Cisco EGW 2200 Alarms

This section lists alarms generated by the Cisco EGW 2200 software.

Identifying Alarm Components

The affected component for each alarmis identified in the EGW Component column of the EGW Alarms screen. Use the following list to map the contents of the EGW Component column to your system.

- DPNSS voice-enabled gateway

    - MGCP link—*gateway name*-mgcp-ip1 and *gateway name*-mgcp-ip2 (if redundancy is used)

    - MGCP path—*gateway name*-mgcp-path

    - Backhaul—*gateway name*-bh-asso

    - T1/E1—*gateway name-slot number-port number*-path and *gateway name-slot number-port number*-dch

    ✎
    Note   When a T1/E1 problem occurs, two identical alarms are issued: one for the signaling path and another for the D-channel. Perform any corrective actions for the alarm on the signaling path. The alarm on the D-channel can be ignored.

- QSIG or PRI voice-enabled gateway

    - MGCP link—*gateway name*-mgcp-ip1 and *gateway name*-mgcp-ip2 (if redundancy is used)

    - MGCP path—*gateway name*-mgcp-path

    - Backhaul—*gateway name*-bh-sess-1 and *gateway name*-bh-sess-2 (if redundancy is used)

    - T1/E1—*gateway name-slot number-port number*-path and *gateway name-slot number-port number*-dch

    ✎
    Note   When a T1/E1 problem occurs, two identical alarms are issued: one for the signaling path and another for the D-channel. Perform any corrective actions for the alarm on the signaling path. The alarm on the D-channel can be ignored.

- Cisco CallManager

    - H.323 link—h323-1-ip

    - H.323 path—h323-1-path

    - CTI—ccm1

    - AXL—axlsvr1

- IP Routes—iproute*number* (iproute1, iproute2, etc.)

Alarm Categories

This section contains information on the alarms categories that can generated by the Cisco EGW 2200 software.

Admin State Locked

This alarm occurs when a user places a component in the locked administrative stat. The lock procedure gracefully takes down the calls and marks bearer channels as locked.

- Severity**—**Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action necessary. For more information, refer to the Admin State Unlocked event below.

Admin State Unlocked

This alarm occurs when a user places a component in the unlocked administrative state. The unlocked procedure marks bearer channels as available for call processing.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action necessary. For more information, refer to the Admin State Locked event, above.

All Conn Cntl Links Fail

This alarm occurs when all MGCP IP links have failed.

- Severity—Major
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

All ISDN IP Conn Fail

This alarm occurs when all IP connections that support the backhaul of the upper layers of ISDN have failed.

- Severity—Major
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW with Alarms.

ANAL: ALoopCtrExceeded

This alarm occurs when the A-loop counter threshold is exceeded. It indicates that the A-number analysis function has gone into an infinite loop. The A-loop counter limits the number of passes through the analysis tree to 30.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: ATableFail_GetDigTree

This alarm occurs when an invalid path has been specified for A-number analysis or the A-number analysis table is not loaded.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: ATableFail_GetDigMod

This alarm occurs when an A-number failed to get a modification table. It indicates that the modification table is not loaded or a pointer to a nonexistent location in the modification table is given.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: ATableFail_GetResult

This alarm occurs when a table failed to get a result table during main anlaysis. The problem occurs when the result table is not loaded or a pointer to a nonexistent location in the result table is given.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: ATableFlt_DgtRangeError

This alarm occurs when an A-Number analysis digit tree is accessed with an overdecadic digit.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: ATableFlt_IdxRangeError

This alarm occurs when an A-number analysis digit tree is accessed with a start-index out of range. This alarm can indicate that the start-index is pointing to an undefined location in the dial plan.

- Severity—Information

- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: BLoopCtrExceeded

This alarm occurs when the B-loop counter threshold is exceeded. It indicates that the B-number analysis function has gone into an infinite loop. The B-loop counter limits the number of passes through the analysis tree to 30.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: BTableFail_GetDigMod

This alarm occurs when a B-number failed to get a modification table. The alarm is caused by the modification table not being loaded or if a pointer to a nonexistent location in the modification table is given.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: BTableFail_GetDigTree

This alarm occurs when a B-table failed to get an analysis table. The alarm is caused by an invalid path being specified for B-number analysis or if the B-number analysis table is not loaded.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: BTableFail_GetResult

This alarm occurs when a B-table failed to get a result table during main analysis. The alarm is caused when a result table is not loaded or if a pointer is given to a nonexistent location in the result table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: BTableFlt_DgtRangeError

This alarm occurs when a B-Number analysis digit tree is accessed with an overdecadic digit.

- Severity—Critical

- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: BTableFlt_IdxRangeError

This alarm occurs when a B-number analysis digit tree is accessed with a start index out of range. It indicates that the start index is pointing to an undefined location in the dial plan.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Cause_GetFail_DigModTbl

This alarm occurs during cause analysis when a B-number modification result is encountered, and the digit modification string is unreadable. It is caused by a digit modification table being corrupted or an incorrect digit modification index being stored in the B-number modification result data.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Cause_GetFail_InvldRsltType

This alarm occurs during cause analysis when a result is encountered that is unsupported. It is caused by corruption of the cause or location tables or the result table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Cause_GetFail_LocTbl

This alarm occurs during cause analysis when the location table is unreadable. It can be due to the location table being corrupted, a failure in the underlying software, or the location table not being fully populated with all possible references from the cause table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Cause_GetFail_RsltTbl

This alarm occurs during cause analysis when the result table is unreadable. It can be due to the result table being corrupted, a failure in the underlying software, or the result table not being fully populated with all possible references from the cause and location tables.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Cause_MdfyBFail_AppPtInvld

This alarm occurs during cause analysis when a B-number modification result is encountered, and the specified application point (where digits are inserted) is beyond the end of the digit string. It is caused by an incorrect application point being specified in the result data, a corrupt result table, or incorrectly constructed cause analysis values.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Cause_Rte_Loop Detected

This alarm occurs during cause analysis when a route or announcement result is encountered. In these cases, the indicated route identifier is checked against a list of previously provided results. If a match is found, this alarm is raised and an error is returned to call processing. This is done to prevent calls from endlessly routing to a single route or series of routes infinitely due to cause analysis interactions.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: CustId/StartIdx Missing

This alarm occurs when a required property, customer ID number, or B-number origination start index number is not present on the originator. Both properties are required to find the correct place to begin analysis.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: DataBaseAccessFail

This alarm occurs when access to the on-board database (for example, for screening) fails. This alarm is set any time there is a database access failure, regardless of the query being made.

- Severity—Minor
- Cause—Access to the on-board database
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Data Failure Rcvd

This alarm occurs when an external data failure indication is received from the routing engine.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL:dpselection_table_fail

This alarm occurs when there is an error reading the dial plan selection table.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL:getDialplanBase_fail

This alarm occurs when the system fails to load or generate the dial plan.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: InvalidtrkGrpType

This alarm occurs when the analysis module has not provided a valid trunk group type. It is caused when the route analysis table specifies an invalid trunk group type.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: ISUP: T4 Expired

This alarm occurs when the system recieves a remote user unavailable indication in reponse to a message. The T4 timer is started and the message is sent again. When the T4 timer expires the second time, the message is not sent again.

- Severity—Information

- SNMP Trap Type—0 (No error, no trap)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_GetFail_CPCTbl

This alarm occurs when the generic analysis function is unable to read the calling party category (CPC) table.

- Severity—Information

- SNMP Trap Type—0 (No error, no trap)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_GetFail_DigModTbl

This alarm occurs during profile analysis when a B-number modification result is encountered, and the digit modification string is unreadable. It is caused by a corrupt digit modification table or by an incorrect digit modification index being stored in the B-number modification results data.

- Severity—Information

- SNMP Trap Type—0 (No error, no trap)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_GetFail_InvldRslt

This alarm occurs during profile analysis when a result is encountered that is not supporte. It is caused by a corrupt nature of address (NOA) table, numbering plan indicator (NPI) table, or result table.

- Severity—Information

- SNMP Trap Type—0 (No error, no trap)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_GetFail_NOATbl

This alarm occurs during profile analysis when the NOA table is unreadable. It is caused by a corrupt NOA table, a failure in the underlying software, or the NOA table being built without all the existing call context NOA values.

- Severity—Information

- SNMP Trap Type—0 (No error, no trap)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_GetFail_NOATbl_A

This alarm occurs during profile analysis when the A-number NOA table is unreadable. It is caused by a corrupt NOA table, a failure in the underlying software, or the NOA table being built without all the existing call context NOA values.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_GetFail_NPITbl

This alarm occurs during profile analysis when the NPI table is unreadable. It is caused by a corrupt NPI table, a failure in the underlying software, or the NPI table not being fully populated with all the possible references from the NOA table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_GetFail_NPITbl_A

This alarm occurs during profile analysis when the A-number NPI table is unreadable. It is caused by a corrupt NPI table, a failure in the underlying software, or the NPI table not being fully populated with all the possible references from the NOA table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_GetFail_RsltTbl

This alarm occurs during profile analysis when the result table is unreadable. This alarm can be due to the result table being corrupted, a failure in the underlying software, or the result table not being fully populated with all the possible references from the NOA or NPI tables.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL:Prof_GetFail_TMRTbl

This alarm occurs when the generic analysis function is unable to read the transmission medium requirements (TMR) table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)

• Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL:Prof_GetFail_TNSTbl

This alarm occurs when the generic analysis function is unable to read the calling transit network selection (TNS) table.

• Severity—Information

• SNMP Trap Type—0 (No error, no trap)

• Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_InvldNPAValue

This alarm occurs during profile analysis when a 7-digit B-number is encountered, and the numbering plan area (NPA) property is set against the originating trunk group. An NPA string must be 3 characters. This alarm is most likely caused by data corruption.

• Severity—Information

• SNMP Trap Type—0 (No error, no trap)

• Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_InvRslts_NOATbl

This alarm occurs during profile analysis when the value returned by the NOA table is logically invalid. It is caused by a failure of the underlying software or a corrupt NOA table.

• Severity—Information

• SNMP Trap Type—0 (No error, no trap)

• Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_InvRslts_NOATbl_A

This alarm occurs during profile analysis when the value returned by the A-number NOA table is logically invalid. It is caused by a failure of the underlying software or a corrupt NOA table.

• Severity—Information

• SNMP Trap Type—0 (No error, no trap)

• Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: Prof_MdfyBFail_AppPtInvld

This alarm occurs during profile analysis when a B-number modification result is encountered, and the specified application point (where digits are inserted) is beyond the end of the digit string. It is caused by an incorrect application point being specified in the result data, a corrupt result table, or incorrectly constructed profile analysis values.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: RedirectingNbrFail

This alarm occurs when a redirecting number is being used during A-number tree analysis, and a result type other than blacklist has been encountered. It indicates that screening by means of the A-digit tree has started with the redirecting number. The blacklist result type is not configured, so A-number analysis continues with the calling number bing used instead.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. Processing continues using the calling number.

ANAL: RteStartIndexInvalid

This alarm occurs when the route start index invalid.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: RteTableFail_GetRteList

This alarm occurs when the route table failes to get a route list. The alarm is caused when the index to the route list is not valid or if the route list is not loaded.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: RteTableFail_GetTrkAttrdata

This alarm occurs when the route table fails to get trunk group attribute data. The alarm is caused by the index to the trunk group attribute data table not being valid or the table not being loaded.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: RteTableFail_GetTrkGrpdata

This alarm occurs when the route table fails to get trunk group data. The alarm is caused by the index to the trunk group data not being valid or the trunk group data table not being loaded.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: RteTableFail_GetTrunkList

This alarm occurs when the route table fails to get trunk list. The alarm is caused by the index to the trunk group list not being valid or the trunk group list not being loaded.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL:Rte_TableHopCtrExceeded

This alarm occurs when the generic analysis function has encountered excessive analysis table hops.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: SerialCountExceeded

This alarm occurs when the serial intelligent network (IN) triggering counter exceeds its threshold. The call has been released, and there might be a loop in the local dial plan or remote SCP database.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—None required. This alarm is for informational purposes only.

ANAL:TableFail_BearerCapTable

This alarm occurs when the generic analysis function is unable to read the bearer capacity data table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL:TableFail_CondRouteDescTable

This alarm occurs when the generic analysis function is unable to read the conditional route description table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: TableFail_CondRouteTable

This alarm occurs when the system fails to read the conditional routing table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL:TableFail_CPCTable

This alarm occurs when the generic analysis function is unable to read the calling party category (CPC) table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL:TableFail_PercRouteTable

This alarm occurs when the generic analysis function is unable to read the percentage route table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: TableFail_RouteHolTable

This alarm occurs when the system fails to read the route holiday table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL:TableFail_TMRTable

This alarm occurs when the generic analysis function is unable to read the calling transmission medium requirements (TMR) table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL:TableFail_TNSTable

This alarm occurs when the generic analysis function is unable to read the calling transit network selection (TNS) table.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ANAL: TrunkGrpRsltCtrExceeded

This alarm occurs when a trunk group result counter exceeds its threshold. The analysis module has provided the maximum number of candidate trunk groups allowed (20). The purpose of the alarm is to limit the time spent searching for candidate trunk groups.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Association Degraded

This alarm occurs when a destination address of the association has failed, and the association is still in an UP state.

- Severity—Minor
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Association Fail

This alarm occurs when an SCTP association has failed. This alarm is reported when the destination node is out of service or there is an IP connectivity failure.

- Severity—Major
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Call Back feature insertion failure

This alarm occurs when an attempt to insert a call back feature entry in the main memory database fails. When this insertion fails, the call back feature does not work.

- Severity—Minor
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Call Back feature deletion failure

This alarm occurs when an attempt to delete a call back feature entry from the main memory database fails. When this deletion fails, the call back feature does not work.

- Severity—Minor
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

CHAN LINK ESTAB 15

This alarm occurs when number of resets on this channel (DS-0) for the last 15-minute period exceeds the alarm threshold value. The channel remains in an in-service state.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—This event is informational only and does not require an immediate response; however, the condition should be monitored closely so that the service level does not degrade further.

CHAN LINK ESTAB 24

This alarm occurs when number of resets on this channel (DS-0) for the last 24-hour period exceeds the alarm threshold value. The channel remains in an in-service state.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No immediate response is required; however, the condition should be monitored closely so that the service level does not degrade further.

CHAN LINK ESTAB 60

This alarm occurs when number of resets on this channel (DS-0) for the last 60-minute period exceeds the alarm threshold value. The channel remains in an in-service state.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—This event is informational only and does not require an immediate response; however, the condition should be monitored closely so that the service level does not degrade further.

Chkpt Synch Inprogress

This alarm occurs when an active and standby host synchronization process is in progress.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—This event does not require an immediate response.

Comm Srvc Creation Error

This alarm occurs when the system fails to create communication services.

- Severity—Minor
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

CONFIG_CHANGE

This alarm occurs when the running configuration is modified, indicating that a new configuration has been activated within a provisioning session.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required.

Config Fail

This alarm occurs when a signaling configuration has failed.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

CONFIGURATION_FAILURE

This alarm occurs when the H.323 configuration has failed. It indicates that a major error has occurred in the configuration of the H.323 software packages. This is a potentially nonrecoverable situation that requires an application restart.

- Severity—Major
- SNMP Trap Type—4 (Equipment error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

CPM: Leg1chanDeletedUnpackError

This alarm occurs when a fault is found in data received from the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

CPM: Leg1chanFailed

This alarm occurs when a resource failure occurs in the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg1chanModifiedUnpackError

This alarm occurs when a fault is found in data received from the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg1chanOpFailed

This alarm occurs when a resource failure occurs in the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg1chanSeizedUnpackError

This alarm occurs when a fault is found in data received from the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg1ConfigError

This alarm occurs when Inconsistent VirtualSwitch and oConPlaneCtrl are triggered. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)

- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg1DeleteChanPackError

This alarm occurs when required call context data was not available. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg1ModifyChanPackError

This alarm occurs when the required call context data was not available. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg1RQNTChanPackError

This alarm occurs when a call-context variable is not available. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg1SeizeChanPackError

This alarm occurs when required call context data was not available. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg1StateError

This alarm occurs when a requested action is incompatible with the CPM leg state. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg1Timeout

This alarm occurs when a response is not received from the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2chanDeletedUnpackError

This alarm occurs when a fault is found in data received from the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2chanFailed

This alarm occurs when there is a resource failure in the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2chanModifiedUnpackError

This alarm occurs when a fault is found in data received from the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2chanOpFailed

This alarm occurs when a resource failure occurs in the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2chanSeizedUnpackError

This alarm occurs when a fault is found in data received from the engine. It indicates an MDL source code issue.

- Severity—Information
- Cause—Indicates an MDL source code issue.
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2ConfigError

This alarm occurs when Inconsistent VirtualSwitch and oConPlaneCtrl are triggered. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2DeleteChanPackError

This alarm occurs when required call context data was not available. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2ModifyChanPackError

This alarm occurs when the required call context data was not available. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)

- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2RMXmitCotError

This alarm occurs when the parameter, RMXmitCot, is returned false. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2SeizeChanPackError

This alarm occurs when the required call context data was not available. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2SeizeConnectionPackError

This alarm occurs when the required call context data was not available. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2StateError

This alarm occurs when the requested action is incompatible with the CPM leg state. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: Leg2Timeout

This alarm occurs when a response is not received from the engine. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: NotifyUnexpected

This alarm occurs when an unsolicited chanNotify has been received. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: UnknownLeg

This alarm occurs when LCM has requested action, not Leg1 or Leg2. It indicates an MDL source code issue.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

CPM: UnknownNotifySNMP Trap Type

This alarm occurs when the ISDN User Part timer T28 has expired. It indicates that a chanNotify message with unknown notify type has been received.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. The Cisco TAC can use this information to troubleshoot call-processing problems.

Crash Information Collected

This alarm occurs when a process core-dumped and the core dump was saved. When a process exits and produces a core dump, this alarm indicates that the core file is saved for troubleshooting. The alarm has an associated component ID identifying the process that produced the core dump.

- Severity—Information

- SNMP Trap Type—3 (Processing error alarm)

- Action—No action is required. The Cisco TAC can use this information to troubleshoot the problem.

CTI connection failed

This alarm occurs when the CTI connection to the Cisco CallManager cluster has failed.

- Severity—Major

- SNMP Trap Type—1 (Communication alarm)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

CTI version mismatch

This alarm occurs when the CTI version of the CTI Manager component configured on Cisco EGW is not compatible with the version on the Cisco CallManager CTI Manager. Cisco EGW uses a CTI protocol to communicate with the Cisco CallManager CTI Manager. The CTI protocol version is checked during establishment of the CTI connection. The CTI connection cannot be established if the versions are not compatible.

- Severity—Minor

- SNMP Trap Type—1 (Communication alarm)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Dial Plan Loading Failed

This alarm occurs when the system fails to load a dial plan.

- Severity—Minor

- SNMP Trap Type—3 (Processing error alarm)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

DISK

This alarm occurs when there is a low amount of available disk space.

- Severity—Major

- SNMP Trap Type—4 (Equipment error alarm)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

EISUP_PATH_FAILURE

This alarm occurs when a failure of the RUDP layer has occurred, indicating that both IP links A and B to a single Cisco EGW have gone down.

- Severity—Major

- SNMP Trap Type—4 (Equipment error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ENDPOINT_CALL_CONTROL_INTERFACE_FAILURE

This alarm occurs when an individual call failure has occurred. This informational event is reported to the management interface and can be obtained with SNMP.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—This is an informational alarm only. No action is required.

ENDPOINT_CHANNEL_INTERFACE_FAILURE

This alarm occurs when an individual call failure has occurred.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—This is an informational alarm only. No action is required.

EQPT M-OOS

This alarm occurs when the equipment is taken manually out of service by a user.

- Severity—Major
- SNMP Trap Type—4 (Equipment error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

FAIL

This alarm occurs after a non-specific failure. It indicates that the referenced component has failed. The failure might affect service, and if it does, other alarms are raised.

- Severity—Minor
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

FailoverPeerLost

This alarm occurs when communication with failover peer is lost.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

FailoverPeerOOS

This alarm occurs when the failover peer is out of service.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

FailoverToInit

This alarm occurs when the failover daemon is in the initializing state.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—This is an informational alarm only. No action is required.

FailoverToMaster

This alarm occurs when the failover daemon is in the active state.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—This is an informational alarm only. No action is required.

FailoverToOOS

This alarm occurs when the failover daemon is out of service or when a response is not received from the process manager process.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

FailoverToSlave

This alarm occurs when the failover daemon is in standby state.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—This is an informational alarm only. No action is required.

FAIL REMOTE STANDBY

This alarm occurs when the standby Cisco EGW 2200 host fails to acknowledge synchronization messages from the active Cisco EGW 2200 host.

- Severity—Minor
- SNMP Trap Type—2 (Quality of service alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Force Node Restart

This alarm occurs on the standby host when a new data path is added dynamically. The standby host is restarted automatically; this alarm does not affect operations on the active host.

- Severity—Critical
- Cause—Generated only
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

GAPPED_CALL_NORMAL

This alarm occurs when a normal call is rejected due to call gapping.

- Severity—Information
- SNMP Trap Type—2 (Quality of service alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

GAPPED_CALL_PRIORITY

This alarm occurs when a priority or emergency call is rejected due to call gapping.

- Severity—Information
- SNMP Trap Type—2 (Quality of service alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Gateway Trunk Held

This alarm occurs when a gateway trunk is held without an associated call.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—No action required. The application clears itself through an automatic audit.

GENERAL PROCESS FAIL

This alarm occurs when the H.323 program quits unexpectedly. This alarm is cleared when the H.323 program is restarted.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

GEN FAIL

This alarm occurs when there is a general process failure. It is caused by resource exhaustion or configuration problems, including memory exhaustion, queue overflow, message congestion, an IPC file that cannot be opened, and timer expiration.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

H323:FAIL ORIG 15

This alarm occurs when the number of failed calls originating in H.323 exceeds the 15-minute (900 seconds) threshold.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

H323:FAIL ORIG 24

This alarm occurs when the number of failed calls originating in H.323 exceeds the 24-hour threshold.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

H323:FAIL ORIG 60

This alarm occurs when the number of failed calls originating in H.323 exceeds the 60 minute (3600 seconds) threshold.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

H323:FAIL TERM 15

This alarm occurs when the number of failed calls terminating in H.323 exceeds the 15-minute (900 seconds) threshold.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)

- Action—None required. This alarm is for informational purposes only.

H323:FAIL TERM 24

This alarm occurs when the number of failed calls terminating in H.323 exceeds the 24-hour threshold.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

H323:FAIL TERM 60

This alarm occurs when the number of failed calls terminating in H.323 exceeds the 60-minute (3600 seconds) threshold.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

H323_STACK_FAILURE

This alarm occurs when there is an irrecoverable failure in the H.323 stack. The H.323 stack has failed to correctly initialize on an application startup. An automatic application restart is initiated, and the application reverts to the base configuration data.

- Severity—Critical
- SNMP Trap Type—4 (Equipment error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Holiday Table Access Failure

This alarm occurs when the system failed to access the charge holiday table.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Holiday Table Load Failure

This alarm occurs when the system failed to load the holiday table.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW with Alarms.

Invalid Virtual_IP_Addr

This alarm occurs when the virtual IP address configured doesn't belong to the networks defined for the system.

- Severity—Major
- SNMP Trap Type—3 (Processing error)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

IP_LINK_FAILURE

This alarm occurs when one of the two IP links to a single Cisco EGW 2200 fails.

- Severity—Major
- SNMP Trap Type—4 (Equipment error)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

IP RTE CONF FAIL

This alarm occurs when an IP route is out of service due to a configuration failure.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

IP RTE FAIL

This alarm occurs when an IP route is out of service.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

LCM: Invalid destination for RO/PR routing number

This alarm occurs when the RO request routing number does not translate to a DPNSS trunk group. This alarm is reported by UCM when a RO or PR routing number fails to be translated by generic analysis into a destination that enables the feature to be performed.

- Severity—Minor
- SNMP Trap Type—2 (Quality of service alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

LCM: No Response from Call Instance

This alarm occurs when LCM has not received a message response within the expected time period.

- Severity—Minor
- SNMP Trap Type—2 (Quality of service alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW with Alarms.

LOW_DISK_SPACE

This alarm occurs when the disk space is low. The alarm automatically clears when the disk usage decreases below the alarm limit.

- Severity—Major
- SNMP Trap Type—4 (Equipment alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

MAJOR M-OOS

This alarm occurs when a software process necessary for normal system operation has been requested manually out of service by a user.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ManualSwitchOver

This alarm occurs when a user has initiated a manual switchover.

- Severity—Critical
- SNMP Trap Type—3 (Processing error alarm)
- Action—No action is necessary. The alarm clears once the switchover has completed.

MMDB: Database unavailable

This alarm occurs when the main memory database is currently unavailable to provide any services. Recovery is attempted, and the alarm clears when or if the database becomes available.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

MMDB: Database cause failover

This alarm occurs when the main memory database is unavailableon a redundant system. The system performs an automatic switchover and an attempt to recover the database is attempted. The alarm clears when the database becomes available.

- Severity—Critical
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

MMDB: Database nearly full

This alarm occurs when the main memory database detects that the allocated resources for data storage are nearly all utilized.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OLC: Leg1chanDeletedUnpackError

This alarm occurs when the system fails to parse a DLCX Acknowledgement message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OLC: Leg1chanModifiedUnpackError

This alarm occurs when the system fails to parse a MDCX Acknowledgement message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OLC: Leg1chanOpsFailed

This alarm occurs when an action fails due to the detection of an internal error or a gateway-related problem.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OLC: Leg1chanSeizedUnpackError

This alarm occurs when the system fails to parse a CRCX Acknowledgement message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OLC: Leg1deleteChanUnpackError

This alarm occurs when the system fails to parse a DLCX message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OLC: Leg1notifyRequestAckUnpackError

This alarm occurs when the system fails to parse a RQNT Acknowledgement message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OLC: Leg1notifyUnpackError

This alarm occurs when the system fails to parse a NTFY message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OOS TRAFFIC RE-ROUTE

This alarm occurs when traffic is rerouted by a far-end network element. It indicates that the traffic channels (bearer channels or the IP network) on one side of the Cisco EGW 2200 have been lost, causing the Cisco EGW 2200 to reroute traffic. The loss of traffic channels is generally due to a network or equipment failure but might be due to a provisioning failure.

- Severity—Minor
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OS

This alarm occurs when there is an operating system failure.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OverloadHeavy

This alarm occurs when an overload heavy condition exists. The call engine has reached a critical overload condition because it has too many protocol messages. An automatic switchover from active to standby host occurs. Calls are not processed unless this condition is corrected.

- Severity—Critical
- SNMP Trap Type—4 (Equipment error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OVERLOAD_LEVEL1

This alarm occurs when the CPU occupancy or the number of active calls rises above the upper limit set in the overload configuration for level 1. Gapping is then initiated.

- Severity—Information
- SNMP Trap Type—4 (Equipment error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OVERLOAD_LEVEL2

This alarm occurs when the CPU occupancy or the number of active calls rises above the upper limits set in the overload configuration for level 2. Gapping is then initiated. This alarm automatically clears when the CPU occupancy or the number of active calls drops below the lower limit set in the overload configuration for level 2.

- Severity—Minor
- SNMP Trap Type—4 (Equipment error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OVERLOAD_LEVEL3

This alarm occurs when the CPU occupancy or the number of active calls rises above the upper limits set in the overload configuration for level 3. Gapping is then initiated. This alarm automatically clears when the CPU occupancy or the number of active calls drops below the lower limit set in the overload configuration for level 3.

- Severity—Critical
- SNMP Trap Type—4 (Equipment error alarm)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OverloadLight

This alarm occurs when the call engine has reached a light overload condition because it has too many protocol messages. The condition should be corrected as soon as possible, but it does not cause an automatich switchover from the active to the standby host.

- Severity—Minor
- SNMP Trap Type—4 (Equipment error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

OverloadMedium

This alarm occurs when the call engine has reached a medium overload condition because it has too many protocol messages. The condition degrades performance and should be corrected as soon as possible, but it does not cause automatic switchover from the active to the standby host.

- Severity—Major
- SNMP Trap Type—4 (Equipment error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Peer IP Links Failure

This alarm occurs when the IP links to a peer Cisco EGW 2200 host have failed.

- Severity—Major
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

PEER LINK A FAILURE

This alarm occurs when the system fails to communicate with peer module over link A. This alarm is caused if the communication path between peer modules is lost or the peer module stops communicating.

- Severity—Minor
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

PEER LINK B FAILURE

This alarm occurs when the system fails to communicate with peer module over link B. This alarm is caused if the communication path between peer modules is lost or the peer module stops communicating.

- Severity—Minor
- SNMP Trap Type—1 (Communication alarm)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

PEER MODULE FAILURE

This alarm occurs when the system cannot communicate with a peer module over configured links.

- Severity—Major
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

POM: DynamicReconfiguration

This alarm is sent at the start of the dynamic reconfiguration procedure, and it is cleared once the procedure is successfully completed.

- Severity—Minor
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

POM INACTIVITY TIMEOUT

This alarm occurs when the system receives an inactivity timeout indication. The current provisioning session has not received any provisioning commands for 20 minutes. If there is still no activity within the next 5 minutes, the session is terminated.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

POM SESSION TERMINATE

This alarm occurs when a provisioning session is terminated. No further provisioning commands are accepted.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

PRI: B-Channel Not Available

This alarm occurs when the B-channel is not available. It indicates that the Cisco EGW 2200 has received a PRI setup message, and the requested B-channel is not available or cannot be allocated to the call.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

ProcM No Response

This alarm occurs when the process manager process does not respond to state information changes sent by the failover daemon.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

PROVISIONING_INACTIVITY_TIMEOUT

This alarm occurs when a provisioning session has been inactive for 20 minutes. The provisioning session will be closed if there is no activity within the next 5 minutes.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

PROVISIONING_SESSION_TIMEOUT

This alarm occurs when the current provisioning session has been terminate, due to the provisioning session being inactive for longer than the time allowed.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

REPL: all connections failure

This alarm occurs when all links to the peer Cisco EGW 2200 host have failed.

- Severity—Critical
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

RSET CONFIG FAIL

This alarm occurs when an attempt to reset your configuration failed. It indicates that the provisioning data for the route to a DPC has invalid or incompatible parameter values. This alarm is not generated due to a mismatch between the network topology and the DPC data.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)

- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

SC CONFIG FAIL

This alarm occurs when there is a signal channel configuration failure. It indicates that the provisioning parameters for the data link layer of a signaling channel are inconsistent or invalid. The signaling channel might already be provisioned. The configuration file might be corrupted and if it is, it cannot be read by the system.

- Severity—Major
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

SC FAIL

This alarm occurs when there is a signal channel failure. It indicates that the signaling channel is down and unable to process traffic. The channel cannot negotiate a D-channel session. Automatic restarts are not able to recover the session. The data link layer has failed.

- Severity—Major
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

SC M-OOS

This alarm occurs when a signal channel is manually taken out of service by a user.

- Severity—Minor
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

SIP: 400 XMIT TOT

This alarm occurs when alarm threshold for the number of bad messages received is reached.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

SIP: 405 RCV TOT

This alarm occurs when the Cisco EGW 2200 has received messages for methods that are not supported. A 405 response is sent for each 405 message received. The 405 message transmit counter has reached the set alarm threshold.

- Severity—Major

- SNMP Trap Type—3 (Processing error alarm)

- Action—None required. This alarm is for informational purposes only.

SIP: 406 RCV TOT

This alarm occurs when the Cisco EGW 2200 has received messages for methods that are not acceptable. A 406 response is sent for each 406 message received. The 406 message transmit counter has reached the set alarm threshold.

- Severity—Major

- SNMP Trap Type—3 (Processing error alarm)

- Action—None required. This alarm is for informational purposes only.

SIP: 411 MSG RCV

This alarm occurs when a LENGTH REQUIRED (411) message was received.

- Severity—Major

- SNMP Trap Type—3 (Processing error alarm)

- Action—None required. This alarm is for informational purposes only.

SIP: 481 RCV TOT

This alarm occurs when the Cisco EGW 2200 has received a series of CALL LEG/TRANSACTION DOES NOT EXIST (481) messages. The 481 received counter has reached the set alarm threshold.

- Severity—Major

- SNMP Trap Type—3 (Processing error alarm)

- Action—None required. This alarm is for informational purposes only.

SIP: 487 RCV TOT

This alarm occurs when the alarm threshold for the number of REQUEST CANCELLED RESPONSE RECEIVED (487) messages received is reached.

- Severity—Major

- SNMP Trap Type—3 (Processing error alarm)

- Action—None required. This alarm is for informational purposes only.

SIP: 501 MSG RCV

This alarm occurs when a NOT IMPLEMENTED (501) message is received.

- Severity—Major

- SNMP Trap Type—3 (Processing error alarm)

- Action—None required. This alarm is for informational purposes only.

SIP: 502 RCV TOT

This alarm occurs when the Cisco EGW 2200 has received a series of BAD GATEWAY (502) messages. The 502 received counter has reached the set alarm threshold.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

SIP: 504 RCV TOT

This alarm occurs when the Cisco EGW 2200 has received a series of GATEWAY TIMEOUT (504) messages. The 504 received counter has reached the set alarm threshold.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

SIP: 504 XMIT TOT

This alarm occurs when the Cisco EGW 2200 has transmitted a series of GATEWAY TIMEOUT (504) messages. The 504 transmit counter has reached the set alarm threshold.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

SIP: 505 MSG RCV

This alarm occurs when a VERSION NOT SUPPORTED (505) message is received.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

SIP: 505 MSG XMIT

This alarm occurs whenthe Cisco EGW 2200 has transmitted a series of VERSION NOT SUPPORTED (505) messages. The 505 received counter has reached the set alarm threshold.

- Severity—Major
- Cause—T
- SNMP Trap Type—3 (Processing error alarm)

- Action—None required. This alarm is for informational purposes only.

SIP: 603 RCV TOT

This alarm occurs when the Cisco EGW 2200 has received a series of REQUEST DECLINED (603) messages. The 603 received counter has reached the set alarm threshold.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

SIP: 606 RCV TOT

This alarm occurs when the Cisco EGW 2200 has received a series of NOT ACCEPTABLE (606) messages. The 606 received counter has reached the set alarm threshold.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

SIP: DNS CACHE NEARLY FULL

This alarm occurs when the DNS cache is nearly full.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW with Alarms.

SIP: DNS SERVICE OOS

This alarm occurs when the DNS servers are not responding or access to the servers has been lost.

- Severity—Major
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW with Alarms.

SIP: INVALID MSG RCV

This alarm occurs when an invalid SIP message has been received.

- Severity—Minor
- SNMP Trap Type—3 (Processing error alarm)
- Action—None required. This alarm is for informational purposes only.

SIP: OOS

This alarm occurs when the IP link used by SIP is out of service.

- Severity—Major
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

SIP: RE-XMIT MSG TOT

This alarm occurs when the alarm threshold for the number of SIP message retransmissions is exceeded.

- Severity—Major
- SNMP Trap Type—2 (Quality of service error alarm)
- Action—None required. This alarm is for informational purposes only.

SIP Service Fail Over

This alarm occurs when the virtual addresses for the Cisco EGW 2200 cannot be reached due to failure of the associated LAN/WAN interfaces. This alarm is cleared automatically when the LAN/WAN interfaces are ready for traffic again.

- Severity—Critical
- SNMP Trap Type—1 (Communication error)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

SOFTW NON

This alarm occurs when there is a nonrequired process failure. The process is not necessary for normal operation of the system; however, failure of nonrequired software might reduce the reliability or performance of the system.

- Severity—Minor
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

SOFTW REQ

This alarm occurs when there is a required process failure. The process provides a necessary service on the Cisco EGW 2200 that is not related to call processing.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Standby Warm Start

This alarm occurs when a warm start is initiated. This message can also be displayed by the standby host after a synchronization of host data is requested.

- Severity—Minor
- SNMP Trap Type—3 (Processing error alarm)
- Action—No action required.

SUPPORT FAILED

This alarm occurs when a supporting entity fails. The supporting entity can be hardware, such as a disk or line card or software, such as an application process.

- Severity—Minor
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

SW FAIL

This alarm occurs when there is a software failure. It indicates software logic problems, such as an unknown message received, a process in undesirable state, unexpected logic being executed (for example, conditional code that should never be executed is being executed), and some timer expirations.

- Severity—Information
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

SwitchoverFail

This alarm occurs when your system fails to switch network interfaces to active system.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

TLC: Leg2chanDeletedUnpackError

This alrm occurs when the system fails to parse a DLCX Acknowledgement message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

TLC: Leg2chanModifiedUnpackError

This alrm occurs when the system fails to parse a MDCX Acknowledgement message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

TLC: Leg2chanOpFailed

This alarm occurs when a TLC action fails due to an internal error or gateway-related problem.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

TLC: Leg2chanSeizedUnpackError

This alrm occurs when the system fails to parse a CRCX Acknowledgement message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

TLC: Leg2deleteChanUnpackError

This alrm occurs when the system fails to parse a DLCX Acknowledgement message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

TLC: Leg2notifyRequestAckUnpackError

This alarm occurs when the system fails to parse a RQNT Acknowledgement message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

TLC: Leg2notifyUnpackError

This alrm occurs when the system fails to parse a NTFY Acknowledgement message received from the gateway.

- Severity—Major
- SNMP Trap Type—3 (Processing error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

UCM: CCodeModFailed

This alarm occurs when a trunk group country code prefix is required and has not been correctly applied.

- Severity—Major
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

UCM: MGCPDIALAuthFail

This alarm occurs when UCM has automatically switched over and did not receive a Notify message from the media gateway within a 1-minute time period. The call has been torn down.

- Severity—Information
- SNMP Trap Type—0 (No error, no trap)
- Action—No action is required. Processing will continue using the calling number.

Virtual_IP_Addr Mismatch

This alarm occurs when the virtual IP addresses configured on the active and standby Cisco EGW 2200s do not match.

- Severity—Major
- SNMP Trap Type—3 (Processing error)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

VSC_FAILURE

This alarm occurs when links to the active and standby Cisco EGW 2200s have failed.

- Severity—Major
- SNMP Trap Type—0 (No error, no trap)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

Wrong IP Path

This alarm occurs when the IP route or local interface provisioned for the specified component is not being used. This alarm is reported when generic analysis cannot access the conditional route description table.

A route has been overridden by another route in the operating system routing table or a route added by the Cisco EGW 2200 has been manually removed from this table with operating system route delete command. This alarm can also occur if an IP signaling channel has been misconfigured.

- Severity—Minor
- SNMP Trap Type—1 (Communication alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.

XE Rsrc Fail

This alarm occurs when there is a resource failure.

- Severity—Information
- SNMP Trap Type—4 (Equipment error alarm)
- Action—Refer to the procedure for this alarm in Troubleshooting the Cisco EGW 2200 with Alarms.