Troubleshooting the Cisco EGW 2200 with Alarms

This section contains procedures for the Cisco EGW 2200 alarms that require you to perform specific corrective actions.You can find a complete list of the alarms in Cisco EGW 2200 Alarms.

Alarm Troubleshooting Information

Corrective actions for Cisco EGW 2200 alarms are listed below.

All Conn Cntl Links Fail

This alarm occurs when the all of the MGCP IP links fail.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the Ethernet interfaces between the Cisco EGW 2200 and the associated media gateway are working properly.

You can determine the status of the Ethernet interfaces on the Cisco EGW 2200 using the Cisco IPT Platform Administration application. Refer to the online help topic for this subject for more information. You can find information on verifying the proper functioning of an Ethernet interface on the media gateway in the associated documentation.

If the Ethernet connections are working correctly, proceed to Step 4. Otherwise, proceed to Step 3.

Step 3 If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Once the replacement is complete, return to Step 2.

Information on removing and replacing an Ethernet interface card on either platform can be found in the documentation that came with the platform.

Cisco Systems

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Step 4 Verify that the MGCP sessions are operating normally. Refer to the documentation for the affected media gateway for more information on verifying the functioning of the MGCP sessions.

If the MGCP sessions are not operating normally, return the MGCP sessions to normal operations, as described in the documentation for the affected media gateway. Otherwise, proceed to Step 5.

Step 5 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

All ISDN IP Conn Fail

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

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the affected media gateways are operating normally, as described in the associated documentation.

Step 3 Verify that the Ethernet interfaces between the Cisco EGW 2200 and the associated media gateway are working properly.

You can determine the status of the Ethernet interfaces on the Cisco EGW 2200 using the Cisco IPT Platform Administration application. Refer to the online help topic for this subject for more information. You can find information on verifying the proper functioning of an Ethernet interface on the media gateway in the associated documentation.

If the Ethernet connections are working correctly, proceed to Step 5. Otherwise, proceed to Step 4.

Step 4 If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Once the replacement is complete, return to Step 2.

Information on removing and replacing an Ethernet interface card on either platform can be found in the documentation that came with the platform.

Step 5 Verify that the configuration for your system is correct. To verify the provisioning data for your Cisco EGW 2200, use the Cisco EGW Administration application, as described in the Cisco EGW Administration online help. To verify the provisioning data for the media gateways, use show commands, as described in the associated documentation.

If your system configuration is incorrect, modify the configuration data. Refer to the Cisco EGW Administration online help for information on modifying Cisco EGW 2200 data. Refer to the documentation associated with the media gateway for more information on modifying the media gateway configuration data.

If the configuration of the Cisco EGW 2200 and the media gateways are correct, proceed to Step 6.

Step 6 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

ANAL: ALoopCtrExceeded

This alarm occurs when an A-number analysis operation has gone into an infinite loop. The purpose of the alarm is to limit the number of passes spent in the analysis tree to 30.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: ATableFail_GetDigMod

This alarm occurs when a retrieval of a modification string failed during A-number analysis. The problem occurs when the modification table is not loaded or a pointer to a nonexistent location in the modification table is given.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: ATableFail_GetResult

This alarm occurs when access to the result table failed during A-number analysis. The problem occurs if the result table is not loaded or a pointer to a nonexistent location in the result table is given.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: ATableFlt_DgtRangeError

This alarm occurs when the A-number analysis digit tree has been accessed with a digit that is out of range for the digit tree table. This alarm could occur if the system was incorrectly configured to support a base 10 dial plan, and an overdecadic digit was received from the line and passed to analysis.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: BLoopCtrExceeded

The alarm occurs when a B-number analysis operation has gone into an infinite loop. The purpose of the alarm is to limit the number of passes spent in the analysis tree to 30.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: BTableFail_GetDigMod

This alarm occurs when retrieval of a modification string failed during B-number analysis. The problem occurs if the modification table is not loaded or a pointer to a nonexistent location in the modification table is given.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: BTableFail_GetDigTree

This alarm occurs when an invalid path for B-number analysis has been given or that the B-number analysis table is not loaded. The problem occurs when an invalid path has been specified for B-number analysis or the B-number analysis table is not loaded.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: BTableFail_GetResult

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

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: BTableFlt_DgtRangeError

This alarm occurs when the B-number analysis digit tree is accessed with an overdecadic digit.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: BTableFlt_IdxRangeError

This alarm occurs when the 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.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

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. This can be due to the digit modification table being corrupted or an incorrect digit modification index being stored in the B-number modification result's data.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Cause_GetFail_InvldRsltType

This alarm occurs during cause analysis when a result is encountered that is not supported in cause analysis. This is due to corruption of the cause or location tables or the result table.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL:Cause_GetFail_LocTbl

This alarm occurs during cause analysis when the location table is unreadable. This 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.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL:Cause_GetFail_RsltTbl

This alarm occurs during cause analysis when the result table is unreadable. This 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.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL:Cause_InvldRslts_CauseTbl

This alarm occurs when cause analysis successfully reads the cause table but the value returned is logically invalid. Cause analysis gets two values from the cause table: an immediate result index and a location index. The immediate result index indicates that analysis should start reading results now, but the location index indicates that another table read is required to find the correct result table index. These results are logically incompatible. Most likely this results from a failure of the underlying software or a corruption of the cause table.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Cause_MdfyBFail_AppPtInvld

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

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Cause_Rte_LoopDetected

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.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: CustId/StartIdx Missing

This alarm occurs when a customer group identification number is not present on the identified trunk group. This is required to find the correct place to begin analysis.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Determine the value of the customer group identification number for the associated trunk group. Refer to the Cisco EGW Administration online help topic for this subject for more information.

Step 2 If the affected trunk group does not have a customer group identification number, or the number is incorrect, modify the trunk group by adding a new customer group identification number. Refer to the Cisco EGW Administration online help topic for this subject for more information.

ANAL:DataBaseAccessFail

This alarm occurs when access to the MMDB has failed. It is set any time there is a database access failure, regardless of the query being made.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Data Failure Rcvd

This alarm occurs when during analysis, a data failure is found in the external routing engine.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL:dpselection_table_fail

This alarm occurs when the correct dial plan selection could not be determined.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL:getDialplanBase_fail

This alarm occurs when the Cisco EGW 2200 could not load or generate the dial plan.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: InvalidtrkGrpType

This alarm occurs when the analysis module has not provided a valid trunk group type. The problem occurs if the route analysis table specifies an invalid trunk group type.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: ISUP: T4 Expired

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

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_GetFail_CPCTbl

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

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

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. This can be due to the digit modification table being corrupted or an incorrect digit modification index being stored in the B-number modification result's data.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_GetFail_InvldRslt

This alarm occurs during profile analysis when a result is encountered that is not supported in profile analysis. This is due to corruption of either the NOA or NPI tables or the result table.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_GetFail_NOATbl

This alarm occurs during profile analysis when the NOA table is unreadable. This can be due to the NOA table being corrupted, a failure in the underlying software, or the NOA table being built without all the existing call context NOA values.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_GetFail_NOATbl_A

This alarm occurs during profile analysis when the A-number NOA table is unreadable. This can be due to the NOA table being corrupted, a failure in the underlying software, or the NOA table being built without all the existing call context NOA values.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_GetFail_NPITbl

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

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_GetFail_NPITbl_A

This alarm occurs during profile analysis when the A-number NPI table is unreadable. This can be due either to the NOA table being corrupted, or to a failure in the underlying software.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_GetFail_RsltTbl

This alarm occurs during profile analysis when the result table is unreadable. This 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.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_GetFail_TMRTbl

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

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_GetFail_TNSTbl

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

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_InvldNPAValue

This alarm occurs during profile analysis when a 7-digit B-number is encountered and the NPA property is set against the originating trunk group. An NPA string of more or less than 3 characters is invalid. This is most likely caused by data corruption.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_InvRslts_NOATbl

This alarm occurs when the value returned by the NOA table is logically invalid. It results from a failure of the underlying software or a corrupt NOA table.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Prof_InvRslts_NOATbl_A

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

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

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. This is caused by an incorrect application point being specified in the result data, a corrupt result table, or incorrectly constructed Profile analysis values.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: RteStartIndexInvalid

This alarm occurs when the start index for the route analysis table is invalid.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: RteTableFail_GetRteList

This alarm occurs when access to the route list failed. The problem occurs if the index to the route list is not valid or if the route list is not loaded.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: RteTableFail_GetTrkAttrdata

This alarm occurs when access to the trunk group attribute data table failed. The problem occurs if the index to the trunk group attribute data table is not valid or if the table is not loaded.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: RteTableFail_GetTrkGrpdata

This alarm occurs when access to the trunk group data failed. The problem occurs if the index to the trunk group data is not valid or if the trunk group data table is not loaded.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: RteTableFail_GetTrunkList

This alarm occurs when access to the trunk group list failed. The problem occurs if the index to the trunk group list is not valid or if the trunk group list is not loaded.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: Rte_TableHopCtrExceeded

This alarm occurs when generic analysis fails due to excessive number of routing table changes.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: TableFail_BearerCapTable

This alarm occurs when the bearer capability table could not be read during generic analysis.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: TableFail_CondRouteDescTable

This alarm occurs when the conditional route description table could not be read during generic analysis.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: TableFail_CondRouteTable

This alarm occurs when the conditional routing table could not be read during generic analysis.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: TableFail_CPCTable

This alarm occurs when the calling party category (CPC) table could not be read during generic analysis.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: TableFail_PercRouteTable

This alarm occurs when the percentage route holiday table could not be read during generic analysis.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: TableFail_RouteHolTable

This alarm occurs when route holiday table could not be read during generic analysis.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: TableFail_TMRTable

This alarm occurs when the transmission medium requirements (TMR) table could not be read during generic analysis.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: TableFail_TNSTable

This alarm occurs when the transit network selection (TNS) table could not be read during generic analysis.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

ANAL: TrunkGrpRsltCtrExceeded

This alarm occurs when the analysis module has provided the maximum number of candidate trunk groups allowed. The maximum number is 20. The purpose of the alarm is to limit the time spent searching for candidate trunk groups.

Corrective Action

Resolve this dial plan alarm using the procedure in Resolving a Dial Plan Alarm.

Association Degraded

This alarm occurs when one of the destination addresses for an SCTP association has failed, but the association is still in-service (IS).

Corrective Action

To correct the problem identified by this alarm, perform the procedure in Resolving an Association Alarm.

Association Fail

This alarm occurs when an SCTP association has failed due to an IP connectivity failure or an out-of-service (OOS) destination.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the Resolving an Association Alarm.

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.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

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.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

Comm Srvc Creation Error

This alarm occurs when an error occurred while creating or opening a communication service.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

Config Fail

This alarm occurs when the configuration has failed.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

CONFIGURATION_FAILURE

This alarm occurs when 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.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

CTI connection failed

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

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the Ethernet interfaces between the Cisco EGW 2200 and the Cisco CallManager cluster are working properly.

You can determine the status of the Ethernet interfaces on the Cisco EGW 2200 using the Cisco IPT Platform Administration application. Refer to the on-line help topic for this subject for more information. You can find information on verifying the proper functioning of an Ethernet interface on the Cisco CallManager cluster in the associated documentation.

If the Ethernet connections are working correctly, proceed to Step 4. Otherwise, proceed to Step 3.

Step 3 If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Once the replacement is complete, return to Step 2.

Information on removing and replacing an Ethernet interface card on either platform can be found in the documentation that came with the platform.

Step 4 Verify that the MGCP sessions are operating normally. Refer to the documentation for the affected media gateway for more information on verifying the functioning of the MGCP sessions.

If the MGCP sessions are not operating normally, return the MGCP sessions to normal operations, as described in the documentation for the affected Cisco CallManger cluster. Otherwise, proceed to Step 5.

Step 5 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

CTI version mismatch

This alarm occurs when the CTI version of the CTI Manager component configured on Cisco EGW 2200 is not compatible with the version on the CTI Manager.

Corrective Action

Check the version of CTI Manager and install appropriate patches on the Cisco EGW 2200 to make it compatible with the version on CTI Manager.

Dial Plan Loading Failed

This alarm occurs when a dial plan has not loaded properly.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

DISK

This alarm occurs when the system disk is running out of space.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

EISUP_PATH_FAILURE

This alarm occurs when a failure of the RUDP layer occurs, indicating that both IP links A and B to single Cisco EGW 2200 have gone down.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

EQPT M-OOS

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

Corrective Action

To correct the problem identified by this alarm, restore the identified equipment to the in-service state.

FAIL

This alarm occurs when the component referenced in the alarm has failed. The failure may be service affecting, in which case other alarms are raised.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

FailoverPeerLost

This alarm occurs when the failover daemon on the standby Cisco EGW 2200 is not reachable.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the Ethernet interfaces between the active and standby Cisco EGW 2200s and the Cisco switches are working properly.

Note Information on verifying the proper operation of an Ethernet interface on the Cisco EGW 2200 host can be found in the Cisco IPT Platform Administration application online help. Information on verifying the proper functioning of an Ethernet interface on the Cisco switches can be found in the documentation for your switch.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 3.

Note Information on removing and replacing an Ethernet interface card on the Cisco EGW 2200 host can be found in the Cisco IPT Platform Administration application online help. Information on removing and replacing an Ethernet interface card on the Cisco switch can be found in the documentation for your switch.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

FailoverPeerOOS

This alarm occurs when the failover daemon goes out-of-service in the standby Cisco EGW 2200.

Corrective Action

To correct the problem identified by this alarm, check the alarms on the standby Cisco EGW 2200 and resolve those alarms.

FAIL REMOTE STANDBY

This alarm occurs on the active Cisco EGW 2200 when a synchronization operation between the active and standby Cisco EGW 2200 fails. This alarm is automatically cleared if a successful synchronization operation occurs after the failure. As a result, the Standby Warm Start alarm is triggered. Refer to Standby Warm Start for more information.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the standby Cisco EGW 2200 is in the standby platform state. Refer to the Cisco EGW Administration online help for more information.

If the standby Cisco EGW 2200 is in the standby platform state, proceed to Step 3. Otherwise, proceed to Step 4.

Step 3 Synchronize the standby Cisco EGW 2200 with the active Cisco EGW 2200. Refer to the Cisco EGW Administration online help for more information.

Step 4 Restart the Cisco EGW 2200 software on your standby Cisco EGW 2200. Refer to the Cisco EGW Administration online help for more information.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 5.

Step 5 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

GAPPED_CALL_NORMAL

This alarm occurs when gapping levels cause a normal call to be rejected.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

GAPPED_CALL_PRIORITY

This alarm occurs when gapping levels cause a priority or emergency call to be rejected.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

Gen Fail

This alarm occurs when a failure has occurred due to resource exhaustion or configuration problems, including:

- Memory exhaustion.
- Queue overflow.
- Message congestion.
- IPC file cannot be opened.
- A timer has expired.

Log messages in the active system log file indicate the nature of the failure.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

GENERAL_PROCESS_FAILURE

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

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

H323_STACK_FAILURE

This alarm occurs when 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.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

Holiday Table Access Failure

This alarm occurs when the Cisco EGW 2200 could not access the holiday table.

Corrective Action

To correct the problem identified by this alarm, check for the presence of the Holiday Table Load Failure alarm. If this alarm is present, perform the corrective action for that alarm. Otherwise, the procedure is complete.

Holiday Table Load Failure

This alarm occurs when a Cisco EGW 2200 process is unable to load the holiday table.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

Invalid Virtual_IP_Addr

This alarm occurs when the configured virtual IP address is not part of the networks associated with the IP addresses set for the Cisco EGW 2200.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

IP_LINK_FAILURE

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

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the Ethernet interfaces between the Cisco EGW 2200 and the associated media gateway are working properly.

You can determine the status of the Ethernet interfaces on the Cisco EGW 2200 using the Cisco IPT Platform Administration application. Refer to the online help topic for this subject for more information. You can find information on verifying the proper functioning of an Ethernet interface on the media gateway in the associated documentation.

If the Ethernet connections are working correctly, proceed to Step 4. Otherwise, proceed to Step 3.

Step 3 If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Once the replacement is complete, return to Step 2.

Information on removing and replacing an Ethernet interface card on the Cisco EGW 2200 can be found in the Cisco IPT Platform Administration applicationonline help. Information on removing and replacing an Ethernet interface card on a media gateway can be found in the associated documentation.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

IP RTE CONF FAIL

This alarm occurs when an IP route cannot access the local interface defined by its IP address parameter.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the Ethernet interfaces between the Cisco EGW 2200 and the associated media gateway are working properly.

You can determine the status of the Ethernet interfaces on the Cisco EGW 2200 using the Cisco IPT Platform Administration application. Refer to the online help topic for this subject for more information. You can find information on verifying the proper functioning of an Ethernet interface on the media gateway in the associated documentation.

If the Ethernet connections are working correctly, proceed to Step 4. Otherwise, proceed to Step 3.

Step 3 If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Once the replacement is complete, return to Step 2.

Information on removing and replacing an Ethernet interface card on the Cisco EGW 2200 can be found in the Cisco IPT Platform Administration applicationonline help. Information on removing and replacing an Ethernet interface card on a media gateway can be found in the associated documentation.

Step 4 Check the media gateway associated with the IP route to determine whether redirect messages are being sent to the Cisco EGW 2200. These messages would indicate that a new router was added to the data path.

If redirect messages are *not* being sent to the Cisco EGW 2200, proceed to Step 5. Otherwise, modify the configuration of the affected IP route to include the IP address of the new router.

Step 5 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

IP RTE FAIL

This alarm occurs when an IP route is in the OOS state with a cause other than off-duty or commanded out-of-service.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the configuration of the affected IP route is correct. Refer to the Cisco EGW Administration online help for more information on this subject.

If the configuration is correct, proceed to Step 4. Otherwise, proceed to Step 3.

Step 3 Correct the configuration of the affected IP route. Refer to the Cisco EGW Administration online help for more information on this subject.

If the alarm clears automatically, the procedure is complete. Otherwise, proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

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.

Corrective Action

To correct the problem identified by this alarm, you should verify that the dial plans associated with the DPNSS incoming trunk group match up with the routing numbers in the PBX network.

If the dial plans are correct, contact the Cisco TAC to further analyze the problem and determine a solution. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

LCM: No Response from Call Instance

This alarm occurs when LCM has not received a message response within the expected time period. This alarm is reported by UCM when a keep-alive message or some other call processing message has not received a response.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

If there are multiple occurances of this alarm (more than once per day), you should disable RO/PR and escalate the problem with the Cisco TAC.

LOW_DISK_SPACE

This alarm occurs when the percentage of disk usage is greater than the alarm limit.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

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.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

MMDB: Database cause failover

This alarm occurs when the main memory database is currently unavailable on a redundant system and is indicating that the system should failover. Recovery is attempted and the alarm clears when or if the database becomes available.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

MMDB: Database nearly full

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

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

OLC: Leg1chanDeletedUnpackError

This alarm occurs when a Delete Channel (DLCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

OLC: Leg1chanModifiedUnpackError

This alarm occurs when an Modify Channel (MDCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

OLC: Leg1chanOpsFailed

This alarm occurs when the Cisco EGW 2200 has detected an internal error or a media gateway related problem.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

OLC: Leg1chanSeizedUnpackError

This alarm occurs when an Seized Channel (CRCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

OLC: Leg1deleteChanUnpackError

This alarm occurs when a Delete Channel (DLCX) message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

OLC: Leg1notifyRequestAckUnpackError

This alarm occurs when an Request Notify (RQNT) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

OLC: Leg1notifyUnpackError

This alarm occurs when a Notify (NTFY) message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

OOS TRAFFIC RE-ROUTE

This alarm occurs when the traffic channels (bearer channels, IP network) on one side of the Cisco EGW 2200 have been lost, causing the Cisco EGW 2200 to reroute channels away from the affected component. This is generally due to a network or equipment failure, but might be due to a provisioning failure.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Other alarms associated with the affected component should also be displayed. Resolve those alarms first.

If resolving those alarms does not clear this alarm, proceed to Step 3.

Step 3 Verify that the configuration settings for the Cisco EGW 2200 and the affected media gateway are correct.

If your system configuration is incorrect, modify the configuration data for your system. Refer to the Cisco EGW Administration online help for information on modifying a Cisco EGW configuration. Refer to the documentation for the media gateway for more information on modifying its configuration.

If the configuration of both the Cisco EGW 2200 and the affected media gateway are correct, then proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

OS

This alarm occurs when there is an operating system failure.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

OverloadHeavy

This alarm occurs when the system has reached the threshold for overload level 3. The system performs an automatic switchover operation. If the call rejection percentage setting for overload level 3 is unchanged from its default value, all new calls are rejected until the abate threshold for overload level 3 is reached. This alarm is automatically cleared at that time.

Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the Cisco EGW Administration online help and re-route some of your traffic.

Note This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session.

OVERLOAD_LEVEL1

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 1. Gapping is then initiated.

Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the Cisco EGW Administration online help and re-route some of your traffic.

Note This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session.

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.

Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the Cisco EGW Administration online help and re-route some of your traffic.

Note This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session.

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.

Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the Cisco EGW Administration online help and re-route some of your traffic.

Note This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session.

OverloadLight

This alarm occurs when the system has reached the threshold for overload level 1. A percentage of new calls, based on the call rejection percentage setting for overload level 1, are rejected until the abate threshold for overload level 1 is reached.

Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the Cisco EGW Administration online help and re-route some of your traffic.

Note This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session.

OverloadMedium

This alarm occurs when the system has reached the threshold for overload level 2. A percentage of new calls, based on the call rejection percentage setting for overload level 2, are rejected until the abate threshold for overload level 2 is reached. This alarm is automatically cleared at that time.

Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the Cisco EGW Administration online help and re-route some of your traffic.

Note This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session.

Peer IP Links Failure

This alarm occurs when the IP links to the peer Cisco EGW 2200 are removed or down.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the Ethernet interfaces for the active and standby Cisco EGW 2200s are working properly. Refer to the Cisco EGW Administration online help system for more information.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

PEER LINK A FAILURE

This alarm occurs either because a communication path between peer modules was lost or a peer module has stopped communicating.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in Resolving a Failed Connection to a Peer.

PEER LINK B FAILURE

This alarm occurs either because a communication path between peer modules was lost or a peer module has stopped communicating.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in Resolving a Failed Connection to a Peer.

PEER MODULE FAILURE

This alarm occurs when communications to a peer module are lost, indicating failure.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in Resolving a Failed Connection to a Peer.

POM: DynamicReconfiguration

This alarm occurs when a dynamic reconfiguration procedure is started. It is cleared once the dynamic reconfiguration is successfully completed.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

POM INACTIVITY TIMEOUT

This alarm occurs when the current provisioning session had been idle for 20 minutes without input any provisioning commands. If there is still no provisioning activity within the next five minutes, the session is terminated.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

POM SESSION TERMINATE

This alarm occurs when a provisioning session is terminated. Any additional provisioning commands are not accepted.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

PRI: B-Channel not available

This alarm occurs when 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.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

ProcM No Response

The process manager is not responding to state information changes from the failover daemon.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

PROVISIONING_INACTIVITY_TIMEOUT

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

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

PROVISIONING_SESSION_TIMEOUT

This alarm occurs when the provisioning session has been inactive for longer than the time allowed.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

REPL: all connections failure

This alarm occurs when the Cisco EGW 2200 cannot establish communication to the peer Cisco EGW 2200.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the Ethernet interfaces for the Cisco EGW 2200s are working properly. Refer to the Cisco EGW Administration online help system for more information.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 3.

Note Information on removing and replacing an Ethernet interface card on the Cisco EGW 2200 host can be found in the documentation that came with your system.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

SC CONFIG FAIL

This alarm occurs when the provisioning parameters for the data link layer of a signaling channel are inconsistent or invalid. The signaling channel may already be provisioned. The configuration file might be corrupted and cannot be read by the system.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Place the affected signaling channel in the out-of-service state. Refer to the Cisco EGW Administration online help system for more information.

Step 3 Remove the affected signaling channel from your configuration. Refer to the Cisco EGW Administration online help system for more information.

Step 4 Referring to your local provisioning parameters, re-provision the signaling channel. Refer to the Cisco EGW Administration online help system for more information.

Step 5 Place the signaling channel in the in-service state. Refer to the Cisco EGW Administration online help system for more information.

If that does not resolve the problem, proceed to Step 6.

Step 6 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

SC FAIL

This alarm occurs when the signaling channel is down and unable to process traffic. As a result, the signaling channel is failing to negotiate a D-channel session, automatic restarts are not able to recover the session, and the data link-layer has failed. This can occur when SS7 SLTM/SLTA fails or when a PRI D-channel fails.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Ensure that the near-end and far-end data link terminations are operating.

If the near-end or far-end data link terminations are not operating, fix as necessary.

If the near-end and far-end data link terminations are operating, proceed to Step 3.

Step 3 Ensure that the provisioning settings for the signaling channel match the settings used on the far-end.

If the configuration data for the signaling channel is incorrect, modify your configuration. Refer to the Cisco EGW Administration online help system for more information.

If the configuration data for the signaling channel is correct, then proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

SC M-OOS

This alarm occurs when a signaling channel has been manually taken out of service.

Corrective Action

To correct the problem identified by this alarm, restore the affected signaling channel to the in-service state, using the appropriate procedure.

SIP: DNS CACHE NEARLY FULL

This alarm occurs when the domain name service (DNS) cache is nearly full.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

SIP: DNS SERVICE OOS

This alarm occurs when the DNS servers are not responding to queries. The DNS servers may be out of service or the access to them is lost.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

SIP: OOS

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

Corrective Action

To correct the problem identified by this alarm, attempt to restore the IP link to service. Refer to the Cisco EGW Administration online help system for more information.

SIP Service Fail Over

This alarm is caused by the failure of switch interfaces, due to either physical failure or administrative shut down.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Determine whether the failure is caused by a physical failure or an administrative shutdown.

If the failure is caused by a physical failure, proceed to Step 3.

If the failure is caused by an administrative shutdown, check for this alarm again once the interface has been restored. If this alarm is still active, proceed to Step 4.

Step 3 Verify that the switch interfaces between the Cisco EGW 2200 and the affected SIP element are working properly.

Note Information on verifying the proper operation of a switch interface on the Cisco EGW 2200 host can be found in the documentation that came with your system. Information on verifying the proper functioning of a switch interface on other devices can be found in the user documentation that came with that device.

If an element of the switch connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 4.

Note Information on removing and replacing an Ethernet interface card on the Cisco EGW 2200 host can be found in the documentation that came with your system. Information on removing and replacing components on other devices can be found in the user documentation that came with that device.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

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.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

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.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

Standby Warm Start

This alarm occurs on the active Cisco EGW 2200 when a synchronization operation between the active and standby Cisco EGW 2200 begins. This alarm clears automatically when the synchronization operation is completed. If a synchronization operation should fail, this alarm is automatically cleared and a FAIL REMOTE STANDBY alarm is generated. Refer to FAIL REMOTE STANDBY for more information.

Corrective Action

Corrective action is only required when the alarm does not clear automatically. If this alarm does not clear automatically, contact the Cisco TAC to further analyze the problem and determine a solution. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

SUPPORT FAILED

This alarm occurs when the identified entity cannot provide service because a supporting entity is not providing service. The supporting entity may be hardware or software.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Check for other alarms that further identify the failed entity.

Step 3 Once you have identified the failed entity, replace it and restore it to service. If the entity is hardware, refer to the appropriate documentation for replacement. If it is software, attempt to reboot the software.

If the alarms clear, the procedure is complete. Otherwise, proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

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.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

SwitchoverFail

This alarm occurs when a switchover operation from the active Cisco EGW 2200 to the standby Cisco EGW 2200 has failed.

Corrective Action

To correct the problem identified by this alarm, perform the following procedure:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 View the current alarms for the Cisco EGW 2200.

Step 3 Identify the critical alarm that caused the switchover attempt. To do this, review the alarm(s) that are listed in the response. There should be at least one critical alarm, and an alarm indicating that a switchover began and another alarm indicating that the switchover failed.

If there is only one critical alarm listed, that alarm caused the switchover attempt.

If there is more than one critical alarm listed, compare the timestamp of the critical alarms with the timestamp of the alarm indicating that a switchover began. The critical alarm that occurred before the switchover was begun is the alarm that caused the switchover attempt.

Step 4 Perform any corrective actions for the identified alarm.

Step 5 Use the ping tool to generate a ping from the active Cisco EGW 2200 to the standby Cisco EGW 2200.

If the ping fails, proceed to Step 6. Otherwise, proceed to Step 7.

Step 6 Verify the Ethernet interfaces between the active Cisco EGW 2200 and the standby Cisco EGW 2200. Refer to the documentation that came with your system for more information.

If an element of the Ethernet interfaces between the active Cisco EGW 2200 and the standby Cisco EGW 2200is found to be faulty, replace it. Otherwise, proceed to Step 7. Refer to the documentation that came with your system for more information.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 7.

Step 7 Verify that the host name for each Cisco EGW 2200 host is unique. If a Cisco EGW 2200 host does not have a unique host name, give that host a unique host name.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 8.

Step 8 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

TLC: Leg2chanDeletedUnpackError

This alarm occurs when a Delete Channel (DLCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

TLC: Leg2chanModifiedUnpackError

This alarm occurs when a Modify Channel (MDCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

TLC: Leg2chanOpFailed

This alarm occurs when the Cisco EGW has detected an internal error or a media gateway related problem.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

TLC: Leg2chanSeizedUnpackError

This alarm occurs when a Seize Channel (CRCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

TLC: Leg2deleteChanUnpackError

This alarm occurs when a Delete Channel (DLCX) message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

TLC: Leg2notifyRequestAckUnpackError

This alarm occurs when an Request Notify (RQNT) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

TLC: Leg2notifyUnpackError

This alarm occurs when a Notify (NTFY) message received from the media gateway could not be unpacked.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

UCM: CCodeModfailed

This alarm occurs when the country code prefix could not be applied or removed.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

Virtual_IP_Addr Mismatch

This alarm occurs when the virtual IP addresses on the active and the standby Cisco EGWs do not match.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

VSC_FAILURE

This alarm occurs when links to both (active and standby) Cisco EGW 2200s have gone down.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Ensure that the near-end and far-end data link terminations are operating.

If the near-end or far-end data link terminations are not operating, fix as necessary.

If the near-end and far-end data link terminations are operating, proceed to Step 3.

Step 3 Ensure that the provisioning settings for the signaling channel match the settings used on the far-end.

If the configuration data for the signaling channel is incorrect, modify your configuration. Refer to the Cisco EGW Administration online help system for more information.

If the configuration data for the signaling channel is correct, then proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

Wrong IP Path

This alarm occurs when an IP route or local interface associated with the identified component cannot be used. This can happen when one of the following occurs:

- A route has been overridden by another route in the operating system routing table.
- A route configured on your system has been deleted by someone.
- An IP link or route has been provisioned incorrectly.
- This alarm can also occur if an IP signaling channel has been misconfigured.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Performing a Call Trace.

XE Rsrc Fail

This alarm occurs when memory resources have been exhausted on the active Cisco EGW 2200 host. If this alarm occurs frequently you may need to add additional memory to your Cisco EGW 2200. Refer to the documentation for your Cisco EGW 2200 host for more information about adding additional memory.

Corrective Action

The problem identified by this alarm can only be resolved by the Cisco TAC. Before you contact the Cisco TAC, you should perform the procedure in Collecting Diagnostic Information for Cisco TAC.

Common Corrective Action Procedures

Many of the alarms require identical corrective action procedures. The procedures below are used by several of the alarms, as identified in the corrective action information.

Collecting Diagnostic Information for Cisco TAC

Perform the following steps when preparing to collect system diagnostic information before contacting the Cisco TAC to resolve your problem.

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

Performing a Call Trace

Perform the following steps when the corrective actions indicate you should perform a call trace:

Step 1 If you have not already done so, collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Perform a call trace on the affected interface. Refer to the Cisco EGW Administration online help for more information on this subject.

Note The affected interface can be determined using the content of the EGW Component field of the EGW Alarms screen. For information on identifying the inteface associated with a component, refer to the Identifying Alarms Components section of Cisco EGW 2200 Alarms..

Note Call trace information is only available to review for 48 hours after the trace has terminated.

Caution Running a call trace impacts call processing on your system. Cisco recommends that you take the following guidelines into consideration before enacting call traces:

Execute call traces for only the amount of time necessary to collect the required debug data for your particular situation. Allowing call traces to perpetuate can severely impact CPU availability, leading to less-than-optimum call processing in your system. As the default duration for a call trace is 30 minutes, you could potentially impact your system's ability to process calls for 30 minutes or more, depending on how many traces have been enacted and at what interval.

Execute call traces during off-peak hours to help minimize CPU impact and prevent less-than-optimum call processing in your system.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

Resolving a Dial Plan Alarm

When referred here by an alarm indicating a failure of a dial plan, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 View the settings for the affected dial plan, searching for any errors. Refer to the Cisco EGW Administration online help for more information on this subject.

If the settings for your dial plan are correct, proceed the Step 4.

If the settings for your dial plan are incorrect, proceed to Step 3.

Step 3 Modify the incorrect settings for the affected dial plan. Refer to the Cisco EGW Administration online help for more information on this subject.

If the alarm clears automatically, the procedure is complete. Otherwise, proceed to Step 4.

Step 4 Perform a call trace and contact the Cisco TAC to further analyze the problem and determine a solution, as described in Performing a Call Trace.

Resolving an Association Alarm

When referred here by an alarm indicating a failure on an association, perform the following steps:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify the functioning of the cabling between the Cisco EGW 2200 and the destination address.

If the cables are functioning properly, proceed to Step 4.

If bad cable(s) are found, replace them. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 3.

Step 3 Verify the functioning of the associated Cisco switch.

If the switch is functioning properly, proceed to Step 6.

If the switch is not functioning properly, refer to the documentation for your switch for troubleshooting information. If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 6.

Step 4 Debug the IP connectivity between the Cisco EGW 2200 and the associated media gateway.

If the IP connectivity is working correctly, proceed to Step 5.

If the IP connectivity is not working correctly, refer to the documentation for the external node to determine a method to identify and fix the IP connectivity problem. If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 5.

Step 5 Determine the health of the associated media gateway.

If the media gateway is working correctly, proceed to Step 6.

If the media gateway is not healthy, refer to the documentation for the external node for troubleshooting information. If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 6.

Step 6 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.

Resolving a Failed Connection to a Peer

If you have lost connection to a peer component in your network, perform the following procedure to resolve the problem:

Step 1 Collect diagnostic information from your system. Refer to the Cisco EGW Administration online help for more information on this subject.

Step 2 Verify that the interface to the affected peer is out-of-service. Refer to the Cisco EGW Administration online help for more information.

If the destination is in-service, or there is no destination associated with the peer, proceed to Step 3.

If the destination associated with the peer is out-of-service, bring the destination back into service. Refer to the Cisco EGW Administration online help for more information.

If that resolves the problem, this procedure is complete. Otherwise, proceed to Step 3.

Step 3 Ensure that the data path to the peer is working correctly.

If the data path to the peer is working correctly, proceed to Step 5.

If the data path to the peer is not working correctly, proceed to Step 4.

Step 4 Log in to the peer identified in Step 3 and verify that the Ethernet interfaces for this peer are working correctly. Refer to the documentation for the peer for more information.

If the Ethernet interfaces are working properly, proceed to Step 5.

If the Ethernet interfaces are not working properly, replace the element that is not working properly. Refer to the documentation of the peer for more information. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 5.

Step 5 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to Obtaining Technical Assistance.