CHAPTER 10

Signaling Troubleshooting

Revised: May 14, 2012, OL-25016-02

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the Signaling events
- Troubleshooting Signaling Alarms—Provides the information needed for troubleshooting and correcting the 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; the event and alarms are arranged in numerical order. Table 10-1 lists all of the signaling events and alarms by severity.

Note Refer to the "Obtaining Documentation and Submitting a Service Request" section on page 1 for detailed instructions on contacting Cisco TAC and opening a service request.

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	Information	Not Used
Signaling (12)	Signaling (7)	Signaling (10)	Signaling (4)	Signaling (1)	Signaling (2)
Signaling (64)	Signaling (8)	Signaling (14)	Signaling (6)	Signaling (42)	Signaling (3)
Signaling (65)	Signaling (9)	Signaling (15)	Signaling (25)	Signaling (43)	Signaling (5)
Signaling (69)	Signaling (11)	Signaling (16)	Signaling (26)	Signaling (44)	Signaling (35)
Signaling (75)	Signaling (13)	Signaling (17)	Signaling (27)	Signaling (45)	Signaling (37)
Signaling (80)	Signaling (19)	Signaling (18)	Signaling (28)	Signaling (46)	Signaling (38)
Signaling (81)	Signaling (20)	Signaling (22)	Signaling (29)	Signaling (49)	Signaling (39)
Signaling (82)	Signaling (21)	Signaling (24)	Signaling (30)	Signaling (50)	Signaling (41)
Signaling (83)	Signaling (23)	Signaling (36)	Signaling (31)	Signaling (51)	Signaling (47)
Signaling (84)	Signaling (40)	Signaling (78)	Signaling (32)	Signaling (52)	Signaling (48)
Signaling (85)	Signaling (59)	Signaling (92)	Signaling (33)	Signaling (53)	Signaling (56)
Signaling (107)	Signaling (63)	Signaling (93)	Signaling (34)	Signaling (54)	Signaling (67)
Signaling (110)	Signaling (66)	Signaling (94)	Signaling (60)	Signaling (55)	Signaling (123)
Signaling (119)	Signaling (68)	Signaling (95)	Signaling (70)	Signaling (57)	Signaling (128)
Signaling (120)	Signaling (79)	Signaling (96)	Signaling (71)	Signaling (58)	Signaling (129)
Signaling (142)	Signaling (86)	Signaling (97)	Signaling (72)	Signaling (61)	Signaling (130)
Signaling (144)	Signaling (87)	Signaling (98)	Signaling (73)	Signaling (62)	Signaling (131)
Signaling (153)	Signaling (88)	Signaling (99)	Signaling (74)	Signaling (76)	Signaling (148)
Signaling (154)	Signaling (89)	Signaling (100)	Signaling (115)	Signaling (77)	Signaling (149)
Signaling (162)	Signaling (90)	Signaling (101)	Signaling (132)	Signaling (104)	
Signaling (173)	Signaling (91)	Signaling (102)	Signaling (138)	Signaling (105)	
Signaling (174)	Signaling (103)	Signaling (106)	Signaling (141)	Signaling (133)	
Signaling (175)	Signaling (108)	Signaling (112)	Signaling (146)	Signaling (134)	
Signaling (176)	Signaling (109)	Signaling (117)	Signaling (147)	Signaling (135)	
	Signaling (111)	Signaling (118)	Signaling (158)	Signaling (136)	

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

Critical	Major	Minor	Warning	Information	Not Used
	Signaling (113)	Signaling (124)	Signaling (159)	Signaling (137)	
	Signaling (114)	Signaling (143)	Signaling (160)	Signaling (139)	
	Signaling (116)	Signaling (145)	Signaling (161)	Signaling (140)	
	Signaling (121)	Signaling (150)	Signaling (165)	Signaling (152)	
	Signaling (122)	Signaling (151)	Signaling (166)	Signaling (155)	
	Signaling (125)	Signaling (170)	Signaling (167)	Signaling (169)	
	Signaling (126)	Signaling (171)	Signaling (168)	Signaling (178)	
	Signaling (127)		Signaling (177)		
	Signaling (156)				
	Signaling (157)				
	Signaling (163)				
	Signaling (164)				
	Signaling (172)				
	Signaling (179)				
	Signaling (182)				

Signaling (1)

Table 10-2 lists the details of the Signaling (1) informational event. For additional information, refer to the "Test Report—Signaling (1)" section on page 10-103.

Table 10-2 Signaling (1) Details

Description	Test Report
Severity	Information
Threshold	10000
Throttle	0

Signaling (2)

Signaling (2) is not used.

Signaling (3)

Signaling (3) is not used.

Signaling (4)

Table 10-3 lists the details of the Signaling (4) warning event. To monitor and correct the cause of the event, refer to the "Invalid Message Received—Signaling (4)" section on page 10-103.

Table 10-3 Signaling (4) Details

Description	Invalid Message Received
Severity	Warning
Threshold	100
Throttle	0
Datawords	Endpoint Name—STRING [40] Message Type—STRING [40]
Primary Cause	This event is 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 reprovisioned.

Signaling (5)

Signaling (5) is not used.

Signaling (6)

Table 10-4 lists the details of the Signaling (6) warning event. To monitor and correct the cause of the event, refer to the "Database Module Function Call Failure—Signaling (6)" section on page 10-103.

Table 10-4 Signaling (6) Details

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 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)

Table 10-5 lists the details of the Signaling (7) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Socket Failure—Signaling (7)" section on page 10-136.

Table 10-5 Signaling (7) Details

Description	Socket Failure
Severity	Major
Threshold	30
Throttle	0
Datawords	Reason Text—STRING [30]
Primary Cause	Issued when there is a failure in creating or binding to the User Datagram Protocol (UDP) socket.
Primary Action	Verify that there is no conflict in the port assignment with other processes in the system and ensure that no previous instance of the same process is still running.
Secondary Cause	A software logic problem has occurred.
Secondary Action	Contact the Cisco Technical Assistance Center (TAC).

Signaling (8)

Table 10-6 lists the details of the Signaling (8) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Session Initiation Protocol Message Receive Failure—Signaling (8)" section on page 10-137.

Table 10-6 Signaling (8) Details

Description	Session Initiation Protocol Message Receive Failure (SIP Message Receive Failure)
Severity	Major
Threshold	30
Throttle	0
Datawords	Reason Text—STRING [50]
Primary Cause	Operating system level network errors have occurred or an invalid network configuration exists.
Primary Action	Have your network administrator resolve the network errors. Contact Cisco TAC if you need assistance. Manually clear the alarm. Restart this call agent instance using the **platform start** command.

Signaling (9)

Table 10-7 lists the details of the Signaling (9) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Timeout on Internet Protocol Address—Signaling (9)" section on page 10-137.

Table 10-7 Signaling (9) Details

Description	Timeout on Internet Protocol Address (Timeout on IP 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 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 the **control mgw** command to put it in service.

Signaling (10)

Table 10-8 lists the details of the Signaling (10) minor alarm. 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 10-138.

Table 10-8 Signaling (10) Details

Description	Failed to Send Complete Session Initiation Protocol Message (Failed to Send Complete SIP 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 a SIP message because the message exceeded 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.

Signaling (11)

Table 10-9 lists the details of the Signaling (11) major alarm. 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 10-138.

Table 10-9 Signaling (11) Details

Description	Failed to Allocate Session Initiation Protocol Control Block (Failed to Allocate SIP 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 for the changes to take effect.

Signaling (12)

Table 10-10 lists the details of the Signaling (12) critical alarm. 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 10-138.

Table 10-10 Signaling (12) Details

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	The feature server platform is down or is not operating properly.
Primary Action	Restart the applicable feature server.

Signaling (13)

Table 10-11 lists the details of the Signaling (13) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling System 7 Signaling Link Down—Signaling (13)" section on page 10-138.

Table 10-11 Signaling (13) Details

Description	Signaling System 7 Signaling Link Down (SS7 Signaling Link Down)
Severity	Major
Threshold	100
Throttle	0
Datawords	Link_Number—ONE_BYTE Link_Name—STRING [25]
Primary Cause	The Signaling System 7 (SS7) trunk group may be out-of-service (OOS).
Primary Action	Use the **control ss7-trunk-grp** command 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	The SS7 link may be disconnected or faulty.
Ternary Action	Check the Ulticom local configuration.
Subsequent Cause	The remote SS7 signaling site may be down or incorrectly configured.
Subsequent Action	Check the Ulticom remote configuration.

Signaling (14)

Table 10-12 lists the details of the Signaling (14) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Is Remotely Inhibited—Signaling (14)" section on page 10-139.

Table 10-12 Signaling (14) Details

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 the events at the network level for any that are related to the specified SS7 link. Restorative actions need to be taken on the remote end.

Signaling (15)

Table 10-13 lists the details of the Signaling (15) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Is Locally Inhibited—Signaling (15)" section on page 10-139.

Table 10-13 Signaling (15) Details

Description	Link is Locally Inhibited
Severity	Minor
Threshold	100
Throttle	0
Datawords	Link Number—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 nonoperational, restore it to service.

Signaling (16)

Table 10-14 lists the details of the Signaling (16) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Is Congested—Signaling (16)" section on page 10-139.

Table 10-14 Signaling (16) Details

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)

Table 10-15 lists the details of the Signaling (17) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link: Local Processor Outage—Signaling (17)" section on page 10-139.

Table 10-15 Signaling (17) Details

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 the underlying platform instances that support the specified SS7 link. Verify that the process and or platform are restarted and returned to service.

Signaling (18)

Table 10-16 lists the details of the Signaling (18) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link: Remote Processor Outage—Signaling (18)" section on page 10-139.

Table 10-16 Signaling (18) Details

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)

Table 10-17 lists the details of the Signaling (19) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Set Inaccessible—Signaling (19)" section on page 10-139.

Table 10-17 Signaling (19) Details

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)

Table 10-18 lists the details of the Signaling (20) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Set Congestion—Signaling (20)" section on page 10-140.

Table 10-18 Signaling (20) Details

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)

Table 10-19 lists the details of the Signaling (21) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Route Set Failure—Signaling (21)" section on page 10-140.

Table 10-19 Signaling (21) Details

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 to verify its restoral to service.

Signaling (22)

Table 10-20 lists the details of the Signaling (22) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Route Set Congested—Signaling (22)" section on page 10-140.

Table 10-20 Signaling (22) Details

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 the 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)

Table 10-21 lists the details of the Signaling (23) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Destination Point Code Unavailable—Signaling (23)" section on page 10-141.

Table 10-21 Signaling (23) Details

Description	Destination Point Code Unavailable (DPC 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 and the affected DPC.
Primary Action	Verify that an alternate routing has been assigned for traffic destined to the affected DPC.

Signaling (24)

Table 10-22 lists the details of the Signaling (24) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Destination Point Code Congested—Signaling (24)" section on page 10-142.

Table 10-22 Signaling (24) Details

Description	Destination Point Code Congested (DPC 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 the 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)

Table 10-23 lists the details of the Signaling (25) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Blocking Message—Signaling (25)" section on page 10-106.

Table 10-23 Signaling (25) Details

Description	Unanswered Blocking Message (Unanswered BLO)
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 are 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)

Table 10-24 lists the details of the Signaling (26) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Unblocking Message—Signaling (26)" section on page 10-106.

Table 10-24 Signaling (26) Details

Description	Unanswered Unblocking Message (Unanswered UBL)
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 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 are 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)

Table 10-25 lists the details of the Signaling (27) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Circuit Group Blocking Message—Signaling (27)" section on page 10-107.

Table 10-25 Signaling (27) Details

Description	Unanswered Circuit Group Blocking Message (Unanswered CGB)
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 are 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)

Table 10-26 lists the details of the Signaling (28) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Circuit Group Unblocking Message—Signaling (28)" section on page 10-107.

Table 10-26 Signaling (28) Details

Description	Unanswered Circuit Group Unblocking Message (Unanswered CGU)
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 are 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)

Table 10-27 lists the details of the Signaling (29) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Circuit Query Message—Signaling (29)" section on page 10-107.

Table 10-27 Signaling (29) Details

Description	Unanswered Circuit Query Message (Unanswered CQM)
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 are 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)

Table 10-28 lists the details of the Signaling (30) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Circuit Validation Test Message—Signaling (30)" section on page 10-108.

Table 10-28 Signaling (30) Details

Description	Unanswered Circuit Validation Test Message (Unanswered CVT)
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 are 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)

Table 10-29 lists the details of the Signaling (31) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Reset Circuit Message—Signaling (31)" section on page 10-108.

Table 10-29 Signaling (31) Details

Description	Unanswered Reset Circuit Message (Unanswered RSC)
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 are 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)

Table 10-30 lists the details of the Signaling (32) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Group Reset Message—Signaling (32)" section on page 10-108.

Table 10-30 Signaling (32) Details

Description	Unanswered Group Reset Message (Unanswered GRS)
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 are 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)

Table 10-31 lists the details of the Signaling (33) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Release Message—Signaling (33)" section on page 10-109.

Table 10-31 Signaling (33) Details

Description	Unanswered Release Message (Unanswered REL)
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 are 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)

Table 10-32 lists the details of the Signaling (34) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Continuity Check Request Message—Signaling (34)" section on page 10-109.

Table 10-32 Signaling (34) Details

Description	Unanswered Continuity Check Request Message (Unanswered CCR)
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 are 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 (35)

Signaling (35) is not used.

Signaling (36)

Table 10-33 lists the details of the Signaling (36) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Trunk Locally Blocked—Signaling (36)" section on page 10-142.

Table 10-33 Signaling (36) Details

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	No action required.

Signaling (37)

Signaling (37) is not used.

Signaling (38)

Signaling (38) is not used.

Signaling (39)

Signaling (39) is not used.

Signaling (40)

Table 10-34 lists the details of the Signaling (40) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Trunk Remotely Blocked—Signaling (40)" section on page 10-142.

Table 10-34 Signaling (40) Details

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 an SS7 trunk. Issued when a service OOS message is received for Integrated Services Digital Network (ISDN) trunks. Issued when Reverse Make Busy (RBZ) signal is received for channel-associated signaling (CAS) operator trunk.
Primary Action	No action required. You can manually recover from this condition locally by controlling the affected trunks to the unequipped (UEQP) state and back to the INS state.

Signaling (41)

Signaling (41) is not used.

Signaling (42)

Table 10-35 lists the details of the Signaling (42) informational event. For additional information, refer to the "Continuity Testing Message Received on the Specified Circuit Identification Code—Signaling (42)" section on page 10-110.

Table 10-35 Signaling (42) Details

Description	Continuity Testing Message Received on the Specified Circuit Identification Code (COT Message Received on the Specified CIC)
Severity	Information
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)

Table 10-36 lists the details of the Signaling (43) informational event. 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 10-110.

Table 10-36 Signaling (43) Details

Description	Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code (RLC Received in Response to RSC Message on the Specified CIC)
Severity	Information
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 an RSC message on the specified CIC.
Primary Action	No action required.

Signaling (44)

Table 10-37 lists the details of the Signaling (44) informational event. For additional information, refer to the "Continuity Recheck Is Performed on Specified Circuit Identification Code—Signaling (44)" section on page 10-110.

Table 10-37 Signaling (44) Details

Description	Continuity Recheck is Performed on Specified Circuit Identification Code (Continuity Recheck is Performed on Specified CIC)
Severity	Information
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)

Table 10-38 lists the details of the Signaling (45) informational event. For additional information, refer to the "Circuit Is Unequipped on Remote Side—Signaling (45)" section on page 10-110.

Table 10-38 Signaling (45) Details

Description	Circuit is Unequipped on Remote Side
Severity	Information
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 find out if an existing circuit was unequipped causing a status mismatch with the local end.

Signaling (46)

Table 10-39 lists the details of the Signaling (46) informational event. For additional information, refer to the "Specified Circuit Identification Code Is Invalid for the Operation—Signaling (46)" section on page 10-110.

Table 10-39 Signaling (46) Details

Description	Specified Circuit Identification Code is Invalid for the Operation (Specified CIC is Invalid for the Operation)
Severity	Information
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.

Signaling (47)

Signaling (47) is not used.

Signaling (48)

Signaling (48) is not used.

Signaling (49)

Table 10-40 lists the details of the Signaling (49) informational event. For additional information, refer to the "A General Processing Error Encountered—Signaling (49)" section on page 10-111.

Table 10-40 Signaling (49) Details

Description	A General Processing Error Encountered
Severity	Information
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 ensure proper operation.

Signaling (50)

Table 10-41 lists the details of the Signaling (50) informational event. For additional information, refer to the "Unexpected Message for the Call State Is Received: Clear Call—Signaling (50)" section on page 10-111.

Table 10-41 Signaling (50) Details

Description	Unexpected Message for the Call State is Received: Clear Call
Severity	Information
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 ensure proper operation.

Signaling (51)

Table 10-42 lists the details of the Signaling (51) informational event. For additional information, refer to the "Set Trunk State as Remotely Unequipped—Signaling (51)" section on page 10-111.

Table 10-42 Signaling (51) Details

Description	Set Trunk State as Remotely Unequipped
Severity	Information
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 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)

Table 10-43 lists the details of the Signaling (52) informational event. For additional information, refer to the "Set Trunk State as Not Remotely Blocked—Signaling (52)" section on page 10-111.

Table 10-43 Signaling (52) Details

Description	Set Trunk State as Not Remotely Blocked
Severity	Information
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)

Table 10-44 lists the details of the Signaling (53) informational event. For additional information, refer to the "Set Trunk State as Remotely Blocked—Signaling (53)" section on page 10-111.

Table 10-44 Signaling (53) Details

Description	Set Trunk State as Remotely Blocked
Severity	Information
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)

Table 10-45 lists the details of the Signaling (54) informational event. For additional information, refer to the "Circuit Validation Test Aborted—Signaling (54)" section on page 10-111.

Table 10-45 Signaling (54) Details

Description	Circuit Validation Test Aborted
Severity	Information
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 failed a validation test due to an internal failure.
Primary Action	Verify that the SS7 signaling adapter process and the SS7 interface are operating normally.

Signaling (55)

Table 10-46 lists the details of the Signaling (55) informational event. For additional information, refer to the "Circuit Validation Successful—Signaling (55)" section on page 10-112.

Table 10-46 Signaling (55) Details

Description	Circuit Validation Successful
Severity	Information
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.

Signaling (56)

Signaling (56) is not used.

Signaling (57)

Table 10-47 lists the details of the Signaling (57) informational event. For additional information, refer to the "Continuity Recheck Failed—Signaling (57)" section on page 10-112.

Table 10-47 Signaling (57) Details

Description	Continuity Recheck Failed
Severity	Information
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 that the SS7 signaling adapter process and the SS7 interface are operating normally.

Signaling (58)

Table 10-48 lists the details of the Signaling (58) informational event. For additional information, refer to the "Continuity Recheck Successful—Signaling (58)" section on page 10-112.

Table 10-48 Signaling (58) Details

Description	Continuity Recheck Successful
Severity	Information
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)

Table 10-49 lists the details of the Signaling (59) major alarm. 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 10-142.

Table 10-49 Signaling (59) Details

Description	Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway (Auto State Change for ISDN 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)

Table 10-50 lists the details of the Signaling (60) warning event. 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 10-112.

Table 10-50 Signaling (60) Details

Description	Integrated Services Digital Network Status Message Containing Error Indication Received (ISDN 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 the service state.

Signaling (61)

Table 10-51 lists the details of the Signaling (61) informational event. For additional information, refer to the "Trunk Operational State Changed by Service Message—Signaling (61)" section on page 10-112.

Table 10-51 Signaling (61) Details

Description	Trunk Operational State Changed by Service Message
Severity	Information
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 by 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)

Table 10-52 lists the details of the Signaling (62) informational event. For additional information, refer to the "Received Integrated Services Digital Network Restart Message—Signaling (62)" section on page 10-113.

Table 10-52 Signaling (62) Details

Description	Received Integrated Services Digital Network Restart Message (Received ISDN Restart Message)
Severity	Information
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)

Table 10-53 lists the details of the Signaling (63) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Media Gateway/Termination Faulty—Signaling (63)" section on page 10-142.

Table 10-53 Signaling (63) Details

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, an unknown package type, an 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)

Table 10-54 lists the details of the Signaling (64) critical alarm. 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 10-143.

Table 10-54 Signaling (64) Details

Description	Media Gateway Adapter Running out of Shared Memory Pools (MGA 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 storage for an inter-process communication (IPC) message due to a lack of resources.
Primary Action	Contact Cisco TAC for assistance.

Signaling (65)

Table 10-55 lists the details of the Signaling (65) critical alarm. 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 10-143.

Table 10-55 Signaling (65) Details

Description	Media Gateway Adapter Running out of Heap Memory (MGA Running out of Heap Memory)
Severity	Critical
Threshold	100
Throttle	0
Primary Cause	Issued when the MGCP signaling adapter was unable to allocate data storage for an IPC message from the heap due to a lack of resources.
Primary Action	Contact Cisco TAC for assistance.

Signaling (66)

Table 10-56 lists the details of the Signaling (66) major alarm. 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 10-143.

Table 10-56 Signaling (66) Details

Description	Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) (CA Internal Error (Because of Which MGA 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 the log files to Cisco TAC for analysis and corrective action.

Signaling (67)

Signaling (67) is not used.

Signaling (68)

Signaling (68) is not used.

Signaling (69)

Table 10-57 lists the details of the Signaling (69) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Call Agent Is Not Up or Is Not Responding to the Feature Server—Signaling (69)" section on page 10-143.

Table 10-57 Signaling (69) Details

Description	Call Agent is not Up or is not Responding to the Feature Server
Severity	Critical
Threshold	100
Throttle	0
Datawords	Configured CA Name—STRING [70]
Primary Cause	The Call Agent (CA) to Feature Server (FS) link has had a communication failure due to wrong system configuration; or the CA or FS is down.
Primary Action	Check the configuration related to the CA to FS communication link. Check the FS table entries and the CA entry.

Signaling (70)

Table 10-58 lists the details of the Signaling (70) warning event. 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 10-114.

Table 10-58 Signaling (70) Details

Description	Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication (ISDN 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 that the provisioning of the backhaul port is correct at both the call agent and media gateway.

Signaling (71)

Table 10-59 lists the details of the Signaling (71) warning event. 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 10-114.

Table 10-59 Signaling (71) Details

Description	Integrated Services Digital Network Unable to Establish D-channel (ISDN 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)

Table 10-60 lists the details of the Signaling (72) warning event. 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 10-114.

Table 10-60 Signaling (72) Details

Description	Integrated Services Digital Network—Calls Lost Due to D-channel Down for Period of Time (ISDN—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 the connection between the private branch exchange (PBX) and the media gateway.
Primary Action	Resupply power to the media gateway and verify that the connection between the PBX and the media gateway is intact.

Signaling (73)

Table 10-61 lists the details of the Signaling (73) warning event. 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 10-114.

Table 10-61 Signaling (73) Details

Description	Integrated Services Digital Network—Unable to Send Restart Due to Restart Timer Expired (ISDN—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)

Table 10-62 lists the details of the Signaling (74) warning event. 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 10-115.

Table 10-62 Signaling (74) Details

Description	Integrated Services Digital Network: Unable to Send the Service Due to the Service Timer Expired (ISDN: 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 service timer is set to an appropriate level.

Signaling (75)

Table 10-63 lists the details of the Signaling (75) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling System 7 Stack Not Ready—Signaling (75)" section on page 10-143.

Table 10-63 Signaling (75) Details

Description	Signaling System 7 Stack Not Ready (SS7 Stack Not Ready)
Severity	Critical
Threshold	100
Throttle	0
Datawords	LogicalName—STRING [64]
Primary Cause	SS7 stack is not configured properly.
Primary Action	Check SS7 stack configuration.
Secondary Cause	SS7 stack is not up and functioning.
Secondary Action	Check SS7 stack status. Execute the platform **start -i omni** command to bring up SS7 stack.

Signaling (76)

Table 10-64 lists the details of the Signaling (76) informational event. For additional information, refer to the "Timeout on Remote Instance—Signaling (76)" section on page 10-115.

Table 10-64 Signaling (76) Details

Description	Timeout on Remote Instance
Severity	Information
Threshold	100
Throttle	0
Datawords	Port Number—TWO_BYTES Hostname—STRING [64]
Primary Cause	The communication between the call agent and the remote instance is faulty.
Primary Action	No action needed.

Signaling (77)

Table 10-65 lists the details of the Signaling (77) informational event. For additional information, refer to the "Integrated Services Digital Network D-Channel Switchover for Not Facility Associated Signaling—Signaling (77)" section on page 10-115.

Table 10-65 Signaling (77) Details

Description	Integrated Services Digital Network D-channel Switchover for Not Facility Associated Signaling (ISDN D-channel Switchover for NFAS)
Severity	Information
Threshold	100
Throttle	0
Datawords	Trunk Group ID—FOUR_BYTES Trunk Group Index—FOUR_BYTES
Primary Cause	The D-channels were manually switched through use of the command line interface (CLI).
Primary Action	Verify the operator action.
Secondary Cause	The active D-channel is lost.
Secondary Action	Verify that the gateway is operational and that the connection to the PBX is good.

Signaling (78)

Table 10-66 lists the details of the Signaling (78) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Integrated Services Digital Network Single D-Channel Down for Not Facility Associated Signaling—Signaling (78)" section on page 10-144.

Table 10-66 Signaling (78) Details

Description	Integrated Services Digital Network Single D-channel Down for Not Facility Associated Signaling (ISDN Single D-channel Down for NFAS)
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 the primary rate interface (PRI) is down.
Primary Action	Check the gateway power and the gateway connection to the PBX.

Signaling (79)

Table 10-67 lists the details of the Signaling (79) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Trunking Gateway Unreachable—Signaling (79)" section on page 10-144.

Table 10-67 Signaling (79) Details

Description	Trunking 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	The Trunking Gateway is not responding to keep-alive Audit Endpoint messages.
Primary Action	Check the IP connectivity status between Cisco BTS 10200 Call Agent and the Trunking Gateway.

Signaling (80)

Table 10-68 lists the details of the Signaling (80) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Out of Bounds, Memory/Socket Error—Signaling (80)" section on page 10-144.

Table 10-68 Signaling (80) Details

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	Increase the random access memory (RAM) and contact Cisco TAC.
Secondary Cause	Out of IPC pool memory.
Secondary Action	Resize the IPC pool size in the platform configuration file.
Ternary Cause	A socket error has occurred. An inappropriate or already bound socket is in use.
Ternary Action	Check the UDP port supplied with the media gateway adapter (MGA) command-line for validity and prior use.

Signaling (81)

Table 10-69 lists the details of the Signaling (81) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Insufficient Heap Memory—Signaling (81)" section on page 10-144.

Table 10-69 Signaling (81) Details

Description	Insufficient Heap Memory
Severity	Critical
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32]
Primary Cause	Issued when the H.323 Protocol (H.323) signaling adapter is unable to allocate memory from the system.
Primary Action	Contact Cisco TAC for assistance.

Signaling (82)

Table 10-70 lists the details of the Signaling (82) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Insufficient Shared Memory Pools—Signaling (82)" section on page 10-144.

Table 10-70 Signaling (82) Details

Description	Insufficient Shared Memory Pools
Severity	Critical
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32]
Primary Cause	Issued when the H.323 signaling adapter was unable to allocate storage.
Primary Action	Contact Cisco TAC for corrective action.

Signaling (83)

Table 10-71 lists the details of the Signaling (83) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Error While Binding to Socket—Signaling (83)" section on page 10-145.

Table 10-71 Signaling (83) Details

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]
Primary Cause	An error has occurred while the system was binding to a socket.
Primary Action	Contact Cisco TAC.

Signaling (84)

Table 10-72 lists the details of the Signaling (84) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Reached Maximum Socket Limit—Signaling (84)" section on page 10-145.

Table 10-72 Signaling (84) Details

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 the platform.cfg file is wrong.
Primary Action	Reconfigure the platform.cfg file and restart the H3A process.

Signaling (85)

Table 10-73 lists the details of the Signaling (85) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Initialization Failure—Signaling (85)" section on page 10-145.

Table 10-73 Signaling (85) Details

Description	Initialization Failure
Severity	Critical
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Reason—STRING [128]
Primary Cause	A process initialization failure has occurred.
Primary Action	Check Dataword 2 (Reason) for the failure cause and take action accordingly.

Signaling (86)

Table 10-74 lists the details of the Signaling (86) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Remote H.323 Gateway Is Not Reachable—Signaling (86)" section on page 10-145.

Table 10-74 Signaling (86) Details

Description	Remote H.323 Gateway is not Reachable
Severity	Major
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Remote GW TSAP Addr—STRING [32]
Primary Cause	A loss of communication with a remote gateway has occurred.
Primary Action	Perform the standard connectivity tests—both the physical checks and the IP tests. Also, ensure that the gateway is not out of service.

Signaling (87)

Table 10-75 lists the details of the Signaling (87) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "H.323 Message Parsing Error—Signaling (87)" section on page 10-145.

Table 10-75 Signaling (87) Details

Description	H.323 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 H.323 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 its content or contact Cisco TAC.

Signaling (88)

Table 10-76 lists the details of the Signaling (88) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "H.323 Message Encoding Error—Signaling (88)" section on page 10-145.

Table 10-76 Signaling (88) Details

Description	H.323 Message Encoding Error
Severity	Major
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Reason—STRING [128]
Primary Cause	Unable to encode an H.323 message for sending.
Primary Action	This is indicative of a software bug. Contact Cisco TAC.

Signaling (89)

Table 10-77 lists the details of the Signaling (89) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Gatekeeper not Available/Reachable—Signaling (89)" section on page 10-146.

Table 10-77 Signaling (89) Details

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	The gatekeeper is not available or is unreachable.
Primary Action	Check network connectivity. Check to ensure that the gatekeeper (GK) is reachable by trying to ping GK IP address. If the GK is reachable, check to ensure that the GK is configured up.

Signaling (90)

Table 10-78 lists the details of the Signaling (90) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Alternate Gatekeeper Is Not Responding—Signaling (90)" section on page 10-146.

Table 10-78 Signaling (90) Details

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	The alternate gatekeeper is not responding.
Primary Action	Check network connectivity. Check to ensure that the alternate GK is reachable by trying to ping the alternate GK IP address. If the GK is reachable, check to ensure that the alternate GK is configured up.

Signaling (91)

Table 10-79 lists the details of the Signaling (91) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Endpoint Security Violation—Signaling (91)" section on page 10-146.

Table 10-79 Signaling (91) Details

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 H.323 security violation has occurred.
Primary Action	The password on the Cisco BTS 10200 and/or the gatekeeper is wrong—the H.323 gateway (H.323GW) table may not be provisioned properly or there is a time synchronization problem between the Cisco BTS 10200 and/or gatekeeper and the Network Time Protocol (NTP) server. Ensure that both the Cisco BTS 10200 and the gatekeeper are pointing to the same NTP server.

Signaling (92)

Table 10-80 lists the details of the Signaling (92) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Invalid Call Identifier—Signaling (92)" section on page 10-146.

Table 10-80 Signaling (92) Details

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	There is a software problem on the Cisco BTS 10200 or on an endpoint. Contact Cisco TAC.

Signaling (93)

Table 10-81 lists the details of the Signaling (93) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Invalid Call Reference Value—Signaling (93)" section on page 10-146.

Table 10-81 Signaling (93) Details

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	There is a software problem on the Cisco BTS 10200 or on an endpoint. Contact Cisco TAC.

Signaling (94)

Table 10-82 lists the details of the Signaling (94) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Invalid Conference Identifier—Signaling (94)" section on page 10-146.

Table 10-82 Signaling (94) Details

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	There is a software problem on the Cisco BTS 10200 or on an endpoint. Contact Cisco TAC.

Signaling (95)

Table 10-83 lists the details of the Signaling (95) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Invalid Message from the Network—Signaling (95)" section on page 10-147.

Table 10-83 Signaling (95) Details

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	An unsupported or invalid message type received from network.
Primary Action	Contact Cisco TAC.

Signaling (96)

Table 10-84 lists the details of the Signaling (96) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Internal Call Processing Error—Signaling (96)" section on page 10-147.

Table 10-84 Signaling (96) Details

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	Contact Cisco TAC.

Signaling (97)

Table 10-85 lists the details of the Signaling (97) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Insufficient Information to Complete Call—Signaling (97)" section on page 10-147.

Table 10-85 Signaling (97) Details

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	Contact Cisco TAC.

Signaling (98)

Table 10-86 lists the details of the Signaling (98) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "H.323 Protocol Inconsistencies—Signaling (98)" section on page 10-147.

Table 10-86 Signaling (98) Details

Description	H.323 Protocol Inconsistencies
Severity	Minor
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Call ID—EIGHT_BYTES Reason—STRING [128]
Primary Cause	The H.323 endpoint and the Cisco BTS 10200 are running different protocol versions.
Primary Action	This is only an issue where the endpoint is running a higher version of the H.323 protocol than the Cisco BTS 10200. Contact Cisco TAC.

Signaling (99)

Table 10-87 lists the details of the Signaling (99) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Abnormal Call Clearing—Signaling (99)" section on page 10-147.

Table 10-87 Signaling (99) Details

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	Contact Cisco TAC.

Signaling (100)

Table 10-88 lists the details of the Signaling (100) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Codec Negotiation Failed—Signaling (100)" section on page 10-147.

Table 10-88 Signaling (100) Details

Description	Codec Negotiation Failed
Severity	Minor
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Call ID—EIGHT_BYTES Reason—STRING [128]
Primary Cause	The codec negotiation has failed.
Primary Action	Find a compatible set of codec settings for both sides, reprovision the endpoints of the call, and try the call again.

Signaling (101)

Table 10-89 lists the details of the Signaling (101) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Per Call Security Violation—Signaling (101)" section on page 10-147.

Table 10-89 Signaling (101) Details

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)

Table 10-90 lists the details of the Signaling (102) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "H.323 Network Congested—Signaling (102)" section on page 10-148.

Table 10-90 Signaling (102) Details

Description	H.323 Network Congested
Severity	Minor
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Gatekeeper ID—STRING [32]
Primary Cause	The H.323 application process has depleted its 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.

Signaling (103)

Table 10-91 lists the details of the Signaling (103) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Aggregation Connection Down—Signaling (103)" section on page 10-148.

Table 10-91 Signaling (103) Details

Description	Aggregation Connection Down (AGGR Connection Down)
Severity	Major
Threshold	100
Throttle	0
Datawords	AGGR-ID—STRING [16]
Primary Cause	The Transmission Control Protocol (TCP) connection is down.
Primary Action	Check the associated cabling and perform a ping to test the connectivity.

Signaling (104)

Table 10-92 lists the details of the Signaling (104) informational event. For additional information, refer to the "Aggregation Unable to Establish Connection—Signaling (104)" section on page 10-119.

Table 10-92 Signaling (104) Details

Description	Aggregation Unable To Establish Connection (AGGR Unable To Establish Connection)
Severity	Information
Threshold	100
Throttle	0
Datawords	AGGR-ID—STRING [16]
Primary Cause	A TCP connection establish failure has occurred.
Primary Action	Check the IP connectivity of the call agent (CA) and the cable modem termination system (CMTS).

Signaling (105)

Table 10-93 lists the details of the Signaling (105) informational event. For additional information, refer to the "Aggregation Gate Set Failed—Signaling (105)" section on page 10-119.

Table 10-93 Signaling (105) Details

Description	Aggregation Gate Set Failed (AGGR Gate Set Failed)
Severity	Information
Threshold	100
Throttle	0
Datawords	AGGR-ID—STRING [16] Error-Code—TWO_BYTES Sub-Error-Code—TWO_BYTES
Primary Cause	The gate set acknowledgement never came from the CMTS.
Primary Action	None

Signaling (106)

Table 10-94 lists the details of the Signaling (106) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down—Signaling (106)" section on page 10-148.

Table 10-94 Signaling (106) Details

Description	Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down (ESA Cisco BTS 10200 DF Connection Down)
Severity	Minor
Threshold	100
Throttle	0
Primary Cause	The delivery function (DF) server is not responding.
Primary Action	Check the encryption key or the IP connectivity to the DF server.

Signaling (107)

Table 10-95 lists the details of the Signaling (107) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Logical Internet Protocol Addresses Not Mapped Correctly—Signaling (107)" section on page 10-148.

Table 10-95 Signaling (107) Details

Description	Logical Internet Protocol Addresses not Mapped Correctly (Logical IP 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	A contact name in the configuration file is not configured in the domain name system (DNS).
Primary Action	Verify that the name in the DNS matches the name in the platform.cfg and opticall.cfg files.
Secondary Cause	A contact could not be resolved to an IP address on the host.
Secondary Action	Verify that the DNS resolves to the IP addresses reserved for the process on the Cisco BTS 10200.
Ternary Cause	The IP address manager is not running.
Ternary Action	Verify that the Internet Protocol Manager (IPM) process is running and check for alarms from the IPM.
Subsequent Cause	A mis-configuration occurred during installation or manual changes were made after installation.
Subsequent Action	Contact Cisco TAC for support.

Signaling (108)

Table 10-96 lists the details of the Signaling (108) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Simplex Only Operational Mode—Signaling (108)" section on page 10-148.

Table 10-96 Signaling (108) Details

Description	Simplex Only Operational Mode
Severity	Major
Threshold	30
Throttle	0
Datawords	Host Domain Name—STRING [128]
Primary Cause	The hostname parameter is specified in the platform.cfg file instead of being specified in the -contact parameter.
Primary Action	Check to see if the Cisco BTS 10200 is configured as a simplex system.

Signaling (109)

Table 10-97 lists the details of the Signaling (109) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Stream Control Transmission Protocol Association Failure—Signaling (109)" section on page 10-149.

Table 10-97 Signaling (109) Details

Description	Stream Control Transmission Protocol Association Failure (SCTP Association Failure)
Severity	Major
Threshold	100
Throttle	0
Datawords	SCTP Association ID—STRING [17]
Primary Cause	The Ethernet cables for the signaling gateway process (SGP) are unplugged or severed.
Primary Action	Plug Ethernet cables in or fix the severed connection.
Secondary Cause	SGP is not operational.
Secondary Action	Check the SGP alarms to determine why SGP is not operating properly.

Signaling (110)

Table 10-98 lists the details of the Signaling (110) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Group Is Out of Service—Signaling (110)" section on page 10-152.

Table 10-98 Signaling (110) Details

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 the CA and the SGs are out-of-service.
Primary Action	Make sure all Ethernet connections on the CA and the SGs are plugged in. Also make sure all of the associated IP routers are operational.
Secondary Cause	The MTP3 user adapter (M3UA) layer is down between the CA and the SGs.
Secondary Action	Use the Cisco snooper application to determine why the M3UA layer is down.

Signaling (111)

Table 10-99 lists the details of the Signaling (111) major alarm. 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 10-153.

Table 10-99 Signaling (111) Details

Description	Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) (SCTP Association Degraded (One of Two IP connections Down))
Severity	Major
Threshold	100
Throttle	0
Datawords	SCTP Association ID—STRING [17] Destination IP Address—STRING [11]
Primary Cause	A single Ethernet connection on the CA or the SGP is unplugged or severed.
Primary Action	Plug in all of the Ethernet connections or repair if severed.
Secondary Cause	An SCTP communication problem—protocol timeout.
Secondary Action	Use the Cisco snooper application to determine why the SCTP association is degraded.

Signaling (112)

Table 10-100 lists the details of the Signaling (112) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Stream Control Transmission Protocol Association Configuration Error—Signaling (112)" section on page 10-154.

Table 10-100 Signaling (112) Details

Description	Stream Control Transmission Protocol Association Configuration Error (SCTP Association Configuration Error)
Severity	Minor
Threshold	100
Throttle	0
Datawords	SCTP Association ID—STRING [17]
Primary Cause	The destination IP address is invalid.
Primary Action	Input a new destination IP address—see log for additional details.
Secondary Cause	The local IP address is invalid.
Secondary Action	Input new local IP address information.
Ternary Cause	The IP Routing table is not configured properly.
Ternary Action	Have the system administrator configure the IP Routing table.

Signaling (113)

Table 10-101 lists the details of the Signaling (113) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Failure—Signaling (113)" section on page 10-155.

Table 10-101 Signaling (113) Details

Description	Signaling Gateway Failure
Severity	Major
Threshold	100
Throttle	0
Datawords	Signaling Gateway ID—STRING [17]
Primary Cause	All of the associated signaling gateway processes are out-of-service.
Primary Action	Determine why each of the associated SGP processes is out-of-service (see the SGP alarm definition).

Signaling (114)

Table 10-102 lists the details of the Signaling (114) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Process Is Out of Service—Signaling (114)" section on page 10-155.

Table 10-102 Signaling (114) Details

Description	Signaling Gateway Process is Out-of-Service
Severity	Major
Threshold	100
Throttle	0
Datawords	Signaling Gateway—STRING [17]
Primary Cause	All of the SCTP associations between the SGP and the CA are out-of-service.
Primary Action	See the SCTP association alarm definition to determine how to rectify the problem.
Secondary Cause	The M3UA layer is down between the CA and the SGP.
Secondary Action	Use the Cisco snooper utility to determine why M3UA layer is down. Also see the log for additional information.

Signaling (115)

Table 10-103 lists the details of the Signaling (115) warning event. To monitor and correct the cause of the event, refer to the "Invalid Routing Context Received—Signaling (115)" section on page 10-121.

Table 10-103 Signaling (115) Details

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	The routing context was configured improperly on the CA or the signaling gateway (SG).
Primary Action	Reconfigure the routing context on the CA or the SG so that it matches in both places.

Signaling (116)

Table 10-104 lists the details of the Signaling (116) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Destination Point Code User Part Unavailable—Signaling (116)" section on page 10-156.

Table 10-104 Signaling (116) Details

Description	Destination Point Code User Part Unavailable (DPC User Part Unavailable)
Severity	Major
Threshold	100
Throttle	0
Datawords	DPC ID—STRING [17]
Primary Cause	An SGP sent a destination user part unavailable (DUPU) M3UA message to the CA indicating that a User Part is unavailable on a DPC.
Primary Action	Contact the SS7 Network Administrator to report the User Part Unavailable problem on the DPC so that communication can be restored.

Signaling (117)

Table 10-105 lists the details of the Signaling (117) minor alarm. 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 10-156.

Table 10-105 Signaling (117) Details

Description	Circuit Validation Test Message Received for an Unequipped Circuit Identification Code (CVT Message Received for an Unequipped CIC)
Severity	Minor
Threshold	100
Throttle	0
Datawords	CIC—TWO_BYTES TGN-ID—EIGHT_BYTES DPC—STRING [13]
Primary Cause	The CIC is not provisioned
Primary Action	Provision the CIC.

Signaling (118)

Table 10-106 lists the details of the Signaling (118) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Circuit Verification Response Received With Failed Indication—Signaling (118)" section on page 10-156.

Table 10-106 Signaling (118) Details

Description	Circuit Verification Response Received with Failed Indication (CVR 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	A CIC mismatch occurred.
Primary Action	Perform an internal test such as checking that the CIC is assigned to a circuit between the sending and the receiving switch.

Signaling (119)

Table 10-107 lists the details of the Signaling (119) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling System 7 Adapter Process Faulty—Signaling (119)" section on page 10-156.

Table 10-107 Signaling (119) Details

Description	Signaling System 7 Adapter Process Faulty (S7A Process Faulty)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Reason—STRING [36]
Primary Cause	An OMNI or S7A exception has occurred.
Primary Action	Check the OMNI process. The S7A will restart itself if the S7A maximum number of restarts is not exceeded.

Signaling (120)

Table 10-108 lists the details of the Signaling (120) critical alarm. 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 10-156.

Table 10-108 Signaling (120) Details

Description	Signaling System 7 Module/Signaling System 7 Adapter Faulty (S7M/S7A Faulty)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Reason—STRING [36]
Primary Cause	An OMNI failure has occurred.
Primary Action	Check the OMNI status; a failover will occur in a duplex configuration.

Signaling (121)

Table 10-109 lists the details of the Signaling (121) major alarm. 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 10-157.

Table 10-109 Signaling (121) Details

Description	Message Transfer Part 3 User Adapter Cannot Go Standby (M3UA/SUA Cannot Go Standby)
Severity	Major
Threshold	100
Throttle	0
Datawords	Platform ID—STRING [17]
Primary Cause	No inactive acknowledge (ACK) messages are received from any SG or SCTP. The associations are probably down.
Primary Action	Investigate any other alarms to see if SGs are down or the SCTP associations are down. Take corrective action according to those alarms.

Signaling (122)

Table 10-110 lists the details of the Signaling (122) major alarm. 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 10-157.

Table 10-110 Signaling (122) Details

Description	Message Transfer Part 3 User Adapter Cannot Go Active (M3UA/SUA Cannot Go Active)
Severity	Major
Threshold	100
Throttle	0
Datawords	Platform ID—STRING [17]
Primary Cause	No active acknowledgement messages are being received from any SG or SCTP. The associations are probably down.
Primary Action	Investigate any other alarms to see if the SGs are down or the SCTP associations are down. Take corrective action according to those alarms.

Signaling (123)

Signaling (123) is not used.

Signaling (124)

Table 10-111 lists the details of the Signaling (124) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Remote Subsystem is Out Of Service—Signaling (124)" section on page 10-157.

Table 10-111 Signaling (124) Details

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	A link loss has occurred or the remote subsystem is out of service.
Primary Action	Check the links. Check the remote location, if possible.

Signaling (125)

Table 10-112 lists the details of the Signaling (125) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Connection Control Part Routing Error—Signaling (125)" section on page 10-157.

Table 10-112 Signaling (125) Details

Description	Signaling Connection Control Part Routing Error (SCCP Routing Error)
Severity	Major
Threshold	100
Throttle	0
Primary Cause	The signaling connection control part (SCCP) route is invalid or is not available.
Primary Action	Provision the right SCCP route.

Signaling (126)

Table 10-113 lists the details of the Signaling (126) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Connection Control Part Binding Failure—Signaling (126)" section on page 10-158.

Table 10-113 Signaling (126) Details

Description	Signaling Connection Control Part Binding Failure (SCCP Binding Failure)
Severity	Major
Threshold	100
Throttle	0
Datawords	Local Point Code—STRING [20] Local Subsystem Numb—ONE_BYTE
Primary Cause	A Trillium stack binding failure has occurred.
Primary Action	Reinitialize the TCAP signaling adapter (TSA) process or remove the subsystem from the Element Management System (EMS) table and add it again.

Signaling (127)

Table 10-114 lists the details of the Signaling (127) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Transaction Capabilities Application Part Binding Failure—Signaling (127)" section on page 10-158.

Table 10-114 Signaling (127) Details

Description	Transaction Capabilities Application Part Binding Failure (TCAP Binding Failure)
Severity	Major
Threshold	100
Throttle	0
Primary Cause	A Trillium stack binding failure has occurred.
Primary Action	Reinitialize the TSA process or remove the subsystem from the EMS table and add it again.

Signaling (128)

Signaling (128) is not used.

Signaling (129)

Signaling (129) is not used.

Signaling (130)

Signaling (130) is not used.

Signaling (131)

Signaling (131) is not used.

Signaling (132)

Table 10-115 lists the details of the Signaling (132) warning event. 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 10-123.

Table 10-115 Signaling (132) Details

Description	Transaction Capabilities Application Part Reaches the Provisioned Resource Limit (TCAP Reaches the Provisioned Resource Limit)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Dialogue/Invoke ID—FOUR_BYTES
Primary Cause	The Transaction Capabilities Application Part (TCAP) has run out of all the preconfigured dialogue IDs or invoke IDs.

Signaling (133)

Table 10-116 lists the details of the Signaling (133) informational event. For additional information, refer to the "Unable to Decode Generic Transport Descriptor Message—Signaling (133)" section on page 10-123.

Table 10-116 Signaling (133) Details

Description	Unable to Decode Generic Transport Descriptor Message (Unable to Decode GTD Message)
Severity	Information
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)

Table 10-117 lists the details of the Signaling (134) informational event. For additional information, refer to the "Signaling System 7 Message Encoding Failure—Signaling (134)" section on page 10-124.

Table 10-117 Signaling (134) Details

Description	Signaling System 7 Message Encoding Failure (SS7 Message Encoding Failure)
Severity	Information
Threshold	100
Throttle	0
Datawords	CIC Number—TWO_BYTES TGN-ID—FOUR_BYTES DPC—STRING [20] OPC—STRING [20]
Primary Cause	An error in the ISDN user part (ISUP) stack or in a signaling adapter interface (SAI) message has occurred.
Primary Action	Capture the SS7 trace of circuit for examination by support personnel and contact Cisco TAC.

Signaling (135)

Table 10-118 lists the details of the Signaling (135) informational event. For additional information, refer to the "Signaling System 7 Message Decoding Failure—Signaling (135)" section on page 10-124.

Table 10-118 Signaling (135) Details

Description	Signaling System 7 Message Decoding Failure (SS7 Message Decoding Failure)
Severity	Information
Threshold	100
Throttle	0
Datawords	CIC Number—TWO_BYTES TGN-ID—FOUR_BYTES DPC—STRING [20] OPC—STRING [20]
Primary Cause	An error in the ISUP stack or in an SAI message has occurred.
Primary Action	Capture the SS7 trace of circuit for examination by support personnel and contact Cisco TAC.

Signaling (136)

Table 10-119 lists the details of the Signaling (136) informational event. For additional information, refer to the "Signaling System 7 Message Invalid Received—Signaling (136)" section on page 10-124.

Table 10-119 Signaling (136) Details

Description	Signaling System 7 Message Invalid Received (SS7 Message Invalid Received)
Severity	Information
Threshold	100
Throttle	0
Datawords	CIC Number—TWO_BYTES TGN-ID—FOUR_BYTES DPC—STRING [20] OPC—STRING [20]
Primary Cause	An invalid message was received from the line in the ISUP stack.
Primary Action	Capture the SS7 trace of circuit for examination by support personnel and contact Cisco TAC.
Secondary Cause	An invalid message was received from the line in the ISUP stack.
Secondary Action	Verify that the signal switching point (SSP) sending the message to the CA is correctly configured.

Signaling (137)

Table 10-120 lists the details of the Signaling (137) informational event. For additional information, refer to the "Signaling System 7 Confusion Message Received—Signaling (137)" section on page 10-124.

Table 10-120 Signaling (137) Details

Description	Signaling System 7 Confusion Message Received (SS7 Confusion Message Received)
Severity	Information
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 a parameter received was not recognized or understood.
Primary Action	Check the log for more information (including confusion (CFN) diagnostic output). Capture an SS7 trace of the affected circuits. If the diagnostic data indicates that messages or parameters that must be supported are being dropped, refer the captured data to Cisco TAC along with a description of the call scenario.

Signaling (138)

Table 10-121 lists the details of the Signaling (138) warning event. 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 10-124.

Table 10-121 Signaling (138) Details

Description	Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit (Number of Open SIP 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	A call failure has occurred or a feature is unavailable.
Primary Action	The system configuration and the 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 TAC.

Signaling (139)

Table 10-122 lists the details of the Signaling (139) informational event. For additional information, refer to the "Signaling System 7 Trunk was Found to be in Erroneous State—Signaling (139)" section on page 10-125.

Table 10-122 Signaling (139) Details

Description	Signaling System 7 Trunk was Found to be in Erroneous State (SS7 Trunk was Found to be in Erroneous State)
Severity	Information
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	A discrepancy between the local and the remote trunk states has occurred.
Primary Action	Automatic corrective action is enforced when using American National Standards Institute (ANSI) ISUP.

Signaling (140)

Table 10-123 lists the details of the Signaling (140) informational event. For additional information, refer to the "Unanswered Information Message—Signaling (140)" section on page 10-125.

Table 10-123 Signaling (140) Details

Description	Unanswered Information Message (Unanswered INF Message)
Severity	Information
Threshold	100
Throttle	0
Datawords	CIC—TWO_BYTES TGN-ID—FOUR_BYTES DPC—STRING [20] OPC—STRING [20]
Primary Cause	The far-end switch is not responding to an information (INF) message with an information request (INR) message.
Primary Action	Verify that the far-end switch can correctly respond to an INF message.

Signaling (141)

Table 10-124 lists the details of the Signaling (141) warning event. 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 10-125.

Table 10-124 Signaling (141) Details

Description	Address not Resolved by Domain Name System Server (Address not Resolved by DNS Server)
Severity	Warning
Threshold	100
Throttle	0
Datawords	TSAP_Address/Hostname—STRING [256] Reason—STRING [64]
Primary Cause	The transport service access point (TSAP) address or hostname is not defined in the DNS.
Primary Action	Add an entry for the TSAP address to the DNS server, or fix the Cisco BTS 10200 provisioning.

Signaling (142)

Table 10-125 lists the details of the Signaling (142) critical alarm. 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 10-158.

Table 10-125 Signaling (142) Details

Description	Session Initiation Protocol Trunk Operationally Out-of-Service (SIP Trunk Operationally out of Service)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Trunk Group Description —STRING [21] Trunk SIP Element ID—STRING [65] Trunk Server Group ID—STRING [65]
Primary Cause	Issued when the Cisco BTS 10200 is unable to communicate with a remote SIP party (Call-Agent or Proxy) over a SIP or a SIP-T trunk.
Primary Action	Verify that the DNS resolution exists, if TSAP address of the remote entity is a domain name. Verify that 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, verify that the network connection is operational.
Secondary Cause	The 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 that the SIP application is running on the remote host and is listening on the port specified in the TSAP address.

Signaling (143)

Table 10-126 lists the details of the Signaling (143) minor alarm. 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 10-158.

Table 10-126 Signaling (143) Details

Description	Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down (IP Interface Link to the SS7 Signaling Gateway is Down)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [65] Interface IP Address—STRING [65]
Primary Cause	A hardware problem has occurred.
Primary Action	Check the link interfaces.

Signaling (144)

Table 10-127 lists the details of the Signaling (144) critical alarm. 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 10-158.

Table 10-127 Signaling (144) Details

Description	All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down (All IP Interface Links to SS7 Signaling Gateway are Down)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [65] Interface IP Address—STRING [65]
Primary Cause	A hardware problem has occurred.
Primary Action	Check the link interfaces.

Signaling (145)

Table 10-128 lists the details of the Signaling (145) minor alarm. 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 10-159.

Table 10-128 Signaling (145) Details

Description	One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down (One IP Interface to SS7 Signaling Gateway is Down)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [65] Interface IP Address—STRING [65]
Primary Cause	A hardware problem has occurred.
Primary Action	Check the link interfaces.

Signaling (146)

Table 10-129 lists the details of the Signaling (146) warning event. 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 10-126.

Table 10-129 Signaling (146) Details

Description	All Retransmission Attempts of Session Initiation Protocol Request or Response Failed (All Retransmission Attempts of SIP 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 the DNS or the IP address of request uniform resource identifier (URI). SIP response: All retransmission attempts for a SIP response failed for the received socket IP address of the request and the DNS (or the IP address) listed in the header.
Primary Action	Ensure that if the DNS server is up and running for the host name resolution and ensure that the DNS server is provisioned properly to resolve the correct order of the IP addresses. Ensure that the previous hop network component is alive and in a healthy state.

Signaling (147)

Table 10-130 lists the details of the Signaling (147) warning event. To monitor and correct the cause of the event, refer to the "Domain Name System Service Addresses Exhausted—Signaling (147)" section on page 10-126.

Table 10-130 Signaling (147) Details

Description	Domain Name System Service Addresses Exhausted (DNS SRV Addresses Exhausted)
Severity	Warning
Threshold	100
Throttle	0
Datawords	SRV Hostname—STRING [256]
Primary Cause	The DNS service (SRV) hostname resolution to the IP addresses is exhausted.
Primary Action	Add an entry to the SRV in the DNS server. Fix the Cisco BTS 10200 provisioning.

Signaling (148)

Signaling (148) is not used.

Signaling (149)

Signaling (149) is not used.

Signaling (150)

Table 10-131 lists the details of the Signaling (150) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Stream Control Transmission Protocol Association Congested—Signaling (150)" section on page 10-159.

Table 10-131 Signaling (150) Details

Description	Stream Control Transmission Protocol Association Congested (SCTP Association Congested)
Severity	Minor
Threshold	100
Throttle	0
Datawords	SCTP Association ID—STRING [17] Congestion Level—ONE_BYTE
Primary Cause	The network is congested.
Primary Action	Clean off the network congestion caused by routing or switching issues.
Secondary Cause	The central processing unit (CPU) is throttled.
Secondary Action	You might need to upgrade to a more powerful platform or offload some traffic.

Signaling (151)

Table 10-132 lists the details of the Signaling (151) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Subscriber Line Faulty—Signaling (151)" section on page 10-160.

Table 10-132 Signaling (151) Details

Description	Subscriber Line Faulty
Severity	Minor
Threshold	100
Throttle	0
Datawords	End Point /Termination - STRING [54] Media Gateway Type - STRING [54] Error Details - STRING [54]
Primary Cause	The residential gateway returned an error code in response to a command from the MGW.
Primary Action	Try controlling subscriber termination to OOS and back to INS using the Cisco BTS 10200 CLI command. If the problem persist after more calls, check the configuration in the Cisco BTS 10200 and the RGW. If the error codes returned by the MGW are harmless, the error codes can be suppressed by adding a new entry in the MGCP-RETCODE-ACTION table and by changing the EP-ACTION to reset/none.

Signaling (152)

Table 10-133 lists the details of the Signaling (151) informational event. For additional information, refer to the "Termination Transient Error Received—Signaling (152)" section on page 10-127.

Table 10-133 Signaling (152) Details

Description	Termination Transient Error Received
Severity	Information
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	Contact Cisco TAC.

Signaling (153)

Table 10-134 lists the details of the Signaling (153) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Emergency Trunks Become Locally Blocked—Signaling (153)" section on page 10-160.

Table 10-134 Signaling (153) Details

Description	Emergency Trunks Become Locally Blocked
Severity	Critical
Threshold	100
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 an emergency trunk (CAS, SS7, or ISDN) gets locally blocked.
Primary Action	No action is required.

Signaling (154)

Table 10-135 lists the details of the Signaling (154) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Emergency Trunks Become Remotely Blocked—Signaling (154)" section on page 10-160.

Table 10-135 Signaling (154) Details

Description	Emergency Trunks Become Remotely Blocked
Severity	Critical
Threshold	100
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 an emergency trunk (CAS, SS7, or ISDN) gets remotely blocked.
Primary Action	No action is required.

Signaling (155)

Table 10-136 lists the details of the Signaling (155) informational event. For additional information, refer to the "Packet Cable Multi-Media Unsolicited Gate Delete—Signaling (155)" section on page 10-127.

Table 10-136 Signaling (155) Details

Description	Packet Cable Multi-Media Unsolicited Gate Delete (PCMM Unsolicited Gate Delete)
Severity	Information
Threshold	100
Throttle	0
Datawords	AGGR-ID—STRING [16] Subscriber-IP-Address—STRING [32] Gate-Direction—STRING [16]
Primary Cause	An error condition has been encountered by the CMTS.
Primary Action	Check the alarms and warnings from the CMTS.

Signaling (156)

Table 10-137 lists the details of the Signaling (156) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Integrated Services Digital Network Signaling Gateway Down—Signaling (156)" section on page 10-161.

Table 10-137 Signaling (156) Details

Description	Integrated Services Digital Network Signaling Gateway Down (ISDN Signaling Gateway Down)
Severity	Major
Threshold	100
Throttle	0
Datawords	Media Gateway ID—STRING [16] Media Gateway TSAP Address—STRING [64]
Primary Cause	Cannot communicate to the ISDN gateway because it is down due to a failure in the gateway. The SCTP association might be down.
Primary Action	Check to see if the SCTP association is down due to an issue on the network.
Secondary Cause	The IUA layer might be down in the gateway.
Secondary Action	No action is needed. The IUA layer will be automatically recovered.

Signaling (157)

Table 10-138 lists the details of the Signaling (157) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)" section on page 10-161.

Table 10-138 Signaling (157) Details

Description	Integrated Services Digital Network Signaling Gateway Inactive (ISDN Signaling Gateway Inactive)
Severity	Major
Threshold	100
Throttle	0
Datawords	Media Gateway ID—STRING [16]
Primary Cause	A **shutdown** command was executed in the application server on the ISDN gateway side.
Primary Action	No action is needed. The ISDN gateway will be automatically recovered.

Signaling (158)

Table 10-139 lists the details of the Signaling (158) warning event. To monitor and correct the cause of the event, refer to the "Invalid Integrated Services Digital Network Interface Identification—Signaling (158)" section on page 10-128.

Table 10-139 Signaling (158) Details

Description	Invalid Integrated Services Digital Network Interface Identification (Invalid ISDN Interface ID)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Received Interface ID—TWO_BYTES
Primary Cause	The interface ID is not configured correctly on the ISDN gateway side.
Primary Action	Configure the D-channel correctly on the gateway side. The D-channel configuration on the call-agent side should match with that on the gateway side.

Signaling (159)

Table 10-140 lists the details of the Signaling (159) warning event. To monitor and correct the cause of the event, refer to the "Integrated Services Digital Network User Adaptation Layer Cannot Go Active—Signaling (159)" section on page 10-128.

Table 10-140 Signaling (159) Details

Description	Integrated Services Digital Network User Adaptation Layer Cannot Go Active (IUA Cannot Go Active)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Not applicable.
Primary Cause	No active acknowledgement messages are being received from any signaling gateway. The ISDN signaling gateway or the SCTP associations are probably down.
Primary Action	Investigate other alarms to see if the signaling gateways are down or the SCTP associations are down. Take corrective action according to those alarms.

Signaling (160)

Table 10-141 lists the details of the Signaling (160) warning event. To monitor and correct the cause of the event, refer to the "Integrated Services Digital Network User Adaptation Layer Cannot Go Standby—Signaling (160)" section on page 10-128.

Table 10-141 Signaling (160) Details

Description	Integrated Services Digital Network User Adaptation Layer Cannot Go Standby (IUA Cannot Go Standby)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Not applicable.
Primary Cause	No UP acknowledgement messages are being received from any signaling gateway. The ISDN signaling gateway or the SCTP associations are probably down.
Primary Action	Investigate other alarms to see if the signaling gateways are down or the SCTP associations are down. Take corrective action according to those alarms.

Signaling (161)

Table 10-142 lists the details of the Signaling (161) warning event. To monitor and correct the cause of the event, refer to the "Session Initiation Protocol Update Not Allowed for Operator Service Position System Calls—Signaling (161)" section on page 10-128.

Table 10-142 Signaling (161) Details

Description	Session Initiation Protocol Update not Allowed for Operator Service Position System Calls (SIP Update not Allowed for OSPS Calls)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Trunk Group Description—STRING [21] TSAP Address—STRING [65]
Primary Cause	The remote switch does not allow the Cisco BTS 10200 to send SIP UPDATE messages. The update message is mandatory in CMSS and is used exclusively by the Cisco BTS 10200 for operator service calls over SIP including BLV, emergency interrupt, and 911 ringback calls.
Primary Action	Upgrade or reprovision the remote switch so it can process incoming SIP update messages.

Signaling (162)

Table 10-143 lists the details of the Signaling (162) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)" section on page 10-161.

Table 10-143 Signaling (162) Details

Description	Session Initiation Protocol Server Group Element Operationally Out of Service (SIP Server Group Element Operationally out of Service)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Server Group Description—STRING [64] TSAP Address of the SIP-Element.—STRING [64]
Primary Cause	Issued when the Cisco BTS 10200 is unable to communicate with a remote SIP party (Call-Agent or Proxy) over a SIP server group element.
Primary Action	If the TSAP address of the remote entity is a domain name, verify that the DNS resolution exists. Verify that the remote entity is reachable by ICMP ping, using the TSAP address from the Event Report. If the same alarm is reported for other TSAP addresses on several softswitch trunk groups and/or server-group elements, verify that the network connection is operational.
Secondary Cause	The remote SIP party is not operational.
Secondary Action	If the ping is not successful, diagnose the issue that prevents the TSAP address from being reached. Verify that the SIP application is running on the remote host and listening on the port specified in the TSAP address.

Signaling (163)

Table 10-144 lists the details of the Signaling (163) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Routing Key Inactive—Signaling (163)" section on page 10-161.

Table 10-144 Signaling (163) Details

Description	Routing Key Inactive
Severity	Major
Threshold	100
Throttle	0
Datawords	Routing Key ID—STRING [17] Routing Context—STRING [17] Signaling Gateway ID—STRING [17]
Primary Cause	Inactive ACK messages were received from a Signaling Gateway. The SGs or the SCTP associations are probably down.
Primary Action	Investigate other alarms to see if the SGs are down or the SCTP associations are down. Take corrective action according to those alarms. Also check the AS status for the routing context on ITP.

Signaling (164)

Table 10-145 lists the details of the Signaling (164) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Traffic Mode Mismatch—Signaling (164)" section on page 10-162.

Table 10-145 Signaling (164) Details

Description	Signaling Gateway Traffic Mode Mismatch
Severity	Major
Threshold	100
Throttle	0
Datawords	Signaling Gateway ID—STRING [17] Signaling Gateway Process ID—STRING [17]
Primary Cause	The traffic mode does not match on the Cisco BTS 10200 and the Signaling Gateway.
Primary Action	Verify the AS traffic-mode configuration in the Signaling Gateway. Check that the SG internal redundancy mode for the traffic-mode setting has been set correctly in the Cisco BTS 10200.

Signaling (165)

Table 10-146 lists the details of the Signaling (165) warning event. To monitor and correct the cause of the event, refer to the "No Session Initiation Protocol P-DCS Billing Information Header Received—Signaling (165)" section on page 129.

Table 10-146 Signaling (165) Details

Description	No Session Initiation Protocol P-DCS Billing Information Header Received (No SIP P-DCS Billing Info Hdr Rcvd)
Severity	Warning
Threshold	10
Throttle	0
Datawords	Trunk Group ID—STRING [21] TSAP Address—STRING [65]
Primary Cause	The originating switch is not provisioned to add the P-DCS Billing Information header to outgoing SIP requests and responses.
Primary Action	Provision the originating switch to add the P-DCS Billing Information header to outgoing messages.
Secondary Cause	The header could have been stripped off by an intermediate proxy.
Secondary Action	Determine if the header has been stripped off by an intermediate proxy and, if it has, configure for corrective action if so.
Ternary Cause	There was a SIP message encode error at the sending switch.
Ternary Action	Determine if a SIP message encode error occurred at the sending switch and if so, call the technical assistance center to determine a fix for the problem.

Signaling (166)

Table 10-147 lists the details of the Signaling (166) warning event. To monitor and correct the cause of the event, refer to the "No Routing Keys Are Active—Signaling (166)" section on page 129.

Table 10-147 Signaling (166) Details

Description	No Routing Keys are Active
Severity	Warning
Threshold	0
Throttle	0
Primary Cause	Routing keys are not set to the active state.
Primary Action	Set the routing keys to the active state.
Secondary Cause	The ITP provisioning is incorrect.
Secondary Action	Check the ITP provisioning.

Signaling (167)

Table 10-148 lists the details of the Signaling (167) warning event. To monitor and correct the cause of the event, refer to the "No Signaling Gateways Are Active—Signaling (167)" section on page 130.

Table 10-148 Signaling (167) Details

Description	No Signaling Gateways are Active
Severity	Warning
Threshold	0
Throttle	0
Primary Cause	A communication problem between the ITP and the Cisco BTS 10200 has occurred.
Primary Action	Check the communication path between the Cisco BTS 10200 and the ITP.

Signaling (168)

Table 10-149 lists the details of the Signaling (168) warning event. To monitor and correct the cause of the event, refer to the "A Session Initiation Protocol Server Group Has No Child Elements Provisioned—Signaling (168)" section on page 130.

Table 10-149 Signaling (168) Details

Description	A Session Initiation Protocol Server Group has no Child Elements Provisioned (A SIP Server Group has no Child Elements Provisioned)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Server Group ID—STRING [64]
Primary Cause	Issued when a SIP Server Group is provisioned as in-service but has no child elements provisioned.
Primary Action	This server group is considered administratively out of service. If that is acceptable, no action is required. If the group was expected to be workable, place the server group back out of service, resolve the provisioning problem, and place the group back in service.

Signaling (169)

Table 10-150 lists the details of the Signaling (169) informational event. For additional information, refer to the "Session Initiation Protocol Element Provisioned With Service Enabled Is Internally Disabled—Signaling (169)" section on page 130.

Table 10-150 Signaling (169) Details

Description	Session Initiation Protocol Element Provisioned with Service Enabled is Internally Disabled (SIP Element Provisioned with SRV Enabled is Internally Disabled)
Severity	Information
Threshold	100
Throttle	0
Datawords	SIP Element ID—STRING [64]
Primary Cause	A SIP element was provisioned with SRV enabled and is associated with at least one or more Server Groups.
Primary Action	The SRV flag will be assumed disabled. However, to resolve this informational message, provision the SRV flag disabled on the SIP element.

Signaling (170)

Table 10-151 lists the details of the Signaling (170) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)" section on page 10-162.

Table 10-151 Signaling (170) Details

Description	Residential Gateway Endpoints are out of Service at the Gateway (Residential Gateway Endpoints are out of Service at the GW)
Severity	Minor
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	The residential gateway has been administratively taken OOS through use of the command at the GW.
Primary Action	Bring the residential gateway administratively into INS using the command at the GW.

Signaling (171)

Table 10-152 lists the details of the Signaling (171) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Residential Gateway Unreachable—Signaling (171)" section on page 10-162.

Table 10-152 Signaling (171) Details

Description	Residential Gateway Unreachable
Severity	Minor
Threshold	100
Throttle	0
Datawords	Entity Name—STRING [40] General Context—STRING [40] Specific Context—STRING [40] Failure Context—STRING [40]
Primary Cause	An MGCP signaling interop error has occurred with the residential media gateway.
Primary Action	Check the IP connectivity status between Cisco BTS 10200 call agent and the trunking gateway. Check to see if the residential gateway is not physically connected, but controlled INS at the Cisco BTS 10200.

Signaling (172)

Table 10-153 lists the details of the Signaling (172) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)" section on page 10-162.

Table 10-153 Signaling (172) Details

Description	Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to its IP Address (MTA Effective-Aggr-Id Becomes Unavailable Due to its IP Address)
Severity	Major
Threshold	100
Throttle	0
Datawords	MTA IP Address—STRING [64]
Primary Cause	The MTA has been moved to a new subnet which is not provisioned, or provisioned with the aggr-id=null.
Primary Action	Provision the subnet aggr-id for the MTA.

Signaling (173)

Table 10-154 lists the details of the Signaling (173) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)" section on page 10-162.

Table 10-154 Signaling (173) Details

Description	ENUM Server Domain Cannot be Resolved into Any IP Address
Severity	Critical
Threshold	100
Throttle	0
Datawords	ENUM Server Domain - STRING [128] ENUM Profile ID - STRING [64]
Primary Cause	Misconfiguration in the DNS.
Primary Action	Fix the configuration in the DNS according to the documentation.

Signaling (174)

Table 10-155 lists the details of the Signaling (174) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "ENUM Server Unavailable—Signaling (174)" section on page 10-163.

Table 10-155 Signaling (174) Details

Description	ENUM Server Unavailable
Severity	Critical
Threshold	100
Throttle	0
Datawords	ENUM Server IP Address - STRING [16] ENUM Server Farm Name - STRING [128] ENUM Profile ID - STRING [64]
Primary Cause	A network or server problem has occurred.
Primary Action	Fix the network or server problem.

Signaling (175)

Table 10-156 lists the details of the Signaling (175) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "ENUM Server Farm Unavailable—Signaling (175)" section on page 10-163.

Table 10-156 Signaling (175) Details

Description	ENUM Server Farm Unavailable
Severity	Critical
Threshold	100
Throttle	0
Datawords	ENUM Server Farm Name - STRING [128] ENUM Profile ID - STRING [64]
Primary Cause	A network or server problem has occurred.
Primary Action	Fix the network or server problem.

Signaling (176)

Table 10-157 lists the details of the Signaling (176) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "No Resources Available to Launch ENUM Query—Signaling (176)" section on page 10-163.

Table 10-157 Signaling (176) Details

Description	No Resources Available to Launch ENUM Query
Severity	Critical
Threshold	100
Throttle	0
Datawords	
Primary Cause	Internal or network congestion or slow server response has occurred.
Primary Action	Fix the network congestion or improve the server response.

Signaling (177)

Table 10-158 lists the details of the Signaling (177) warning event. To monitor and correct the cause of the event, refer to the "ISDN Unable to Restore D-Channel Into In-Service Active State—Signaling (177)" section on page 10-131.

Table 10-158 Signaling (177) Details

Description	ISDN Unable to Restore D-Channel into In-Service Active State
Severity	Warning
Threshold	100
Throttle	0
Datawords	D-Chan ID - STRING [20] D-Chan Index - FOUR_BYTES D-Chan Type - STRING [10]
Primary Cause	The Cisco BTS 10200 does not receive the Service Ack from the remote end in response to Service message to make the D-Channel active.
Primary Action	Verify that the NFAS provisioning at the PBX/media gateway is correct.

Signaling (178)

Table 10-159 lists the details of the Signaling (178) informational event. For additional information, refer to the "Possible Overlap Dialing Misconfiguration—Signaling (178)" section on page 132.

Table 10-159 Signaling (178) Details

Description	Possible Overlap Dialing Misconfiguration
Severity	Information
Threshold	100
Throttle	0
Datawords	TGN-ID - FOUR_BYTES DIALED-DIGIT - STRING [20]
Primary Cause	The Cisco BTS 10200 sent out an invite with an overlap flag, and has received one or more additional digits to be forwarded. However, the call attempt fails while the Cisco BTS 10200 is still waiting to send out the first additional digit. A possible cause is a misconfiguration of the Overlap Dialing feature between the local and peer switch.
Primary Action	Make sure that the peer switch is configured to support the Overlap Dialing feature. Check that the feature is enabled and that the dial-plan is configured correctly. Also make sure that the Destination/Route/Trunk group on the peer switch is marked to support the Overlap Sending feature.

Signaling (179)

Table 10-160 lists the details of the Signaling (179) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Trunk Group Registration Expired—Signaling (179)" section on page 10-163.

Table 10-160 Signaling (179) Details

Description	Trunk Group Registration Expired
Severity	Major
Threshold	100
Throttle	0
Datawords	TGN-ID - FOUR_BYTES SIP Reg Contact - STRING [256] Reg Expiry Time - STRING [32]
Primary Cause	The trunk group did not register in time before the contact expiry.
Primary Action	The receipt of a subsequent registration will clear the alarm.

Signaling (182)

Table 10-161 lists the details of the Signaling (182) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Transient Issue Occurred on the Emergency End-points—Signaling (182)" section on page 10-163.

Table 10-161 Signaling (182) Details

Description	Transient Issue Occurred on the Emergency End-points
Severity	Major
Threshold	100
Throttle	0
Datawords	Endpoint-Name or Calling party—STRING[8]; (If available, otherwise is blank) Mgw-Name or Called party—STRING[8]; (If available, otherwise is blank) Error-description (in brief)—STRING[8]; (If available, otherwise is blank) Detailed error description—STRING[8]
Primary Cause	A transient error such as, 5XX error for CRCX, or a transient shm error, or an out-of-sequence message received at the MGA (MGCP protocol adapter) occurred on emergency end-points. Additionally, an error occurred for 911 call at BCM (Basic Call Module) such as trunk group OOS. This behavior is controlled by a new CA_CONFIG type —SPECIAL-ALARM-FOR-911-TRANS-ISSUES DATATYPE. The default value of this field is N. Set it to Y to enable logging of Signaling (182). For more information on the primary cause, see the "Transient Issue Occurred on the Emergency End-points—Signaling (182)" section on page 10-163.
Primary Action	Take action based on the description provided when the alarm is logged. For example, If the description indicates that the trunk is OOS, control the trunk back to INS, if required. Since these alarms only denote a transient error and do not have any corresponding trigger point to clear the alarm, the operator needs to clear the alarms from the CLI frequently (if the operator has opted for logging of this alarm).

Monitoring Signaling Events

This section provides the information you need for monitoring and correcting signaling events. Table 10-162 lists all of the signaling events in numerical order and provides cross-references to each subsection.

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

Table 10-162 Cisco BTS 10200 Signaling Events

Event Type	Event Name	Event Severity
Signaling (1)	Test Report—Signaling (1)	Information
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 Message—Signaling (25)	Warning
Signaling (26)	Unanswered Unblocking Message—Signaling (26)	Warning
Signaling (27)	Unanswered Circuit Group Blocking Message—Signaling (27)	Warning

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
Signaling (28)	Unanswered Circuit Group Unblocking Message—Signaling (28)	Warning
Signaling (29)	Unanswered Circuit Query Message—Signaling (29)	Warning
Signaling (30)	Unanswered Circuit Validation Test Message—Signaling (30)	Warning
Signaling (31)	Unanswered Reset Circuit Message—Signaling (31)	Warning
Signaling (32)	Unanswered Group Reset Message—Signaling (32)	Warning
Signaling (33)	Unanswered Release Message—Signaling (33)	Warning
Signaling (34)	Unanswered Continuity Check Request Message—Signaling (34)	Warning
Signaling (36)	Trunk Locally Blocked—Signaling (36)	Minor
Signaling (40)	Trunk Remotely Blocked—Signaling (40)	Major
Signaling (42)	Continuity Testing Message Received on the Specified Circuit Identification Code—Signaling (42)	Information
Signaling (43)	Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code—Signaling (43)	Information
Signaling (44)	Continuity Recheck Is Performed on Specified Circuit Identification Code—Signaling (44)	Information
Signaling (45)	Circuit Is Unequipped on Remote Side—Signaling (45)	Information
Signaling (46)	Specified Circuit Identification Code Is Invalid for the Operation—Signaling (46)	Information
Signaling (49)	A General Processing Error Encountered—Signaling (49)	Information
Signaling (50)	Unexpected Message for the Call State Is Received: Clear Call—Signaling (50)	Information
Signaling (51)	Set Trunk State as Remotely Unequipped—Signaling (51)	Information
Signaling (52)	Set Trunk State as Not Remotely Blocked—Signaling (52)	Information
Signaling (53)	Set Trunk State as Remotely Blocked—Signaling (53)	Information
Signaling (54)	Circuit Validation Test Aborted—Signaling (54)	Information
Signaling (55)	Circuit Validation Successful—Signaling (55)	Information
Signaling (57)	Continuity Recheck Failed—Signaling (57)	Information
Signaling (58)	Continuity Recheck Successful—Signaling (58)	Information
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)	Information
Signaling (62)	Received Integrated Services Digital Network Restart Message—Signaling (62)	Information

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
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 (69)	Call Agent Is Not Up or Is Not Responding to the Feature Server—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
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)	Information
Signaling (77)	Integrated Services Digital Network D-Channel Switchover for Not Facility Associated Signaling—Signaling (77)	Information
Signaling (78)	Integrated Services Digital Network Single D-Channel Down for Not Facility Associated Signaling—Signaling (78)	Minor
Signaling (79)	Trunking Gateway Unreachable—Signaling (79)	Major
Signaling (80)	Out of Bounds, Memory/Socket Error—Signaling (80)	Critical
Signaling (81)	Insufficient Heap Memory—Signaling (81)	Critical
Signaling (82)	Insufficient Shared Memory Pools—Signaling (82)	Critical
Signaling (83)	Error While Binding to Socket—Signaling (83)	Critical
Signaling (84)	Reached Maximum Socket Limit—Signaling (84)	Critical
Signaling (85)	Initialization Failure—Signaling (85)	Critical
Signaling (86)	Remote H.323 Gateway Is Not Reachable—Signaling (86)	Major
Signaling (87)	H.323 Message Parsing Error—Signaling (87)	Major
Signaling (88)	H.323 Message Encoding Error—Signaling (88)	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)	Major
Signaling (92)	Invalid Call Identifier—Signaling (92)	Minor

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
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)	H.323 Protocol Inconsistencies—Signaling (98)	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)	H.323 Network Congested—Signaling (102)	Minor
Signaling (103)	Aggregation Connection Down—Signaling (103)	Major
Signaling (104)	Aggregation Unable to Establish Connection—Signaling (104)	Information
Signaling (105)	Aggregation Gate Set Failed—Signaling (105)	Information
Signaling (106)	Enhanced Subscriber Authentication Cisco BTS 10200 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 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

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
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)	Information
Signaling (134)	Signaling System 7 Message Encoding Failure—Signaling (134)	Information
Signaling (135)	Signaling System 7 Message Decoding Failure—Signaling (135)	Information
Signaling (136)	Signaling System 7 Message Invalid Received—Signaling (136)	Information
Signaling (137)	Signaling System 7 Confusion Message Received—Signaling (137)	Information
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)	Information
Signaling (140)	Unanswered Information Message—Signaling (140)	Information
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
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

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
Signaling (147)	Domain Name System Service Addresses Exhausted—Signaling (147)	Warning
Signaling (150)	Stream Control Transmission Protocol Association Congested—Signaling (150)	Minor
Signaling (151)	Subscriber Line Faulty—Signaling (151)	Minor
Signaling (152)	Termination Transient Error Received—Signaling (152)	Information
Signaling (153)	Emergency Trunks Become Locally Blocked—Signaling (153)	Critical
Signaling (154)	Emergency Trunks Become Remotely Blocked—Signaling (154)	Critical
Signaling (155)	Packet Cable Multi-Media Unsolicited Gate Delete—Signaling (155)	Information
Signaling (156)	Integrated Services Digital Network Signaling Gateway Down—Signaling (156)	Major
Signaling (157)	Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)	Major
Signaling (158)	Invalid Integrated Services Digital Network Interface Identification—Signaling (158)	Warning
Signaling (159)	Integrated Services Digital Network User Adaptation Layer Cannot Go Active—Signaling (159)	Warning
Signaling (160)	Integrated Services Digital Network User Adaptation Layer Cannot Go Standby—Signaling (160)	Warning
Signaling (161)	Session Initiation Protocol Update Not Allowed for Operator Service Position System Calls—Signaling (161)	Warning
Signaling (162)	Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)	Critical
Signaling (163)	Routing Key Inactive—Signaling (163)	Major
Signaling (164)	Signaling Gateway Traffic Mode Mismatch—Signaling (164)	Major
Signaling (165)	No Session Initiation Protocol P-DCS Billing Information Header Received—Signaling (165)	Warning
Signaling (166)	No Routing Keys Are Active—Signaling (166)	Warning
Signaling (167)	No Signaling Gateways Are Active—Signaling (167)	Warning
Signaling (168)	A Session Initiation Protocol Server Group Has No Child Elements Provisioned—Signaling (168)	Warning
Signaling (169)	Session Initiation Protocol Element Provisioned With Service Enabled Is Internally Disabled—Signaling (169)	Information
Signaling (170)	Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)	Minor
Signaling (171)	Residential Gateway Unreachable—Signaling (171)	Minor
Signaling (172)	Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)	Major

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
Signaling (173)	ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)	Critical
Signaling (174)	ENUM Server Unavailable—Signaling (174)	Critical
Signaling (175)	ENUM Server Farm Unavailable—Signaling (175)	Critical
Signaling (176)	No Resources Available to Launch ENUM Query—Signaling (176)	Critical
Signaling (177)	ISDN Unable to Restore D-Channel Into In-Service Active State—Signaling (177)	Warning
Signaling (178)	Possible Overlap Dialing Misconfiguration—Signaling (178)	Information
Signaling (179)	Trunk Group Registration Expired—Signaling (179)	Major
Signaling (182)	Transient Issue Occurred on the Emergency End-points—Signaling (182)	Major

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 reprovisioned.

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 10-136.

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 10-137.

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 10-137.

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 10-138.

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 10-138.

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 10-138.

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 10-138.

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 10-139.

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 10-139.

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 10-139.

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 10-139.

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 10-139.

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 10-139.

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 10-140.

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 10-140.

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 10-140.

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 10-141.

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 10-142.

Unanswered Blocking Message—Signaling (25)

The Unanswered Blocking Message 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.T
- he 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Circuit Group Blocking Message—Signaling (27)

The Unanswered Circuit Group Blocking Message 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Circuit Group Unblocking Message—Signaling (28)

The Unanswered Circuit Group Unblocking Message 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Circuit Validation Test Message—Signaling (30)

The Unanswered Circuit Validation Test Message 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Reset Circuit Message—Signaling (31)

The Unanswered Reset Circuit Message event serves as a warning that an 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 are running normally.

The call agent platform is active.

The SS7 interface hardware is in service.

The associated SS7 signaling link is available.

The T13 timer is set to an appropriate level.

The SS7 link is not congested.

Unanswered Group Reset Message—Signaling (32)

The Unanswered Group Reset Message 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.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Release Message—Signaling (33)

The Unanswered Release Message event serves as a warning that an 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Continuity Check Request Message—Signaling (34)

The Unanswered Continuity Check Request Message event serves as a warning that a continuity check request (CCR) message was not answered. The primary cause of the event is that an 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- 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 10-142.

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 10-142.

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 no 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 indicating that 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 find out whether 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 is 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 an informational alert that a general processing error has occurred. The primary cause of the event is that a general SS7 processing error occurred because all resources were busy or because an invalid even occurred. To correct the primary cause of the event, check 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 event is that an unexpected message was received for the current call state. To correct the primary cause of the event, examine 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 as 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 that 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 that the SS7 signaling adapter process and the SS7 interface are 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 a 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 10-142.

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 by 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, an unknown package type, an 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 10-142.

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 10-143.

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 10-143.

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 10-143.

Call Agent Is Not Up or Is Not Responding to the Feature Server—Signaling (69)

The Call Agent Is Not Up or Is Not Responding to the Feature Server alarm (critical) indicates that a CA and FS communications message timed out. To troubleshoot and correct the cause of the Call Agent Is Not Up or Is Not Responding to the Feature Server alarm, refer to the "Call Agent Is Not Up or Is Not Responding to the Feature Server—Signaling (69)" section on page 10-143.

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 troubleshoot 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 10-143.

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 Not Facility Associated Signaling—Signaling (77)

The Integrated Services Digital Network D-Channel Switchover for Not Facility Associated Signaling event functions as an informational alert that an ISDN D-channel switchover has occurred for 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 the gateway is operational and connection to PBX is good.

Integrated Services Digital Network Single D-Channel Down for Not Facility Associated Signaling—Signaling (78)

The Integrated Services Digital Network Single D-Channel Down for Not 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 Not Facility Associated Signaling alarm, refer to the "Integrated Services Digital Network Single D-Channel Down for Not Facility Associated Signaling—Signaling (78)" section on page 10-144.

Trunking Gateway Unreachable—Signaling (79)

The Trunking Gateway Unreachable alarm (major) indicates that the trunking gateway is not responding to keep-alive Audit Endpoint messages. To troubleshoot and correct the cause of the Media Gateway Unreachable alarm, refer to the "Trunking Gateway Unreachable—Signaling (79)" section on page 10-144.

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 10-144.

Insufficient Heap Memory—Signaling (81)

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)" section on page 10-144.

Insufficient Shared Memory Pools—Signaling (82)

The Insufficient Shared Memory Pools alarm (critical) indicates that there are 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)" section on page 10-144.

Error While Binding to Socket—Signaling (83)

The Error While Binding to Socket alarm (critical) indicates that an error occurred while the system was 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 10-145.

Reached Maximum Socket Limit—Signaling (84)

The Reached Maximum Socket Limit alarm (critical) indicates that the Cisco BTS 10200 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)" section on page 10-145.

Initialization Failure—Signaling (85)

The Initialization Failure alarm (critical) indicates that the Cisco BTS 10200 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 10-145.

Remote H.323 Gateway Is Not Reachable—Signaling (86)

The Remote H.323 Gateway Is Not Reachable alarm (major) indicates that the remote H.323 gateway is not reachable. To troubleshoot and correct the cause of the Remote H.323 Gateway Is Not Reachable alarm, refer to the "Remote H.323 Gateway Is Not Reachable—Signaling (86)" section on page 10-145.

H.323 Message Parsing Error—Signaling (87)

The H.323 Message Parsing Error alarm (major) indicates that a H.323 message-parsing error has occurred. To troubleshoot and correct the cause of the H.323 Message Parsing Error alarm, refer to the "H.323 Message Parsing Error—Signaling (87)" section on page 10-145.

H.323 Message Encoding Error—Signaling (88)

The H.323 Message Encoding Error alarm (major) indicates that a H.323 message-encoding error has occurred. To troubleshoot and correct the cause of the H.323 Message Encoding Error alarm, refer to the "H.323 Message Encoding Error—Signaling (88)" section on page 10-145.

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 10-146.

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 10-146.

Endpoint Security Violation—Signaling (91)

The Endpoint Security Violation alarm (major) indicates that an H.323 security violation has occurred. To troubleshoot and correct the cause of the Endpoint Security Violation alarm, refer to the "Endpoint Security Violation—Signaling (91)" section on page 10-146.

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 10-146.

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 10-146.

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 10-146.

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 10-147.

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 10-147.

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 10-147.

H.323 Protocol Inconsistencies—Signaling (98)

The H.323 Protocol Inconsistencies alarm (minor) indicates that the H.323 endpoint and Cisco BTS 10200 are running different protocol versions. To troubleshoot and correct the cause of the H.323 Protocol Inconsistencies alarm, refer to the "H.323 Protocol Inconsistencies—Signaling (98)" section on page 10-147.

Abnormal Call Clearing—Signaling (99)

The Abnormal Call Clearing alarm (minor) indicates that an unsupported or invalid message type was received from the network. To troubleshoot and correct the cause of the Abnormal Call Clearing alarm, refer to the "Abnormal Call Clearing—Signaling (99)" section on page 10-147.

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 10-147.

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 10-147.

H.323 Network Congested—Signaling (102)

The H.323 Network Congested alarm indicates (minor) that the H.323 application process has depleted its resources and no more calls can be completed. To troubleshoot and correct the cause of the H.323 Network Congested alarm, refer to the "H.323 Network Congested—Signaling (102)" section on page 10-148.

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 10-148.

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 Delivery Function Connection Down—Signaling (106)

The Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down alarm (minor) indicates that the enhanced subscriber authentication (ESA) Cisco BTS 10200 DF connection is down. To troubleshoot and correct the cause of the Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down alarm, refer to the "Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down—Signaling (106)" section on page 10-148.

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 10-148.

Simplex Only Operational Mode—Signaling (108)

The Simplex Only Operational Mode alarm (major) indicates that the Cisco BTS 10200 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 10-148.

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 10-149.

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 10-152.

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 10-153.

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

The Stream Control Transmission Protocol Association Configuration Error alarm (minor) indicates that an 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 10-154.

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 10-155.

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 10-155.

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 10-156.

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 10-156.

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 10-156.

Signaling System 7 Adapter Process Faulty—Signaling (119)

The Signaling System 7 Adapter Process Faulty alarm (critical) indicates that an S7A process is faulty. To troubleshoot and correct the cause of the Signaling System 7 Adapter Process Faulty alarm, refer to the "Signaling System 7 Adapter Process Faulty—Signaling (119)" section on page 10-156.

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 "Signaling System 7 Module/Signaling System 7 Adapter Faulty—Signaling (120)" section on page 10-156.

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 10-157.

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 10-157.

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 10-157.

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 10-157.

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 10-158.

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 10-158.

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 preconfigured dialogue IDs or invoke IDs. To correct the primary cause of the event, increase the number of preconfigured 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 an 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.

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 an 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 an SS7 trace of the circuit for examination by Cisco TAC.

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 an SS7 trace of the circuit for examination by Cisco TAC.

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 an 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.

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, 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 the limit.

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

The Signaling System 7 Trunk was Found to be in Erroneous State event functions as an informational alert that an 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 by use of the 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 an 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 provisioning.

The following tips might help you troubleshoot NLP/DNS related issues:

- Grep for GET_HOST_BY_NAME keyword in the traces at INFO3 trace level.
- Grep for warning/error keyword in the traces at INFO3 trace level.

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 10-158.

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 10-158.

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 10-158.

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 10-159.

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 that 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 correct the order of IP addresses and ensure that previous hop network component is alive and in a healthy state.

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 provisioning.

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 10-159.

Subscriber Line Faulty—Signaling (151)

The Subscriber Line Faulty alarm (minor) indicates that the residential gateway returned an error code in response to a command from the MGW. To troubleshoot and correct the cause of the Subscriber Line Faulty alarm, refer to the "Subscriber Line Faulty—Signaling (151)" section on page 10-160.

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 is that the MGCP signaling process has inter-operational errors. To correct the primary cause of the event, notify Cisco TAC.

Emergency Trunks Become Locally Blocked—Signaling (153)

The Emergency Trunks Become Locally Blocked alarm (critical) indicates that an emergency trunk (CAS, SS7, or ISDN) is locally blocked. To troubleshoot and correct the cause of the Emergency Trunks Become Locally Blocked alarm, refer to the "Emergency Trunks Become Locally Blocked—Signaling (153)" section on page 10-160.

Emergency Trunks Become Remotely Blocked—Signaling (154)

The Emergency Trunks Become Remotely Blocked alarm (critical) indicates that an emergency trunk (CAS, SS7, or ISDN) is remotely blocked. To troubleshoot and correct the cause of the Emergency Trunks Become Remotely Blocked alarm, refer to the "Emergency Trunks Become Remotely Blocked—Signaling (154)" section on page 10-160.

Packet Cable Multi-Media Unsolicited Gate Delete—Signaling (155)

The Packet Cable Multi-Media Unsolicited Gate Delete event serves as an informational alert that an error condition was encountered by the CMTS. To correct the cause of the event, check the alarms and warnings from the CMTS.

Integrated Services Digital Network Signaling Gateway Down—Signaling (156)

The Integrated Services Digital Network Signaling Gateway Down alarm (major) indicates that the Cisco BTS 10200 system cannot communicate with the ISDN gateway. To troubleshoot and correct the cause of the Integrated Services Digital Network Signaling Gateway Down alarm, refer to the "Integrated Services Digital Network Signaling Gateway Down—Signaling (156)" section on page 10-161.

Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)

The Integrated Services Digital Network Signaling Gateway Inactive alarm (major) indicates that a **shutdown** command has been executed in the application server on the ISDN gateway side. To troubleshoot and correct the cause of the Integrated Services Digital Network Signaling Gateway Inactive alarm, refer to the "Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)" section on page 10-161.

Invalid Integrated Services Digital Network Interface Identification—Signaling (158)

The Invalid Integrated Services Digital Network Interface Identification event serves as a warning that an interface ID is not configured correctly on the ISDN gateway side. To correct the cause of the event, configure the D-channel correctly on the gateway side. The D-channel configuration on the call-agent side should match that on the gateway side.

Integrated Services Digital Network User Adaptation Layer Cannot Go Active—Signaling (159)

The Integrated Services Digital Network User Adaptation Layer Cannot Go Active event serves as a warning that no active acknowledgement messages are being received from any signaling gateway. This indicates that the ISDN signaling gateway or the SCTP associations are probably down. To correct the cause of the event, investigate other alarms to see if the signaling gateways are down or to see if the SCTP associations are down. Take corrective action according to the alarm indications.

Integrated Services Digital Network User Adaptation Layer Cannot Go Standby—Signaling (160)

The Integrated Services Digital Network User Adaptation Layer Cannot Go Standby event serves as a warning that no active acknowledgement messages are being received from any signaling gateway. This indicates that the ISDN signaling gateway or the SCTP associations are probably down. To correct the cause of the event, investigate other alarms to see if the signaling gateways are down or the SCTP associations are down. Take corrective action according to the alarm indications.

Session Initiation Protocol Update Not Allowed for Operator Service Position System Calls—Signaling (161)

The Session Initiation Protocol Update Not Allowed for Operator Service Position System Calls event serves as a warning that the remote switch is not allowing the Cisco BTS 10200 to send SIP update messages. The update messages are mandatory in the CMSS and are used exclusively by the Cisco BTS 10200 for operator service calls over SIP including BLV, emergency interrupt, and 911 ringback calls. To correct the cause of the event, upgrade or reprovision the remote switch so it can process incoming SIP update messages.

Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)

The Session Initiation Protocol Server Group Element Operationally Out of Service alarm (critical) indicates that the Cisco BTS 10200 is unable to communicate with a remote SIP party (call-agent or proxy) over a SIP server group element. To troubleshoot and correct the cause of the Session Initiation Protocol Server Group Element Operationally Out of Service alarm, refer to the "Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)" section on page 10-161.

Routing Key Inactive—Signaling (163)

The Routing Key Inactive alarm (major) indicates that inactive acknowledgement messages were received from a Signaling Gateway. The SG or SCTP associations are probably down. To troubleshoot and correct the primary cause of the Routing Key Inactive alarm, refer to the "Routing Key Inactive—Signaling (163)" section on page 10-161.

Signaling Gateway Traffic Mode Mismatch—Signaling (164)

The Signaling Gateway Traffic Mode Mismatch alarm (major) indicates that the traffic mode does not match on the Cisco BTS 10200 and the Signaling Gateway. To troubleshoot and correct the primary cause of the Signaling Gateway Traffic Mode Mismatch alarm, refer to the "Signaling Gateway Traffic Mode Mismatch—Signaling (164)" section on page 10-162.

No Session Initiation Protocol P-DCS Billing Information Header Received—Signaling (165)

The No Session Initiation Protocol P-DCS Billing Information Header Received event serves as a warning that no SIP P-DCS billing information headers are being received. The primary cause of the event is that the originating switch is not provisioned to add the P-DCS Billing Information header to outgoing SIP requests and responses. To correct the primary cause of the event, provision the originating switch to add P-DCS Billing Information header to outgoing messages. The secondary cause of the event is that the header could have been stripped off by an intermediate proxy. To correct the secondary cause of the event, determine if the header has been stripped off by an intermediate proxy and configure the system for corrective action if so. The ternary cause of the event is that there was a SIP message encoding error at the sending switch. To correct the ternary cause of the event, determine if a SIP message encoding error occurred at the adjacent switch and if so, call the technical assistance center to determine a fix for the problem.

No Routing Keys Are Active—Signaling (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. To correct the primary cause of the event, check the communication path between Cisco BTS 10200 and the ITP.

A Session Initiation Protocol Server Group Has No Child Elements Provisioned—Signaling (168)

The A Session Initiation Protocol Server Group Has No Child Elements Provisioned event is issued as a warning when a SIP Server Group administrative in-service is provisioned but has no child elements provisioned. This Server Group will be considered as if it were administratively out of service. If that is acceptable, no action is required. If the server group was expected to be workable, place the server group back out of service, resolve the provisioning problem, and place it back into service.

Session Initiation Protocol Element Provisioned With Service Enabled Is Internally Disabled—Signaling (169)

The Session Initiation Protocol Element Provisioned with Service Enabled is Internally Disabled event functions as an informational alert that a SIP element was provisioned with SRV enabled and is associated to at least one or more Server Groups. The SRV flag will be assumed disabled. However, to resolve this informational message, provision the SRV flag disabled on the SIP element.

Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)

The Residential Gateway Endpoints Are Out of Service at the Gateway alarm (minor) indicates that the residential gateway has been administratively taken OOS using the command at the gateway. To troubleshoot and correct the primary cause of the Residential Gateway Endpoints Are Out of Service at the Gateway alarm, refer to the "Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)" section on page 10-162.

Residential Gateway Unreachable—Signaling (171)

The Residential Gateway Unreachable alarm (minor) indicates that a MGCP signaling interop error has occurred with the residential media gateway. To troubleshoot and correct the primary cause of the Residential Gateway Unreachable alarm, refer to the "Residential Gateway Unreachable—Signaling (171)" section on page 10-162.

Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)

The Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address alarm (major) indicates that the MTA has been moved to a new subnet which is not provisioned, or provisioned with the aggr-id=null. To troubleshoot and correct the primary cause of the Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address alarm, refer to the "Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)" section on page 10-162.

ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)

The ENUM Server Domain Cannot be Resolved Into Any IP Address alarm (critical) indicates that a misconfiguration has occurred in the DNS configuration. To troubleshoot and correct the cause of the ENUM Server Domain Cannot be Resolved Into Any IP Address alarm, refer to the "ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)" section on page 10-162.

ENUM Server Unavailable—Signaling (174)

The ENUM Server Unavailable alarm (critical) indicates that a network or server problem has occurred. To troubleshoot and correct the cause of the ENUM Server Unavailable alarm, refer to the "ENUM Server Unavailable—Signaling (174)" section on page 10-163.

ENUM Server Farm Unavailable—Signaling (175)

The ENUM Server Farm Unavailable alarm (critical) indicates that a network or server problem has occurred. To troubleshoot and correct the cause of the ENUM Server Farm Unavailable alarm, refer to the "ENUM Server Farm Unavailable—Signaling (175)" section on page 10-163.

No Resources Available to Launch ENUM Query—Signaling (176)

The No Resources Available to Launch ENUM Query alarm (critical) indicates that no resources are available to launch the ENUM query. The primary cause of the alarm is that there is internal or network congestion or that the server response is slow. To troubleshoot and correct the primary cause of the alarm, refer to the "No Resources Available to Launch ENUM Query—Signaling (176)" section on page 10-163.

ISDN Unable to Restore D-Channel Into In-Service Active State—Signaling (177)

The ISDN Unable to Restore D-Channel Into In-Service Active State warning event indicates that the Cisco BTS 10200 did not receive the Service Ack from the remote end in response to the Service message to make the D-Channel active. To correct the cause of the event, ensure that the NFAS provisioning at the PBX/media gateway is correct.

Possible Overlap Dialing Misconfiguration—Signaling (178)

The Possible Overlap Dialing Misconfiguration event serves as an informational alert that the Cisco BTS 10200 sent out an invite with an overlap flag, and has received one or more additional digits to be forwarded. However, the call attempt fails while the Cisco BTS 10200 is still waiting to send out the first additional digit. A possible cause is a misconfiguration of the Overlap Dialing feature between the local and peer switches. To correct the cause of the event, make sure that the peer switch is configured to support the Overlap Dialing feature. Check that the feature is enabled and that the dial-plan is configured correctly. Also make sure that the Destination/Route/Trunk group on the peer switch is marked to support the Overlap Sending feature.

Trunk Group Registration Expired—Signaling (179)

The Trunk Group Registration Expired alarm (major) indicates that a trunk group registration has expired. The primary cause of the alarm is that the trunk group did not register in time before the contact expiry. To troubleshoot and correct the primary cause of the Trunk Group Registration Expired alarm, refer to the "Trunk Group Registration Expired—Signaling (179)" section on page 10-163.

Troubleshooting Signaling Alarms

This section provides the information you need for monitoring and correcting signaling alarms. Table 10-163 lists all of the signaling alarms in numerical order and provides cross-references to each subsection.

Note Refer to the "Obtaining Documentation and Submitting a Service Request" section on page 1 for detailed instructions on contacting Cisco TAC and opening a service request.

Table 10-163 Cisco BTS 10200 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

Table 10-163 Cisco BTS 10200 Signaling Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
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 (69)	Call Agent Is Not Up or Is Not Responding to the Feature Server—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 Not Facility Associated Signaling—Signaling (78)	Minor
Signaling (79)	Trunking Gateway Unreachable—Signaling (79)	Major
Signaling (80)	Out of Bounds, Memory/Socket Error—Signaling (80)	Critical
Signaling (81)	Insufficient Heap Memory—Signaling (81)	Critical
Signaling (82)	Insufficient Shared Memory Pools—Signaling (82)	Critical
Signaling (83)	Error While Binding to Socket—Signaling (83)	Critical
Signaling (84)	Reached Maximum Socket Limit—Signaling (84)	Critical
Signaling (85)	Initialization Failure—Signaling (85)	Critical
Signaling (86)	Remote H.323 Gateway Is Not Reachable—Signaling (86)	Major
Signaling (87)	H.323 Message Parsing Error—Signaling (87)	Major
Signaling (88)	H.323 Message Encoding Error—Signaling (88)	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)	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)	H.323 Protocol Inconsistencies—Signaling (98)	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)	H.323 Network Congested—Signaling (102)	Minor
Signaling (103)	Aggregation Connection Down—Signaling (103)	Major
Signaling (106)	Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down—Signaling (106)	Minor
Signaling (107)	Logical Internet Protocol Addresses Not Mapped Correctly—Signaling (107)	Critical

Table 10-163 Cisco BTS 10200 Signaling Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
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
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)	Subscriber Line Faulty—Signaling (151)	Minor
Signaling (153)	Emergency Trunks Become Locally Blocked—Signaling (153)	Critical

Table 10-163 Cisco BTS 10200 Signaling Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
Signaling (154)	Emergency Trunks Become Remotely Blocked—Signaling (154)	Critical
Signaling (156)	Integrated Services Digital Network Signaling Gateway Down—Signaling (156)	Major
Signaling (157)	Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)	Major
Signaling (162)	Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)	Critical
Signaling (163)	Routing Key Inactive—Signaling (163)	Major
Signaling (164)	Signaling Gateway Traffic Mode Mismatch—Signaling (164)	Major
Signaling (170)	Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)	Minor
Signaling (171)	Residential Gateway Unreachable—Signaling (171)	Minor
Signaling (172)	Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)	Major
Signaling (173)	ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)	Critical
Signaling (174)	ENUM Server Unavailable—Signaling (174)	Critical
Signaling (175)	ENUM Server Farm Unavailable—Signaling (175)	Critical
Signaling (176)	No Resources Available to Launch ENUM Query—Signaling (176)	Critical
Signaling (179)	Trunk Group Registration Expired—Signaling (179)	Major

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 that 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.

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 might 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 might 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.

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 the **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 is unable to communicate with a gateway. Verify that the gateway is 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 resending 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.

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.

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, a 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 restarted; 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 nonoperational, 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 cause 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 the 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 is unable to communicate with the specified DPC in the SS7 network. Use these steps to determine if the issue is a communication problem between the Cisco BTS 10200 and the IP transfer point (ITP) or if it is related to communication problems between the ITP and the DPC:

Step 1 Use the Cisco BTS 10200 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 10-152. 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 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 10-157. Otherwise, proceed to Step 3.

Step 3 If you arrive at this step, there is probably communication between the Cisco BTS 10200 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. Please contact the Cisco TAC.

Step 5 Check whether the DPC has been removed from the Cisco BTS 10200 database. At the Cisco BTS 10200 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, that is, 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. No action is required.

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. The alarm is issued when service OOS message is received for ISDN trunks or 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 affected 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 the specified ISDN trunk group 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.

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.

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.

Call Agent Is Not Up or Is Not Responding to the Feature Server—Signaling (69)

The Call Agent Is Not Up or Is Not Responding to the Feature Server 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 Not Facility Associated Signaling—Signaling (78)

The Integrated Services Digital Network Single D-Channel Down for Not 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.

Trunking Gateway Unreachable—Signaling (79)

The Trunking Gateway Unreachable alarm (major) indicates that the trunking gateway is not responding to keep-alive Audit Endpoint messages. To correct the primary cause of the alarm, check the IP connectivity status between Cisco BTS 10200 call agent and the trunking gateway.

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. 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.

Note Heap memory usage is automatically monitored once per hour.

Insufficient Heap Memory—Signaling (81)

The Insufficient Heap Memory alarm (critical) indicates that there is insufficient heap memory. The primary cause of the alarm is that the H.323 signaling adapter was unable to allocate memory from the system. To correct the primary cause of the alarm, contact Cisco TAC for assistance.

Note Heap memory usage is automatically monitored once per hour.

Insufficient Shared Memory Pools—Signaling (82)

The Insufficient Shared Memory Pools alarm (critical) indicates that there is that there are not enough shared memory pools. The primary cause of the alarm is that the H.323 signaling adapter was unable to allocate storage. To correct the primary cause of the alarm, contact Cisco TAC for corrective action.

Error While Binding to Socket—Signaling (83)

The Error While Binding to Socket alarm (critical) indicates that an error occurred while the system was binding to the socket. To correct the primary cause of the alarm, contact Cisco TAC for corrective action.

Reached Maximum Socket Limit—Signaling (84)

The Reached Maximum Socket Limit alarm (critical) indicates that the Cisco BTS 10200 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 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 the Reason dataword for the failure cause and take action accordingly.

Remote H.323 Gateway Is Not Reachable—Signaling (86)

The Remote H.323 Gateway Is Not Reachable alarm (major) indicates that the remote H.323 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.

H.323 Message Parsing Error—Signaling (87)

The H.323 Message Parsing Error alarm (major) indicates that an H.323 message parsing error has occurred. The primary cause of the alarm is that the system was unable to successfully parse an incoming H.323 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.

H.323 Message Encoding Error—Signaling (88)

The H.323 Message Encoding Error alarm (major) indicates that an H.323 message encoding error has occurred. The primary cause of the alarm is that the system was unable to encode an H.323 message for sending. The alarm is indicative a software bug. To correct the primary cause of the alarm, contact Cisco TAC.

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.

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.

Endpoint Security Violation—Signaling (91)

The Endpoint Security Violation alarm (major) indicates that an H.323 security violation has occurred. The primary cause of the alarm is that an H.323 security violation has occurred. To correct the primary cause of the alarm, check to make sure the password selections on the Cisco BTS 10200 and the gatekeeper are correct. The secondary cause of the alarm is that the H.323GW table may not be provisioned properly or there is a time synchronization problem between the Cisco BTS 10200 and/or the gatekeeper and the NTP server. To correct the secondary cause of the alarm, ensure that both the Cisco BTS 10200 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 or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC.

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 or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC.

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 or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC.

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.

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.

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.

H.323 Protocol Inconsistencies—Signaling (98)

The H.323 Protocol Inconsistencies alarm (minor) indicates that the H.323 endpoint and Cisco BTS 10200 are running different protocol versions. The primary cause of the alarm is that the H.323 endpoint and the Cisco BTS 10200 are running different protocol versions. This is only an issue where the endpoint is running a higher version of the H.323 protocol than the Cisco BTS 10200. To correct the primary cause of the alarm, contact Cisco TAC.

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.

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, reprovision 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.

H.323 Network Congested—Signaling (102)

The H.323 Network Congested alarm indicates (minor) that the H.323 application process has depleted its resources and no more calls can be completed. The primary cause of this alarm is that the H.323 application process has depleted its 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, reprovision the water marks or check the network for overload. Also verify that alternate routes have been provisioned on the Cisco BTS 10200.

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 Delivery Function Connection Down—Signaling (106)

The Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down alarm (minor) indicates that the ESA Cisco BTS 10200 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. 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.

Simplex Only Operational Mode—Signaling (108)

The Simplex Only Operational Mode alarm (major) indicates that the Cisco BTS 10200 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 is configured as a simplex system.

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 is unable to communicate with an SGP at the SCTP protocol level. 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 CLI prompt:

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

If the response displays adminstrator 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/en/US/products/sw/wirelssw/ps1862/tsd_products_support_series_home.html

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. If the ASP on the active Cisco BTS 10200 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.

a. Determine the Cisco BTS 10200 configured values for the Cisco BTS 10200 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 are derived from the DNS name, which is given directly after the -h option. At the Cisco BTS 10200 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 configured local IP addresses are given in the Addresses: line.

b. Determine the ITP configured values of the ITP Cisco BTS 10200 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 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 side of the SCTP association. The two remote-IP addresses are the addresses that the ITP has configured for the Cisco BTS 10200 side of the SCTP association. Make sure all of these values match the values found in Step 2A.

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

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

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

The output shows the IP addresses and port. For example:

```
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 IP addresses and port.

- Log on to the ITP and get into enable mode.
- Enter **sho run**.
- Press **Enter** until the m3ua (or sua) configuration is displayed. In our example, we are considering the SCTP association connection between the Cisco BTS 10200 and the ITP, so we will look at the ITP m3ua configuration. For example:

  ```
  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 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 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 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 is reachable from the ITP.

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

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

show run

c. Press **Enter** until the ASP configuration is displayed. A section similar to the following will display the Cisco BTS 10200 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 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 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 shows either operator state -> SCTP-ASSOC out of service or operator state -> SCTP-ASSOC in service.

If the operator 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 the 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 CLI command:

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

The output displays either operator state -> SCTP-ASSOC out of service or operator state -> SCTP-ASSOC in service.

If the operator 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 10-155 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 10-153, 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 an 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 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 10-153 to verify that your IP addresses and ports are properly configured on the Cisco BTS 10200.

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.

Signaling Gateway Failure—Signaling (113)

Note When a port on an ITP is removed from service by use of the **shut** command, multiple Signaling 113 and 114 alarms are raised (on status). When the port is recovered, through cycling of the ITP power, all alarms raised are cleared (off status) and are removed from CURRENT_ALARM table. However, not all cleared alarms (off status) are displayed on the subscriber terminal. Only the first instance of the cleared alarms (off status) with a variation in type, number, and component-ID **is** displayed. Multiple instances of the cleared alarms (off status) where the type, number, and component-ID are identical **are not** displayed.

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.

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 10-153 to determine why the associated SGPs are down.

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

Note When a port on an ITP is removed from service by use of the **shut** command, multiple Signaling 113 and 114 alarms are raised (on status). When the port is recovered, through cycling of the ITP power, all alarms raised are cleared (off status) and are removed from CURRENT_ALARM table. However, not all cleared alarms (off status) are displayed on the subscriber terminal. Only the first instance of the cleared alarms (off status) with a variation in type, number, and component-ID **is** displayed. Multiple instances of the cleared alarms (off status) where the type, number, and component-ID are identical **are not** displayed.

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 the 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 10-153. 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 a user part is unavailable on 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 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 10-153 to determine why the Cisco BTS 10200 is unable to communicate with any of the SGs at the M3UA layer. See the "Check the Stream Control Transmission Protocol Association Status" section on page 13-3 to determine why the Cisco BTS 10200 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 node that is trying to go into platform Active mode. It occurs when this Cisco BTS 10200 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. See the "Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down)—Signaling (111)" section on page 10-153 to determine why the Cisco BTS 10200 is unable to communicate with any of the ITPs at the M3UA layer. Refer to the "Check the Stream Control Transmission Protocol Association Status" section on page 13-3 to determine why the Cisco BTS 10200 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. To correct the primary cause of the alarm, contact your service control point (SCP) service provider for assistance.

Note This alarm can occur when there is an SS7 outage affecting a nonadjacent remote destination point code (DPC) where the global title translation (GTT) database resides. The SS7 SCP subsystems in the Cisco BTS 10200 show the allowed status but the related DPC is shown to be unavailable.

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, reinitialize 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 points (SAPs) 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; such as, 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, reinitialize 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 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 the TSAP address of the remote entity is a domain name. Verify that 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 find out what is preventing the TSAP address from being reached. Verify that 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, eliminate 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.

Subscriber Line Faulty—Signaling (151)

The Subscriber Line Faulty alarm (minor) indicates that the residential gateway returned an error code in response to a command from the MGW. To correct the primary cause of the alarm, try controlling subscriber termination to OOS and back into INS using the Cisco BTS 10200 CLI command. If the problem persist after more calls, check the configuration in the Cisco BTS 10200 and the RGW. If the error codes returned by MGW are harmless, the error codes can be suppressed by adding a new entry in the MGCP-RETCODE-ACTION table and changing the EP-ACTION to reset/none.

Note The following additional troubleshooting information is applicable to Release 5.0 MR2 and above.

If the VXSM is OOS at the GW side, a 501 error message for CRCX/AUEP may be transmitted. This generally occurs if there is resource state mismatch between the Cisco BTS 10200 (ACTV IDLE) and the VXSM (DOWN). For additional information on the 501 error message, refer to Appendix A, "Recoverable and Nonrecoverable Error Codes."

When the mismatch occurs the default behavior is update for both the create connection (CRCX) and audit endpoint (AUEP) messages. For example:

```
CLI> add mgcp-retcode-action mgw-profile-id=<abc>; mgcp-msg=AUEP; mgcp-retcode=501;
call-action=release; ep-action=update

CLI> add mgcp-retcode-action mgw-profile-id=<abc>; mgcp-msg=AUEP; mgcp-retcode=501;
call-action=release; ep-action=update
```

If a 501 response is received for the CRCX message on execution of the EP-ACTION=update for CRCX, the Cisco BTS 10200 will start auditing the endpoint by sending an AuditEndpoint message requesting restart-method (rm parameter reported in the RSIP message, which indicates the service state at the GW). If the restart-method information reported in AUEP message is different from the Cisco BTS 10200 termination state, the termination state will be updated accordingly. If rm=forced, the termination oper-status is set to down; if rm=restart, the termination oper-status is set to up.

If a 501 response is received for the AUEP message on execution of the EP-ACTION=update for AUEP, the Cisco BTS 10200 will unconditionally mark the termination as down.

To clear down from the termination oper-status, you either need to control the trunk/subscriber-termination OOS/INS mode=forced; or trigger RSIP rm=restart from the GW.

Emergency Trunks Become Locally Blocked—Signaling (153)

The Emergency Trunks Become Locally Blocked alarm (critical) is issued when an emergency trunk (CAS, SS7, or ISDN) becomes locally blocked.

Emergency Trunks Become Remotely Blocked—Signaling (154)

The Emergency Trunks Become Remotely Blocked alarm (critical) is issued when an emergency trunk (CAS, SS7, or ISDN) becomes remotely blocked.

Integrated Services Digital Network Signaling Gateway Down—Signaling (156)

The Integrated Services Digital Network Signaling Gateway Down alarm (major) is issued when the Cisco BTS 10200 cannot communicate to the ISDN gateway. The primary cause of the alarm is that the Cisco BTS 10200 cannot communicate to the ISDN gateway due to a failure in the gateway. Additionally, the SCTP association might be down. To correct the primary cause of the alarm, find out whether the SCTP association is down and restore the SCTP association. The secondary cause of the alarm is that the IUA layer may be down in the gateway. If the IUA layer is down, it will be automatically recovered; no further action is required.

Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)

The Integrated Services Digital Network Signaling Gateway Inactive alarm (major) indicates that a **shutdown** command has been executed in the application server on the ISDN gateway side. No action needed. The application server will be automatically recovered.

Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)

The Session Initiation Protocol Server Group Element Operationally Out of Service alarm (critical) is issued when the Cisco BTS 10200 is unable to communicate with a remote SIP party. The primary cause of the alarm is that the Cisco BTS 10200 is unable to communicate with a remote SIP party (call-agent or proxy) over a SIP server group element. To correct the primary cause of the alarm, verify 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 TSAP address from the Event Report. If the same alarm is reported for other TSAP addresses on several softswitch trunk groups and/or server-group elements, then verify that the network connection is operational. The secondary cause of the alarm is that the remote SIP party is not operational. To correct the secondary cause of the alarm, diagnose the issue that prevents the TSAP address from being reached if a ping is not successful. Verify that the SIP application is running on the remote host and listening on the port specified in the TSAP address.

Routing Key Inactive—Signaling (163)

The Routing Key Inactive alarm (major) indicates that inactive acknowledgement messages were received from a Signaling Gateway. The SG or SCTP associations are probably down. To troubleshoot and correct the primary cause of the Routing Key Inactive alarm, investigate other alarms to see if SGs are down or the SCTP associations are down. Take corrective action according to those alarms. Also check the AS status for the routing context on ITP.

Signaling Gateway Traffic Mode Mismatch—Signaling (164)

The Signaling Gateway Traffic Mode Mismatch alarm (major) indicates that the traffic mode does not match on the Cisco BTS 10200 and the Signaling Gateway. To troubleshoot and correct the primary cause of the Signaling Gateway Traffic Mode Mismatch alarm, verify the AS traffic-mode configuration in the Signaling Gateway. Check that the SG internal redundancy mode for the traffic-mode setting has been set correctly in the Cisco BTS 10200.

Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)

The Residential Gateway Endpoints Are Out of Service at the Gateway alarm (minor) indicates that the residential gateway has been administratively taken OOS using the command at the gateway. To troubleshoot and correct the primary cause of the Residential Gateway Endpoints are out of Service at the Gateway alarm, bring the residential gateway administratively into INS using the command at the gateway.

Residential Gateway Unreachable—Signaling (171)

The Residential Gateway Unreachable alarm (minor) indicates that a MGCP signaling interop error has occurred with the residential media gateway. To troubleshoot and correct the primary cause of the Residential Gateway Unreachable alarm, check the IP connectivity status between the Cisco BTS 10200 call agent and the trunking gateway if the residential gateway is not physically connected, but controlled INS at the Cisco BTS 10200.

Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)

The Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address alarm (major) indicates that the MTA has been moved to new subnet which is not provisioned, or provisioned with the aggr-id=null. To troubleshoot and correct the primary cause of the Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address alarm, provision the subnet aggr-id for the MTA.

ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)

The ENUM Server Domain Cannot be Resolved Into Any IP Address alarm (critical) indicates that a misconfiguration has occurred in the DNS configuration. To troubleshoot and correct the cause of the alarm, fix the DNS configuration according the documentation. Use the **status** command to check the status of the ENUM profile. If it is out of service (OOS), use the control INS command to bring it back into service. For example:

```
control enum-profile id=privateENUM;mode=forced;target-state=INS
change call_agent_profile id=CA146;enum_supp=Y;
```

ENUM Server Unavailable—Signaling (174)

The ENUM Server Unavailable alarm (critical) indicates that a network or server problem has occurred. To troubleshoot and correct the cause of the alarm, fix the network or server problem. Use the **status** command to check the status of the ENUM profile. If it is out of service (OOS), use the control INS command to bring it back into service. For example:

```
control enum-profile id=privateENUM;mode=forced;target-state=INS
change call_agent_profile id=CA146;enum_supp=Y;
```

ENUM Server Farm Unavailable—Signaling (175)

The ENUM Server Farm Unavailable alarm (critical) indicates that a network or server problem has occurred. To troubleshoot and correct the cause of the alarm, fix the network or server problem. Use the **status** command to check the status of the ENUM profile. If it is out of service (OOS), use the control INS command to bring it back into service. For example:

```
control enum-profile id=privateENUM;mode=forced;target-state=INS
change call_agent_profile id=CA146;enum_supp=Y;
```

No Resources Available to Launch ENUM Query—Signaling (176)

The No Resources Available to Launch ENUM Query alarm (critical) indicates that no resources are available to launch the ENUM query. The primary cause of the alarm is that there is internal or network congestion or that the server response is slow. To troubleshoot and correct the primary cause of the alarm, fix the network congestion or improve the server response.

Trunk Group Registration Expired—Signaling (179)

The Trunk Group Registration Expired alarm (major) indicates that a trunk group registration has expired. The primary cause of the alarm is that the trunk group did not register in time before the contact expiry. To troubleshoot and correct the primary cause of the Trunk Group Registration Expired alarm, verify that the receipt of a subsequent registration clears the alarm.

Transient Issue Occurred on the Emergency End-points—Signaling (182)

The Transient Issue Occurred on the Emergency End-points alarm (major) indicates that a transient error has occurred. The primary cause of the alarm is that:

- A transient error such as, 5XX error for CRCX, or a transient shm error, or an out-of-sequence message received at the MGA (MGCP protocol adapter) occurred on emergency end-points. Previously, the Signaling (152) alarm was raised at INFO level for all type of end-points. Beginning Release 6.0.4, the Signaling (182) is raised at a major severity level for such events on emergency end-points.
- Additionally, an error occurred for 911 call at BCM (Basic Call Module) like trunk group OOS, causing the Signaling (182) alarm to be raised at major severity, apart from other CALLP alarms at INFO level.

This behavior is controlled by a new CA_CONFIG type—SPECIAL-ALARM-FOR-911-TRANS-ISSUES DATATYPE. The default value of this field is N. Set it to Y to enable logging of Signaling (182).

To troubleshoot and correct the primary cause of the Transient Issue Occurred on the Emergency End-points alarm, take action based on the description provided when the alarm is logged. For example, if the description indicates that the trunk is OOS, control the trunk back to INS, if required. Since these alarms only denote a transient error and do not have any corresponding trigger point to clear the alarm, the operator needs to clear the alarms from the CLI frequently (if the operator has opted for logging of this alarm).