm, refer to the "Link Set Congestion - Signaling (20)" section on page 10-116.

Route Set Failure - Signaling (21)

The Route Set Failure alarm (major) indicates that the specified route set has a experienced a failure. To troubleshoot and correct the cause of the Route Set Failure alarm, refer to the "Route Set Failure - Signaling (21)" section on page 10-116.

Route Set Congested - Signaling (22)

The Route Set Congested alarm (minor) indicates that the specified route set is congested. To troubleshoot and correct the cause of the Route Set Congested alarm, refer to the "Route Set Congested - Signaling (22)" section on page 10-116.

Destination Point Code Unavailable - Signaling (23)

The Destination Point Code Unavailable alarm (major) indicates that the specified DPC is not available. To troubleshoot and correct the cause of the Destination Point Code Unavailable alarm, refer to the "Destination Point Code Unavailable - Signaling (23)" section on page 10-117.

Destination Point Code Congested - Signaling (24)

The Destination Point Code Congested alarm (minor) alarm indicates that the specified DPC is congested. To troubleshoot and correct the cause of the Destination Point Code Congested alarm, refer to the "Destination Point Code Congested - Signaling (24)" section on page 10-118.

Unanswered Blocking - Signaling (25)

The Unanswered Blocking event serves as a warning that a BLO message was not answered. The primary cause of the event is that a BLO message was not acknowledged before the T13 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Unanswered Unblocking Message - Signaling (26)

The Unanswered Unblocking Message event serves as a warning that an UBL message was not answered. The primary cause of the event is that a UBL message was not acknowledged before the T15 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Unanswered Circuit Group Blocking - Signaling (27)

The Unanswered Circuit Group Blocking event serves as a warning that a CGB message was not answered. The primary cause of the event is that a CGB message was not acknowledged before the T19 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Unanswered Circuit Group Unblocking - Signaling (28)

The Unanswered Circuit Group Unblocking event serves as a warning that a CGU message was not answered. The primary cause of the event is that a CGU message was not acknowledged before the T21 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Unanswered Circuit Query Message - Signaling (29)

The Unanswered Circuit Query Message event serves as a warning that a CQM message was not answered. The primary cause of the event is that a CQM message was not acknowledged before the T28 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Unanswered Circuit Validation Test - Signaling (30)

The Unanswered Circuit Validation Test event serves as a warning that a CVT message was not answered. The primary cause of the event is that a CVT message was not acknowledged before the Tcvt expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Unanswered Reset Circuit - Signaling (31)

The Unanswered Reset Circuit event serves as a warning that a RSC message was not answered. The primary cause of the event is that a RSC message was not acknowledged before the T17 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Unanswered Group Reset - Signaling (32)

The Unanswered Group Reset event serves as a warning that a GRS message was not answered. The primary cause of the event is that a a GRS message was not acknowledged before the T23 expired for the associated CIC. To correct the primary cause of the event, Verify that the SS7 signaling adapter processes is running normally. verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Unanswered Release - Signaling (33)

The Unanswered Release event serves as a warning that a REL message was not answered. The primary cause of the event is that a REL message was not acknowledged before the T5 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Unanswered Continuity Check Request - Signaling (34)

The Unanswered Continuity Check Request event serves as a warning that a continuity check request (CCR) message was not answered. The primary cause of the event is that a LPA message was not acknowledged before the T_{CCR} expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

Trunk Locally Blocked - Signaling (36)

The Trunk Locally Blocked alarm (minor) indicates that the trunk is locally blocked. To troubleshoot and correct the cause of the Trunk Locally Blocked alarm, refer to the "Trunk Locally Blocked - Signaling (36)" section on page 10-118. For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x."

Trunk Remotely Blocked - Signaling (40)

The Trunk Remotely Blocked alarm (major) indicates that the trunk is remotely blocked. To troubleshoot and correct the cause of the Trunk Remotely Blocked alarm, refer to the "Trunk Remotely Blocked - Signaling (40)" section on page 10-118.

Continuity Testing Message Received on the Specified Circuit Identification Code - Signaling (42)

The Continuity Testing Message Received on the Specified Circuit Identification Code event functions as an informational alert that the COT message was received on the specified CIC. The event is informational and no further action is required.

Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code - Signaling (43)

The Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code event functions as an informational alert that the RLC was received in response to the RSC message received on the specified CIC. The event is informational and no further action is required,

Continuity Recheck is Performed on Specified Circuit Identification Code - Signaling (44)

The Continuity Recheck is Performed on Specified Circuit Identification Code event functions as an informational alert that a continuity recheck was performed on the specified CIC. The event is informational and further action is required.

Circuit is UNEQUIPPED on Remote Side - Signaling (45)

The Circuit is UNEQUIPPED on Remote Side event functions as an informational alert the circuit is unequipped on the remote side. The primary cause of the event is that an unequipped circuit has been detected on the remote side. To correct the primary cause of the event, monitor the event reports at the network level to verify if an existing circuit was unequipped causing a status mismatch with the local end.

Specified Circuit Identification Code is Invalid for the Operation - Signaling (46)

The Specified Circuit Identification Code is Invalid for the Operation event functions as an informational alert that the specified CIC in invalid for the attempted operation. The primary cause of the event is that an invalid operation was performed on the specified CIC. To correct the primary cause of the event, verify that the SS7 provisioning tables are properly configured at the circuit level.

A General Processing Error Encountered - Signaling (49)

The A General Processing Error Encountered event functions as a informational alert that a general processing error has occurred. The primary cause of the event is that a general SS7 processing error occurred due to all resources being busy or an invalid event occurring. To correct the primary cause of the event, verify the status of the signaling adapter process and the SS7 signaling interface to verify proper operation.

Unexpected Message for the Call State is Received: Clear Call - Signaling (50)

The Unexpected Message for the Call State is Received: Clear Call event functions as an informational alert that an unexpected message for the call state has been received. The primary cause of the even is that an unexpected message was received for the current call state. To correct the primary cause of the event, verify the status of the signaling adapter process and the SS7 signaling interface to verify proper operation.

Set Trunk State as Remotely Unequipped - Signaling (51)

The Set Trunk State as Remotely Unequipped event functions as an informational alert that the trunk state is currently set as remotely unequipped. The primary cause of the event is that the specified CIC is marked at remotely unequipped due to the CQM response indicating that it is unequipped at the far end. To correct the primary cause of the event, equip the trunk circuit at the far end.

Set Trunk State as NOT Remotely Blocked - Signaling (52)

The Set Trunk State as NOT Remotely Blocked event functions as an informational alert that the trunk state has been set as not remotely blocked. The primary cause of the event is that the specified CIC is marked as not remotely blocked due to the CQM response indicating that it is not remotely blocked at the far end. The event is informational and no further action is required.

Set Trunk State as Remotely Blocked - Signaling (53)

The Set Trunk State as Remotely Blocked event functions as an informational alert that the trunk state is set as remotely blocked. The primary cause of the event is that the specified CIC is marked as remotely blocked due to the CQM response indicating that it is remotely blocked at the far end. To correct the primary cause of the event, clear the blocking situation at the far end based on network level event reports.

Circuit Validation Test Aborted - Signaling (54)

The Circuit Validation Test Aborted event functions as an informational alert that the circuit validation test has been aborted. The primary cause of the event is that the circuit specified failed a validation test due to an internal failure. To correct the primary cause of the event, verify the SS7 signaling adapter process and SS7 interface is operating normally.

Circuit Validation Successful - Signaling (55)

The Circuit Validation Successful event functions as an informational alert that the circuit validation was successful. The event is informational and no further actions is required.

Continuity Recheck Failed - Signaling (57)

The Continuity Recheck Failed event functions as an informational alert that the continuity recheck failed. The primary cause of the event is that a continuity recheck of the specified CIC failed. To correct the primary cause of the event, verify the SS7 signaling adapter process and SS7 interface is operating normally.

Continuity Recheck Successful - Signaling (58)

The Continuity Recheck Successful event functions as an informational alert that the continuity recheck of the specified CIC was successful. The event is informational and no further action is required.

Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)

The Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway alarm (major) indicates that specified ISDN trunk group status was changed due to a media gateway operation. To troubleshoot and correct the cause of the Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway alarm, refer to the "Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)" section on page 10-118.

Integrated Services Digital Network STATUS Message Containing Error Indication Received - Signaling (60)

The Integrated Services Digital Network STATUS Message Containing Error Indication Received event functions as a warning that an ISDN status message containing an error indication has been received. The primary cause of the event is that an ISDN status message was received containing an error indication for the specified termination. To correct the primary cause of the event, place the specified termination in service state if the specified termination is not operating normally.

Trunk Operational State Changed by Service Message - Signaling (61)

The Trunk Operational State Changed by Service Message event functions as an informational alert that the trunk operational state was changed by a service message. The primary cause of the event is that the specified trunk group operational status was changed via a service message from the specified gateway. To correct the primary cause of the event, monitor the event reports at the network level to verify that the specified gateway and terminations are operating normally.

Received Integrated Services Digital Network RESTART Message - Signaling (62)

The Received Integrated Services Digital Network RESTART Message event functions as an informational alert that a ISDN restart message was received. The primary cause of the event is that an ISDN restart message was received from the specified gateway. To correct the primary cause of the event, monitor the event reports at the network level to verify that the specified gateway and terminations are operating normally.

Media Gateway/Termination Faulty - Signaling (63)

The Media Gateway/Termination Faulty alarm (major) indicates that a media gateway or termination has gone faulty due to the detection of an unknown endpoint, unknown package type, and unknown event, a hardware failure, or a general call agent error. To troubleshoot and correct the cause of the Media Gateway/Termination Faulty alarm, refer to the "Media Gateway/Termination Faulty - Signaling (63)" section on page 10-119.

Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)

The Media Gateway Adapter Running out of Shared Memory Pools alarm (critical) indicates that the MGCP signaling adapter was unable to allocate data store for an IPC message due to a lack of resources. To troubleshoot and correct the cause of the Media Gateway Adapter Running out of Shared Memory Pools alarm, refer to the "Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)" section on page 10-119.

Media Gateway Adapter Running out of Heap Memory - Signaling (65)

The Media Gateway Adapter Running out of Heap Memory alarm (critical) indicates that the MGCP signaling adapter was unable to allocate data store for an IPC message from the heap due to a lack of resources. To troubleshoot and correct the cause of the Media Gateway Adapter Running out of Heap Memory alarm, refer to the "Media Gateway Adapter Running out of Heap Memory - Signaling (65)" section on page 10-119.

Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)

The Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) alarm (major) indicates that a call agent internal error has occurred causing the restart of the MGCP signaling adapter. To troubleshoot and correct the cause of the Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) alarm, refer to the "Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)" section on page 10-119.

Media Gateway Endpoints are out of Service at Gateway - Signaling (68)

The Media Gateway Endpoints are out of Service at Gateway alarm (major) indicates that the media gateway endpoints are out of service at the GW. To troubleshoot and correct the cause of the Media Gateway Endpoints are out of Service at Gateway alarm, refer to the "Media Gateway Endpoints are out of Service at Gateway - Signaling (68)" section on page 10-119.

Call Agent and Feature Server Communication Message Timeout - Signaling (69)

The Call Agent and Feature Server Communication Message Timeout alarm (critical) indicates that a CA and FS communications message timed out. To troubleshoot correct the cause of the Call Agent and Feature Server Communication Message Timeout alarm, refer to the "Call Agent and Feature Server Communication Message Timeout - Signaling (69)" section on page 10-120.

Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication - Signaling (70)

The Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication event serves as a warning that the ISDN signaling adapter is unable to restore D-channel due to a communication failure. The primary cause of the event is that the ISDN signaling adapter is unable to restore a D-channel due to incorrect backhaul provisioning at the media gateway or call agent. To correct the primary cause of the event, ensure the provisioning of the backhaul port is correct at both the call agent and media gateway.

Integrated Services Digital Network Unable to Establish D-channel - Signaling (71)

The Integrated Services Digital Network Unable to Establish D-channel event serves as a warning that the ISDN signaling adaptor is unable to establish D-channel. The primary cause of the event is that ISDN signaling adapter is unable to establish a D-channel due to layer 1 parameters not being provisioned correctly or improper provisioning of the network or user side. To correct the primary cause of the event, verify the correct provisioning at the media gateway.

Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time - Signaling (72)

The Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time event serves as a warning that calls were lost due to the D-channels being down for a period of time. The primary cause of the event is that ISDN signaling adapter has lost calls due to a D-channel being down as a result of a media gateway power loss or a loss of connection between the PBX and media gateway. To correct the primary cause of the event, resupply power to the media gateway and verify that the connection between the PBX and media gateway is intact.

Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired - Signaling (73)

The Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired event serves as a warning that the ISDN signaling adapter was unable to send a restart due to the restart timer being expired. The primary cause of the event is that the ISDN signaling adapter was unable to send a RESTART message due to the expiration of the RESTART timer. To correct the primary cause of the event, verify that the RESTART timer is set to an appropriate level.

Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired - Signaling (74)

The Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired event serves as a warning that the ISDN signal adapter was unable to send a service message due to the service timer being expired. The primary cause of the event is that the ISDN signaling adapter was unable to send a SERVICE message due to the expiration of the SERVICE timer. To correct the primary cause of the event, ensure that the RESTART timer is set to an appropriate level.

Signaling System 7 Stack not Ready - Signaling (75)

The Signaling System 7 Stack not Ready alarm (critical) indicates that the SS7 stack in not ready. To trouble and correct the cause of the Signaling System 7 Stack not Ready alarm, refer to the "Signaling System 7 Stack not Ready - Signaling (75)" section on page 10-120.

Timeout on Remote Instance - Signaling (76)

The Timeout on Remote Instance event functions as an informational alert that communication on a remote instance timed out. The primary cause of the event is that communication between call agent and remote instance is faulty. The event is informational and no further action is required.

Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling - Signaling (77)

The Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling event functions as an informational alert that an ISDN D-channel switchover has occurred non-facility associated signaling (NFAS). The primary cause of the event is that the operator manually switched the D-channels using the CLI. To verify the primary cause of the event, verify operator action. The secondary cause of the event is that the active D-channel was lost. To correct the secondary cause of the event, verify that gateway is operational and connection to PBX is good.

Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)

The Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling alarm (minor) indicates that one of the ISDN D-channels in the PRI is down. To troubleshoot and correct the cause of the Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling alarm, refer to the "Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)" section on page 10-120.

Media Gateway Unreachable - Signaling (79)

The Media Gateway Unreachable alarm (major) indicates that the media gateway is unreachable. To troubleshoot and correct the cause of the Media Gateway Unreachable alarm, refer to the "Media Gateway Unreachable - Signaling (79)" section on page 10-120. For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x."

Out of Bounds, Memory/Socket Error - Signaling (80)

The Out of Bounds, Memory/Socket Error alarm (critical) indicates that a memory socket out of bounds error has occurred. To troubleshoot and correct the cause of the Out of Bounds, Memory/Socket Error alarm, refer to the "Out of Bounds, Memory/Socket Error - Signaling (80)" section on page 10-120.

Insufficient Heap Memory - Signaling (81) (H.323)

The Insufficient Heap Memory alarm (critical) indicates that there is insufficient heap memory. To troubleshoot and correct the cause of the Insufficient Heap Memory alarm, refer to the "Insufficient Heap Memory - Signaling (81) (H.323)" section on page 10-121.

Insufficient Shared Memory Pools - Signaling (82) (H.323)

The Insufficient Shared Memory Pools alarm (critical) indicates that there is insufficient shared memory pools. To troubleshoot and correct the cause of the Insufficient Shared Memory Pools alarm, refer to the "Insufficient Shared Memory Pools - Signaling (82) (H.323)" section on page 10-121.

Error While Binding to Socket - Signaling (83)

The Error While Binding to Socket alarm (critical) indicates that an error occurred while binding to the socket. To troubleshoot and correct the cause of the Error While Binding to Socket alarm, refer to the "Error While Binding to Socket - Signaling (83)" section on page 10-121.

Reached Maximum Socket Limit - Signaling (84) (H.323)

The Reached Maximum Socket Limit alarm (critical) indicates that the Cisco BTS 10200 Softswitch system has reached the maximum socket limit. To troubleshoot and correct the cause of the Reached Maximum Socket Limit alarm, refer to the "Reached Maximum Socket Limit - Signaling (84) (H.323)" section on page 10-121.

Initialization Failure - Signaling (85)

The Initialization Failure alarm (critical) indicates that the Cisco BTS 10200 Softswitch system failed to initialize. To troubleshoot and correct the cause of the Initialization Failure alarm, refer to the "Initialization Failure - Signaling (85)" section on page 10-121.

Remote H323 Gateway is not Reachable - Signaling (86) (H.323)

The Remote H323 Gateway is not Reachable alarm (major) indicates that the remote H323 gateway is not reachable. To troubleshoot and correct the cause of the Remote H323 Gateway is not Reachable alarm, refer to the "Remote H323 Gateway is not Reachable - Signaling (86) (H.323)" section on page 10-121.

H323 Message Parsing Error - Signaling (87) (H.323)

The H323 Message Parsing Error alarm (major) indicates that a H323 message parsing error has occurred. To troubleshoot and correct the cause of the H323 Message Parsing Error alarm, refer to the "H323 Message Parsing Error - Signaling (87) (H.323)" section on page 10-122.

H323 Message Encoding Error - Signaling (88) (H.323)

The H323 Message Encoding Error alarm (major) indicates that a H323 message encoding error has occurred. To troubleshoot and correct the cause of the H323 Message Encoding Error alarm, refer to the "H323 Message Encoding Error - Signaling (88) (H.323)" section on page 10-122.

Gatekeeper not Available/Reachable - Signaling (89)

The Gatekeeper not Available/Reachable alarm (major) indicates that the gatekeeper is not available or the gatekeeper is not reachable. To troubleshoot and correct the cause of the Gatekeeper not Available/Reachable alarm, refer to the "Gatekeeper not Available/Reachable - Signaling (89)" section on page 10-122.

Alternate Gatekeeper is not Responding - Signaling (90)

The Alternate Gatekeeper is not Responding alarm (major) indicates that the alternate gatekeeper is not responding. To troubleshoot and correct the cause of the Alternate Gatekeeper is not Responding alarm, refer to the "Alternate Gatekeeper is not Responding - Signaling (90)" section on page 10-122.

Endpoint Security Violation - Signaling (91) (H.323)

The Endpoint Security Violation alarm (major) indicates that an H323 security violation has occurred. To troubleshoot and correct the cause of the Endpoint Security Violation alarm, refer to the "Endpoint Security Violation - Signaling (91) (H.323)" section on page 10-123.

Invalid Call Identifier - Signaling (92)

The Invalid Call Identifier alarm (minor) indicates that the Call ID was invalid or changed mid-call. To troubleshoot and correct the cause of the Invalid Call Identifier alarm, refer to the "Invalid Call Identifier - Signaling (92)" section on page 10-123.

Invalid Call Reference Value - Signaling (93)

The Invalid Call Reference Value alarm (minor) indicates that the Call ID was invalid or changed mid-call. To troubleshoot and correct the cause of the Invalid Call Reference Value alarm, refer to the "Invalid Call Reference Value - Signaling (93)" section on page 10-123.

Invalid Conference Identifier - Signaling (94)

The Invalid Conference Identifier alarm (minor) indicates that the Call ID was invalid or changed mid-call. To troubleshoot and correct the cause of the Invalid Conference Identifier alarm, refer to the "Invalid Conference Identifier - Signaling (94)" section on page 10-123.

Invalid Message from the Network - Signaling (95)

The Invalid Message from the Network alarm (minor) indicates that an unsupported or invalid message type was received from network. To troubleshoot and correct the cause of the Invalid Message from the Network alarm, refer to the "Invalid Message from the Network - Signaling (95)" section on page 10-123.

Internal Call Processing Error - Signaling (96)

The Internal Call Processing Error alarm (minor) indicates that an internal call processing error has occurred. To troubleshoot and correct the cause of the Internal Call Processing Error alarm, refer to the "Internal Call Processing Error - Signaling (96)" section on page 10-124.

Insufficient Information to Complete Call - Signaling (97)

The Insufficient Information to Complete Call alarm (minor) indicates that there was insufficient information to complete a call. To troubleshoot and correct the cause of the Insufficient Information to Complete Call alarm, refer to the "Insufficient Information to Complete Call - Signaling (97)" section on page 10-124.

H323 Protocol Inconsistencies - Signaling (98) (H.323)

The H323 Protocol Inconsistencies alarm (minor) indicates that the H323 endpoint and Cisco BTS 10200 Softswitch are running different protocol versions. To troubleshoot and correct the cause of the H323 Protocol Inconsistencies alarm, refer to the "H323 Protocol Inconsistencies - Signaling (98) (H.323)" section on page 10-124.

Abnormal Call Clearing - Signaling (99)

The Abnormal Call Clearing alarm (minor) indicates that an unsupported or invalid message type was received from network. To troubleshoot and correct the cause of the Abnormal Call Clearing alarm, refer to the "Abnormal Call Clearing - Signaling (99)" section on page 10-124.

Codec Negotiation Failed - Signaling (100)

The Codec Negotiation Failed alarm (minor) indicates that the codec negotiation has failed. To troubleshoot and correct the cause of the Codec Negotiation Failed alarm, refer to the "Codec Negotiation Failed - Signaling (100)" section on page 10-124.

Per Call Security Violation - Signaling (101)

The Per Call Security Violation alarm (minor) indicates that a call security violation has occurred. To troubleshoot and correct the cause of the Per Call Security Violation alarm, refer to the "Per Call Security Violation - Signaling (101)" section on page 10-124.

H323 Network Congested - Signaling (102) (H.323)

The H323 Network Congested alarm indicates (minor) that the H323 application process has depleted its resources and no more calls can be completed. To troubleshoot and correct the cause of the H323 Network Congested alarm, refer to the "H323 Network Congested - Signaling (102) (H.323)" section on page 10-125.

Aggregation Connection Down - Signaling (103)

The Aggregation Connection Down alarm (major) indicates that the aggregation (AGGR) TCP connection is down. To troubleshoot and correct the cause of the Aggregation Connection Down alarm, refer to the "Aggregation Connection Down - Signaling (103)" section on page 10-125.

Aggregation Unable To Establish Connection - Signaling (104)

The Aggregation Unable To Establish Connection event functions as an informational alert that the AGGR is unable to establish a connection. The primary cause of the event is that the TCP connection failed to establish. To correct the primary cause of the event, check the IP Connectivity of CA and CMTS.

Aggregation Gate Set Failed - Signaling (105)

The Aggregation Gate Set Failed event functions as an informational alert that the AGGR gate set failed. The primary cause of the event is that the gate set acknowledgement never came from the CMTS. The event is informational and no further action is required.

Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)

The Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down alarm (minor) indicates that the enhanced subscriber authentication (ESA) Cisco BTS 10200 Softswitch DF connection is down. To troubleshoot and correct the cause of the Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down alarm, refer to the "Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)" section on page 10-125.

Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)

The Logical Internet Protocol Addresses not Mapped Correctly alarm (critical) indicates that the logical IP addresses are not mapped correctly. To troubleshoot and correct the cause of the Logical Internet Protocol Addresses not Mapped Correctly alarm, refer to the "Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)" section on page 10-125.

Simplex Only Operational Mode - Signaling (108)

The Simplex Only Operational Mode alarm (major) indicates that the Cisco BTS 10200 Softswitch system can only operate in the simplex mode. To troubleshoot and correct the cause of the Simplex Only Operational Mode alarm, refer to the "Simplex Only Operational Mode - Signaling (108)" section on page 10-126.

Stream Control Transmission Protocol Association Failure - Signaling (109)

The Stream Control Transmission Protocol Association Failure alarm (major) indicates that the SCTP association failed. To troubleshoot and correct the cause of the Stream Control Transmission Protocol Association Failure alarm, refer to the "Stream Control Transmission Protocol Association Failure - Signaling (109)" section on page 10-126.

Signaling Gateway Group is Out-of-Service - Signaling (110)

The Signaling Gateway Group is Out-of-Service alarm (major) indicates that the signaling gateway group is out-of-service. To troubleshoot and correct the cause of the Signaling Gateway Group is Out-of-Service alarm, refer to the "Signaling Gateway Group Is Out-of-Service - Signaling (110)" section on page 10-130.

Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)

The Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) alarm (major) indicates that the SCTP association is degraded. To troubleshoot and correct the cause of the Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) alarm, refer to the "Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)" section on page 10-130.

Stream Control Transmission Protocol Association Configuration Error - Signaling (112)

The Stream Control Transmission Protocol Association Configuration Error alarm (minor) indicates that a SCTP association configuration error has occurred. To troubleshoot and correct the cause of the Stream Control Transmission Protocol Association Configuration Error alarm, refer to the "Stream Control Transmission Protocol Association Configuration Error - Signaling (112)" section on page 10-130.

Signaling Gateway Failure - Signaling (113)

The Signaling Gateway Failure alarm (major) indicates that all associated signaling gateway processes are out-of-service. To troubleshoot and correct the cause of the Signaling Gateway Failure alarm, refer to the "Signaling Gateway Failure - Signaling (113)" section on page 10-131.

Signaling Gateway Process is Out-of-Service - Signaling (114)

The Signaling Gateway Process is Out-of-Service alarm (major) indicates that all SCTP associations between the SGP and the CA are out-of-service. To troubleshoot and correct the cause of the Signaling Gateway Process is Out-of-Service alarm, refer to the "Signaling Gateway Process Is Out-of-Service - Signaling (114)" section on page 10-131.

Invalid Routing Context Received - Signaling (115)

The Invalid Routing Context Received event serves as a warning that an invalid routing context was received. The primary cause of the event is that the routing context was configured improperly on the CA or the SG. To correct the primary cause of the event, reconfigure the routing context on the CA or the SG so that the routing context matches in both places.

Destination Point Code User Part Unavailable - Signaling (116)

The Destination Point Code User Part Unavailable alarm (major) indicates that a layer 4 user part, such as ISUP, is unavailable at the DPC in the SS7 network. To troubleshoot and correct the cause of the Destination Point Code User Part Unavailable alarm, refer to the "Destination Point Code User Part Unavailable - Signaling (116)" section on page 10-132.

Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)

The Circuit Validation Test Message Received for an Unequipped Circuit Identification Code alarm (minor) indicates that a CVT message was received for an unequipped CIC. To troubleshoot and correct the cause of the Circuit Validation Test Message Received for an Unequipped Circuit Identification Code alarm, refer to the "Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)" section on page 10-132.

Circuit Verification Response Received with Failed Indication - Signaling (118)

The Circuit Verification Response Received with Failed Indication alarm (minor) indicates that a circuit verification response (CVR) message was received with a failure indication. To troubleshoot and correct the cause of the Circuit Verification Response Received with Failed Indication alarm, refer to the "Circuit Verification Response Received with Failed Indication - Signaling (118)" section on page 10-132.

Signaling System 7 Adapter Process Faulty - Signaling (119)

The Signaling System 7 Adapter Process Faulty alarm (critical) indicates that a S7A process is faulty. To troubleshoot and correct the cause of the Signaling System 7 Adapter Process Faulty alarm, refer to the "S7A Process Faulty - Signaling (119)" section on page 10-116.

Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)

The Signaling System 7 Module/Signaling System 7 Adapter Faulty alarm (critical) indicates that the S7M/S7A processes are faulty. To troubleshoot and correct the cause of the Signaling System 7 Module/Signaling System 7 Adapter Faulty alarm, refer to the "S7M/S7A Faulty - Signaling (120)" section on page 10-116.

Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)

The Message Transfer Part 3 User Adapter Cannot Go Standby alarm (major) indicates that the M3UA process cannot go into standby mode. To troubleshoot and correct the cause of the Message Transfer Part 3 User Adapter Cannot Go Standby alarm, refer to the "Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)" section on page 10-133.

Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)

The Message Transfer Part 3 User Adapter Cannot Go Active alarm (major) indicates that the M3UA process cannot go into active mode. To troubleshoot and correct the cause of the Message Transfer Part 3 User Adapter Cannot Go Active alarm, refer to the "Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)" section on page 10-133.

Remote Subsystem is out of Service - Signaling (124)

The Remote Subsystem is out of Service alarm (minor) indicates that the remote subsystem is out-of-service. To troubleshoot and correct the cause of the Remote Subsystem is out of Service alarm, refer to the "Remote Subsystem is Out Of Service - Signaling (124)" section on page 10-133.

Signaling Connection Control Part Routing Error - Signaling (125)

The Signaling Connection Control Part Routing Error alarm (major) indicates that the SCCP route was invalid or not available. To troubleshoot and correct the cause of the Signaling Connection Control Part Routing Error alarm, refer to the "Signaling Connection Control Part Routing Error - Signaling (125)" section on page 10-133.

Signaling Connection Control Binding Failure - Signaling (126)

The Signaling Connection Control Binding Failure alarm (major) indicates that the SCCP binding failed. To troubleshoot and correct the cause of the Signaling Connection Control Binding Failure alarm, refer to the "Signaling Connection Control Part Binding Failure - Signaling (126)" section on page 10-134.

Transaction Capabilities Application Part Binding Failure - Signaling (127)

The Transaction Capabilities Application Part Binding Failure alarm (major) indicates that the TCAP binding failed. To troubleshoot and correct the cause of the Transaction Capabilities Application Part Binding Failure alarm, refer to the "Transaction Capabilities Application Part Binding Failure - Signaling (127)" section on page 10-134.

Transaction Capabilities Application Part Reaches the Provisioned Resource Limit - Signaling (132)

The Transaction Capabilities Application Part Reaches the Provisioned Resource Limit event serves as a warning that the TCAP process has reached or reaches the provisioned resource limit. The primary cause of the event is that the TCAP process runs out of all of the pre-configured dialogue IDs or invoke IDs. To correct the primary cause of the event, increase the number pre-configured dialogue IDs or invoke IDs.

Unable to Decode Generic Transport Descriptor Message - Signaling (133)

The Unable to Decode Generic Transport Descriptor Message event functions as an informational alert that a GTD message could not be decoded. The primary cause of the event is that the GTD parser failed to decode a GTD message received from the specified endpoint. To correct the primary cause of the event, verify that the version of the GTD protocol used by the device at the remote endpoint is consistent with the version expected by the call agent. Examine the associated signaling link to see if there is any interruption of the supplementary services on the link.

Signaling System 7 Message Encoding Failure - Signaling (134)

The Signaling System 7 Message Encoding Failure event functions as an informational alert that a SS7 message encoding failed. The primary cause of the event is that there was an error in the ISUP stack or the SAI message. To correct the primary cause of the event, capture a SS7 trace of the circuit for examination by Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Signaling System 7 Message Decoding Failure - Signaling (135)

The Signaling System 7 Message Decoding Failure event functions as an informational alert that the decoding of a SS7 message failed. The primary cause of the event is that an error occurred in the ISUP stack or the SAI message. To correct the primary cause of the event, capture a SS7 trace of the circuit for examination by Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Signaling System 7 Message Invalid Received - Signaling (136)

The Signaling System 7 Message Invalid Received event functions as an informational alert that an invalid SS7 message was received. The primary cause of the event is that an invalid message was received from the line in the ISUP stack. To correct the primary cause of the event, verify the SSP sending the message to the CA is correctly configured. Capture a SS7 trace of the circuit for examination by Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Signaling System 7 Confusion Message Received - Signaling (137)

The Signaling System 7 Confusion Message Received event functions as an informational alert that the received SS7 message was confused. The primary cause of the event is that an ISUP message or parameter received was not recognized or understood. To correct the primary cause of the event, check the log for more information (including CFN diagnostic output). Capture SS7 trace of affected circuits. If diagnostic data indicates messages/parameters that must be supported are being dropped, refer the captured data to Cisco TAC along with a description of the call scenario. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138)

The Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit event functions as an informational alert that the number of open SIP connections is reaching the engineered limit. The primary cause of the event is that the call failed or a feature is not available. To correct the primary cause of the event, is to increase the engineered limit to allow for more open connections. System configuration and traffic load have caused the number of open connections to approach the

engineered limit. Contact Cisco TAC for assistance in increasing in the limit. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Signaling System 7 Trunk was Found to be in Erroneous State - Signaling (139) (SS7)

The Signaling System 7 Trunk was Found to be in Erroneous State event functions as an informational alert that a SS7 trunk was found to be in an erroneous state. The primary cause of the event is that a discrepancy exists between the local and the remote trunk states. The corrective action is automatically enforced when using ANSI ISUP.

Unanswered Information Message - Signaling (140)

The Unanswered Information Message event functions as an informational alert that an INF message has not been answered. The primary cause of the event is that the far-end switch is not responding to INF message with an INR message. To correct the primary cause of the event, verify that the far-end switch can correctly respond to an INF message.

Address not Resolved by Domain Name System Server - Signaling (141)

The Address not Resolved by Domain Name System Server event serves as a warning that an address was not resolved by the DNS server. The primary cause of the event is that the TSAP address/hostname is not defined in the DNS. To correct the primary cause of the event, add an entry for TSAP address to the DNS server or fix the Cisco BTS 10200 Softswitch provisioning.

Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)

The Session Initiation Protocol Trunk Operationally Out-of-Service alarm (critical) indicates that the SIP trunk is operationally out-of-service. To troubleshoot and correct the cause of the Session Initiation Protocol Trunk Operationally Out-of-Service alarm, refer to the "Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)" section on page 10-134.

Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)

The Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down alarm (minor) indicates that an IP interface link to the SS7 signaling gateway is down. To troubleshoot and correct the cause of the Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down alarm, refer to the "Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)" section on page 10-134.

All Internet Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)

The All Internet Interface Links to Signaling System 7 Signaling Gateway are Down alarm (critical) indicates that all IP interface links to the SS7 signaling gateway are down. To troubleshoot and correct the cause of the All Internet Interface Links to Signaling System 7 Signaling Gateway are Down alarm, refer to the "All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)" section on page 10-134.

One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)

The One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down alarm (minor) indicates that one IP interface link to the SS7 signaling gateway is down. To troubleshoot and correct the cause of the One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down alarm, refer to the "One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)" section on page 10-135.

All Retransmission Attempts of Session Initiation Protocol Request or Response Failed - Signaling (146)

The All Retransmission Attempts of Session Initiation Protocol Request or Response Failed event serves as a warning the all retransmission attempts of a SIP request or response failed. The primary cause of the event is that all retransmission attempts for a SIP request failed for a DNS or an IP address of the request URI or all retransmission attempts for a SIP response failed for the received socket IP address of the request and the DNS (or IP address). To correct the primary cause of the event, ensure that the DNS server is up and running for host name resolution and provisioned properly to resolve to correct order of IP addresses and ensure that previous hop network component is alive and in a healthy state for failures related to SIP responses.

Domain Name System Service Addresses Exhausted - Signaling (147)

The Domain Name System Service Addresses Exhausted event serves as a warning that all DNS SRV addresses are exhausted. The primary cause of the event is that the DNS SRV hostname resolution to IP address is exhausted. To correct the primary cause of the event, add an entry to the SRV in the DNS server and fix the Cisco BTS 10200 Softswitch provisioning.

Softswitch Audit Released Stale Memory - Signaling (148)

The Softswitch Audit Released Stale Memory event serves as a warning that an audit released stale memory event has occurred. The primary cause of the event is that a loss of communication with originating or terminating side has occurred. To correct the primary cause of the event, check to see if adjacent network element is up and having proper communication link with the BTS 10200 Softswitch. The secondary cause of the event is that an adjacent network device has had a protocol error. To correct the secondary cause of the event, check the adjacent network device protocol for compatibility. The ternary cause of the event is that an internal software error has occurred. To correct the ternary cause of the event, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Stream Control Transmission Protocol Association Congested - Signaling (150)

The Stream Control Transmission Protocol Association Congested alarm (minor) indicates that the SCTP association is congested. To troubleshoot and correct the cause of the Stream Control Transmission Protocol Association Congested alarm, refer to the "Stream Control Transmission Protocol Association Congested - Signaling (150)" section on page 10-135.

Termination Permanent Error Code Received - Signaling (151)

The Termination Permanent Error Code Received alarm (minor) indicates that a termination permanent error code was received. To troubleshoot and correct the cause of the Termination Permanent Error Code Received alarm, refer to the "Termination Permanent Error Code Received - Signaling (151)" section on page 10-135.

Termination Transient Error Received - Signaling (152)

The Termination Transient Error Received event functions as an informational alert that a termination transient error was received. The primary cause of the event that the MGCP signaling process has inter-operational errors. To correct the primary cause of the event, notify Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

No Routing Keys are Active - Signal (166)

The No Routing Keys are Active event serves as a warning that no routing keys are active. The primary cause of the event is that the routing keys are not controlled into ACTIVE state. To correct the primary cause of the event, control the routing keys to the ACTIVE state. The secondary cause of the event is that the ITP provisioning is incorrect. To correct the secondary cause of the event, check the ITP provisioning.

No Signaling Gateways are Active – Signaling (167)

The No Signaling Gateways are Active event serves as a warning that no signaling gateways are active. The primary cause of the event is that there is a communication problem between ITP and the Cisco BTS 10200 Softswitch. To correct the primary cause of the event, check the communication path between Cisco BTS 10200 Softswitch and the ITP.

Troubleshooting Signaling Alarms

This section provides the information needed to monitor and correct Signaling alarms. Table 10-3 lists all Signaling alarms in numerical order and provides cross reference to each subsection in this section.

Table 10-3 Cisco BTS 10200 Softswitch Signaling Alarms

Alarm Type	Alarm Name	Alarm Severity
SIGNALING(7)	Socket Failure - Signaling (7)	MAJOR
SIGNALING(8)	Session Initiation Protocol Message Receive Failure - Signaling (8)	MAJOR
SIGNALING(9)	Timeout on Internet Protocol Address - Signaling (9)	MAJOR
SIGNALING(10)	Failed to Send Complete Session Initiation Protocol Message - Signaling (10)	MINOR
SIGNALING(11)	Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)	MAJOR
SIGNALING(12)	Feature Server is not Up or is not Responding to Call Agent - Signaling (12)	CRITICAL
SIGNALING(13)	Signaling System 7 Signaling Link Down - Signaling (13)	MAJOR
SIGNALING(14)	Link is Remotely Inhibited - Signaling (14)	MINOR
SIGNALING(15)	Link is Locally Inhibited - Signaling (15)	MINOR
SIGNALING(16)	Link is Congested - Signaling (16)	MINOR
SIGNALING(17)	Link: Local Processor Outage - Signaling (17)	MINOR
SIGNALING(18)	Link: Remote Processor Outage - Signaling (18)	MINOR
SIGNALING(19)	Link Set Inaccessible - Signaling (19)	MAJOR
SIGNALING(20)	Link Set Congestion - Signaling (20)	MAJOR
SIGNALING(21)	Route Set Failure - Signaling (21)	MAJOR
SIGNALING(22)	Route Set Congested - Signaling (22)	MINOR
SIGNALING(23)	Destination Point Code Unavailable - Signaling (23)	MAJOR
SIGNALING(24)	Destination Point Code Congested - Signaling (24)	MINOR
SIGNALING(36)	Trunk Locally Blocked - Signaling (36)	MINOR
SIGNALING(40)	Trunk Remotely Blocked - Signaling (40)	MAJOR
SIGNALING(59)	Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)	MAJOR
SIGNALING(63)	Media Gateway/Termination Faulty - Signaling (63)	MAJOR
SIGNALING(64)	Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)	CRITICAL
SIGNALING(65)	Media Gateway Adapter Running out of Heap Memory - Signaling (65)	CRITICAL
SIGNALING(66)	Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)	MAJOR
SIGNALING(68)	Media Gateway Endpoints are out of Service at Gateway - Signaling (68)	MAJOR
SIGNALING(69)	Call Agent and Feature Server Communication Message Timeout - Signaling (69)	CRITICAL
SIGNALING(75)	Signaling System 7 Stack not Ready - Signaling (75)	CRITICAL
SIGNALING(78)	Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)	MINOR
SIGNALING(79)	Media Gateway Unreachable - Signaling (79)	MAJOR

Table 10-3 Cisco BTS 10200 Softswitch Signaling Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
SIGNALING(80)	Out of Bounds, Memory/Socket Error - Signaling (80)	CRITICAL
SIGNALING(81)	Insufficient Heap Memory - Signaling (81) (H.323)	CRITICAL
SIGNALING(82)	Insufficient Shared Memory Pools - Signaling (82) (H.323)	CRITICAL
SIGNALING(83)	Error While Binding to Socket - Signaling (83)	CRITICAL
SIGNALING(84)	Reached Maximum Socket Limit - Signaling (84) (H.323)	CRITICAL
SIGNALING(85)	Initialization Failure - Signaling (85)	CRITICAL
SIGNALING(86)	Remote H323 Gateway is not Reachable - Signaling (86) (H.323)	MAJOR
SIGNALING(87)	H323 Message Parsing Error - Signaling (87) (H.323)	MAJOR
SIGNALING(88)	H323 Message Encoding Error - Signaling (88) (H.323)	MAJOR
SIGNALING(89)	Gatekeeper not Available/Reachable - Signaling (89)	MAJOR
SIGNALING(90)	Alternate Gatekeeper is not Responding - Signaling (90)	MAJOR
SIGNALING(91)	Endpoint Security Violation - Signaling (91) (H.323)	MAJOR
SIGNALING(92)	Invalid Call Identifier - Signaling (92)	MINOR
SIGNALING(93)	Invalid Call Reference Value - Signaling (93)	MINOR
SIGNALING(94)	Invalid Conference Identifier - Signaling (94)	MINOR
SIGNALING(95)	Invalid Message from the Network - Signaling (95)	MINOR
SIGNALING(96)	Internal Call Processing Error - Signaling (96)	MINOR
SIGNALING(97)	Insufficient Information to Complete Call - Signaling (97)	MINOR
SIGNALING(98)	H323 Protocol Inconsistencies - Signaling (98) (H.323)	MINOR
SIGNALING(99)	Abnormal Call Clearing - Signaling (99)	MINOR
SIGNALING(100)	Codec Negotiation Failed - Signaling (100)	MINOR
SIGNALING(101)	Per Call Security Violation - Signaling (101)	MINOR
SIGNALING(102)	H323 Network Congested - Signaling (102) (H.323)	MINOR
SIGNALING(103)	Aggregation Connection Down - Signaling (103)	MAJOR
SIGNALING(106)	Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)	MINOR
SIGNALING(107)	Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)	CRITICAL
SIGNALING(108)	Simplex Only Operational Mode - Signaling (108)	MAJOR
SIGNALING(109)	Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)	MAJOR
SIGNALING(110)	Signaling Gateway Group Is Out-of-Service - Signaling (110)	CRITICAL
SIGNALING(111)	Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)	MINOR
SIGNALING(112)	Stream Control Transmission Protocol Association Configuration Error - Signaling (112)	MINOR
SIGNALING(113)	Signaling Gateway Failure - Signaling (113)	MAJOR

Table 10-3 Cisco BTS 10200 Softswitch Signaling Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
SIGNALING(114)	Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)	MAJOR
SIGNALING(114)	Signaling Gateway Process Is Out-of-Service - Signaling (114)	MAJOR
SIGNALING(116)	Destination Point Code User Part Unavailable - Signaling (116)	MAJOR
SIGNALING(117)	Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)	MINOR
SIGNALING(118)	Circuit Verification Response Received with Failed Indication - Signaling (118)	MINOR
SIGNALING(119)	Signaling System 7 Adapter Process Faulty - Signaling (119)	CRITICAL
SIGNALING(120)	Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)	CRITICAL
SIGNALING(121)	Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)	MAJOR
SIGNALING(122)	Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)	MAJOR
SIGNALING(124)	Remote Subsystem is Out Of Service - Signaling (124)	MINOR
SIGNALING(125)	Signaling Connection Control Part Routing Error - Signaling (125)	MAJOR
SIGNALING(126)	Signaling Connection Control Part Binding Failure - Signaling (126)	MAJOR
SIGNALING(142)	Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)	CRITICAL
SIGNALING(143)	Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)	MINOR
SIGNALING(144)	All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)	CRITICAL
SIGNALING(145)	One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)	MINOR
SIGNALING(150)	Stream Control Transmission Protocol Association Congested - Signaling (150)	MINOR
SIGNALING(151)	Termination Permanent Error Code Received - Signaling (151)	MINOR

Socket Failure - Signaling (7)

The Socket Failure alarm (major) indicates that there is a failure in creating/binding to the UDP socket. The primary cause of the alarm is that there is a failure in creating or binding to the UDP socket. To correct the primary cause of the alarm, verify that there is no conflict in port assignment with other processes in the system and ensure no previous instance of the same process is still running. The secondary cause of the alarm is that a software logic problem has occurred. To correct the secondary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Media Gateway Control Protocol

The Socket Failure alarm is issued when there is a failure in creating the UDP port used by the MGCP stacks. Some other application may already be active on the same UDP port and IP address to which the Call Agent MGCP stack is assigned. Reconfigure the MGCP stack to use a free UDP port.

Session Initiation Protocol

The Socket Failure alarm is issued when there is a failure in creating the UDP port used by the SIA process. Some other application may already be active on the same UDP port and IP address to which the SIA process is assigned. Reconfigure the SIA port to use a free port or the SIP default port 5060.

Session Initiation Protocol Message Receive Failure - Signaling (8)

The Session Initiation Protocol Message Receive Failure alarm (major) indicates that a SIP message receive has failed. The primary cause of the alarm is that Operating System level network errors have occurred or the network configuration is invalid. To correct the primary cause of the alarm, have the network administrator resolve the network errors. Contact Cisco TAC if you need assistance. Manually clear alarm. Restart this call agent instance using the platform start command. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Session Initiation Protocol

The SIP Message Receive Failure alarm is issued when SIP messages cannot be received. This could be due to port conflict (two processes attempting to use the same UDP port). Examine the "HOSTNAME" field in the alarm report to determine the IP address or domain name of the Call Agent that generated this alarm. Telnet into this Call Agent instance as a root user. In this Call Agent, configure another UDP port for the SIA process to avoid port conflict, by setting the SIA port in platform.cfg file to another port number. Call Cisco TAC if you need assistance. Restart this Call Agent instance using the platform start command.

Timeout on Internet Protocol Address - Signaling (9)

The Timeout on Internet Protocol Address alarm (major) indicates that an IP address has timed out. The alarm is issued when the OptiCall is unable to communicate with a gateway. To correct the primary cause of the alarm, verify that the gateway is both configured for service and that it has been set in service. Attempt to ping the gateway using the IP address from the Event Report. If the ping is not successful, then diagnose the issue that prevents the address from being reached. Use the Status MGW ID=xxx, where xxx is the IP address given in the Event Report. If the status is not INS, then use control mgw command to put it in service.

Media Gateway Control Protocol

The Timeout on IP Address alarm is issued when the Cisco BTS 10200 Softswitch is unable to communicate with a gateway. Verify that the gateway is both configured for service and that it has been set in service. Attempt to ping the gateway using the IP address from the Event Report. If the ping is not successful, then diagnose the issue that prevents the address from being reached. Use the Status MGW ID=xxx, where xxx is the IP address given in the Event Report. If the status is not INS, then use the **control mgw** command to put it in service.

Session Initiation Protocol

The Timeout on IP Address alarm is issued when the Call Agent did not receive SIP response messages from Call Agent specified in the Event Report. The Call Agent has already taken the necessary action to handle this situation by re-sending the SIP messages to the redundant IP address of the remote Call Agent.

Failed to Send Complete Session Initiation Protocol Message - Signaling (10)

The Failed to Send Complete Session Initiation Protocol Message alarm (minor) indicates that a SIP message failure has occurred. The primary cause of the alarm is that the SIP stack failed to send an SIP message due to it exceeding the maximum length of a UDP packet. To correct the primary cause of the alarm, the message should be captured on passive testing equipment and sent to Cisco TAC for evaluation if that alarm occurred during normal network operations. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)

The Failed to Allocate Session Initiation Protocol Control Block alarm (major) indicates that a SIP control block allocation failed. The primary cause of the alarm is that there is not enough memory to allocate a SIP Call Control Block. To correct the primary cause of the alarm, Increase the SIP CCB count specified in mem.cfg file and restart the Call Agent for the changes to take effect.

Feature Server is not Up or is not Responding to Call Agent - Signaling (12)

The Feature Server is not Up or is not Responding to Call Agent alarm (critical) indicates that the feature server is not up or is not responding to the call agent server. The primary cause of the alarm is that the feature server platform is down or is not operating properly. To correct the primary cause of the alarm, restart the applicable feature server.

Use the following steps to locate and correct provisioning errors which may be associated with the Feature Server is not Up or is not Responding to Call Agent alarm:

Step 1 Verify that the ID, TSAP-ADDR, and TYPE are properly provisioned in the Feature Server (feature-server) table.

Step 2 Verify that Alerting Notification is provisioned properly.

Step 3 Verify one of the following cases, as applicable:

- Verify that Alerting Notification is included in the SERVICE table applicable to the specific subscriber.
- Verify that Alerting Notification is included in the SERVICE table applicable to the specific POP (the service ID identified by the office-service-id token in the POP table).
- Verify that Alerting Notification is included in the default office service ID (if the feature is intended to be offered by default to all subscribers on the switch).

Note In the procedures included in this document, Alerting Notification is provisioned using the feature identifier FNAME=ALERT_NOTIFY. The feature identifier can be any unique string of up to 16 ASCII characters chosen by the service provider. If you are not sure of the name used in your system for this feature, use the SHOW FEATURE command and view the system response to find the name.

Example:

```
SHOW FEATURE-SERVER;
SHOW FEATURE FNAME=ALERT_NOTIFY;
SHOW POP;
SHOW SERVICE ID=<the value of the office-service-id in POP table>
SHOW CA-CONFIG TYPE=DEFAULT-OFFICE-SERVICE-ID;
SHOW SERVICE ID=<the value of the default-office-service-id in ca-config table>
SHOW SERVICE ID=silverservice;
SHOW SUBSCRIBER-SERVICE-PROFILE SERVICE-ID=silverservice;
```

Step 4 If a TSAP address is used for the 3PTYFS, verify that the domain name is correctly provisioned in the DNS and resolves to the intended 3PTYFS.

Step 5 Enter the CLI command to check for SIGNALING alarm #12—Feature Server is not up or is not responding to the Call Agent. If this alarm is raised, there is a communications problem between the Cisco BTS 10200 Softswitch and the 3PTYFS.

Example:

```
show alarm type=signaling;
show alarm type=signaling; number=12;
```

The following details apply to SIGNALING alarm #12:

- For a 3PTYFS that is more than one hop away from the Cisco BTS 10200 Softswitch, SIGNALING alarm #12 is raised when communications between the Cisco BTS 10200 Softswitch and the first-hop node go down. However, the alarm is not raised if communications on the second (or more distant) hop go down, or if the DNS value for the 3PTYFS does not resolve correctly.
- The system can take up to two minutes to detect a communications failure in the first hop toward the 3PTYFS.

Step 6 Verify that you have connectivity from the Cisco BTS 10200 Softswitch to the 3PTYFS.

Step 7 Verify that the 3PTYFS is provisioned to support this feature in accordance with the applicable product documentation. The Cisco BTS 10200 Softswitch does not send any provisioning or status/control commands to the 3PTYFS.

Step 8 Verify that the 3PTYFS and peripheral devices are operating properly according to the applicable product documentation.

Signaling System 7 Signaling Link Down - Signaling (13)

The Signaling System 7 Signaling Link Down alarm (major) indicates the SS7 signaling link is down. The primary cause of the alarm is that the SS7 trunk group may be out-of-service (OOS). To correct the primary cause of the alarm, use the control ss7-trunk-grp command to place the trunk group in service (INS). The secondary cause of the alarm is that the local Ulticom stack may be down. To correct the secondary cause of the alarm, run the Ulticom stack command again. The ternary cause of the alarm is that the SS7 link may be disconnected or faulty. To correct the ternary cause of the alarm, check the Ulticom local configuration. The subsequent cause of the alarm is that the remote SS7 signaling site may be down or incorrectly configured. To correct the subsequent cause of the alarm, check the Ulticom remote configuration.

Signal System 7 and Call Agent Fail-over Interaction

When an ISUP SS7 signaling link goes into the link failure state, an Signaling System 7 Signaling Link Down alarm (13) is activated and the call-agent will begin a 120 second timer. When the SS7 signaling link is restored, in-progress calls are cleared if they were in a transient state, if an event occurred that required the sending of an ISUP message during the link failure, or if the 120 second timer has expired.

Should the call-agent fail-over for any reason, the state of the 120 second timer or any indication of a request for an outgoing message that could not be sent will not be preserved. If the signaling links are in the failure state on the stand-by side, the 120 second timer will be re-started; however, if the links should restore prior to that the timer expiry, any stable calls will NOT be cleared.

This applies should multiple fail-overs occur prior to eventual signaling link restoration. In these situations, if a call clearing event has been missed, any calls remaining up will be cleared by the normal ISUP network recovery and message retransmission mechanisms.

Link is Remotely Inhibited - Signaling (14)

The Link is Remotely Inhibited alarm (minor) indicates that the SS7 link is inhibited at the remote end. The primary cause of the alarm is that the specified SS7 link is inhibited at the remote end. To correct the primary cause of the alarm, monitor events and alarms at the network level for any related to the specified SS7 link. Restorative actions need to be taken on the remote end.

Link is Locally Inhibited - Signaling (15)

The Link is Locally Inhibited alarm (minor) indicates that the SS7 link is inhibited at the local end. The primary cause of the alarm is that the specified SS7 link is inhibited at the local end. To correct the primary cause of the alarm, verify that the SS7 signaling adapter process is running and that the SS7 interface card(s) are in service. If a component is found to be non-operational, restore it to service.

Link is Congested - Signaling (16)

The Link is Congested alarm (minor) indicates that the SS7 link is congested. The primary cause of the alarm is that the specified SS7 link is experiencing congestion. To correct the primary cause of the alarm, monitor event reports at the network level to determine if the traffic load on the specified SS7 link is too high on the local end, or if the remote end is lagging in processing the traffic. Verify that the SS7 link has not degraded in quality. Verify that the traffic load has not become unbalanced if multiple SS7 links are used. Verify that local SS7 signaling adapter process is running normally.

Link: Local Processor Outage - Signaling (17)

The Link: Local Processor Outage alarm (minor) indicates that the SS7 link has experienced a local processor outage. The primary cause of the alarm is that the specified SS7 link has experienced a processor outage. To correct the primary cause of the alarm, monitor the system for maintenance event reports associated with the signaling adapter or underlying platform instance that support the specified SS7 link. Verify that the process and or platform are restarted and returned to service.

Link: Remote Processor Outage - Signaling (18)

The Link: Remote Processor Outage alarm (minor) indicates that the SS7 link has experienced a remote processor outage. The primary cause of the alarm is that the specified SS7 link has experienced a processor outage. To correct the primary cause of the alarm, monitor the network level event reports for any events associated with the processing complex used by the specified SS7 link. Verify that the SS7 link is returned to service.

Link Set Inaccessible - Signaling (19)

The Link Set Inaccessible alarm (major) indicates that the specified SS7 link in inaccessible. The primary cause of the alarm is that the specified SS7 link set is inaccessible. To correct the primary cause of alarm, return the SS7 signaling adapter and the associated call agent platform to service if the SS7 signaling adapter is not running normally and the associated call agent platform is not active.

Link Set Congestion - Signaling (20)

The Link Set Congestion alarm (major) indicates that the specified SS7 link set is congested. The primary cause of the alarm is that the specified SS7 link set is experiencing congestion. To correct the primary cause of the alarm, monitor the alarm and event reports at the network level to determine if the traffic load on the specified SS7 link set is too high on the local end, or if the remote end is lagging in processing the traffic. Verify that the SS7 link set has not degraded in quality. Verify that the traffic load has not become unbalanced if multiple SS7 link sets are used. Verify that local SS7 signaling adapter process is running normally.

Route Set Failure - Signaling (21)

The Route Set Failure alarm (major) indicates that the specified route set has a experienced a failure. The primary cause of the alarm is the specified route set has experienced a failure. To correct the primary cause of the alarm, verify that the processing complex supporting the route set is functional. Monitor event reports at the network level to determine the failing component and verify its restoral to service.

Route Set Congested - Signaling (22)

The Route Set Congested alarm (minor) indicates that the specified route set is congested. The primary of the alarm is that the specified route set is experiencing congestion. To correct the primary cause of the alarm, monitor event reports at the network level to determine if the traffic load on the specified SS7 link set is too high on the local end, or if the remote end is lagging in processing the traffic. Verify that the SS7 link set has not degraded in quality. Verify that the traffic load has not become unbalanced if multiple SS7 link sets are used. Verify that local SS7 signaling adapter process is running normally.

Destination Point Code Unavailable - Signaling (23)

The Destination Point Code Unavailable alarm (major) indicates that the specified DPC is not available. This alarm indicates that the Cisco BTS 10200 Softswitch is unable to communicate with the specified DPC in the SS7 network. Determine if the issue is a communication problem between the Cisco BTS 10200 Softswitch and the IP transfer point (ITP) or if it is related to communication problems between the ITP and the DPC by following these steps:

Step 1 Use the Cisco BTS 10200 Softswitch CLI show alarm command to determine if there is an active Signaling Gateway Group Out of Service alarm. This will occur if communication has been lost to at least one of the SGs in the SG-Group. If so, proceed to the "Signaling Gateway Group Is Out-of-Service - Signaling (110)" section on page 10-130. Otherwise, proceed to Step 2.

Step 2 Determine if there is an M3UA Cannot Go Active alarm. This occurs if, at the time of startup or failover, the Cisco BTS 10200 Softswitch is not able to communicate with any of the SGs. If this is the case, proceed to the "Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)" section on page 10-133. Otherwise, proceed to Step 3.

Step 3 If you arrive at this step, there is probably communication between the Cisco BTS 10200 Softswitch and ITP at the M3UA and SCCP user adapter (SUA) layers, and a communication problem exists between the ITP and the unavailable DPC. To confirm this, log on to each ITP, get into enable mode, and enter **show cs7 route**. The output of this command tells you if the associated DPC is accessible or not from the ITP point of view and will look similar to the following:

```
va-2651-82#show cs7 route
Destination            Prio Linkset Name        Route
---------------------- ---- ------------------- -------
229.123.2/24     INACC   1  lset1chn            UNAVAIL
```

This output indicates that DPC 229.123.2 is unavailable from the ITP point of view.

Step 4 Determine if the problem is at the link level or at a higher level outage in the DPC by typing **show cs7 linkset**. If the ITP shows that the DPC is AVAIL, there is a mismatch between the ITP and Cisco BTS 10200 Softswitch. Please contact the Cisco TAC.

Step 5 Check whether the DPC has been removed from the Cisco BTS 10200 Softswitch database. At the Cisco BTS 10200 Softswitch CLI prompt, enter **show call-ctrl-route** or **show sccp-route** and see if the DPC is in any of the routes. If not, the alarm was raised before the associated routes were deleted. If this is the case, manually clear the alarm.

Step 6 If you still cannot determine the cause of the problem, contact the Cisco TAC.

Destination Point Code Congested - Signaling (24)

The Destination Point Code Congested alarm (minor) alarm indicates that the specified DPC is congested. This alarm indicates that the DPC in the SS7 network is congested, i.e., is in a state where it has received more traffic than it can handle. This should be a temporary state. If the type of network is National, which is generally the case in the United States, there will also be a level of congestion associated with the alarm.

The ITP should continually communicate with the DPC in the SS7 network to determine if congestion has abated. If this alarm does not clear or keeps reappearing after clearing, contact your SS7 service provider to determine why the DPC is congested.

The DPC Congested alarm is issued when the specified destination point code is congested. Monitor event reports at the network level to determine if the traffic load to the specified DPC is too high on the local end, or if the remote end is lagging in processing the traffic.

Trunk Locally Blocked - Signaling (36)

The Trunk Locally Blocked alarm (minor) indicates that the trunk is locally blocked. The primary cause of the alarm is that a BLO or CGB message was sent on the specified CIC. For add it on al information on correcting the cause of the alarm, refer to Appendix B, “System Usage of MGW Keepalive Parameters, Release 4.5.x.”

Trunk Remotely Blocked - Signaling (40)

The Trunk Remotely Blocked alarm (major) indicates that the trunk is remotely blocked. The primary cause of the alarm is that a BLO or CGB message was received on the specified CIC if it is SS7 trunk. Issued when SERVICE OOS message is received for ISDN trunks. Issued when Reverse Make Busy (rbz) signal is received for CAS operator trunk. No action is required. The system can be manually recovered from this condition locally by controlling the effected trunks to UEQP state and back INS.

Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)

The Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway alarm (major) indicates that specified ISDN trunk group status was changed due to a media gateway operation. The primary cause of the alarm is that the specified ISDN trunk group’s status was changed due to a media gateway operation. To correct the primary cause of the alarm, monitor the event reports at the network level to determine which media gateway caused the status change of the trunk group. Verify that the gateway is reconfigured properly to support the usage of the trunk group.

Media Gateway/Termination Faulty - Signaling (63)

The Media Gateway/Termination Faulty alarm (major) indicates that a media gateway or termination has gone faulty due to the detection of an unknown endpoint, unknown package type, and unknown event, a hardware failure, or a general call agent error. The primary cause of the alarm is that a media gateway or termination has gone faulty due to the detection of an unknown endpoint, unknown package type, and unknown event (either a hardware failure or a general call agent error). To correct the primary cause of the alarm, verify the proper operation of the media gateway specified. Place the termination out-of-service and then back into service from the call agent.

Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)

The Media Gateway Adapter Running out of Shared Memory Pools alarm (critical) indicates that the MGCP signaling adapter was unable to allocate data store for an IPC message due to a lack of resources. The primary cause of the alarm is that the MGCP signaling adapter was unable to allocate data store for an IPC message due to a lack of resources. To correct the primary cause of the alarm, contact Cisco TAC technologies for assistance. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Media Gateway Adapter Running out of Heap Memory - Signaling (65)

The Media Gateway Adapter Running out of Heap Memory alarm (critical) indicates that the MGCP signaling adapter was unable to allocate data store for an IPC message from the heap due to a lack of resources. The primary cause of the alarm is that the MGCP signaling adapter was unable to allocate data store for an IPC message from the heap due to a lack of resources. To correct the primary cause of the alarm, contact Cisco TAC for assistance. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)

The Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) alarm (major) indicates that a call agent internal error has occurred causing the restart of the MGCP signaling adapter. The primary cause of the alarm is that a call agent internal error has occurred causing the restart of the MGCP signaling adapter. To correct the primary cause of the alarm, send the log files to Cisco TAC for analysis and corrective action. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Media Gateway Endpoints are out of Service at Gateway - Signaling (68)

The Media Gateway Endpoints are out of Service at Gateway alarm (major) indicates that the media gateway endpoints are out of service at the GW. The primary causes of the alarm are that the Media gateway has been administratively taken the OOS using a command in GW or the Endpoint is in an alarmed or OOS state. To correct the primary cause of the alarm, bring into service the Media gateway that has been administratively taken INS using the command in GW and fix the endpoint alarms.

Call Agent and Feature Server Communication Message Timeout - Signaling (69)

The Call Agent and Feature Server Communication Message Timeout alarm (critical) indicates that a CA and FS communications message timed out. The primary cause of the alarm is that CA to FS communication has failed due to wrong system configuration; -OR- CA or FS is down. To correct the primary cause of the alarm, check the configuration related to the CA to FS communication. Also, check the FS table entries and the CA entry.

Signaling System 7 Stack not Ready - Signaling (75)

The Signaling System 7 Stack not Ready alarm (critical) indicates that the SS7 stack in not ready. The primary cause of the alarm that the SS7 stack not configured properly. To correct the primary cause of the alarm, check SS7 stack configuration. The secondary cause of the alarm is that the SS7 stack is not ready. To correct the secondary cause of the alarm, check the SS7 stack status. Do a platform "**start -i omni**" command to bring up the SS7 stack.

Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)

The Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling alarm (minor) indicates that one of the ISDN D-channels in the PRI is down. The primary cause of the alarm is that one of the ISDN D-channels in PRI is down. To correct the primary cause of the alarm, check the gateway power and the gateway connection to the PBX.

Media Gateway Unreachable - Signaling (79)

The Media Gateway Unreachable alarm (major) indicates that the media gateway is unreachable. The primary cause of the alarm is that a MGCP signaling inter-operational error has occurred. To correct the primary cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x"or contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request. For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x."

Out of Bounds, Memory/Socket Error - Signaling (80)

The Out of Bounds, Memory/Socket Error alarm (critical) indicates that a memory socket out of bounds error has occurred. The primary cause of the alarm is that the system is out of heap memory. To correct the primary cause of the alarm, contact Cisco TAC and increase RAM memory. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request. The secondary cause of the alarm is that the system is out of IPC pool memory. To correct the secondary cause of the alarm, resize the IPC pool size in Platform Configuration file. The ternary cause of the alarm is that a socket error has occurred. An inappropriate or already bound socket may be in use. To correct the ternary cause of the alarm, check the UDP port supplied with the MGA command-line for validity and prior use.

Insufficient Heap Memory - Signaling (81) (H.323)

The Insufficient Heap Memory alarm (critical) indicates that there is insufficient heap memory. The primary cause of the alarm is that the H323 signaling adapter was unable to allocate memory from the system. To correct the primary cause of the alarm, contact Cisco TAC for assistance. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Insufficient Shared Memory Pools - Signaling (82) (H.323)

The Insufficient Shared Memory Pools alarm (critical) indicates that there is insufficient shared memory pools. The primary cause of the alarm is that the H323 signaling adapter was unable to allocate storage. To correct the primary cause of the alarm, contact Cisco TAC for corrective action. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Error While Binding to Socket - Signaling (83)

The Error While Binding to Socket alarm (critical) indicates that an error occurred while binding to the socket.

Reached Maximum Socket Limit - Signaling (84) (H.323)

The Reached Maximum Socket Limit alarm (critical) indicates that the Cisco BTS 10200 Softswitch system has reached the maximum socket limit. The primary cause of the alarm is that the configuration setting of an H3A parameter in the platform.cfg file is wrong. To correct the primary cause of the alarm, reconfigure the platform.cfg file and restart the H3A process.

Initialization Failure - Signaling (85)

The Initialization Failure alarm (critical) indicates that the Cisco BTS 10200 Softswitch system failed to initialize. The primary cause of the alarm that a process initialization failure has occurred. To correct the primary cause of the alarm, check "Reason" dataword for the failure cause and take action accordingly.

Remote H323 Gateway is not Reachable - Signaling (86) (H.323)

The Remote H323 Gateway is not Reachable alarm (major) indicates that the remote H323 gateway is not reachable. The primary cause of the alarm is that a loss of communication with a remote gateway has occurred. To correct the primary cause of the alarm, perform the standard connectivity tests - both the physical checks and the IP tests. Also, ensure that the gateway is not out of service.

H323 Message Parsing Error - Signaling (87) (H.323)

The H323 Message Parsing Error alarm (major) indicates that a H323 message parsing error has occurred. The primary cause of the alarm is that the system was unable to successfully parse an incoming H323 message. This alarm is a result of either a software bug or bad message being received - a message with a valid message type but an invalid field within the message. To correct the primary cause of the alarm, snoop the message from the endpoint and verify its content or contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

H323 Message Encoding Error - Signaling (88) (H.323)

The H323 Message Encoding Error alarm (major) indicates that a H323 message encoding error has occurred. The primary cause of the alarm is that the system was unable to encode an H323 message for sending. The alarm is indicative a software bug. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Gatekeeper not Available/Reachable - Signaling (89)

The Gatekeeper not Available/Reachable alarm (major) indicates that the gatekeeper is not available or the gatekeeper is not reachable. The primary cause of the alarm is that the gatekeeper is not available or is unreachable. To correct the primary cause of the alarm, check the network connectivity. Check to ensure the GK is reachable by trying to ping the GK IP address. If reachable, then check to ensure that the GK is configured up.

This is a result of either a software bug or bad message being received - a message with a valid message type but an invalid field within the message. Snoop the message from the endpoint and verify its content or contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Alternate Gatekeeper is not Responding - Signaling (90)

The Alternate Gatekeeper is not Responding alarm (major) indicates that the alternate gatekeeper is not responding. The primary cause of the alarm is that the alternate gatekeeper is not responding. To correct the primary cause of the alarm, check network connectivity. Check to ensure the alternate GK is reachable by trying to ping the alternate GK IP address. If reachable, then check to ensure that the alternate GK is configured up.

This is a result of either a software bug or bad message being received - a message with a valid message type but an invalid field within the message. Snoop the message from the endpoint and verify its content or contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Endpoint Security Violation - Signaling (91) (H.323)

The Endpoint Security Violation alarm (major) indicates that an H323 security violation has occurred. The primary cause of the alarm is that an H323 security violation has occurred. To correct the primary cause of the alarm, check to make sure the password selections on the Cisco BTS 10200 Softswitch and the gatekeeper are correct. The secondary cause of the alarm is that the H323GW table may not be provisioned properly or there is a time synchronization problem between the Cisco BTS 10200 Softswitch and/or the gatekeeper and the NTP server. To correct the secondary cause of the alarm, ensure that both the Cisco BTS 10200 Softswitch and the gatekeeper are pointing to the same NTP server.

Invalid Call Identifier - Signaling (92)

The Invalid Call Identifier alarm (minor) indicates that the Call ID was invalid or changed mid-call. The primary cause of the alarm is that the Call ID was invalid or changed mid-call. The alarm indicates that a software problem has occurred on the Cisco BTS 10200 Softswitch or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Invalid Call Reference Value - Signaling (93)

The Invalid Call Reference Value alarm (minor) indicates that the Call ID was invalid or changed mid-call. The primary cause of the alarm is that the Call ID was invalid or changed mid-call. The alarm indicates that a software problem has occurred on the Cisco BTS 10200 Softswitch or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Invalid Conference Identifier - Signaling (94)

The Invalid Conference Identifier alarm (minor) indicates that the Call ID was invalid or changed mid-call. The primary cause of the alarm is that the Call ID was invalid or changed mid-call. The alarm indicates that a software problem has occurred on the Cisco BTS 10200 Softswitch or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Invalid Message from the Network - Signaling (95)

The Invalid Message from the Network alarm (minor) indicates that an unsupported or invalid message type was received from network. The primary cause of the alarm is that an unsupported or invalid message type was received from the network. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Internal Call Processing Error - Signaling (96)

The Internal Call Processing Error alarm (minor) indicates that an internal call processing error has occurred. The primary cause of the alarm is that a software error has occurred. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Insufficient Information to Complete Call - Signaling (97)

The Insufficient Information to Complete Call alarm (minor) indicates that there was insufficient information to complete a call. The primary cause of the alarm is that there was not enough initial call setup information received to establish the call. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

H323 Protocol Inconsistencies - Signaling (98) (H.323)

The H323 Protocol Inconsistencies alarm (minor) indicates that the H323 endpoint and Cisco BTS 10200 Softswitch are running different protocol versions. The primary cause of the alarm is that the H323 endpoint and the Cisco BTS 10200 Softswitch are running different protocol versions. This is only an issue where the endpoint is running a higher version of the H323 protocol than the Cisco BTS 10200 Softswitch. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Abnormal Call Clearing - Signaling (99)

The Abnormal Call Clearing alarm (minor) indicates that an unsupported or invalid message type was received from network. The primary cause of the alarm is that an unsupported or an invalid message type was received from network. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Codec Negotiation Failed - Signaling (100)

The Codec Negotiation Failed alarm (minor) indicates that the codec negotiation has failed. The primary cause of the alarm is that the codec negotiation failed. To correct the primary cause of the alarm, find a compatible set of codec settings for both sides, re-provision the endpoints of the call and try the call again.

Per Call Security Violation - Signaling (101)

The Per Call Security Violation alarm (minor) indicates that a call security violation has occurred. This is a future trap definition - it will not be issued in the 3.x release series.

H323 Network Congested - Signaling (102) (H.323)

The H323 Network Congested alarm indicates (minor) that the H323 application process has depleted its resources and no more calls can be completed. The primary cause of this alarm is that the H323 application processes has depleted it's resources and no more calls can be completed. The high water mark has been reached and all new call requests are rejected until the low water mark is reached. To correct the primary cause of the alarm, re-provision the water marks or check the network for overload. Also verify that alternate routes have been provisioned on the Cisco BTS 10200 Softswitch.

Aggregation Connection Down - Signaling (103)

The Aggregation Connection Down alarm (major) indicates that the AGGR TCP connection is down. The primary cause of the alarm is that the TCP connection is down. To correct the primary cause of the alarm, check the associated cabling and perform PINGs to test the connectivity.

Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)

The Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down alarm (minor) indicates that the ESA Cisco BTS 10200 Softswitch DF connection is down. The primary cause of the alarm is that the DF server is not responding. To correct the primary cause of the alarm, check the encryption key or the IP connectivity to the DF.

Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)

The Logical Internet Protocol Addresses not Mapped Correctly alarm (critical) indicates that the logical IP addresses are not mapped correctly. The primary cause of the alarm is that the contact name in the configuration file is not configured in the DNS. To correct the primary cause of the alarm, verify that the name in the DNS matches the name in the platform.cfg and opticall.cfg files. The secondary cause of the alarm is the contact could not be resolved to an IP address on the host. To correct the secondary cause of the alarm, verify that the DNS resolves to the IP addresses reserved for process on the Cisco BTS 10200 Softswitch. The ternary cause of the alarm is that the IP address manager is not running. To correct the ternary cause of the alarm, verify that the IPM process is running and check for alarms from IPM. The subsequent cause of the alarm is mis-configuration during installation or manual changes made after installation. To correct the subsequent cause of the alarm, contact Cisco TAC for support. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Simplex Only Operational Mode - Signaling (108)

The Simplex Only Operational Mode alarm (major) indicates that the Cisco BTS 10200 Softswitch system can only operate in the simplex mode. The primary cause of the alarm is that the -hostname parameter is specified in the platform.cfg file (instead of the -contact parameter). The Cisco BTS 10200 Softswitch is configured as a SIMPLEX system. The secondary cause of the alarm is that the SIA host and contact parameters are the same in platform.cfg file or the SIA is configured for use on a simplex system. To correct the secondary cause of the alarm, if this is a duplex installation, regardless of current operational state, contact Cisco TAC. If this is a simplex installation only, this alarm can be turned off. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Stream Control Transmission Protocol Association Failure - Signaling (109)

The Stream Control Transmission Protocol Association Failure alarm (major) indicates that the SCTP association failed. This alarm indicates that the Cisco BTS 10200 Softswitch is unable to communicate with an SGP at the SCTP protocol level. The problem may be at the M3UA or SUA layer. The primary cause of the alarm is that the Ethernet cables on the SGP are unplugged or severed. To correct the primary cause of the alarm, plug the Ethernet cables in or fix the severed connection. The secondary cause of the alarm is that the SGP is not operational. To correct the secondary cause of the alarm, check the SGP alarms to determine why it is not operating properly. To troubleshoot the M3UA or the SUA layers, use the following procedures.

Message Transfer Part 3 User Adapter Troubleshooting Procedure

Use the following steps to determine the source of the problem at the M3UA layer:

Step 1 Determine if the administrative state of the SCTP is correct.

a. Type the following command at the Cisco BTS 10200 Softswitch CLI prompt:

```
status sctp-assoc id=<sctp-assoc-name>
```

If the response displays ADMIN STATE ->ADMIN_OOS, the SCTP association has been taken administratively out of service and needs to be put back in service.

b. Enter the following command to put the SCTP association in service:

```
control sctp-assoc id=<sctp-assoc-name>; mode=forced; target-state=INS;
```

c. If the administrative state is ADMIN_INS, determine if the association has been taken out of service on the ITP. Log on to the ITP. If you are unable to log on to the ITP, proceed to Step 2.

d. If you are able to log on to the ITP, check the state of the associated application service provider (ASP) by entering the following command:

```
show cs7 asp
```

The following is an example of the output:

```
ASP Name      AS Name       State     Type  Rmt Port Remote IP Addr  SCTP
------------  ------------  --------  ----  -------- --------------- ----------
hrn11asp      hrn11bts      shutdown  M3UA  11146    10.0.5.13
```

e. If the state of the ASP indicates shutdown, someone has administratively taken the association out of service. Refer to the *Cisco ITP User's Guide*, at the following universal resource locator (URL), to put the ASP (SCTP association) back in service:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/itp/23sw/index.htm

f. If the state is down proceed to Step 2.

g. If the state of the ASP is inactive, the ASP is probably on the standby Cisco BTS 10200 Softswitch. If the ASP on the active Cisco BTS 10200 Softswitch is inactive, proceed to Step 7.

Step 2 Determine if the problem is an IP address or port configuration mismatch between the ITP and the Cisco BTS 10200 Softswitch.

a. Determine the Cisco BTS 10200 Softswitch configured values for the Cisco BTS 10200 Softswitch IP addresses and port. Look for the DNS name and port number that are configured for the SGA process in /opt/OptiCall/CA146/bin/platform.cfg. Go to the specified directory and enter:

```
cat platform.cgf | grep mdl
```

The output will look similar to the following:

```
Args=-t 1 -h mgcp-HRN11CA.hrndevtest.cisco.com -p 11146 -mdldir. /mdl -mdltracedir
../mdltrace -mdltestmode 0 -mdlloadmdo 0 -mdltriggertimer 200 -mdlgarbagetimer 5146
-resetcics 1 -fcmtimer 900 -fcmparalleljobs 4
```

- The local IP port number is shown directly after the -p option.
- The local IP addresses that are used by the Cisco BTS 10200 Softswitch are derived from the DNS name, which is given directly after the -h option. At the Cisco BTS 10200 Softswitch UNIX prompt, enter:

```
NSlookup <DNS name>
```

The output will look similar to the following:

```
Server:  hrnbtsjs-1.cisco.com
Address:  10.82.70.199
Name:    mgcp-HRN11CA.hrndevtest.cisco.com
Addresses:  10.0.5.136, 10.128.1.147
```

The Cisco BTS 10200 Softswitch configured local IP addresses are given in the Addresses: line.

b. Determine the ITP configured values of the ITP Cisco BTS 10200 Softswitch IP addresses and port.

- Log on to the ITP and get into enable mode.
- Enter the following command:

```
show run
```

- Hit enter until the ASP configurations are displayed. A section similar to the following will appear which shows you the ITP configured values for the Cisco BTS 10200 Softswitch IP addresses of the SCTP association:

```
cs7 asp hrn11asp 11146 2905 m3ua
remote-IP 10.0.5.136
remote-IP 10.128.1.147
```

The number after the ASP name "hrn11asp" is the port number that the ITP has configured for the Cisco BTS 10200 Softswitch side of the SCTP association. The two remote-IP addresses are the addresses that the ITP has configured for the Cisco BTS 10200 Softswitch side of the SCTP association. Make sure all of these values match the values found in Step 2A.

c. Determine the Cisco BTS 10200 Softswitch configured values for the ITP IP addresses and port

On the Cisco BTS 10200 Softswitch EMS CLI console, type the following:

```
CLI> show sctp-assoc id=<SCTP assoc id>
```

An example of the output will show the IP addresses and port as follows:

```
REMOTE_PORT=2905
REMOTE_TSAP_ADDR1=10.0.1.54
REMOTE_TSAP_ADDR2=10.128.1.239
```

d. Determine the ITP configured values of the ITP Cisco BTS 10200 Softswitch IP addresses and port

- Logon to the ITP and get into enable mode.
- Enter **sho run**.
- Hit enter until the m3ua (or sua) configuration is displayed. In our example, we are considering the SCTP association connection between the Cisco BTS 10200 Softswitch and the ITP, so we will look at the ITP m3ua configuration. An example of this is as follows:

```
cs7 m3ua 2905
local-IP 10.0.1.54
local-IP 10.128.1.239
```

- Make sure that the IP addresses and port number are the same values as found in step 2C.

Step 3 Determine if all Ethernet connections on the Cisco BTS 10200 Softswitch have been disconnected or if communication has been lost to the IP router. In the platform.log, look for the following ERROR message:

"All the IP interfaces are faulty!!"

If this message is found, the Ethernet connections of the Cisco BTS 10200 Softswitch have been pulled or cut. If this message is not found, proceed to Step 4.

Step 4 Determine if the problem is an IP routing issue.

a. Determine what has been provisioned in the Cisco BTS 10200 Softswitch for the destination IP interfaces of the SCTP association by typing the following command:

show sctp-association id=<sctp-association-id>

Information similar to the following will appear and display the destination IP addresses:

```
REMOTE_TSAP_ADDR1=10.0.1.54
REMOTE_TSAP_ADDR2=10.128.1.239
```

b. Ping each of the destination IP addresses If one of the addresses does not respond to the ping, there is an IP routing problem that has disabled SCTP communication. Contact the Cisco TAC for assistance. If the ping commands are successful, proceed to Step 5.

Step 5 Determine if the Cisco BTS 10200 Softswitch is reachable from the ITP.

a. Log on to the ITP and get into enable mode.

b. Find the Cisco BTS 10200 Softswitch SCTP association endpoint IP addresses by typing the following command:

show run

c. Hit enter until the ASP configuration is displayed. A section similar to the following will display the Cisco BTS 10200 Softswitch IP addresses of the SCTP association:

```
cs7 asp hrn11asp 11146 2905 m3ua
remote-IP 10.0.5.136
remote-IP 10.128.1.147
```

d. Ping each of the IP addresses. If you do not receive a response to the ping command for at least one of the Cisco BTS 10200 Softswitch IP endpoint addresses, there is an IP routing problem that is causing the SCTP association to be down. Contact the Cisco TAC for assistance. Otherwise, proceed to Step 6.

Step 6 Bounce the SCTP association (take it administratively out of service and then put it in service)

a. At the Cisco BTS 10200 Softswitch CLI prompt, enter the following commands:

```
control sctp-assoc id=<sctp-assoc-name>; mode=forced; target-state=OOS;
control sctp-assoc id=<sctp-assoc-name>; mode=forced; target-state=INS;
```

b. Check if the SCTP association has come back in service by entering the following:

```
status sctp-assoc id=<sctp-assoc-name>;
```

The output will either show OPER STATE -> SCTP-ASSOC out of service or OPER STATE -> SCTP-ASSOC in service.

If the OPER STATE still shows that the SCTP association is out-of-service, proceed to Step 7.

Step 7 Bounce the SCTP association from the ITP side by performing the following steps:

a. Log on to the ITP and get into enable mode.

b. Get into configure mode by typing configure terminal.

c. Type t he following commands to bounce the SCTP association back in service:

```
va-2651-82(config)#cs7 asp hrn11asp
va-2651-82(config-cs7-asp)#shut
va-2651-82(config-cs7-asp)#no shut
va-2651-82(config-cs7-asp)#end
```

d. Determine if the SCTP association has come back in service by typing the following Cisco BTS 10200 Softswitch CLI command:

```
status sctp-assoc id=<sctp-assoc-name>;
```

The output will display either OPER STATE -> SCTP-ASSOC out of service or OPER STATE -> SCTP-ASSOC in service.

If the OPER STATE still shows that the SCTP association is out-of-service, there is probably an SCTP communication issue that must be debugged at the SCTP protocol level. Contact the Cisco TAC for assistance.

Signaling Connection Control Part User Adapter Troubleshooting Procedures

Refer to Chapter 13, “Network Troubleshooting” to determine the source of the problem at the SUA layer.

Signaling Gateway Group Is Out-of-Service - Signaling (110)

The Signaling Gateway Group is Out-of-Service alarm (major) indicates that the signaling gateway group is out-of-service. The primary cause of the alarm is that all the SCTP associations between the CA and the SGs are out-of-service. To correct the primary cause of the alarms, make sure that all Ethernet connections on the CA and SGs are plugged in. Also make sure all associated IP routers are operational. The secondary cause of the alarm is that the M3UA layer is down between the CA and SGs. To correct the secondary cause of the alarm, use a snooper application to determine why the M3UA layer is down.

This alarm indicates that after communication to the SG group was established, it was lost. This indicates that communication to associated SGs is down, which also indicates that communication to all SGPs is down. See the "Signaling Gateway Failure - Signaling (113)" section on page 10-131 to determine why the associated SGs are down.

Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)

The Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) alarm (major) indicates that the SCTP association is degraded. The primary cause of the alarm is that a single Ethernet connection on CA or SGP is unplugged or severed. To correct the primary cause of the alarm, plug in all Ethernet connections or repair if severed. The secondary cause of the alarm is a SCTP communication problem - or protocol timeout. To correct the secondary cause of the alarm, use a snooper application to determine why the SCTP association is degraded.

Message Transfer Part 3 User Adapter Troubleshooting Procedure

This alarm indicates that one of the two sides of the multi-homed SCTP connection is down. Communication still exists if the other side of the multi-homed connection is up. Refer to the "Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)" section on page 10-130, or contact the Cisco TAC for assistance in resolving this issue.

Signaling Connection Control Part User Adapter Troubleshooting Procedure

This is either an IP routing problem or an ITP Ethernet port hardware failure. Change the hardware immediately, if it is a hardware failure, to prevent dual outage of the ITP's IP communication.

Stream Control Transmission Protocol Association Configuration Error - Signaling (112)

The Stream Control Transmission Protocol Association Configuration Error alarm (minor) indicates that a SCTP association configuration error has occurred. The primary cause of the alarm is that the destination IP address is invalid. To correct the primary cause of the alarm, input a new destination IP address, see the log for additional details. The secondary cause of the alarm is that the local IP address is invalid. To correct the secondary cause of the alarm, input new local IP address information. The ternary cause of the alarm is that the IP Routing Table is not configured properly. To correct the ternary cause of the alarm, have the system administrator configure IP routing table.

Message Transfer Part 3 User Adapter Troubleshooting Procedure

This alarm indicates that there is a provisioning error keeping the Cisco BTS 10200 Softswitch from properly configuring the SCTP association. Perform the following steps to resolve the problem:

Step 1 To get more information about this alarm, look at the platform.log for error messages containing the string "Multipurpose Internet Mail (MIM) configuration (CFG)."

Step 2 Perform Step 2 of the "Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)" section on page 10-130 to verify that your IP addresses and ports are properly configured on the Cisco BTS 10200 Softswitch.

Step 3 Contact the Cisco TAC for assistance in resolving this issue.

Signaling Connection Control Part User Adapter Troubleshooting Procedure

Refer to Chapter 13, "Network Troubleshooting" to verify that the IP addresses and ports are properly configured on the Cisco BTS 10200 Softswitch.

Signaling Gateway Failure - Signaling (113)

The Signaling Gateway Failure alarm (major) indicates that all associated signaling gateway processes are out-of-service. The primary cause of the alarm is that all associated Signaling Gateway Processes are out-of-service. To correct the primary cause of the alarm, determine why each associated Signaling Gateway Process is out-of-service (see SGP alarm definition).

This alarm indicates that communication at the M3UA layer to an SG has failed. M3UA communications at all SGPs that make up the SG are unavailable. See the "Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)" section on page 10-130 to determine why the associated SGPs are down.

Signaling Gateway Process Is Out-of-Service - Signaling (114)

The Signaling Gateway Process is Out-of-Service alarm (major) indicates that all SCTP associations between the SGP and the CA are out-of-service. The primary cause of the alarm is that all SCTP associations between the SGP and the CA are out-of-service. To correct the primary cause of the alarm, see the SCTP Association Alarm definition to determine how to rectify the problem. The secondary cause of the alarm is that the M3UA layer is down between the CA and the SGP. To correct the secondary cause of the alarm, use a snooper utility to determine why M3UA layer is down. Also see the log for additional information.

This alarm indicates that communication at the M3UA layer to an SGP has failed. In the majority of cases, there will also be a related SCTP Association Failure alarm. If this is the case, proceed to the "Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)" section on page 10-130. Otherwise, the problem is at the M3UA layer. Call the Cisco TAC for assistance.

Destination Point Code User Part Unavailable - Signaling (116)

The Destination Point Code User Part Unavailable alarm (major) indicates that a layer 4 user part, such as ISUP, is unavailable at the DPC in the SS7 network. The primary cause of the alarm is that the SGP sent a DUPU M3UA message to the CA indicating that an user part is unavailable on at a DPC. To correct the primary cause of the alarm, contact the SS7 network administrator to report the user part unavailable problem related to the DPC so communication can be restored.

Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)

The Circuit Validation Test Message Received for an Unequipped Circuit Identification Code alarm (minor) indicates that a CVT message was received for an unequipped CIC. The primary cause of the alarm is that the CIC is not provisioned. To correct the primary cause of the alarm, provision the CIC.

Circuit Verification Response Received with Failed Indication - Signaling (118)

The Circuit Verification Response Received with Failed Indication alarm (minor) indicates that a CVR message was received with a failure indication. The primary cause of the alarm is that a CIC mismatch has occurred. To correct the primary cause of the alarm, perform an internal test such as checking that the CIC is assigned to a circuit between the sending and the receiving switch.

Signaling System 7 Adapter Process Faulty - Signaling (119)

The Signaling System 7 Adapter Process Faulty alarm (critical) indicates that a S7A process is faulty. The primary cause of the alarm is that an OMNI or a S7A exception has occurred. To correct the primary cause of the alarm, check OMNI process. The S7A process will restart itself if the S7A maximum restart threshold has not been exceeded.

Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)

The Signaling System 7 Module/Signaling System 7 Adapter Faulty alarm (critical) indicates that the S7M/S7A processes are faulty. The primary cause of the alarm is that an OMNI failure has occurred. To correct the primary cause of the alarm, check the OMNI status. An automatic failover will occur in a duplex configuration.

Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)

The Message Transfer Part 3 User Adapter Cannot Go Standby alarm (major) indicates that the M3UA process cannot go into standby mode. The primary cause of the alarm is that no INACTIVE ACK messages are being received from any Signaling Gateway. The SG or SCTP associations are probably down. To correct the primary cause of the alarm, investigate other alarms to see if SGs are down or if SCTP associations are down. Take corrective action according to those alarms.

This alarm is raised at initial startup or during failover by the Cisco BTS 10200 Softswitch node that is trying to go into platform Standby mode. See the "Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)" section on page 10-130 to determine why the Cisco BTS 10200 Softswitch is unable to communicate with any of the SGs at the M3UA layer. See the "Verify the Stream Control Transmission Protocol Association Status" section on page 13-2 to determine why the Cisco BTS 10200 Softswitch is unable to communicate with any of the ITPs at the SUA layer.

Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)

The Message Transfer Part 3 User Adapter Cannot Go Active alarm (major) indicates that the M3UA process cannot go into active mode. The primary cause of the alarm is that no ACTIVE ACK messages are being received from any Signaling Gateway. The SG or SCTP associations are probably down. To correct the primary cause of the alarm, investigate other alarms to see if SGs are down or if the SCTP associations are down. Take corrective action according to those alarms.

This alarm is raised at initial startup or during failover by the Cisco BTS 10200 Softswitch node that is trying to go into platform Active mode. It occurs when this Cisco BTS 10200 Softswitch node is unable to communicate properly with any SGs to tell them that all active call traffic should be routing towards the Cisco BTS 10200 Softswitch. See the "Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)" section on page 10-130 to determine why the Cisco BTS 10200 Softswitch is unable to communicate with any of the ITPs at the M3UA layer. Refer to the "Verify the Stream Control Transmission Protocol Association Status" section on page 13-2 to determine why the Cisco BTS 10200 Softswitch is unable to communicate with any of the ITPs at the SUA layer.

Remote Subsystem is Out Of Service - Signaling (124)

The Remote Subsystem is out of Service alarm (minor) indicates that the remote subsystem is out-of-service. The primary cause of the alarm is that the link lost connection or the remote subsystem is out-of-service. This alarm indicates the remote subsystem is out-of-service. To correct the primary cause of the alarm, contact your service control point (SCP) service provider for assistance.

Signaling Connection Control Part Routing Error - Signaling (125)

The Signaling Connection Control Part Routing Error alarm (major) indicates that the SCCP route was invalid or not available. The primary cause of the alarm is that the SCCP route is invalid or is not available. To correct the primary cause of the alarm, provision the right SCCP route.

Signaling Connection Control Part Binding Failure - Signaling (126)

The Signaling Connection Control Part Binding Failure alarm (major) indicates that the SCCP binding failed. The primary cause of the SCCP Binding Failure alarm is that the Trillium stack binding failed. To correct the primary cause of the alarm, re-initialize the TSA process or remove the subsystem from the EMS table and add it again.

Transaction Capabilities Application Part Binding Failure - Signaling (127)

The Transaction Capabilities Application Part Binding Failure alarm (major) indicates that the TCAP binding failed. This alarm is raised when the TCAP layer does not have enough service access point (SAP) to bind for the subsystem. Currently only 16 subsystems are allowed on the same platform. Check the Subsystem table to see if you have more than 16 subsystems on the same platform, Feature Server for POTS, Tandem, and Centrex services (FSPTC) or Feature Server for AIN services (FSAIN). The primary cause of the TCAP Binding Failure alarm is that the Trillium stack binding failed. To correct the primary cause of the alarm, re-initialize the TSA process or remove the subsystem from the EMS table and add it again.

Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)

The Session Initiation Protocol Trunk Operationally Out-of-Service alarm (critical) indicates that the SIP trunk is operationally out-of-service. The primary cause of the alarm is that the Cisco BTS 10200 Softswitch is unable to communicate with a remote SIP party (Call-Agent or Proxy) over a SIP or SIP-T trunk. To correct the primary cause of the alarm, verify that the DNS resolution exists, if TSAP address of the remote entity is a domain name. Verify the remote entity is reachable by ICMP ping, using the Trunk TSAP address from the alarm event report. If the same alarm is reported on all the softswitch trunk groups, then verify that the network connection is operational. If the ping is not successful, then diagnose the issue that prevents the TSAP address from being reached. Verify the SIP application is running on the remote host and listening on the port specified in the TSAP address.

Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)

The Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down alarm (minor) indicates that an IP interface link to the SS7 signaling gateway is down. The primary cause of the alarm is an interface hardware problem. To correct the primary cause of the alarm, check the link interfaces.

All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)

The All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down alarm (critical) indicates that all IP interface links to the SS7 signaling gateway are down. The primary cause of the alarm is an interface hardware problem. To correct the primary cause of the alarm, check the link interfaces.

One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)

The One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down alarm (minor) indicates that one IP interface link to the SS7 signaling gateway is down. The primary cause of the alarm is an interface hardware problem. To correct the primary cause of the alarm, check the link interfaces.

Stream Control Transmission Protocol Association Congested - Signaling (150)

The Stream Control Transmission Protocol Association Congested alarm (minor) indicates that the SCTP association is congested. The primary cause of the alarm is that the network is congested. To correct the primary cause of the alarm, clean off the network congestion caused by routing or switching issues. The secondary cause of the alarm is that the CPU is throttled. To correct the secondary cause of the alarm, upgrade to a more powerful platform or offload some traffic.

Termination Permanent Error Code Received - Signaling (151)

The Termination Permanent Error Code Received alarm (minor) indicates that a termination permanent error code was received. The primary cause of the alarm is that a fault has occurred in the gateway device. To correct the primary cause of the alarm, maintenance required on the gateway or termination.