



Fault Management

This chapter describes how to view appropriate fault information on the Cisco 12000 series internet routers you are managing. The Cisco 12000 series internet routers can be configured to send snmp traps when various conditions are detected. This may be a fault, the correction/resolution of a previous condition or a status update. Traps are translated into Cisco EMF alarms and raised against the appropriate C12kM object. These alarms are cleared automatically (if the resolution can be clearly detected by C12kM) or manually.

This chapter contains the following information:

- [Cisco 12000 Manager \(C12kM\) Alarms](#)
- [Cisco 12000 Series Internet Router Trap Support](#)
- [Heartbeat Polling](#)
- [ATM Interface Faults](#)

Cisco 12000 Manager (C12kM) Alarms

C12kM enables you to identify faults or alarms generated by Cisco 12000 series internet routers. Within the Map Viewer application, you are notified of alarms on individual objects by the colored status icons next to each managed object. The following table details all status colors and their related severities.

Table 14-1 Severity Colors

Color	Severity of Alarm
Red	Critical
Orange	Major
Yellow	Minor
Cyan	Warning
Green	No Alarms (Normal)
Blue	Card Decommissioned or Not Installed
White	Informational
Dark green	Pre-Provisioned

Alarms are propagated up the object hierarchy, and are reflected up to the highest level. For example, say a critical (red) alarm occurs on an interface. If you do not have the chassis map open, and if the interface text is not apparent, how would you know an alarm had occurred at that level? The answer is: propagation. The interface alarm would be propagated up the hierarchy to site level. This means that whatever level you are working at, you will see that an alarm has occurred. You can follow the path to discover where the alarm exists.

**Note**

C12kM is complimented by the Event Manager application. Among other features, the Event Manager enables you to set thresholds for certain system parameters and to monitor any supported C12kM MIB variables. Refer to the *Cisco Element Management Framework User Guide Release 3.2 (78-12536-01)* for further information.

Viewing Alarms

Alarms can be viewed using the Event Browser application that is part of the Cisco Element Management Framework (Cisco EMF).

Event Browser can be launched in two ways:

- Click the **Events** icon in the Cisco EMF Launchpad (see [Figure 3-2 on page 3-5](#)) to launch the Event Browser application. The Event Browser window appears.

Event Browser allows you to view all alarms on all objects. The Query Editor window appears automatically when you launch the Event Browser application. The Query Editor allows you to set up a query (or filter) that allows you to filter all the alarms available and display only the alarms matching the query criteria you selected.

When the event browser is launched against an object, by default, all the alarms against that object and its descendents are displayed in the event browser. For e.g., if the event browser is launched against a chassis, then by default it displays all the alarms against the chassis and the module and interfaces objects available in that chassis. Refer to the *Cisco Element Management Framework User Guide Release 3.2 (78-12536-01)* for further details on using the Event Browser.

- To view a specific alarm on one object, open the Map Viewer application (**Viewer**), right-click the object that generated the alarm, then choose **Tools>Open Event Browser**. The selected object alarm and its child objects alarms are displayed. You can open the Query Editor from the Event Browser window to modify your criteria to include only the selected object. Refer to the *Cisco Element Management Framework User Guide Release 3.2 (78-12536-01)* for detailed information on using the Query Editor.

Cisco 12000 Series Internet Router Trap Support

When a fault occurs on a managed object in the network, C12kM receives immediate notification, through a “trap” that is sent through the network. This trap manifests itself as an alarm in C12kM. A trap of any of the above category can be one of five severity types:

- Critical
- Major
- Warning
- Informational
- Normal

Chassis Alarms

Table 14-2 provides information on traps that result in alarms raised against the chassis object.

Table 14-2 Alarms Raised Against Chassis Objects

Trap	Alarm Description	Severity	Clears
Cold start	Cold Start: Agent reinitializing; configuration may have changed.	Major	not applicable
RPR+ Switchover	RPR+ Cold Start: Agent reinitializing; configuration may have changed	Major	not applicable
Warm start	Warm Start: Agent reinitializing; configuration is unaltered.	Major	not applicable
Authentication Failure	Authentication Failure	Major	not applicable
Voltage Normal	Voltage higher Chassis, normal, <value> mV	Normal	Normal, Critical, Shutdown, Warning, NotPresent
Voltage Warning	Voltage higher Chassis, warning, <value> mV	Warning	Critical, Shutdown, Warning, NotPresent
Voltage Critical	Voltage higher Chassis, critical, <value> mV	Critical	Critical, Shutdown, Warning, NotPresent
Voltage Shutdown	Voltage higher Chassis, shutdown, <value> mV	Critical	Critical, Shutdown, Warning, NotPresent
Voltage Not Present	Voltage higher Chassis, notPresent, <value> mV	Informational	Critical, Shutdown, Warning, NotPresent
Temperature Normal	Slot <no>: Switch Fabric Card Hot Sensor, normal, <value> degree celsius	Normal	Normal, Critical, Shutdown, Warning, NotPresent
Temperature Warning	Slot <no>: Switch Fabric Card Hot Sensor, warning, <value> degree celsius	Warning	Critical, Shutdown, Warning, NotPresent
Temperature Critical	Slot <no>: Switch Fabric Card Hot Sensor, critical, <value> degree celsius	Critical	Critical, Shutdown, Warning, NotPresent
Temperature Shutdown	Slot <no>: Switch Fabric Card Hot Sensor, shutdown, <value> degree celsius	Shutdown	Critical, Shutdown, Warning, NotPresent

Table 14-2 Alarms Raised Against Chassis Objects (continued)

Temperature Not Present	Slot <no>: Switch Fabric Card Hot Sensor, notPresent, <value> degree celsius	Informational	Critical, Shutdown, Warning, NotPresent
Fan Normal	Fan Tray 1, normal	Normal	Normal, Critical, Shutdown, Warning, NotPresent
Fan Warning	Fan Tray 1, warning	Warning	Critical, Shutdown, Warning, NotPresent
Fan Critical	Fan Tray 1, critical	Critical	Critical, Shutdown, Warning, NotPresent
Fan Shutdown	Fan Tray 1, shutdown	Critical	Critical, Shutdown, Warning, NotPresent
Fan Not Present	Fan Tray 1, notPresent	Informational	Critical, Shutdown, Warning, NotPresent
Power Supply Normal	Power Supply 1, normal	Normal	Normal, Critical, Shutdown, Warning, NotPresent
Power Supply Warning	Power Supply 1, warning	Warning	Critical, Shutdown, Warning, NotPresent
Power Supply Critical	Power Supply 1, critical	Critical	Critical, Shutdown, Warning, NotPresent
Power Supply Shutdown	Power Supply 1, shutdown	Critical	Critical, Shutdown, Warning, NotPresent
Power Supply Not Present	Power Supply 1, notPresent	Informational	Critical, Shutdown, Warning, NotPresent
BGP Connection Established	BGP Connection Established with Peer <peer-IP-Address>, Connection is in <peer-state> State	Normal	BGP Connection Established, BGP Connection Broken
BGP Connection Broken	BGP Connection Broken with Peer <peer-IP-Address>, Connection is in <peer-state> State	Major	BGP Connection Broken
FlashDeviceChange	A Flash Device has been inserted or removed from the chassis	Informational	FlashDeviceChange

**Note**

Temperature traps include the affected slot in the alarm description.

As can be seen from the table, Cisco EMF alarms may be cleared by other alarms. The general pattern is that an alarm clears alarms of the same or higher severity. All other alarms should be cleared manually.

Interface Alarms

Table 14-3 provides information on traps that result in alarms raised against interface objects.

Table 14-3 Alarms Raised Against Interface Objects

Trap	Alarm Description	Severity	Clears
Link down	Link <interface index> down	Major	Link down
Link up	Link <interface index> up	Normal	Link up, link down
Flow Created	A New Flow has been generated for <rsvp-FlowIndex> from Link <interface index>	normal	Flow Created, Flow Lost
Flow Lost	Flow Lost for <rsvp-FlowIndex> from Link <interface index>	informational	Flow Lost
PVC Failed	Total <no_of_failed_PVCs> PVCs are not up on ATM Interface <interface Index>	informational	PVC Failed

Table 14-4 Alarms Raised Against SRP Side Interface Objects for Wrap Status

Trap	Alarm Description	Severity	Clears
SRP Ring Wrapped	SRP Ring Wrapped	Major	SRP Ring Wrapped
SRP Ring Restored	SRP Ring Restored	Normal	SRP Ring Wrapped, SRP Ring Restored

Syslog Traps



Note

Care should be taken when using the Syslog alarm feature since there are multiple possible severity levels that can be activated which can result in large trap volumes. This can affect C12kM performance (for example, when opening an Event Browser) and hinder effective monitoring because of the high numbers of alarms that will be raised. It is advised that only the high severity traps are monitored by default, switching on others if more information is required.

Cisco IOS can be configured to send Syslog traps to a designated server. There are eight levels of Syslog information which are mapped into four categories of Cisco EMF alarm severity. Syslog specific data is inserted into the Message portion of the Cisco EMF alarm. In all cases, alarms are raised against the Chassis object. There is no automatic clearing of Syslog Alarms. Table 14-5 summarizes the severity mapping between trap and alarm:

Table 14-5 Syslog to Cisco EMF Mappings

Syslog Severity	Cisco EMF Severity
Emergency	Critical
Alert	Critical
Critical	Critical
Error	Major
Warning	Minor
Notification	Minor
Informational	Informational
Debug	Informational

Syslog alarms have a Description in the Event Browser application in the following format:

"Asserted [<clogHistMsgText>] by facility [<clogHistFacility>], Message name [<clogHistMsgName>]"

Where:

clogHistMsgText is the message text

clogHistFacility is the facility name (where the message came from)

clogHistMsgName is the message name

An example Syslog Alarm Description is

"Asserted [Critical/high priority process ATM Periodic may not dismiss.] by facility [SCHED], Message name [EDISMSCRIT]"

Configuration Management Traps

When a change is made to the configuration of a Cisco 12000 series internet router, Cisco IOS can send a "configuration management event trap". This trap is translated into a Cisco EMF alarm with the following description:

"Config Change, Command Source: <ccmHistoryEventCommandSource>, Config Source: <ccmHistoryEventConfigSource>, Config Destination: <ccmHistoryEventConfigDestination>"

Where:

- ccmHistoryEventCommandSource is the source of the command that instigated the event – either command line or snmp.
- ccmHistoryEventConfigSource is the configuration data source for the event
- ccmHistoryEventConfigDestination is the configuration data destination for the event

An example Configuration Management Event Alarm Description is:

"Config Change, Command Source: commandLine, Config Source: running, Config Destination: commandSource".

This would be received when a <write memory> command was issued.

Alarms are raised against the Chassis object with Informational Severity. There is no automatic clearing.

Heartbeat Polling

Heartbeat polling begins automatically when you commission a chassis. The chassis and all objects within the chassis are polled every five minutes. There are two types of heartbeat polling: Connectivity Management and Operational Status Polling.

The Heartbeat Polling section covers the following areas:

- [Connectivity Management](#)
- [Operational Status Polling](#)
- [Disabling Heartbeat Polling](#)
- [Performance Logging](#)

Connectivity Management

C12kM polls the management interface on the Cisco 12000 series internet router every 60 seconds to determine network connectivity. If management connectivity is lost, the chassis enters into a lost comms state and this state ripples down to all subchassis objects. A major lost comms alarm is raised against the chassis. The chassis continues to poll. If it detects re-establishment, it puts the chassis state back to the relevant state and this state ripples down to all subchassis objects as well. An alarm of Normal severity is then raised which clears the major lost comms alarm.

Operational Status Polling

Operational Status Polling— Occurs at module and interface levels. Each module and interface polls for its own operational status, for Modules/Interfaces, this is every 5 minutes. If a module detects that its operational status is down, it enters the Errored state and raises a Major alarm. The Errored state does not propagate down to PVCs and SVCs. If an interface goes down, you can see this in the Generic Interface Status window. In the Errored state the module or interface will continue to poll if the condition has been rectified. If it detects that the operational state has moved back to healthy then the object will transition into the Normal state and raise an alarm of Normal severity which will clear the previous Major alarm.

Disabling Heartbeat Polling

You can stop heartbeat polling on an individual interface by decommissioning the interface. You might want to do this if you have interfaces that are not yet connected or live. For example, when you commission a chassis, subchassis discovery is automatically initiated. If you have pre-deployed interfaces that are not yet live, these are discovered and put into an Errored state, after no connectivity is detected on them. An alarm is also be raised on the interface. To correct this situation, you need to decommission the inactive interface and clear the alarm manually.

Performance Logging

Heartbeat polling is unaffected if an object is in the performance logging state.

ATM Interface Faults

The ATM Interface Faults section covers the following areas:

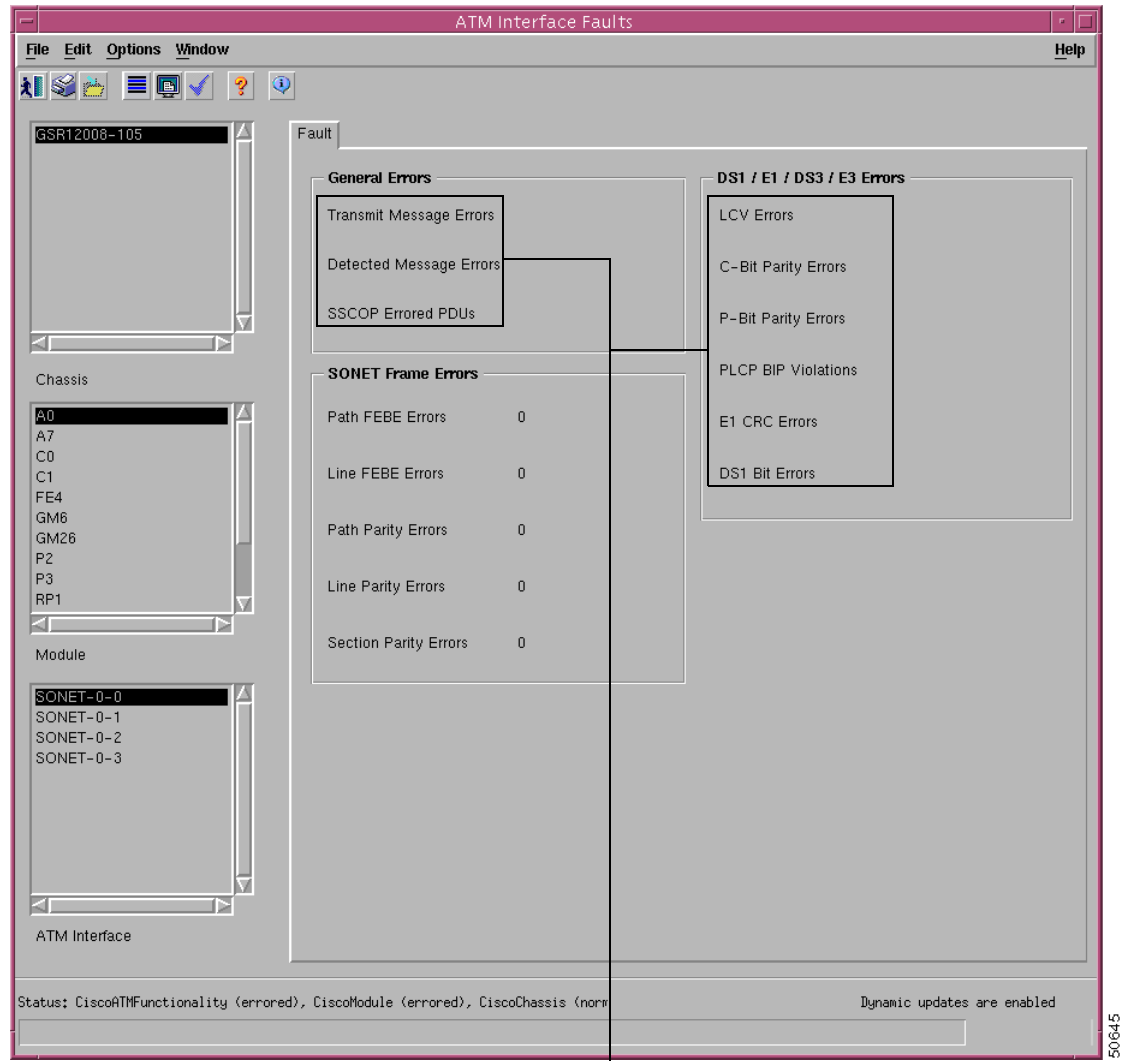
- [Viewing the ATM Interface Faults Window](#)
- [ATM Interface Faults Window—Detailed Description](#)

Viewing the ATM Interface Faults Window

To view the ATM Interface Faults window, proceed as follows:

-
- Step 1** Right-click on a selected ATM interface, then choose **C12kM Management>Physical>Interface>ATM>Fault**. The ATM Interface Faults window appears:

Figure 14-1 ATM Interface Faults Window



Not applicable to C12kM

- Step 2** Choose a **Chassis**, **Module**, and **ATM Interface** from the lists displayed at the left of the window. The fault information is displayed for the selected ATM interface.

ATM Interface Faults Window—Detailed Description

The ATM Interface Faults window displays a single Fault tab.

Fault Tab

The Fault tab (see Figure 14-1) displays three areas: General Errors, SONET Frame Errors, and DS1/E1/DS3/E3 Errors.

General Errors

The General Errors area is not applicable to C12kM.

SONET Frame Errors

The SONET Frame Errors area displays the following information:

Path FEBE Errors—Number of G1 (path FEBE) errors on the physical interface.

Line FEBE Errors—Number of Z2 (line FEBE) errors on the physical interface.

Path Parity Errors—Number of B3 (BIP) errors on the physical interface.

Line Parity Errors—Number of B2 (BIP) errors on the physical interface.

Section Parity Errors—Number of B1 (BIP) errors on the physical interface.

DS1/E1/SD3/E3 Errors

The DS1/E1/DS3/E3 Errors area is not applicable to C12kM.