Alarm Monitoring and Management

This chapter describes Cisco Transport Controller (CTC) alarm management. To troubleshoot specific alarms, refer to the *Cisco ONS 15327 Troubleshooting Guide*. Chapter topics include:

9.1 Overview

CTC detects and reports SONET alarms generated by the Cisco ONS 15327 and the larger SONET network. You can use CTC to monitor and manage alarms at the card, node, or network level. Default alarm severities conform to the Telcordia GR-253 standard, but you can set alarm severities in customized alarm profiles or suppress CTC alarm reporting. For a detailed description of the standard Telcordia categories employed by Optical Networking System (ONS) nodes, refer to the *Cisco ONS 15327 Troubleshooting Guide.*

Note ONS 15327 alarms can also be monitored and managed through Transaction Language One (TL1) or a network management system (NMS).

9.2 Viewing Alarms

In the card-, node-, or network-level CTC view, click the Alarms tab to display the alarms for that card, node, or network. The Alarms window shows alarms in conformance with Telcordia GR-253. This means that if a network problem causes two alarms, such as loss of frame (LOF) and loss of signal (LOS), CTC only shows the LOS alarm in this window because it supersedes the LOF and replaces it.

In Release 5.0, the Path Width column on the Alarms and Conditions tabs will expand upon alarmed object information contained in the TL1 access identifier (AID) string (such as "STS-4-1-3") by giving the number of STSs contained in the alarmed path. For example, the Path Width will tell you whether a Critical alarm applies to a synchronous transport signal 1 (STS1) or an STS48c. The column reports the width as a 1, 3, 6, 12, 48, etc. as appropriate, understood to be "STS-*n*."

Table 9-1 lists the column headings and the information recorded in each column.

Table 9-1 Alarms Column Descriptions

Column	Information Recorded
New	Indicates a new alarm. To change this status, click either the Synchronize button or the Delete Cleared Alarms button.
Date	Date and time of the alarm.
Node	Node where the alarm occurred (appears only in network view).
Object	TL1 access identifier (AID) for the alarmed object. For an STSmon or VTmon, this is the monitored STS or VT object, which is explained in Table 9-3 on page 9-3.
Eqpt Type	Card type in this slot.
Slot	Slot where the alarm occurred (appears only in network and node view).
Port	Port where the alarm is raised. For STSTerm and VTTerm, the port refers to the upstream card it is partnered with.
Path Width	Indicates how many STSs are contained in the alarmed path. This information complements the alarm object notation, which is explained in Table 9-3.
Sev	Severity level: CR (Critical), MJ (Major), MN (Major), NA (Not Alarmed), NR (Not Reported).
ST	Status: R (raised), C (clear).
SA	When checked, indicates a service-affecting alarm.
Cond	The error message/alarm name. These names are alphabetically defined in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15327 Troubleshooting Guide.*
Description	Description of the alarm.
Num	Num (number) is the quantity of alarm messages received, and is incremented automatically as alarms occur to display the current total of received error messages.
Ref	Ref (reference) is a unique identification number assigned to each alarm to reference a specific alarm message that is displayed.

Table 9-2 lists the color codes for alarm and condition severities. In addition to the severities listed in the table, CTC alarm profiles list inherited (I) and unset (U) severities. These are only listed in the network view Provisioning > Alarm Profiles tab and are not currently implemented.

Table 9-2 Color Codes for Alarm and Condition Severities

Color	Description
Red	Raised Critical (CR) alarm
Orange	Raised Major (MJ) alarm
Yellow	Raised Minor (MN) alarm
Magenta	Raised Not Alarmed (NA) condition

Table 9-2 Color Codes for Alarm and Condition Severities (continued)

Color	Description
Blue	Raised Not Reported (NR) condition
White	Cleared (C) alarm or condition

Note Major and Minor alarms may appear yellow in CTC under certain circumstances. This is not due to a CTC problem but to a workstation memory and color utilization problem. For example, a workstation might run out of colors if many color-intensive applications are running. When using Netscape, you can limit the number of colors used by launching it from the command line with either the -install option or the -ncols 32 option.

In network view, CTC identifies STS and VT alarm objects using a TL1-type AID, as shown in Table 9-3.

Table 9-3 STS and Alarm Object Identification

Object	STS or VT AID	Port No.
MON object	STS-<Slot>-<Port>-STS For example, STS-6-1-6 VT1-<Slot>-<Port>-<STS>-<VT Group>-<VT> For example, VT1-6-1-6-1-1	Port=1
TERM object	STS-<Upstream Slot>-<Port>-<STS> For example, STS-6-3-6 VT1-<Upstream Slot>-<Port>-<STS>-<VT Group>-<VT> For example, VT1-6-3-6-1-1	Port=1

9.2.1 Viewing Alarms With Each Node's Time Zone

By default, alarms and conditions are displayed with the time stamp of the CTC workstation where you are viewing them. You can set the node to report alarms (and conditions) using the time zone where the node is located by clicking Edit > Preferences, and then clicking the Display Events Using Each Node's Timezone check box.

9.2.2 Controlling Alarm Display

You can control the display of the alarms shown on the Alarms window. Table 9-4 shows the actions you can perform in the Alarms window.

Table 9-4 Alarm Display

Button/Check Box/Tool	Action
Filter button	Allows you to change the display on the Alarms window to show only alarms that meet a certain severity level, occur in a specified time frame, and/or reflect specific conditions. For example, you can set the filter so that only Critical alarms display on the window. If you enable the Filter feature by clicking the Filter icon button in one CTC view, such as node view, it is enabled in the others as well (card view and network view).
Synchronize button	Updates the alarm display. Although CTC displays alarms in real time, the Synchronize button allows you to verify the alarm display. This is particularly useful during provisioning or troubleshooting.
Delete Cleared Alarms button	Deletes alarms that have been cleared.
AutoDelete Cleared Alarms check box	If checked, CTC automatically deletes cleared alarms.
Filter tool	Enables or disables alarm filtering in the card, node, or network view. When enabled or disabled, this state applies to other views for that node and for all other nodes in the network. For example, if the Filter tool is enabled in the node (default login) view Alarms window, the network view Alarms window and card view Alarms window also show the tool enabled. All other nodes in the network also show the tool enabled.

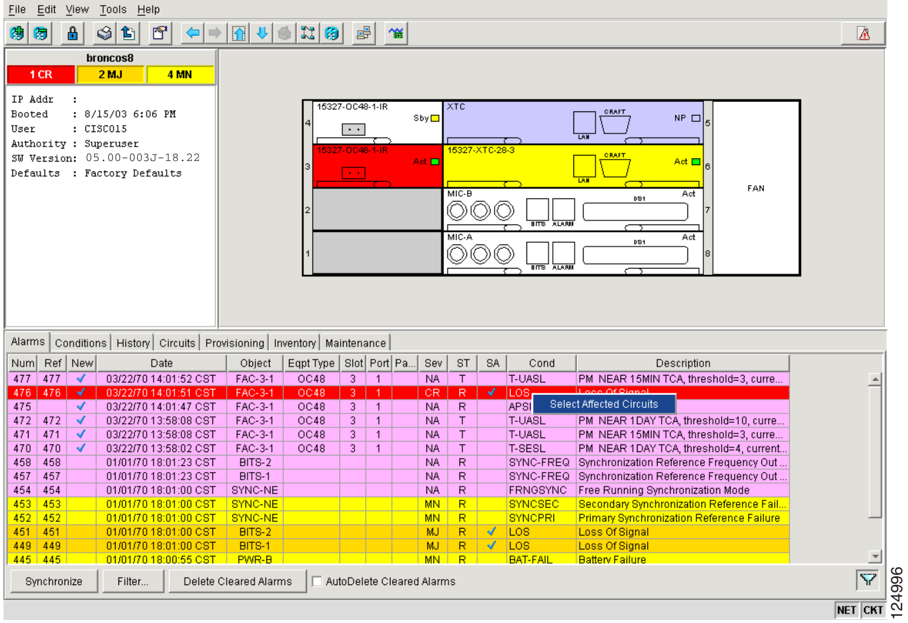
9.2.3 Filtering Alarms

The alarm display can be filtered to prevent display of alarms with certain severities or alarms that occurred between certain dates. You can set the filtering parameters by clicking the Filter button at the bottom-left of the Alarms window. You can turn the filter on or off by clicking the Filter tool at the bottom-right of the window. CTC retains your filter activation setting. For example, if you turn the filter on and then log out, CTC keeps the filter active the next time you log in.

9.2.4 Viewing Alarm-Affected Circuits

A user can view which ONS 15327 circuits are affected by a specific alarm by positioning the cursor over the alarm in the Alarm window and right-clicking. A shortcut menu appears (Figure 9-1). When the user selects the Select Affected Circuits option, the Circuits window appears to show the circuits that are affected by the alarm (Figure 9-2).

Figure 9-1 Select Affected Circuits Option

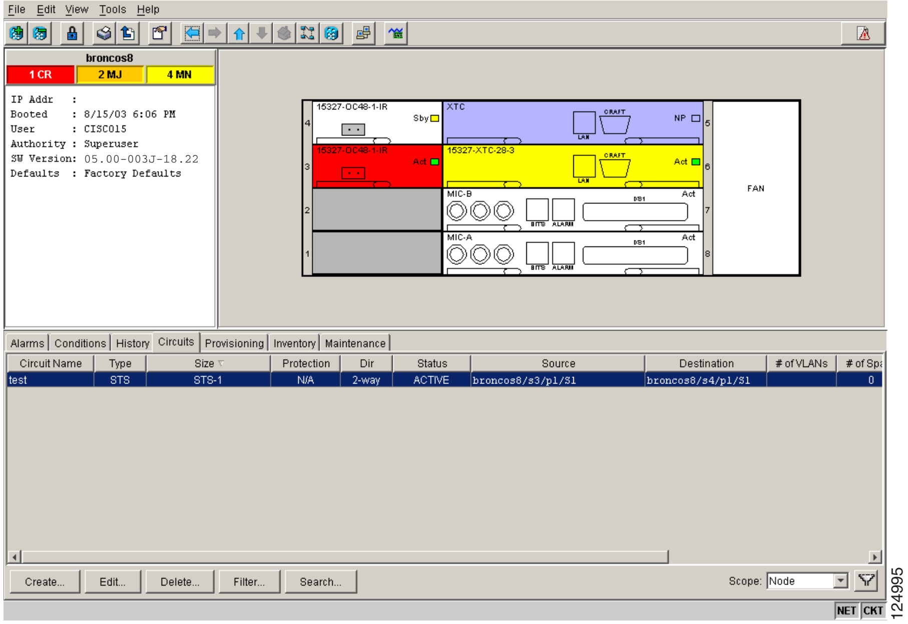


IP Addr :
Booted : 8/15/03 6:06 PM
User : CISCO15
Authority : Superuser
SW Version: 05.00-003J-18.22
Defaults : Factory Defaults

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Pa...	Sev	ST	SA	Cond	Description
477	477	✓	03/22/70 14:01:52 CST	FAC-3-1	OC48	3	1		NA	T		T-UASL	PM NEAR 15MIN TCA, threshold=3, curre...
476	476	✓	03/22/70 14:01:51 CST	FAC-3-1	OC48	3	1		CR	R	✓	LOS	Loss Of Signal
475		✓	03/22/70 14:01:47 CST	FAC-3-1	OC48	3	1		NA	R		APSI	
472	472	✓	03/22/70 13:58:08 CST	FAC-3-1	OC48	3	1		NA	T		T-UASL	PM NEAR 1DAY TCA, threshold=10, curre...
471	471	✓	03/22/70 13:58:08 CST	FAC-3-1	OC48	3	1		NA	T		T-UASL	PM NEAR 15MIN TCA, threshold=3, curre...
470	470	✓	03/22/70 13:58:02 CST	FAC-3-1	OC48	3	1		NA	T		T-SESL	PM NEAR 1DAY TCA, threshold=4, current...
458	458		01/01/70 18:01:23 CST	BITS-2					NA	R		SYNC-FREQ	Synchronization Reference Frequency Out ...
457	457		01/01/70 18:01:23 CST	BITS-1					NA	R		SYNC-FREQ	Synchronization Reference Frequency Out ...
454	454		01/01/70 18:01:00 CST	SYNC-NE					NA	R		FRNGSYNC	Free Running Synchronization Mode
453	453		01/01/70 18:01:00 CST	SYNC-NE					MN	R		SYNCSEC	Secondary Synchronization Reference Fail...
452	452		01/01/70 18:01:00 CST	SYNC-NE					MN	R		SYNCPRI	Primary Synchronization Reference Failure
451	451		01/01/70 18:01:00 CST	BITS-2					MJ	R	✓	LOS	Loss Of Signal
449	449		01/01/70 18:01:00 CST	BITS-1					MJ	R	✓	LOS	Loss Of Signal
445	445		01/01/70 18:00:55 CST	PWR-B					MN	R		BAT-FAIL	Battery Failure

□ AutoDelete Cleared Alarms

Figure 9-2 Viewing Alarm-Affected Circuits



IP Addr :
Booted : 8/15/03 6:06 PM
User : CISCO15
Authority : Superuser
SW Version: 05.00-003J-18.22
Defaults : Factory Defaults

Circuit Name	Type	Size	Protection	Dir	Status	Source	Destination	# of VLANs	# of Spa
test	STS	STS-1	N/A	2-way	ACTIVE	broncos8/s3/p1/S1	broncos8/s4/p1/S1		0

Scope: Node

9.2.5 Conditions Tab

The Conditions window displays retrieved fault conditions. A condition is a fault or status detected by ONS 15327 hardware or software. When a condition occurs and continues for a minimum period, CTC raises a condition, which is a flag showing that this particular condition currently exists on the ONS 15327.

The Conditions window shows all conditions that occur, including those that are superseded. For instance, if a network problem causes two alarms, such as LOF and LOS, CTC shows both the LOF and LOS conditions in this window (even though LOS supersedes LOF). Having all conditions visible can be helpful when troubleshooting the ONS 15327. If you want to retrieve conditions that obey a root-cause hierarchy (that is, LOS supersedes and replaces LOF), you can exclude the same root causes by checking a check box in the window.

Fault conditions include reported alarms and Not Reported or Not Alarmed conditions. Refer to the trouble notifications information in the *Cisco ONS 15327 Troubleshooting Guide* for more information about alarm and condition classifications.

9.2.6 Controlling the Conditions Display

You can control the display of the conditions on the Conditions window. Table 9-5 shows the actions you can perform in the window.

Table 9-5 Conditions Display

Button	Action
Retrieve	Retrieves the current set of all existing fault conditions, as maintained by the alarm manager, from the ONS 15327.
Filter	Allows you to change the Conditions window display to only show the conditions that meet a certain severity level or occur in a specified time. For example, you can set the filter so that only Critical conditions display on the window. There is a Filter button on the lower-right of the window that allows you to enable or disable the filter feature.

9.2.6.1 Retrieving and Displaying Conditions

The current set of all existing conditions maintained by the alarm manager can be seen when you click the Retrieve button. The set of conditions retrieved is relative to the view. For example, if you click the button while displaying the node view, node-specific conditions are displayed. If you click the button while displaying the network view, all conditions for the network (including ONS 15327 nodes and other connected nodes) are displayed, and the card view shows only card-specific conditions.

You can also set a node to display conditions using the time zone where the node is located, rather than the time zone of the PC where they are being viewed. See the "9.2.1 Viewing Alarms With Each Node's Time Zone" section on page 9-3 for more information.

9.2.6.2 Conditions Column Descriptions

Table 9-6 lists the Conditions window column headings and the information recorded in each column.

Table 9-6 Conditions Column Description

Column	Information Recorded
New	Indicates a new condition.
Date	Date and time of the condition.
Object	TL1 AID for the condition object. For an STSmon or VTmon, the object.
Eqpt Type	Card type in this slot.
Slot	Slot where the condition occurred (appears only in network and node view).
Port	Port where the condition occurred. For STSTerm and VTTerm, the port refers to the upstream card it is partnered with.
Sev[1]	Severity level: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR)
SA	Indicates a service-affecting (when checked)
Cond	The error message/alarm name; these names are alphabetically defined in the *Cisco ONS 15327 Troubleshooting Guide*.

[1] All alarms, their severities, and service-affecting status are also displayed in the Conditions tab unless you choose to filter the alarm from display using the Filter button.

9.2.6.3 Filtering Conditions

The condition display can be filtered to prevent display of conditions (including alarms) with certain severities or that occurred between certain dates. You can set the filtering parameters by clicking the Filter button at the bottom-left of the Conditions window. You can turn the filter on or off by clicking the Filter tool at the bottom-right of the window. CTC retains your filter activation setting. For example, if you turn the filter on and then log out, CTC keeps the filter active the next time your user ID is activated.

9.2.7 Viewing History

The History window displays historic alarm or condition data for the node or for your login session. You can chose to display only alarm history, only events, or both by checking check boxes in the History > Node window. You can view network-level alarm and condition history, such as for circuits, at that level. At the node level, you can see all port (facility), card, STS, and system-level history entries. For example, protection-switching events or performance-monitoring threshold crossings appear here. If you double-click a card, you can view all port, card, and STS alarm or condition history that directly affects the card.

The ONS 15327 can store up to 640 Critical alarm messages, 640 Major alarm messages, 640 Minor alarm messages, and 640 condition messages. When any of these limits is reached, the ONS 15327 discards the oldest events in that category.

Note In the Preference dialog box General tab, the Maximum History Entries value only applies to the Session window.

Different views of CTC display different kinds of history:

- The History > Session window is shown in network view, node view, and card view. It shows alarms and conditions that occurred during the current user CTC session.
- The History > Node window is only shown in node view. It shows the alarms and conditions that occurred on the node since CTC software was operated on the node.
- The History > Card window is only shown in card view. It shows the alarms and conditions that occurred on the card since CTC software was installed on the node.

Tip Double-click an alarm in the History window to display the corresponding view. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.

If you check the History window Alarms check box, you display the node history of alarms. If you check the Events check box, you display the node history of Not Alarmed and transient events (conditions). If you check both check boxes, you retrieve node history for both.

9.2.7.1 History Column Descriptions

Table 9-7 lists the History window column headings and the information recorded in each column.

Table 9-7 History Column Description

Column	Information Recorded
Num	An incrementing count of alarm or condition messages. (The column is hidden by default; to view it, right-click a column and choose Show Column > Num.)
Ref	The reference number assigned to the alarm or condition. (The column is hidden by default; to view it, right-click a column and choose Show Column > Ref.)
Date	Date and time of the condition.
Object	TL1 AID for the condition object. For an STSmon or VTmon, the object.
Sev	Severity level: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR).
Eqpt Type	Card type in this slot (only displays in network view and node view).
ST	Status: raised (R), cleared (C), or transient (T).
Description	Description of the condition.
Port	Port where the condition occurred. For STSTerm and VTTerm, the port refers to the upstream card it is partnered with.
Cond	Condition name.
Slot	Slot where the condition occurred (only displays in network view and node view).
SA	A service-affecting alarm (when checked).

9.2.7.2 Retrieving and Displaying Alarm and Condition History

You can retrieve and view the history of alarms and conditions, as well as transients (passing notifications of processes as they occur) in the CTC history window. The information in this window is specific to the view where it is shown (that is, network history in the network view, node history in the node view, and card history in the card view).

The node and card history views are each divided into two tabs. In node view, when you click the Retrieve button, you can see the history of alarms, conditions, and transients that have occurred on the node in the History > Node window, and the history of alarms, conditions, and transients that have occurred on the node during your login session in the History > Session window. In the card history window, after you retrieve the card history, you can see the history of alarms, conditions, and transients on the card in the History > Card window, or a history of alarms, conditions, and transients that have occurred during your login session in the History > Session window.

You can also filter the severities and occurrence period in these history windows, but you cannot filter out Not Reported conditions or transients.

9.3 Alarm Severities

ONS 15327 alarm severities follow the Telcordia GR-253 standard, so a condition may be alarmed (at a severity of Critical [CR], Major [MJ], or Minor [MN]), Not Alarmed (NA), or Not Reported (NR). These severities are reported in the CTC software Alarms, Conditions, and History windows at all levels: network, shelf, and card.

ONS equipment provides a standard profile named Default that lists all alarms and conditions with severity settings based on Telcordia GR-253 and other standards, but users can create their own profiles with different settings for some or all conditions and apply these wherever desired. (See the "9.4 Alarm Profiles" section on page 9-9.) For example, in a custom alarm profile, the default severity of a carrier loss (CARLOSS) alarm on an Ethernet port could be changed from Major to Critical. The profile allows setting to Not Reported or Not Alarmed, as well as the three alarmed severities.

Critical and Major severities are only used for service-affecting alarms. If a condition is set as Critical or Major by profile, it will raise as Minor alarm in the following situations:

- In a protection group, if the alarm is on a standby entity (side not carrying traffic)
- If the alarmed entity has no traffic provisioned on it, so no service is lost.

Because of this possibility of being raised at two different levels, the alarm profile pane shows Critical as "CR / MN" and Major as "MJ / MN."

9.4 Alarm Profiles

The alarm profiles feature allows you to change default alarm severities by creating unique alarm profiles for individual ONS 15327 ports, cards, or nodes. A created alarm profile can be applied to any node on the network. Alarm profiles can be saved to a file and imported elsewhere in the network, but the profile must be stored locally on a node before it can be applied to the node, its cards, or its cards' ports.

CTC can store up to ten active alarm profiles at any time to apply to the node. Custom profiles can take eight of these active profile positions. Two other profiles, Default profile and Inherited profile, are reserved by the NE, and cannot be edited. The reserved Default profile contains Telcordia GR-253 severities. The reserved Inherited profile allows port alarm severities to be governed by the card-level severities, or card alarm severities to be determined by the node-level severities.

If one or more alarm profiles have been stored as files from elsewhere in the network onto the local PC or server hard drive where CTC resides, you can utilize as many profiles as you can physically store by deleting and replacing them locally in CTC so that only eight are active at any given time.

9.4.1 Creating and Modifying Alarm Profiles

Alarm profiles are created in the network view using the Provisioning > Alarm Profiles tabs. A default alarm severity following Telcordia GR-253 standards is preprovisioned for every alarm. After loading the default profile or another profile on the node, you can use the Clone feature to create custom profiles. After the new profile is created, the Alarm Profiles window shows the original profile—frequently Default—and the new profile.

Note The Default alarm profile list contains alarm and condition severities that correspond when applicable to default values established in Telcordia GR-253.

Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in non-service-affecting situations as defined in Telcordia GR-474.

Tip To see the full list of profiles including those available for loading or cloning, click the Available button. You must load a profile before you can clone it.

Note Up to ten profiles, including the two reserved profiles—Inherited and Default—can be stored in CTC.

Wherever it is applied, the Default alarm profile sets severities to standard Telcordia GR-253 settings. In the Inherited profile, alarms inherit, or copy, severity from the next-highest level. For example, a card with an Inherited alarm profile copies the severities used by the node housing the card. If you choose the Inherited profile from the network view, the severities at the lower levels (node and card) are copied from this selection.

You do not have to apply a single severity profile to the node-, card-, and port-level alarms. Different profiles can be applied at different levels. You could use the inherited or default profile on a node and on all cards and ports, but apply a custom profile that downgrades an alarm on one particular card. For example, you might choose to downgrade an OC-N unequipped path alarm (UNEQ-P) from Critical (CR) to Not Alarmed (NA) on an optical card because this alarm raises and then clears every time you create a circuit. UNEQ-P alarms for the card with the custom profile would not display on the Alarms tab (but they would still be recorded on the Conditions and History tabs).

When you modify severities in an alarm profile:

- All Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.
- Default severities are used for all alarms and conditions until you create a new profile and apply it.

9.4.2 Alarm Profile Buttons

The Alarm Profiles window displays six buttons on the right side. Table 9-8 lists and describes each of the alarm profile buttons and their functions.

Table 9-8 Alarm Profile Buttons

Button	Description
New	Adds a new alarm profile.
Load	Loads a profile to a node or a file.
Store	Saves profiles on a node (or nodes) or in a file.
Delete	Deletes profiles from a node.
Compare	Displays differences between alarm profiles (for example, individual alarms that are not configured equivalently between profiles).
Available	Displays all profiles available on each node.
Usage	Displays all entities (nodes and alarm subjects) present in the network and shows which profiles contain the alarm. Can be printed.

9.4.3 Alarm Profile Editing

Table 9-9 lists and describes the five profile-editing options available when you right-click an alarm item in the profile column (such as Default).

Table 9-9 Alarm Profile Editing Options

Button	Description
Store	Saves a profile in a node or in a file.
Rename	Changes a profile name.
Clone	Creates a profile that contains the same alarm severity settings as the profile being cloned.
Reset	Restores a profile to its previous state or to the original state (if it has not yet been applied).
Remove	Removes a profile from the table editor.

9.4.4 Alarm Severity Options

To change or assign alarm severity, left-click the alarm severity you want to change in the alarm profile column. Seven severity levels appear for the alarm:

- Not Reported (NR)
- Not Alarmed (NA)
- Minor (MN)
- Major (MJ)
- Critical (CR)

- Use Default
- Inherited (I)

Inherited and Use Default severity levels only appear in alarm profiles. They do not appear when you view alarms, history, or conditions.

9.4.5 Row Display Options

In the network view, the Alarm Profiles window displays two check boxes at the bottom of the window:

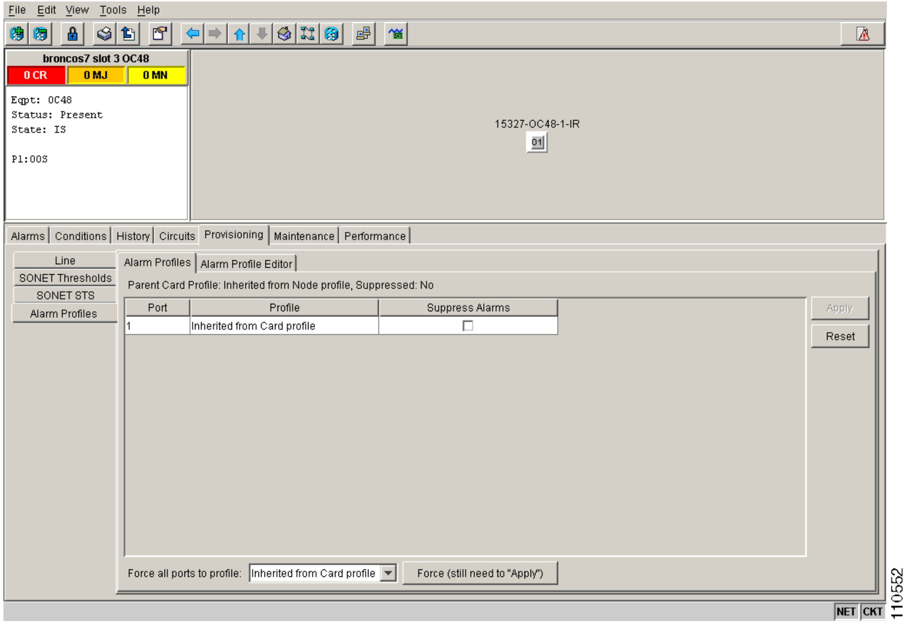
- Hide reference values—Highlights alarms with non-default severities by clearing alarm cells with default severities.
- Hide identical rows—Hides rows of alarms that contain the same severity for each profile.

9.4.6 Applying Alarm Profiles

In CTC node view, the Alarm Behavior window displays alarm profiles for the node. In card view, the Alarm Behavior window displays the alarm profiles for the selected card. Alarm profiles form a hierarchy. A node-level alarm profile applies to all cards in the node except cards that have their own profiles. A card-level alarm profile applies to all ports on the card except ports that have their own profiles.

At the node level, you can apply profile changes on a card-by-card basis or set a profile for the entire node. At the card-level view, you can apply profile changes on a port-by-port basis or set alarm profiles for all ports on that card. Figure 9-3 shows the card view of an optical alarm profile.

Figure 9-3 Card View of an Optical Card Alarm Profile



broncos7 slot 3 OC48

0 CR | 0 MJ | 0 MN

Eqpt: OC48
Status: Present
State: IS

P1:OOS

Parent Card Profile: Inherited from Node profile, Suppressed: No

Port	Profile	Suppress Alarms
1	Inherited from Card profile	□

Force all ports to profile: Inherited from Card profile

9.5 Suppressing Alarms

ONS 15327 nodes have an alarm suppression option that clears raised alarm messages for the node, chassis, one or more slots (cards), or one or more ports. After they are cleared, these alarms change appearance from their normal severity color to white and they can be cleared from the display by clicking Synchronize. Alarm suppression itself raises an alarm called AS-CMD that is shown in applicable Alarms windows. Node-level suppression is shown in the node view Alarms window, and card or port-level suppression is shown in all views. The AS-CMD alarm itself is not cleared by the suppress command. Each instance of this alarm indicates its object separately in the Object column.

A suppression command applied at a higher level does not supersede a command applied at a lower level. For example, applying a node-level alarm suppression command makes all raised alarms for the node appear to be cleared, but it does not cancel out card-level or port-level suppression. Each of these conditions can exist independently and must be cleared independently.

Suppression causes the entity alarm to behave like a Not Reported event. This means that the alarms, having been suppressed from view in the Alarms window, are now only shown in the Conditions window. The suppressed alarms are displayed with their usual visual characteristics (service-affecting status and color-coding) in the window. The alarms still appear in the History window.

Note Use alarm suppression with caution. If multiple CTC or TL1 sessions are open, suppressing the alarms in one session suppresses the alarms in all other open sessions.

9.6 Provisioning External Alarms and Controls

External alarm physical connections are made on the mechanical interface card (MIC). However, the alarms are provisioned using the XTC card view for external sensors such as an open door and flood sensors, temperature sensors, and other environmental conditions. External control outputs on these two cards allow you to drive external visual or audible devices such as bells and lights. They can control other devices such as generators, heaters, and fans.

You provision external alarms in the XTC card view Provisioning> External Alarms tab and controls in the XTC card view Provisioning > External Controls tab. Up to six external alarm inputs and two external controls are available with the XTC card.

9.6.1 External Alarm Input

You can provision each alarm input separately. Provisionable characteristics of external alarm inputs include:

- Alarm type
- Alarm severity (CR, MJ, MN, NA, and NR)
- Alarm-trigger setting (open or closed); open means that the normal condition is no current flowing through the contact, and the alarm is generated when current does flow; closed means that normal condition is to have current flowing through the contact, and the alarm is generated with current stops flowing
- Virtual wire associated with the alarm
- CTC alarm log description (up to 63 characters)

Note If you provision an external alarm to raise upon an open contact before you physically connect to the ONS equipment, the alarm will raise until you create the physical connection.

Note When you provision an external alarm, the alarm object is ENV-IN-*nn*. The variable *nn* refers to the external alarm's number, regardless of the name you assign.

9.6.2 External Control Output

You can provision each alarm output separately. Provisionable characteristics of alarm outputs include:

- Control type
- Trigger type (alarm or virtual wire)
- Description for CTC display
- Closure setting (manually or by trigger). If you provision the output closure to be triggered, the following characteristics can be used as triggers:
  - Local NE alarm severity—A chosen alarm severity (for example, Major) and any higher-severity alarm (in this case, Critical) causes output closure.
  - Remote NE alarm severity—Similar to local NE alarm severity trigger setting, but applies to remote alarms.
  - Virtual wire entities—You can provision an alarm that is input to a virtual wire to trigger an external control output.

9.7 Audit Trail

The ONS 15327 maintains an audit trail log that resides on the XTC. This record shows who has accessed the system and what operations were performed during a given period of time and is in accordance with GR-839-CORE. The log includes authorized Cisco logins and logouts using the operating system command line interface, CTC, and TL1; the log also includes FTP actions, circuit creation/deletion, and user/system generated actions.

Event monitoring is also recorded in the audit log. An event is defined as the change in status of an element within the network. External events, internal events, attribute changes, and software upload/download activities are recorded in the audit trail.

Audit trails are useful for maintaining security, recovering lost transactions and enforcing accountability. Accountability is the ability to trace user activities and is done by associating a process or action with a specific user. To view the Audit Trail log, refer to *Cisco ONS 15327 Procedure Guide*. Users can access the audit trail logs from any management interface (CTC, CTM, TL1).

The audit trail is stored in persistent memory and is not corrupted by processor switches, resets or upgrades. However, if a user pulls both TCCs, the audit trail log is lost.

9.7.1 Audit Trail Log Entries

Audit trail records capture the following activities:

- User—Name of the user performing the action
- Host—Host from where the activity is logged
- Device ID—IP address of the device involved in the activity
- Application—Name of the application involved in the activity
- Task—Name of the task involved in the activity (View a dialog, apply configuration and so on)
- Connection Mode—Telnet, Console, SNMP
- Category—Type of change; Hardware, Software, Configuration
- Status—Status of the user action… (Read, Initial, Successful, Timeout, Failed)
- Time—Time of change
- Message Type—Denotes if the event is Success/Failure type
- Message Details—A description of the change

9.7.2 Audit Trail Capacities

The system is able to store 640 log entries.When this limit is reached, the oldest entries are overwritten with new events.

When the log server is 80 percent full, an AUD-LOG-LOW condition is raised and logged (by way of CORBA/CTC).

When the log server reaches a maximum capacity of 640 entries and begins overwriting records that were not archived, an AUD-LOG-LOSS condition is raised and logged. This event indicates that audit trail records have been lost. Until the user off-loads the file, this event occurs once regardless of the amount of entries that are overwritten by the system. To export the Audit Trail log, refer to the NTP-B214 Offload the Audit Trail Record procedure in the *Cisco ONS 15327 Procedure Guide*.