NavisXtend Fault Server User's Guide

Ascend Communications, Inc.

Product Code: 80041
Revision 00
November 1997

ASCEND COMMUNICATIONS, INC. END-USER LICENSE AGREEMENT

ASCEND COMMUNICATIONS, INC. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE AND ACCOMPANYING USER DOCUMENTATION (COLLECTIVELY, THE “PROGRAM”) TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE(S) OR USING THE ASCEND SWITCH(ES) CONTAINING THE SOFTWARE, AND BEFORE USING THE ACCOMPANYING USER DOCUMENTATION. OPENING THE PACKAGE(S) OR USING THE ASCEND SWITCH(ES) CONTAINING THE PROGRAM WILL INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, ASCEND IS UNWILLING TO LICENSE THE PROGRAM TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE PROGRAM WITHIN TEN (10) DAYS FROM SHIPMENT TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR LICENSE FEE WILL BE REFUNDED. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE PROGRAM BETWEEN YOU AND ASCEND, AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION OR UNDERSTANDING BETWEEN THE PARTIES.

1. License Grant. Ascend hereby grants to you, and you accept, a non-exclusive, non-transferable license to use the computer software, including all patches, error corrections, updates and revisions thereto in machine-readable, object code form only (the “Software”), and the accompanying User Documentation, only as authorized in this License Agreement. The Software may be used only on a single computer owned, leased, or otherwise controlled by you; or in the event of inoperability of that computer, on a backup computer selected by you. You agree that you will not pledge, lease, rent, or share your rights under this License Agreement, and that you will not, without Ascend’s prior written consent, assign or transfer your rights hereunder. You agree that you may not modify, reverse assemble, reverse compile, or otherwise translate the Software or permit a third party to do so. You may make one copy of the Software and User Documentation for backup purposes. Any such copies of the Software or the User Documentation shall include Ascend’s copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the Program or any portions thereof may be made by you or any person under your authority or control.

2. Ascend’s Rights. You agree that the Software and the User Documentation are proprietary, confidential products of Ascend or Ascend's licensor protected under US copyright law and you will use your best efforts to maintain their confidentiality. You further acknowledge and agree that all right, title and interest in and to the Program, including associated intellectual property rights, are and shall remain with Ascend or Ascend's licensor. This License Agreement does not convey to you an interest in or to the Program, but only a limited right of use revocable in accordance with the terms of this License Agreement.

3. License Fees. The license fees paid by you are paid in consideration of the license granted under this License Agreement.

4. Term. This License Agreement is effective upon your opening of the package(s) or use of the switch(es) containing Software and shall continue until terminated. You may terminate this License Agreement at any time by returning the Program and all copies or portions thereof to Ascend. Ascend may terminate this License Agreement upon the breach by you of any term hereof. Upon such termination by Ascend, you agree to return to Ascend the Program and all copies or portions thereof. Termination of this License Agreement shall not prejudice Ascend's rights to damages or any other available remedy.

5. Limited Warranty. Ascend warrants, for your benefit alone, for a period of 90 days from the date of shipment of the Program by Ascend (the "Warranty Period") that the program diskettes in which the Software is contained are free from defects in material and workmanship. Ascend further warrants, for your benefit alone, that during the Warranty Period the Program shall operate substantially in accordance with the User Documentation. If during the Warranty Period, a defect in the Program appears, you may return the Program to the party from which the Program was acquired for either replacement or, if so elected by such party, refund of amounts paid by you under this License Agreement. You agree that the foregoing constitutes your sole and exclusive remedy for breach by Ascend of any warranties made under this Agreement. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE PROGRAM IS LICENSED "AS IS", AND ASCEND DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTIES OF NONINFRINGEMENT.

6. Limitation of Liability. Ascend's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this License Agreement shall not exceed the greater of: (i) ten thousand US dollars ($10,000) or (ii) the total license fee paid to Ascend for the use of the Program. In no event shall Ascend be liable for any indirect, incidental, consequential, special, punitive or exemplary damages or lost profits, even if Ascend has been advised of the possibility of such damages.

7. Proprietary Rights Indemnification. Ascend shall at its expense defend you against and, subject to the limitations set forth elsewhere herein, pay all costs and damages made in settlement or awarded against you resulting from a claim that the Program as supplied by Ascend infringes a United States copyright or a United States patent, or misappropriates a United States trade secret, provided that you: (a) provide prompt written notice of any such claim, (b) allow Ascend to direct the defense and settlement of the claim, and (c) provide Ascend with the authority, information, and assistance that Ascend deems reasonably necessary for the defense and settlement of the claim. You shall not consent to any judgment or decree or do any other act in compromise of any such claim without first obtaining Ascend's written consent. In any action based on such a claim, Ascend may, at its sole option, either: (1) obtain for you the right to continue using the Program, (2) replace or modify the Program to avoid the claim, or (3) if neither (1) nor (2) can reasonably be effected by Ascend, terminate the license granted hereunder and give you a prorata refund of the license fee paid for such Program, calculated on the basis of straight-line depreciation over a five-year useful life. Notwithstanding the preceding sentence,

Ascend will have no liability for any infringement or misappropriation claim of any kind if such claim is based on: (i) the use of other than the current unaltered release of the Program and Ascend has provided or offers to provide such release to you for its then current license fee, or (ii) use or combination of the Program with programs or data not supplied or approved by Ascend to the extent such use or combination caused the claim.

8. Export Control. You agree not to export or disclose to anyone except a United States national any portion of the Program supplied by Ascend without first obtaining the required permits or licenses to do so from the US Office of Export Administration, and any other appropriate government agency.

9. Governing Law. This License Agreement shall be construed and governed in accordance with the laws and under the jurisdiction of the Commonwealth of Massachusetts, USA. Any dispute arising out of this Agreement shall be referred to an arbitration proceeding in Boston, Massachusetts, USA by the American Arbitration Association.

10. Miscellaneous. If any action is brought by either party to this License Agreement against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorneys' fees and expenses of arbitration. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

Contents

List of Figures

List of Tables

About This Guide

The *NavisXtend Fault Server User's Guide* describes how to use the Fault Server to view and manage Simple Network Management Protocol (SNMP) traps in an Ascend switch network. The *NavisXtend Fault Server User's Guide* is a task-oriented guide that describes, step-by-step, the process for installing, configuring, and using the Fault Server.

What You Need to Know

This guide is intended for the following types of users.

System Operator

The guide is intended for system operators who will use the Fault Server application to view and manage traps. As a system operator, you should have a working knowledge of network management in an Ascend network. You should be familiar with Web-based applications and know how to use a mouse.

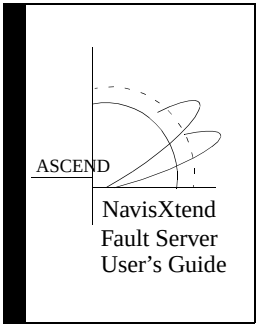
System Administrator

The guide is intended for the system administrator responsible for installing and setting up the Fault Server. As a system administrator, you should have a working knowledge of network management in an Ascend network. This guide assumes that you have installed the Ascend switch hardware. You need to be knowledgeable about UNIX operating system commands and of relational database software to properly maintain Sybase.

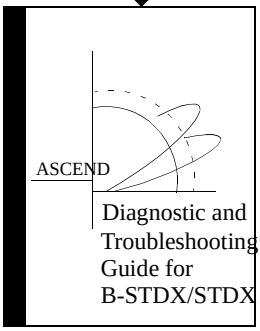
Documentation Reading Path

Before you read this guide, read the *Software Release Notes for NavisXtend Fault Server (SRN)* that accompanies the software. The SRN will alert you to any documentation updates or special conditions that you should be aware of.

The complete document set for the NavisXtend Fault Server includes the following manuals:

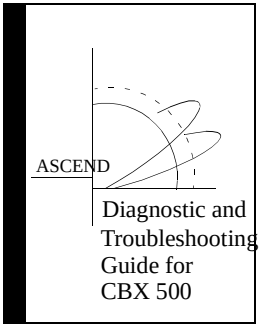


This guide describes how to install, configure, and use the Fault Server. In addition, this guide describes how to use the Fault Server application to view and manage traps.



After installing and configuring the Fault Server, use this guide as a reference when monitoring and troubleshooting your B-STDX/STDX network.

OR



After installing and configuring the Fault Server, use this guide as a reference when monitoring and troubleshooting your CBX 500 network.

How to Use This Guide

The following table summarizes the information contained in this guide.

Read	To Learn About
Chapter 1	General aspects of the Fault Server and the Fault Server application and how they interact with other components on the network.
Chapter 2	Prerequisites for each of the components of the system, including the server, client, and switch requirements.
Chapter 3	The steps involved in installing each of the components of the system, including Sybase, the Fault Server, and the Web Server components.
Chapter 4	The steps involved in configuring the system, including switches to be included in the Fault Server system and configuring the Fault Server to execute a UNIX script.
Chapter 5	How to start and exit the Fault Server application and how to use the application to configure the Fault Server.
Chapter 6	How to use the Fault Server application to manage alarms, events, and traps.
Appendix A	Fault Server reference information, including event, alarm, and rule mappings available for the Fault Server, and variables in the Fault Server MIB database.
Appendix B	Sybase and Fault Server component installation worksheets.
Appendix C	Fault Server un-installation procedures.

What's New in This Guide?

This guide documents the first release of the Fault Server product.

Related Documents

The following related Ascend documentation may be useful to reference.

- *Diagnostic and Troubleshooting Guide for B-STDX/STDX* (product code 80018)
- *Diagnostic and Troubleshooting Guide for CBX 500* (product code 80050)

Conventions

This guide uses the following conventions to emphasize certain information, such as user input, screen options and output, and menu selections. For example:

Convention	Indicates	Example
`Courier Bold`	User input on a separate line.	**`eject cdrom`**
[*bold italics*]	Variable parameters to enter.	**[*your IP address*]**
`Courier Normal`	Output from a program to the screen	`Please wait ...`
Boldface	User input in text.	Type **cd install** and press Return.
Menu ⇒ Option	Select an option from the menu.	CascadeView ⇒ Logon
Black border surrounding text	Notes and warnings.	See examples below.
Italics	File names, path names, directories, book titles, new terms, and emphasized text.	*Network Management Station Installation Guide*

Provides helpful suggestions or reference to materials not contained in this manual.

Warns the reader to proceed carefully in order to avoid equipment damage or personal harm.

1

Fault Server Overview

The NavisXtend Fault Server product provides fault management processing of Simple Network Management Protocol (SNMP) trap information between Ascend switches and user applications. User applications include the Fault Server application and other management platforms and applications, such as help desk applications and trouble-ticket systems.

A *trap* is real-time information that represents a pre-defined event occurring on the switch. An event can indicate a problem, such as a physical port failure, a failed login attempt, or a performance problem. Or, an event can indicate other dynamic information about network activity, such as a network component being brought down by a system administrator, or a threshold level being exceeded.

A trap can trigger an *alarm*, which is a message that notifies an operator or administrator of a network problem. A variety of traps for alarm indications or statistics logging are available for all objects in the Ascend network, including switches, trunks, physical ports, logical ports, and permanent virtual circuits (PVCs).

The Fault Server collects and stores traps in a database. Users can query the database to view the fault information that they are interested in, and obtain information related to each trap, including correlated alarm message, alarm aging, alarm severity, and other information.

The Fault Server provides an simple mechanism for trap reporting. It enables filtering of traps so that user applications can receive only the events that they require, such as the traps that result in a failure condition. The Fault Server provides a central repository and retrieval mechanism to obtain traps across an Ascend network based on specific filter criteria.

The Fault Server does not control the generation of traps or the setting of alarm thresholds from the switch. It does, however, generate traps for alarm forwarding and trap forwarding.

Client-Server Architecture

The Fault Server is based on a client-server network management architecture:

The Fault Server — The server is an intelligent agent that provides fault management processing of switch trap information. Multiple Fault Servers can reside on the network, each responsible for one or more switches.

The Client — The client is an application that displays information about alarms, events, and traps. The client could be a management platform or application, such as a help desk application or trouble-ticket system. Or, the client could be the Fault Server application, which is accessible through a Java-enabled Web browser. The Fault Server application actively generates requests to the server to display information about alarms, events, and traps, as well as server configuration information.

The application runs on a workstation and interacts with a Fault Server. The Fault Server collects traps from Ascend switches, processes the traps, stores them in a Sybase database, and passes information to the application. In the case of the Fault Server application, the server responds to client requests to display information from its database. While there can be multiple instances of the client and the Fault Server running on the network, any client typically interacts with only one Fault Server at a time.

Because the Fault Server uses information stored in the CascadeView database, the server should reside in the same subnetwork as CascadeView/UX and the CascadeView database. The CascadeView database must contain information about the Ascend switches in the network.

Figure 1-1 shows the relationship among the Fault Server, the Fault Server client, other clients, and network devices (switches) on the network.

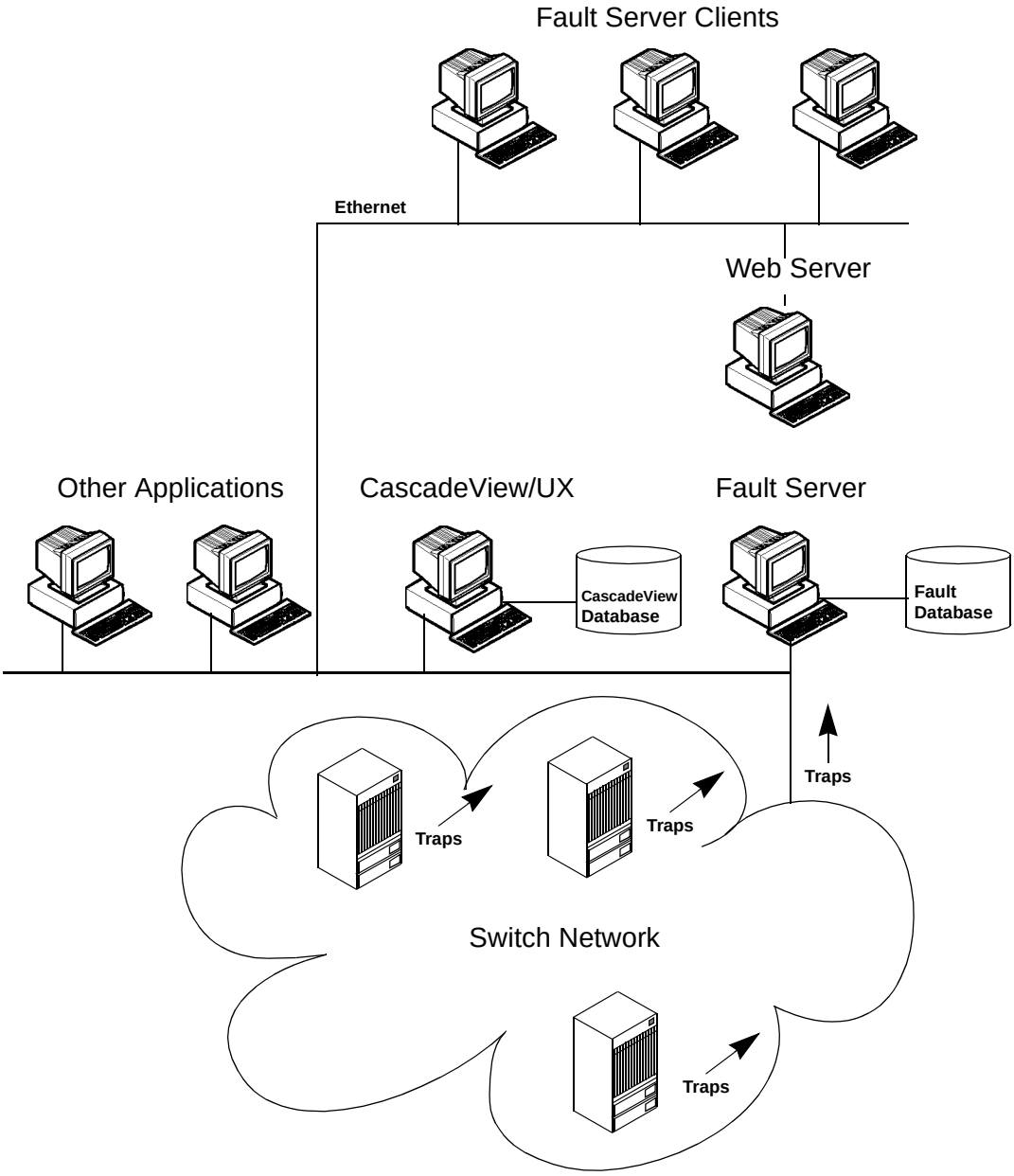


Figure 1-1. Components in the Fault Server System

The configuration illustrated in Figure 1-1 represents one of several possible system configurations. The Fault Server system allows several components to be located on either the same machine or on separate machines. For details on system configuration and installation, refer to Chapter 3.

Fault Server

The Fault Server collects, processes, and stores traps in its Sybase database. As part of the processing, the server applies incoming traps to a set of filters (maps) that determine whether the trap will traverse from a *trap* to an *event* to an *alarm*:

Figure 1-2. Processing Flow of Traps

Only a trap that meets the criteria specified by a particular event map becomes an *event*. The map specifies which traps become events:

- Traps of a particular type
- Traps that contain particular variables

In the same way, only an event that meets the criteria specified by a particular alarm map becomes an *alarm*.

In addition, event maps can be used to select events that do not originate as traps. This feature supports future network management scenarios, where events may be generated from a number of sources, including those that do not generate SNMP traps.

For a list of which traps become which events and which events become which alarms, refer to “Event, Alarm, and Rule Mappings” on page A-1. Trap processing occurs in a series of phases; each phase is handled by its own processor:

Trap Collector — Collects and forwards traps.

Event Processor — Maps traps to events.

Alarm Processor — Maps events to alarms.

Rule Processor — Applies alarms to a set of rules, which specify what action to take on each alarm.

Figure 1-3 shows how these Fault Server components process traps.

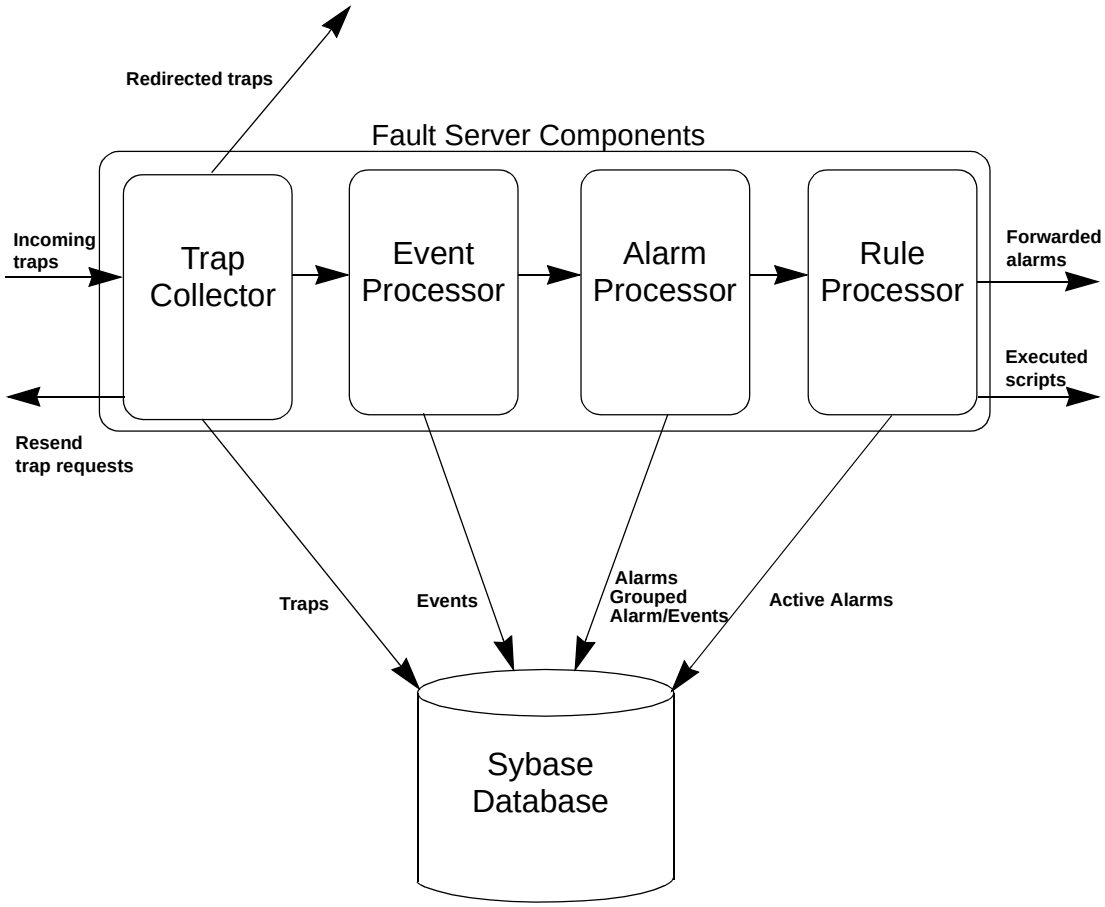


Figure 1-3. Fault Server Processors

Each of these components is described in detail in the sections that follow.

Trap Collector

The Fault Server's Trap Collector component collects and forwards incoming traps.

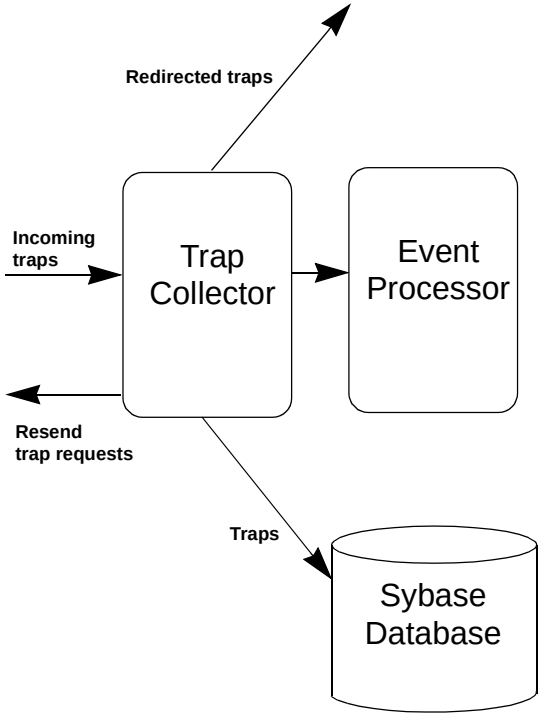


Figure 1-4. The Trap Collector

Specifically, the Trap Collector performs the following tasks:

- Buffers incoming traps
- Processes traps
- Redirects traps
- Requests a trap to be resent from a switch

Trap Buffering

The Trap Collector buffers incoming traps so that no traps are lost during high rate periods. For example, when a problem occurs on a network, many traps can be generated. When the Trap Collector receives more traps than it can process, it stores the overflow on a queue that it can process later. The queue can hold a very large number of traps without dropping any. The queue's size is limited only by the amount of available memory on the machine.

Trap Processing

The Trap Collector processes traps in the order in which they arrive (or were buffered on the queue). In the case of reliable traps, the Trap Collector looks at the sequence number of each trap to ensure that it receives all incoming traps. *Reliable traps* are traps that originate from a switch that maintains a buffer of outgoing traps and can resend any trap that was lost before it reached its destination.

The Trap Collector stores information about each trap in its Sybase database, including the trap source (the switch component that generated the trap), the time at which the trap occurred, and the SNMP trap itself.

The Trap Collector forwards specific information about each trap to the Event Processor. The Event Processor uses this information to apply the trap to a set of event maps. For more information, refer to "Event Processor" on page 1-9.

You can configure the Fault Server to disable database storage and forwarding of traps to the Event Processor. You can also configure the Fault Server to forward traps to other NMS applications or other Fault Servers. A Fault Server configured this way functions as a forwarding server. For details, refer to "Configuring the Fault Server" on page 5-5.

Trap Redirecting

The Trap Collector redirects traps to other locations. This function allows the Fault Server to act as a single point of contact for one or more switches, redirecting traps to other NMS applications or other Fault Servers. Trap redirecting is performed by applying each trap to a set of filters (maps) to determine if and where the trap should be redirected. Only a trap that meets the criteria specified by a particular map is redirected to a particular IP address. For more information, refer to “Configuring Alarm Forwarding” on page 5-11.

Requesting a Trap be Resent

The Trap Collector looks at the sequence number of reliable traps to ensure that it receives all incoming traps. If the Trap Collector determines that a trap was dropped, it can request that the trap be resent from the switch. As long as the switch supports reliable traps and still has the trap in its buffer, the switch can resend the trap.

For more information on configuring reliable traps, refer to “Enabling or Disabling Reliable Traps” on page 5-10.

Event Processor

The Fault Server Event Processor component maps traps to events.

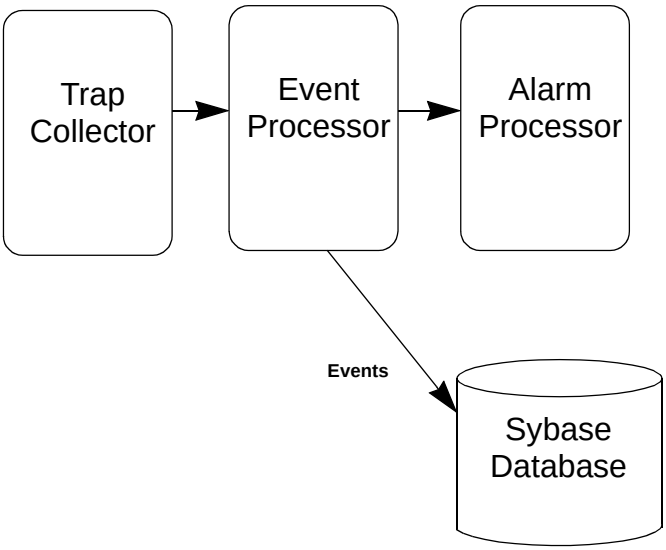


Figure 1-5. The Event Processor

Mapping Traps to Events

The Event Processor applies each trap to a set of event maps to determine if the trap should become an event. Only a trap that meets the criteria specified by a particular map becomes an event. Each event is stored in the Sybase database and forwarded to the Alarm Processor.

More than one event can be generated from a single trap.

For a list of which traps become which events, refer to “Event, Alarm, and Rule Mappings” on page A-1.

Alarm Processor

The Fault Server Alarm Processor component maps events to alarms.

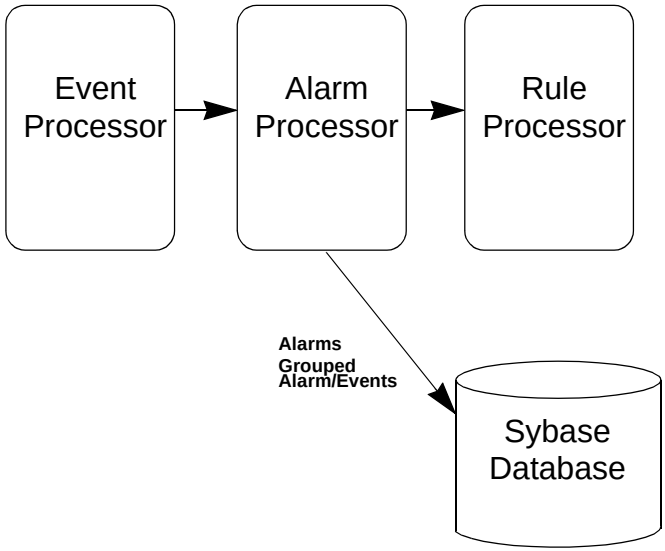


Figure 1-6. The Alarm Processor

The Alarm Processor supports single alarms and *group alarms*. Group alarms are groups of events that form a single alarm. Their purpose is to correlate events and allow them to cause a single alarm condition. For example, if a PPort keeps changing state from up to down, and distinct events are created each time the state goes up or comes down, a single alarm could be created that would alert an administrator that the physical port is unsettled and its state keeps changing.

Alarms have an associated severity value:

1. **Critical** — Alarm is considered critical.
2. **Major** — Alarm is considered major.
3. **Minor** — Alarm is considered minor.
4. **Warning** — Alarm is considered a warning.
5. **Indeterminate** — Alarm's severity level has not been determined.
6. **Cleared** — Alarm was closed by the system or the system administrator.

For a list of what severity value is assigned each alarm, refer to “Event, Alarm, and Rule Mappings” on page A-1.

Mapping Events to Alarms

The Alarm Processor applies each event to a set of alarm maps to determine if the event should become an alarm. Only an event that meets the criteria specified by a particular map becomes an alarm. Alarm maps support groups of events forming a single alarm.

More than one alarm can be generated from a single event. Whenever an alarm is created, it does not become active until after the Rule Processor determines that the generated alarm passes all the rule tests and therefore should be displayed to the administrator.

Single alarms and group alarms are stored in the Sybase database. In the case of a group alarm, both the alarm and its associated events are stored in the database. Single alarms and group alarms are forwarded to the Rules Processor.

For a list of which event becomes which alarm, refer to “Event, Alarm, and Rule Mappings” on page A-1.

Rule Processor

The Fault Server Rule Processor component applies alarms to a set of rules, which specifies what action to take on each alarm.

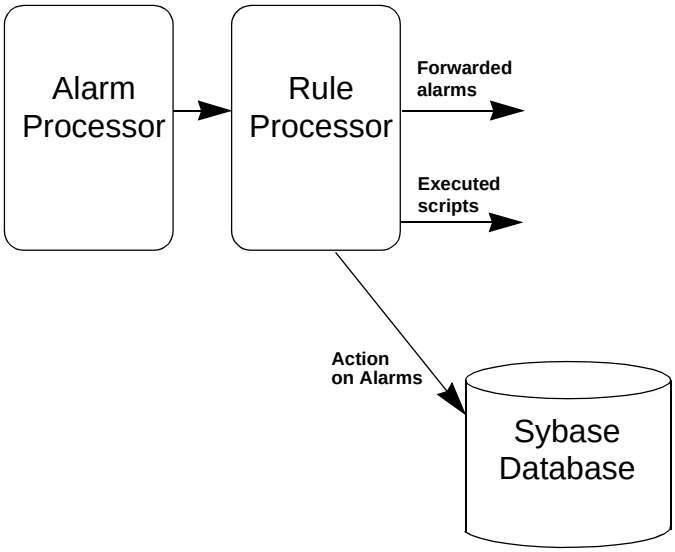


Figure 1-7. The Rule Processor

Specifically, the Rule Processor performs the following tasks:

- Applies alarms to a set of rules
- Executes scripts
- Forwards alarms

Applying Alarms to a Set of Rules

The Rule Processor applies each alarm to a set of rules to determine what action to take on the alarm. If there are no rules applied to the alarm, the alarm is immediately sent to archive. If there are rules that apply to the alarm, the rules are invoked. The applied rules may cause the alarm to be closed, held, or subjected to some other such action. Once an alarm passes through the rules, the alarm then becomes active.

Table 1-1 shows the actions supported by the Rule Processor.

Table 1-1. Rule Processor Actions

Action	Description
Close	Causes the alarm to remove and suppress other alarms. Removes alarms that have previously been displayed and suppresses future alarms from being displayed. Affects alarms directly, not recursively. For example, Alarm X closes Alarm Y. Alarm Y closes Alarm Z. When Alarm X occurs, it removes previous Y Alarms and suppresses future Y Alarms. However, it does not remove or suppress any Z Alarms. Keep in mind that an alarm can affect other alarms only while it is still open. Once an alarm is closed, it can no longer close other alarms.
Cancel	Causes the alarm to remove and suppress other alarms. Removes alarms that have previously been displayed and suppresses future alarms from being displayed. Affects alarms recursively. For example, Alarm X cancels Alarm Y. Alarm Y cancels Alarm Z. When Alarm X occurs, it removes previous Y and Z Alarms and suppresses future Y and Z Alarms. An alarm can affect other alarms only while it is still open. Once an alarm is closed, it can no longer cancel other alarms.

Table 1-1. Rule Processor Actions (Continued)

Action	Description
Clear	Causes the alarm to suppress other alarms received after the specified alarm and and to place other alarms on hold. Suppresses only alarms that have not been displayed. Suppresses alarms recursively. For example, Alarm X clears Alarms Y. Alarm Y clears Alarm Z. When Alarm X occurs, it suppresses future Y and Z Alarms. An alarm can affect other alarms only while it is still open. Once an alarm is closed, it can no longer clear other alarms.
Hold	Holds the alarm for a specified time interval (in seconds) before displaying it. The purpose of this rule is to permit other rules (such as Cancel or Clear) to take action before the alarm is displayed.

For a list of what rule action(s) are taken on behalf of each alarm, refer to “Event, Alarm, and Rule Mappings” on page A-1.

Script Execution

Once an alarm successfully passes through the rules, a user-defined UNIX script can be executed. An example of a script could be one that informs a trouble-ticket application or paging system about the alarm.

For details on how to configure the Fault Server to execute a UNIX script, refer to “Executing Scripts” on page 4-6.

Alarm Forwarding

The Rule Processor forwards alarms to other locations using traps. Although the Rule Processor uses traps to forward the alarms, it uses Alarm Forwarding (not Trap Forwarding) to do so. This function allows the Fault Server to act as a single point of contact for one or more switches, forwarding alarms to other NMS applications or other Fault Servers. Alarm forwarding is performed by applying each alarm to a set of filters (maps) to determine if and where the alarm should be forwarded. Only an alarm that meets the criteria specified by a particular map is redirected to a particular IP address.

Fault Server Management

This section presents several examples that illustrate how the Fault Server components interact in response to traps occurring in the switch network.

Example 1: PPort Goes Down

In this example, a PPort goes down in the Ascend network. The Fault Server system handles this network event by performing a series of actions. Figure 1-8 shows the processing flow of the event through the components of the Fault Server system.

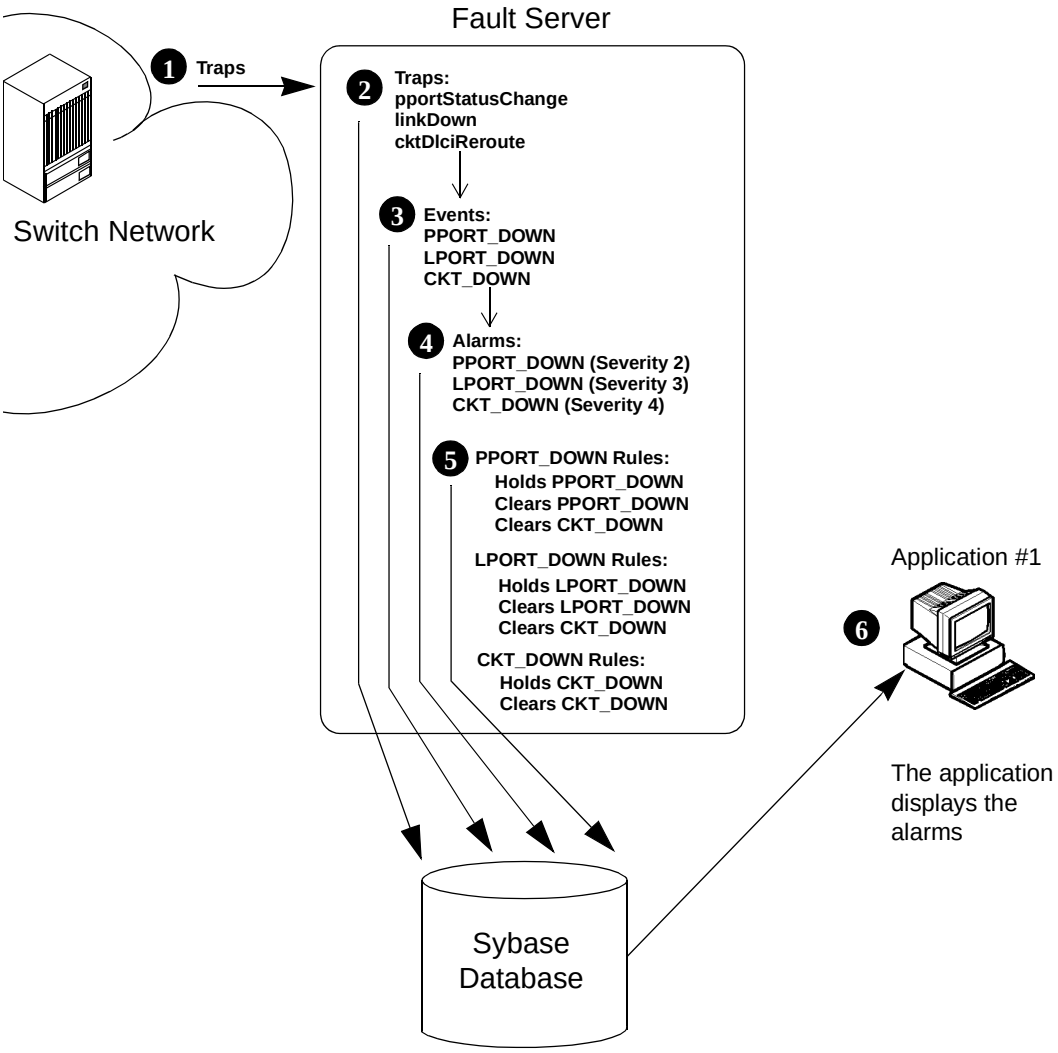


Figure 1-8. PPort Down Example

When the PPort goes down, the following steps occur:

Step 1. The switch generates several SNMP traps, including pportStatusChange traps and corollary linkDown and cktDlciReroute traps.

Step 2. The Fault Server that manages the switch receives the traps and stores them in the trap log of its Sybase database.

Step 3. The Fault Server applies each trap to a set of event maps to determine if the trap should become an event. Each trap meets the map criteria, so the Fault Server opens a PPORT_DOWN event, an LPORT_DOWN event, and a CKT_DOWN event and stores each event in the event log of its Sybase database.

Step 4. The Fault Server applies each event to a set of alarm maps to determine if the event should become an alarm. Each event meets the map criteria, so the Fault Server opens an alarm for each and gives each a severity level. The PPORT_DOWN alarm is given severity 2, the LPORT_DOWN alarm is given severity 3, and the CKT_DOWN alarm is given severity 4. The Fault Server stores each alarm in the alarm log of its Sybase database.

Step 5. The Fault Server applies each alarm to a set of rules that take action on the alarms:

PPORT_DOWN rules:

- Hold rule places the PPORT_DOWN alarm on hold for 60 seconds.
- Clear rule clears any future PPORT_DOWN alarms.
- Clear rule clears any future CKT_DOWN alarms.

LPORT_DOWN rules:

- Hold rule places the LPORT_DOWN alarm on hold for 60 seconds.
- Clear rule clears any future LPORT_DOWN alarms.
- Clear rule clears any future CKT_DOWN alarms.

CKT_DOWN rules:

- Hold rule places the CKT_DOWN alarm on hold for 60 seconds.
- Clear rule clears any future CKT_DOWN alarms.

Step 6. Fault Server application #1 has requested to be notified of all open alarms from the Fault Server. It receives information about the open PPORT_DOWN and LPORT_DOWN alarms, but not the cleared CKT_DOWN alarm.

Example 2: PPort Comes Back Up

In this example, some time after the PPort goes down in the Ascend network, the PPort comes back up. The Fault Server system handles this network event by performing a series of actions. Figure 1-9 shows the processing flow of the event through the components of the Fault Server system.

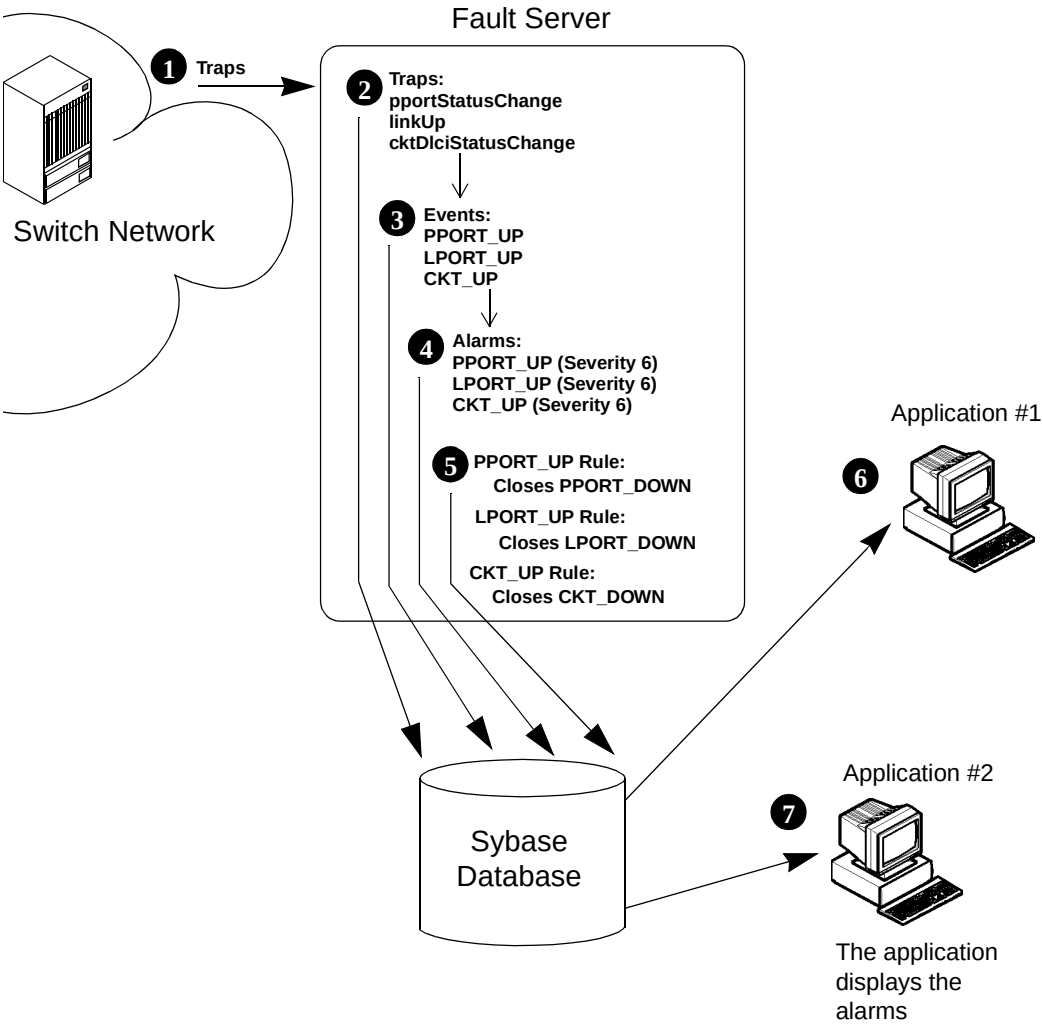


Figure 1-9. PPort Up Example

When the PPort comes back up, the following steps occur:

Step 1. The switch generates several SNMP traps, including pportStatusChange traps and corollary linkUp and cktDlciStatusChange traps.

Step 2. The Fault Server that manages the switch receives the traps and stores them in the trap log of its Sybase database.

Step 3. The Fault Server applies each trap to a set of event maps to determine if the trap should become an event. Each trap meets the map criteria, so the Fault Server opens a PPORT_UP event, an LPORT_UP event, and a CKT_UP event and stores each event in the event log of its Sybase database.

Step 4. The Fault Server applies each event to a set of alarm maps to determine if the event should become an alarm. Each event meets the map criteria, so the Fault Server opens an alarm for each and gives each a severity of 6 (alarm was closed by the system). The Fault Server stores the new alarms in the alarm log of its Sybase database.

Step 5. The Fault Server applies each alarm to a set of rules to determine what action to take:

PPORT_UP rule:

- Close rule closes any previous or future PPORT_DOWN alarm.

LPORT_UP rule:

- Close rule closes any previous or future LPORT_DOWN alarm.

CKT_UP rule:

- Close rule closes any previous or future CKT_DOWN alarm.

Step 6. Fault Server application #1 has requested to be notified of all open alarms from the Fault Server. The user screen does not list the new PPORT_UP, LPORT_UP, or CKT_UP alarms because they are closed alarms (severity 6). The original PPORT_DOWN alarm is cleared from the user screen because it was closed by the new PPORT_UP alarm.

Step 7. Fault Server application #2 has requested to be notified of both the open and closed alarms from the Fault Server. The user screen lists the original PPORT_DOWN, LPORT_DOWN, and CKT_DOWN alarms, as well as the PPORT_UP, LPORT_UP, and CKT_UP alarms. All alarms are shown as being closed by the system.

Example 3: Bouncing PPort

In this example, a PPort goes down and comes back up more than 30 times within 30 minutes. The Fault Server system handles these network events by performing a series of actions. Figure 1-10 shows the processing flow of the events through the Fault Server system.

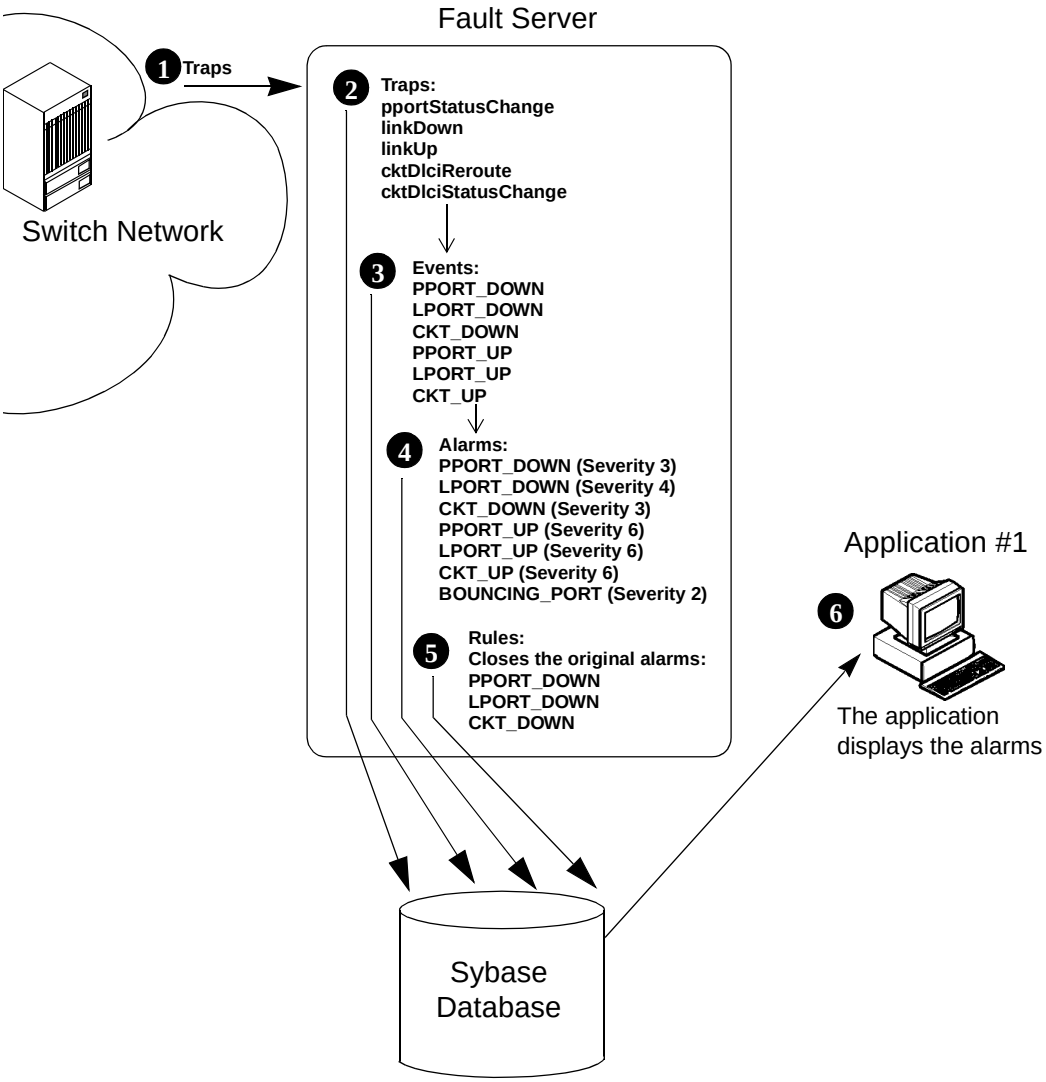


Figure 1-10. Bouncing PPort Example

When the PPort goes down and comes back up more than 30 times within 30 minutes, the following steps occur:

Step 1. The switch generates several SNMP traps, including pportStatusChange, linkDown, linkUp, cktDlciReroute, and cktDlciStatusChange traps.

Step 2. The Fault Server that manages the switch receives the traps and stores them in the trap log of its Sybase database.

Step 3. The Fault Server applies each trap to a set of event maps to determine if the trap should become an event. Each trap meets the map criteria, so the Fault Server opens an event for each and stores it in the event log of its Sybase database.

Step 4. The Fault Server applies each event to a set of alarm maps to determine if the event should become an alarm. Each event meets the map criteria, so the Fault Server opens an alarm for each and gives each a severity level. The Fault Server stores the new alarms in the alarm log of its Sybase database.

Because the PPort goes down and comes back up more than 30 times within 30 minutes, the Fault Server opens a BOUNCING_PPORT alarm, which is a group alarm with severity of 2. The Fault Server stores the new group alarm in the alarm log of its Sybase database.

Step 5. The Fault Server applies each alarm to a set of rules to determine what action to take. Every time the Fault Server stores a new PPORT_UP, LPORT_UP, or CKT_UP alarm in the alarm log, it closes the original PPORT_DOWN, LPORT_DOWN, or CKT_DOWN alarm.

A BOUNCING_PPORT rule clears any future BOUNCING_PPORT alarms. Another BOUNCING_PPORT rule clears any future PPORT_DOWN alarms.

Step 6. Fault Server application #1 has requested to be notified of all open alarms from the Fault Server. It receives information about each new open alarm. On the user screen, several alarms are superseded by new alarms. Specifically, every time a new PPORT_UP, LPORT_UP, or CKT_UP alarm occurs, the original PPORT_DOWN, LPORT_DOWN, or CKT_DOWN alarm is cleared from the user screen. The new PPORT_UP, LPORT_UP, or CKT_UP alarms are not displayed because they have the status closed (severity 6). Once the BOUNCING_PPORT alarm is displayed, future PPORT_DOWN alarms are not displayed on the user screen.

2

System Prerequisites

System Configuration

The Fault Server system prerequisites depend on your actual system configuration. You can install the Web Server and the Fault Server either on the same machine or on separate machines. And, you can install the Fault Server and the Fault Server database on the same or separate machines. The Fault Server application is accessible from a machine running a Java-enabled Web browser that has access to the Web Server. Multiple clients can access the same Web Server.

Table 2-1 specifies the four Fault Server system configurations.

Table 2-1. Fault Server System Configuration Matrix

Config.	Workstation 1	Workstation 2	Workstation 3	Workstation 4
1	Web Server software Fault Server software Sybase (Fault Server database)	CascadeView/UX Sybase (CascadeView database)		
2	Fault Server software Sybase (Fault Server database)	Web Server software	CascadeView/UX Sybase (CascadeView database)	
3	Sybase (Fault Server database and CascadeView database) CascadeView/UX	Fault Server software	Web Server software	
4	Sybase (Fault Server database and CascadeView database)	Fault Server software	Web Server software	CascadeView/UX

For details on system configuration and installation, refer to Chapter 3.

Fault Server Requirements

Ascend recommends using an Ultra 1 workstation, however the minimum workstation requirement for the Fault Server is any Sun SPARCstation, configured with:

- 128 MB onboard memory
- 1 GByte internal disk drive

The minimum software requirements for the Fault Server are as follows:

- Solaris 2.4 or 2.5.1 and any maintenance release patches
- Fault Server software

In addition, the following software must be installed on the network:

- CascadeView/UX, version 2.0 or higher. The Fault Server must be a client of the CascadeView database. For more information, refer to "CascadeView Sybase Server Requirements" on page 2-5.

Fault Server Sybase Server Requirements

The minimum workstation requirement for the Fault Server Sybase Server is a Sun SPARCstation, configured with:

- 128 MB onboard memory
- 3 GByte internal disk drive (2 hard disks)

The actual amount of disk space that you need depends upon the size of the trap, event, and alarms database that the system will maintain. To calculate the size of the database you need, estimate the number of traps you expect the switches to generate. A 400 MByte database is required to maintain the traps, events, and alarms generated from 1,000,000 traps.

The minimum software requirement for the Fault Server Sybase Server are as follows:

- Solaris 2.4 with Sun patch 101945-36 or Solaris 2.5.1 with any maintenance release patches
- Sybase SQL, version 11

Web Server Requirements

The minimum workstation requirement for the Web Server is any Sun SPARCstation.

The minimum software requirements for the Web Server are as follows:

- Ascend Web Server software
- Solaris 2.4 or 2.5.1 and any maintenance release patches

The Web Server is configured to interact with the CascadeView Sybase Server, and thus must be dedicated to Ascend Web products, including the Fault Server. The Web Server cannot be used to maintain other Web systems, such as a corporate Web site.

Fault Server Web Client Requirements

The Fault Server application is accessible from a machine running the Java-enabled Web browser, Netscape Navigator 3.0.1. The machine can be a UNIX machine or a Windows machine running Windows NT or Windows 95.

The Fault Server application is installed on the Web Server. To access the Fault Server application, the Web browser must have access to the Web server. Multiple machines can access the same Web Server.

The following sections describe the requirements for each machine type.

UNIX Workstations

The UNIX machine must be running Solaris 2.4 or 2.5.1 and any maintenance release patches. It must use one of the following windowing systems:

- OpenWindows
- Motif
- CDE (Common Desktop Environment)

It is recommended that the machine use a high-resolution monitor (1024 x 768). The minimum memory requirement for the machine is 64 MB.

For best results, the machine should access the Web Server via an Ethernet connection. Access across a modem connection may be slow.

Windows Workstation

It is recommended that the Windows machine use a high-resolution monitor (1024 x 768). The minimum memory requirement for the machine is 32 MB.

For best results when using the Fault Server application on a Windows machine, use the following recommendations:

- The machine should access the Web Server via an Ethernet connection. Access across a modem connection may be slow.
- When using the Netscape Navigator under Windows:
  - Unmark the setting Options ⇒ Show Location
  - Unmark the setting Options ⇒ Show Directory Buttons
  - Mark the setting Options ⇒ General Preferences ⇒ Appearance ⇒ Show Main Tool Bar as Text

CascadeView Sybase Server Requirements

The minimum workstation requirement for the CascadeView Sybase Server is a Sun SPARCstation.

The minimum software requirement for the CascadeView Sybase Server is CascadeView/UX 2.0 or higher, using Sybase SQL, version 11.

Switch Network Requirements

The switches in the Ascend network can be any of the following revision levels:

- STDX, version 2.3 or greater
- B-STDX, version 4.0 or greater
- CBX 500, version 1.1 or greater

If you want to use the reliable traps feature of the Fault Server, the switches must support reliable traps (CBX 500, version 2.0 or greater).

The switches must be managed by the CascadeView Sybase Server.

3

Installing the Fault Server System

This chapter describes how to perform a new installation of the various components of the Fault Server system. If you need instructions for upgrading an existing Fault Server system, refer to the *Software Release Notes for NavisXtend Fault Server.*

The sequence of steps that you follow to install the Fault Server system depends on your system configuration. You can install the Web Server and the Fault Server either on the same machine or on separate machines. And, you can install the Fault Server and the Fault Server database on the same or separate machines. For example, you may want to install the Fault Server database on the same machine as the CascadeView database. Keep in mind that the Fault Server database must be dedicated to a single Fault Server; it cannot be shared with other Fault Servers.

The Fault Server application is installed on the Web Server. The application is accessible from a machine running a Java-enabled Web browser that has access to the Web Server. Ascend currently supports Netscape Navigator only. You must obtain and install the browser separately; it does not ship with the Fault Server system.

The Fault Server system components are shown in Figure 3-1.

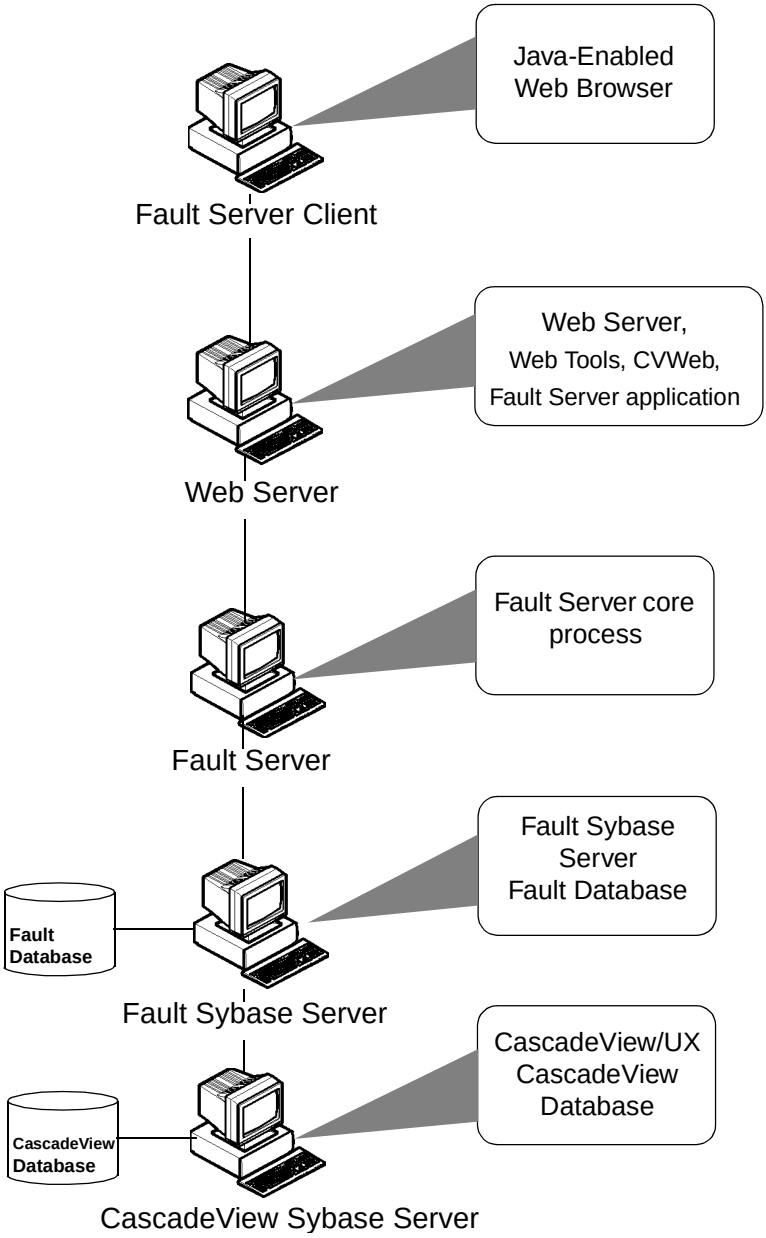


Figure 3-1. Fault Server System Components

The general steps for installing the Fault Server system are shown in Figure 3-2.

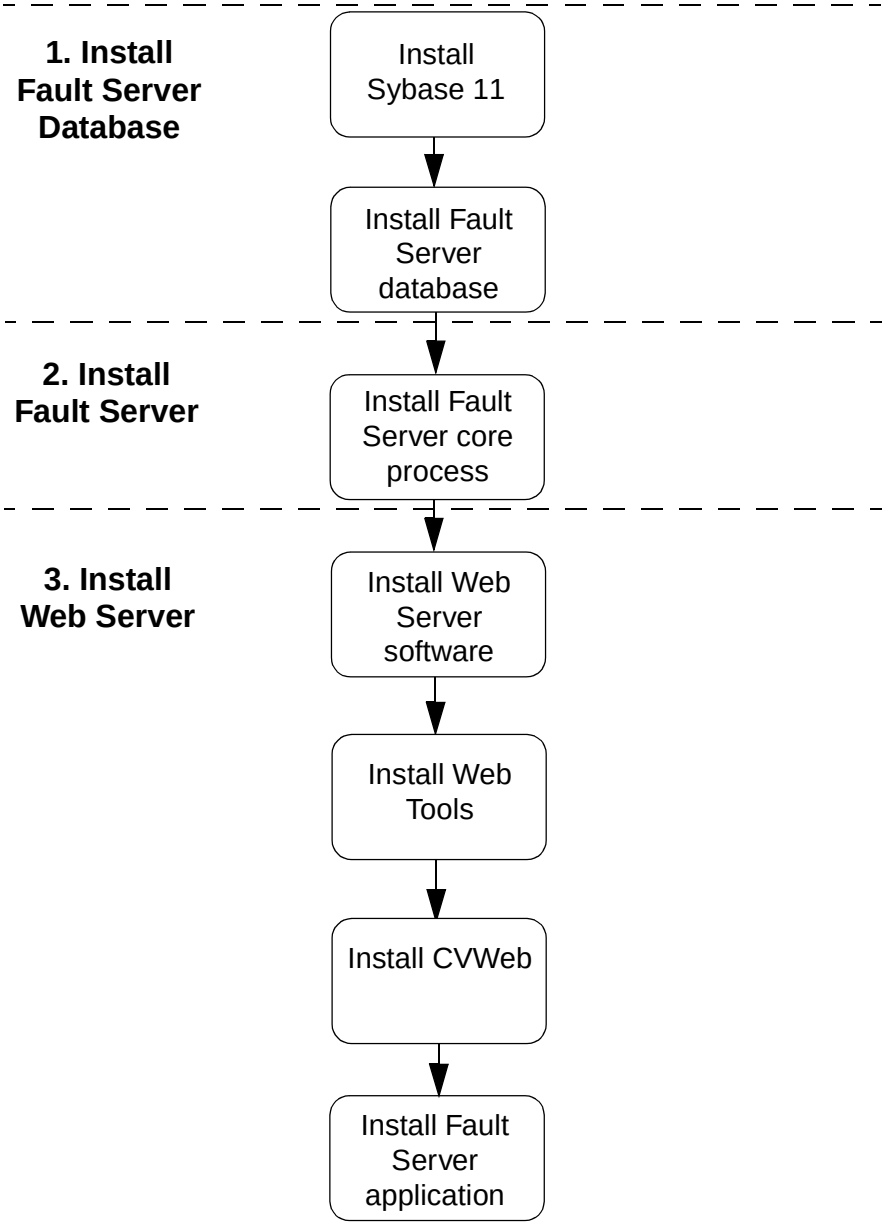


Figure 3-2. Fault Server System Installation Sequence

Using Software Package Tools

To install the Fault Server and the Web Server components, you use the UNIX utility called pkgadd. This utility allows you to extract the contents of the software package from the media and install the various components onto the system.

The following list describes the basic pkgadd commands:

- To extract the Fault Server package from media to a particular pathname, enter:

  pkgadd -s *spool-pathname* -d [*media device pathname*]

  where **spool-pathname** is the path where you want the packages stored and **media device pathname** is the media device pathname (for example, */cdrom/fltsrvr_1010*).

- To install the Fault Server package from a particular device or pathname, enter:

  pkgadd -d *spool-pathname package-name*

  where **spool-pathname** is the location where the package is stored and **package-name** is the name of the package you want to install.

- To install the Fault Server package directly from media, enter:

  pkgadd -d [*media device pathname*] *package-name*

  where **media device pthaname** is the media device pathname and **package-name** is the name of the package you want to install.

To un-install Fault Server components, you use the UNIX utility called pkgrm. This utility allows you to remove a Fault Server package after or during installation:

pkgrm *package-name*

where **package-name** is the name of the package you want to un-install.

To view information such as version numbers and install dates for the Fault Server package and other packages applications on the system, you use the UNIX utility called pkginfo:

pkginfo -l *package-name*

where **package-name** is the name of the package you want information on.

System Configurations

This section presents four checklists that specify the installation procedures you should follow for the four types of Fault Server system installations. Table 3-1 lists each installation type and indicates the installation checklist that you should use for each type.

Table 3-1. Installation Sequence Checklists

For this type of configuration	Use this checklist
Two workstations: • **Workstation 1** Solaris Sybase (Fault Server database) Fault Server software Web Server software • **Workstation 2** CascadeView/UX Sybase (CascadeView database)	Checklist 1, page 3-7
Three workstations: • **Workstation 1** Solaris Sybase (Fault Server database) Fault Server software • **Workstation 2** Solaris Web Server software • **Workstation 3** CascadeView/UX Sybase (CascadeView database)	Checklist 2, page 3-8

Table 3-1. Installation Sequence Checklists (Continued)

For this type of configuration	Use this checklist
Three workstations: • **Workstation 1** Solaris Sybase (Fault Server database and CascadeView database) CascadeView/UX • **Workstation 2** Solaris Fault Server software • **Workstation 3** Solaris Web Server software	Checklist 3, page 3-9
Four workstations: • **Workstation 1** Solaris Sybase (Fault Server database and CascadeView database) • **Workstation 2** Solaris Fault Server software • **Workstation 3** Solaris Web Server software • **Workstation 4** CascadeView/UX	Checklist 4, page 3-10

Checklist 1: Two-System Installation Sequence

In this configuration, the Fault Server software and Web Server software are located on one machine (see Figure 3-3).

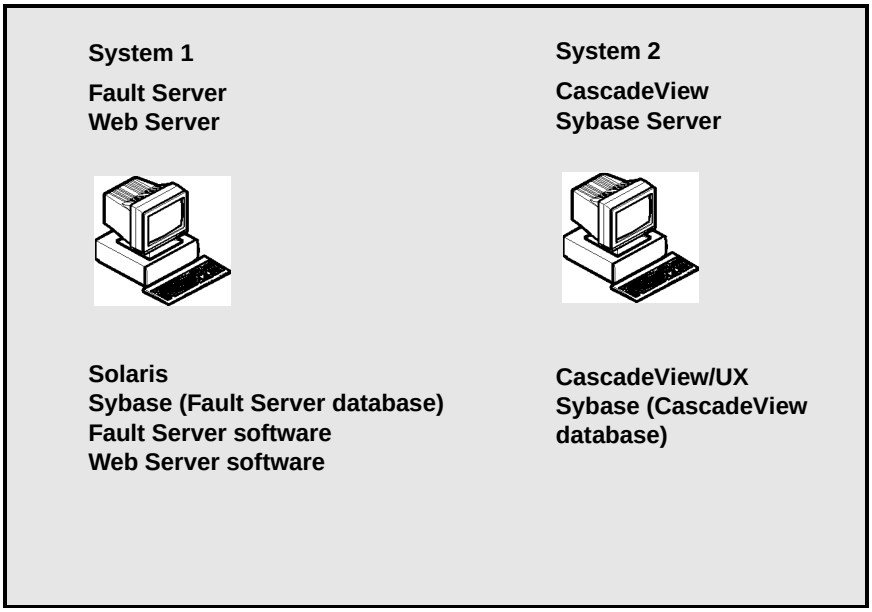


Figure 3-3. Installation Configuration 1

- ☑ Install CascadeView/UX and all CascadeView/UX required software components on system 2 by following the instructions in the *Network Management Station Installation Guide.*
- ☑ Install Solaris on system 1.
- ☑ Install the Sybase Fault Server database on system 1.
- ☑ Install the Fault Server core process on system 1.
- ☑ Install the Web Server software on system 1.

Checklist 2: Three-System Installation Sequence

In this configuration, the Fault Server software and the Web Server software are located on separate machines (see Figure 3-4).

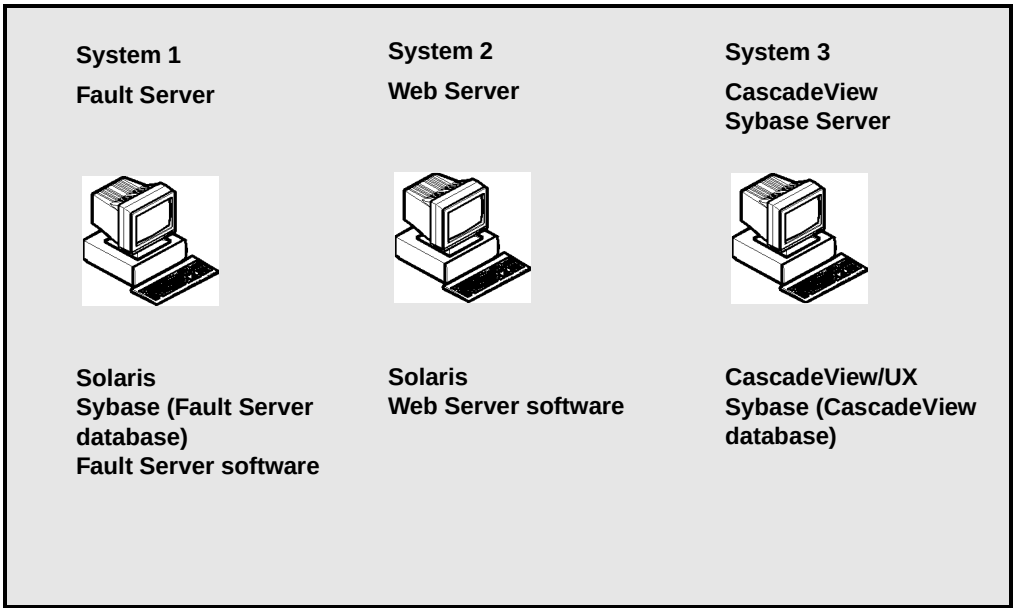


Figure 3-4. Installation Configuration 2

- ☑ Install CascadeView/UX and all CascadeView/UX required software components on system 3 by following the instructions in the *Network Management Station Installation Guide.*
- ☑ Install Solaris on system 1.
- ☑ Install the Sybase Fault Server database on system 1.
- ☑ Install the Fault Server core process on system 1.
- ☑ Install Solaris on system 2.
- ☑ Install the Web Server software on system 2.

Checklist 3: Three-System Installation Sequence

Like configuration 2, this configuration uses three systems. In this configuration, the Fault Server database, the CascadeView database, and CascadeView/UX are located on the same machine (see Figure 3-5). Keep in mind that the Fault Server database in System 1 must be dedicated to the Fault Server in System 2.

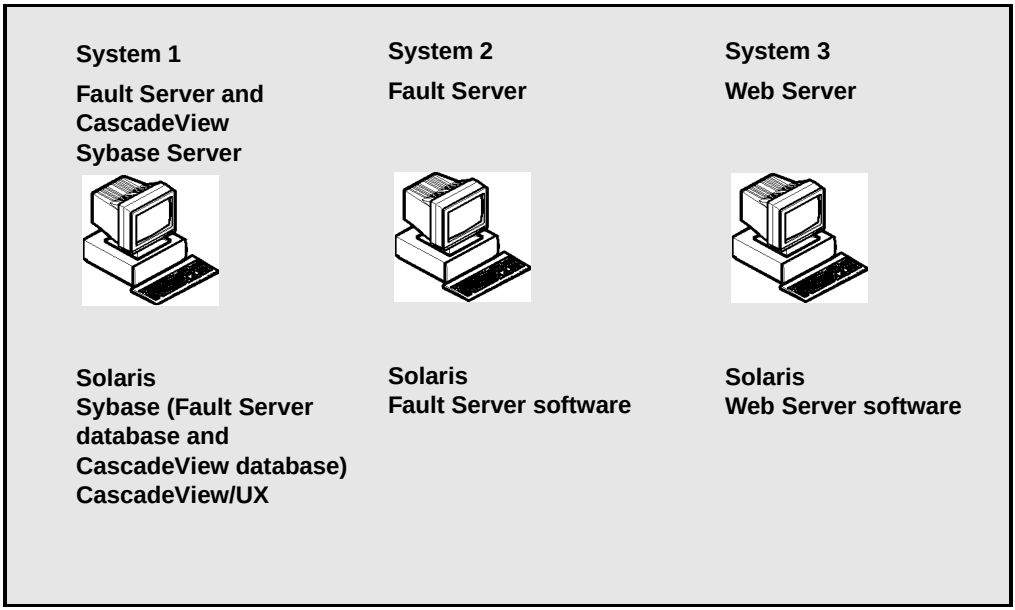


Figure 3-5. Installation Configuration 3

- ☑ Install CascadeView/UX and all CascadeView/UX required software components on system 1 by following the instructions in the *Network Management Station Installation Guide.*
- ☑ Install the Sybase Fault Server database on system 1.
- ☑ Install Solaris on system 2.
- ☑ Install the Fault Server core process on system 2.
- ☑ Install Solaris on system 3.
- ☑ Install the Web Server software on system 3.

Checklist 4: Four-System Installation Sequence

Like configuration 3, this configuration has the Fault Server database and the CascadeView database located on the same machine (see Figure 3-6). CascadeView/UX is located on a separate machine. Keep in mind that the Fault Server database in System 1 must be dedicated to the Fault Server in System 2.

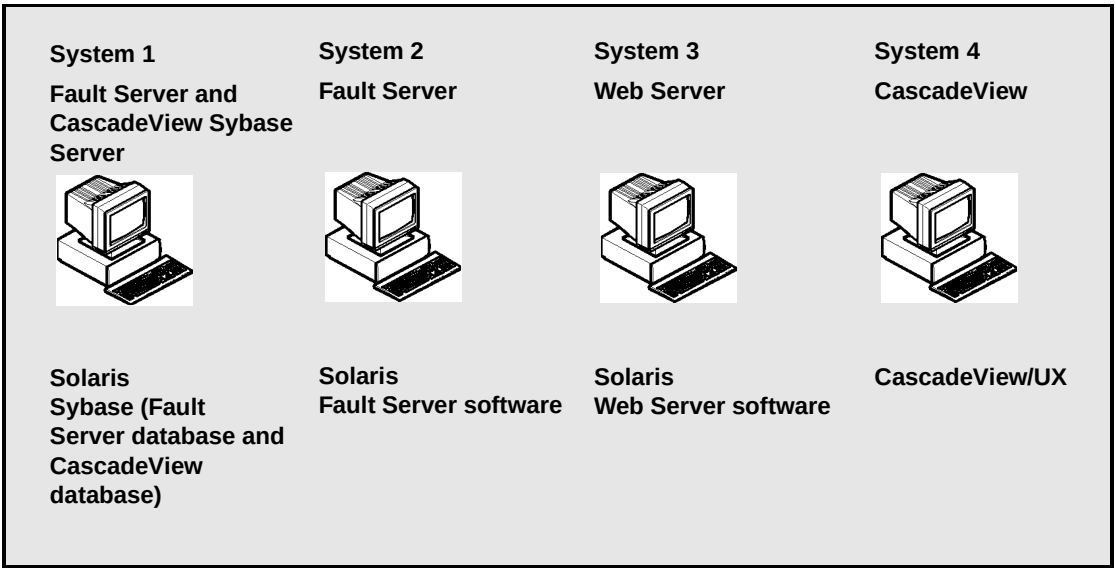


Figure 3-6. Installation Configuration 4

- ☑ Install CascadeView/UX and all CascadeView/UX required software components on system 4 by following the instructions in the *Network Management Station Installation Guide.*
- ☑ Install Solaris on system 1.
- ☑ Install the Sybase CascadeView database on system 1.
- ☑ Install the Sybase Fault Server database on system 1.
- ☑ Install Solaris on system 2.
- ☑ Install the Fault Server core process on system 2.

- ☑ Install Solaris on system 3.
- ☑ Install the Web Server software on system 3.

Fault Server Installation Instructions

This section presents the instructions for installing each of the Fault Server system components. You can install the Fault Server database on an existing CascadeView Sybase server or on a different Sybase server. The procedures to follow vary according to the choice you make.

- To install the Fault Server Database on an existing CascadeView Sybase Server, follow the instructions in "Installing the Fault Server Database on an Existing CascadeView Sybase Server" on page 3-12.
- To install the Fault Server Database on a new Sybase Server, follow the instructions in "Installing the Fault Server Database on a New Sybase Server" on page 3-16.

Before you being any of the installation procedures, complete the Installation Worksheets in Appendix B. The installation script prompts you for worksheet information for completing the following tasks:

- Setting up your system for Sybase 11.
- Installing Sybase 11.
- Installing the other components of the Fault Server system.

The procedures that you follow to install the Fault Server database vary depending on whether you are installing the Fault Server database on an existing CascadeView Sybase server or on a separate Sybase server.

Installing the Fault Server Database on an Existing CascadeView Sybase Server

Complete the following steps to install the Fault Server database on an existing CascadeView Sybase server:

1. On the Fault Server database workstation, verify that you are root. You should see the # prompt. If you are not root, enter **su - root**. At the prompt, enter the root password.

If you are logged in via a remote connection (rlogin/rsh/telnet), set your DISPLAY variable to the value of the local host. Enter the following:

DISPLAY=[local hostname]:0.0
export DISPLAY

(This example uses the Korn shell syntax.)

*In addition, in a new command tool window, run **xhost +** as the user who controls the system console. Executing this command enables you to open the window that displays the installation log.*

2. Insert the Ascend-supplied Sybase media into the media drive.
3. In the command tool window, enter **cd /opt** to move to the */opt* directory.
4. Type **cd cv_scripts** and press Return.
5. Enter the following command to start the Sybase script:

   ```
   ./install_sybase
   ```

   The following message appears:

   ```
   Verifying super user privileges...
   Would you like to view (tail -f) the install log (default=y)?
   ```

   The Tail window allows users to view a log of the installation process.
6. Press Return to accept the default (yes).

The Tail (Installation Log) window appears in front of the Sybase installation window.

7. Move the Tail window behind the Sybase installation window so you can continue with the installation prompts. Whenever necessary, you can refer to the Tail window if you want to see a listing of installation events.

   The installation window now contains the Sybase Installation menu (refer to Figure 3-7).

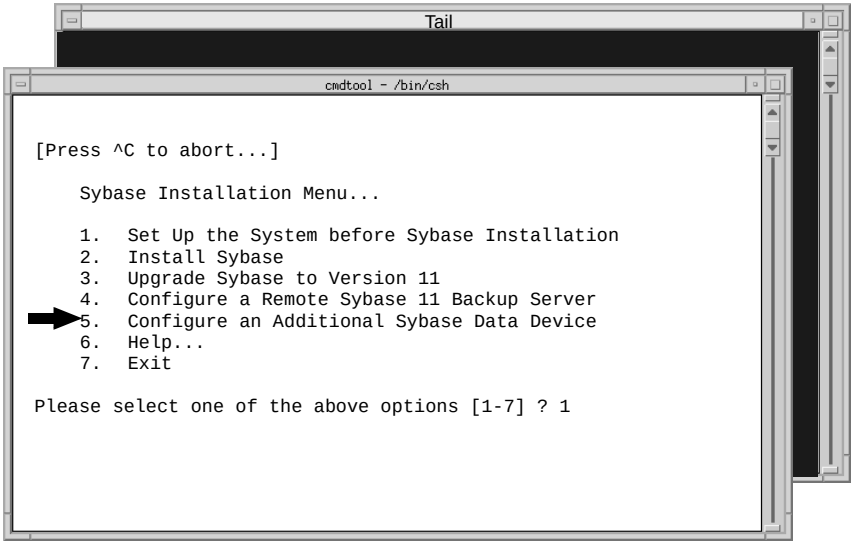


Figure 3-7. Sybase Installation Menu

8. At the Sybase Installation Menu, enter **5** to configure an additional Sybase data device.

   The Device Installation menu appears (refer to Figure 3-8). This menu allows you to define the device that uses the Sybase database.

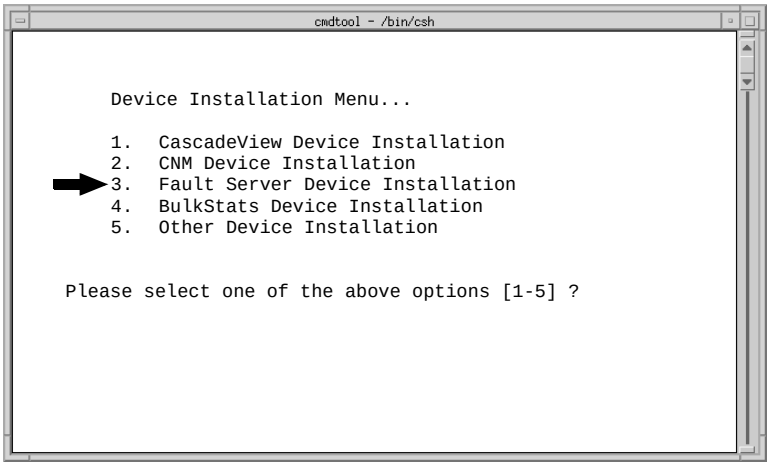


Figure 3-8. Device Installation Menu

9. Enter **3** to select the Fault Server Device Installation.

   The Sybase Information Request menu appears.

10. When prompted for the Sybase install path, do one of the following:

    - Press Return to accept the default of */opt/sybase*.
    - Enter **[*Sybase 11 home directory*]**.

11. When prompted for the database server name, do one of the following:

    - Press Return to accept the default of *CASCADE*.
    - Enter ***[Sybase server name]***.

12. When prompted for the database SA password, do one of the following:

    - Enter the recommended value **superbase**. When prompted again for the password, re-enter the password.
    - Enter **[*database SA password*]**. When prompted again for the password, re-enter the password.

The following menu appears:

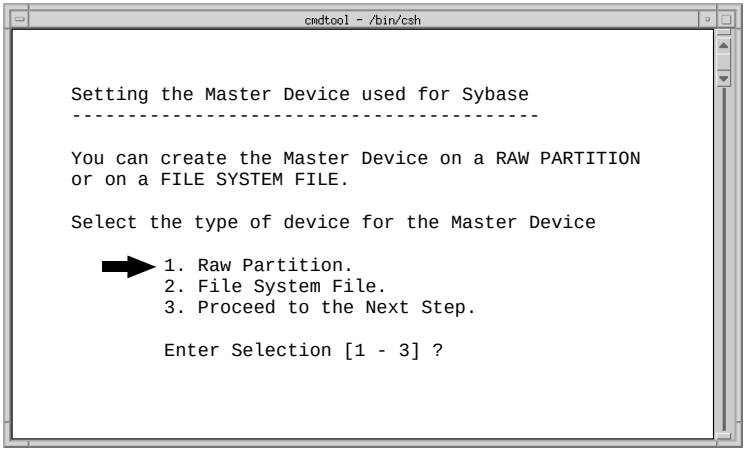


Figure 3-9. Setting the Master Device Used for Sybase Menu

13. At the Setting the Master Device menu, enter **1** to select Raw Partition.

    The following message appears:

    ```
    WARNING: IF YOU INSTALL THE SQL SERVER ON A RAW PARTITION,
    ANY EXISTING FILES ON THAT PARTITION WILL BE OVERWRITTEN.

    Do you wish to continue? [default=y]:
    ```

14. Press Return to continue.

    The following message appears:

    ```
    Setting up Raw Partition Devices
    ---------------------------------
    Enter the Data Device Path Name (e.g. /dev/rdsk/c0t1d0s7):
    ```

15. At the Data Device Pathname prompt, enter the number of the disk partition for the Fault Server database (such as **/dev/rdsk/c0t1d0s7**). Refer to your Sybase Installation Worksheet in Appendix B for the number of the disk partition.

    The Fault Server data device has been created.

The last disk partition should be approximately 1GByte in size, provided that the second disk was partitioned according to the CascadeView installation recommendations in the Network Management Station Installation Guide*.*

16. At the Sybase Installation Menu, enter **7** to exit.
17. You are now ready to install the Fault Server core process. Follow the instructions in "Installing the Fault Server Core Process" on page 3-42.

During installation of the Fault Server core process, be sure to answer yes when you are prompted whether you want to install the database on an existing Sybase server.

Installing the Fault Server Database on a New Sybase Server

To install the Fault Server database on a new Sybase server, you must first prepare your system for a new installation of Sybase as described in the section that follows.

Preparing for a New Installation of Sybase 11

In this section, you perform the following tasks:

- Partition the second disk using raw partitions.
- Load the Ascend-supplied Sybase 11 media and extract the script.
- Run the Sybase 11 installation script to perform the prerequisite tasks.
- Reboot your system.

Before you begin the Sybase prerequisite tasks, be sure to complete the following tasks:

☑ Review the recommended Fault Server system configuration (refer to "System Configurations" on page 3-5).

☑ Fill out the Installation Worksheets in Appendix B.

Partitioning the Second Disk Using Raw Partitions

The Fault Server database Sybase installation requires you to use two disks and to partition the second disk using raw partitions. Prior to partitioning the second disk for Sybase, you should have already partitioned the first disk during the Solaris installation.

This section describes how to partition the second disk with the recommended settings listed in Table 3-2.

Table 3-2. Recommended Partition Settings

Partition(s)	Function
0	Master device
1	System Procs device
2	Backup device
3	Data device
4	Log device
5	Partition used for remainder of unallocated space.
6	Partition used for remainder of unallocated space.
7	Partition used for remainder of unallocated space.

*Before you partition the second disk, make sure the disk you are about to partition **is not** the same disk you partitioned during the Solaris install.*

If you did not use the recommended partition settings, consult your UNIX Administrator before completing this section.

Follow these steps to partition the second disk:

1. Log on to the Fault Server database workstation. Become root by entering **su - root**. At the prompt, enter the root password.
2. In a command tool window, type **format** and press Return.
3. When prompted to specify a disk, enter ***[the number of the disk that you did not partition during the Solaris install]***.

   The Format menu appears, listing the format options.

If you specify the partitioned disk, the following message is displayed:

Warning: Current Disk has mounted partitions.

*Enter **quit**. Return to Step 3 and select the disk that you did not partition.*

4. At the Format prompt, enter **partition**.

   The Partition menu appears. You are now ready to begin partitioning the disk.

Defining Partition 0 as the Master Device

Complete the following steps to create a master device on partition 0. Accept the default settings in brackets [default] by pressing Return when indicated.

1. At the Partition prompt, type **0** and press Return.
2. At the following prompts, press Return to accept the default settings:

```
Enter partition id tag [unassigned]: <Return>
Enter partition permission flags [wm]: <Return>
```

3. At the New Starting Cylinder prompt, enter **1**.
4. At the Partition Size prompt, enter **40mb**. Do not accept the default of zero.

If you accept the default value of zero for the partition size, the database will be corrupt after you complete the installation and reboot the system.

5. At the Partition prompt, enter **print** to view the current partition table.

A partition table, similar to Table 3-3, appears. Make a note of the ending cylinder value for partition 0. You need this information to define the new starting cylinder for the next partition.

Table 3-3. Sample Partition Table

Part	Tag	Flag	Cylinders	Size	Blocks
0	unassigned	wm	1 - 54	40 MB	(54/0/0)
1	unassigned	wm	55 - 121	50 MB	(67/0/0)
2	backup	wm	0 - 2733	1.98 GB	(2733/0/0)
3	unassigned	wm	122 - 788	500 MB	(667/0/0)
4	unassigned	wm	789 - 1455	500 MB	(667/0/0)
5	unassigned	wm	1456 - 1588	100 MB	(133/0/0)
6	unassigned	wm	1589 - 2122	400 MB	(534/0/0)
7	unassigned	wm	2123 - 2733	400 MB	(611/0/0)

Defining Partition 1 as the System Procs Device

Complete the following steps to create a System Procs device on partition 1. Accept the default settings in brackets [default] by pressing Return when indicated.

1. At the Partition prompt, enter **1** and press Return to define the next partition.
2. At the following prompts, press Return to accept the default settings:

```
Enter partition id tag [unassigned]: <Return>
Enter partition permission flags [wm]: <Return>
```

3. At the New Starting Cylinder prompt, enter ***[a number equal to the ending cylinder from partition 0 plus 1]***. (Calculate this number using the ending cylinder value that you made a note of when you set partition 0.)
4. At the Partition Size prompt, enter **50mb**.

5. At the Partition prompt, enter **print** to view the partition table. Make a note of the ending cylinder value for partition 1. You need this information to define the new starting cylinder for the next partition.

Defining Partition 3 as the Fault Server Data Device

Complete the following steps to create a Data device on partition 3. Accept the default settings in brackets [default] by pressing Return when indicated.

1. At the Partition prompt, enter **3** for partition 3.
2. At the following prompts, press Return to accept the default settings:

```
Enter partition id tag [unassigned]: <Return>
Enter partition permission flags [wm]: <Return>
```

3. At the New Starting Cylinder prompt, enter ***[a number equal to the ending cylinder from partition 1 plus 1]***. (Calculate this number using the ending cylinder value that you made a note of when you set partition 1).
4. At the Partition Size prompt, enter **500mb**. This value will accommodate the Fault Server's default database size of 400 MBytes.
5. At the Partition prompt, enter **print** to view the partition table. Make a note of the ending cylinder value for partition 3. You need this information to define the new starting cylinder for the next partition.

Defining Partition 4 as the Log Device

Complete these steps to create a log device on partition 4.

1. At the Partition prompt, enter **4** for partition 4.
2. At the following prompts, press Return to accept the default settings:

```
Enter partition id tag [unassigned]: <Return>
Enter partition permission flags [wm]: <Return>
```

3. At the New Starting Cylinder prompt, enter ***[a number equal to the ending cylinder from partition 3 plus 1]***. (Calculate this number using the ending cylinder value that you made a note of when you set partition 3.)

4. At the Partition Size prompt, enter **500mb**.

5. At the Partition prompt, enter **print** to view the partition table. Make a note of the ending cylinder value for partition 4. You need this information to define the new starting cylinder for the next partition.

Defining Partition 5

Perform these steps to define partition 5.

1. At the Partition prompt, enter **5** for partition 5.

2. At the following prompts, press Return to accept the default settings:

```
Enter partition id tag [unassigned]: <Return>
Enter partition permission flags [wm]: <Return>
```

3. At the New Starting Cylinder prompt, enter ***[a number equal to the ending cylinder from partition 4 plus 1]***. (Calculate this number using the ending cylinder value that you made a note of when you set partition 4.)

4. At the Partition Size prompt, enter **100mb**.

5. At the Partition prompt, enter **print** to view the partition table. Make a note of the ending cylinder value for partition 5. You need this information to define the new starting cylinder for the next partition.

Defining Partition 6

Perform these steps to define partition 6.

1. At the Partition prompt, enter **6** for partition 6.

2. At the following prompts, press Return to accept the default settings:

```
Enter partition id tag [unassigned]: <Return>
Enter partition permission flags [wm]: <Return>
```

3. At the New Starting Cylinder prompt, enter ***[a number equal to the ending cylinder from partition 5 plus 1]***. (Calculate this number using the ending cylinder value that you made a note of when you set partition 5.)

4. At the Partition Size prompt, enter **400mb**.

5. At the Partition prompt, enter **print** to view both the current partition table and the information about the total disk cylinders available.

6. Make a note of the ending cylinder value for partition 6. You need this information to define the new starting cylinder for the next partition.

7. Make a note of the number of total disk cylinders available. You need this information to calculate the remaining unallocated space.

   The entry describing the total disk cylinders available is located directly above the partition table. The entry has the following format:

   ```
   Total disk cylinders available: 1866 + 2 (reserved
   cylinders)
   ```

   In the example above, 1866 is the value you would record. Do not add the 2 to the 1866 value.

Defining Partition 7

Perform these steps for partition 7.

1. At the Partition prompt, enter **7** for partition 7.

2. At the following prompts, press Return to accept the default settings:

   ```
   Enter partition id tag [unassigned]: <Return>
   Enter partition permission flags [wm]: <Return>
   ```

3. At the New Starting Cylinder prompt, enter ***[a number equal to the ending cylinder from the partition 6 plus 1]***. (Calculate this number using the ending cylinder value that you made a note of when you set partition 6.)

4. At the Partition Size [0b, 0c, 0.00mb] prompt, enter ***[remaining unallocated space on drive after all other settings have been set]***. Append the suffix **c** to the value to indicate cylinders (150c, for example).

To calculate the remaining unallocated space, subtract the number of the ending cylinder of partition 6 from the number of total disk cylinders available. Refer to Step 5 through Step 7, starting on page 3-22.

5. At the Partition prompt, enter **quit** to exit the partition mode.
6. At the Format prompt, enter **label** to label and save the partitions.
7. At the “Ready to label disk, continue>” prompt, enter **y**.
8. At the Format prompt, enter **quit**.

Loading the Ascend-supplied Sybase Media

You are now ready to load the Sybase installation media and extract the scripts. You will need your Sybase Installation Worksheet in Appendix B to complete the install.

Follow these steps:

1. On the Fault Server database workstation, verify that you are root. You should see the # prompt. If you are not root, enter **su - root**. At the prompt, enter the root password.

If you are logged in via a remote connection (rlogin/rsh/telnet), set your DISPLAY variable to the value of the local host. Enter the following:

DISPLAY=[local hostname]:0.0
export DISPLAY

(This example uses the Korn shell syntax.)

*In addition, in a new command tool window, run **xhost +** as the user who controls the system console. Executing this command enables you to open the window that displays the installation log.*

2. Insert the Ascend-supplied Sybase media into the media drive.
3. In the command tool window, enter **cd /opt** to move to the */opt* directory.
4. To extract the tar file from the media device, enter:

   `tar -xvpf [`*`media device pathname`*`] cv_scripts`

   Refer to your Sybase Installation Worksheet in Appendix B for the pathname of the media device.

This command copies the tar file from the media device, extracts the scripts from the tar file, and places the scripts in a directory called *cv_scripts* in the */opt* directory. The whole process takes about 10 minutes.

You are now ready to set up your system for the Sybase 11 installation.

Setting Up the System for Sybase 11

Follow these steps to set up your system for Sybase 11:

1. Move to the */opt/cv_scripts* directory. Since you are already in the */opt* directory, type **cd cv_scripts** and press Return.
2. Enter the following command to start the Sybase script:

   ```
   ./install_sybase
   ```

   The following message appears:

   ```
   Verifying super user privileges...
   Would you like to view (tail -f) the install log (default=y)?
   ```

   The Tail window allows users to view a log of the installation process.

If the install_sybase script is not found in the cv_scripts directory, extract it from the Sybase media.

3. Press Return to accept the default (yes).

   The Tail (Installation Log) window appears in front of the Sybase installation window.
4. Move the Tail window behind the Sybase installation window so you can continue with the installation prompts. Whenever necessary, you can refer to the Tail window if you want to see a listing of installation events.

   The installation window now contains the Sybase Installation menu (see Figure 3-10).

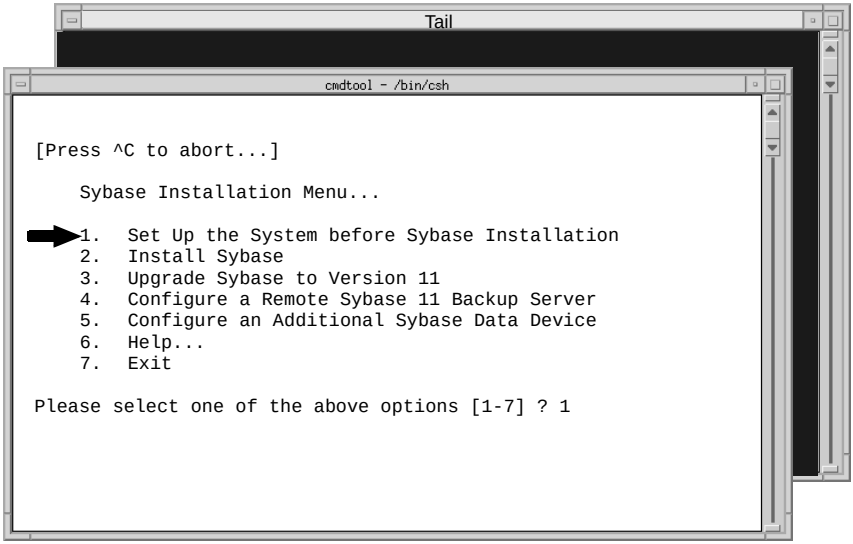


Figure 3-10. Sybase Installation Menu

5. At the Sybase Installation Menu, enter **1** to set up the system.

   The following message appears:

```
Complete all prerequisite tasks before continuing. See
Cascade's installation documentation for more information.

Do you wish to continue? <y|n> [default=y]:
```

6. Since you have performed all prerequisite tasks, press Return to continue.

   The following message appears:

```
Setting up your system for the Sybase Install
-----------------------------------------------
Creating the dba group for database system administrator.
Successfully added group 'dba' with gid 300

Creating a user account for sybase
---------------------------------------
Enter User's home directory [default : /opt/sybase] ?
```

Refer to your Sybase Installation Worksheet in Appendix B to complete the remaining steps.

7. When prompted for the user's home directory, do one of the following:

   - Press Return to accept the default of */opt/sybase*.
   - Enter **[*Sybase 11 home directory*]**.

   The following message appears:

```
Adding user sybase. Please wait...
Successfully added user sybase...
Configuring the user account with environment files.
-------------------------------------------------------
Enter the Database Server Name (default=CASCADE) ?
```

8. When prompted for the database server name, enter the name of Sybase server that will maintain the Fault Server database.

9. When prompted for the name of the error log, do one of the following:

   - Enter the recommended value **CASCADE_err.log**.
   - Enter **[*error log filename*]**.

10. When prompted for the database SA password, do one of the following:

    - Enter the recommended value **superbase**. When prompted again for the password, re-enter the password.
    - Enter **[*database SA password*]**. When prompted again for the password, re-enter the password.

    The following message appears:

```
Creating /etc/rc2.d/S97sybase...Done.
Creating /etc/rc0.d/K01sybase...Done.
Creating /etc/rc2.d/S98sybase...Done.
```

The install script creates the three files listed above. These files are used to start up and shut down the Sybase server.

```
You must add at least one more user account.
Enter name of the user [default : nms] ?
```

11. When prompted for the name of the user, do one of the following:
    - Press Return to accept the default of nms.
    - Enter **[*name of NMS user*]**.
12. When prompted for the user's group, do one of the following:
    - Press Return to accept the default of staff.
    - Enter **[*NMS user's group name*]**.

    Assuming your user name is nms, the following message appears:

```
Creating a user account for nms
---------------------------------------
Enter User's home directory [default : /opt/nms] ?
```

13. When prompted for the user's home directory, do one of the following:
    - Press Return to accept the default of */opt/nms*.
    - Enter **[*NMS user's home directory*]**.

    Assuming your user name is nms, the following message appears:

```
Adding user nms. Please wait ...
Successfully added user nms ...
Configuring the user account with environment files.
-----------------------------------------------------
Setting Shared Memory Allocations
```

*The script increases Sybase's shared memory. The script accomplishes this by appending the line **set shmsys:shminfo_shmmax=131072000** to the /etc/system file.*

The following message appears:

```
Making a backup copy of '/etc/system' in '/etc/system.cv'
Setting TCP Socket device for Sybase
-----------------------------------
The Socket Number for Sybase is 1025
The Socket Number for Sybase BACKUP is 1026
```

If the sockets are available, the script assigns the TCP socket number 1025 to Sybase and 1026 to the Backup Server. If the system is already using these sockets, the script uses the next available numbers.

The following message appears:

```
Do you wish to continue? <y|n> [default=y]:
```

14. Press Return to continue.

    The following message appears:

    ```
    Creating Additional User Accounts
    ---------------------------------
    1. Create User Account.
    2. Proceed to the Next Step.
    ```

15. Because the Fault Server allows only one user account, enter **2** to proceed to the next step.

    The Device Installation menu appears (see Figure 3-11). This menu allows you to define the device that uses the Sybase database.

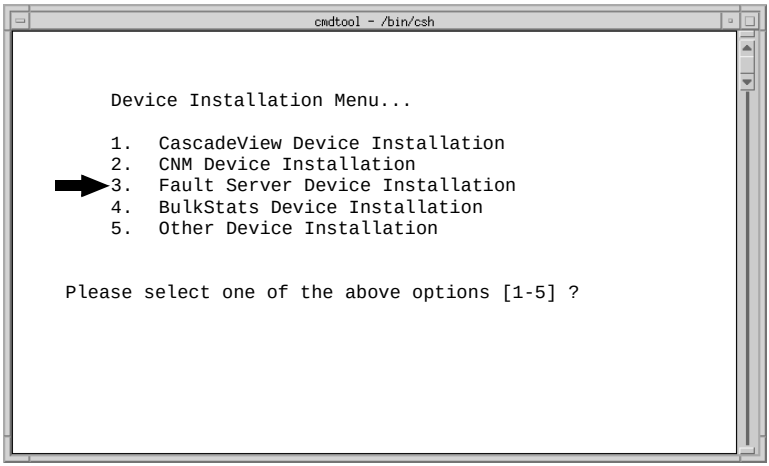


Figure 3-11. Device Installation Menu

16. Enter **3** to select the Fault Server Device Installation.

    The following message appears.

    ```
    The Fault Server Device Installation selected.
    ```

    The Setting the Master Device Used for Sybase Menu (Figure 3-12) appears:

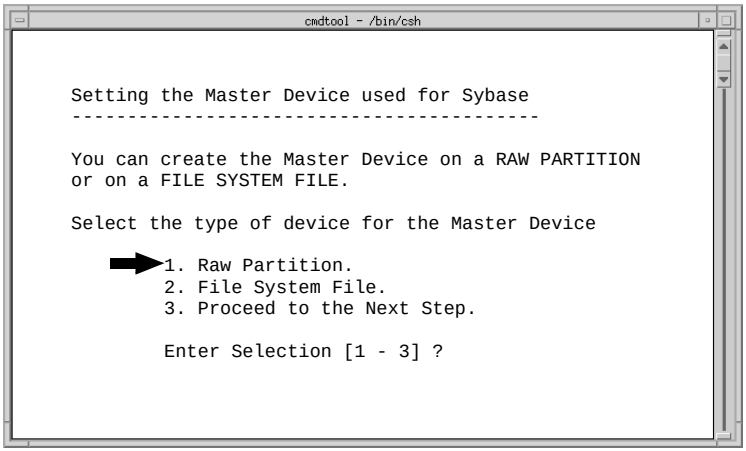


Figure 3-12. Setting the Master Device Used for Sybase Menu

17. At the Setting the Master Device menu, enter **1** for Raw Partitions.

    The following message appears:

```
WARNING: IF YOU INSTALL THE SQL SERVER ON A RAW PARTITION,
ANY EXISTING FILES ON THAT PARTITION WILL BE OVERWRITTEN.

Do you wish to continue? [default=y]:
```

18. Press Return to continue.

Refer to the Sybase Installation Worksheet in Appendix B for the following prompts. If you partitioned the second disk with the recommended partition settings in Table 3-2 on page 3-17, be sure to enter the recommended values for the pathname and size of devices.

The following message appears:

```
Setting up Raw Partition Devices
--------------------------------
Enter the Master Device Path Name (e.g. /dev/rdsk/c0t1d0s0):
```

19. At the Master Device Pathname prompt, do one of the following:

    - Enter the recommended value **/dev/rdsk/c0t1d0s0**.
    - Enter ***[master device pathname]***

    The following message appears:

```
Setting device permissions. Please Wait ...
Device /dev/rdsk/c0t1d0s0 has been set.

Enter the Procs Device Path Name (e.g. /dev/rdsk/c0t1d0s4):
```

20. At the Procs Device Path Name prompt, do one of the following:

    - Enter the recommended value **/dev/rdsk/c0t1d0s1**.
    - Enter **[*procs device pathname*]**.

The following message appears:

```
Setting device permissions. Please Wait ...
Device /dev/rdsk/c0t1d0s1 has been set.

Enter the Cascade Device Path Name (e.g.
/dev/rdsk/c0t1d0s5):
```

21. At the Cascade Device Path Name prompt, do one of the following:
    - Enter the recommended value **/dev/rdsk/c0t1d0s3**.
    - Enter **[*Cascade device pathname*]**.

In Step 21, the Cascade device pathname refers to the Fault Server data device, not CascadeView.

The following message appears:

```
Setting device permissions. Please wait...
Device /dev/rdsk/c0t1d0s3 has been set

Enter the Log Device Pathname (e.g. /dev/rdsk/c0t1d0s6):
```

22. At the Log Device Path Name prompt, do one of the following:
    - Enter the recommended value **/dev/rdsk/c0t1d0s4**.
    - Enter **[*log device pathname*]**.

The following message appears:

```
Setting device permissions. Please wait...

Device /dev/rdsk/c0t1d0s4 has been set.

The maximum value for your Master Device has been calculated
to maximize the size of your raw partition. By accepting the
default you will be utilizing the whole raw device. A minimum
value has been established at 40 Mbytes. You will not be
allowed to go below that threshold.

NOTE: It is recommended that you accept the maximum value.
Otherwise, the space left over will be wasted.

Enter size of your Master Device in Megabytes [default=40]:
```

23. At the Master Device Size prompt, enter **40mb**.

    The following message appears:

    ```
    Press Enter to return...
    ```

24. Press Return to continue.

    The following message appears:

    ```
    If you have completed the initial Sybase setup successfully,
    please REBOOT the workstation now.
    ```

25. To reboot the workstation and enable the new parameters, enter the following command at the # prompt:

    ```
    init 6
    ```

    The init 6 command reboots the system.

When the system is up and running again, you can install Sybase 11. Proceed to the next section.

Installing Sybase 11

This section describes how to install Sybase 11. You use the same installation script you used for the Sybase setup tasks earlier in this chapter.

> *This manual describes a new installation of Sybase 11, not an upgrade. Refer to the Sybase 11 SQL Server Upgrade Guide for instructions on upgrading a system to Sybase 11.*

Before you begin the Sybase installation, be sure to complete the following:

- ☑ Fill out the Sybase Installation Worksheet (Appendix B).
- ☑ Partition the disk using raw partitions (refer to "Partitioning the Second Disk Using Raw Partitions" on page 3-17).
- ☑ Extract the installation script (refer to "Loading the Ascend-supplied Sybase Media" on page 3-23).
- ☑ Complete the Sybase prerequisite tasks and reboot the workstation (refer to "Setting Up the System for Sybase 11" on page 3-24).

Follow these steps to install Sybase 11:

1. When the system is up and running again, enter **root** at the User Name prompt. When prompted for the password, enter the root password.
2. Enter the following command to move to the */opt/cv_scripts* directory:

   ```
   cd /opt/cv_scripts
   ```

If you are logged in via a remote connection (rlogin/rsh/telnet), set your DISPLAY variable to the value of the local host. Enter the following:

DISPLAY=[local hostname]:0.0
export DISPLAY

(This example uses the Korn shell syntax.)

In addition, in a new command tool window, run ***xhost +*** *as the user who controls the system console. Executing this command enables you to open the window that displays the installation log.*

3. Enter the following command to run the Ascend-supplied Sybase script:

   ```
   ./install_sybase
   ```

   The following message appears:

   ```
   Verifying super user privileges...
   Would you like to view (tail -f) the install log (default=y)?
   ```

   The Tail window allows users to view a log of the installation process.

4. Press Return to accept the default (yes) so the log is displayed during installation.

   The Tail window appears in front of the Sybase installation window.

5. Move the Tail window behind the Sybase installation window so you can continue with the installation prompts.

   The installation window now contains the Sybase Installation menu (see Figure 3-13).

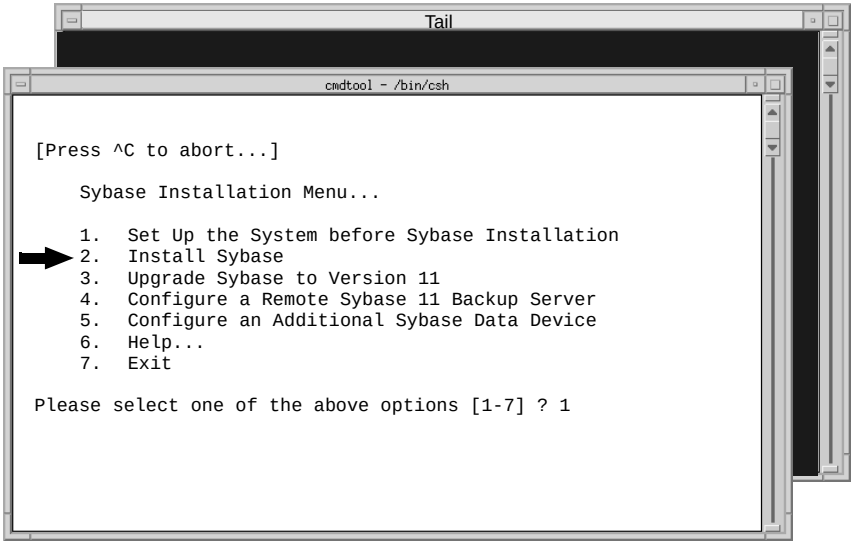


Figure 3-13. Sybase Installation Menu

6. At the Sybase Installation Menu, enter **2** to install Sybase.

   The system prompts you to make sure Sybase prerequisite tasks are completed and then asks you to confirm the installation.

7. Press Return to continue.

   The system displays the parameters you entered previously (see Figure 3-14).

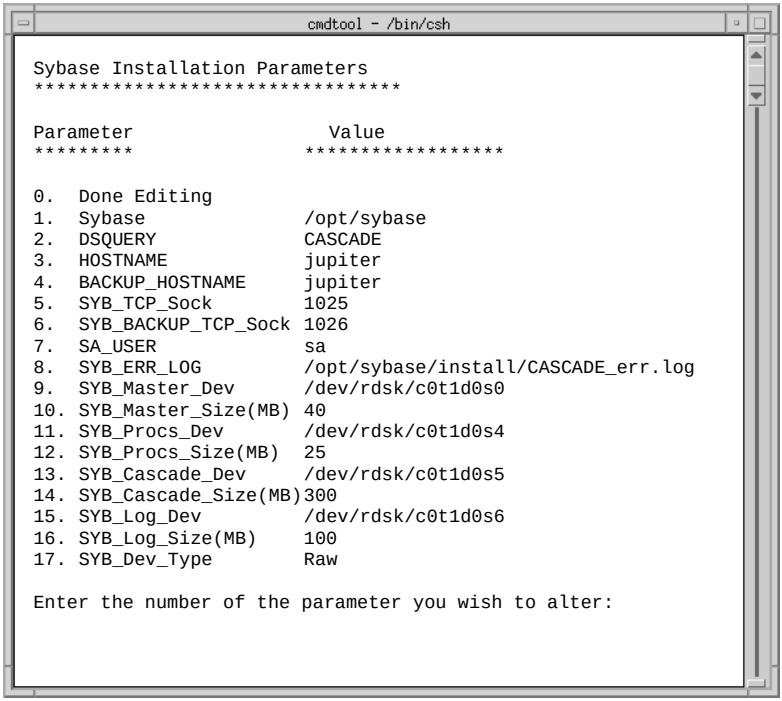


Figure 3-14. Sybase Installation Menu and Installation Parameters

8. If you want to change the values of parameters, review the parameter descriptions in Table 3-4, then enter the parameter number and make the appropriate changes.

   - If you change parameters 11-17, the Setting the Master Device Used for Sybase menu reappears. Refer to Step 17 on page 3-30.
   - If you change parameter 1, the script prompts you to change parameter 8.

.

Once you complete the Sybase installation, you cannot change the values of these parameters. If you need to change these values after installation, re-install Sybase 11.

Table 3-4. Sybase Configuration Parameters

Sybase Parameter	Description
Sybase	Target directory for Sybase installation. Default: */opt/sybase*
DSQUERY	Sybase server name. Recommended value: CASCADE
HOSTNAME	Name of Fault Server database workstation.
BACKUP_HOSTNAME	Name of Fault Server database workstation (same as HOSTNAME).
SYB_TCP_Sock	TCP socket number for Sybase. Default: 1025
SYB_BACKUP_TCP_Sock	TCP socket number for the back-up Sybase. Default: 1026
SA_USER	Default Sybase system administrator user name. Default: sa
SYB_ERR_LOG	Default pathname of log file that contains all SQL Sybase errors. Default: */opt/sybase/install/[DSQUERY value]_err.log*
SYB_Master_Dev	Pathname of Sybase Master device (partition 0). Sample format: */dev/rdsk/c0t1d0s0*
SYB_Master_Size (MB)	Size (in megabytes) of Master device. Default: 40
SYB_Procs_Dev	Pathname of Sybase Procs device (partition 1). Sample format: */dev/rdsk/c0t1d0s1*
SYB_Procs_Size (MB)	Size (in megabytes) of Procs device. Default: 50
SYB_Cascade_Dev	Pathname of the Fault Server data device (partition 3). Sample format: */dev/rdsk/c0t1d0s3*
SYB_Cascade_Size (MB)	Size (in megabytes) of the Fault Server data device. Recommended value: 400
SYB_Log_Dev	Pathname of Sybase Log device (partition4). Sample format: */dev/rdsk/c0t1d0s4*
SYB_Log_Size (MB)	Size (in megabytes) of Sybase log device. Default: 500
SYB_Dev_Type	Type of installation of Sybase devices (FileSystem or Raw). The install program sets this value automatically.

9. Once you have finished making changes to the Sybase Installation Parameters menu, enter **0** to continue.

   The following message appears:

   ```
   Install the media in your local device now.
   ************************************************
   Enter the full path of the media device:
   ```

10. When you are prompted to enter the full path of the media device, enter:

    [*media device pathname*]

    Refer to your Sybase Installation Worksheet in Appendix B for this information.

    The following message appears:

    ```
    The device was found and is ready for extraction.
    Press Return to Continue...
    ```

11. Press Return to continue.

    The following messages appear:

    ```
    Extracting Sybase Installation media from the device...Done.

    Running 'sybinit' and creating the sybase server...Done
    Successfully.
    ```

    (Running the sybinit utility takes approximately 15 minutes.)

    ```
    Running 'alter' commands to expand the master device and the
    tempdb file. This may take a few moments.
    Please Wait...Done Successfully.

    Increasing the Memory allocations to 20480 for improved
    performance...
    ```

Because the system has insufficient byte memory, the script increases memory allocation so that Sybase can execute basic commands. For more information, refer to the Sybase SQL Server Installation and Configuration Guide*.*

The screen displays the following:

```
Increasing the Number of Remote Users
-------------------------------------

By Default, the Sybase installation sets the number of user
connections to 25. If you need to increase the total
connections above 25, then enter the number of connections
you require.

Enter the number of user connections [default=25] ?
```

12. At the Number of User Connections prompt, do one of the following:
    - Press Return to accept the default of 25.
    - Enter [***number of user connections***].

    The following message appears:

    ```
    Press enter to continue...
    ```

13. Press Return to continue.

    The following message appears:

    ```
    Restarting Server with increased options
    ```

The Sybase server shuts down and restarts, enabling the new configuration parameter to take effect.

If you encounter errors during the Sybase Server startup, call the Technical Assistance Center at one of the following numbers:

1-800-DIAL-WAN (1-800-342-5926) (in the United States and Canada)

0-800-96-2229 (in the United Kingdom)

1-978-952-7299 (outside the U.S., Canada, and United Kingdom)

When the system is up and running again, the script automatically configures a local Backup Server even though the Backup Server is not used by the Fault Server. The script displays the following message:

```
Configuring Local Backup Server
**********************************

Running ‘sybinit’ and creating the sybase server...Backup
Server Install Successful....
```

The Sybase Installation Menu (Figure 3-15) appears.

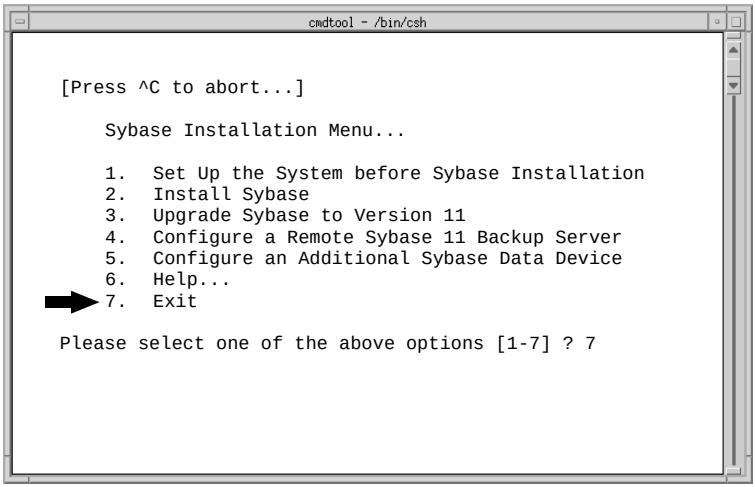


Figure 3-15. Sybase Installation Menu

14. At the Sybase Installation Menu, enter **7** to exit.

    The following message appears:

```
Cleaning up temporary files......Done.
Exiting Installation script.
```

The Sybase installation is complete and Sybase is running. You are now ready to install the remaining components of the Fault Server system.

Installing the Fault Server

To install the remaining components of the Fault Server system, you use the UNIX utility called pkgadd. Refer to "Using Software Package Tools" on page 3-4 for a review of the basic pkgadd commands.

You can install the components directly from the Fault Server media. With this method, you need a maximum of 170 MBytes of available disk space (the actual disk space you need depends on which system components you decide to install on which machine).

Or, you can first extract the files from the Fault Server media, and then install the components. With this method, you need approximately 344 MBytes of available disk space.

If your installation software is on tape, rather than CD-ROM, you must *extract the contents of the software packages from the installation media onto your system prior to performing the installation.*

Extracting Files from Fault Server Media

Follow these steps to extract the Fault Server packages:

1. Log on to the workstation where you want the packages extracted. Become root by entering **su - root**. At the prompt, enter the root password.
2. Insert the Fault Server media into the media drive.
3. To extract the Fault Server packages from media to a particular pathname, enter:

   pkgadd -s *spool-pathname* -d [*media device pathname*]

   where **spool-pathname** is the path where you want the packages stored and **media device pathname** is the media device pathname (for example, */cdrom/fltsrvr_1010*).

   Keep in mind that you need approximately 344 MBytes of disk space available on the **spool-pathname** file system.

The pkgadd menu appears, listing of all the components that you can install:

```
The following packages are available:
   1 CASCfs    Cascade Fault Server
      (sparc) 01.00.00.00
   2 CASCfsc   Cascade Fault Server Application
      (sparc) 01.00.00.00
   3 CASCwc    Cascade CVWeb
      (sparc) 01.00.00.00
   4 CASCws    Cascade Web Server
      (sparc) 01.00.00.00
   5 CASCwt    Cascade Web Tools
      (sparc) 01.00.00.00

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

4. Extract the packages you want (the actual packages you need depends on which system components you decide to install on which machine).

The packages use the following approximate amounts of disk space:

- Fault Server: 62 MBytes
- Fault Server Application: 58 MBytes
- CVWeb: 416 KBytes
- Web Server: 712 KBytes
- Web Tools: 7 MBytes

Installing the Fault Server Core Process

This section describes how to install the Fault Server core process using the pkgadd utility.

If your installation software is on tape, rather than CD-ROM, you must use the pkgadd utility to extract the Fault Server software package (CASCfs) from the tape onto your system prior to performing the installation. For information, refer to "Using Software Package Tools" on page 3-4.

Follow these steps to install the Fault Server core process:

1. Log on to the Fault Server workstation. Become root by entering **su - root**. At the prompt, enter the root password.

2. Add the Fault Server core host name to the */.rhosts* file on the Fault Server database machine.

3. Install the Fault Server core process using pkgadd.

   If you extracted the files from the Fault Server media, enter a command to install the Fault Server package from a particular device or pathname:

   `pkgadd -d spool-pathname CASCfs`

   where **spool-pathname** is the location where the package is stored.

   Or, if you want to install the Fault Server package directly from media, enter:

   `pkgadd -d [media device pathname] CASCfs`

   where **media device pathname** is the media device pathname.

   The installation utility indicates what directory it will use as a package base directory and prompts you to enter the destination directory for the package:

   ```
   Please enter the directory to install <CASCfs> [default=/opt]:
   ```

4. Enter the directory where you want the package installed. The Fault Server takes up approximately 62 MBytes of disk space.

   The installation utility performs various verification functions and displays the message:

   ```
   This package contains scripts which will be executed with
   super-user permission during the process of installing this
   package.

   Do you want to continue with the installation of <CASCfs> [y,n,?]
   ```

5. Enter **y** to continue. The installation utility executes a pre-installation script and displays the confirmation message:

   ```
   Are you sure you want to install Fault Server [y/n]?
   ```

6. Enter **y** to continue. The installation utility displays the message:

```
Do you want to install the Fault Server Database on an
existing CascadeView Sybase Server [y/n]?
```

7. If you installed the Fault Server database on an existing CascadeView Sybase Server (using the instructions on page 3-12), enter **y**.

   If you installed the Fault Server database on a new Sybase Server (using the instructions on page 3-16), enter **n**.

   The installation utility displays the Fault Server Database Configuration menu:

```
Fault Server Database Configuration
***********************************

Parameter                          Value
*****************************************************

1.  Fault db host                          ""
2.  Fault db server name                   CASCFS
3.  Fault db name                          faultdb
4.  Fault db port                          1025
5.  Fault db device size                   400
6.  Fault db log device size               400
7.  Fault db Sybase Admin user             sa
8.  Fault db Sybase Admin password         ""
9.  CascadeView db host                    ""
10. CascadeView db server name             CASCADE
11. CascadeView db name                    cascview
12. CascadeView db port                    1025
13. Fault Server name                      FaultServer1
14. Set default value

s.  Save values
x.  Abort

Enter the number of the parameter you wish to alter :
```

   The installation utility provides default values for all parameters except parameters 1, 8, and 9. You need to define values for these parameters (refer to Table 3-5.) and the instructions that follow. You do not need to define values for the remaining parameters because default values are provided.

.:

Table 3-5. Required Configuration Parameters for Fault Server Database

Parameter	Description
1. Fault db host	The machine name of the Sybase server that maintains the Fault Server database
8. Fault db Sybase Admin password	The Sybase Administrator password
9. CascadeView db host	The machine name of the Sybase server that maintains the CascadeView database

8. Define the Fault db host as follows:

   a. Enter **1** to specify the Fault db host parameter.

   b. At the New Value prompt, enter the machine name of the Sybase server that maintains the Fault Server database.

      The installation utility redisplays the Fault Server Database Configuration menu. The Fault db host name appears in the parameter list.

9. Define the Fault db Sybase Admin password as follows:

   a. Enter **8** to specify the Fault db Sybase Admin password parameter.

   b. At the New Value prompt, enter the Sybase Administrator password.

      The installation utility redisplays the Fault Server Database Configuration menu. The Fault db Sybase Admin password appears in the parameter list.

10. Define the CascadeView db host as follows:

    a. Enter **9** to specify the CascadeView db host parameter.

    b. At the New Value prompt, enter the machine name of the Sybase server that maintains the CascadeView database.

       The installation utility redisplays the Fault Server Database Configuration menu. The CascadeView db host name appears in the parameter list.

11. You do not need to define values for the remaining parameters because default values are already provided. In particular, **do not** modify the values for the Fault db server name parameter or the CascadeView db server name parameter. If you need to change any other default values, follow these steps:

    a. Refer to Table 3-6 for a description of the default parameters.

Table 3-6. Default Configuration Parameters for Fault Server Database

Parameter	Description
2. Fault db server name	The server name of the Sybase server that maintains the Fault Server database
3. Fault db name	The name of the Fault Server database
4. Fault db port	The port number of the Sybase server
5. Fault db device size	The device size of the Fault Server database
6. Fault db log device size	The log device size of the Fault Server database
7. Fault db Sybase Admin user	The name of the Sybase Administrator
10. CascadeView db server name	The name of the Sybase server that maintains the CascadeView database
11. CascadeView db name	The name of the CascadeView database
12. CascadeView db port	The port number of the CascadeView database
13. Fault Server name	The name of the Fault Server

    b. Enter the number of the parameter you want to define.

    c. At the New Value prompt, enter the parameter value.

12. To reset all the parameters to their default values, enter **14**.

13. When you finish, enter **s** to save the configuration. The installation utility saves the values you specified.

If the installation utility detects an existing Fault Server database on the Sybase server, the utility displays the following message:

```
Do you want to overwrite the existing database [y/n] ?
```

14. If you want to preserve the existing fault data, enter **n**.

    If you do not need to preserve the data, enter **y**.

    The installation utility restarts the Sybase server on which the Fault Server database resides.

15. If you are upgrading from a previous release of the Fault Server, the following prompt appears:

    ```
    Do you want to upgrade to version x.x.x.x [y/n] ?
    ```

    where **x.x.x.x** is the software version, enter **y** to upgrade the software.

    The installation utility completes the installation:

    ```
    Install complete

    Installation of <CASCfs> was successful.
    ```

The installation of the Fault Server core process is complete.

If you decide to un-install the Fault Server core process, refer to Appendix C for instructions.

Installing the Web Server Components

This section describes how to install the following Web Server components using the pkgadd utility:

- Web Server package (CASCws)
- Web Tools package (CASCwt)
- CVWeb package (CASCwc)
- Fault Server application package (CASCfsc)

If your installation software is on tape, rather than CD-ROM, you must use the pkgadd utility to extract the contents of the software packages from the installation media onto your system prior to performing the installation.

Follow these steps to install the Web Server components:

1. Log on to the Web Server workstation. Become root by entering **su - root**. At the prompt, enter the root password.
2. Install the packages using pkgadd. Enter individual commands to install each package.

   You must install the packages in the proper order, as described in the following sections. You start with the Web Server package.

Installing the Web Server Package

1. Install the Web Server using pkgadd.

   If you extracted the files from the Fault Server media, enter a command to install the Web Server package from a particular device or pathname:

   pkgadd -d *spool-pathname* CASCws

   where **spool-pathname** is the location where the package is stored.

   Or, if you want to install the Web Server package directly from media, enter:

   pkgadd -d [*media device pathname*] CASCws

where **media device pathname** is the media device pathname.

The utility indicates what directory it will use as a package base directory and prompts you to enter the destination directory for the package:

```
Please enter the directory to install <CASCws>
[default=/opt/cvweb/products]:
```

2. Enter the directory where you want the package installed. The disk space requirement for the Web Server component is 712 KBytes.

   The installation utility performs various verification functions and displays the message:

   ```
   This package contains scripts which will be executed with
   super-user permission during the process of installing this
   package.

   Do you want to continue with the installation of <CASCws> [y,n,?]
   ```

3. Enter **y** to continue.

   The installation utility executes a pre-installation script and displays the confirmation message:

   ```
   Are you sure you want to install CV Web Server [y/n]?
   ```

4. Enter **y** to continue.

   The utility displays the URL that users should use to access the Fault Server application on the Web Server. For example:

   ```
   http://machine1:9050/cvweb
   ```

   where **machine1** is the name of the host name of the Web Server and **9050** is the port number the Web Server uses. Record this information so that you can inform users about which URL to enter from a Web browser.

   The utility completes the installation:

   ```
   Installation of <CASCws> was successful.
   ```

The installation of the Web Server package is complete. Next, you install the Web Tools package.

Installing the Web Tools Package

1. Install the Web Tools using pkgadd.

   If you extracted the files from the Fault Server media, enter a command to install the Web Tools package from a particular device or pathname:

   pkgadd -d *spool-pathname* CASCwt

   where **spool-pathname** is the location where the package is stored.

   Or, if you want to install the Web Tools package directly from media, enter:

   pkgadd -d [*media device pathname*] CASCwt

   where **media device pathname** is the name of the media device pathname.

   The installation utility indicates what directory it will use as a package base directory and prompts you to enter the destination directory for the package:

   ```
   Please enter the directory to install <CASCwt>
   [default=/opt/cvweb]:
   ```

2. Enter the directory where you want the package installed. The disk space requirement for the Web Tools component is approximately 7 MBytes.

   The installation utility performs various verification functions and displays the following message:

   ```
   This package contains scripts which will be executed with
   super-user permission during the process of installing this
   package.

   Do you want to continue with the installation of <CASCwt> [y,n,?]
   ```

3. Enter **y** to continue.

   The utility executes a pre-installation script and completes the installation:

   ```
   Installation of <CASCwt> was successful.
   ```

The installation of the Web Tools package is complete. Next, you install the CVWeb package.

Installing the CVWeb Package

1. Install CVWeb using pkgadd.

   If you extracted the files from the Fault Server media, enter a command to install the CVWeb package from a particular device or pathname:

   pkgadd -d *spool-pathname* CASCwc

   where **spool-pathname** is the location where the package is stored.

   Or, if you want to install the CVWeb package directly from media, enter:

   pkgadd -d [*media device pathname*] CASCwc

   where **media device pathname** is the media device pathname.

   The installation utility indicates what directory it will use as a package base directory and prompts you to enter the destination directory for the package:

   ```
   Please enter the directory to install <CASCwc>
   [default=/opt/cvweb/products]:
   ```

2. Enter the directory where you want the package installed. The disk space requirement for the CVWeb component is approximately 416 KBytes.

   The installation utility performs various verification functions and displays the message:

   ```
   This package contains scripts which will be executed with
   super-user permission during the process of installing this
   package.

   Do you want to continue with the installation of <CASCwc> [y,n,?]
   ```

3. Enter **y** to continue.

   The installation utility executes a pre-installation script and displays the confirmation message:

   ```
   Are you sure you want to install CV Web [y/n]?
   ```

   The utility completes the installation:

   ```
   Installation of <CASCwc> was successful.
   ```

The installation of the CVWeb package is complete. Next, you install the Fault Server application package.

Installing the Fault Server Application Package

1. Install the Fault Server application using pkgadd.

   If you extracted the files from the Fault Server media, enter a command to install the Fault Server application package from a particular device or pathname:

   pkgadd -d *spool-pathname* CASCfsc

   where **spool-pathname** is the location where the package is stored.

   Or, if you want to install the Fault Server application package directly from media, enter:

   pkgadd -d [*media device pathname*] CASCfsc

   where **media device pathname** is the media device pathname.

   The installation utility indicates what directory it will use as a package base directory and prompts you to enter the destination directory for the package:

   ```
   Please enter the directory to install <CASCfsc>
   [default=/opt/cvweb/products]:
   ```

2. Enter the directory where you want the package installed. The disk space requirement for the Fault Server application is approximately 58 MBytes.

   The installation utility performs various verification functions and displays the message:

   ```
   This package contains scripts which will be executed with
   super-user permission during the process of installing this
   package.

   Do you want to continue with the installation of <CASCfsc> [y,n,?]
   ```

3. Enter **y** to continue.

The installation utility executes a pre-installation script and displays the confirmation message:

```
Are you sure you want to install Fault Server Application
[y/n]?
```

4. Enter **y** to continue.

5. The installation utility displays the Database Configuration menu:

```
Welcome to Cascade Fault Server Management Utility
            Database Configuration Menu

Please choose one of the following operations.

   1. Add Record
   2. Delete Record
   3. Modify Record
   4. List Record

   0.  Quit

Enter 1,2,3,4 or 0:
```

6. Enter **1** to add a record to the Fault Server configuration. This record provides information to the Fault Server application. You need to create a separate record for each Fault Server that the Fault Server application communicates with.

The installation utility displays the Add Record menu:

```
   Add Record Menu
   ***********************************
Note: Fault db server name and Active NMS db server name
could be different from Sybase server which maintains Fault
Database and/or Active NMS Database.

   Parameter                        Value
   ***************************** ***************************

   1.  Fault Server name            FaultServer1
   2.  Fault Server host            ""
   3.  Fault db host                ""
   4.  Fault db server name         CASCfs
   5.  Fault db name                faultdb
   6.  Fault db port                1025
   7.  Active NMS db host           ""
   8.  Active NMS db server name    CASCADE
   9.  Active NMS db name           cascview
   10. Active NMS db port           1025


   s.  Save values
   x.  Abort and return to previous menu


   Enter the number of the parameter you wish to alter :
```

Default values are provided for all parameters except parameters 2, 3, and 7. You need to define values for these parameters (refer to Table 3-7).

Table 3-7. Parameters for the Fault Server Database Record

Parameter	Description
2. Fault Server host	The name of the machine that maintains the Fault Server
3. Fault db host	The machine name of the Sybase server that maintains the Fault Server database
7. Active NMS db host	The machine name of the Sybase server that maintains the CascadeView database

7. Define the Fault Server host as follows:
   a. Enter **2** to specify the Fault Server host parameter.
   b. At the New Value prompt, enter the name of the machine that maintains the Fault Server.
   c. The installation utility redisplays the Add Record menu. The Fault Server host name appears in the parameter list.
8. Define the Fault db host as follows:
   a. Enter **3** to specify the Fault db host parameter.
   b. At the New Value prompt, enter the machine name of the Sybase server that maintains the Fault Server database.
   c. The installation utility redisplays the Add Record menu. The Fault db host name appears in the parameter list.
9. Define the Active NMS db host as follows:
   a. Enter **7** to specify the Active NMS db host parameter.
   b. At the New Value prompt, enter the machine name of the Sybase server that maintains the CascadeView database.
   c. The installation utility redisplays the Add Record menu. The Active NMS db host name appears in the parameter list.

10. You do not need to define values for the remaining parameters because default values are provided. In particular, **do not** modify the values for the Fault db server name parameter or the Active NMS db server name parameter. If you need to change any other default value, follow these steps:

    a. Refer to Table 3-8 for information about the default parameters.

Table 3-8. Default Parameters for the Fault Server Database Record

Parameter	Description
1. Fault Server name	The name of the Fault Server
4. Fault db server name	The name of the Sybase server that maintains the Fault Server database
5. Fault db name	The name of the Fault Server database
6. Fault db port	The port number of the Sybase server
8. Active NMS db server name	The name of the Sybase server that maintains the CascadeView database
9. Active NMS db name	The name of the CascadeView database
10. Active NMS db port	The port number of the CascadeView database

    b. Enter the number of the parameter you want to define.

    c. At the new value prompt, enter the parameter value.

11. To reset all the parameters to their default values, enter **11**.

12. When you finish, enter **s** to save the configuration.

    The installation utility redisplays the parameters and values to be stored with the record and displays the following prompt:

    ```
    Do you really want to Add the record? [y/n]
    ```

13. Enter **y** to continue.

The utility displays the following prompt:

```
Do you want to process another record? [y/n]
```

14. You need to create a separate record for each Fault Server that the Fault Server application communicates with:

    - To add another record, enter **y**. Repeat Step 7 through Step 12 to enter the specifics of the record.
    - If you have no other records to add, enter **n.**

      The utility completes the installation:

      ```
      Install complete.
      Installation of <CASCfsc> was successful.
      ```

The installation of the Fault Server application is complete.

If you decide to un-install the Web Server components, refer to Appendix C for instructions.

4

Configuring the Fault Server System

This chapter describes how to configure the Fault Server system.

Configuring Switches

On each switch you want included in the Fault Server system, you must define an NMS Entry for the Fault Server. On the gateway switch, you must define an NMS Path for the Fault Server. You use CascadeView/UX to set these parameters.

To set the NMS Entries for the switch, enter the IP address of each Fault Server that will receive traps from the switch. Enter a community name for each Fault Server you define. The file, cascadeview.cfg, in */opt/CascadeView/etc* provides the default read/write community name.

To set the NMS Entries for a switch:

1. Start CascadeView/UX and access the network map.

2. From the Misc menu, choose CascadeView ⇒ Logon. Enter your operator password.

3. Select the switch object and from the Administer menu, choose Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears for the selected switch.

4. To configure switch parameters, choose *Set Sw Attr.* The Set Switch Attributes dialog box appears.

5. Choose the NMS Entries command. The Set NMS Entries dialog box appears, displaying the current NMS entries as shown in Figure 4-1.

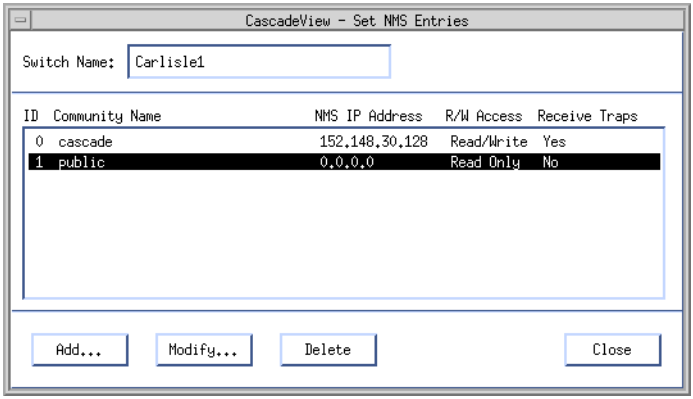


Figure 4-1. Set NMS Entries Dialog Box

6. Choose Add. The Add NMS Entry dialog box appears as shown in Figure 4-2.

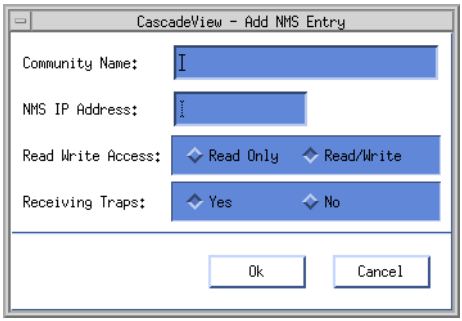


Figure 4-2. Add NMS Entry Dialog Box

7. Complete the dialog box fields as described in Table 4-1.

Table 4-1. Add NMS Entry Dialog Box Fields

Field	Action/Description
Community Name	Enter the community name for the target Fault Server. *Note: If you need to modify the Community Name, you must first edit this dialog box and then edit the value* CV_SNMP_READ_WRITE_ COMMUNITY *in the cascadeview.cfg file.*
NMS IP Address	Enter the IP address for the target Fault Server.
Read Write Access	Select the access rights for the Fault Server: *Read Only* - Allows the Fault Server to receive standard traps. *Read/Write* - Allows the Fault Server to receive standard traps and to request that reliable traps be resent.
Receiving Traps	Select the default, *Yes*, to enable the Fault Server to receive traps.

8. Choose OK.

   A message box appears, prompting you to synchronize PRAM.

9. Choose OK to return to the Switch Back Panel dialog box.

10. Select the CP module.

11. Choose the PRAM command. The Pram Synch dialog box appears.

12. Select Synchronize PRAM and choose OK. This sends the configuration to the CP module and causes it to reboot.

13. Repeat Step 5 through Step 12 for each Fault Server that you want to receive traps from the switch.

14. Choose OK to set the parameters.

The NMS path configuration is node-specific and identifies each Fault Server that attaches via the gateway switch. To set the NMS Path for the gateway switch:

1. On the network map, select the gateway switch to be connected to the Fault Server.

2. From the Administer menu, choose Cascade Parameters ⇒ Set NMS Paths. The Set NMS Paths dialog box appears (Figure 4-3).

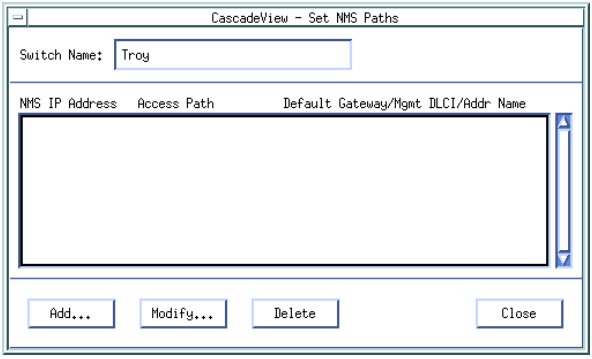


Figure 4-3. Set NMS Paths Dialog Box

3. Choose Add. The Add NMS Path dialog box appears (Figure 4-4). The following example shows an Ethernet (Direct) NMS Path.

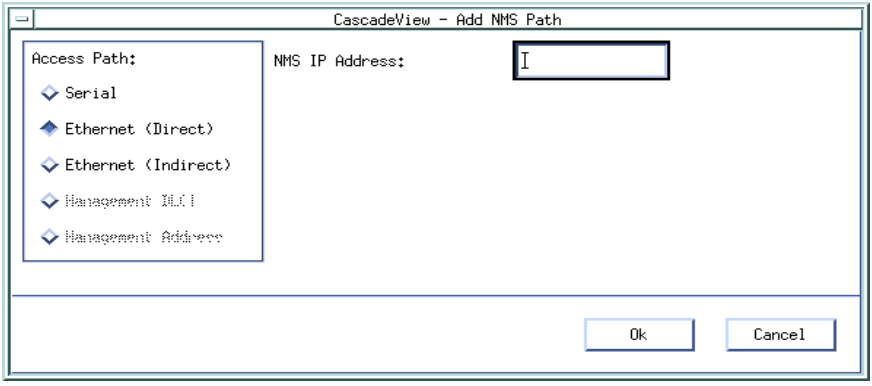


Figure 4-4. Add NMS Path Dialog Box

4. Complete the Add NMS Path dialog box fields as follows:

   a. In the Access Path field, select the connectivity method you used to connect the Fault Server to the gateway switch.

   b. In the NMS IP address field, enter the IP address of the Fault Server.

   c. The following fields appear depending on the type of access path you select:

      Ethernet **(***Indirect)* – In the Default Gateway IP Address field, enter the IP address of the gateway router that connects the Fault Server to the switch.

      Management DLCI – In the Management DLCI Name field, select the name of the Management DLCI.

      Management Address – In the Management Port Name field, select the name of the logical port that has the In-Band Management Address defined.

   d. Choose OK to save your changes or Cancel to exit without saving.

5. Choose Close to return to the network map.

Executing Scripts

You can configure the Fault Server to execute a UNIX script when an alarm is generated. There are two types of alarm scripts: a generic alarm script that runs for every alarm, and an individual named alarm script that runs for a named alarm. An example of an individually-named script could be one that informs a trouble-ticket application or paging system about the alarm.

When the Fault Server generates an alarm, it looks for any scripts to execute in the directory */opt/cvFaultServer/alarms_scripts*. The Fault Server identifies which scripts to execute by their filenames. The Fault Server looks first for any named alarm scripts to execute. If none are present, it executes the generic alarm script.

Script Naming Convention

The Fault Server identifies individual scripts by their file naming convention:

```
ALARM_SCRIPT_[alarm-name]
```

where **alarm_name** is the name of the alarm that triggers the script. For example, an alarm script named *ALARM_SCRIPT_LPORT_DOWN* would be executed each time the Fault Server generates an LPORT_DOWN alarm. If no individual named alarm script exists, the generic alarm script is executed.

Script Contents

The Fault Server provides the following input information to the script:

```
ALARM_TEXT ALARM_ID SEVERITY COMPONENT TIME STATE
```

`ALARM_TEXT` — The name of the alarm, such as LPORT_DOWN.

`ALARM_ID` — The number of the alarm.

`SEVERITY` — The severity level of the alarm.

`COMPONENT` — The switch component that generated the alarm.

`TIME` — The timestamp at which the alarm occurred.

`STATE` — The status of the alarm, such as open or closed.

When you produce a script, use the following script variables to parse the script input:

```
#!/bin/csh
set ALARM_TEXT=$1
set ALARM_ID=$2
set SEVERITY=$3
set COMPONENT=$4
set TIME=$5
set STATE=$6

set SWITCH=`echo $COMPONENT | awk -F- '{print $1}'`
set CARD=`echo $COMPONENT | awk -F- '{print $2}'`
set PPORT=`echo $COMPONENT | awk -F- '{print $3}'`
set CHANNEL=`echo $COMPONENT | awk -F- '{print $4}'`
set LPORT=`echo $COMPONENT | awk -F- '{print $5}'`
set CIRCUIT=`echo $COMPONENT | awk -F- '{print $6}'`
```

In your script, use C shell commands to define conditional statements and specify what action to take.

As a starting point to develop a script, use the template file that ships with the Fault Server. The template file (*ALARM_SCRIPT_TEMPLATE*) is located in the directory */opt/cvFaultServer/alarms_scripts.*

5

Using the Fault Server Application

This chapter describes how to start and exit the Fault Server application and how to use the application to configure the Fault Server.

About the Fault Server Application

The Fault Server application is the graphical application that displays information about alarms, events, and traps.

To run the Fault Server application, you need to run the Java-enabled Web browser, Netscape Navigator. You must obtain and install the Web browser separately; it is not shipped with the Fault Server system.

The Fault Server application is installed on the Web Server. To access the Fault Server application, the Web browser must have access to the Web server. For instructions on installing the Web Server, refer to Chapter 3.

Starting the Fault Server Application

The start the Fault Server application:

1. From a workstation running Netscape Navigator, start the Java-enabled Web browser.

2. In the location text field of the browser, enter the URL (Uniform Resource Locator) of the Fault Server application on the Web Server. For example:

   ```
   http://machine1:9050/cvweb
   ```

   where **machine1** is the name of the Web Server machine and **9050** is the port number the Web Server uses.

   The NavisXtend Dashboard page appears (see Figure 5-1 on page 5-3). From this web page, you can access several network management applications available from Ascend, including the Fault Server application.

3. If necessary, size the browser window so that the NavisXtend Dashboard page displays in its entirety.

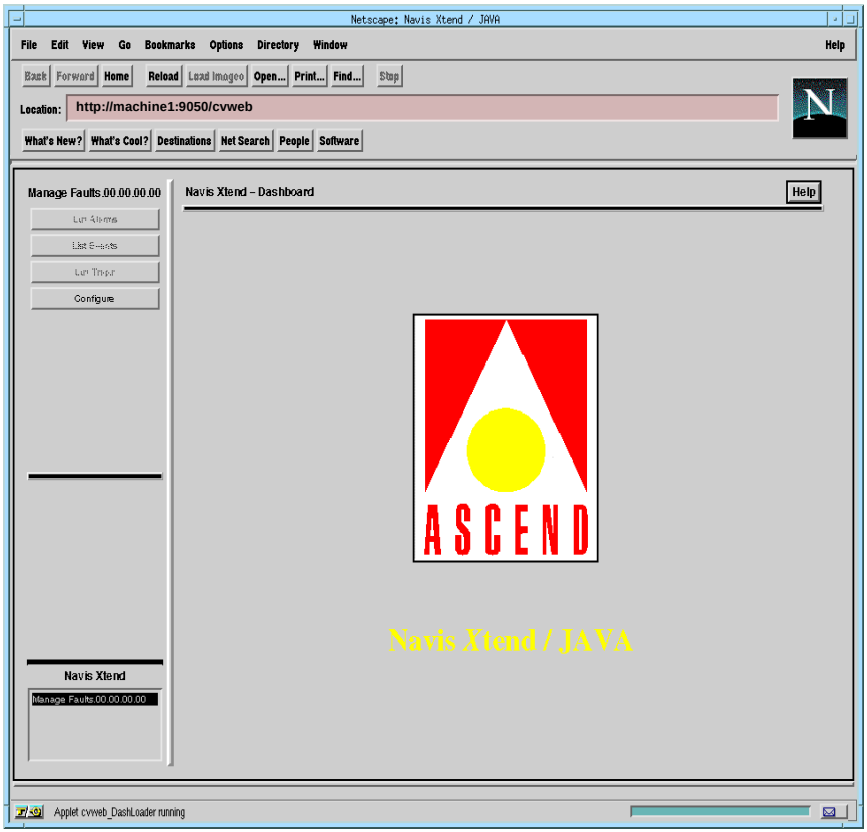


Figure 5-1. NavisXtend Dashboard Page

4. From the list of commands in the NavisXtend box (in the lower-left corner of the page), select Manage Faults.

   The NavisXtend page displays the Fault Server application (see Figure 5-2 on page 5-4).

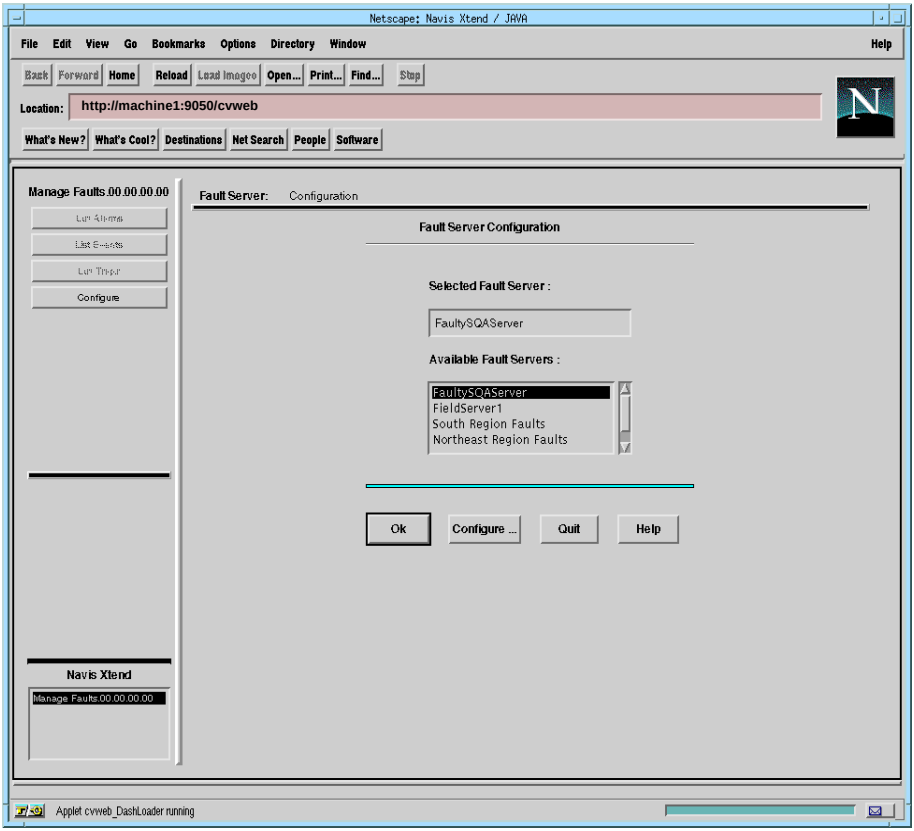


Figure 5-2. Fault Server Application Dialog Box

Exiting the Fault Server Application

Once you are running the Fault Server application, you can exit at any time. To exit the Fault Server application, choose Quit to return to the NavisXtend Dashboard page. Then, perform one of the following actions:

- Select another command from the list in the NavisXtend box.
- Exit the Web browser.

Using Online Help

Online Help is available for the Fault Server application. To obtain Help, choose Help from any screen or dialog box.

To quit Help, choose Close from the Help window. If you choose Exit from the window, you exit the Fault Server application.

Configuring the Fault Server

To configure the Fault Server:

1. Start the Fault Server application (see “Starting the Fault Server Application” on page 5-2).

   The Fault Server Configuration dialog box appears, listing a default Fault Server and other available Fault Servers (see Figure 5-3 on page 5-6).

2. Select the Fault Server you want to use. You can accept the default Fault Server or select another one from the drop-down list of the Available Fault Servers field.

   Choose OK.

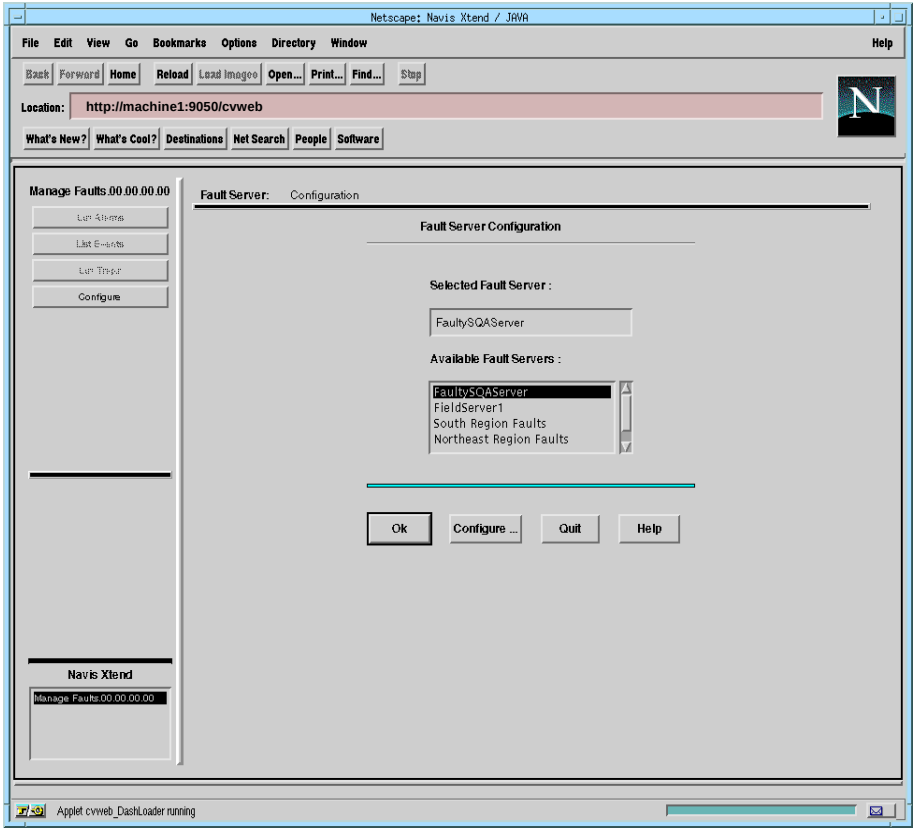


Figure 5-3. Fault Server Configuration Dialog Box

3. Choose Configure.

   The Fault Server and Database Configuration dialog box appears (Figure 5-4), listing current information about the Fault Server and its database. For a description of the fields, see Table 5-1 on page 5-8.

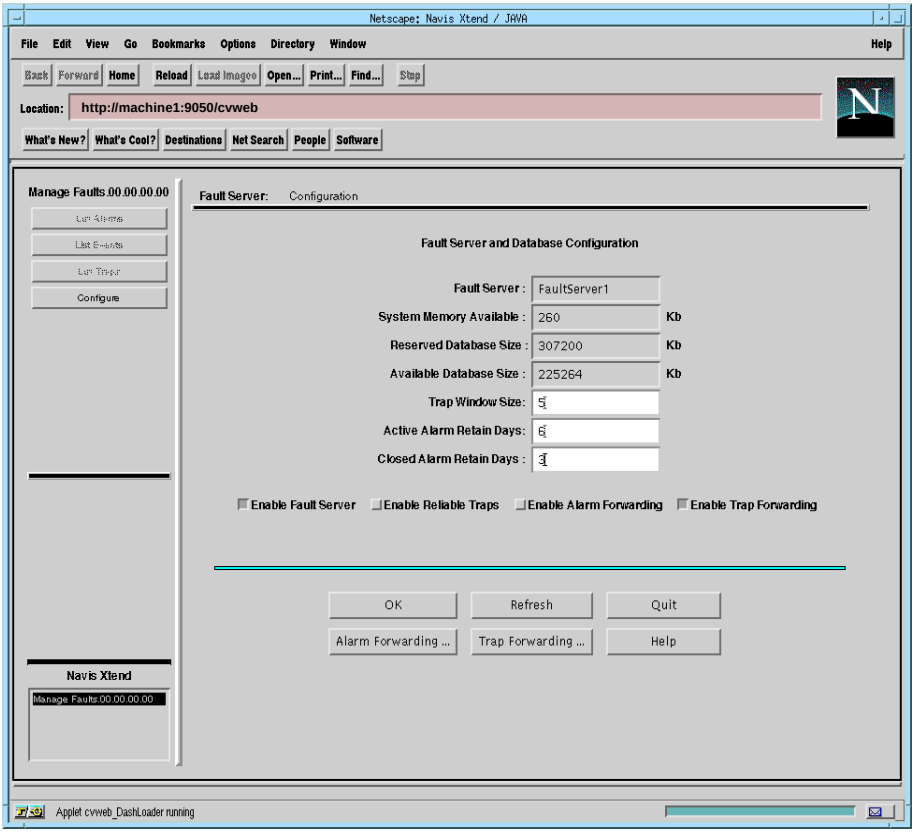


Figure 5-4. The Fault Server and Database Configuration Dialog Box

Table 5-1 describes the Fault Server and Database Configuration Fields.

Table 5-1. Fault Server and Database Configuration Fields

Field	Description
Fault Server	The machine name on which the Fault Server resides
System Memory Available	Kilobytes of memory available on the machine
Reserved Database Size	Kilobytes reserved for the Fault Server database
Available Database Size	Kilobytes not yet used by the Fault Server database
Trap Window Size	Number of higher-numbered traps that must arrive before a trap is considered missing
Active Alarm Retain Days	Number of days of open alarms to be saved when the database is purged
Closed Alarm Retain Days	Number of days of closed alarms to be saved when the database is purged

4. Anytime you want an updated status on the Fault Server or its database, choose Refresh.

Configuration Tasks

From the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7), you can perform the following configuration tasks:

- Configure the Fault Server database
- Enable or disable the Fault Server
- Enable or disable reliable traps
- Configure alarm forwarding
- Configure trap forwarding

Configuring the Fault Server Database

The Fault Server database is limited to a particular size. Depending on the rate of the traps being generated from the network, the database can fill up quickly. To prevent the database from filling up, the database is purged daily by a cron job. The following actions take place during the database purge:

The cron job purges traps, events, and alarms, including:

- Open alarms that are older than a particular day
- Closed alarms that are older than a particular day
- All events and traps associated with the purged alarms

By default, the cron job will purge the database at midnight. If you want to perform daily backups of your database, you must run the backup prior to midnight to avoid data loss.

To specify how many days of open and closed alarms to retain when the database is purged, use the following fields in the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7):

Active Alarm Retain Days — Specify the number of days of open alarms to be saved when the database is purged. The default value is 30.

Closed Alarm Retain Days — Specify the number of days of closed alarms to be saved when the database is purged. The default value is 15.

When you finish making changes, choose OK.

Enabling or Disabling the Fault Server

By default, the Fault Server processes traps by storing them in its database and forwarding them to the Event Processor to be mapped to events. You can disable the Fault Server so that it does not store traps in its database or forward them to the Event Processor.

To *enable* the Fault Server, select the Enable Fault Server button in the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7).

To *disable* the Fault Server, deselect the Enable Fault Server button in the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7).

When you finish making changes, choose OK. If you do not want to save your changes, choose Quit.

You can also configure the Fault Server to forward traps to other locations. A Fault Server configured this way functions as a single point of contact for one or more switches, forwarding traps to other NMS applications or other Fault Servers. For instructions, refer to "Configuring Trap Forwarding" on page 5-15.

Enabling or Disabling Reliable Traps

Reliable traps are traps that originate from a switch that maintains a buffer of outgoing traps and can resend any trap that was lost before it reached its destination. When the Fault Server receives reliable traps, it looks at their sequence numbers to ensure that it receives all incoming traps. If the Fault Server does not receive the trap corresponding to a particular sequence number, it can request that the switch resend the missing trap.

To *enable* reliable traps, select the Enable Reliable Traps button in the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7).

To *disable* reliable traps, deselect the Enable Reliable Traps button in the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7).

If reliable traps are enabled, you must specify how many higher-numbered traps must arrive before a trap is considered missing. To do this, enter a number in the Trap Window Size field on the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7).

For example, assuming you set the Fault Server Trap Window Size value to 5 and the Fault Server received traps in the following sequential order:

```
1  2  3     5  6  7  8  9  10
```

The Fault Server would then request that the trap with sequence number 4 be resent. The server makes the request to resend the trap once the sequence number 9 is received, 5 traps after the missing trap.

When you finish making changes, choose OK. If you do not want to save your changes, choose Quit.

Configuring Alarm Forwarding

You can configure the Fault Server to use traps to forward alarms to other locations. Alarm forwarding is performed by applying each alarm to a set of maps to determine if and where the alarm should be forwarded. Only an alarm that meets the criteria specified by a particular forwarding map is redirected to a particular IP address.

To *enable* alarm forwarding, select the Enable Alarm Forwarding button (see Figure 5-4 on page 5-7).

To *disable* alarm forwarding, deselect the Enable Alarm Forwarding button (see Figure 5-4 on page 5-7).

To specify alarm forwarding maps:

1. From the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7), choose Alarm Forwarding.

   The Alarm Forward List appears (see Figure 5-5 on page 5-12), listing the criteria for the alarm forwarding maps:

   Alarms — Names of alarms to be forwarded

   Component Mask — The source IP addresses of the switches that originate the alarms. The component ID is also listed as a series of asterisks representing wildcard values.

   Destination IP — The IP address where the alarms are to be forwarded.

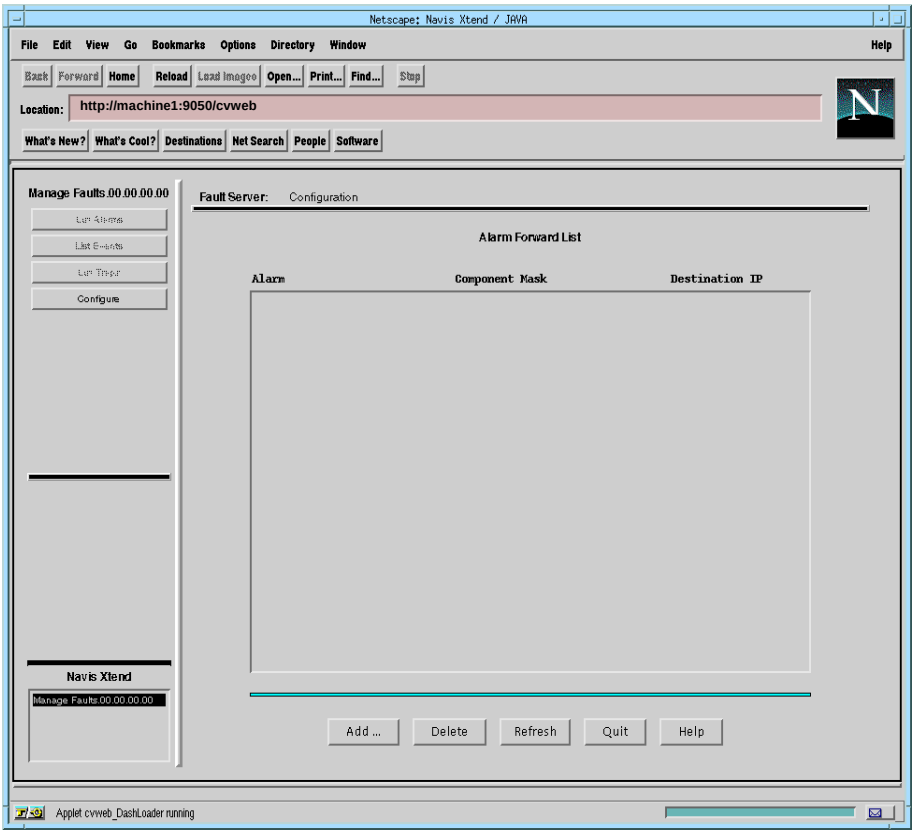


Figure 5-5. The Alarm Forward List

2. From the Alarm Forward List, you can remove, update, or add an alarm map from the list.

   - To *remove* an alarm map, select the map from the list and choose Delete.
   - To *update* an alarm map, choose Refresh.
   - To *add* an alarm map, choose Add. The Alarm Forwarding dialog box appears (see Figure 5-6 on page 5-13). Proceed with the remaining steps.

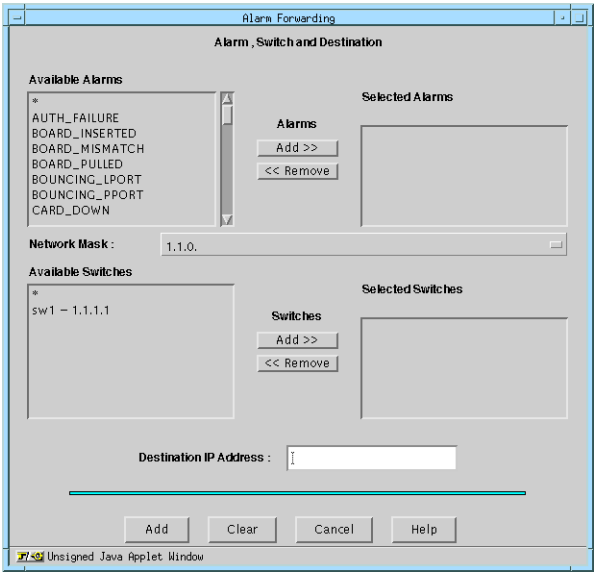


Figure 5-6. Alarm Forwarding Dialog Box

3. Use the fields in the dialog box to specify the criteria of the forwarding map:

   - Use the Available Alarms field to select the alarms you want forwarded:
     - To *select an alarm*, select the alarm name from the list and choose Add. The alarm is added to the Selected Alarms list.
     - To *select all alarms*, select the wildcard character (*) from the list and choose Add.
     - To *remove an alarm* from the Selected Alarms list, select the alarm name from the list and choose Remove. The alarm is removed from the Selected Alarms list.
   - Use the drop-down list of the Network Mask field to select the IP address of the network that generates the alarms you want forwarded.

- Use the Available Switches field to select the originating switch for the alarms you want forwarded:
  - To *specify a switch*, select the switch name from the list and choose Add. The switch is added to the Selected Switches list.
  - To *select all switches*, select the wildcard character (*) from the list and choose Add.
  - To *remove a switch* from the Selected Switches list, select the switch name from the list and choose Remove. The switch is removed from the Selected Switches list.
- In the Destination IP Address field, enter the IP address where the alarms are to be forwarded.

You can choose Clear at any time to clear all selections you have made so far in the dialog box.

4. When you finish specifying the forwarding map, choose Add. The Fault Server updates the Alarm Forward List with the new information. If you do not want to save your changes, choose Cancel.

5. For your changes to take effect, you must disable and re-enable Alarm Forwarding. To do so:

   a. Choose Quit to return to the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7).

   b. If the Enable Alarm Forwarding button is selected, deselect it, then wait 15 seconds before proceeding with Step c.

   c. Select the Enable Alarm Forwarding button.

Configuring Trap Forwarding

You can configure the Fault Server to forward traps to other locations, such as other NMS applications. Trap forwarding is performed by applying each trap to a set of maps to determine if and where the trap should be forwarded. Only a trap that meets the criteria specified by a particular forwarding map is redirected to a particular IP address.

To *enable* trap forwarding, select the Enable Trap Forwarding button (see Figure 5-4 on page 5-7).

To *disable* trap forwarding, deselect the Enable Trap Forwarding button (see Figure 5-4 on page 5-7).

To specify trap forwarding maps:

1. From the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7), choose Trap Forwarding.

   The Trap Forward List appears (see Figure 5-7 on page 5-16), listing the criteria for the trap forwarding maps:

   Trap — Names of traps to be forwarded, or the wildcard character (*) representing all traps.

   Enterprise ID — Enterprise ID of the traps.

   Component Mask — The source IP addresses of the switches that originate the traps. The component ID is also listed as a series of asterisks representing wildcard values.

   Destination IP — The IP address where the traps are to be forwarded.

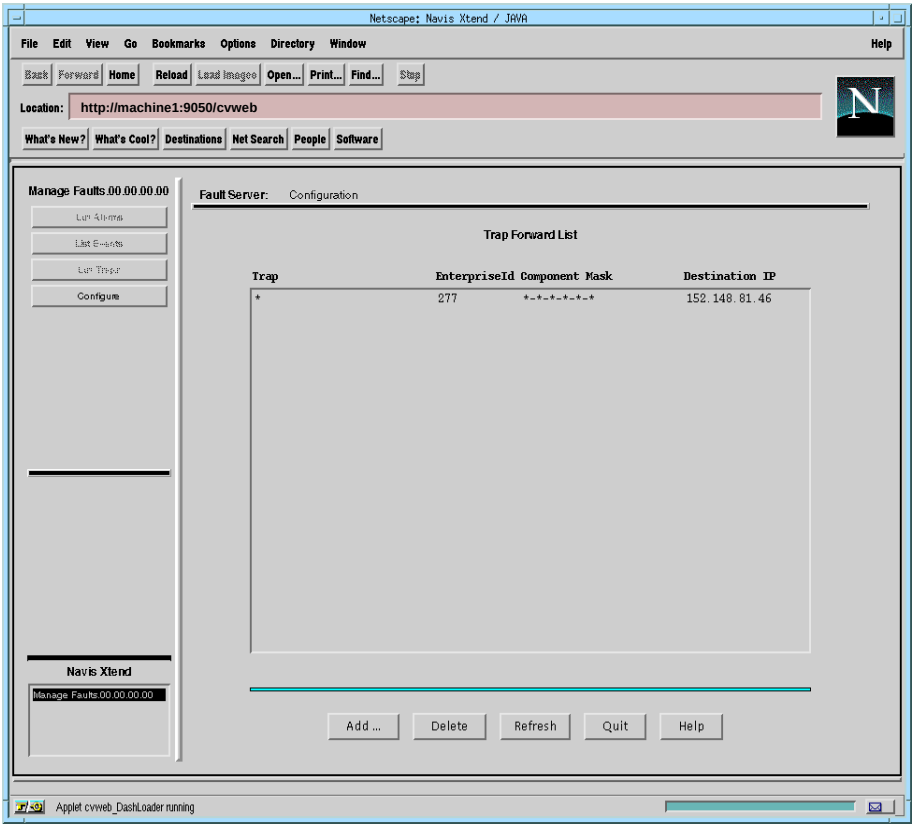


Figure 5-7. Trap Forward List

2. From the Trap Forward List, you can remove, update, or add trap maps as follows:

   - To *remove* a trap map from the list, select the map and choose Delete.
   - To *update* the Trap Forward List, choose Refresh.
   - To *add* a new trap map, choose Add. The Trap Forwarding dialog box appears (see Figure 5-8 on page 5-17). Proceed with the remaining steps.

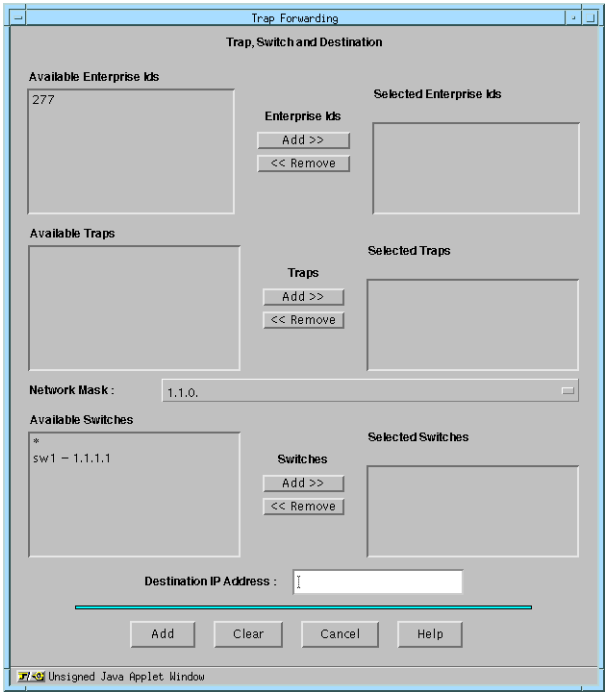


Figure 5-8. Trap Forwarding Dialog Box

3. Use the fields in the dialog box to specify the criteria of the forwarding map:

   - Use the Available Enterprise IDs field to select the Enterprise ID of the network for the traps you want forwarded:

     - To *add* an Enterprise ID, select it from the list and choose Add. The ID is added to the Selected Enterprise IDs list.

     - To *remove* an Enterprise ID from the Selected Enterprise IDs list, select it from the list and choose Remove. The ID is removed from the Selected Enterprise IDs list.

     The Enterprise ID for Ascend is 277.

- Use the Available Traps field to select the traps you want forwarded:
  - To *select a trap*, select its name from the list and choose Add. The trap is added to the Selected Traps list.
  - To *select all traps*, select the wildcard character (*) from the list and choose Add.
  - To *remove a trap* from the Selected Traps list, select the trap from the list and choose Remove. The trap is removed from the Selected Traps list.
- Use the drop-down list of the Network Mask field to select the IP address of the network that generates the traps you want forwarded.
- Use the Available Switches field to select the originating switch for the traps you want forwarded:
  - To *select a switch*, select the switch name from the list and choose Add. The switch is added to the Selected Switches list.
  - To *select all switches*, select the wildcard character (*) from the list and choose Add.
  - To *remove a switch* from the Selected Switches list, select the switch name from the list and choose Remove. The switch is removed from the Selected Switches list.
- In the Destination IP Address field, enter the IP address where the traps are to be forwarded.

You can choose Clear at any time to clear all selections you have made so far in the dialog box.

4. When you finish specifying the forwarding map, choose Add. The Fault Server updates the Trap Forward List with the new information. If you do not want to save your changes, choose Cancel.

5. For your changes to take effect, you must disable and re-enable Trap Forwarding. To do so:

   a. Choose Quit to return to the Fault Server and Database Configuration dialog box (see Figure 5-4 on page 5-7).

   b. If the Enable Trap Forwarding button is selected, deselect it, then wait 15 seconds before proceeding with Step c.

   c. Select the Enable Trap Forwarding button.

6

Managing Fault Server Components

This chapter describes how to manage Fault Server components, such as alarms, events, and traps. For instructions on how to start the Fault Server application, refer to Chapter 5.

Managing Alarms

The Fault Server application enables you to perform the following management tasks on alarms:

- Change the sort order of the alarm list.
- View information and additional details about alarms.
- Save alarm information to a disk file.
- Print alarm information.
- Modify information about an alarm, such as changing alarm state, adding or changing remarks, and assigning an alarm to an individual or group.

- Query for a different alarm list

To access the alarms you want to manage:

1. Start the Fault Server application (see “Starting the Fault Server Application” on page 5-2).

   The Fault Server Configuration dialog box appears, listing a default Fault Server and other available Fault Servers.

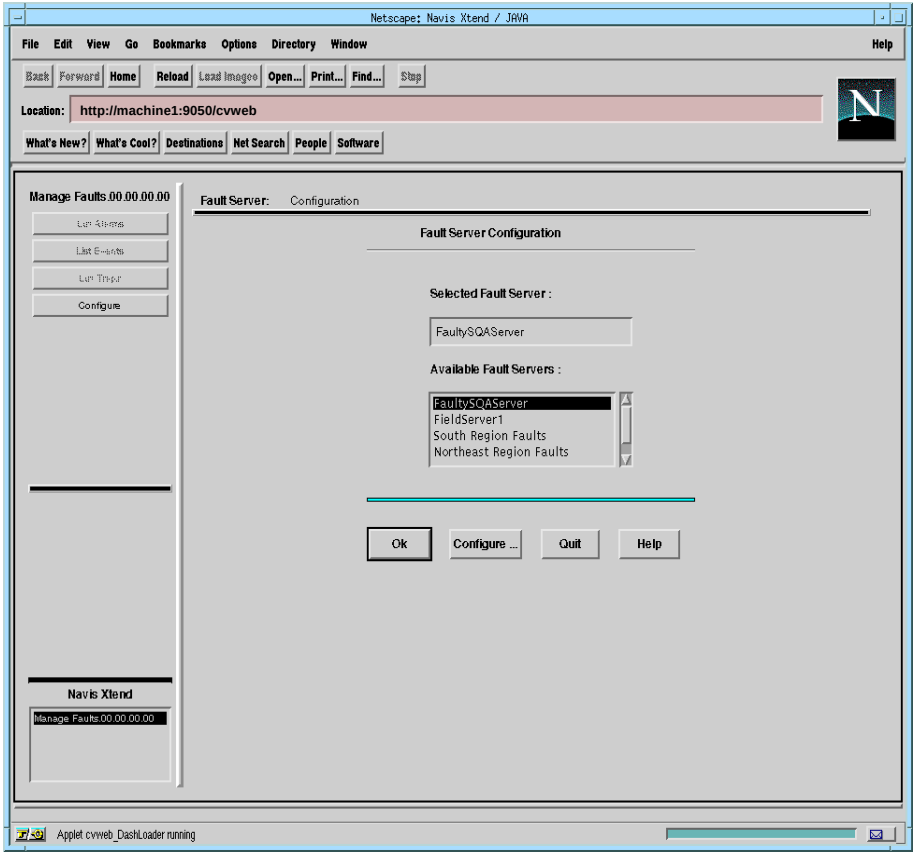


Figure 6-1. Fault Server Configuration Dialog Box

2. Select the Fault Server that manages the alarms you want to see. You can accept the default Fault Server or select another one from the drop-down list of the Available Fault Servers field. Choose OK

3. In the Manage Faults area (in the upper-left corner of the page), choose List Alarms.

   The Alarm List dialog box appears (Figure 6-2), showing alarms generated by the switches managed by the Fault Server. By default, the list shows all open alarms, sorted by alarm severity.

   The Count field indicates the total number of alarms in the list. The Total Alarms field indicates the total number of alarms in the database.

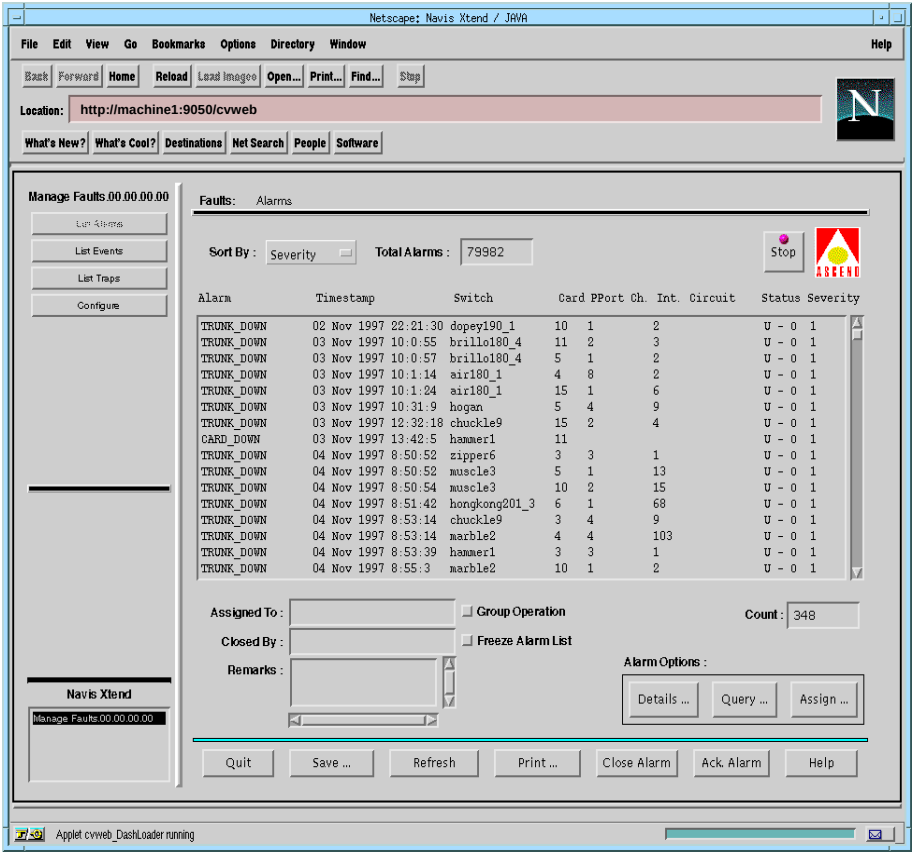


Figure 6-2. Alarm List Dialog Box

Keep in mind that with a long list of alarms, it may take some time for the entire list to display. If the list exceeds 500 alarms, the application displays the first 500 alarms. As additional alarms are generated, they are added to the list of 500. The total list cannot exceed 1,000 alarms.

If you do not want to continue downloading the entire list, choose Stop at any time. The alarm list stops downloading, but continues to update with new alarm information. Whenever monitoring is in progress, the Ascend logo blinks at a constant rate. If you do not want the alarm list to update, click on the Ascend logo. The alarm list remains static until you choose Refresh.

Changing the Sort Order

To change the sort order or an alarm list, select a sort order item from the drop-down list of the Sort By field (see Figure 6-2 on page 6-3). You can sort alarms by:

- Alarm severity (numerically)
- Alarm name (alphabetically)
- Alarm timestamp (from newest to oldest)
- Switch name (alphabetically)

The secondary sort order within any category is by alarm timestamp, from newest to oldest.

Viewing Information about Alarms

The alarm list (see Figure 6-2 on page 6-3) shows the following information about each alarm:

- Name of the alarm.
- Timestamp of the alarm.
- Name of the switch that generated the alarm.
- Component that generated the alarm, relative to the switch. For example, the component could be a circuit with the DLCI number 100, located on LPort interface 16, on PPort 3, on the card in slot 4 of the specified switch.
- Status of the alarm (A for Acknowledged, U for Unacknowledged, O for Open, CS for Closed by System, CU for Closed by User).
- Severity of the alarm.

As you view information about alarms, the alarm list dynamically updates with new alarm information. For each new alarm generated, the workstation sounds a beep and the new alarm is added to the alarm list. Some alarms in the list can be replaced by new alarms. For example, a BOARD_PULLED alarm in the list can be replaced by a newer BOARD_INSERTED alarm. And, a series of PPORT_UP and PPORT_DOWN alarms can be replaced by a BOUNCING_PORT group alarm.

If you do not want the alarm list to update while you are viewing alarms, select Freeze Alarm List. The alarm list remains static until you either:

- Choose Refresh
- Deselect Freeze Alarm List

To view additional information about an alarm, select the alarm from the list. Fields at the bottom of the screen display additional information about the alarm (see Figure 6-3 on page 6-6):

Assigned To — Displays the individual or group to whom the alarm is assigned.

Closed By — Displays whether the alarm was closed by the system or by a user (or Not Applicable, if the alarm is Open).

Remarks — Displays comments entered for the alarm.

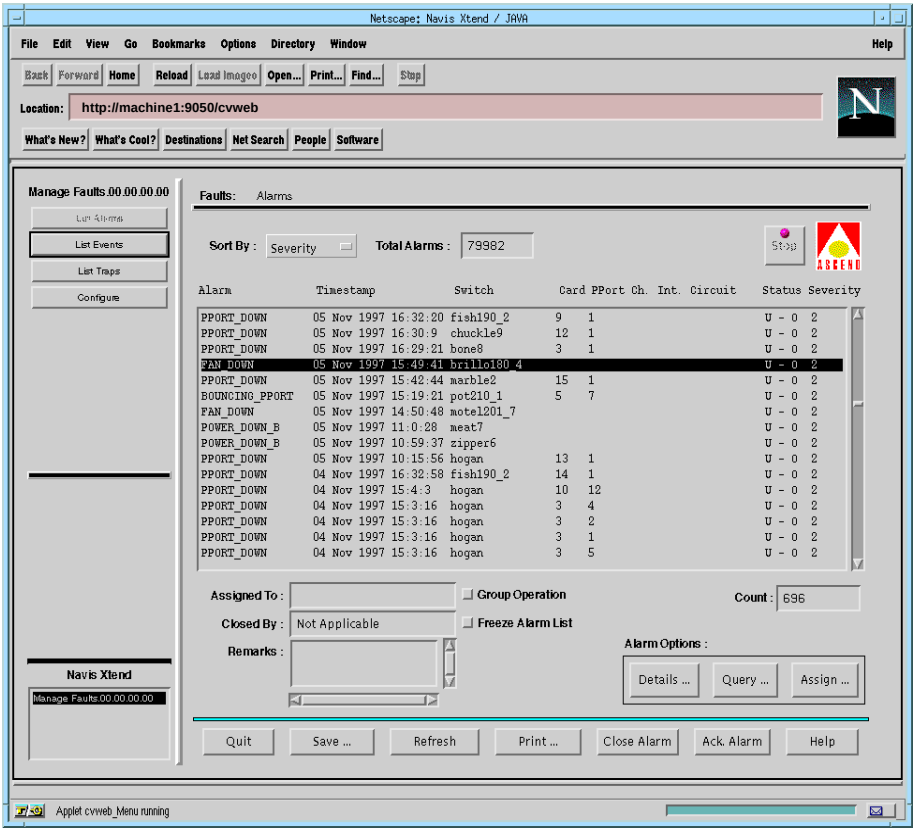


Figure 6-3. Alarm List with Additional Information Displayed

Saving Alarm Information

To save alarm information to a disk file on the Fault Server machine, choose Save. You are prompted to specify a destination file pathname where the alarm information will reside. The pathname is saved on the Fault Server machine.

Printing Alarm Information

To print the alarm information to a printer that is configured on the Fault Server machine, choose Print. You are prompted to specify a UNIX command to generate and spool the alarm report to the printer on the Fault Server machine.

Viewing Details about an Alarm

To display details about an alarm, select the alarm from the list and choose Details from the Alarm Options field.

The Alarm Details dialog box appears (see Figure 6-4 on page 6-8), showing the following details about the alarm you selected:

- Description of the alarm. For example: A physical port is down.
- Probable cause of the alarm. For example: A cable may be loose.
- Recommendations of how to rectify the problem. For example: Check the cable and connection.
- Remarks entered for the alarm. You can use this field to add or change remarks.
- State of the alarm, such as:
  - whether the alarm is open or closed
  - whether the alarm is acknowledged or unacknowledged
  - whether the alarm was closed by the system or by a user (or Not Applicable, if the alarm is Open)
- Individual or group to whom the alarm is assigned. You can use this field to reassign the alarm to someone else.
- Alarm severity level. You can use this field to modify the severity level of the alarm.
- Timestamp when the alarm was last modified.
- Occurrence value for this alarm.
- IP address of the switch that generated the alarm.

- Fields indicating the component that generated the alarm, relative to the switch, including card ID, PPort ID, channel ID, LPort interface ID, LPort name, circuit ID and circuit name.

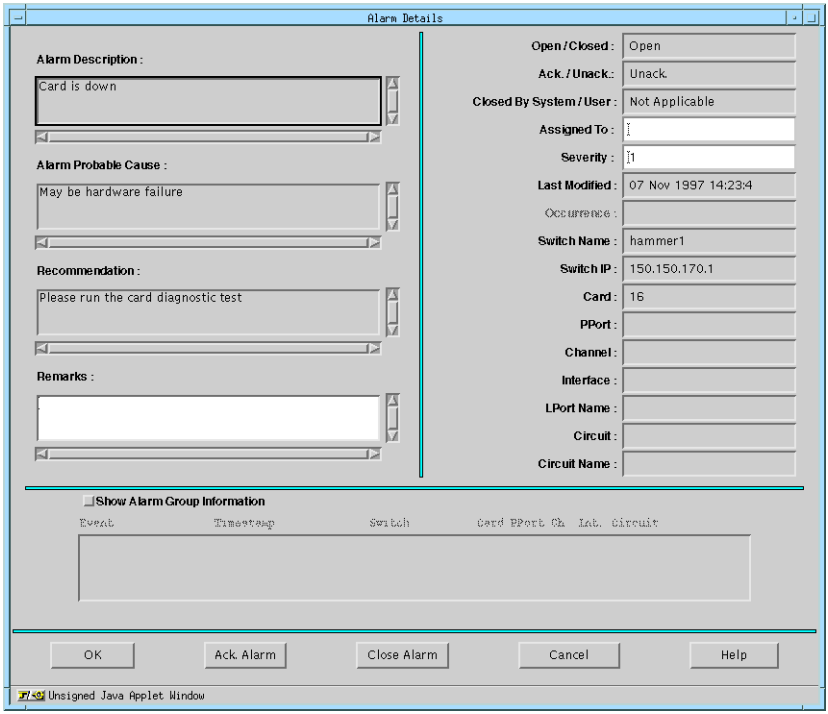


Figure 6-4. Alarm Details Dialog Box

If the alarm is a group alarm, you can view any related events. Select Show Alarm Group Information. The Alarm Group Information fields update with event information (Figure 6-5).

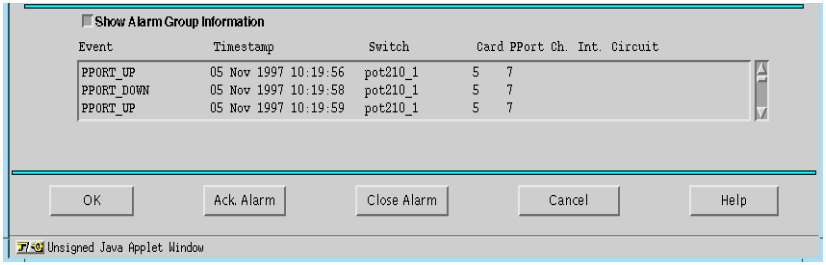


Figure 6-5. Alarm Group Information Fields

You can change the state of the alarm:

- Choose Ack. Alarm to acknowledge the alarm (see Figure 6-4 on page 6-8).
- Choose Close Alarm to close the alarm.

You are prompted to confirm the change.

When you finish viewing details, choose OK. If you made changes to the alarm, the Fault Server updates the alarm with the new information. If you do not want to save your changes, choose Cancel.

Modifying Alarm Information

You can make the following modifications to alarm information:

- Change the state of an alarm
- Add or change remarks for an alarm
- Assign an alarm to an individual or group

Changing the Alarm State

To change the state of an alarm:

1. From the alarm list (see Figure 6-2 on page 6-3), select one or more alarms to change:
   - To select a *single* alarm, highlight the alarm.
   - To select *multiple* alarms, choose Group Operation. Then, highlight the alarms to be changed.
2. Change the state of the alarm(s):
   - Choose Ack. Alarm to acknowledge the alarm(s).
   - Choose Close Alarm to close the alarm(s).

   You are prompted to confirm the change.

When you finish making changes, choose Save. You are prompted to confirm the save.

You can also use the Alarm Details dialog box to change the state of an alarm. For instructions, refer to “Viewing Details about an Alarm” on page 6-7.

You can also change the severity level of an alarm using the Alarm Details dialog box. For instructions, refer to “Viewing Details about an Alarm” on page 6-7.

Adding or Changing Remarks

You can add or change remarks for an alarm or alarms. If you select a single alarm, any remarks that you add will be appended to existing remarks for that alarm. In single alarm mode, you can also modify existing remarks. If you select multiple alarms, any remarks that you add will overwrite existing remarks for those alarms.

To add or change remarks for alarms:

1. Select one or more alarms from the alarm list (see Figure 6-2 on page 6-3) and choose Assign from the Alarm Options field.

   The Alarm Assignment dialog box appears (Figure 6-6).

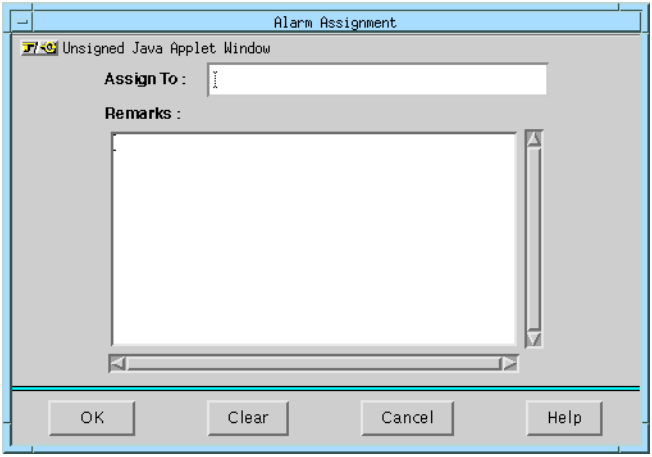


Figure 6-6. Alarm Assignment Dialog Box

2. Enter remarks directly in the Remarks field:

   – If you selected a single alarm, the remarks that you add will be appended to any existing remarks for that alarm. In single alarm mode, you can also modify any existing remarks.

   – If you selected multiple alarms, the remarks that you enter will overwrite any existing remarks for those alarms.

   You can choose Clear at any time to clear the entries in both the Assign To and the Remarks fields.

3. When you finish making changes, choose OK. If you do not want to save your changes, choose Cancel.

You can also use the Alarm Details dialog box to add or change remarks for an alarm. For instructions, refer to "Viewing Details about an Alarm" on page 6-7.

Assigning an Alarm

To assign one or more alarms to an individual or a group:

1. Select one or more alarms from the alarm list (see Figure 6-2 on page 6-3) and choose Assign from the Alarm Options field.

   The Alarm Assignment dialog box appears (see Figure 6-6 on page 6-10).

2. Enter the following information in the dialog box:

   – In the Assign To field, enter the name of the individual or group to whom you want the alarm(s) assigned.

   – In the Remarks field, enter any remarks to be added to the alarm(s). If you selected a single alarm, you can add new remarks or change existing remarks. If you selected multiple alarms, any remarks that you enter will overwrite existing remarks for those alarms.

   You can choose Clear at any time to clear the entries in both the Assign To and the Remarks fields.

3. When you finish making changes in the Alarm Assignment dialog box, choose OK. If you do not want to save your changes, choose Cancel.

You can also use the Alarm Details dialog box to reassign an alarm to a different individual or group. For instructions, refer to “Viewing Details about an Alarm” on page 6-7.

Querying for Alarms

By default, the alarm list displays all open alarms that are managed by the selected Fault Server. You can perform a query to display a different list of alarms.

For example, instead of listing all open alarms, you can specify only the alarms you are interested in. You can specify alarms of a particular severity, alarms from a particular list of switches, alarms generated during a particular time period, and so on.

Before you perform a query, select the Fault Server that manages the alarms you want to see:

1. In the Manage Faults area (in the upper-left corner of the page), choose Configure.

   The Fault Server Configuration dialog box appears, listing a default Fault Server and other available Fault Servers (see Figure 6-1 on page 6-2).

2. Select the Fault Server you want from the drop-down list of the Available Fault Servers field.

   Choose OK.

3. In the Manage Faults area (in the upper-left corner of the page), choose List Alarms.

   The Alarm List dialog box appears, showing alarms generated by the switches managed by the Fault Server you selected (see Figure 6-2 on page 6-3). By default, the list shows the most recent 500 open alarms, sorted by alarm severity.

Specifying the Query Criteria

To perform a query:

1. From the Alarm Options field, choose Query.

   The Alarm Query dialog box appears (Figure 6-7).

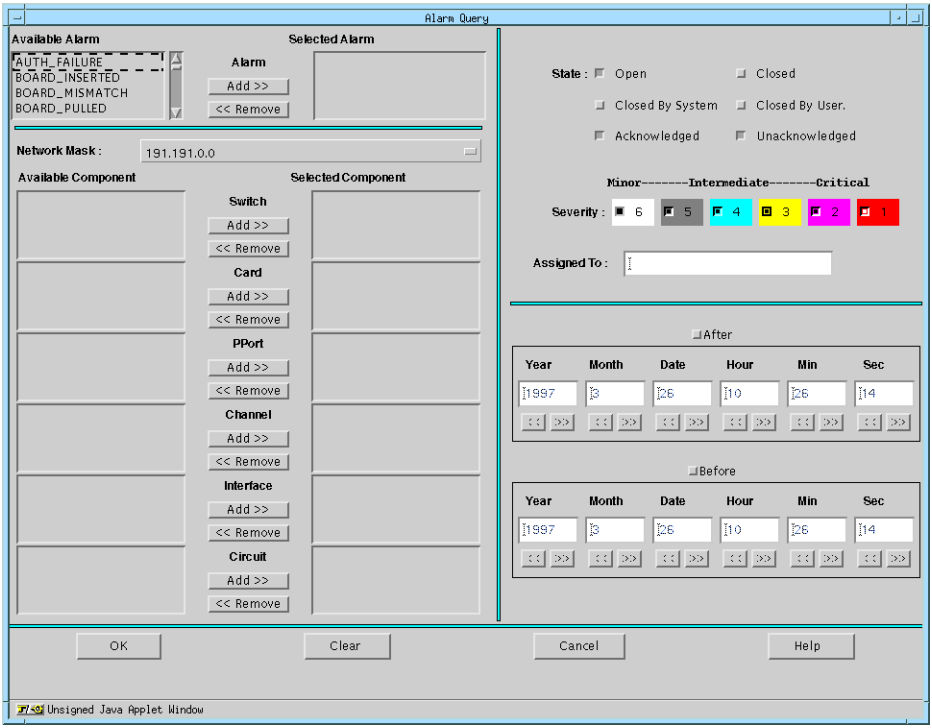


Figure 6-7. Alarm Query Dialog Box

2. Use the fields in the dialog box to specify the criteria of the query:

   a. Use the Available Alarm field to select the particular alarms you want:

      - To *add* an alarm, select the alarm name from the list and choose Add. The alarm is added to the Selected Alarm list.
      - To *remove* an alarm from the Selected Alarm list, select the alarm name from the list and choose Remove. The alarm is removed from the Selected Alarm List.

b. Use the drop-down list of the Network Mask field to select the IP address of the network that generates the alarms you want.

c. Use the Available Component fields to select the switches or the switch components that generate the alarms you want. To specify a component, first specify the component's parent in the hierarchy and then specify the object relative to that parent.

Example 1

To query for PPort alarms, specify the switch that contains a particular PPort (such as switch with IP address 148.152.0.1), the card that contains the PPort (the card in slot 2), and the PPort itself (the PPort in port 3).

Using this example, you would do the following:

- Specify the parent switch by selecting the appropriate switch from the Switch list and choosing Add to add it to the Selected Component field.
- Specify the card by selecting it from the Card list and choosing Add.
- Specify the PPort by selecting it from the PPort list and choosing Add.
- Leave the Channel, Interface, and Circuit fields blank.

Example 2

To query for alarms from multiple switches, specify the switches by selecting each switch from the Switch list and choosing Add. When you add multiple switches to the Selected Component field, you cannot specify individual switch components.

d. Use the State field to specify one or more states of the alarms you want.

e. Use the Severity field to specify one or more severities of the alarms you want.

Example 3

If you are interested in only certain high-severity alarms such as TRUNK_DOWN or BOARD_PULLED, but are not interested in low-severity alarms such as CARD_ERROR or BOARD_INSERTED, specify only alarms of severity 1 and/or 2. Then, the alarm list will display only alarms of higher severity.

f. Use the Assigned To field to specify who is assigned to the alarms you want.

g. Use either the After or Before fields to enter a specific timestamp for the alarms you want to query. Use both fields to define a range.

- Use *After* to request alarms with timestamps on or after a particular date. Enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value.
- Use *Before* to request alarms with timestamps on or before a particular date. Enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value.
- Use *both After and Before* to request alarms within a timestamp range. With time range queries, newly generated alarms are *not* dynamically added to the Alarm list. To specify the lower limit in the range, select After. Then, either enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value. To specify the upper limit in the range, select Before. Then, either enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value.

You can choose Clear at any time to clear all selections you have made so far in the Alarm Query dialog box. Doing so specifies a default query for all open alarms managed by the Fault Server that you selected.

3. When you finish making changes in the Alarm Query dialog box, choose OK. If you do not want to save your changes, choose Cancel.

Once you choose OK, you return to the alarm list. The alarms listed match those you specified in your query.

Keep in mind that with a long list of alarms, it may take some time for the entire list to be displayed. If the list exceeds 500 alarms, the application displays the first 500 alarms. As additional alarms are generated, they are added to the list of 500 (unless you specified a time range query). The total list cannot exceed 1,000 alarms.

Managing Events

The Fault Server application enables you to perform the following management tasks on events:

- Change sort order of the event list
- View information about events
- Save event information to a disk file
- Print event information
- Query for a different event list

To access the events you want to manage:

1. Start the Fault Server application (see “Starting the Fault Server Application” on page 5-2).

   The Fault Server Configuration dialog box appears, listing a default Fault Server and other available Fault Servers (see Figure 6-1 on page 6-2).

2. Select the Fault Server that manages the events you want to see. You can accept the default Fault Server or select another one from the drop-down list of the Available Fault Servers field.

   Choose OK.

3. In the Manage Faults area (in the upper-left corner of the page), choose List Events.

   The Event List dialog box appears (see Figure 6-8 on page 6-17), showing events generated by the switches managed by the Fault Server you selected. By default, the list shows all events, sorted by timestamp.

   The Count field indicates the total number of events in the list. The Total Events field indicates the total number of events in the database.

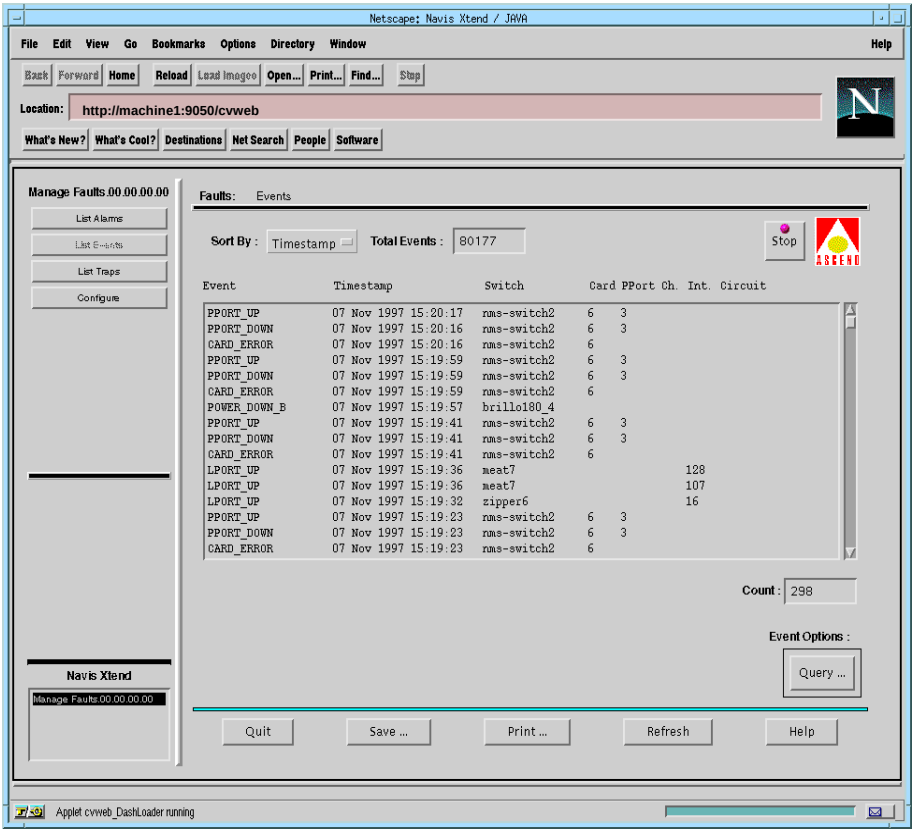


Figure 6-8. Event List Dialog Box

Keep in mind that with a long list of events, it may take some time for the entire list to display. If the list exceeds 500 events, the application displays the first 500 events. As additional events are generated, they are added to the list of 500. The total list cannot exceed 1,000 events.

If you do not want to continue downloading the entire list, you can choose Stop at any time. The event list stops downloading, but continues to update with new event information. Whenever monitoring is in progress, the Ascend logo blinks at a constant rate. If you do not want the event list to update, select the Ascend logo. The event list remains static until you choose Refresh.

Changing Sort Order

To change the sort order, select a sort order item from the drop-down list of the Sort By field (see Figure 6-8 on page 6-17). You can sort events by:

- Event name (alphabetically)
- Event timestamp (from newest to oldest)
- Switch name (alphabetically)

The secondary sort order within any category is by event timestamp, from newest to oldest.

Viewing Information about Events

The event list shows the following information about each event:

- Name of the event.
- Timestamp of the event.
- Name of the switch that generated the event.
- Component that generated the event, relative to the switch. For example, the component could be a circuit with the DLCI number 100, located on LPort interface 16, on PPort 3, on the card in slot 4 of the specified switch.

As you view information about events, the event list dynamically updates with new event information. For each new event generated, the workstation sounds a beep and the new event is added to the event list.

Saving Event Information

To save event information to a disk file on the Fault Server machine, choose Save. You are prompted to specify a destination file pathname where the event information will reside. The pathname is saved on the Fault Server machine.

Printing Event Information

To print the event information to a printer that is configured on the Fault Server machine, choose Print. You are prompted to specify a UNIX command to generate and spool the event report to the printer on the Fault Server machine.

Querying for Events

By default, the event list displays all events that are managed by the selected Fault Server. You can perform a query to display a different list of events.

For example, instead of listing all events, you can specify only the events you are interested in. You can specify events from a particular list of switches, events generated during a particular time period, events by name, and so on.

Before you perform a query, select the Fault Server that manages the events you want to see:

1. In the Manage Faults area (in the upper-left corner of the page), choose Configure.

   The Fault Server Configuration dialog box appears, listing a default Fault Server and other available Fault Servers (see Figure 6-1 on page 6-2).

2. Select the Fault Server you want from the drop-down list of the Available Fault Servers field.

   Choose OK.

3. In the Manage Faults area (in the upper-left corner of the page), choose List Events.

   The Event List dialog box appears, showing events generated by the switches managed by the Fault Server you selected (see Figure 6-8 on page 6-17). By default, the list shows the most recent 500 events, sorted by timestamp.

Specifying the Query Criteria

To perform a query:

1. From the Events Options field, choose Query.

   The Event Query dialog box appears (Figure 6-9).

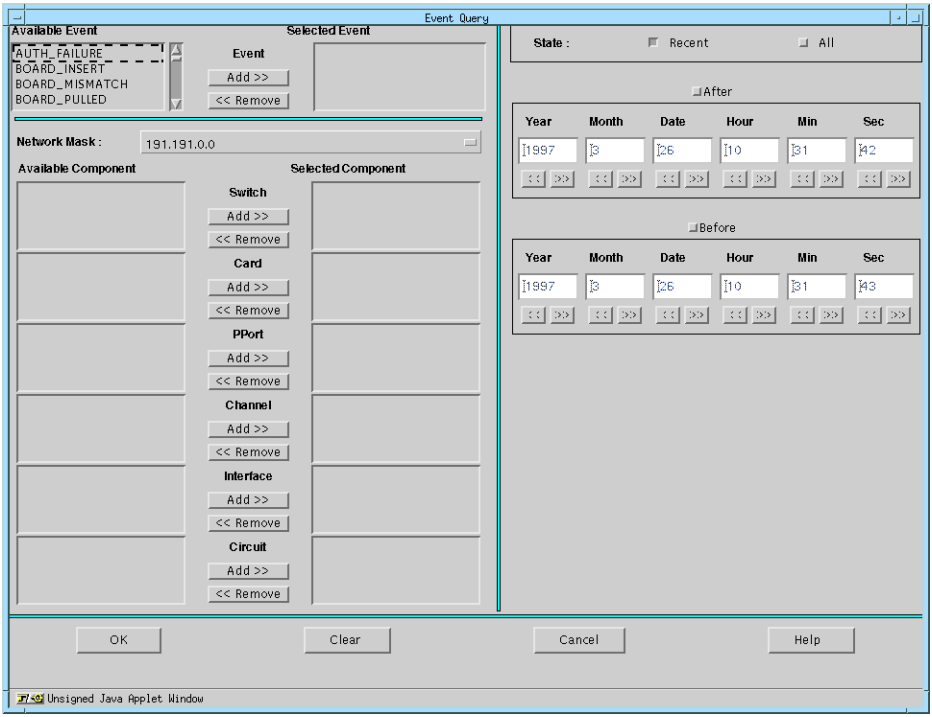


Figure 6-9. Event Query Dialog Box

2. Use the fields in the dialog box to specify the criteria of the query:

   a. Use the Available Event field to select the particular events you want:

   - To *add* an event, select the event name from the list and choose Add. The event is added to the Selected Event list.
   - To *remove* an event from the Selected Event list, select the event name from the list and choose Remove. The event is removed from the Selected Event List.

b. Use the drop-down list of the Network Mask field to select the IP address of the network that generates the events you want.

c. Use the Available Component fields to select the switches or the switch components that generate the events you want. To specify a component, first specify the component's parent in the hierarchy and then specify the object relative to that parent.

Example 1

To query for PPort events, specify the switch that contains a particular PPort (such as switch with IP address 148.152.0.1), the card that contains the PPort (the card in slot 2), and the PPort itself (the PPort in port 3).

Using this example, you would do the following:

- Specify the parent switch by selecting the appropriate switch from the Switch list and choosing Add to add it to the Selected Component field.
- Specify the card by selecting it from the Card list and choosing Add.
- Specify the PPort by selecting it from the PPort list and choosing Add.
- Leave the Channel, Interface, and Circuit fields blank.

Example 2

To query for events from multiple switches, specify the switches by selecting each switch from the Switch list and choosing Add. When you add multiple switches to the Selected Component field, you cannot specify individual switch components.

d. Use the State fields to dictate whether to query for the most recent events or all events. The default selection is Recent. If you select Recent, events are queried from the event buffer table, which maintains only the most recent events, up to 1,000 total. If you select All, events are queried from the base event table, which maintains all events (both recent and old).

If you select All, performance may be impacted. The All query is a one-time query; no automatic updates occur in All mode.

e. Use either the After or Before fields to enter a specific timestamp for the events you want to query. Use both fields to define a range.

- Use *After* to request events with timestamps on or after a particular date. Enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value.
- Use *Before* to request events with timestamps on or before a particular date. Enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value.
- Use *both After and Before* to request events within a timestamp range. With time range queries, newly generated events are *not* dynamically added to the Events list. To specify the lower limit in the range, select After. Then, either enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value. To specify the upper limit in the range, select Before. Then, either enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value.

You can choose Clear at any time to clear all selections you have made so far in the Events Query dialog box. Doing so specifies a default query for all open alarms managed by the Fault Server that you selected.

3. When you finish making changes in the Event Query dialog box, choose OK. If you do not want to save your changes, choose Cancel.

Once you choose OK, you return to the event list. The events listed match those you specified in your query.

Be aware that with a long list of events, or if you selected All mode in the State field, it may take some time for the entire list to display. If the list exceeds 500 events, the application displays the first 500 events. As additional events are generated, they are added to the list of 500 (unless you specified a time range query). The total list cannot exceed 1,000 events.

Managing Traps

The Fault Server application enables you to perform the following management tasks on traps:

- Change sort order of the trap list
- View information about traps
- Save trap information to a disk file
- Print trap information
- Query for a different trap list

To access the traps you want to manage:

1. Start the Fault Server application (see “Starting the Fault Server Application” on page 5-2).

   The Fault Server Configuration dialog box appears, listing a default Fault Server and other available Fault Servers (see Figure 6-1 on page 6-2).

2. Select the Fault Server that manages the traps you want to see. You can accept the default Fault Server or select another one from the drop-down list of the Available Fault Servers field.

   Choose OK.

3. In the Manage Faults area (in the upper-left corner of the page), choose List Traps.

   The Trap List dialog box appears (see Figure 6-10 on page 6-24), showing traps generated by the switches managed by the Fault Server. By default, the list shows all traps, sorted by timestamp.

   The Count field indicates the total number of traps in the list. The Total Traps field indicates the total number of traps in the database.

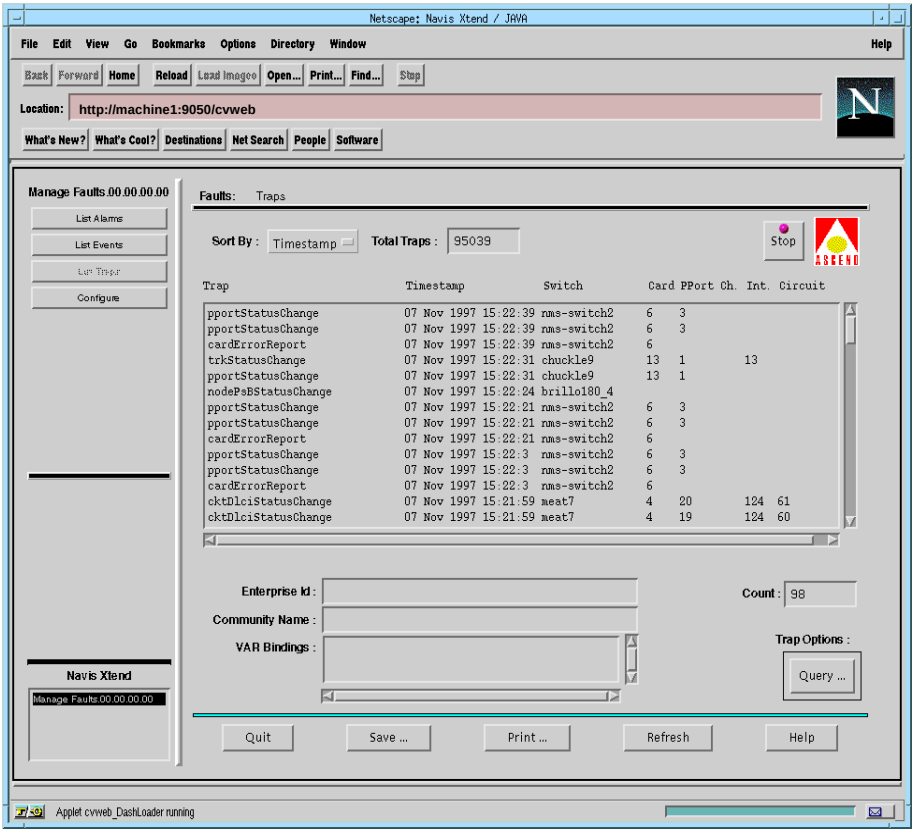


Figure 6-10. Trap List Dialog Box

Keep in mind that with a long list of traps, it may take some time for the entire list to be displayed. If the list exceeds 500 traps, the application displays the first 500 traps. As additional traps are generated, they are added to the list of 500. The total list cannot exceed 1,000 events.

If you do not want to continue downloading the entire list, you can choose Stop at any time. The trap list stops downloading, but continues to update with new trap information. Whenever monitoring is in progress, the Ascend logo blinks at a constant rate. If you do not want the trap list to update, click on the Ascend logo. The trap list remains static until you choose Refresh.

Changing the Sort Order

To change the sort order of the trap list, select a sort order item from the drop-down list of the Sort By field (see Figure 6-10 on page 6-24). You can sort traps by:

- Trap timestamp (from newest to oldest)
- Switch name (alphabetically)
- Trap name (alphabetically)

The secondary sort order within any category is by trap timestamp, from newest to oldest.

Viewing Information about Traps

The trap list shows the following information about each trap:

- Name of the trap.
- Timestamp of the trap.
- Name of the switch that generated the trap.
- Component that generated the trap, relative to the switch. For example, the component could be a circuit with the DLCI number 100, located on LPort interface 16, on PPort 3, on the card in slot 4 of the specified switch.

To view additional information about a trap, select the trap from the list. Fields at the bottom of the screen display additional information about the trap (see Figure 6-11 on page 6-26).

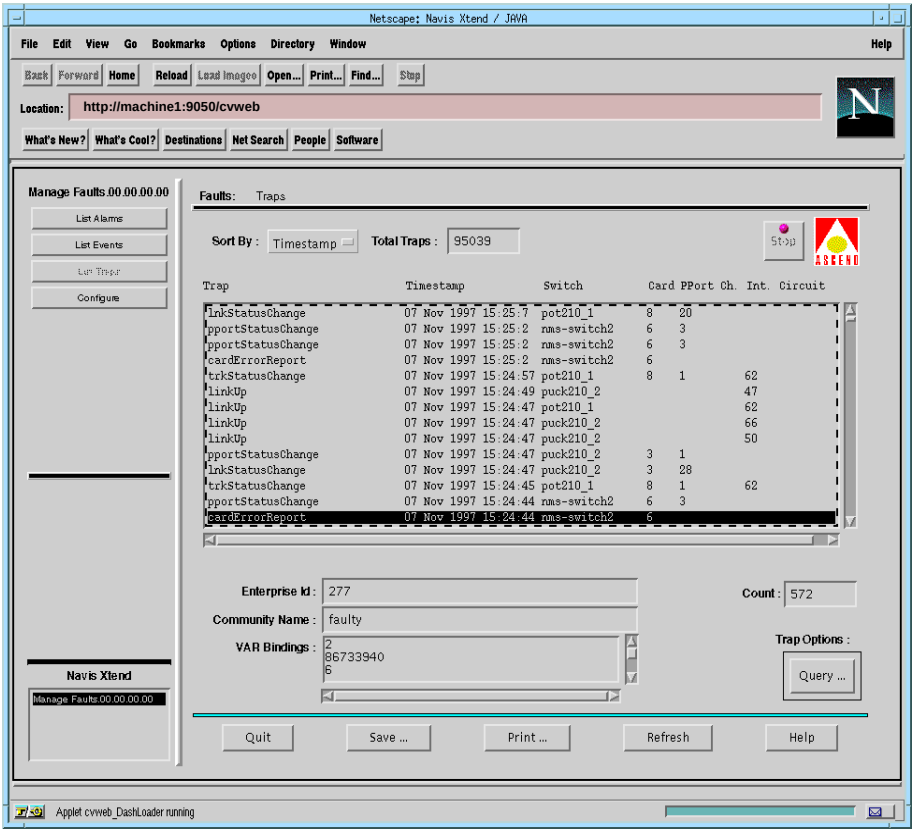


Figure 6-11. Trap List with Additional Information Displayed

This information identifies what MIB to use to interpret the trap:

Enterprise Id — Displays the enterprise ID associated with the trap.

Community Name — Displays the community string associated with the trap.

VAR Bindings — Displays the variable values associated with the trap.

As you view information about traps, the trap list dynamically updates with new trap information. For each new trap generated, the workstation sounds a beep and the new trap is added to the trap list.

Saving Trap Information

To save trap information to a disk file on the Fault Server machine, choose Save. You are prompted to specify a destination file pathname where the trap information will reside. The pathname is saved on the Fault Server machine.

Printing Trap Information

To print the trap information to a printer that is configured on the Fault Server machine, choose Print. You are prompted to specify a UNIX command to generate and spool the trap report to the printer on the Fault Server machine.

Querying for Traps

By default, the trap list displays all traps that are managed by the selected Fault Server. You can perform a query to display a different list of traps.

For example, instead of listing all traps, you can specify only the traps you are interested in. You can specify traps from a particular list of switches, traps generated during a particular time period, traps by name, and so on.

Before you perform a query, select the Fault Server that manages the traps you want to see:

1. In the Manage Faults area (in the upper-left corner of the page), choose Configure.

   The Fault Server Configuration dialog box appears, listing a default Fault Server and other available Fault Servers (see Figure 6-1 on page 6-2).

2. Select the Fault Server you want from the drop-down list of the Available Fault Servers field.

   Choose OK.

3. In the Manage Faults area (in the upper-left corner of the page), choose List Traps.

   The Trap List dialog box appears (see Figure 6-10 on page 6-24) appears, showing traps generated by the switches managed by the Fault Server you selected. By default, the list shows the most recent 500 traps, sorted by timestamp.

Specifying the Query Criteria

To perform a query:

1. From the Trap Options field, choose Query.

   The Trap Query dialog box appears (Figure 6-12).

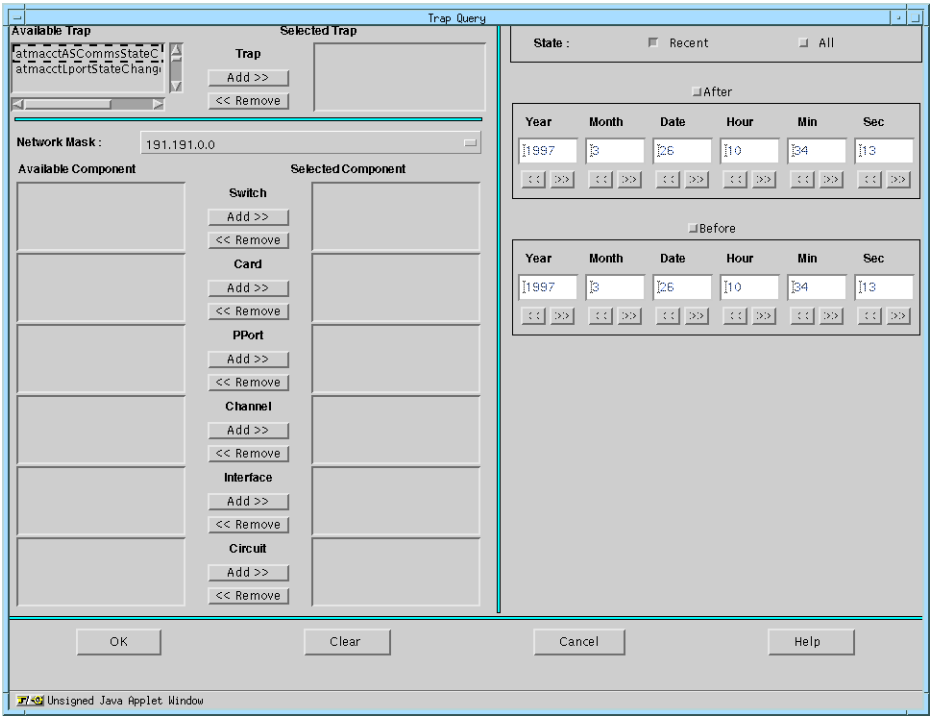


Figure 6-12. Trap Query Dialog Box

2. Use the fields in the dialog box to specify the criteria of the query:

   a. Use the Available Trap field to select the particular traps you want:

      - To *add* a trap, select the trap name from the list and choose Add. The selected trap is added to the Selected Trap list.
      - To *remove* a trap from the Selected Trap list, select the trap name from the list and choose Remove. The selected trap is removed from the Selected Trap List.

b. Use the drop-down list of the Network Mask field to select the IP address of the network that generates the traps you want.

c. Use the Available Component fields to select the switches or the switch components that generate the traps you want. To specify a component, first specify the component's parent in the hierarchy and then specify the object relative to that parent.

Example 1

To query for PPort traps, specify the switch that contains a particular PPort (such as switch with IP address 148.152.0.1), the card that contains the PPort (the card in slot 2), and the PPort itself (the PPort in port 3).

Using this example, you would do the following:

- Specify the parent switch by selecting the appropriate switch from the Switch list and choosing Add to add it to the Selected Component field.
- Specify the card by selecting it from the Card list and choosing Add.
- Specify the PPort by selecting it from the PPort list and choosing Add.
- Leave the Channel, Interface, and Circuit fields blank.

Example 2

To query for traps from multiple switches, specify the switches by selecting each switch from the Switch list and choosing Add. When you add multiple switches to the Selected Component field, you cannot specify individual switch components.

d. Use the State fields to dictate whether to query for the most recent traps or all traps. The default selection is Recent. If you select Recent, traps are queried from the trap buffer table, which maintains only the most recent traps, up to 1,000 total. If you select All, traps are queried from the base trap table, which maintains all traps (both recent and old).

If you select All, performance may be impacted. The All query is a one-time query; no automatic updates occur in All mode.

e. Use either the After or Before fields to enter a specific timestamp for the traps you want to query. Use both fields to define a range.

- Use *After* to request traps with timestamps on or after a particular date. Enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value.
- Use *Before* to request traps with timestamps on or before a particular date. Enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value.
- Use *both After and Before* to request traps within a timestamp range. With time range queries, newly generated traps are *not* dynamically added to the Traps list. To specify the lower limit in the range, select After. Then, either enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value. To specify the upper limit in the range, select Before. Then, either enter values for the specific year, month, date, hour, minute, and second, or use the >> and << buttons to select the value.

You can choose Clear at any time to clear all selections you have made so far in the Trap Query dialog box. Doing so specifies a default query for all traps managed by the Fault Server that you selected.

3. When you finish making changes in the Trap Query dialog box, choose OK. If you do not want to save your changes, choose Cancel.

Once you choose OK, you return to the trap list. The traps listed match those you specified in your query.

Be aware that with a long list of events, or if you selected All mode in the State field, it may take some time for the entire list to display. If the list exceeds 500 traps, the application displays the first 500 traps. As additional traps are generated, they are added to the list of 500 (unless you specified a time range query). The total list cannot exceed 1,000 alarms.

A

Reference Information

This appendix lists and describes the following information:

- Event, alarm, and rule mappings available for the Fault Server.
- Variables in the Fault Server MIB database.

Event, Alarm, and Rule Mappings

The Fault Server applies incoming traps to a set of maps that determine whether the trap will traverse from a trap to an event to an alarm:

- A trap that meets the criteria specified by a particular event map becomes an event.
- An event that meets the criteria specified by a particular alarm map becomes an alarm.

In the same way, the Fault Server applies each alarm to a set of rules to determine what action to take on the alarm. An alarm that meets the criteria specified by a particular rule is subjected to the action.

Table A-1 lists the event mappings for the Fault Server. The table shows which trap(s) become which event(s).

Table A-1. Event Mappings

Trap Name Trap Binding Value	Generic Trap ID	Specific Trap ID	Event Name (Description)
cardDown		29	CARD_DOWN
cardErrorReport		34	CARD_ERROR
cardRedundSwitchOver		33	REDUND_CARD_SO (Redundant card switchover)
cardUp		28	CARD_UP
chands1AlarmStateChange		107	DS1_ALARM_STATE
cktAtmStatusChange Trap binding 4 = 2		78	CKT_UP (Circuit up)
cktAtmReroute		79	CKT_REROUTE (Circuit rerouted)
cktAtmStatusChange Trap binding 4 = 1		78	CKT_DOWN (Circuit down)
cktDlciStatusChange Trap binding 3 = 1		20	CKT_DOWN (Circuit down)
cktDlciStatusChange Trap binding 3 = 2		20	CKT_UP (Circuit up)
cktNdcThreshCrossAlarmClp0		100	THRESHOLD_CROSS (Threshold crossing alert)
coldStart	0		COLDSTART (Switch coldstart)
linkDown	2		LPORT_DOWN
linkUp	3		LPORT_UP
lportAuthenticationFailure		86	AUTH_FAILURE (Authentication failure)

Table A-1. Event Mappings (Continued)

Trap Name Trap Binding Value	Generic Trap ID	Specific Trap ID	Event Name (Description)
lportCongests		18	LPORT_CONGESTED
lportErrorExceedThreshold		23	FRAME_ERR_THRESH (Frame error threshold exceeded)
lportIlmiSC Trap binding 2 = 1		138	ILMI_DOWN
lportIlmiSC Trap binding 2 = 2		138	ILMI_REGISTERING
lportIlmiSC Trap binding 2 = 3		138	ILMI_UP
lportNtmSeverCongestStatusChange		99	LPORT_CONGESTED
nodeAuthenticationFailure		102	AUTH_FAILURE (Authentication failure)
nodeBoardInserted		1	BOARD_INSERT
nodeBoardMismatch		3	BOARD_MISMATCH
nodeBoardPulled		2	BOARD_PULLED
nodeFanStatusChange Trap binding 2 = 1		6	FAN_UP
nodeFanStatusChange Trap binding 2 = 2		6	FAN_DOWN
nodeFanStatusChange Trap binding 2 = 3		6	FAN_MARGINAL
nodeFlashMemErr		13	MEM_ERR_FLASH
nodeInternalErr		16	INTERNAL_ERR
nodePramErr		14	MEM_ERR_PRAM
nodePsAStatusChange Trap binding 1 = 2		4	POWER_DOWN_A (Power supply A down)

Table A-1. Event Mappings (Continued)

Trap Name Trap Binding Value	Generic Trap ID	Specific Trap ID	Event Name (Description)
nodePsAStatusChange Trap binding 1 = 4		4	POWER_MARGINAL_A (Power supply A marginal)
nodePsAStatusChange Trap binding 1 = 1		4	POWER_UP_A (Power supply A up)
nodePsBStatusChange Trap binding 1 = 2		5	POWER_DOWN_B (Power supply B down)
nodePsBStatusChange Trap binding 1 = 4		5	POWER_MARGINAL_B (Power supply B marginal)
nodePsBStatusChange Trap binding 1 = 1		5	POWER_UP_B (Power supply B up)
nodePsCStatusChange Trap binding 1 = 2		113	POWER_DOWN_C (Power supply C down)
nodePsCStatusChange Trap binding 1 = 4		113	POWER_MARGINAL_C (Power supply C marginal)
nodePsCStatusChange Trap binding 1 = 1		113	POWER_UP_C (Power supply C up)
nodeRamErr		15	MEM_ERR_RAM
pportDSOLoopDownChange		41	DSO_LOOP_START
pportDSOLoopUpChange		42	DSO_LOOP_STOP
pportds1LoopChange Trap binding 3 ≠ 1		45	DS1_LOOP_START
pportds1LoopChange Trap binding 3 = 1		45	DS1_LOOP_STOP
pportdsx3LoopChange Trap binding 3 ≠ 1		44	DSX3_LOOP_START

Table A-1. Event Mappings (Continued)

Trap Name Trap Binding Value	Generic Trap ID	Specific Trap ID	Event Name (Description)
pportdsx3LoopChange Trap binding 3 = 1		44	DSX3_LOOP_STOP
pportInterfaceMismatch		22	IF_MISMATCH (Interface mismatch)
pportPerfMonTCA		109	THRESHOLD_CROSS (Threshold crossing alert)
pportStatusChange Trap binding 3 = 2		17	PPORT_DOWN
pportStatusChange Trap binding 3 = 3		17	PPORT_TESTING
pportStatusChange Trap binding 3 = 1		17	PPORT_UP
trkBuAttempt		38	TRUNK_BACKUP
trkBuFailure		39	TRNK_BKUP_FAIL (Trunk backup failure)
trkBuReleased		40	TRNK_BKUP_RELEASED (Trunk backup released)
trkStatusChange Trap binding 5 ≠ 7		19	TRUNK_DOWN
trkStatusChange Trap binding 5 = 7		19	TRUNK_UP
warmStart	1		WARMSTART (Switch coldstart)

Table A-2 lists the alarm mappings for the Fault Server. Specifically, the table shows:

- Which event becomes which alarm.
- What severity is assigned each alarm.

Table A-2. Alarm Mappings

Event Name (Description)	Alarm Name	Severity
AUTH_FAILURE (Authentication failure)	AUTH_FAILURE	4
BOARD_INSERT	BOARD_INSERTED	4
BOARD_MISMATCH	BOARD_MISMATCH	4
BOARD_PULLED	BOARD_PULLED	2
CARD_DOWN	CARD_DOWN	1
CARD_ERROR	CARD_ERROR	4
CARD_UP	CARD_UP	6
CKT_DOWN (Circuit down)	CKT_DOWN	4
CKT_REROUTE (Circuit rerouted)	CKT_REROUTE	6
CKT_UP (Circuit up)	CKT_UP	6
COLDSTART (Switch coldstart)	COLDSTART	3
DS1_ALARM_STATE (Threshold crossing alert)	DS1_ALARM_STATE	4
FAN_DOWN	FAN_DOWN	2
FAN_MARGINAL	FAN_MARGINAL	4
FAN_UP	FAN_UP	6
FRAME_ERR_THRESH (Frame error threshold exceeded)	FRAME_ERR_THRESH	4
IF_MISMATCH (Interface mismatch)	IF_MISMATCH	4
INTERNAL_ERR	INTERNAL_ERR	3

Table A-2. Alarm Mappings (Continued)

Event Name (Description)	Alarm Name	Severity
LPORT_CONGESTED	LPORT_CONGESTED	4
LPORT_DOWN	LPORT_DOWN	3
LPORT_UP	LPORT_UP	6
MEM_ERR_FLASH	MEMORY_ERR	4
MEM_ERR_PRAM	MEMORY_ERR	3
MEM_ERR_RAM	MEMORY_ERR	3
POWER_DOWN_A (Power supply A down)	POWER_DOWN_A	2
POWER_DOWN_B (Power supply B down)	POWER_DOWN_B	2
POWER_DOWN_C (Power supply C down)	POWER_DOWN_C	2
POWER_MARGINAL_A (Power supply A marginal)	POWER_MARGINAL_A	4
POWER_MARGINAL_B (Power supply B marginal)	POWER_MARGINAL_B	4
POWER_MARGINAL_C (Power supply C marginal)	POWER_MARGINAL_C	4
POWER_UP_A (Power supply A up)	POWER_UP_A	6
POWER_UP_B (Power supply B up)	POWER_UP_B	6
POWER_UP_C (Power supply C up)	POWER_UP_C	6
PPORT_DOWN	PPORT_DOWN	2
PPORT_TESTING	PPORT_TESTING	5
PPORT_UP	PPORT_UP	6

Table A-2. Alarm Mappings (Continued)

Event Name (Description)	Alarm Name	Severity
REDUND_CARD_SO (Redundant card switchover)	REDUND_CARD_SO	4
TRUNK_BACKUP	TRUNK_BACKUP	2
TRNK_BKUP_FAIL (Trunk backup failure)	TRUNK_BKUP_FAIL	1
TRNK_BKUP_RELEASED (Trunk backup released)	TRUNK_BKUP_RELEASED	4
TRUNK_DOWN	TRUNK_DOWN	1
TRUNK_UP	TRUNK_UP	6

Table A-3 lists the group alarm mappings for the Fault Server. Specifically, the table shows:

- Which individual events become which group alarm.
- How often the events must occur in a particular time period to cause the group alarm to occur.
- What severity is assigned each group alarm.

Table A-3. Group Alarm Mappings

Individual Events	Recurrence Time	Recurrence Count	Group Alarm Name	Severity
PPORT_UP PPORT_DOWN	1800 Seconds	30	BOUNCING_PPORT	2
LPORT_UP LPORT_DOWN	1800 Seconds	30	BOUNCING_LPORT	3

Table A-4 lists the rule mappings for the Fault Server. Specifically, the table shows what rule action(s) are taken on behalf of each alarm.

Table A-4. Rule Mappings

Alarm Name (Description)	Rules
BOARD_INSERTED	Clear BOARD_INSERTED alarm Close BOARD_PULLED alarm
BOARD_MISMATCH	Clear BOARD_MISMATCH alarm
BOARD_PULLED	Clear BOARD_PULLED alarm Clear CARD_DOWN alarm Close BOARD_INSERTED alarm
BOUNCING_LPORT	Clear BOUNCING_LPORT alarm Clear LPORT_DOWN alarm
BOUNCING_PPORT	Clear BOUNCING_PPORT alarm Clear PPORT_DOWN alarm
CARD_DOWN	Hold 60 seconds Clear CARD_DOWN alarm Clear PPORT_DOWN alarm
CARD_ERROR	Clear CARD_ERROR alarm
CARD_UP	Close CARD_DOWN alarm
CKT_DOWN (Circuit down)	Hold 60 seconds Clear CKT_DOWN alarm
CKT_UP (Circuit up)	Close CKT_DOWN alarm
FAN_DOWN	Clear FAN_DOWN alarm Cancel FAN_MARGINAL alarm
FAN_MARGINAL	Clear FAN_MARGINAL alarm
FAN_UP	Close FAN_DOWN alarm Close FAN_MARGINAL alarm

Table A-4. Rule Mappings (Continued)

Alarm Name (Description)	Rules
FRAME_ERR_THRESH	Close FRAME_ERR_THRESH
LPORT_CONGESTED	Close LPORT_CONGESTED
LPORT_DOWN	Hold 60 seconds Clear LPORT_DOWN alarm Clear CKT_DOWN alarm
LPORT_UP	Close LPORT_DOWN alarm
POWER_DOWN_A (Power supply A down)	Clear POWER_DOWN_A alarm Cancel POWER_MARGINAL_A alarm
POWER_DOWN_B (Power supply B down)	Clear POWER_DOWN_B alarm Cancel POWER_MARGINAL_B alarm
POWER_DOWN_C (Power supply C down)	Clear POWER_DOWN_C alarm Cancel POWER_MARGINAL_C alarm
POWER_MARGINAL_A (Power supply A marginal)	Clear POWER_MARGINAL_A alarm
POWER_MARGINAL_B (Power supply B marginal)	Clear POWER_MARGINAL_B alarm
POWER_MARGINAL_C (Power supply C marginal)	Clear POWER_MARGINAL_C alarm
POWER_UP_A (Power supply A up)	Close POWER_DOWN_A alarm Close POWER_MARGINAL_A alarm
POWER_UP_B (Power supply B up)	Close POWER_DOWN_B alarm Close POWER_MARGINAL_B alarm
POWER_UP_C (Power supply C up)	Close POWER_DOWN_C alarm Close POWER_MARGINAL_C alarm
PPORT_DOWN	Hold 60 seconds Clear PPORT_DOWN alarm Clear CKT_DOWN alarm

Table A-4. Rule Mappings (Continued)

Alarm Name (Description)	Rules
PPORT_UP	Close PPORT_DOWN alarm
TRUNK_DOWN	Clear TRUNK_DOWN alarm
TRUNK_UP	Close TRUNK_DOWN alarm

Fault Server MIB Definitions

This section lists the variables in the Fault Server MIB database. The Fault Server uses this SNMP MIB to generate its own trap alarms.

```
-- The cascfltsrv Group

--

-- The following Mib objects are only used by the FaultServer

fltsrvSeverity OBJECT-TYPE
    SYNTAX  INTEGER {
        critical(1),
        major(2),
        minor(3),
        warning(4),
        info (5),
        cleared(6)
}
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
```

"This is the severity that the alarm is being changed to."

::= { cascfltsrv 1 }

fltsrvComponentID OBJECT-TYPE

SYNTAX OCTET STRING

ACCESS read-only

STATUS mandatory

DESCRIPTION

"This is the component ID for the component that the alarm

transition applies to. The format of this string is :

<switch IP>-<card number>-<Pport>-<Channel>-<Lport>-<Circuit>

This should enable the receiver to identify the specific object that is affected by this alarm."

::= { cascfltsrv 2 }

fltsrvAlarmText OBJECT-TYPE

SYNTAX OCTET STRING

ACCESS read-only

STATUS mandatory

DESCRIPTION

"This is a text string that describes the alarm. It is assumed that the severity field will identify whether an alarm condition is opened or closed. An example of a alarm text may be LPORT_DOWN. A severity value of 6 would mean that this condition had been cleared."

::= { cascfltsrv 3 }

B

Installation Worksheets

This appendix provides worksheets that you can use during the installation of Sybase 11 and other components of the Fault Server system. The installation scripts ask you for the parameter values listed on these worksheets. If you establish these values before the installation, the installation process will be easier.

We suggest that you photocopy the pages from this appendix and write the parameter values on the photocopied page. Refer to these entries during the installation process.

Sybase Installation Worksheet

The Sybase installation script prompts you for the parameter values in this worksheet. Complete this form before you start the Sybase installation.

Installing the Fault Server on an Existing CascadeView Sybase Server

General Installation Parameter

1. Media device pathname: _____

Setting Up the System for Sybase 11 Installation

2. Sybase 11 home directory: _____

   Recommended value: /opt/sybase

3. Database server name: _____

4. Error log filename: _____

   Recommended value: CASCADE_err.log

5. Database SA password: _____

   Recommended value: superbase

Using Raw Partitions for the Master Device

6. Fault Server data device pathname (Partition 7): _____

   Recommended value: /dev/rdsk/c0t1d0s7

Installing the Fault Server on a New Sybase Server

General Installation Parameter

1. Media device pathname: _____

Setting Up the System for Sybase 11 Installation

2. Sybase 11 home directory: _____
   Recommended value: /opt/sybase
3. Database server name: _____
4. Error log filename: _____
   Recommended value: CASCADE_err.log
5. Database SA password: _____
   Recommended value: superbase
6. NMS user's name: _____
   Recommended value: nms
7. NMS user's group name: _____
   Recommended value: staff
8. NMS user's home directory: _____
   Recommended value: /opt/nms

Using Raw Partitions For The Master Device

9. Master device pathname (Partition 0): _____
   Recommended value: /dev/rdsk/c0t1d0s0
10. System Procs device pathname (Partition 1): _____
    Recommended value: /dev/rdsk/c0t1d0s1

11. Fault Server data device pathname (Partition 3): _____

    Recommended value: /dev/rdsk/c0t1d0s3

12. Log device pathname (Partition 4): _____

    Recommended value: /dev/rdsk/c0t1d0s4

13. Master device size: _____

    Recommended value: 50MB (This is a minimum value.)

Installing Sybase 11

14. Number of user connections: _____

    Recommended value: 25 (This is a minimum value.)

Fault Server Components Installation Worksheet

The Fault Server system installation requires you to define parameter values for several of the Fault Server components — the Fault Server, the Fault Server application, and the Fault Server database and CascadeView database systems. Complete this form before you begin the installation.

General Installation Parameters

1. Media device pathname:_____

Database Configuration Parameters When Installing the Fault Server

2. Fault db host: _____

   Machine name of the Sybase server that maintains the Fault Server database.

3. Fault db Sybase Admin password: _____

   Sybase Administrator password.

4. CascadeView db host:_____

   Machine name of the Sybase server that maintains the CascadeView database.

Database Record Parameters When Installing the Fault Server Application

You need to create a separate record for each Fault Server with which the Fault Server application communicates. Establish the following values for each record:

5. Fault server host:_____

   Name of the machine that maintains the Fault Server.

6. Fault db host: _____

   Machine name of the Sybase server that maintains the Fault Server database.

7. Active NMS db host: _____

   Machine name of the Sybase server that maintains the CascadeView database.

C

Uninstallation Procedures

Uninstallation Instructions

This appendix presents instructions for uninstalling several of the Fault Server system components. For example, if you receive an updated version of the Fault Server product, you can first uninstall the older version of the components and then install the new version. To uninstall the Fault Server components, you use the UNIX utility called pkgrm.

The general steps for uninstalling the Fault Server system are shown in Figure C-1 on page C-2.

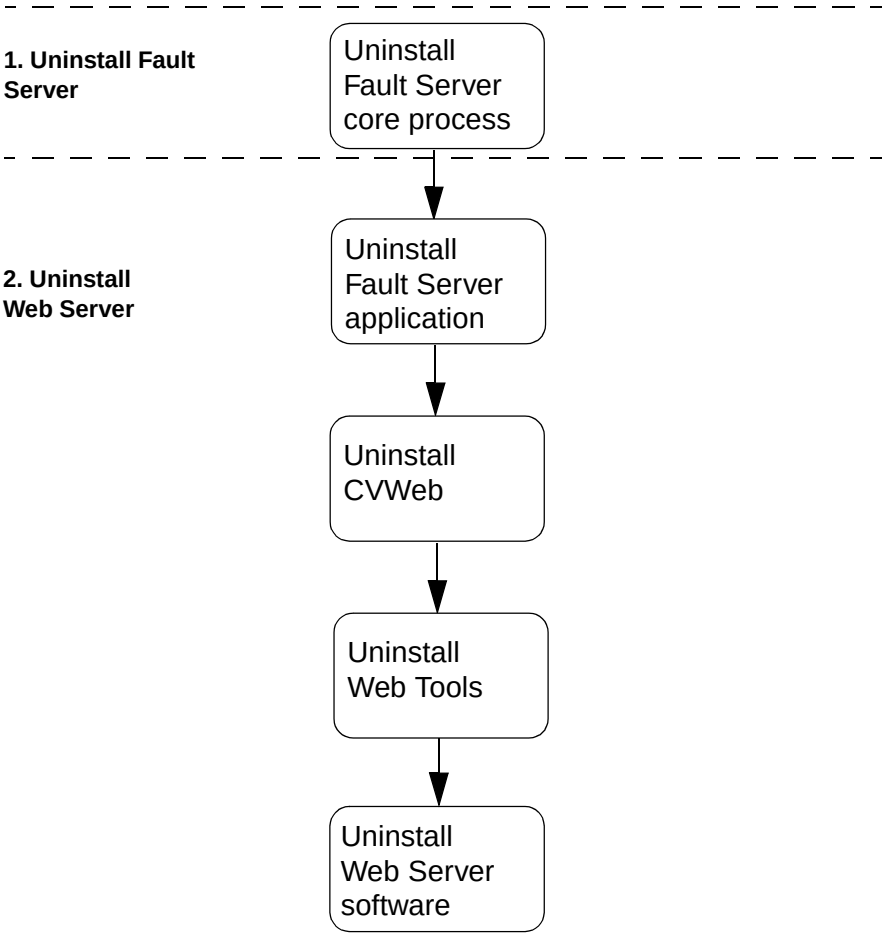


Figure C-1. Fault Server System Uninstallation Sequence

Uninstalling the Fault Server

This section describes how to uninstall the Fault Server core process using the pkgrm utility.

Follow these steps to uninstall the Fault Server core process:

1. Log on to the Fault Server workstation. Become root by entering **su - root**. At the prompt, enter the root password.

2. To uninstall the Fault Server core process using pkgrm, enter:

   ```
   pkgrm CASCfs
   ```

   The utility prompts you to verify the uninstall:

   ```
   The following package is currently installed:
      1 CASCfs    Cascade Fault Server
         (sparc) 01.00.00.00

   Do you want to remove this package?
   ```

3. To uninstall the Fault Server package, enter **y**.

   The uninstallation utility displays the message:

   ```
   ## Removing installed package instance <CASCfs>

   This package contains scripts which will be executed with
   super-user permission during the process of removing this package.

   Do you want to continue with the removal of <CASCfs> [y,n,?, q]
   ```

4. Enter **y** to continue.

   The uninstallation utility performs various verification functions and executes a pre-removal script.

   The uninstallation utility displays the confirmation message:

   ```
   Are you sure you want to UNINSTALL the Fault Server [y/n]?
   ```

5. Enter **y** to continue.

The utility completes the uninstallation:

```
Uninstall complete

Removal of <CASCfs> was successful.
```

If the Fault Server was installed in a directory other than the default directory (/opt), the uninstallation utility may fail. If you receive the message:

Removal of <CASCfs> partially failed

you need to rerun the pkgrm utility (starting at Step 2 on page C-3).

The uninstallation of the Fault Server core process is complete.

Uninstalling the Web Server Components

This section describes how to uninstall the Web Server components using the pkgrm utility.

To uninstall the Web Server components, you remove the following packages:

- Fault Server application package (CASCfsc)
- CVWeb package (CASCwc)
- Web Tools package (CASCwt)
- Web Server package (CASCws)

Use the steps in the following section to uninstall the Web Server components:

1. Log on to the Web Server workstation. Become root by entering **su - root**. At the prompt, enter the root password.
2. To uninstall the Web Server components using pkgrm, enter:

   `pkgrm CASCfsc CASCwc CASCwt CASCws`

   This command removes each of the packages in listed order. The utility starts with the Fault Server application package.

Uninstalling the Fault Server Application Package

The utility prompts you to verify the uninstall:

```
The following package is currently installed:
   1 CASCfsc   Cascade Fault Server Application
      (sparc) 01.00.00.00

Do you want to remove this package?
```

1. To uninstall the Fault Server application package, enter **y**.

   The uninstallation utility displays the message:

   ```
   ## Removing installed package instance <CASCfsc>

   This package contains scripts which will be executed with
   super-user permission during the process of removing this package.

   Do you want to continue with the removal of <CASCfsc> [y,n,?, q]
   ```

2. Enter **y** to continue.

   The uninstallation utility performs various verification functions and executes a pre-removal script.

   The uninstallation utility displays the confirmation message:

   ```
   Are you sure you want to UNINSTALL the Fault Server
   Application [y/n]?
   ```

3. Enter **y** to continue.

   The utility completes the uninstallation:

```
Uninstall complete

Removal of <CASCfsc> was successful.
```

If the Fault Server application was installed in a directory other than the default directory (/opt/cvweb/products), the uninstallation utility may fail. If you receive the message:

Removal of <CASCfsc> partially failed

you need to rerun the pkgrm utility.

The uninstallation of the Fault Server application is complete. Next, the utility removes the CVWeb package.

Uninstalling the CVWeb Package

The utility prompts you to verify the uninstall:

```
The following package is currently installed:
   1 CASCwc    Cascade CVWeb
      (sparc) 01.00.00.00

Do you want to remove this package?
```

1. To uninstall the CVWeb package, enter **y**.

   The uninstallation utility displays the message:

```
## Removing installed package instance <CASCwc>

This package contains scripts which will be executed with
super-user permission during the process of removing this package.

Do you want to continue with the removal of <CASCwc> [y,n,?, q]
```

2. Enter **y** to continue.

The uninstallation utility performs various verification functions and executes a pre-removal script.

The uninstallation utility displays the confirmation message:

```
Are you sure you want to UNINSTALL the CVWeb [y/n]?
```

3. Enter **y** to continue.

   The utility completes the uninstallation:

```
Uninstall complete

Removal of <CASCwc> was successful.
```

If the CVWeb package was installed in a directory other than the default directory (/opt/cvweb/products), the uninstallation utility may fail. If you receive the message:

Removal of <CASCwc> partially failed

you need to rerun the pkgrm utility.

The uninstallation of the CVWeb package is complete. Next, the utility removes the Web Tools package.

Uninstalling the Web Tools Package

The utility prompts you to verify the uninstall:

```
The following package is currently installed:
   1 CASCwt    Cascade Web Tools
      (sparc) 01.00.00.00

Do you want to remove this package?
```

1. To uninstall the Web Tools package, enter **y**.

The uninstallation utility displays the following message:

```
## Removing installed package instance <CASCwc>

This package contains scripts which will be executed with
super-user permission during the process of removing this package.

Do you want to continue with the removal of <CASCwc> [y,n,?, q]
```

2. Enter **y** to continue.

   The uninstallation utility performs various verification functions and executes a pre-removal script.

   The utility completes the uninstallation:

```
Removal of <CASCwt> was successful.
```

If the Web Tools package was installed in a directory other than the default directory (/opt/cvweb), the uninstallation utility may fail. If you receive the message:

Removal of <CASCwt> partially failed

you need to rerun the pkgrm utility.

The uninstallation of the Web Tools is complete. Next, the utility removes the Web Server package.

Uninstalling the Web Server Package

The utility prompts you to verify the uninstall:

```
The following package is currently installed:
   1 CASCws    Cascade Web Server
      (sparc) 01.00.00.00

Do you want to remove this package?
```

1. To uninstall the Web Server package, enter **y**.

The uninstallation utility displays the message:

```
## Removing installed package instance <CASCws>

This package contains scripts which will be executed with
super-user permission during the process of removing this package.

Do you want to continue with the removal of <CASCws> [y,n,?, q]
```

2. Enter **y** to continue.

   The uninstallation utility performs various verification functions and executes a pre-removal script.

   The uninstallation utility displays the confirmation message:

   ```
   Are you sure you want to UNINSTALL the CVWeb Web Server
   [y/n]?
   ```

3. Enter **y** to continue.

   The utility completes the uninstallation:

   ```
   Uninstall complete

   Removal of <CASCws> was successful.
   ```

If the Web Server was installed in a directory other than the default directory (/opt/cvweb/products), the uninstallation utility may fail. If you receive the message:

Removal of <CASCws> partially failed

you need to rerun the pkgrm utility.

The uninstallation of the Web Server is complete.

Index

V

W