I

Management and Monitoring Services

Novell® ZENworks® for Servers (ZfS) Management and Monitoring Services provides industry-standards-based monitoring, management, and reporting for heterogeneous network environments, including support for multi-protocol LAN/WAN networks and servers.

In addition, ZfS Management and Monitoring Services help you to proactively manage your NetWare® and Windows* NT* servers by responding faster to network problems and increasing overall system availability.

Management and Monitoring Services has the following components:

- **ConsoleOne®**, which provides the interface where you can manage and administer your network.
- **Management Site Services**, including:
  - Alarm Management
  - Database Administration
  - MIB Tools Administration
  - Monitoring Services
  - Network Discovery
  - Reporting
  - Role-Based Services
  - Topology Mapping
- **Server Management** for monitoring all the servers in your network
- **Traffic Analysis** for monitoring all traffic on Ethernet, token ring, or Fiber Distributed Data Interface (FDDI) network segments

The Management and Monitoring Services documentation contains the following sections:

- Chapter 1, “Configuring Management and Monitoring Services,” on page 25
- Chapter 2, “Using ConsoleOne with Management and Monitoring Services,” on page 59
- Chapter 3, “Understanding Network Discovery and Atlas Management,” on page 71
- Chapter 4, “Understanding Alarm Management,” on page 127
- Chapter 5, “Understanding Server Management,” on page 155
- Chapter 6, “Using the MIB Tools,” on page 211
- Chapter 7, “Monitoring Services,” on page 241
- Chapter 8, “Understanding Traffic Analysis,” on page 251
- Chapter 9, “Customizing Agent Configuration,” on page 367
- Chapter 10, “Protocol Decodes Suites Supported by ZfS,” on page 377
- Chapter 11, “ZENWorks Management and Monitoring Services Database,” on page 389
- Chapter 12, “Using Reports in Management and Monitoring Services,” on page 393
- Chapter 13, “Using SNMP Community Strings,” on page 411
- Chapter 14, “Documentation Content Changes,” on page 417

1 Configuring Management and Monitoring Services

To use ZENworks® for Servers (ZfS) Management and Monitoring Services effectively, you must correctly install and configure the components on your network. You should have already performed a basic installation of ZfS (see Installing and Setting Up Management and Monitoring Services in the ZfS *Installation* guide).

The following sections provide you with the concepts and instructions to help you configure ZfS so that you can use its features to manage your network:

- "Understanding Management and Monitoring Services" on page 25
- "Planning the Configuration" on page 31
- "Role-Based Administration" on page 34
- "Configuring Management and Monitoring Services" on page 52

Understanding Management and Monitoring Services

This guide provides information on understanding, planning, managing, and monitoring ZfS Management and Monitoring Services. This section provides information about the components of the ZfS Management and Monitoring Services.

Management and Monitoring Services contains the following components:

- "Management Site Services" on page 26
- "Server Management" on page 29
- "Traffic Analysis" on page 29
- "ConsoleOne" on page 30

Management Site Services

The Management Site Services include the following:

- "Network Discovery" on page 26
- "Database Administration" on page 26
- "Alarm Management" on page 27
- "Role-Based Services" on page 27
- "Reporting" on page 27
- "Topology Mapping" on page 28
- "MIB Tools Administration" on page 29
- "Monitoring Services" on page 29

Network Discovery

When network autodiscovery is started, the servers, routers, switches which are SNMP instrumented, and the services hosted on these devices and workstations, are automatically discovered. The discovered data is written to a .DAT file and displayed in the atlas map on ConsoleOne.

Maps reflect the scope of discovery set at the management server. By default, all devices that the management server is able to establish communication with, are discovered and stored at the management server. By defining the scope of NetExplorer™, you can limit the number of discovered objects.

For more detailed information on network discovery, see Chapter 3, "Understanding Network Discovery and Atlas Management," on page 71.

Database Administration

ZfS provides a centralized Common Information Model (CIM)-compliant Sybase* database on the management server. The database serves as a repository for server and network data that can be displayed or formatted in various ways to provide you with the information you need to manage your network. The ZfS data is stored in a topology database containing three logical databases:

- Topology
- Alarms
- Map information

Most database functions are automatic and require very little administration. For more detailed information on ZfS databases, see Chapter 11, "ZENWorks Management and Monitoring Services Database," on page 389.

Alarm Management

Alarms recognized by ZfS include Simple Network Management Protocol (SNMP) traps, connectivity testing, and threshold profiling. Alarm management processes traps and proprietary alarms and forwards the alarms to ConsoleOne that subscribe to the alarms.

You can perform specific actions on an alarm by specifying the action in the alarm disposition. Some actions, like executing a program, sending an e-mail notification, and creating an archive, audible beep at the Console, and ticker messages, are automatically performed. You can set an action to forward specific processed alarms to other ZfS management servers, as well as forward unprocessed SNMP traps directly to a target address of any third-party enterprise management application.

Role-Based Services

ZfS Management and Monitoring Services supports role-based administration and task management through Novell eDirectory™. ZfS uses role-based services (RBS) to organize ZfS Management and Monitoring Services tasks into roles and to assign scope information to a role.

RBS roles specify tasks that users are authorized to perform. Defining an RBS role includes creating an RBS role object and specifying the tasks that the role can perform.

For general information on creating RBS role objects or specifying tasks that RBS roles can perform, see "Configuring Role-Based Administration" on page 50.

For information on how ZfS implements role-based services, see "Role-Based Administration" on page 34.

Reporting

ZfS provides reporting services to generate statistical information. These reports can be displayed on ConsoleOne or exported to databases and Web formats. ZfS allows you to generate the following types of reports:

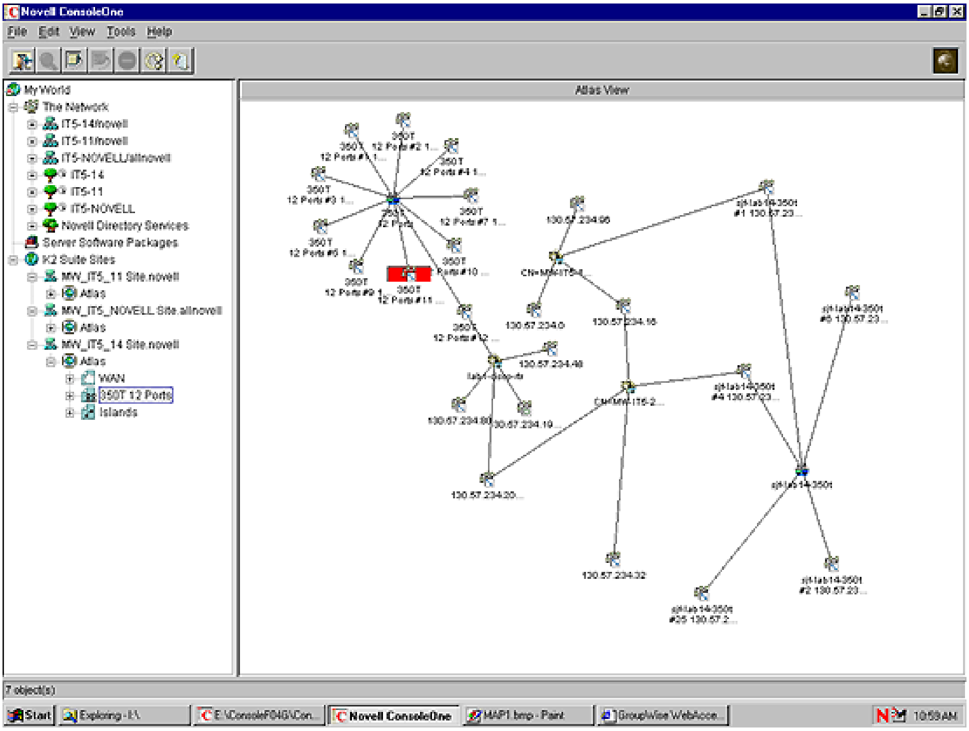
- Health reports
- Topology reports

- Alarm reports

For more detailed information on ZfS Management and Monitoring Services reports, see "Using Reports in Management and Monitoring Services" on page 393.

Topology Mapping

Topology mapping enables you to display maps in the ZfS hierarchical atlas as shown in the figure below. Maps reflect the scope of discovery set at the management server.



For more detailed information on topology mapping, see "Managing the Atlas" on page 120.

MIB Tools Administration

ZfS includes the MIB compiler and MIB browser, to manage SNMP devices.

The MIB tools enable you to:

- Set alarm templates for receiving SNMP traps
- Display and set values on SNMP devices
- Update trap definitions in the alarm template database
- Annotate third-party MIBs

For more detailed information on the MIB tools, see Chapter 6, "Using the MIB Tools," on page 211.

Monitoring Services

Monitoring, or SNMP, services include testing the connectivity and availability of a service on a network device. ConsoleOne is notified whenever the status of the service changes. The services that can be monitored include DHCP, DNS, Echo, FTP, HTTP, HTTPS, IP, IPX™, NFS, NNTP, SMTP, SNMP, Time Service, TFTP, and WUser.

For more detailed information on monitoring services, see Chapter 7, "Monitoring Services," on page 241.

Server Management

The server management component enables you to monitor all the servers in your network. This component must be installed on each of the servers you want to monitor using ConsoleOne. During the ZfS installation you can select the servers to install the server management component.

You can deploy some or all of the server monitoring software components to meet your management needs best. For more detailed information on server management, see "Understanding Server Management" on page 155.

Traffic Analysis

The traffic management component provides the traffic analysis services for a NetWare or Windows NT server, to monitor all traffic on an Ethernet, Fiber Distributed Data Interface (FDDI), or token ring network segments.

The traffic analysis services include:

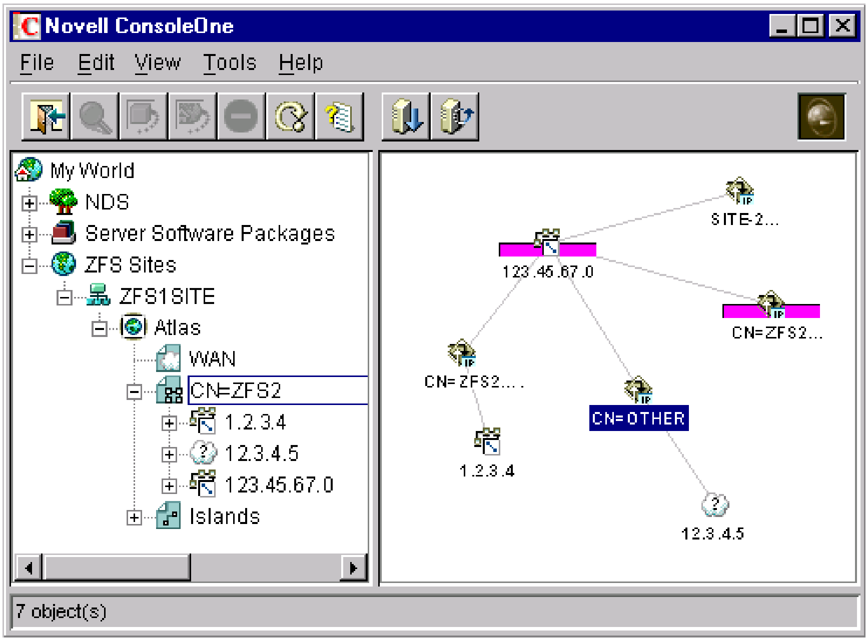
- Standard and enterprise-specific RFC 1757 MIB descriptions for remote network monitoring
- Extensions added to eDirectory, including Remote Monitor (RMON) agent configuration
- Network traffic trending and analysis tools
- Network health report templates
- Integration with topology maps
- Performance threshold configuration and profiling
- A view of conversations on network segment and utilization
- Packet capture tools and view

You can deploy some or all of the traffic analysis software components to meet your management needs best. For more detailed information on analyzing the network traffic, see Chapter 8, “Understanding Traffic Analysis,” on page 251.

ConsoleOne

The Novell ConsoleOne, provides the interface where you can manage and administer your network. ConsoleOne hosts programs (snap-ins) for integrating network administration and management snap-ins, enabling you to manage your network through a single interface.

ZfS provides a graphical user interface (GUI) snap-in to the Novell ConsoleOne under the ZENworks for Servers namespace, as shown in the following figure. It provides access to the unique functions provided by ZfS.



For more information on Novell ConsoleOne, see the ConsoleOne Web site (http://www.novell.com/products/netconsole/consoleone).

Planning the Configuration

This section discusses general planning options for configuring the Management Site Services and some of the ZENworks for Servers (ZfS) agents (alarms, servers, and traffic) on your network. This section also discusses how to plan and implement role-based administration.

Before installing the ZfS Management and Monitoring Services software, you must decide what information you need to manage your network effectively. This section contains the following topics to help you decide the kind of information you would need to manage your network.

This section also explains how to configure the Management and Monitoring Services.

- "Defining Management Information Needs" on page 32
- "Planning a Strategy to Manage Your Network" on page 32
- "Configuring Your Network" on page 33

This guide also contains specific information on planning server management and segment monitoring in the following sections:

- "Planning for Server Management" on page 159
- "Planning for Segment Monitoring" on page 267

Defining Management Information Needs

ZfS is flexible to suit the business needs of different network configurations. You need to understand what information is needed by the groups in your organization and suitably deploy the software to meet those needs.

Typically, the groups in your company may consist of front-line help desk people, back-end information system administrators, and management-level coordinators, who need specific information for planning, budgeting, troubleshooting, and other issues.

For instance, one group might have a set of critical servers that need to be monitored round the clock. You might want real-time monitoring of these servers and receive notification when serious faults occur on these servers. Another example could be a need to generate weekly reports on server trends for a group of defined servers.

Planning a Strategy to Manage Your Network

In order for ZfS to monitor and manage devices on your network, it must actively poll your network segments and devices on your network. ZfS performs polling of these network objects using standard protocols (SNMP, TCP/IP, and IPX).

The design of the ZfS components minimizes the impact on network performance by storing trending information on the servers hosting the Simple Network Management Protocol (SNMP) and Remote Monitor (RMON) agents. Polling is directly performed by the management server based on requests coming from connected ConsoleOne.

The ZfS system administrator should configure the polling frequency to provide an appropriate level of monitoring for the network environment. A good rule for setting appropriate levels of monitoring is to identify systems that are critical for the operation. You can then group systems and segments into three basic management categories:

- **Mission critical:** Segments and devices that need to be actively monitored. Monitoring should be set at a high polling frequency.

- **Important:** Segments and devices that require less monitoring. These might be systems that host certain services that require a balance between polling overhead and performance. You should set the polling frequency to every few minutes, hours, or days.
- **Less important:** Segments and devices that require no active monitoring. Polling can be done on-demand to monitor segments and devices, or set to poll infrequently.

Devices that are either not polled or polled infrequently can be configured to send alarms (traps) to the management server to notify errors occurring on the system.

Configuring Your Network

The ZfS Management and Monitoring Services components rely on standard network protocols to communicate with devices on your network. In order to discover and accurately monitor your network and its devices, you need to ensure that the communication channels are consistent and well-configured.

The following sections discuss important aspects of your network configuration:

- "IP Addressing Strategy" on page 33
- "IPX Transport Software" on page 33
- "eDirectory and DNS Name Resolution" on page 34
- "SNMP Configuration" on page 34

IP Addressing Strategy

If you want to discover devices communicating over IP, ensure that they are configured with a valid IP address to enable you to manage the devices. TCP/IP must be bound on the designated ConsoleOne workstations and IP must be bound on the management server. You can use Dynamic Host Configuration Protocol (DHCP) addressing on ConsoleOne workstation, but a static address must be assigned to the management server.

IPX Transport Software

All devices communicating over IPX that you want to discover and manage must be configured with an IPX/SPX - compatible transport network software stack. NetWare and Windows drivers are included with the operating system installation software. ZfS is compatible with the Novell IP Compatibility Mode Driver.

eDirectory and DNS Name Resolution

Verify that your NetWare and Windows NT servers and network device names are in place before you begin discovering your network. Name resolution can be in the form of local host files, an eDirectory name, or a bindery table. The server names or host names are displayed in maps and configuration views rather than in IP or IPX addresses.

SNMP Configuration

The SNMP agents and RMON agents for Novell NetWare and Windows NT servers and other SNMP-enabled network devices require a community string to be identified on the device. You need to configure each SNMP-enabled device with a community string and trap target destination that includes that ZfS management server.

The community strings are used to ensure secure communication between the manager and the agents. In order for the ZfS system to communicate with an agent, the community string on the manager and agent must be similar and use the same port. In order to prevent all users from accessing information it is required to change the community string.

If the GET and SET community strings are changed from PUBLIC, you need to change settings at ConsoleOne and on the management server (load NXPCON > SNMP > Add/Edit Community Name) to match the names on your network. For details on how to change the community string, after installing the Management Services, see "Changing the SNMP Community String" on page 112.

For information on configuring the NetWare and Windows NT server agents, see Chapter 8, "Understanding Traffic Analysis," on page 251.

Role-Based Administration

You can use ConsoleOne, a directory-enabled framework for running Novell network administration utilities. The ZfS snap-ins to ConsoleOne fully leverage eDirectory to enable role-based administration and higher levels of security. Through eDirectory, users will be able to log in once and have access to the management components as specified by their roles within their specific scope.

The ZfS snap-ins to ConsoleOne allows you to divide the task of network administration amongst administrators. With ConsoleOne, the functions and tasks of ZfS are organized into different, customized "views" based on each administrator's role in your organization.

The following sections discuss role-based administration:

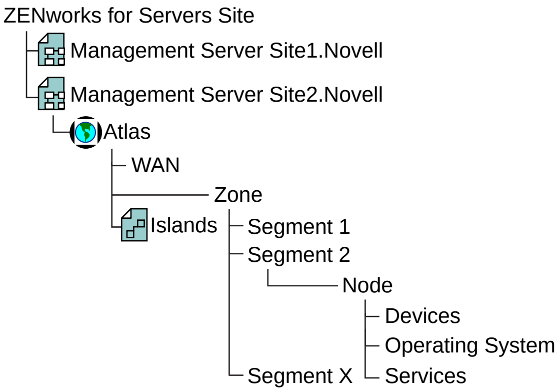
- "ZfS Management Site" on page 35
- "General ZfS Roles" on page 36
- "ZfS Role-Based Modules and Roles" on page 37
- "Configuring Role-Based Administration" on page 50

ZfS Management Site

The ZfS management site sets boundaries for accessing object data on the management server through the role-based services. You can create roles and tasks and further define the level of access to network objects and information from the network container space.

When you install ZfS Management and Monitoring Services, a management site, a system administrator role (RBS Admin), and all the site objects are created in eDirectory. A management site defines the scope of objects (networks, segments, routers, bridges, switches, servers, workstations, and so on) discovered on your network. You can create a single site or multiple sites, depending on the size of your network or network management requirements. A management site could include a single local network configuration or could encompass your entire network. The boundaries of a site are defined by the scope of network discovery. By default, network discovery is set to discover all connected networks and network nodes. The site object is created in the same context as the server object.

During installation, the default management site that is created is shown below. A single administration role is established with rights and permissions to all configuration and management tasks in the management system.


ZENworks for Servers Site
Management Server Site1.Novell
Management Server Site2.Novell
Atlas
WAN
Zone
Islands
Segment 1
Segment 2
Node
Devices
Operating System
Services
Segment X

Some default roles that monitor network traffic, handle alarms, and manage server systems, are available and allow you to add users. You can also use them as examples for your new role creations.

In the ZfS role-based services (RBS), permissions that are required to access network objects, configurations, and information are associated with roles. eDirectory User objects can be assigned to appropriate roles. The levels of abstractions in a role are described below:

- Roles - Created to perform various network management functions in your organization. You can simplify granting of permissions and restrict access to management tools and data by creating appropriate roles.
- Tasks - Actions performed to utilize components of the management system based on the specific responsibilities.
- Component/module - A software tool that provides a network management function. ZfS includes components for managing servers, monitoring segment traffic, and providing common services such as database management, alarm handling, and report generation.

The users added to a role, however, retain the access rights, permissions, and policies granted through the eDirectory user account. For example, a user may be granted permission to access and configure a server through eDirectory, but may not be granted permission to manage the server through the RBS in ZfS. Therefore the management role that the user is assigned has limited access to the management services or components/modules in the ZfS management system.

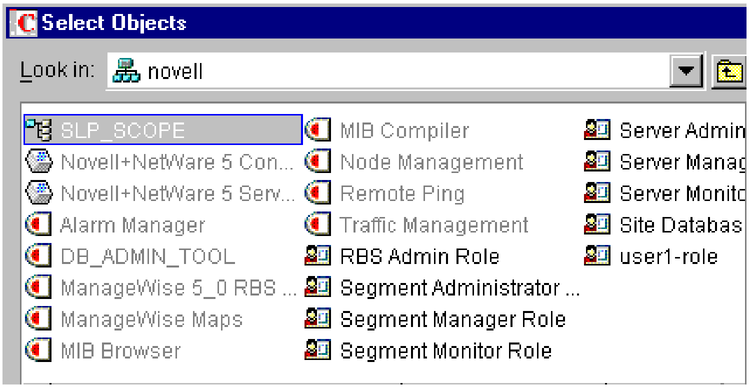
General ZfS Roles

ZfS components support role-based services (RBS) and task management through eDirectory. ZfS uses RBS to organize ZfS tasks into roles and to assign scope information to a role, user or a group.

RBS roles specify the tasks that users are authorized to perform. Defining an RBS role includes creating an RBS role object and specifying the tasks that the role can perform.

The tasks that RBS roles can perform are displayed as RBS Task objects in your eDirectory tree. These objects are organized into one or more RBS modules, which are containers that correspond to the different ZfS components. As shown in the figure below, ZfS provides predefined modules and RBS role objects.

IMPORTANT: You cannot create new modules or tasks. You have to select from the pre-defined modules and tasks that are available.



Look in: novell

You can create any role using the modules and tasks. Each module can have one or more tasks. For example, RBS defines the task for Monitoring Services as Enable Remote Ping. If this task is assigned to your role, you can use the Monitoring Services facility. For a list of the predefined ZfS modules and ZfS roles along with the associated tasks, see "ZfS Role-Based Modules and Roles" on page 37.

For more information on creating role objects using tasks and modules, see "Configuring Role-Based Administration" on page 50.

ZfS Role-Based Modules and Roles

This section provides the following tables:

- ZfS Role-Based Modules and Associated Tasks
- ZfS RBS Predefined Roles and Associated Tasks

  The following table lists each ZfS RBS module and the tasks that can be performed for the module.

ZfS RBS Module	Associated Tasks
Alarm Manager	◆ Add Alarm Note ◆ Assign Alarm ◆ Define Alarm Disposition ◆ Delete Alarm ◆ View Active Alarms ◆ View Active Alarm History ◆ View Alarm Summary

ZfS RBS Module	Associated Tasks
Database Object Editor	Database Object Editor
DB_Admin_Tool	◆ DB_BACKUP ◆ Database Password Change
MIB Browser	Enable MIB Browser
MIB Compiler	Enable MIB Compiler

ZfS RBS Module	Associated Tasks
Node Management	◆ Clearing a Connection ◆ Create Health Profiles ◆ Create Health Reports ◆ Delete Health Profiles ◆ Delete Health Reports ◆ Downing a Server ◆ Loading an NLM ◆ Mounting and Dismounting a Volume ◆ Read Only All ◆ Read Only All Tabular View ◆ Read Only Health Profiles ◆ Read Only Health Reports ◆ Read Only Homepage ◆ Read Only HostFileSystemView ◆ Read Only InstalledSoftwareView ◆ Read Only NetWareLoadableModuleView ◆ Read Only NetWareUserView ◆ Read Only NetworkPerformanceView ◆ Read Only NTDiskListview ◆ Read Only NTMemoryUsageView ◆ Read Only NTNetworkView ◆ Read Only NTPartitionView ◆ Read Only NTApadpterView ◆ Read Only NTConnectionListView ◆ Read Only NWDiskListView ◆ Read Only NWMemoryUsageView ◆ Read Only NWNetworkMediaView ◆ Read Only NWProtocolView ◆ Read Only NWFileListView

ZfS RBS Module	Associated Tasks
	◆ Read Only NWPartitionView ◆ Read Only NWQueueJobsListView ◆ Read Only NWQueueListView ◆ Read Only NWVolumeListView ◆ Read Only NWVolumeSegmentView ◆ Read Only NWVolumeUsageView ◆ Read Only NWRunningSoftwareView ◆ Read Only Set Parameter ◆ Read Only Trend ◆ Read Write All ◆ Read Write All TabularView ◆ Read Write Health Profiles ◆ Read Write Health Reports ◆ Read Write Set Parameter ◆ Read Write Trend ◆ Remote Controlling ◆ Restarting a Server ◆ Unloading an NLM
Remote Ping	Enable Remote Ping
Traffic Management	◆ Adding_Nodes_For_InactivityMonitoring ◆ Adding_Protocols_For_ProtocalDirectory ◆ Capture_Packets ◆ Deleting_Nodes_For_Inactivity ◆ Deleting_Protocols_For_ProtocolDirectory ◆ Freeing Agent Resources ◆ Setting_Segment_Alarms ◆ View_Conversations ◆ View_LANZ_Agents ◆ View_Protocol_Directory ◆ View_RMON_Summary

ZfS RBS Module	Associated Tasks
	◆ View_Segment_Alarms ◆ View_Segment_Dashboard ◆ View_Segment_Monitor_Nodes_For_Inactivity ◆ View_Segment_Protocal_Distribution ◆ View_Segment_Stations ◆ View_Segment_Summary ◆ View_Segment_Trends ◆ View_Switch_Port_Traffic ◆ View_Switch_Summary
Unified View	◆ Unified View for Devices ◆ Unified View for Segments
ZfS Maps	◆ Import ◆ Layout ◆ Print ◆ Rebuild ◆ Rename ◆ Save

The following table lists each predefined ZfS RBS and the specific tasks that can be performed for each of the roles.

Management and Monitoring Services Predefined RBS Role	Management and Monitoring Services RBS Module	Assigned Default Tasks
RBS_Administrator	All Modules	All available tasks
Segment_Administrator	Alarm Manager	◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History ◆ Assign Alarms ◆ Add Alarm Note
	DM_Admin_Tool	No available tasks

Management and Monitoring Services Predefined RBS Role	Management and Monitoring Services RBS Module	Assigned Default Tasks
	MIB Browser	No available tasks
	MIB Compiler	Enable MIB Compiler
	Node Management	◆ Read Only Health Profiles ◆ Read Only Health Reports
	Remote Ping	Enable Remote Ping
	Traffic Management	◆ Adding_Nodes_For_InactivityMonitoring ◆ Adding_Protocols_For_ProtocolDirectory ◆ Capture_Packets ◆ Setting_Segment_Alarms ◆ View_Conversations ◆ View_LANZ_Agents ◆ View_Protocol_Directory ◆ View_RMON_Summary ◆ View_Segment_Alarms ◆ View_Segment_Dashboard ◆ View_Segment_Monitor_Nodes_For_Inactivity ◆ View_Segment_Protocal_Distribution ◆ View_Segment_Stations ◆ View_Segment_Summary ◆ View_Segment_Trends ◆ View_Switch_Port_Traffic ◆ View_Switch_Summary
	ZfS Maps	◆ Layout ◆ Print
	Unified Views	Unified Views for Segments

Management and Monitoring Services Predefined RBS Role	Management and Monitoring Services RBS Module	Assigned Default Tasks
Segment Manager	Alarm Manager	◆ Assign Alarms ◆ Define Alarms Disposition ◆ Delete Alarms ◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History ◆ Add Alarm Note
	DM_Admin_Tool	No available tasks
	MIB Browser	Enable MIB Browser
	MIB Compiler	Enable MIB Compiler
	Node Management	◆ Create Health Profiles ◆ Create Health Reports ◆ Delete Health Profiles ◆ Delete Health Reports ◆ Read Write Health Profiles ◆ Read Only Health Profiles ◆ Read Write Health Reports ◆ Read Only Health Reports
	Remote Ping	Enable Remote Ping

Management and Monitoring Services Predefined RBS Role	Management and Monitoring Services RBS Module	Assigned Default Tasks
	Traffic Management	Adding_Nodes_For_InactivityMonitoring Adding_Protocols_For_ProtocalDirectory Capture_Packets Deleting_Nodes_For_InactivityMonitoring Deleting_Protocols_For_ProtocolDirectory Freeing Agent Resources Setting_Segment_Alarms View_Conversations View_LANZ_Agents View_Protocol_Directory View_RMON_Summary View_Segment_Alarms View_Segment_Dashboard View_Segment_Monitor_Nodes_For_Inactivity View_Segment_Protocal_Distribution View_Segment_Stations View_Segment_Summary View_Segment_Trends View_Switch_Port_Traffic View_Switch_Summary
	ZfS Maps	Import Layout Print Rebuild Rename Save
	Database Object Editor	Database Object Editor

Management and Monitoring Services Predefined RBS Role	Management and Monitoring Services RBS Module	Assigned Default Tasks
Segment Monitor	Alarm Manager	◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History
	DM_Admin_Tool	No available tasks
	MIB Browser	No available tasks
	MIB Compiler	No available tasks
	Node Management	◆ Read Only Health Profiles ◆ Read Only Health Reports
	Remote Ping	Enable Remote Ping
	Traffic Management	◆ Capture_Packets ◆ View_Conversations ◆ View_LANZ_Agents ◆ View_Protocol_Directory ◆ View_RMON_Summary ◆ View_Segment_Alarms ◆ View_Segment_Dashboard ◆ View_Segment_Monitor_Nodes_For_Inactivity ◆ View_Segment_Protocal_Distribution ◆ View_Segment_Stations ◆ View_Segment_Summary ◆ View_Segment_Trends ◆ View_Switch_Port_Traffic ◆ View_Switch_Summary
	ZfS Maps	◆ Layout ◆ Print
	Unified Views	Unified View for Segments

Management and Monitoring Services Predefined RBS Role	**Management and Monitoring Services RBS Module**	**Assigned Default Tasks**
Server Administrator	Alarm Manager	◆ Assign Alarm ◆ Define Alarm Disposition ◆ Delete Alarm ◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History ◆ Add Alarm Note
	DM_Admin_Tool	No available tasks
	MIB Browser	Enable MIB Browser
	MIB Compiler	No available tasks
	Node Management	◆ Clearing a Connection ◆ Loading an NLM ◆ Mounting and Dismounting a Server Volume ◆ Downing a Server ◆ Read Only Health Profiles ◆ Read Only Health Reports ◆ Read Write All ◆ Restarting a Server ◆ Unloading an NLM
	Remote Ping	Enable Remote Ping
	Traffic Management	No available tasks
	ZfS Maps	◆ Layout ◆ Print
	Unified Views	Unified Views for Devices

Management and Monitoring Services Predefined RBS Role	Management and Monitoring Services RBS Module	Assigned Default Tasks
Server Manager	Alarm Manager	- Assign Alarm - Define Alarm Disposition - Delete Alarm - View Alarm Summary - View Active Alarms - View Alarm History - Add Alarm Note
	DM_Admin_Tool	No available tasks
	MIB Browser	No available tasks
	MIB Compiler	No available tasks
	Node Management	- Clearing a Connection - Create Health Profiles - Create Health Reports - Delete Health Profiles - Delete Health Reports - Downing a Server - Loading an NLM - Mounting and Dismounting a Server Volume - Read Only Health Profiles - Read Only Health Reports - Read Write All - Read Write Health Profiles - Read Write Health Reports - Restarting a Server - Unloading an NLM
	Remote Ping	No available tasks
	Traffic Management	No available tasks

Management and Monitoring Services Predefined RBS Role	Management and Monitoring Services RBS Module	Assigned Default Tasks
	ZfS Maps	◆ Import ◆ Layout ◆ Print ◆ Rebuild ◆ Rename ◆ Save
	Database Object Editor	Database Object Editor
	Unified Views	Unified View for Devices
Server Monitor	Alarm Manager	◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History
	DM_Admin_Tool	No available tasks
	MIB Browser	No available tasks
	MIB Compiler	No available tasks

Management and Monitoring Services Predefined RBS Role	Management and Monitoring Services RBS Module	Assigned Default Tasks
	Node Management	- Read Only Health Profiles - Read Only Health Reports - Read Only Homepage - Read Only HostFileSystemView - Read Only InstalledSoftwareView - Read Only NetWareLoadableModulesView - Read Only NetWareUserView - Read Only NetworkPerformanceView - Read Only NTDiskListview - Read Only NTMemoryUsageView - Read Only NTNetworkView - Read Only NWConnectionListView - Read Only NWOpenListView - Read Only NWDiskListView - Read Only NWMemoryUsageView - Read Only NWNetworkMediaView - Read Only NWFileListView - Read Only NWVolumeListView - Read Only NWVolumeUsageView - Read Only RunningSoftwareView - Read Only Trend
	Remote Ping	Enable Remote Ping
	Traffic Management	No available tasks
	ZfS Maps	- Layout - Print
Site Database Administrator	Alarm Manager	No available tasks

Management and Monitoring Services Predefined RBS Role	Management and Monitoring Services RBS Module	Assigned Default Tasks
	DM_Admin_Tool	◆ DB_BACKUP ◆ Database Password Change
	MIB Browser	No available tasks
	MIB Compiler	No available tasks
	Node Management	No available tasks
	Remote Ping	No available tasks
	Traffic Management	No available tasks
	ZfS Maps	No available tasks

Configuring Role-Based Administration

Defining an RBS role includes creating an RBS role object and specifying the tasks that the role can perform.

The following sections discuss how to configure Role- Based Administration:

- "Defining RBS Role" on page 50
- "Creating an External Scope" on page 51
- "Assigning RBS Role Membership and Scope" on page 52

Defining RBS Role

RBS roles specify the tasks that users are authorized to perform in specific administration applications. Defining an RBS role includes the following sections:

- "Creating an RBS Role Object" on page 50
- "Specifying the Tasks that RBS Roles Can Perform" on page 51

Creating an RBS Role Object

To create an RBS role object:

1. Right-click the container that you want to create the RBS role object > click New > click Object.

2. Under Class, select RBS:Role > click OK.
3. Enter a name for the new RBS role object.

   Ensure to follow proper eDirectory naming conventions. For eDirectory naming conventions see Novell eDirectory Administration Guide (http://novell.com/documentation).

   Example: `Password Administrator Role.`
4. Click OK.

Specifying the Tasks that RBS Roles Can Perform

To specify the tasks:

1. Right-click an RBS role > click Properties.

   RBS task objects are located only in RBS module containers
2. In the Role Based Services tab, make the associations you want.
3. Select the Role Content page > Add the list of tasks that the role can perform.
4. Click OK.

Creating an External Scope

To create an external scope:

1. Right-click the container that you want to create the scope object > click New > click Object.
2. Under Class, select MW:Scope > click OK.
3. Enter a name for the new MW:Scope object.

   Ensure to follow proper eDirectory naming conventions. For eDirectory naming conventions see Novell eDirectory Administration Guide (http://novell.com/documentation).

   Example: `Password Administrator Role.`
4. Click OK.

Configuring a Scope Object

To configure a scope object:

1. Right-click the scope object > click Properties.

2. Browse the site object to which the scope is associated.
3. In the Site scope browse to select the computers to the site scope.
4. In the SQL script specify the scope by selecting the object and the operator from the drop-down list.
5. Click OK.

IMPORTANT: By default the scope object will have all-site access.

The effective scope will be a union of Site scope and the objects specified in SQL script.

Assigning RBS Role Membership and Scope

To assign an RBS role and scope to a user:

1. Right-click the user object to which you want to assign the role and scope > click Properties.
2. Click on Role Based Services Tab > Assigned Roles.
3. Click Add to add the required role to the user.
4. Click Scope to add the scope for the user.
5. Click OK.

IMPORTANT: If a user is assigned two different roles with different scopes, the user has rights to all the tasks (union of tasks in role1 and tasks in role2) irrespective of the scopes.

You cannot assign role and scope to User groups and Organization Unit.

Configuring Management and Monitoring Services

ZfS is made up of several components, some of which require certain setup tasks before you can use them, and others that do not.

The following components do not require any specific setup tasks:

- ZfS databases
- Role-based services (RBS)
- Management Information Base (MIB) tools
- ConsoleOne
- Reporting
- SNMP services

The following sections describe the setup tasks that are required to get the following components up and running:

- "Stopping and Starting Management and Monitoring Services" on page 53
- "Setting Up Discovery and Starting Back-End Processes" on page 54
- "Setting Up the Alarm Management System" on page 55
- "Setting Up Monitoring" on page 56
- "Setting Up the Traffic Analysis Agent" on page 56

Stopping and Starting Management and Monitoring Services

If you need to install other software or perform other maintenance functions on your server, you can stop Management and Monitoring Services and down the server. After performing the maintenance, you must reboot the server and restart the services in order for the server to resume its Management and Monitoring Services.

To stop and restart Management and Monitoring Services and down the server, complete the following steps at the management server console prompt:

1. To stop and unload ZfS Management and Monitoring Services, enter **`unmw`**.
2. To stop all JAVA processes, enter **`java -killall`**.
3. To exit JAVA, enter **`java -exit`**.
4. To down the server and restart, enter **`restart server`**.

   To down the server, enter **`down server`**. You need to start the server again.

Because the appropriate commands to start the back-end and discovery processes (SLOADER and NETEXPLOR) were inserted in the AUTOEXEC.NCF file when you installed Management and Monitoring Services, restarting the server will start these processes. If you modified the AUTOEXEC.NCF file and need to manually start these processes, see "Manually Starting Discovery and Back-End Processes" on page 55.

Setting Up Discovery and Starting Back-End Processes

The discovery software on the management server automatically discovers the nodes on your network. Network nodes include servers, desktops, routers, switches, and any other network devices. Discovery starts automatically when the ZfS software is loaded on the management server and runs continually, 24 hours a day. The amount of time to build a complete database depends on the size of your network. Very small networks might take one or two hours; very large networks (several thousand nodes) might require several days.

It is recommended that you run Network discovery on a standalone as the discovery process consumes a longer duration if you use the system.

After installation, your servers are in one of the following states:

- Discovery and back-end services are running.

  If you selected Yes to start the autodiscovery process and back-end services during installation, discovery is running on your ZfS server and your network is continually being discovered. You do not need to do anything further with regards to configuring discovery unless you want to modify your discovery parameters after you check the results of the initial discovery. For instructions on checking the results of discovery and modifying your discovery parameters, see Chapter 3, "Understanding Network Discovery and Atlas Management," on page 71.

  IMPORTANT: After modifying any discovery parameters, you must restart the server as described in "Stopping and Starting Management and Monitoring Services" on page 53.

- Discovery and back-end services are not running.

  If you selected No, and did not start the autodiscovery process and back-end services during installation, you must start discovery after you modify the default discovery parameters. For specific instructions on modifying discovery parameters, see Chapter 3, "Understanding Network Discovery and Atlas Management," on page 71.

  Before discovering your network, you can modify the following discovery parameters:

  - SNMP Community Strings. Ensure that discovery is configured with the community strings of your devices.
  - Discovery Scope. By default, discovery will discover the entire network if correct community strings are provided. If the discovery scope needs to be limited for some reason, it can be modified.

- IPX Discovery. IPX discovery will take place as long as the ZfS server has a valid IPX address binding. If there is no IPX address bound to the ZfS server, but there are IPX networks that need to be discovered, install the NetWare server in CMD mode (load SCMD).

IMPORTANT: After modifying any discovery parameters, you must restart the services as described in "Stopping and Starting Management and Monitoring Services" on page 53. If you never started discovery or the back-end services, you can manually start the services as described in "Manually Starting Discovery and Back-End Processes" on page 55.

Manually Starting Discovery and Back-End Processes

The commands to start autodiscovery and load the back-end services are inserted into the AUTOEXEC.NCF file by the installation program. Restarting the server will automatically start these processes. However, if you remove these commands you will need to manually start autodiscovery and load the back-end services (management site services).

During installation, a search path is added to the AUTOEXEC.NCF file to the management server program file path — ZENWorks\MMS\MWSERVER\BIN

Type the following in order at the management server console prompt, to manually start discovery and the back-end processes:

1. **`mgmtdbs`** — This starts the Sybase database.
2. **`mwserver`** — This starts the Naming service (MMSNAMING.NCF) and the Trap Receiving service (SNMPLOG.NLM).
3. **`netxplor.ncf`** — This starts the autodiscovery process.
4. **`sloader.ncf`** — This starts the basic services like Alarm Manager, Atlas Manager, Topology Manager, etc. The services to be started are listed in the SLOADER.PROPERTIES located in the ZENWorks\MMS\MWSERVER\PROPERTIES directory.

   The server will accept requests from ConsoleOne only after the SLOADER.NCF is completely loaded.

Setting Up the Alarm Management System

The ZfS Alarm Management System (AMS) can receive SNMP traps from any SNMP-enabled device or computer hosting a proxy SNMP agent. If your network device is using Management Agent for NetWare, Management Agent for Windows NT, NetWare LANalyzer® Agent™, or LANalyzer Agent for

Windows NT software, the device is discovered automatically for you. No setup is needed after installing the software.

Third-party SNMP agents require some setup before traps can be received. For information on setting up third-party SNMP agents, see "SNMP Configuration" on page 34.

Setting Up Monitoring

Because the Management Agent for NetWare and the ManageWise® Agent for Windows NT are based on SNMP, all actions that are directed from network management console to a server involve SNMP SET and GET requests from the manager to the agent. Any ConsoleOne requesting data from a managed server does so by issuing an SNMP GET request. An SNMP SET command is required to set server alarm thresholds or configuration parameters. Conducting these management operations from ConsoleOne such as ConsoleOne, raises the issue of ensuring security. In particular, unauthorized users setting configuration parameters on a server could cause severe performance problems or even sabotage network operations.

For these reasons, you should secure communication between the management system and your SNMP agents. For further information on SNMP security, "SNMP Configuration" on page 34.

Setting Up the Traffic Analysis Agent

The Traffic Analysis Agent for NetWare is a distributed network analyzer that complements ZfS. While other ZfS agents collect data about specific network nodes, such as servers, the Traffic Analysis Agent for NetWare observes the interaction among these nodes on a specific LAN segment. The agent is installed on a NetWare 4.*x* or NetWare 5.*x* server. To set up Traffic Analysis Agent for NetWare, see "Starting the Traffic Analysis Agent for NetWare" on page 57.

The Traffic Analysis Agent for Windows NT/2000 uses SNMP to communicate with the management server. After installation, in order for the Traffic Analysis Agent for Windows NT/2000 to operate, you must start the SNMP services. To start SNMP services, complete "Starting the SNMP Service for the Traffic Analysis Agent for Windows NT/2000" on page 57.

After the agents are set up, you must restart the Windows NT/2000 server on which the agent resides.

Starting the Traffic Analysis Agent for NetWare

The installation program for the Traffic Analysis Agent for NetWare modifies the AUTOEXEC.NCF file so that the agent starts automatically. Therefore, you do not need any further configuration. If, however, you are upgrading from a previous version of the Traffic Analysis Agent (referred to as the LANalyzer agent), and did not uninstall the previous version, you must ensure that each server on which you upgraded the agent will run the new Traffic Analysis Agent.

To ensure that the upgraded NetWare servers run the new Traffic Analysis Agent:

1. On each NetWare server where you upgraded the ZfS Traffic Analysis Agent, open the AUTOEXEC.NCF file located in SYS:\SYSTEM.
2. Comment out the following lines by placing a # character at the beginning of the line as follows:

   ```
   #Search add lanzdir
   ```

   ```
   #LANZ.NCF
   ```

   The first statement defines the search path where *lanzdir* is the directory in which the older agent is installed. The second statement loads the older agent.
3. Save the file and restart the server.

The new agent will load and run automatically. The LANZ.NCF file in the *agentinstallfolder*\LANZ will start the Traffic Analysis agent. The ULANZ.NCF in the same folder will stop the Traffic Analysis agent.

Starting the SNMP Service for the Traffic Analysis Agent for Windows NT/2000

If you have configured Windows NT/2000 to start the SNMP service automatically, the agent installed on Windows NT/2000 starts with the SNMP service when you start Windows NT/2000.

If you have not configured Windows NT/2000 to start the SNMP service automatically, do either of the following:

- At the command prompt, enter **`net start snmp`**.
- From the Control Panel, click Services > SNMP > Start.

  When the SNMP service is started, the traffic analysis agent for Windows NT/2000 will also start.

2 Using ConsoleOne with Management and Monitoring Services

The ZENworks® for Servers (ZfS) console is a snap-in to the ConsoleOne® management tool. ZfS expands ConsoleOne management capabilities by adding menu options, property pages for existing Novell®eDirectory™ objects, and ways to browse and organize network resources. This section introduces ConsoleOne features that are unique to ZfS, including:

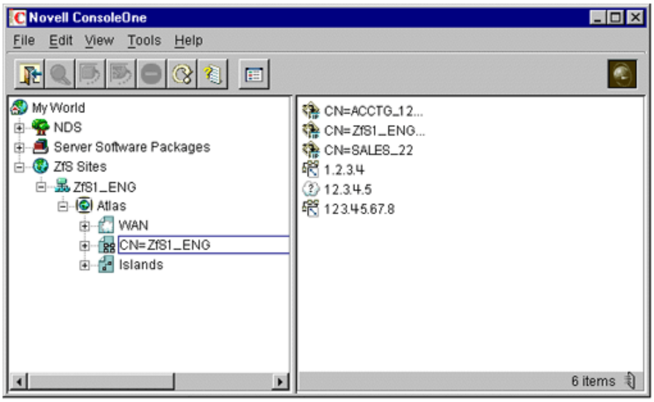
- "Navigating the ZfS Namespace" on page 59
- "Selecting ZfS Options" on page 61
- "Working with Views" on page 63

For more information on basic ConsoleOne capabilities, see the Novell ConsoleOne Administration Guide (http://novell.com/documentation).

Navigating the ZfS Namespace

In ConsoleOne, your network and its resources are regarded as a set of objects and are arranged in various containers. Each top-level object is referred to as a namespace. To view your network and its resources on ConsoleOne, you must log in to the eDirectory tree which contains site server object.

The ZfS ConsoleOne snaps in to ConsoleOne under the ZfS Sites namespace, as shown in the following figure:



In general, you can perform administration tasks by browsing to an object in the left frame, right-clicking it, and clicking an option. Objects within the ZfS namespace are arranged in the following hierarchy:

1. **ZENworks for Servers sites object:** This is the ZfS namespace container. It is the top of the ZfS namespace hierarchy. Expand this object to display a list of ZfS management sites.

2. **ZfS Site:** This object represents a ZfS management server. It represents an eDirectory object that defines a collection of discovered objects that collectively make up a group of services. Expand this object to display the atlas for the site.

3. **Atlas:** This is the container object for all discovered topology objects. The atlas can contain the following types of pages:

   - **WAN page:** Summarizes the entire network.

   - **Area page:** Displays segments on the network. There may be more than one Area page, depending on how your network is organized.

   - **Islands page:** Displays segments with undetermined connectivity.

4. **Segments:** Within each atlas page is a listing of the segment objects that are included in that section of the atlas.

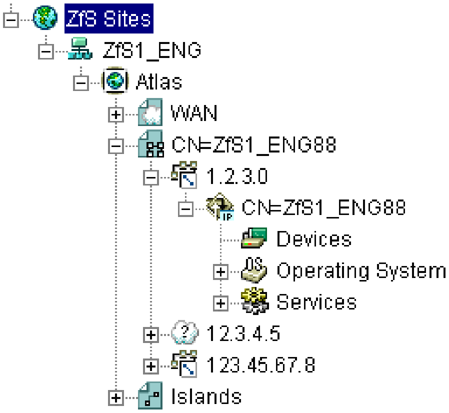
5. **Nodes:** Within each segment object is a listing of server and node objects that reside on the segment. The icon displayed varies by the node type.

6. Node Details: Expand a node object to display a list of system internal components. Server data is grouped into the following three categories:

   - Devices
   - Operating System
   - Services

   You can drill down into the server configuration further by clicking the plus signs next to the Devices, Operating System, and Services objects to display details about the internal components of the server. The internal components include the processors, installed software, volumes, kernel, and adapters associated with the server. For more details about the node objects, see "Object Hierarchy" on page 181.

The following figure illustrates the ZfS namespace hierarchy:



Selecting ZfS Options

To display the ZfS options, you want to monitor or manage in the left frame, right-click the object. The options available are displayed. ZfS provides three main options:

- "Views" on page 62
- "Properties" on page 63
- "Actions" on page 63

Views

Views are different ways of displaying information. ZfS provides a variety of views designed to help you view the information of your network in different ways.The views ZfS provides are:

- **Atlas:** Provides a graphical representation of the discovered network topology, the physical location of nodes, node configuration, and alarm information.
- **Console:** Displays the objects contained in the selected container object. This view is useful while navigating the ZfS site.
- **Trend:** Provides a graphical representation of current and historical trend data by hour, day, week, month, or year. Monitoring trend data helps you with tasks such as determining which server is being used, who is using the server, troubleshooting problems, balancing load across multiple servers, and planning resources.
- **Active Alarms:** Provides a tabular display of alarm statistics for all the current alarms received from segments or devices, per management site. This view is refreshed whenever a new alarm occurs on the network.
- **Alarm History:** Provides a tabular display of all archived alarms, including the handled status of each alarm.This view is refreshed whenever a new alarm occurs on the network.
- **Alarm Summary:** Provides a graphical representation of the summary of alarms you have received. The view is divided into three panels of representation: pie chart panel, bar graph pane, and trend panel. Provides a tabular display of all archived alarms, including the handled status of each alarm.
- **Summary:** Provides a tabular information about the selected object's configuration. For example, the summary view for a server object displays information about NLM™ files, memory usage, adapters, network interfaces, disks and disk controllers, volumes, queues, users, connections, open files, alarms, and installed software.

In addition to these main views, ZfS provides additional views for many of the objects in the hierarchy. For example, if you select a memory object, you can select a disk cache view that displays utilization for disk cache memory. For more information on the available views and the specific information displayed in an object view, see "Object View Details" on page 183.

Properties

The ZfS ConsoleOne provides several property pages that allow you to control ZfS-specific settings. To access the ZfS property pages, right-click an object and then click Properties.

- At the site level, ZfS provides property pages that allow you to edit global properties like Alarm Dispositions, ZfS Database settings, SNMP settings, MIB Pool entries, and health report profiles.
- At the server level, ZfS provides property pages that allow you to modify SNMP settings.

For general information on using ConsoleOne property pages, see the Novell ConsoleOne Administration Guide (http://novell.com/documentation).

Actions

You can perform one or more actions on some objects. For example, if you right-click a server object, the Actions menu provides options for restarting or shutting down the server. However, if you right-click a volume object, the Actions menu provides options for mounting or dismounting the volume. For more information on performing actions on a managed object, see "Executing Server Commands" on page 180.

Working with Views

ZfS ConsoleOne provides two types of views: tabular (list) views and graphical views. The Console, Active Alarms, and Alarm History views are all tabular views. The atlas and Trend views are both graphical views. The Summary view may contain both tabular and graphical elements.

There are many characteristics that are common to all views. This section describes the common tasks you can perform on the ZfS views, including:

- "Changing the Appearance of a View" on page 64
- "Modifying Columns" on page 65
- "Filtering Views" on page 66
- "Sorting Views" on page 67
- "Printing a View" on page 68
- "Exporting a View" on page 69

- "Saving Views" on page 69
- "Deleting and Renaming Custom Views" on page 70

Changing the Appearance of a View

In a view, you can change the following:

- "Changing the Display Font" on page 64
- "Customizing Grid Lines" on page 64
- "Displaying the View Title" on page 65

Changing the Display Font

To change the font of the text on a tabular view's headings or rows:

1. Click View > Settings > Appearance.

   The Appearance dialog box is displayed.

2. To change the header or row font, click the appropriate button as follows:

   - To change the header font, click the Header Font button.
   - To change the row font, click the Row Font button.

   The Fonts dialog box is displayed.

3. Select the font options you want > click OK to close the Fonts dialog box.
4. To save the changes made to the view, click View > Saving > Save.

Customizing Grid Lines

By default, the views displayed by ZfS do not contain grid lines. To display horizontal and/or vertical grid lines and to select a color for the grid lines:

1. Click View > Settings > Appearance.

   The Appearance dialog box is displayed.

2. Select the grid line style you want to use from the Style drop-down list. You can choose to have:

   - No grid lines (default)
   - Horizontal grid lines only
   - Vertical grid lines only
   - Vertical and horizontal lines

3. If you want to select a color for the grid lines, click the Color button.

   The Color Chooser dialog box is displayed. This dialog box includes three tab pages — Color Swatches, HSB, or RGB — allowing three methods of color selection.

4. Select the color you want to use for the grid lines using one of the three tab pages > click OK to close the Color Chooser dialog box.
5. Click OK to close the Appearance dialog box.
6. To save the changes made to the view, click View > Saving > Save.

Displaying the View Title

You may find it useful to display the view name at the top of the right frame to help you keep track of where you are within the ZfS ConsoleOne,

To display the view title:

1. Click View > Show View Title.

Modifying Columns

In a tabular view, you can change the columns in the following ways:

- "Resizing Columns" on page 65
- "Adding and Removing Columns" on page 65
- "Changing the Column Order" on page 66

Resizing Columns

To resize a column:

1. Move the mouse pointer to the margin between the columns you want to adjust.
2. When the pointer changes to a sizing arrow, drag the column to the width you want.
3. To save the changes made to the view, click View > Saving > Save.

Adding and Removing Columns

To add or remove columns from a view:

1. Click View > Settings > Column Selector.

2. To add a column, select the column name from the Available Fields list > click Add.
3. To remove a column, select the column name from the Show These Fields in This Order list > click Remove.
4. Click OK.
5. To save the changes made to the view, click View > Saving > Save.

Changing the Column Order

To change the order in which columns are displayed:

1. Click View > Settings > Column Selector.
2. Select the column you want to move from the Show These Fields in This Order list > click the Move Up or Move Down button to change the location of the column.
3. Click OK.
4. To save the changes made to the view, click View > Saving > Save.

Filtering Views

You can display the alarms in a tabular view based on filter conditions. The filter applies only to the current management session and clears once you exit ConsoleOne.

You set up a filter by selecting a criteria from four drop-down lists or entering a criteria. You can either set up simple filters that require only one line, or complex filters composed of multiple lines or groups of lines. If you set up a filter using more than one line, you must also specify the logical relationship between the line and/or group of lines.

To set up a filter:

1. Go to the required view.
2. Click View > Settings > Filter.
3. Select the column by which you want to filter alarms from the first drop-down list.
4. Select an operator from the second drop-down list.

   The operator defines the constraint value set to the column. You can specify any of the following values for the alarm display - equal to, not equal to, greater than, less than, greater than or equal to, less than or equal to, contain, or start with the value you select in the third drop-down list. The list of available operators depends on the selected column.

5. Select a value from the third drop-down list.
6. Specify how this filter statement relates to other statements you plan to define by selecting a value from the fourth drop-down list.
    - If this is the only filter statement or if it is the last statement in a group, select End.
    - If you want to add a line below the current filter statement, select New Row. A new line is added. You must define the logical relationship between the previous line and the new line. The alarms will be displayed based on the logical condition you have specified. Select And to satisfy both the filter conditions. Select Or to satisfy any one of the filter conditions for the alarm to be displayed.
    - If you want to add one or more lines that are unrelated to the preceding lines, select New Group. A new line is added. An additional drop-down list separates the new line from the preceding lines. Select a value from this drop-down list to indicate the relations between the filter statements. Select And if you want both the filter statements to be satisfied. Select Or if you want only one of the filter statements in one of the groups to be satisfied. Select End from the fourth drop-down list when you add a new group.
7. Click OK if you have finished defining filters.

    The view is updated to display only those entries that meet the filter criteria you defined.

Sorting Views

Using the sorting feature to modify the order in which the entries in a tabular view. You can sort the entries in the following two ways:

- "Sorting the View Using a Single Column" on page 68
- "Sorting the View Using Multiple Columns" on page 68

For instructions on sorting alarms, see "Sorting Alarms" on page 137.

Sorting the View Using a Single Column

To sort the entries displayed in the view by a single column:

1. Double-click the column header for the column by which you want to sort the entries.

   When you double-click the column header, the entries in the view are sorted by that column in descending order (the most recent entries first). To sort the entries by ascending order (oldest entries first), double-click the column header again.

Sorting the View Using Multiple Columns

To sort the view using multiple columns:

1. Click View > Settings > Sort.
2. Select the first column you want the entries sorted by from the Sort Items By field.
3. Select the appropriate radio button to indicate whether you want the entries sorted in ascending or descending order.
4. Select the second column by which you want entries sorted from the Then By field > click the ascending or descending radio button to specify the sort order.
5. Repeat Step 4 for each subsequent column for which you want entries sorted.
6. Click OK.

   The entries are now sorted according to the criteria you specified.

Printing a View

To print a view:

1. Go to the view you want to print.
2. Click File > Print.
3. In the Print dialog box, select the print options you want > click OK.
4. In the next Print dialog box, click OK.

Exporting a View

You can export a tabular or graphical view to one of the following file formats:

- HTML
- Comma-delimited text files (.CSV)
- Tab-delimited text files (.TXT)
- Blank-space-delimited text files (.TXT)

To export a view:

1. Go to the view you want to export.
2. Click File > Export.
3. From the Export File Type drop-down list, select the format to export the view.
4. Enter the path and name of the file you want to save in the File Name field or click Browse to search for a location you want to export the file to.
5. Click OK.

Saving Views

By default, any of the changes you make to the appearance, content, sorting, or filtering of a view are discarded when you exit ConsoleOne. If you want to retain the changes you have to explicitly save the view.

This section includes the following topics:

- "Saving the Existing View" on page 69
- "Creating a New View" on page 70
- "Deleting and Renaming Custom Views" on page 70

Saving the Existing View

If you want to permanently modify the existing view to reflect the changes you made, you can simply save the view as follows:

1. Modify the view as desired.
2. Click View > Saving > Save.

   The next time you display the view, the changes will be retained.

Creating a New View

In some cases, you might find it useful to create a new view with the changes made. The existing view is left unmodified and you can save the new view under a different name.

To save the view under a new name:

1. Modify the view as desired.
2. Click View > Saving > Save As.
3. Enter a name for the view in the Enter New View Name field > click OK.

Deleting and Renaming Custom Views

To rename or delete the custom views you have saved:

1. Click View > Saving.
2. To rename a custom view, select the view from the Saved Views list > click Rename.

   or

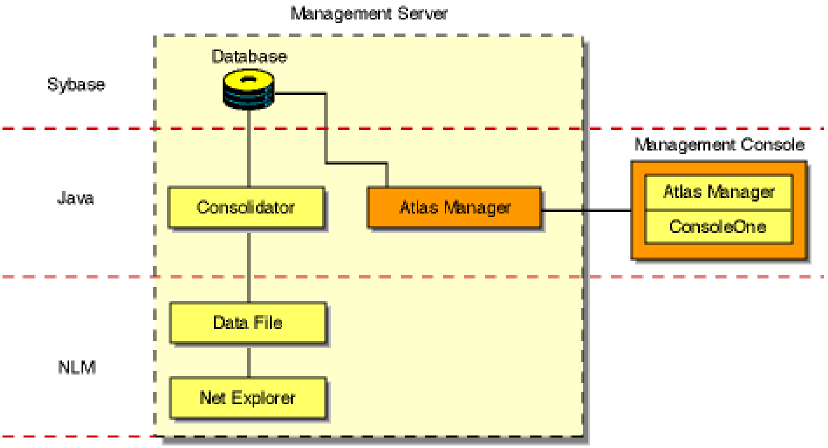
   To delete a custom view, select the view from the Saved Views list > click Delete.
3. When you have finished modifying your saved views, click Close.

3 Understanding Network Discovery and Atlas Management

Discovery is the process of determining the topology of your network. You can manage, monitor and display the components of your network from ConsoleOne®. Discovery involves the following three major components of the ZENworks® for Servers (ZfS) software:

- **Discovery software:** A set of NetWare® Loadable Module™ (NLM™) files that run on a management server and discovers the network topology
- **Consolidator software:** Software that runs on the management server, which reads the data discovered by discovery, and populates the Topology database.
- **Atlas Manager software:** Software that reads the Topology database, creates an atlas database, and displays the network topology in an atlas on ConsoleOne.

The following figure shows a high-level view of the discovery components:



This section deals with the following topics:

- “Understanding Network Discovery” on page 72
- “Setting Up Discovery” on page 106
- “Managing the Atlas” on page 120

Understanding Network Discovery

The NetExplorer™ software drives the discovery process on the management server. The discovered information is populated in the Topology database. The Atlas Manager creates a related atlas database which encapsulates the topology information and adds information related to how the user views the maps.

The following sections will help you understand the network discovery process:

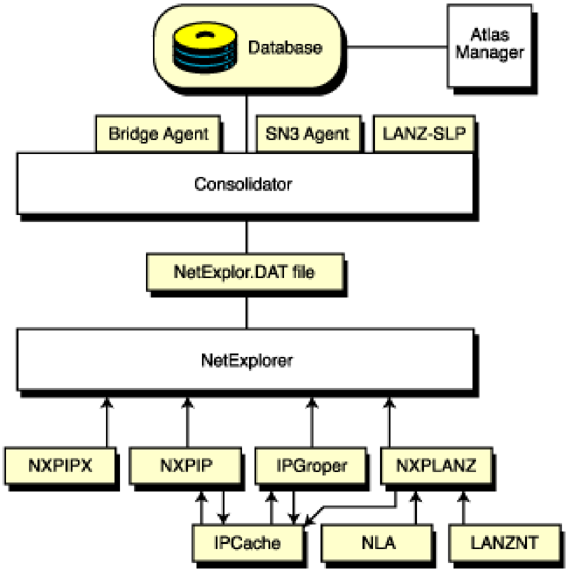
- “Discovery Components” on page 72
- “Discovery Process” on page 80
- “What Is Discovered” on page 89
- “File-Based Discovery” on page 100

Discovery Components

The NetExplorer and Consolidator software that runs on the management server aids in discovering your network and updating the database.

Your network is automatically discovered by NetExplorer when you start it for the first time.

The following illustration shows the discovery components on the server:



The NetExplorer system consists of the following interdependent components:

- "Discovery" on page 73
- "Consolidator" on page 76
- "Atlas Manager" on page 78
- "Database Object Editor" on page 78
- "Management Console Software" on page 79
- "Additional ZfS Components" on page 79

Discovery

The discovery software resides on the management server and uses the discovery NLM™ software to discover the various network devices.

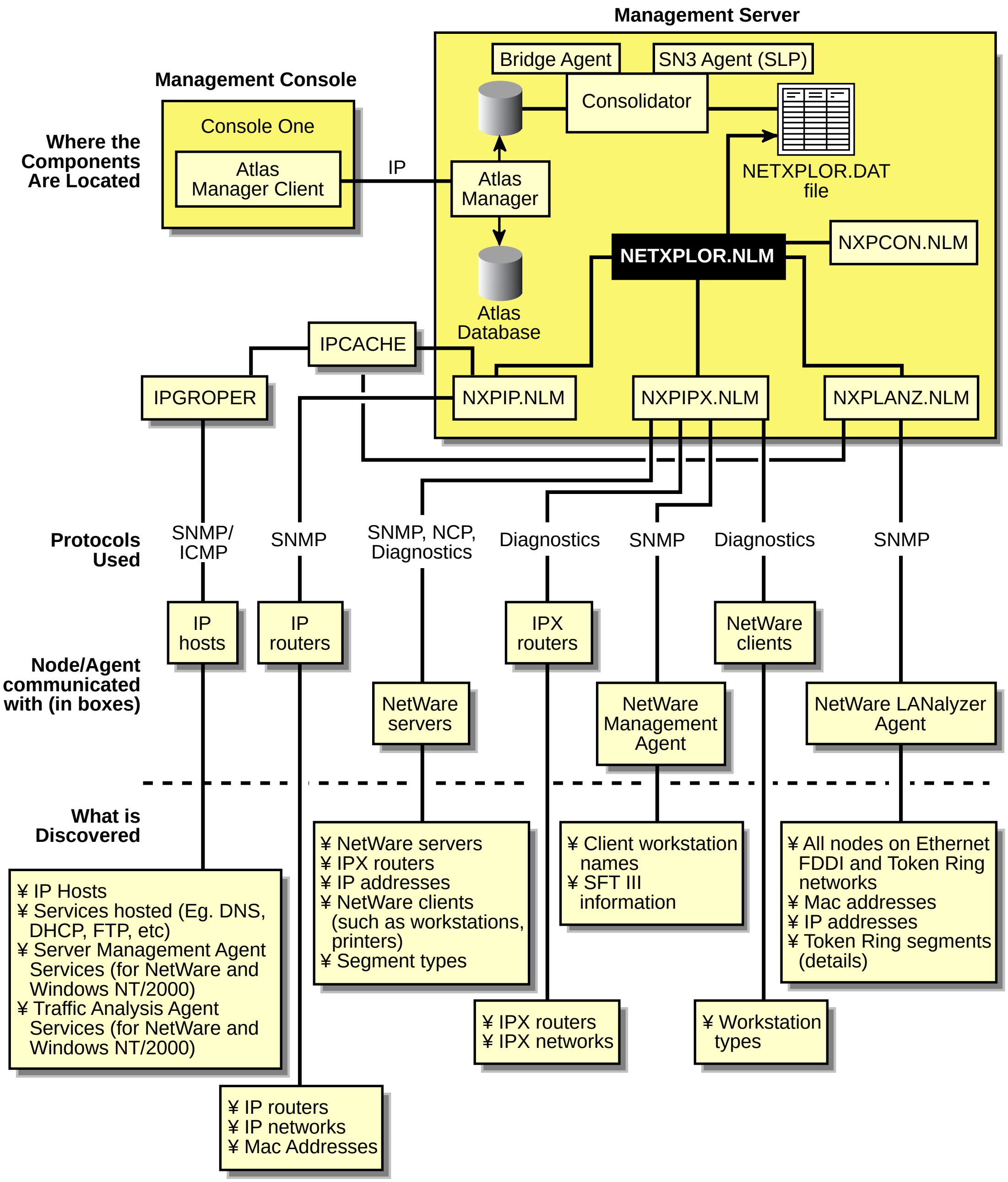
- NXPIP.NLM discovers IP routers on IP networks and sends IP router information to discovery. It communicates with the IPCACHE module to share this information with IPGROPER.
- IPGROPER detects IP host addresses and the following services: Domain Name System (DNS) names, Dynamic Host Configuration Protocol

(DHCP) services, Telnet, Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP).

- NXPIPX.NLM discovers various NetWare systems on IPX™ networks and sends information about systems to NetExplorer.
- NXPLANZ.NLM communicates with Traffic Analysis Agents (LANalyzer®) for NetWare and Windows* NT* to gather information about all systems communicating on the segments that are monitored, and sends this information to discovery.

The following figure illustrates the architecture of the discovery system and shows the roles of the various components, network systems, and agent software.

IMPORTANT: Discovery uses the server and traffic management agents to obtain certain discovery information. Though not required, using these agents across your network enhances the accuracy and detail of logical maps displayed by ConsoleOne.



Management Server
Bridge Agent
SN3 Agent (SLP)
Consolidator
Management Console
Console One
Atlas Manager Client
IP
Atlas Manager
NETXPLOR.DAT file
Where the Components Are Located
NETXPLOR.NLM
NXPCON.NLM
Atlas Database
IPCACHE
IPGROPER
NXPIP.NLM
NXPIPX.NLM
NXPLANZ.NLM
Protocols Used
SNMP/ ICMP
SNMP
SNMP, NCP, Diagnostics
Diagnostics
SNMP
Diagnostics
SNMP
Node/Agent communicated with (in boxes)
IP hosts
IP routers
IPX routers
NetWare clients
NetWare servers
NetWare Management Agent
NetWare LANalyzer Agent
What is Discovered
¥ NetWare servers
¥ IPX routers
¥ IP addresses
¥ NetWare clients (such as workstations, printers)
¥ Segment types
¥ Client workstation names
¥ SFT III information
¥ All nodes on Ethernet FDDI and Token Ring networks
¥ Mac addresses
¥ IP addresses
¥ Token Ring segments (details)
¥ IP Hosts
¥ Services hosted (Eg. DNS, DHCP, FTP, etc)
¥ Server Management Agent Services (for NetWare and Windows NT/2000)
¥ Traffic Analysis Agent Services (for NetWare and Windows NT/2000)
¥ IPX routers
¥ IPX networks
¥ Workstation types
¥ IP routers
¥ IP networks
¥ Mac Addresses

Supported Protocols

ZfS software supports the Service Location Protocol (SLP) on NetWare 5.*x* networks to enhance the discovery speed.

The server management and Traffic Analysis Agents for NetWare use the Service Advertising Protocol (SAP) to identify themselves to other components. SAP filtering prevents routers from passing SAP packets. To enable the management server and ConsoleOne to receive the SAP packets that identify manageable servers, Hub Management Interface (HMI) hubs, and other servers, configure the router that is filtering SAP packets to list the specific SAP numbers that it should pass. NetWare systems and ZfS components use the SAP numbers listed in the following table.

Component	SAP Number (Decimal)	SAP Number (Hexadecimal)
NetExplorer NLM	567	237
NetWare Management Agent	635	27B
ManageWise Agent for Windows NT server	651	28B
NetWare LANalyzer® Agent™ (Traffic Analysis Agent)	570	23A
Print server	7	7
NetWare file server	4	4

Consolidator

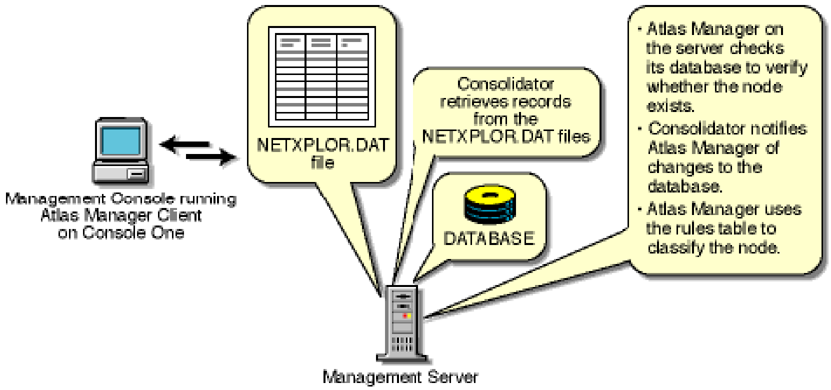
The Consolidator software resides on the management server and performs the following tasks:

- Reads the NetExplorer data files, which contains all the discovered information.
- Interprets the records in the NETXPLOR.DAT file.
- Checks whether the system has already been created in the Topology database. If the system does not exist in the Topology database, the Consolidator creates the system.
- Uses the Bridge agent to query the Bridge Management Information Base on IP networks and discovers which systems are connected to a port of a bridge.

- Uses the SN3 agent to get the eDirectory name of NetWare servers.The SN3 agent enhances the performance of discovery by using SLP to discover NetWare 5.*x* servers.
- Runs the MIBCOMPILER.RULE file on all the discovered devices and verifies for the MIBs mentioned in the rule file on these devices and updates the database. You can also add or delete the MIBs in the MIBCompiler.rule.
- Writes discovery information to the ZfS database.

The following figure shows the tasks of the Consolidator. NETXPLOR.NLM creates the NETXPLOR.DAT file and the Consolidator starts reading the records from the file. If NetExplorer processes are restarted, the NETXPLOR.DAT file is re-created and the Consolidator requests the first record in the new file.

When the Consolidator retrieves a record from the NETEXPLOR.DAT file, it searches for the record in the database. If the system is not in the database, the Consolidator inserts it and notifies the Atlas Manager of the update.


NETXPLOR.DAT file
Consolidator retrieves records from the NETXPLOR.DAT files
DATABASE
· Atlas Manager on the server checks its database to verify whether the node exists.
· Consolidator notifies Atlas Manager of changes to the database.
· Atlas Manager uses the rules table to classify the node.
Management Console running Atlas Manager Client on Console One
Management Server

Command Line Options

If you want to manually operate the Consolidator, use the command line options shown in the following table.

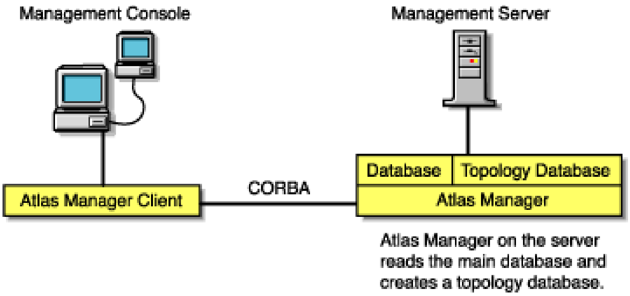
Option	Allows the Consolidator to
-notify	Notify the Atlas Manager that it has updated the database.
-database *data_path*	The specific location of the database file to perform operations on.

Atlas Manager

The Atlas Manager software consists of a server and a client component. The server component resides on the management server along with the ZfS topology database. The Atlas Manager server component retrieves discovery data from the topology database and creates its own atlas database.

The client component of the Atlas Manager resides on ConsoleOne. The server component can communicate with several console components at any given time. Any changes made to the maps on the console (for example, rename, import, and layout) are communicated to the Atlas Manager server component, to update the atlas database.

The following figure shows the Atlas Manager server and client software:



The Atlas Manager looks for a rule in its rules table to help classify the system. The rules help the Atlas Manager make decisions, such as which icon should be used to display the system on the maps. If the system in the record matches one of the rules, the Atlas Manager updates the database according to the rule.

Database Object Editor

The Database Object Editor supplements the discovery system. Sometimes discovery might not discover devices on your network, or might display incorrect information of the devices on your network. You can use Database Object Editor to add the missing entities into the database or edit incorrect information of the entities.

The Database Object Editor client uses ConsoleOne snap-in to display the user interface. Using the Database Object Editor, you can perform operations on a segment or a node.

The Database Object Editor Server interacts with the Consolidator to process information related to the node and segment object and populates the topology database with this information.

You can use the Database Object Editor to add or delete a segment or a node and modify the segment or the node information.

To add a segment or a node:

1. From ConsoleOne, select Tools > Database Object Editor > New.
2. Enter the details for the segment or the node.
3. Click OK.

To edit the information about the segment or the node:

1. From ConsoleOne, select the segment or the node you want to edit.
2. Select Tools > Database Object Editor > Edit.

   Modify the required information.
3. Click OK.

To delete the segment or the node:

1. From ConsoleOne, select the segment or the node you want to delete.
2. Select Tools > Database Object Editor > Delete.

Management Console Software

The management console software snaps in to ConsoleOne. Management sites are created in ConsoleOne. In each site, an atlas is created that maintains the integrity of the discovery information.

Additional ZfS Components

NXPIP.NLM, NXPIPX.NLM, and NXPLANZ.NLM operate in conjunction with the following components:

- "Traffic Analysis Agent for NetWare Servers" on page 79
- "Server Management Agent for NetWare Servers" on page 80
- "Bindery of NetWare Servers" on page 80

Traffic Analysis Agent for NetWare Servers

The traffic analysis (LANalyzer) agent for NetWare is a set of NLM files that provides traffic analysis of Ethernet, Fiber Distributed Data Interface (FDDI), or token ring segments. The Traffic Analysis Agent discovers all systems on the segments it monitors, regardless of the protocols the systems use. You can monitor multiple segments by placing agents on each segment.

The NXPLANZ.NLM software on the management server uses SNMP to query servers running the Traffic Analysis Agent for information about each system that resides on their segments.

IMPORTANT: For an effective discovery process, you should have the Traffic Analysis Agent monitoring each source-routed token ring segment.

Server Management Agent for NetWare Servers

To discover IPX servers and workstations, managed servers are any NetWare 4.*x*, NetWare 5.*x*, or NetWare 6 servers with the server management agent installed. Server management agents respond to SNMP queries from NXPIPX.NLM with the username and address of those workstations that are logged in to the server. NXPIPX.NLM obtains SFT III™ server information from the server management agent. For effective results, you should install a management agent on every NetWare 3.*x*, NetWare 4.*x*, or NetWare 5.*x*, or NetWare 6 server on your network.

Bindery of NetWare Servers

NXPIPX.NLM queries all NetWare servers for information in their binderies. All NetWare servers allow their binderies to be examined by the discovery process when their security settings are set to the default values.

For the NetExplorer NLM software to discover the login names of workstations attached to a Netware server, a server management agent must be installed on the server.

Discovery Process

NetExplorer discovers your network continually. The following sections discuss the discovery processes:

- "Discovery Cycles" on page 80
- "Continuous Discovery" on page 86

Discovery Cycles

When you first start discovery, you should let it run as long as necessary to build the baseline data. Very small networks might take one or two hours, while very large networks (several thousand nodes) might require a day or two to be discovered.

The discovery process occurs in cycles. A cycle is the process by which a discovery module identifies every node it can at a time. You can configure discovery on the server to discover only certain addresses, thus reducing the duration of a cycle. For more information, see "Changing the Discovery Scope" on page 113.

The initial cycle continues until no additional devices are discovered. This initial cycle gathers information that might be insufficient to classify certain devices or to identify the correct segment for each device. Further discovery cycles provide additional, new, and changed information. As discovery cycles proceed, the information becomes more accurate.

Each discovery process queries the network using different methods to discover systems. Four independent discovery modules run in the order mentioned below during each discovery cycle:

1. **IP router discovery on IP networks only.**

   This process, run by the NXPIP module, starts from the local router. Using the local router's routing table information, NXPIP discovers other routers on the network. It then uses the routing table information to further discover the network. This process is repeated for each router discovered.

   The NXPIP module stores the router address information and information about any IP-bound network device in the IPCACHE module.

   NXPIP.NLM is installed on the management server. It uses SNMP to discover IP routers. To use this NLM, your management server must also be running TCP/IP bound to at least one of your network's interface boards. NXPIP.NLM uses MIB-II information, such as the system table, routing table, interface table, interface data-link type and frame type, and segment data-link type. Note that because there are different versions of MIB-II implementations for different vendors, the information you receive might differ.

   IMPORTANT: If you have specified an additional level of control by allowing certain IP addresses to perform SNMP queries to the routers, ensure that the IP address given to the ZfS server is privileged to query all the routers in the network. Otherwise, discovery will not be complete, and incomplete network information will appear in the Islands page of the atlas.

2. **IP discovery of workstations and servers.**

   This process, run by the IPGROPER module, receives the router and network information written into the IPCACHE by the NXPIP module as the input. RMON, based discovery run by the NXPLANZ module also writes the information about the networks and IP hosts that it discovers into IPCACHE. This also acts as an input to the IPGROPER module.

   It queries each router that has been discovered by NXPIP for its ARP tables, identifying each active IP host on the network. For IP addresses that are not found in the ARP table of any of the routers, IPGROPER tries to ping and identify whether a host by that IP address is alive.

IPGROPER queries each IP host that is identified to be alive for information about the following hosted services: HTTP, DHCP, Telnet, SMTP, and DNS. It also verifies whether the server management software and the Traffic Analysis Agents are installed and running on this host.

Simultaneously, the IPGroper module queries the DNS server specified in the SYS:\ECT\RESOLV.CFG file on the management server for the DNS names of all these IP hosts.

IMPORTANT: For a server or a segment to be manageable, it is important to discover the server management agent and the Traffic Analysis Agent running on an IP host on that server or the segment.

3. **IPX discovery on all networks, including NetWare/IP networks:**

   This process, run by the NXPIPX module, starts at the management server itself to discover its IPX address, the LAN type of each adapter, and SAP information about other known devices and their services. After gathering this information, NXPIPX requests the same types of information from each device listed in the bindery. This process is repeated each time NXPIPX discovers a new device.

   NXPIPX.NLM uses a variety of NetWare, SNMP, and IPX protocols, such as IPX diagnostics, to discover NetWare servers, IPX routers, and IPX workstations.

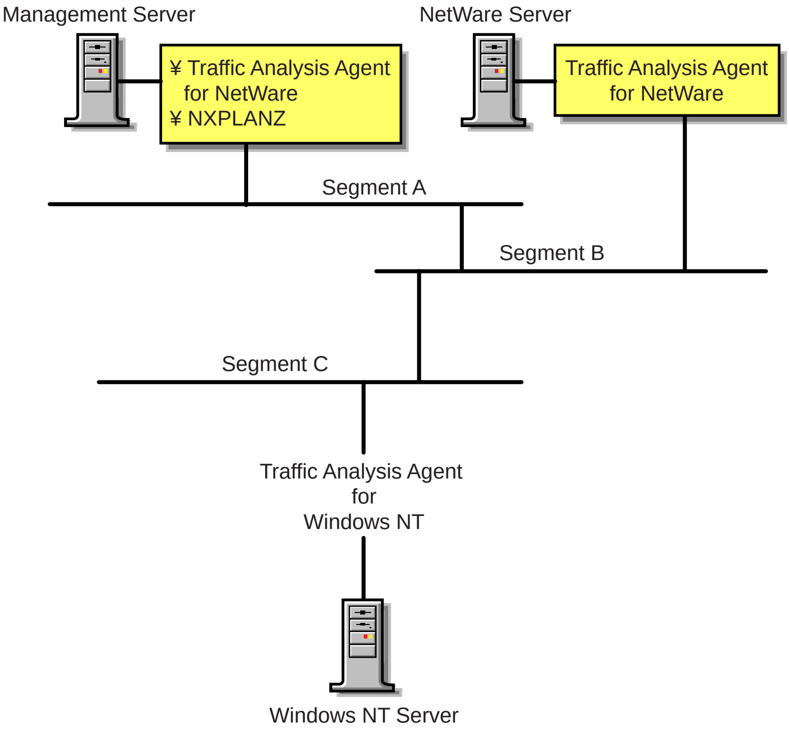
   IMPORTANT: When NXPIPX.NLM is loaded, a working directory named NXPWORK is created by default under the *install_volume*\install_dir\ZENWorks\MMS\MWSERVER\NMDISK subdirectory. During installation, you can specify a different path to create the NXPWORK subdirectory. NXPIPX puts all of its temporary files in this directory. Do not read, modify, or delete any file in this directory because this might cause some discovery process to not function.

4. **RMON based discovery of IP Hosts.**

   This process, run by the NXPLANZ module, starts by identifying all the remote agents, which includes the Traffic Analysis (LANalyzer) Agents for NetWare and Windows NT. The Traffic Analysis Agents on a segment discover devices based on the IP address to MAC address binding data contained in packets that are transmitted on the segment. The NXPLANZ module on the management server retrieves the data by using SNMP to communicate with the Traffic Analysis Agents.

   The NXPLANZ module reports information about the LANalyzer agents on your network and the IP hosts on the segments monitored by these LANalyzer agents to NetExplorer. The information about the networks monitored by the LANalyzer agents and IP hosts on the monitored networks is also written to IPCACHE to enhance the effectiveness of service discovery by the IPGROPER module.

The following figure shows NXPLANZ querying Traffic Analysis Agents software on segments B and C, respectively.


Management Server
¥ Traffic Analysis Agent for NetWare
¥ NXPLANZ
NetWare Server
Traffic Analysis Agent for NetWare
Segment A
Segment B
Segment C
Traffic Analysis Agent for Windows NT
Windows NT Server

To improve the effectiveness of the discovery, ensure that the LANalyzer agent is installed and running on each network segment that you want to discover. If SLP is disabled on your network or if SAP packets are filtered by the routers in your network, NXPLANZ may not be able discover all the LANalyzer agents in the network.

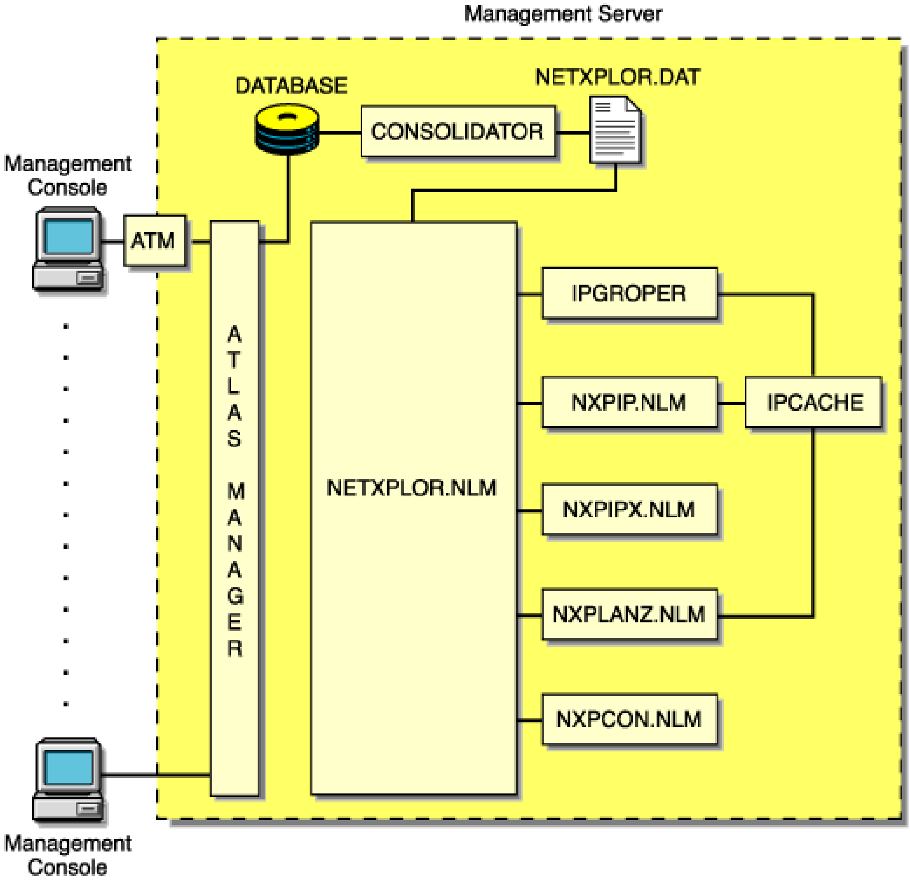
In order to ensure that all the LANalyzer agents on your network are being queried by the NZPLANZ module, specify these LANalyzer agents explicitly using NXPCON.

During the initial discovery cycle, these modules run sequentially. As a result, information about the Traffic Analysis Agent software is discovered late.

In later discovery cycles, the four modules run concurrently. They continue their discovery processes, but send only new or changed data to NETXPLOR.NLM. As additional data arrives, segments can be consolidated, devices can be placed on the appropriate segments, and new devices can be discovered.

Each succeeding cycle of different discovery NLM files has the potential to provide key information that finally identifies a device and provides sufficient data for NetExplorer to consolidate the data.

The data discovered by the NLM processes is communicated to ConsoleOne through the Atlas Manager. The following figure shows the relationship of the discovery NLM processes, NetExplorer, and ConsoleOne. See "Discovery Process" on page 80 for a description of how these pieces operate together to discover the contents and topology of a network.



The following table summarizes the default seed and scope and user-definable changes for each discovery module:

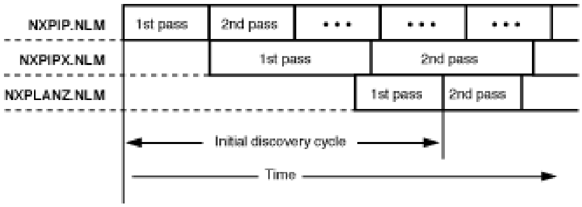
Discovery Module	Default Seed Information	Default Scope	User-Definable Changes
NXPIP	Examines the management server routing table. Places the router addresses in the IPCACHE module.	Entire network if community string matches.	Reduce scope by specifying IP scope information in NXPCON. If public SNMP community string is not used, list SNMP community strings of routers in NXPCON.
IPCACHE	Supporting module in NetExplorer. Contains temporary information about devices and networks which is used by NXPIP, IPGROPER and NXPLANZ.		
IPGROPER	1. Queries each router address in IPCACHE for ARP tables to identify network devices. 2. Queries each network device for the services it hosts (FTP, HTTP, Telnet, SMTP, DNS, and DHCP) and their DNS names. 3. Discovers hosts running server management and Traffic Analysis Agents.	All IP networks connected to routers already discovered by NXPIP	◆ Enable or disable autodiscovery ◆ Enable or disable file-based discovery
NXPIPX	Examines the management server's configuration.	Entire IPX internetwork.	Reduce scope by specifying IPX scope information in NXPCON.

Discovery Module	Default Seed Information	Default Scope	User-Definable Changes
NXPLANZ	Examines the list of servers running Traffic Analysis Agent software listed in NXPCON.	All segments with Traffic Analysis Agent software.	Specify name and IP addresses of Traffic Analysis Agent for Windows NT in NXPCON. If SLP is disabled or SAP is being filtered, specify the name and address in NXPCON for the Traffic Analysis Agent for NetWare.

Continuous Discovery

NetExplorer discovers the internetwork on which it resides, through a process initiated and controlled by NETXPLOR.NLM. Initially, each discovery NLM identifies itself to NETXPLOR.NLM, which then begins the initial discovery cycle. The cycle starts with NXPIP discovery, followed by NXPIPX discovery, and finally NXPLANZ discovery. The discovery cycles of IPGROPER are not controlled by NETXPLOR.NLM. Once started it runs continuously. Information gathered by NetExplorer is stored in the NETXPLOR.DAT file on the management server.

In the following figure, each of the discovery processes is shown in relationship to time. Once NXPIP finishes its first pass, NXPIPX begins and NXPIP starts over. After NXPIPX finishes its first pass, NXPLANZ begins and NXPIPX starts its second pass. Unless otherwise directed, all three of the discovery processes run continually to detect changes to the network. Any changes to the network are saved as records in the NETXPLOR.DAT file. When all three discovery processes have completed one pass, the initial discovery cycle is complete.



The following sections describe each sequence in greater detail:

- "NXPIP" on page 87
- "NXPIPX" on page 87
- "NXPLANZ" on page 88
- "NETXPLOR" on page 88
- "SNMP Community String Discovery" on page 89

NXPIP

The first sequence in the NetExplorer discovery cycle involves the discovery of IP routers. NXPIP locates its local router using TCP/IP configuration information. NXPIP then queries the router for the identity of other routers on the network. NXPIP queries the MIBs on the routers using SNMP to collect the IP addresses, interface types, and MAC addresses.

By default, NXPIP attempts to discover your entire IP network. You can restrict the scope of the IP discovery by specifying the scoping information in NXPCON.

NXPIPX

NXPIPX uses a series of techniques, including SNMP, RIP, IPX, and SPX™ diagnostics to discover the attached IPX or NetWare/IP internetwork. After NXPIP completes its first pass, NXPIPX begins discovery at the management server. NXPIPX examines its own server and discovers the names of other servers. It then queries each of these servers to discover more servers and repeats this process until no more servers are found.

In addition, NXPIPX reads the connection table of each NetWare server to determine which NetWare clients are logged in to the server. NXPIPX sends IPX diagnostic packets to each client to collect additional information. NXPIPX will not discover clients that do not appear in the connection table because they have not been logged in recently and clients whose diagnostics are turned off. It is therefore important to leave IPX diagnostics enabled on NetWare clients.

NXPIPX also discovers IPX routers in your network. Third-party IPX routers are discovered only if there is a NetWare server on the routed segment. NXPIPX does not discover interface information when routed segments do not have NetWare servers.

By default, NXPIPX attempts to discover your entire IPX internetwork. You can restrict the scope of discovery by specifying a list of IPX network numbers using NXPCON. For NXPIPX to discover other IPX nodes ensure that one of the IPX numbers is bound to the management server.

NXPLANZ

The Traffic Analysis Agent for NetWare monitors every packet on the network segment it is installed on. It creates a list of physical (MAC) addresses and IP addresses of all the systems communicating on the segment on the local memory. After NXPIPX completes its first pass, NXPLANZ uses SNMP to query all servers with Traffic Analysis Agents installed to read the list of workstations communicating on the network. NXPLANZ also obtains a list of the agents running on the servers from NXPIPX.

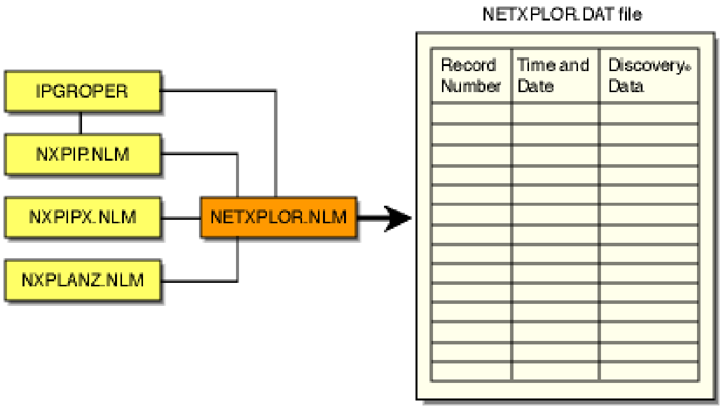
IPGROPER

The information about the routers and network segments written into IPCACHE by NXPIP, and the information about network segments, and hosts written to IPCACHE by NZPLANZ forms the input to the IPGROPER module. For each network segment, IPGROPER tries to discover all the hosts on that network, the DNS names of the hosts, the services hosted on them, server management agents, and Traffic Analysis Agents.

NETXPLOR

As the discovery processes gather information about systems on the network, they forward packets of related data to NETXPLOR.NLM. NETXPLOR.NLM places these packets, along with a record number and a time stamp, into the NETXPLOR.DAT file, as shown in the figure below.

NOTE: Discovery re-creates the NETXPLOR.DAT file each time you load NETXPLOR.NLM. Therefore, the discovery data stored at the management server from previous runs of the NetExplorer NLM processes is not retained when you restart NETXPLOR.NLM.



SNMP Community String Discovery

Each time NetExplorer tries to access a system through SNMP, it uses the community strings that have been configured using the NXPCON utility on the management server. When it encounters a new system, it tries each of the configured community strings. After it has found a community string for a particular IP or IPX address, it records this name in a file so that in subsequent cycles it does not need to retry with the other configured names.

You can view these community strings using NXPCON. The community strings are used in the order specified. Therefore, the most-used community string should be configured first in the list.

IMPORTANT: An SNMP query with an invalid SNMP community string results in no response from the target system and the request times out.

What Is Discovered

NXPIP, NXPIPX, and NXPLANZ use a variety of techniques to discover the following categories of network objects and present them in the atlas:

- "Systems" on page 89
- "Network Segments" on page 98

Generally, information gathered by NXPIP and NXPIPX is sufficient to place systems on the network maps correctly. When NXPIP and NXPIPX have not discovered systems, NXPLANZ retrieves MAC addresses collected by the Traffic Analysis Agent software and the new systems are added to the database. Consequently, all systems are discovered on segments monitored by the Traffic Analysis Agents.

Systems

The following table shows the different types of systems discovered:

System	Comment
NetWare Management Agent	Service type of 563 decimal (NetWare Management Agent 1.5 or 1.6) or 635 decimal (NetWare Management Agent 2.6) or NetWare Management Agent MIB implemented.
Management Agent for Windows NT/2000	NT Management Agent MIB implemented.

System	Comment
NetWare LANalyzer Agent	Service type of 570 decimal or LANalyzer MIB implemented.
LANalyzer Agent for Windows NT/2000	LANalyzer MIB implemented
NetWare File Server	Service type of 4 (file server). NXPIPX discovers all NetWare 3.*x,* 4.*x*, and 5.*x* servers.
NetWare Print Server™	Service type of 71 or 7 decimal.
IPX Router	System with more than one adapter connected to different IPX networks.
IP Router	System that is configured as an IP router in MIB-II (IP forwarding enabled).
NetWare Client Workstation	System that responds to IPX diagnostics requests as an IPX workstation (has the NetWare Shell loaded).
SFT III IOEngine	Discovered by the IPX discovery module; responds with diagnostic information.
SFT III MSEngine	Discovered by the IPX discovery module.
Network Printers	Discovered if the printer generates a well-known service type.
NetWare Connect™	Service type of 590 decimal.
NetWare Communications Server	Used by the NetWare for SAA* services manager products; has a service type of 304 decimal.
Management Server	Running discovery NLM files; has a service type of 567 decimal.
Any System	Any system is discovered if it is connected to a LAN segment being monitored by a Traffic Analysis Agent.

The different types of services discovered are Telnet, HTTP, DNS, SMTP, DHCP, Routers, eDirectory, SFTIII, and SNMP.

The following sections contain more information about the various systems that are discovered:

- "NetWare Client Workstations" on page 91
- "IP Routers" on page 92
- "NetWare SFT III Servers" on page 93
- "Systems Not Equipped with the IPX Diagnostic Responder" on page 94
- "Routers that Use Duplicate MAC Addresses" on page 95
- "Third-Party Routers" on page 95
- "NetWare MultiProtocol Router with WAN Ports" on page 96
- "IPX Networks" on page 96
- "IP Networks" on page 96
- "On-Demand Links" on page 97
- "Third-Party Routers with WAN Ports" on page 97
- "NetWare Connect Servers" on page 97
- "Virtual Switches" on page 97

NetWare Client Workstations

NXPIPX discovers all NetWare client software attached to discovered NetWare 3.*x*, 4.*x*, and 5.*x* servers. Clients that are turned off or are not attached to a server are not discovered. For this reason, a NetExplorer process that is run at night or on a weekend might not yield a complete map. Note that NetWare clients must have IPX diagnostics enabled.

When you configure a NetWare client to perform a bindery login, consider the scenarios in the following table:

Server	Bindery Login—What Is Discovered
NetWare 3.*x*, 4.*x*, or 5.*x* with server management agent installed	Workstation discovered; name is discovered only if logged in with IPX as the transport for NetWare 4.*x* and NetWare 5.*x*
NetWare 3.*x*, 4.*x*, or 5.*x*	Workstation discovered; name is not discovered

When you configure the client to perform a directory login, NetExplorer discovers only those systems that are *logged in* to an eDirectory tree and not those that are merely *attached* to the eDirectory tree. NXPIPX uses SNMP community string to communicate with the management agent and query on all NetWare servers for the username.

After NetExplorer discovers a NetWare client, NXPIPX queries the client using the IPX diagnostic protocol to confirm the discovery and gather more information about it. If IPX diagnostics are turned off, NXPIPX does not report the system. This applies to printers as well.

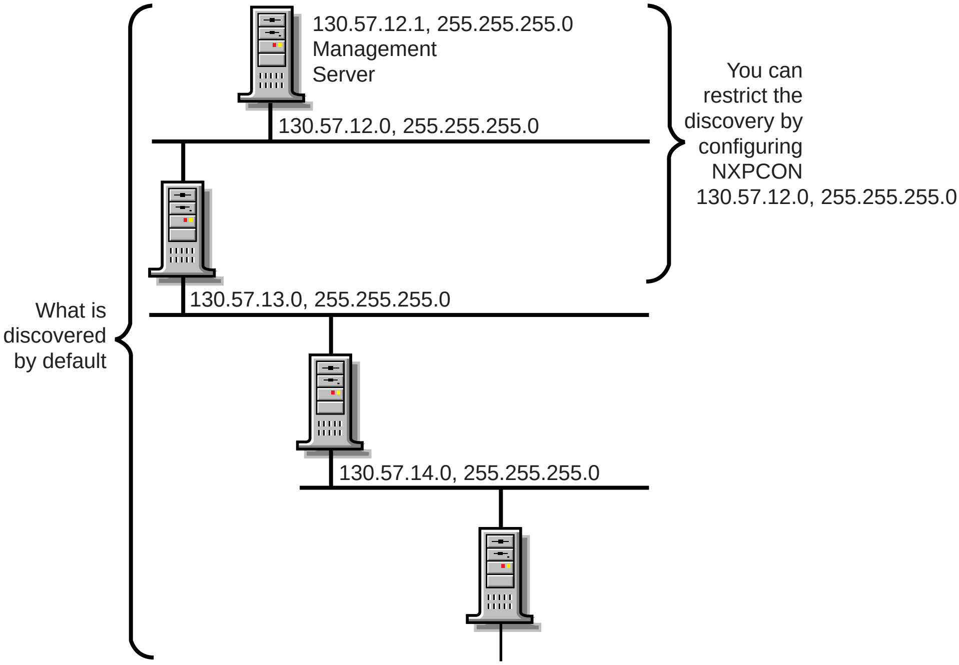
IP Routers

NXPIP uses SNMP to query all IP routers on the network by using the SNMP community string used by the routers. You must enter the list of community strings used by your routers using NXPCON.

You can configure this information into the router's MIB by using any SNMP configuration tool, including the SNMP MIB browser. If you configure router information such as the system name in the routers SNMP MIB, the discovery process records it in the database, allowing IP routers to be displayed with meaningful names.

By default, IP discovery discovers the entire network. The exploration can be restricted by specifying network numbers using the NXPCON Discovery Scope > IP Discovery Scope option. Also, if there are redundant IP routers, use the NXPCON IP Discovery > IP Routers option to specify the redundant IP router address; otherwise, NXPIP does not discover it. As shown in the following illustration, if the management server IP address is 130.57.12.0, the IP discovery NLM discovers the entire 10.57.85.0 network and its subnets.

The following figure shows how ZfS discovers IP routers:

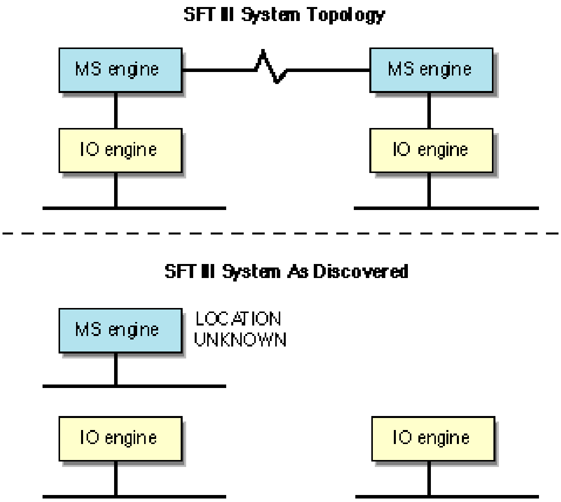


NetWare SFT III Servers

A NetWare SFT III™ server usually consists of two computer systems, each containing an input/output engine (IO engine) and a mirrored server engine (MS engine). Therefore, physically there are two IO engines and two MS engines; logically there are two IO engines and one MS engine.

If NetWare Management Agent is loaded on an SFT III server, the MS engine and both IO engines are discovered correctly with their names and placed in the correct segment in the atlas. However, the MS engine is placed in the Islands page. This happens because the two MS engines are associated with only one logical server on the network, and the location of the MS engine might change depending on which copy of the MS engine is the primary at any given time.

The following figure illustrates NetWare SFT III server discovery:



If the server management agent is not loaded on the MS engine, Discovery discovers only the MS engine and the IO engine that are primary at the time of discovery. The primary IO engine is labeled Noname in the area page. To change the name of an IO engine on a segment map, right-click the icon and click Rename.

Systems Not Equipped with the IPX Diagnostic Responder

NXPIPX discovers the following systems, but does not necessarily place them correctly in the atlas:

- NetWare for UNIX* servers
- Portable NetWare servers
- Access servers
- Modem servers
- Print servers

Because these systems do not respond to IPX diagnostics, they cannot answer queries from NXPIPX. Consequently, the LAN information required to place them on the maps might not be available. In this situation, NetExplorer places these systems in the Islands page of the atlas. In most cases, the presence of a Traffic Analysis Agent on each segment on which these systems appear, enables NetExplorer to obtain the missing information and correctly locate the systems in the maps.

If these systems are running IP, they will be discovered and placed correctly in the maps.

Routers that Use Duplicate MAC Addresses

NetExplorer can experience difficulties in discovering some routers because of the method routers use to identify their adapters. In some cases, the same MAC address is used on several network interfaces of a router. In these cases, it appears to NetExplorer that one adapter is connected to multiple segments. Unless otherwise specified, NetExplorer interprets multiple adapters as one adapter.

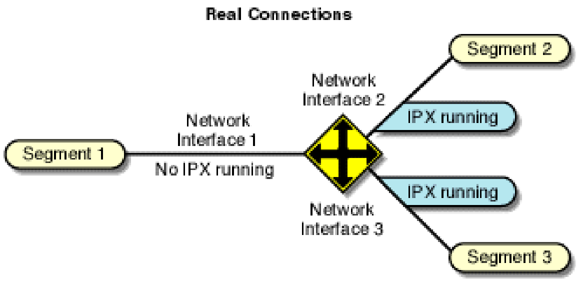
The multiple segments connected to the adapters are seen as one segment and NetExplorer consolidates the multiple segments.

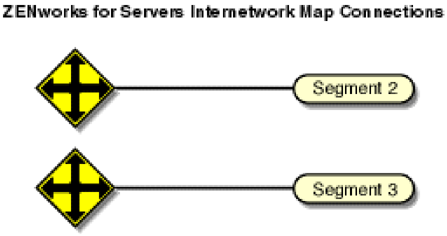
Third-Party Routers

NXPIP discovers IP-bound interfaces only. When IP is not running on a router, NetExplorer discovers the IPX-bound interfaces, which results in:

- A separate router icon is shown for each interface in the router.
- Discovered interfaces are not placed in the same router in the atlas. Therefore interconnections are incorrect on the internetwork map and the router appears as separate, multiple routers, each containing one network interface from the real router.

The following diagram illustrates a router with IPX running on Network Interfaces 2 and 3 but not on Network Interface 1. NetExplorer places this router on the internetwork map as two separate systems. As shown, the connection to Segment 1 is not displayed, and the connections to Segments 2 and 3 are shown attached to two separate systems.





NetWare MultiProtocol Router with WAN Ports

NetWare MultiProtocol Router™ (MPR) 3.0 is now bundled with NetWare 5.*x*.

IPX Networks

NetWare MPR™ 3.0 reports the correct segment type of the WAN links. NetExplorer detects these correctly and displays them with the appropriate icon.

IPXWAN links between NetWare MPR 3.0 systems do not have an IPX network associated with them. When NetExplorer discovers such a link, it creates a name for the WAN segment of the form #UNNUM -*n*, where *n* is an integer assigned to make the segment name unique. On multi-access networks, such as frame relay and X.25, each connection in the network adds another #UNNUM -*n* to the segment name.

IP Networks

With NetWare MPR 3.0, you can configure both numbered and unnumbered IP links. NetExplorer discovers numbered links correctly. NetExplorer does not discover unnumbered IP links, resulting in the Islands page.

If IP is running on a third-party router and NXPIP is running on the management server, NetExplorer discovers only the IP-bound interfaces. The router is shown correctly in the atlas. If IP is not running on a third-party router but NXPIPX is running on the management server, NetExplorer discovers the IPX-bound interfaces. However, these IPX-bound interfaces are not placed in the same router icon in the atlas.

On-Demand Links

An on-demand link is a WAN connection between two routers in which only user data (no routing traffic) is exchanged across the link. The link is brought up only when there is data to send.

NetExplorer discovers on-demand IP and IPX links correctly, if sufficient static routing information has been configured to allow the management server to reach the other side of the on-demand link.

However, if a link is an on-demand and unnumbered IP link, the entire topology on the remote end of the link is not discovered. Click IP Discovery > Additional IP Routers in the NXPCON utility to configure an additional IP router address for the missing router.

Third-Party Routers with WAN Ports

NetExplorer discovers third-party routers correctly if they support MIB-II SNMP. Certain third-party routers can have a WAN link with no IP or IPX network number on the link In this case, the WAN link is not discovered.

NetWare Connect Servers

NetExplorer discovers NetWare Connect servers; however, if you have more than one NetWare Connect® server on the network, NetExplorer consolidates them and they appear as one server.

Virtual Switches

A virtual switch is represented by the same icon used for a switch or bridge in the atlas maps. The display name of a virtual switch is always shown as the "switch on *IP address of network*." It is primarily used in atlas maps to display a meaningful network topology when discovery information is incomplete.

A virtual switch is shown in atlas maps under the following conditions:

- When two or more different physical media are connected by a switch, but the switch is not yet discovered. The virtual switch will disappear as soon as the real switch is discovered.

- When two or more different physical media are connected by a switch, the switch is configured with SNMP community strings other than public, and the SNMP community strings of the switch were not provided through NXPCON before starting discovery.
- When two or more different physical media are connected by a non-manageable switch or a hub.

Network Segments

NetExplorer discovers the following network segments:

- "LAN and WAN Segment Types" on page 98
- "Source-Route Bridged Token Rings" on page 99

NetExplorer cannot fully discover the following:

- "Transparent Bridges" on page 100
- "Configuration Changes" on page 100

LAN and WAN Segment Types

NetExplorer discovers the LAN and WAN segment types shown in the following table:

Known Segments in CIM Database	Unknown Segments in CIM Database
ATM	LAN: ARCnet
LAN: FDDI	LAN: LocalTalk*
LAN: Ethernet	SMDS
LAN: Token Ring	WAN: ISDN
WAN: X.25	WAN: SDLC
WAN: PPP	WAN: Serial
WAN: Frame_Relay	WAN: T1
	WAN: T3

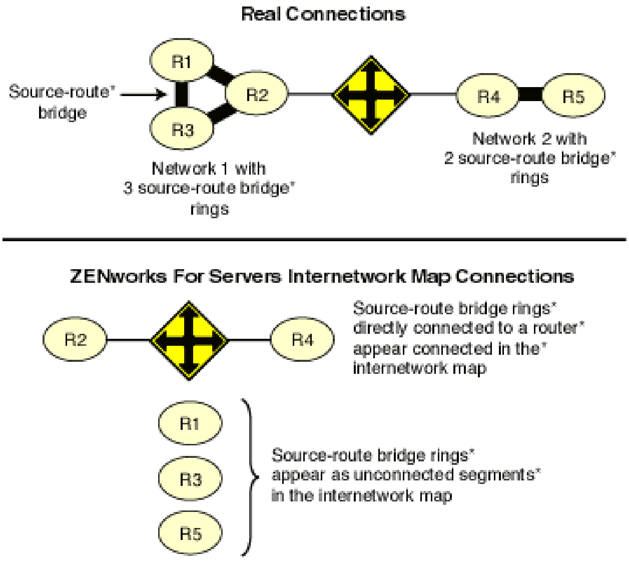
These values are discovered correctly if a system connected to the segment responds with an interface type from MIB-II RFC 1573.

Source-Route Bridged Token Rings

Atlas Manager displays source-route bridged token rings depending on whether the Traffic Analysis Agent for NetWare is installed on each ring.

- If you do not have the Traffic Analysis Agent for NetWare installed on each source-route bridged token ring in your network, NetExplorer discovers the network but consolidates all source-route bridged token rings that share the same IPX network number or IP subnet into a single segment. For example, in the following figure, rings R1, R2, and R3 are displayed as one segment, and rings R4 and R5 are displayed as another segment on the internetwork map.
- If you have the Traffic Analysis Agent for NetWare installed on each source-route bridged token ring, each Traffic Analysis Agent for NetWare discovers its own ring (segment) and every system on it. Atlas Manager displays the ring as a disconnected segment on the internetwork map.
- If you have the Traffic Analysis Agent for NetWare installed on a source-route bridged token ring connected to a router, the WAN page in the atlas shows the correct connections. However, if two networks each have several rings and only one ring in each network is connected to a router, the WAN page shows the correct connections of only the rings that are directly connected to the router. The other source-route bridged token rings in each network are displayed as disconnected segments on the WAN page.

  The following figure illustrates this second case.


Real Connections
Source-route bridge
R1
R2
R3
R4
R5
Network 1 with 3 source-route bridge rings
Network 2 with 2 source-route bridge rings
ZENworks For Servers Internetwork Map Connections
R2
R4
Source-route bridge rings directly connected to a router appear connected in the internetwork map
R1
R3
R5
Source-route bridge rings appear as unconnected segments in the internetwork map

In all cases, bridge information is not discovered. As a result, discovery treats each interface of a source-route bridge as a separate system on the network. One icon appears in the atlas for each interface of the source-route bridge.

When you have the Traffic Analysis Agent for NetWare installed on one server on each ring of an IPX source-route bridged network, the segment names displayed on the WAN page consist of the IPX network number followed by the MAC address of that server's interface to the ring. If the Traffic Analysis Agent for NetWare is monitoring more than one interface, the address shown for a ring is the MAC address of the interface monitoring that ring.

Transparent Bridges

Discovery cannot completely discover transparent bridges. It consolidates groups of transparently bridged segments running the same network number into a single segment on the maps.

Configuration Changes

Discovery detects most changes in the network topology, such as the addition, reconfiguration, or deletion of interfaces, resulting in changes being made to the atlas. However, if you remove the system from the network, it is not detected unless you move it to another location in the network.

File-Based Discovery

The enhancement to the IPGroper.NLM allows the you to use the DiscNodes.txt file to specify the IP Address and mask of a set of nodes to be discovered. The information about the nodes is obtained through SNMP.

The IPGroper NLM must be loaded with specific options that enable it to receive inputs from the DiscNodes.txt file. If these options are not provided, the NLM will discover without taking input from the file. Prior to starting the discovery, the DiscNodes.txt file must be placed in the ZFS-INSTALL-DIR/MWSERVER/NMDISK directory. After the initial discovery, if you want more nodes to be discovered, you must create a new DiscNodes.txt file with the new node entries and place it in the same directory. These nodes will be queried in the next discovery cycle.

The DiscNodes.txt input file has the following format for individual IP addresses:

- Individual IP Address specification format:

  IPAddress <, SubnetMask>

- Specifying addresses using regular expressions

  IPAddress <, SubnetMask>

  IPAddress -> AddressPattern

  Characters allowed in AddressPattern include the numerals 0-9; the period (.); the question mark (?), which represents one character; and the asterix (*), which represents more than one character, up to a maximum of three.

- Wildcard characters are not allowed in the subnet mask.

164.99.149.*	All addresses in the range from 164.99.149.1 to 164.99.149.254
164.99.14?.*	all addresses in the range from 164.99.140.1 to 164.99.149.254
164.99.149.?	all addresses in the range from 164.99.149.1 to 164.99.149.9

NOTE: 164.99.149.0 does not come into the range. ? does not stand for 0 if it is the only letter in the octet.

164.99.149.1?0 - all addresses in the range from 164.99.149.100 to 164.99.149.190. Here ? stands from 0

- In the text file, any line that begins with a " # " is treated as a comment line.

File-based discovery can be used in the following two scenarios:

- "Discovering the Nodes Specified in the file" on page 101
- "Discovering the Nodes with Other Discovery Modules" on page 102

Discovering the Nodes Specified in the file

By default, the ZfS installation loads the NXPCON utility with all the discovery modules running and with file-based discovery enabled.

To discover only the nodes specified in the input file:

1. In NXPCON, click Configuration Options > Discovery Modules.
2. Select Individual Discovery Modules > press Enter.
3. Select No to unload the modules > press Enter.
4. Press Esc to exit the Discovery Modules dialog box.
5. Click Yes to save changes.
6. Click Configuration Options > IP Discovery.
7. Select IP Host Discovery > Press Enter.
8. Select Enable IP Host Discovery > press Enter.
9. Select No to disable autodiscovery of the IP workstation.
10. Make sure that the Enable File-Based Discovery option is set to Yes.
11. Press Esc to exit the IP Host Discovery dialog box.
12. At the Management server prompt, unload NetExplorer by entering **unxp**.
13. Reload the NetExplorer modules by entering **netxplor.**

Discovering the Nodes with Other Discovery Modules

By default, the ZfS installation will start all the discovery modules along with the file-based discovery. Use the following procedure to individually select the modules that need to be started or to change the configuration.

To discover only the nodes specified in the input file:

1. In NXPCON, click Configuration Options > Discovery Modules.
2. Select Individual Discovery Modules > press Enter.
3. Select Yes or No to load or unload each module > press Enter.
4. Press Esc to exit the Discovery Modules dialog box.
5. Click Yes to save changes.
6. Click Configuration Options > IP Discovery.
7. Select IP Host Discovery > Press Enter.
8. Select Enable IP Host Discovery > press Enter.
9. Select No to disable Auto Discovery of the IP workstation.
10. Make sure that the Enable File-Based Discovery option is set to Yes.

11 Press Esc to exit the IP Host Discovery dialog box.

12 At the Management server prompt, unload NetExplorer by entering **unxp**.

13 Re-load the NetExplorer modules by entering **`netxplor.`**

Effects of Discovery on Maps

The Atlas Manager on the management server creates an atlas database as the topology database is populated and the information is displayed as maps on ConsoleOne. The WAN page displays all the Area pages and the connecting routers between them. The Area pages display the segments and the connecting routers.

The discovered systems are placed on the Area pages of the atlas based on the connecting routers or bridges. The Islands page contains segments for which routers have not yet been discovered. The Atlas Manager relocates the segments to the correct pages when connecting routers are discovered.

Review the following sections for more information on the effects of discovery on maps:

- "Name Source Priority" on page 103
- "Representation of Systems in the Atlas" on page 104

Name Source Priority

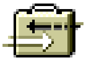
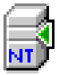
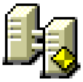
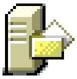
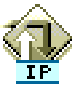
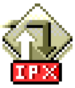
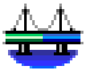
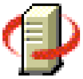
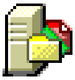
As discovery cycles proceed and more information is discovered, the names displayed in the maps can change. Different priorities are given to names, depending on the source of the name information.

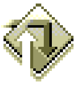
To determine how to display the name of the discovered object, the Atlas Manager uses the following list in the order shown:

1. User Defined Name
2. DNS Name
3. eDirectory Name
4. Bindery Name
5. SNMP Name
6. IP Address
7. IPX Address
8. MAC Address

Representation of Systems in the Atlas

When representing a system in a map, the Atlas Manager refers to the following list of services in the order shown. As soon as it associates the first service with the node, it displays it without looking for further matches. The icon may change if a service with a higher priority is detected later during discovery.

Priority Number	Icon	Description
1.		NetWare server running the server management agent software
2.		Windows NT server running the server management agent software
3.		SFT III server running the MS engine
4.		Server running file server software
5.		Router running IP service
6.		Router running IPX service
7.		A switch or a bridge
8.		Server running the discovery process
9.		Server running the topology database

Priority Number	Icon	Description
10.		NetWare or Windows NT server running the traffic analysis (LANalyzer) agent software
11.		Server running Remote Monitoring
12.		Server running Remote Monitoring II
13.		Server running print server software
14.		Server running IP software
15.		Server running NetWare Connect software
16.		Router
17.		Printer
18.		IP workstation
19.		IPX workstation
20.		Others

If a system has either an IPX or IP router service, the Atlas Manager considers it a router and displays it on the appropriate pages and segments.

Setting Up Discovery

The discovery software on a management server automatically discovers the nodes on your network. Network nodes include servers, desktops, routers, hubs, switches, and any other network devices. The Consolidator on the server populates the database with the discovered data. The Atlas Manager on the server reads the database and creates the atlas.

ZfS allows discovery in two different environments:

- Pure IP environment
- IP/IPX environment

  You must have IP enabled between ConsoleOne and the management server.

Before starting discovery, you must verify the following configurations to ensure that the discovery system is complete:

- Ensure that the router to which ZfS Server is attached is specified as the seed router in NXPCON. If necessary specify, additional IP routers also. For more information on specifying seed router and additional IP routers, see "Specifying a Seed Router and Additional IP Routers" on page 117
- Ensure that the community strings used for all the devices to be managed are specified in NXPCON. For more information on changing SNMP community strings, see "Changing the SNMP Community String" on page 112.
- Ensure that the ZfS Server is privileged to query the routers in your network if the routers are configured to restrict access to only specified IP addresses. For more information on IP router discovery, see "IP router discovery on IP networks only." on page 81.
- If you want to restrict the scope of IP or IPX discovery, specify proper scoping entries. For more information on changing the discovery scope, see "Changing the Discovery Scope" on page 113.
- Ensure that the DNS configuration file SYS:\ETC\RESOLV.CFG has a valid DNS server's IP address. If a valid DNS server is not specified, discovery will fail to discover the DNS names of hosts.
- For effective discovery, ensure that the Traffic Analysis Agent is installed and running on each network segment that you want to discover and

manage. Also, ensure that the names and addresses of these agents are specified in NXPCON. For more information on specifying Traffic Analysis Agents, see "Specifying Traffic Analysis Agents to Be Queried by NXPLANZ" on page 116.

- If a MAC address is being associated with different network numbers, all such network numbers will be merged into a single segment. To avoid the merger, you must specify all such MAC addresses in upper case in the *installation_directory*\MMS\MWSERVER\BIN\CONSOLIDATOR.INI file.

  In CONSOLIDATOR.INI, specify the MAC address as a key value pair in the [DuplicateMacAddress] section.

  A sample CONSOLIDATOR.INI is as follows:

  ```
  [DuplicateMacAddress]

  mac1="00C04F59910D"

  mac2="00C04F5991AB"

  ...

  key_name=value
  ```

  In CONSOLIDATOR.INI, ensure that the keys are unique.

  Before starting the MMS server, edit the ZENWorks\MMS\MWSERVER\PROPERTIES\SLOADER.PROPERTIES file to append the ARGUMENTS value under TOPOLOGY MANAGER with the following entry: `-ini "installation_directory\MMS\MWSERVER\BIN\CONSOLIDATOR.INI"`.

The following tasks will start discovery initially and help you customize discovery to meet your organization's needs:

- "Starting Discovery" on page 108
- "Checking the Status of Initial Discovery" on page 108
- "Checking the Results of Discovery" on page 109
- "Changing the Default Configuration" on page 110
- "Configuring the Java Processes" on page 117
- "Unloading the Management Server" on page 119

Starting Discovery

Discovery starts automatically when the discovery software is loaded on the management server.

To manually start autodiscovery and load the back-end services (management site services), refer to the steps in Installing and Setting Up Management and Monitoring Services in the *Installation* guide.

Restarting the Management Server

If you bring down the management server (for example, for maintenance), the restart affects discovery in the following ways:

- Each time you reload the discovery modules, a new version of NETXPLOR.DAT is created.
- The initial discovery cycle starts again.
- The Consolidator processes all the discovery data again as ZfS rediscovers the network.

To unload the discovery modules:

1. At the NetExplorer server, enter **`unxp`**.

To load the discovery modules:

1. At the NetExplorer server, enter **`netxplor`**.

Checking the Status of Initial Discovery

As discovery progresses, your topology maps in ConsoleOne reflect the discovered data. However, in a large network, it might take a day or two before the initial discovery is complete.

The easiest way to determine whether initial discovery is complete is to use the NXPCON utility on the management server and check the status of each NetExplorer module. Each module must complete at least one full cycle to draw a complete map.

To view the discovery status, look at the discovery status fields at the top of the NXPCON screen. See "Using the Discovery Configuration Utility" on page 111 for information about how to access this screen.

The NXPCON main screen gives you the information you can use to monitor the status of discovery.

The following information is displayed:

- **NetExplorer Up Time:** Shows the time since NetExplorer started running.
- **NetExplorer System Status:** Shows the overall status. It can have one of the following values:
  - Waiting to start - Waiting for one or more of the discovery modules to start.
  - Running - Discovery modules are running.
- **Module Status:** Shows the status of each module and the number of cycles each module has completed. The module status can be one of the following values:
  - Not Loaded - Module is not loaded.
  - Waiting to Start - Module is loaded but not started.
  - Running - Module is running and collecting data.
  - Suspended - Module is suspended because it reached the end of the schedule in which it was running.
  - Completed - Module completed a discovery cycle.
  - Unknown - NetExplorer cannot obtain the module status. (This is usually seen if the module is not loaded.)

Checking the Results of Discovery

When the Consolidator has finished updating the database after the initial discovery, verify if the network topology is accurately represented on the maps.

NetExplorer might not have discovered the type if a node is not on the map. If a node does not appear in the correct segment, NetExplorer may not have received sufficient information to place it correctly. For more information, see "What Is Discovered" on page 89. The following characteristics are captured:

- IP - Discovers IP routers; IP hosts; IP services such as HTTP, Telnet, SMTP, DNS, FTP; and DHCP.
- IPX - Discovers IPX workstations, IPX routers, and IPX services (file, print, any other Service Advertising Protocol [SAP]).
- Subnet mask
- Services

- eDirectory names and tree
- DNS Names

The Consolidator on the management server communicates with NetExplorer to obtain network discovery data. The Consolidator reads the NETEXPLOR.DAT file and populates the database.

IMPORTANT: The NETEXPLOR.DAT file is reset every time you restart NetExplorer.

The Consolidator communicates with two Java* components: the Bridge Agent and the SN3 agent. The Bridge agent retrieves bridges present in the network and the related topology of the network. The SN3 agent does SLP-based discovery for NetWare 5.*x* servers and gets the corresponding eDirectory name for each IP and IPX address discovered.

IMPORTANT: NetExplorer and the Consolidator can run independent of each other on the management server.

NetWare 5.*x* servers are discovered faster because NetWare 5.*x* supports the Service Location Protocol (SLP).

Ensuring Complete Discovery

IPX workstations are discovered with a username if the user is logged in to or attached to a NetWare server running management agent software. To ensure that the user names for IPX devices and workstations on your network can be discovered, install a management agent on all NetWare servers where users log in.

If you want NetExplorer to discover AppleTalk* devices, you need to install the NetWare LANalyzer Agent on one server on each segment.

Changing the Default Configuration

The discovery software is installed with default configuration designed to work in most environments. However, if your network or the data on your database is not discovered, you need to reconfigure discovery.

Read the following sections for more information:

- "Using the Discovery Configuration Utility" on page 111
- "Choosing Which Discovery Modules to Load" on page 111
- "Changing the SNMP Community String" on page 112
- "Changing the Discovery Scope" on page 113

- “Specifying Traffic Analysis Agents to Be Queried by NXPLANZ” on page 116
- “Specifying a Seed Router and Additional IP Routers” on page 117

Using the Discovery Configuration Utility

You can use the NXPCON utility on the management server to change the discovery configuration. For example, you can change the scope of discovery or view the status of the initial discovery process.

To access the NXPCON utility:

1. Access the server console on the management server either directly from the server prompt or remotely.
2. If the discovery modules are already loaded on the server, click the NetExplorer Console Utility option in the Available Screens window.

   or

   If the discovery modules are not loaded, enter **`netxplor`** at the server prompt.

NXPCON is loaded automatically when NetExplorer is loaded and is accessible at the management server.

If NXPCON is not loaded on your management server, check to see if NetExplorer is running. If NetExplorer is running, enter **`load nxpcon`** at the system console prompt. If NetExplorer is not running, enter **`netxplor`** at the system console prompt.

Choosing Which Discovery Modules to Load

By default, the ZfS installation loads the NXPCON utility with all modules running. If you are not using IPX on your network, you can configure NXPCON to not load the NXIPX module.

IMPORTANT: Make sure TCP/IP is bound to at least one of your server’s network boards.

To view or modify which modules are being loaded:

1. In NXPCON, click Configuration Options > NetExplorer Modules.
2. Select the field you want to change > press Enter.
3. Select Yes or No to load or unload the module > press Enter.
4. Press Esc to exit the NetExplorer Modules dialog box.

5 Click Yes.

You can enable IP host discovery or file-based discovery. To enable or disable:

5a Select Configuration Options > IP Discovery.

5b Select IP Host Discovery or File Based Discovery > Press Enter > Press Yes to enable or press No to disable the discovery option.

6 At the management server prompt, unload NetExplorer by entering **`unxp`**.

7 Reload the NetExplorer modules by entering **`netxplor`**.

Changing the SNMP Community String

In ZfS, the default community string is PUBLIC. If your organization's SNMP community string is not PUBLIC, reconfigure the SNMP community string in NXPCON.

NOTE: In order to prevent burdening the routers, some organizations add one more level of control by allowing only certain IP addresses to do SNMP queries to the routers. If this is true in your organization, make sure that the IP address given to the ZFS sever is privileged to query the routers in the network. Otherwise, the discovery will not be complete and incomplete network information will appear under "Islands" in the atlas.

To view, add, modify, or delete SNMP configuration information, such as community strings used for IP and IPX discovery:

1 In NXPCON, click Configuration Options > SNMP.

2 In the SNMP dialog box, click Edit Community Name List.

3 To add a community string, press Insert.

or

To modify a community string, click the community string > press Enter.

or

To delete a community string, click the community string > press Delete.

4 Press Esc > click Activate Changes from the Configuration Options window.

5 Respond to the prompts accordingly.

For information about other configuration options in the SNMP window, see "Using the Discovery Configuration Utility" on page 111, or ConsoleOne online help.

Changing the Discovery Scope

By default, NXPCON is set to discover all IPX and IP networks. You can, however, limit the discovery scope.

You could, for example, limit discovery to discover the IPX addresses or the IP subnet addresses. If you are managing a large network, by setting the scope of discovery, you will be limiting the discovery to a section of your network, which will reduce the network traffic and in turn make your atlas more manageable

If you do not accurately specify the scope of discovery, you will not be able to discover your target device. Therefore it is imperative to specify in the scope, all the devices that are present in the path leading to the target device you want to discover.

For example, consider the following scenario:

Your discovery server D1 is connected to network N1. Router R1 connects network N2 with N1. Assume you need to discover network N2. To do this, the following entries need to be set in the scope:

- Discovery server D1 with subnet mask 255.255.255.255
- Router R1 with subnet mask 255.255.255.255
- Network N2 with its appropriate subnet mask number.

In this scenario, network N2 can be reached from the discovery server through Router R1, and therefore R1 needs to be in the scope even if the user is not interested in the network N1 that R1 is routing.

After initial discovery, until you reset the database, nodes remain in the database even if they have been removed from the network.

Changing the discovery scope does not affect devices that are already in the database due to prior runs of discovery. In particular, devices that were discovered due to a wider scope (or no scope) will not be removed when a restrictive scope is set for later runs of discovery. If it is desired that the atlas shows only those devices that fall in scope, the database needs to be reset to ensure that segments and devices that are out of scope do not appear in atlas. Note that the database being reset would result in loss of data like alarms and alarm disposition unless they are migrated. Alternatively, if the number of such devices which are out of scope is very small, the user can manually delete them from the database using the Database Object Editor.

You can restrict the scope of IP or IPX discovery by entering the IPX network numbers or IP address ranges specified by the mask fields you want to discover. To view of restrict the IP or IPX scope:

1. In NXPCON, from the Configuration Options window, click Discovery Scope.
2. Select IP Discovery Scope or IPX Discovery Scope.
3. Press Enter to view or configure the scope of your discovery.
4. Press Insert to add a new IP or IPX discovery scope entry.

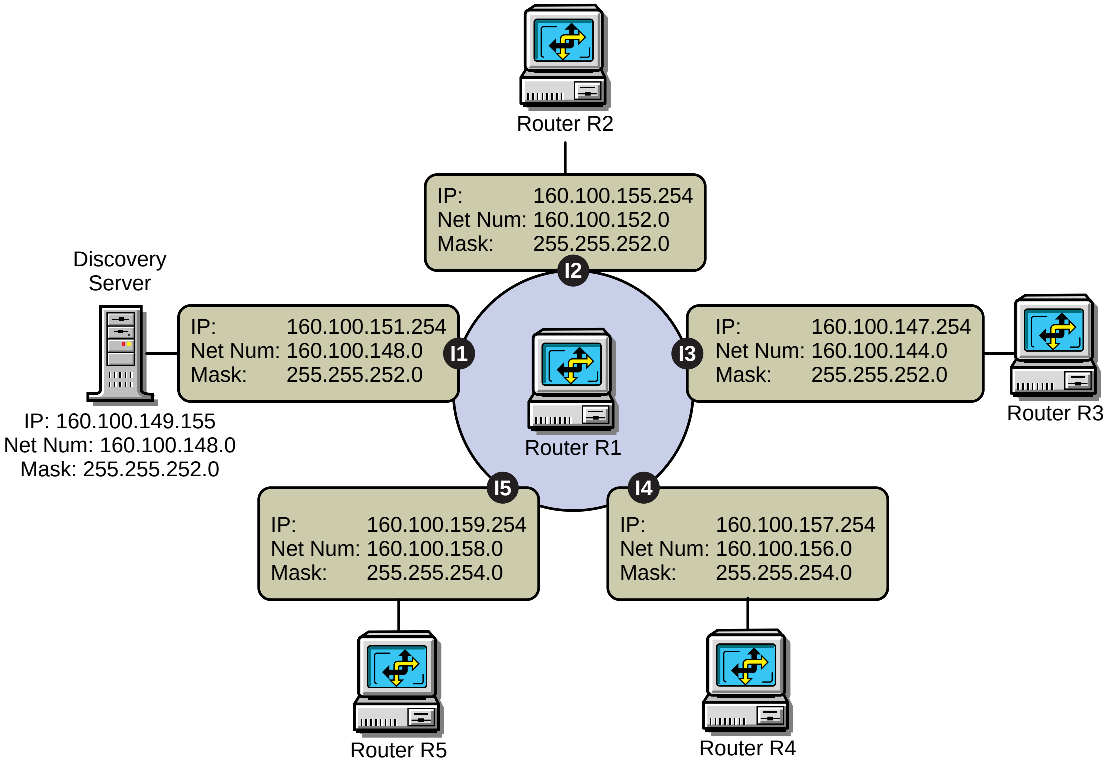
   or

   Press Enter to modify a discovery scope entry.

   or

   Press Delete to delete a discovery scope entry.

   For IP Networks: Discovery scope is tightly bound to the network numbers. The scope can be restricted by specific networks as illustrated in the following diagram.



Case 1: To exclude 160.100.148.0 and discover the other four networks, specify the scope as:

160.100.149.155, 255.255.255.255

160.100.151.254, 255.255.255.255

160.100.144.0, 255.255.252.0

160.100.152.0, 255.255.252.0

160.100.156.0, 255.255.254.0

160.100.158.0, 255.255.254.0

The 255.255.255.255 mask for the ZfS server and the router interface on the local network acts as a machine specific scope. This prevents other machines in the network 160.100.148.0 from being discovered.

Case 2: To discover only the local network 160.100.148.0, specify the scope as:

160.100.148.0, 255.255.252.0

The network 160.100.148.0 (Mask: 255.255.252.0) has IP addresses in the range 160.100.148.1 to 160.100.151.254.

Consider a case where all the important servers in your network have IP addresses in the range 160.100.149.1 to 160.100.149.254. You might specify the following scope:

160.100.149.0,255.255.255.0

The above scope is not allowed by the discovery system. You cannot set a scope to discover only a part of the subnet. You will have to set the entire subnet in scope.

Case 3: To discover only 160.100.156.0 and 160.100.158.0 scope should be given as:

160.100.149.155, 255.255.255.255

160.100.151.254, 255.255.255.255

160.100.156.0, 255.255.254.0

160.100.158.0, 255.255.254.0

Replacing the last two scoping entries with a single entry 160.100.156.0, 255.255.252.0 might not have the same effect.

You cannot create a single scoping entry to cover two or more subnets. You have to create a scope for each subnet.

For IPX Networks: Restrict the scope to the IPX networks to be discovered by entering a single IPX network number and a mask.

The mask indicates which part of the network number needs to match. An F in the mask means that the corresponding digit must match; a 0 (zero) means that no match is required.

For example, network number 12340000 and mask FFFF0000 will match any network number starting with 1234.

Network number C00000FF and mask FF0000FF will match any network number starting with C0 and ending with FF, such as C01234FF or C00000FF.

5. Enter the address and mask for your discovery scope.
6. Press Esc > click Yes to save changes to the configuration file.
7. Press Esc to return to the Discovery Scope window.
8. Unload and reload the NetExplorer modules or restart your management server for the changes to take effect.

Specifying Traffic Analysis Agents to Be Queried by NXPLANZ

Traffic analysis agents in your network are usually discovered by the NXPLANZ module. If SLP is disabled or if SAP packets are filtered by the routers in your network, NXPLANZ might not be able to discover all the Traffic Analysis Agents in the network.

To specify Traffic Analysis Agents to be queried by the NXPLANZ module:

1. In NXPCON, click Configuration Options > NXPLANZ Discovery.
2. To add an agent, press Insert.
3. Enter the address and mask for your discovery scope.
4. Press Esc > click Yes to save changes to the configuration file.
5. Unload and reload the NetExplorer modules or restart your management server.
6. To modify an agent, select the agent > press Enter. Modify the required information.
7. To delete an agent, select the agent > press Delete.

Specifying a Seed Router and Additional IP Routers

Seed router is the router to which ZfS Server is connected. For router discovery to be effective, always specify the seed router using NXPCON and ensure that ZfS server can query the seed router by specifying the proper community name in NXPCON.

You need to specify additional IP routers if you want to discover one part of your network and the ZfS server does not have access to one of the intermediate routers.

To specify a seed router or additional IP Routers:

1. In NXPCON, click Configuration Options > IP Discovery > IP Router Discovery.

   The default for IP Seed Router is <*local*>, which is the ZfS server.

2. To add a seed router, select IP Seed Router and press Enter.
3. Enter the IP address.
4. To add additional routers, select Additional IP Routers and press Enter.
5. Enter the IP address.
6. Press Esc > click Yes to save changes to the configuration file.
7. Unload and reload the NetExplorer modules or restart your management server.

Configuring the Java Processes

The following are the three Java processes of the discovery system:

- Topology Manager
- Bridge Discovery
- SN3 Discovery

These Java processes form a part of the ZfS site server and exist as sections in the SLOADER.PROPERTIES file in the *install_path*\ZENWORKS\MMS\MWSERVER\PROPERTIES directory. They are specified in the following format:

```
[Topology Manager]
Name = Topology Manager
Load Option = auto
Other options
```

To configure the Java processes:

1. Change the value of the Load Option from Auto to Manual to prevent the process from starting the next time you type the SLOADER command on the server.

   IMPORTANT: If you modify the SLOADER.PROPERTIES file after you start the ZfS Site server, you must restart the ZfS Site server for the changes to take effect.

2. Do not change the Load Properties and the Load Sequence options in the SLOADER.PROPERTIES file. These options are necessary for the ZfS site server to work correctly.

Customizing Starting and Stopping Discovery

You can choose to stop or start the discovery NLM files or the Java discovery processes without affecting the other services of the site server, such as the Alarm Manager Service.

Stopping and Starting the Discovery NLM Files

To stop the discovery NLM files, enter **`UNXP`** at the server console.

To start all the discovery NLM files, enter **`NETXPLOR`** at the server console.

NOTE: You cannot start the Discovery NLM files if the Java processes are running. Stop the Java processes and then type **`NETXPLOR`** at the server console to start all the discovery NLM files.

Stopping and Starting the Java Discovery Services

To stop the discovery NLM files, enter **`STOPDIS`** at the server console.

To start all the discovery NLM files, enter **`STARTDIS`** at the server console.

You can customize starting or stopping any of the Java discovery processes at any point in time. For example, you decided not to run the Bridge discovery initially but decide to run it anyway. In such a scenario, you need not stop all the services and restart them. You can edit the STARTDIS.NCF file in the \ZENWORKS\MMS\MWSERVER\BIN directory, which has the following contents:

```
MWSETENV.NCF

java -Xbootclasspath/p:$mwxbpath -classpath
$MMSCP;$CLASSPATHcom.novell.utility.servicemanager.ui.Start
"Topology Manager" "Bridge Discovery" "SN3 Discovery" <ip
address of the server> sloader
```

In the above file, the Java discovery process names like SN3 Discovery must match the names of the sections in the SLOADER.PROPERTIES file. By changing just the names in the NCF files, you can create similar NCF files to selectively stop and start the Java discovery services.

For example, if you want to start just the Bridge discovery process:

1. Create a STARTBRI.NCF file with the following contents:

   ```
   MWSETENV.NCF

   java -Xbootclasspath/p:$mwxbpath -classpath
   $MMSCP;$CLASSPATHcom.novell.utility.servicemanager.ui.St
   art "Bridge Discovery" <ip address of the server> sloader
   ```

2. Copy the STARTBRI.NCF file to the \ZENWORKS\MMS\MWSERVER\BIN directory.

3. Run the STARTBRI.NCF file to start the Java discovery bridge service.

For example, to stop the Java discovery process for the SN3 Agent:

1. Create a STOPSN3.NCF file with the following contents:

   ```
   MWSETENV.NCF

   java -Xbootclasspath/p:$mwxbpath -classpath
   $MMSCP;$CLASSPATHcom.novell.utility.servicemanager.ui.St
   op "SN3 Discovery" <ip address of the server> sloader.
   ```

Unloading the Management Server

To unload the management server:

1. If restarting the server is not feasible, make sure all ServiceLoader processes are exited. At the server console prompt, enter

   ```
   stopService.ncf
   ```

   ```
   java -show
   ```

   HINT: You may sometimes see a process displaying the status "exiting" in the java -show display. If this condition persists, restart the server.

   You can use **`java -exit`** if you can terminate all other Java processes. Unload Java, if all the services are not closed.

2. Enter **`unmw`** to unload all ZfS components.

3. Switch to the Sybase* process by pressing Ctrl+Esc > enter **`q`** to terminate the Sybase database engine.

Managing the Atlas

After the initial discovery, you can stop discovery running on the management server. You can, however, continue to access the database through the Atlas Manager. The discovery cycle starts again the next time NetExplorer is up. The Consolidator populates the database and the Atlas Manager automatically updates the atlas pages.

Depending on the size of your network, writing data from the initial discovery cycle can take few minutes to several days. Subsequent discovery updates to the database require substantially less time.

- "Using the Atlas" on page 120
- "Using Unified Views" on page 123

Using the Atlas

When ZfS is first installed, the server module of the Atlas Manager is automatically installed on the management server, and the client module of the Atlas Manager is installed on ConsoleOne. The Atlas Manager on the management server creates a system atlas and provides a graphical view of the database at the console.

The Atlas Manager on the server reads the database and provides two different views of the database at ConsoleOne: the Console view and Atlas view. Both views provide information about the discovered network topology, the physical location of nodes, node configuration information, and alarm information.

The following sections gives you an understanding about using the atlas:

- "Accessing the Atlas" on page 120
- "Assigning Roles to Help You Manage the Atlas" on page 121
- "Using the Atlas to Troubleshoot" on page 122

Accessing the Atlas

You can access the ZfS atlas from ConsoleOne. Open ConsoleOne and double-click the ZfS Domains namespace, then expand the domain. The system atlas appears.

The following table describes a ZfS atlas consisting of three different pages:

Atlas Pages	Icon	Description
WAN page		Summarizes the entire network, illustrating the WAN-related network topology. Your atlas, typically, has a single WAN page.
Area page		Displays segments on your network. An atlas can have several area pages. For example, areas can be divided based on the geographic location of the network. If a company in San Jose has an overseas branch in Germany, you can divide your network into Area1 for the San Jose network and Area2 for the Germany network.
Islands page		Consists of segments with an undetermined connectivity. During discovery, the Islands page is a placeholder for network objects that are not completely discovered. An atlas has a single Islands page.

Customizing Your Atlas View

You can customize your atlas view in four different ways:

- Insert a custom bitmap as the background on an atlas page.
- Change the position of a node on an atlas page by dragging it.
- Display objects by an alternate name.

Assigning Roles to Help You Manage the Atlas

ZfS lets you assign roles to manage the atlas. By assigning roles, you can restrict the user from performing specific operations on that object.

HINT: The atlas displays maps based on your role on the network. For example, if your role is restricted to managing certain servers in segment A and B, your atlas will contain only those servers in segments A and B.

You can perform the following tasks on any atlas page (WAN, Islands, or Area page) when the Atlas view is displayed on ConsoleOne.

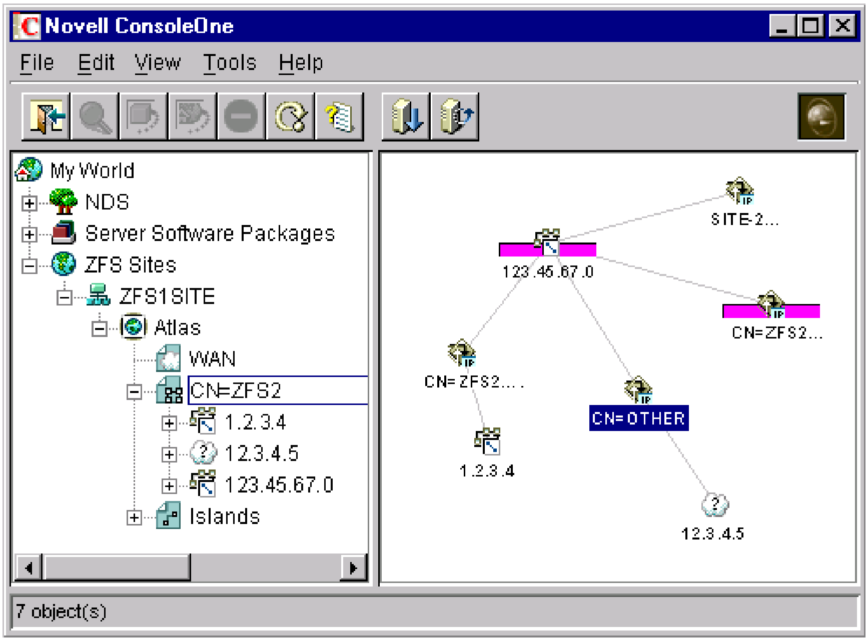
Tasks	Comments
Open	Opens the page
Import	Inserts a custom wallpaper

Tasks	Comments
Save	Updates the changes in the database
Print	Prints the page
Rename	Renames the page
Layout	Displays the page with a different focal point

Using the Atlas to Troubleshoot

By setting the alarm disposition to save alarms in the database, ZfS maps can alert you to alarm conditions on the network. Alarms are of type severe, major, or minor alarm on a segment or node. Upon recognizing any of these alarms, the ZfS ConsoleOne displays a bell-shaped alarm icon above the object. The alarm status is propagated up the hierarchy. For example, if a server has an alarm of type severe, the segment and the page containing the server will display the corresponding alarm icon. For information about alarms, "Managing the Alarm Management System" on page 132.

The following figure shows the atlas namespace in ConsoleOne:



7 object(s)

Using Unified Views

The Unified view service is a service that acts as a filter on the atlas. Using the Unified view, you can filter for a list of devices or segments of a particular type. The Unified view allows easy navigation and quick operations to check the highest severity of the alarms present on a particular node or segment.

The following are the two types of Unified view provided:

- "Unified View for Devices" on page 123
- "Unified View for Segments" on page 124

Unified View for Devices

You can view All, Manageable, or Unmanageable devices in this view. For a corresponding device type, a device is said to be manageable if the list of MIBs implemented by the device satisfies the Manageability_definition property in the UnifiedView.ini file in the ZENWORKS\MMS\MWSERVER\BIN directory. The Manageability_definition property can be updated with a valid boolean expression of MIB names.

Following are the device types that you can filter:

- All (all types of devices)
- Netware Servers
- NCP Print Servers
- TCP Services
- Printers
- IP Routers
- Switches/Bridges
- IPX Routers
- Windows NT Servers

To filter the devices:

1. In the atlas, select View > Unified View for Devices.
2. From the first drop-down list, select All to list all the devices

   or

   Select Manageable to list the manageable devices or

Select Unmanageable to list the unmanageable devices.

3. From the second drop-down list, select a device type.
4. Click Show.

The Unified view will display the list of the devices. The tabular column in the Unified view contains the following information.

- The icons associated with the devices.
- The MIBs implemented by the device. If the device does not implement any MIBs the column will specify "No MIBs implemented" for that device.
- The maximum severity of the alarms against the devices. To view the legend for the alarm, select the alarm legend button on the toolbar.

Unified View for Segments

You can view All, Manageable, or Unmanageable segments in this view. For a corresponding segment type, a segment is said to be manageable if the list of MIBs implemented by at least one device in that segment satisfies the Manageability_definition property in the UnifiedView.ini file. The Manageability_definition property can be updated with a valid boolean expression of MIB names. The following are the segment types you can set filter for:

- All (all types of segments)
- Ethernet
- Frame Relay
- IPX Compatibility Mode
- Token Ring
- X.25
- PPP
- ATM
- FDDI

To filter the segments:

1. At the Atlas level, select View > Unified View for Segments.

2. From the first drop-down list, select All to list all the segments

   or

   Select Manageable to list the manageable segments

   or

   Select Unmanageable to list the unmanageable segments.
3. From the second drop-down list, select a segment type.
4. Click Show.

The Unified view will display the list of the segments. The tabular column in the Unified view contains the following information.

- The icons associated with the segments.
- The name of the segment.
- The maximum severity of the alarms against the segments. To view the legend for the alarm, select the alarm legend button on the toolbar.

4 Understanding Alarm Management

The ZENworks® for Servers (ZfS) Alarm Management System (AMS) alerts you to important events like the SNMP traps, threshold alarms, network discovery events, and ping and connectivity testing faults occurring on your network. This lets you proactively resolve network problems and receive updates on events occurring on your network.

Alarm icons are anchored to objects displayed in ConsoleOne®. The icons change color to depict the level of severity, notifying you of potential problems. The events are reported in the Active Alarm view, and each event is categorized and displayed with a corresponding alarm icon.

AMS will process any device on the network that supports SNMP-standard trap notification. For example, for all NetWare® servers on which the Management Agent for NetWare is installed, notifications of server breakdowns, overloads, and configuration changes are sent to the management server for processing and then made available for viewing at a ZfS ConsoleOne.

You can enable and disable alarms and set alarm thresholds on baseline statistics for segments and servers (for example, segment alarms for utilization and the total number of packets per second), so that an alarm is generated when the threshold for a statistic is reached. You can also set actions to be performed when an alarm or an event occurs. The actions assigned to an alarm or event are specified in the alarm disposition.

This section contains the following topics:

- "Understanding the Alarm Management System" on page 128
- "Managing the Alarm Management System" on page 132
- "Maintaining the Alarm Management System" on page 154
- "Troubleshooting the Alarm Management System" on page 154

Understanding the Alarm Management System

AMS alerts you to network conditions and events. AMS provides you with tools and back-end services to use, distribute, and manage this information. The AMS component is also fully integrated with other ZfS components. It provides access control through the role-based services (RBS) component and report generation through the reporting functions. AMS provides a centralized location for processing and viewing the events and alarms generated by devices and systems throughout your network.

You can view tabular lists of statistical data for active and historical alarms received by AMS from ConsoleOne. This makes it easy to handle alarms and track network events and recurring alarm conditions. In addition, real-time notification of alarms occurring on your network is provided by the following

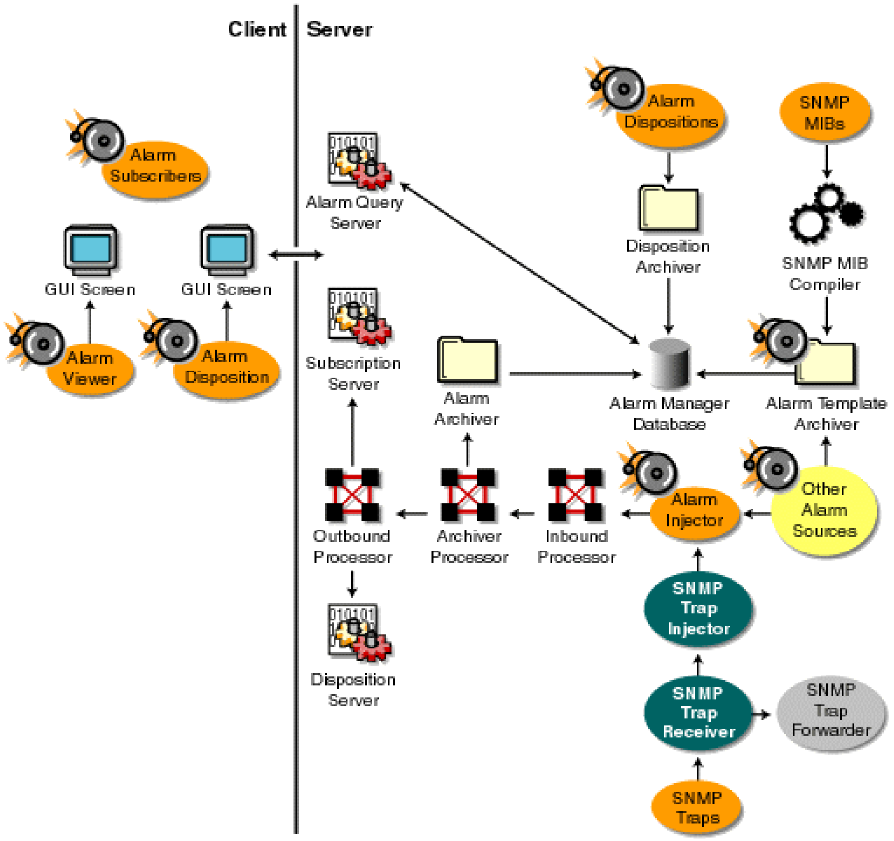
- Severity level, as displayed by the changing color of the alarm indicators
- Audible notification
- Status bar ticker-tape messages

You can also assign an action, such as automatically launching a program when an alarm is received, or sending an e-mail message to notify remote users of events.

Alarm Management System Components

AMS comprised of multiple components for processing, storing, and viewing alarms. All alarms received by AMS are processed and sent to applications that subscribe to them. The ZfS ConsoleOne, by default, subscribes to AMS and receives updates when an alarm is processed. Hierarchical Status Notification (HSN) also subscribes to AMS and changes the color of the atlas map icon accordingly.

The following figure illustrates the AMS components:



The main components that make up AMS are as follows:

- "SNMP Trap Receiver" on page 130
- "SNMP Trap Forwarder" on page 130
- "SNMP Trap Injector" on page 130
- "Alarm Injector" on page 130
- "Alarm Processors" on page 130
- "Alarm Manager Database" on page 130
- "Archivers" on page 131
- "Alarm Viewers" on page 132

SNMP Trap Receiver

SNMP receives traps from network management agents and passes them to the SNMP trap forwarder and the SNMP trap injector.

SNMP Trap Forwarder

After the SNMP trap forwarder receives a trap, it checks the alarm manager database to determine whether the trap has an SNMP trap forwarding disposition. If the trap has a forwarding disposition, the SNMP trap forwarder forwards the trap. Otherwise, the SNMP trap forwarder ignores the trap.

SNMP Trap Injector

The SNMP trap injector converts the trap to an alarm and passes the alarm to the alarm injector.

Alarm Injector

The alarm injector receives alarms from the SNMP trap injector and other applications and passes them to the inbound processor.

Alarm Processors

The alarm processors includes processes for receiving, archiving, and dispatching alarms to subscribers. The inbound processor applies alarm templates to incoming alarms. After inbound processing is completed, the alarm is sent to the archive processor, which facilitates logging and storing of the processed alarm data in the alarm manager database. The archive processor sends the alarm to the outbound processor, which in turn sends the alarms to the subscription server and disposition server.

Alarm Manager Database

The alarm manager database, a repository for alarm information, includes the following:

- "Processed Alarms" on page 131
- "Alarm Templates" on page 131
- "Alarm Dispositions" on page 131

Processed Alarms

The processed alarm data that is stored in the alarm manager database is supplied to ConsoleOne through the alarm query server. The alarm data is used for alarm and alarm summary presentation and reporting.

Alarm Templates

Templates are applied to each alarm received by the inbound processor.The alarm template is based on SNMP trap definitions in the MIB or other proprietary definitions for handling the AMS management and display criteria. When you compile an MIB, the trap definitions are used to create an alarm template that provides a method for presenting and managing alarm data. Proprietary alarms templates are based on proprietary definitions. For example, when a user tries to log in to a server with an incorrect password, an alarm is generated and forwarded to the management server. The management server processes the alarm by identifying the trap object identifier (OID) and assigns the associated alarm template.

A default template is assigned to an SNMP trap sent by a device that does not have a recognizable OID and is categorized as unknown. In order for a trap OID to be recognized by AMS, you need to compile the MIB of the device into the MIB Pool on the management server. For more information, see Installing and Setting Up Management and Monitoring Services in the *Installation* guide.

Alarm Dispositions

Alarm dispositions govern the handling characteristics for each type of SNMP trap or proprietary alarm. AMS allows you to configure the automatic handling of an alarm by defining it in the alarm disposition. The automatic handling functions include specifying an application to launch when an alarm is received, sending e-mail notification, forwarding processed alarms to other ZfS management servers, and forwarding SNMP traps to other network management systems. You can also set options for alarms, such as audible beeps.

Archivers

The following three archivers add data to the alarm manager database:

- "Alarm Archiver" on page 132
- "Disposition Archiver" on page 132
- "Template Archiver" on page 132

Alarm Archiver

The alarm archiver stores alarm statistics and data in the alarm database. By default, all alarms are archived. If you do not want an alarm archived, you can edit the alarm disposition to disable archiving of the alarm. See "Archiving Alarm Statistics" on page 152 for more information.

Disposition Archiver

The disposition archiver receives the alarm disposition from the Disposition Console and saves it in the alarm manager database.

Template Archiver

The template archiver receives alarm templates from a MIB compiler and saves them in the alarm manager database.

Alarm Viewers

ConsoleOne displays three views of alarm data: the Active Alarm view and the Historical Alarm view and the Alarm Summary view.

The Active Alarm view displays statistics in ConsoleOne for events occurring on your network. Alarms displayed in the Active Alarm view can either be owned by you or assigned to a group. The tasks that you can perform on an alarm from this view depend on the access rights allowed through the role-based services. The Active Alarm view continually appends incoming alarms to the list, providing you with the most recent alarms. Once an alarm is handled, it is removed from the Active Alarm list.

The Alarm History view displays information about assignments and ownership of alarms. You can track alarms received by AMS and verify their handling status from this view.

The Alarm Summary view is a graphical representation of all the alarms that you have received.

Managing the Alarm Management System

The ZfS ConsoleOne provides a central location for monitoring, managing, and controlling critical events on your network. You can configure AMS to alert you to errors on critical systems and events to assist you in maintaining your network. This section contains the following information:

Recognizing Alarm Indicators

You can monitor the network for alarm-triggering events by observing nodes on topology maps or Atlas views, Active Alarm, and Alarm History views and in the server/node summary. The following table lists the alarm indicators and the type of alarm they are associated with.

Alarm Indicator	Applies To
Alarm icons anchored to the affected object	Alarms with severe, major, and minor severity are displayed in the Atlas and Console views and the left pane of ConsoleOne. An alarm icon remains anchored to a segment or device object until you handle all alarms outstanding against that object. Alarm icons differ based on the severity level of the alarm. See “Interpreting Alarms” on page 136 for details on alarm severity and the associated icons. Keep in mind that if a segment or device has multiple alarms logged against it, the alarm icon always depicts the highest level of severity.
Ticker-tape message on the status bar	AMS can automatically display alarm messages on the status bar. By default, this option is enabled. You can configure each individual alarm disposition to disable display of the ticker-tape message. Upon recognizing an alarm-triggering event, AMS displays a message in the status bar describing the alarm. For information on setting this option, see “Displaying a Ticker-Tape Message” on page 151.

Alarm Indicator	Applies To
Audible beep	AMS can be configured to produce an audible beep on ConsoleOne when an alarm occurs. By default, this option is disabled. You can configure each individual alarm disposition to enable the audible notification. For information on setting this option, see "Making an Audible Beep" on page 152.

Viewing Alarms

You can access active and historical alarm data from any ConsoleOne location. As an administrator, you can define access restrictions to alarm data and management functions through the role-based services to further define the data presented based on the roles in your organization.

You can modify the presentation of the alarm data displayed in the Active Alarms and Alarm History view by filtering the displayed data, changing the column layout, and changing the sorting order. All options for changing the presentation are under the View menu in ConsoleOne.

The following sections describes the different ways you can view and use alarms:

- "Viewing Active Alarms" on page 134
- "Viewing Historical Alarms" on page 135
- "Viewing the Alarm Summary" on page 135
- "Interpreting Alarms" on page 136
- "Sorting Alarms" on page 137
- "Filtering Alarms" on page 138

Viewing Active Alarms

The ZfS ConsoleOne Active Alarm view displays alarm statistics for all current alarms received from segments or devices, per management domain. The Summary view shows a list of all active alarms for that server or node.

The Active Alarms view and Server Summary view display a table of detailed information about active alarms. These views are updated whenever a new alarm occurs and is archived on your network. New alarms are appended to the list.

To display the Active Alarm view:

1. Click the ZENworks for Servers site object in the left frame of ConsoleOne.
2. Click View > Active Alarms.

   The Active Alarm view is displayed. You can perform the following activities from this view:

   - "Assigning Alarms" on page 141
   - "Owning Alarms" on page 142
   - "Handling Alarms" on page 142
   - "Adding Notes to Alarms" on page 142

Viewing Historical Alarms

The Alarm History view displays information about all archived alarms, including the handling status of each alarm. You can access the Alarm History view only if you have been granted access through the role-based services.

To display the Alarm History view:

1. Click the ZENworks for Servers site object in the left frame of ConsoleOne.
2. Click View > Alarm History.

   The Active Alarm view is displayed. You can perform the following alarm handling activities from this view:

   - "Assigning Alarms" on page 141
   - "Owning Alarms" on page 142
   - "Deleting Alarms" on page 143
   - "Adding Notes to Alarms" on page 142

Viewing the Alarm Summary

The Alarm Summary is a graphical representation of the summary of alarms you have received. The view is divided into three panels of representation: pie chart panel, bar graph panel, and trend panel. You can choose to view the information in these panels for a given period of time. The time duration ranges for the hour, for the day, for the week, and for the month.

- The pie chart panel includes alarm distribution based on severity, category, owner and alarm state
- The bar graph panel includes the Top N Alarm types, Top N Source Address and Top N Affected Node. The value of N is configurable.
- The trend displays the rate at which the alarms are received.

You can customize the pie chart and the bar graph representations to reflect the customized data.

To display the Alarm Summary view:

1 Click the ZENworks for Servers site object in the left frame of ConsoleOne.

2 Click View > Alarm Summary.

The Alarm Summary view displayed.

To customize the pie chart and the bar graph representation:

2a Click the Customize button on the Alarm Summary view.

The Customize Summary view dialog box is displayed.

By default, all the options in this dialog box are selected. However, you can select the required options to customize the view.

Interpreting Alarms

The Active Alarm and Alarm History views display lists of alarms that have been archived in the alarm manager database. The alarms are displayed as a tabular list. The following table describes the data type and contents:

Data Type (Column)	Contents
Severity	Alarm icon that indicates the severity level attributed to the trap. The color of the alarm icon indicates the level of alarm severity, as follows: ● Red = Severe ● Magenta = Major ● Yellow = Minor ● Blue = Informational ● White = Unknown
From	Network address of the device that sent the alarm to AMS.
Summary	Summary of the event, often including the name or address of the object affected by the alarm.
Owner	Person or group responsible for handling the alarm. The default owner is SYSTEM.
Received Time	Date and time when the AMS received the alarm.
Type	Generic description of the alarm. For example, volume out of disk space.
Category	Category identified in the MIB associated with the trap-type object.

You can filter the data displayed in the alarm views based on criteria from statistics displayed in each view; see “Filtering Alarms” on page 138 for details. After selecting one or more alarm entries in an alarm view, you can perform operations by right-clicking them.

Sorting Alarms

You can modify the order in which the alarms are displayed on the Active Alarm or Alarm History views by sorting the alarms. By default, the alarms are sorted in ascending order by received time.

To edit the sort settings:

1. Click View > Settings > Sort.
2. Select the criteria by which you want the alarms sorted. You can sort by
   - Type
   - Severity
   - Category
   - Received time
   - Summary
   - Owner
   - Affected Object
3. Indicate whether you want the alarms sorted in ascending (oldest first) or descending (the most recent alarms first) order by selecting the appropriate radio button from the Sort Order box.
4. Click OK.

   The alarms are now sorted according to the criteria you specified.

Filtering Alarms

You can display the alarms in a tabular view based on filter conditions. The filter applies only to the current management session and clears when you ConsoleOne.

You set up a filter by selecting criteria from four drop-down lists. You can either set up simple filters that require only one line, or complex filters composed of multiple lines or groups of lines. If you set up a filter using more than one line, you must also specify the logical relationship between the line and/or group of lines.

To set up a filter:

1. Go to the view you want to filter.
2. Click View > Settings > Filter.

   The Alarm Filter dialog box is displayed.
3. Select the column by which you want AMS to filter alarms from the first drop-down list. You can filter alarms using the following columns:

- **Severity:** Filters the alarms based on the alarm severity. Alarm severity is assigned to an alarm type.
- **Type:** Filters alarms based on the alarm type. The alarm type is set by the SNMP trap-type defined in the MIB or the proprietary alarm definition.
- **Category:** Filters alarms based on the category of the alarm. Alarm categories are based on the MIB that defines the trap-type objects.
- **Generator Type:** Filters alarms based on the type of agent or system generating the alarms.

4. Select an operator from the second drop-down list.

   The operator defines how to constrain the column you have selected to a value. For example, you can specify that the selected category must be equal to, not equal to, greater than, less than, greater than or equal to, less than or equal to, contain, or start with the value you select in the third drop-down list in order for an alarm to be displayed. Keep in mind that the list of available operators depends on what column you've selected.

5. Select a value from the third drop-down list.
6. Specify how this filter statement relates to other statements you plan to define by selecting a value from the fourth drop-down list.

   - If this is the only filter statement or if it is the last statement in a group, select End.
   - If you want to add a line below the current filter statement, select New Row. A new line is added. You must define the logical relationship between the previous line and the new line. The alarms will be displayed based on the logical condition you have specified. Select And to satisfy both the filter conditions. Select Or to satisfy any one of the filter conditions for the alarm to be displayed.
   - If you want to add one or more lines that are unrelated to the preceding lines, select New Group. A new line is added. An additional drop-down list separates the new line from the preceding lines. Select a value from this drop-down list to indicate the relations between the filter statements. Select And if you want both the filter statements to be satisfied. Select Or if you want only one of the filter statements in one of the groups to be satisfied. Select End from the fourth drop-down list when you add a new group.

7. Click OK if you have defined filters.

The alarm list is updated to display only those alarms that meet the filter criteria you defined.

Enabling and Disabling Alarms

ZfS provides default threshold values for managed NetWare and Windows* NT* servers and network segments hosting the Traffic Analysis Agents for a station connected to a segment. An alarm is generated if the values exceed the threshold values. The server threshold alarms are enabled by default while the segment threshold alarms are not. You will need to enable threshold alarms to receive.

IMPORTANT: In order to modify the segment properties, you must have the Traffic Analysis Agents for NetWare or Windows NT hosted on a station, connected to the segment.

To enable or disable segment threshold alarms:

1. Right-click the segment object > click Properties.
2. If it is not already displayed, select the Segment Alarms tab.
3. Select the alarm you want to enable or disable > click Edit.
4. In the Value field, enter the threshold value after which an alarm should be generated.
5. Enter the time (in seconds) that the threshold value must exceed in order to generate an alarm in the Sampling Interval field.
6. Check the Enable check box.
7. Click OK.

Resolving Alarms

Alarms that occur on segments and devices on your network are added to the alarm manager database and are presented in the Active Alarms and Alarm History views. Entries in the alarm manager database remain in the database until the alarm is deleted. The database records the status of the alarm from first acknowledging the alarm, assigning it to a group or user, owning the alarm, and finally deleting it from the database once the owner has resolved the problem.

Resolution operations for alarms are displayed when you right-click a single entry or multiple entries in an alarm view and click any of the following actions:

- “Assigning Alarms” on page 141
- “Owning Alarms” on page 142
- “Handling Alarms” on page 142
- “Adding Notes to Alarms” on page 142
- “Jump to the Affected Node” on page 143

You can also access the alarm action menu items from the View menu in ConsoleOne.

The order in which you perform the handling, assigning, and owning of an alarm or multiple alarms depends on your organization. Keep in mind that after you handle an alarm, it is removed from the Active Alarms list and only appears in the Alarm History list. A suggested course for resolving an alarm is for you to first assign the alarm to a group or team member, then have someone from the group take ownership of the alarm. When the network problem or event has been resolved, the team member can handle the alarm to remove it from the Active Alarms list. By following this process, you can track the alarm status through resolution, and finally delete the alarm from the Alarm History list.

Assigning Alarms

You can specify the group or user that is assigned to handle an alarm. This allows you to use any team assignments you already have within your organization. For example, you may have a group or team member assigned to handle all alarms relating to NetWare servers. You can assign one or more alarms to a group or user. Note, however, that you must have been granted access to assign alarms through the role-based services. You can use an alarm filter to help you determine groups based on certain filtering criteria. See “Filtering Alarms” on page 138 for information on filtering options.

HINT: This is optional and is provided for tracking the status of alarm resolution.

To assign an alarm:

1. Select the alarm you want to assign from the Active Alarm or Alarm History list.
2. Click View > Assign.
3. Enter the name of the person or group to which you want to assign the alarm in the User Name field.

   The name you enter does not correlate to users in eDirectory and can represent the organization structure you already have in place.
4. Click OK.

Owning Alarms

A user can take ownership of one or more alarms. If a user is a member of a group assigned to resolve a network problem, the team member can take ownership of the alarm and finally delete the alarm to remove it from the alarm manager database.

HINT: This is optional and is provided for tracking the status of alarm resolution.

To take ownership of an alarm:

1. Select the alarm from the Active Alarm or Alarm History view.
2. Click View > Own.

   The value in the Owner field changes to the eDirectory name you are logged in as. Note that you cannot customize this option; the user logged in to ConsoleOne will always become the owner of the alarm when this action is used.

Handling Alarms

Alarms displayed in the Active Alarm view have not been handled by anyone. After the alarm is handled, it is removed from the Active Alarm list, and any alarm indicators shown in other views in ConsoleOne are removed. See "Recognizing Alarm Indicators" on page 133 for information on different types of alarm indicators. Note that the alarm is still displayed in the Alarm History view.

To handle an alarm:

1. Select the alarm from the Active Alarm list.
2. Click View > Handle.

   The alarm is removed from the Active Alarm list. You can still display information about the alarm by switching to the Alarm History view.

Adding Notes to Alarms

You can add a note to any of the alarms displayed in the Active Alarm view or Alarm History view. The note can contain any relevant useful information about the alarm.

To handle an alarm:

1. Select the alarm from the Active Alarm or Alarm History.
2. Click View > Note.

The Note dialog box is displayed.

Create a note for the alarm.

3. Click OK.

   The alarm icon will now have a note icon associated with it, indicating that a note has been added to the alarm.

   If you want to delete the note from the alarm, repeat step 2. Delete the note that you created in the Note dialog box.

   Click Apply. The note will be deleted for the alarm, and the note icon will not be displayed.

Jump to the Affected Node

You can jump to the affected node where the alarm has been triggered and perform the necessary action to rectify the affected node.

To jump to the affected node alarm:

1. Select the alarm from the Active Alarm or Alarm History.
2. Click View > Jump to Affected Node.

   The Console view is displayed and the node on which the alarm has triggered is highlighted.

Deleting Alarms

Alarms displayed in the Alarm History view can be deleted from the alarm list after problem resolution. You can delete one or more alarm entries to remove the alarm from the list. Note that to delete an alarm, you must have been granted access to view alarm history and to delete alarms through the role-based services.

There are two ways to delete alarms:

- You can delete alarms manually from the Alarm History view. See "Deleting Alarms from ConsoleOne" on page 144.
- You can delete alarms automatically using the AMS purge utility. See "Deleting Alarms Using the Purge Utility" on page 144.

IMPORTANT: The alarm manager database, located on the management server, records the status of every alarm instance received by the AMS. You must be diligent in deleting alarms after a problem is resolved in order to keep the database from taking up excessive disk space. Currently, the alarm manager database uses the Alarm purge utility (on by default) to automatically delete entries after a period of time or based on the size of the database.

Deleting Alarms from ConsoleOne

You can manually delete alarms from ConsoleOne.

To delete alarms:

1. Select the alarms you want to delete from the Alarm History list.
2. Click View > Delete.

   The alarms are removed from the Alarm History view.

Deleting Alarms Using the Purge Utility

You can delete alarms automatically using the AMS purge utility. Before you can use this utility, you must set up the utility's configuration file, AMPURGE.PROPERTIES, which is located in the properties directory on the server and volume where you installed the alarm manager database. Then you can schedule the utility to run automatically at a specified time of day. Or, you can run the utility manually from the server console. The following sections describe how to set up and use the AMS purge utility:

- "Setting Up the Purge Utility Configuration File" on page 144
- "Setting Up the Purge Utility to Run Automatically" on page 145

Setting Up the Purge Utility Configuration File

The AMS purge utility configuration file, AMPURGE.PROPERTIES, defines the criteria for selecting the alarms to be purged as well as the time of day the process should run. This file is located in the properties directory on the server and volume where you installed the alarm manager database.

Before you can run the purge utility, you must set up the configuration file as follows:

1. Open the AMPURGE.PROPERTIES file with a text editor.
2. Set the criteria for purging alarms by editing the values of the following lines in the file:
   - `SeverityInformationalPurgeWait`: The number of days before informational alarms will be purged.
   - `SeverityMinorPurgeWait`: The number of days before minor alarms will be purged.
   - `SeverityMajorPurgeWait`: The number of days before major alarms will be purged.

- `SeverityCriticalPurgeWait`: The number of days before critical alarms will be purged.
- `SeverityUnknownPurgeWait`: The number of days before unknown alarms will be purged.

   By default, alarms of all severity levels are purged after seven days.

3. Save the configuration file.

Setting Up the Purge Utility to Run Automatically

You can schedule the purge utility to run daily to ensure that the alarm manager database does not consume excessive disk space. Before you can set up the utility to run automatically, you must make sure to set up the file with your preferences for deleting alarms of various severities. See "Setting Up the Purge Utility Configuration File" on page 144.

To set up the utility to run automatically:

1. Open the AMPURGE.PROPERTIES file with a text editor.
2. Set the time of day you want the utility to run by editing the `PurgeStartTime` entry.

   Valid values are 0 to 23, where 0 is midnight and 23 is 11:00 p.m. Keep in mind that the purge utility is memory intensive and can occupy the server for several minutes. Therefore, you should set the utility to run during off-peak hours.
3. Save and close the file.
4. Open the ALARMMANAGER.PROPERTIES file and verify that the following line exists:

   AlarmPurgeService=yes

   If the line does not exist, add it to the end of the file.
5. Save and close the file.
6. Restart the server.

Performing Actions on Alarms

You can configure an alarm to automatically perform an action when an alarm occurs. You do this by editing the alarm dispositions associated with each alarm template. Alarm dispositions are created for each alarm template in the

Alarm Manager database and default settings are assigned. You can edit the alarm dispositions to enable the following actions:

- "Sending SMTP Mail Notification" on page 146
- "Launching an External Program" on page 148
- "Forwarding SNMP Traps to Other Management Systems" on page 150
- "Forwarding Alarms to Other Management Servers" on page 150
- "Displaying a Ticker-Tape Message" on page 151
- "Making an Audible Beep" on page 152
- "Archiving Alarm Statistics" on page 152
- "Sorting Alarm Templates" on page 153

Sending SMTP Mail Notification

You can send SMTP messages to recipients who are specified to receive e-mail notification.

To modify alarm disposition to automatically send SMTP mail notification:

1. Right-click the ZENworks for Servers site object in the left frame of ConsoleOne > click Properties.
2. Click the Alarm Disposition tab.
3. Select the alarms you want to edit from the Alarm Templates list > click Edit.

   The Edit Alarm Disposition dialog box is displayed.
4. Click the SMTP Mail Notification tab.
5. Check the Notify through SMTP Mail check box.
6. Enter the IP address of the SMTP host server that handles incoming and outgoing e-mail in the SMTP Host field.
7. Enter the name of the person sending the notification in the From field.
8. Enter the e-mail addresses of the recipients in the To field.
9. Enter the subject of the e-mail in the Subject field.
10. Enter a message for the e-mail, if any, in the Message field.
11. Click OK.

Note that the subject and message text strings can contain any of the variables listed in the following table. These variables allow you to add details to your message about the segment or device generating the fault or event. All variables must be preceded by a percent sign (%). For example, the subject line could include the %v variable to display the severity of the alarm. You can also specify the width for the variables. %(*nnn*)X can be used to limit the length of the %X value to *nnn* characters. X represents any format specifier. For example, %(10)a will display the Alarm ID up to 10 characters.

Variable Parameter	Name	Description
a	Alarm ID	Identification number of the alarm as it is stored in the database.
c	Affected class	Class of equipment that sent the alarm. This can be any portion of the network and is categorized in the database for indexing.
o	Affected object number	Identification number of the node that generated the alarm as it is stored in the database.
s	Alarm summary string	Message describing the alarm. (This is the same as the status bar ticker-tape message.)
t	Alarm type string	Description of the alarm. This matches the description in the Alarm Type column in the Alarm Summary window.
v	Severity number	Alarm severity can be 1 = severe 2 = major 3 = minor 4 = informational All others are unknown.
n	Affected object name	Identification name of the node affected by the alarm.
p	Source Address	The source address of the agent that generated the alarm.

Variable Parameter	Name	Description
-h	Remove Default Header	Truncates the default header while sending an SMTP message.

Launching an External Program

As part of editing the disposition of an alarm, you can set options to launch any program on the ZfS server automatically when an alarm is received. For example, you might want an alarm to launch a program that sends a message to the system administrator's pager.

In addition to specifying the program to launch, you can also specify arguments and variables to be passed to the program.

Although ZfS provides the capability to launch applications, the product does not supply any predefined programs. However, you can launch an NLM and run scripting routines or use third-party programs.

To set up automatic application launching:

1. Right-click the ZENworks for Servers site object in the left frame of ConsoleOne > click Properties.
2. Click the Alarm Disposition tab.
3. Select the alarm that you want to edit from the Alarm Templates list > click Edit.

   The Edit Alarm Disposition dialog box is displayed.
4. Click the Launching Application tab.
5. Check the Launch Application check box.
6. Enter the path and name of the application in the Application Name field.
7. Enter any necessary execution arguments or script variables in the Argument field > click OK.

   Arguments are passed directly to the program; text is not parsed, but is read as literal text strings. Variables must be preceded with a percent sign (%). The percent sign can be followed by an optional length field that limits the length to which the parameter can expand. You can also specify the width for the variables. %(*nnn*)X can be used to limit the length of the %X value to *nnn* characters. X represents any format specifier. For example, %(10)a will display the Alarm ID up to 10 characters.

The following table lists the variables you can use when launching a program.

Variable	Name	Description
a	Alarm ID	Identification number of the alarm as it is stored in the database.
c	Affected class	Class of equipment that sent the alarm. This can be any portion of the network and is categorized in the database for indexing.
o	Affected object number	Identification number of the node that generated the alarm as it is stored in the database.
s	Alarm summary string	Message describing the alarm. (This is the same as the status bar ticker-tape message.)
t	Alarm type string	Description of the alarm. This matches the description in the Alarm Type column in the Alarm Summary window.
n	Affected object name	Identification name of the node affected by the alarm.
p	Source Address	The source address of the agent that generated the alarm.
v	Severity number	Alarm severity can be 1 = severe 2 = major 3 = minor 4 = informational All others are unknown.

Forwarding SNMP Traps to Other Management Systems

AMS can be configured to forward an unmodified SNMP trap. Specify the IP address of the target management station or server in the alarm disposition and the trap is automatically forwarded.

To forward SNMP traps:

1. Right-click the ZENworks for Servers site object in the left frame of ConsoleOne > click Properties.
2. Click the Alarm Disposition tab.
3. Select the alarm that you want to edit from the Alarm Templates list > click Edit.

   The Edit Alarm Disposition dialog box is displayed.
4. Click the SNMP Trap Forwarding tab.
5. Enter the IP address of the server to which you want to forward traps in the SNMP Target Address field > click Add.

   The server is added to the List of Targets. Repeat this step for all servers you want to receive the traps.
6. Click OK.

Forwarding Alarms to Other Management Servers

AMS can be configured to forward a processed alarm to other ZfS management servers. You specify the IP address or server name of the target management server in the alarm disposition and the alarm is automatically forwarded.

To forward alarms:

1. Right-click the ZENworks for Servers site object in the left frame of ConsoleOne > click Properties.
2. Click the Alarm Disposition tab.
3. Select the alarm that you want to edit from the Alarm Templates list > click Edit.

   The Edit Alarm Disposition dialog box is displayed.
4. Click the Alarm Forwarding tab.
5. To add a target server to receive the alarms:

5a Select the ZfS site to which you want to forward alarms in the Site Name field.

5b Select the ZfS host to which you want to forward alarms in the Site Host field.

5c Click Add.

The server is added to the List of Targets. Repeat this step for all servers to which you want to forward alarms.

6 Click OK.

Displaying a Ticker-Tape Message

The alarm disposition includes other configuration settings that include displaying a ticker-tape message in the status bar of ConsoleOne. The message provides a summary of the most recent alarm or network event.

This option is enabled by default. You may want to edit your alarm dispositions so that only important alarms that you want to monitor display a ticker-tape message.

To disable or enable a ticker-tape message:

1 Right-click the ZENworks for Servers site object in the left frame of ConsoleOne > click Properties.

2 Click the Alarm Disposition tab.

3 Select the alarm that you want to edit from the Alarm Templates list > click Edit.

The Edit Alarm Disposition dialog box is displayed.

4 Click the Other Configuration tab.

5 To disable the ticker-tape message, uncheck the Show on Ticker Bar check box.

or

To enable the ticker-tape message, check the Show on Ticker Bar check box.

6 Click OK.

Making an Audible Beep

The alarm disposition includes other configuration settings that include making an audible beep at ConsoleOne. The sound alerts the user of an occurrence of an alarm. Useful applications of this function include:

- Server abend
- System: Server downed by user
- File system full

This option is disabled by default. You should enable this option for important alarms that you want to monitor.

To enable or disable an audible beep:

1. Right-click the ZENworks for Servers site object in the left frame of ConsoleOne > click Properties.
2. Click the Alarm Disposition tab.
3. Select the alarm that you want to edit from the Alarm Templates list > click Edit.

   The Edit Alarm Disposition dialog box is displayed.
4. Click the Other Configuration tab.
5. To enable the audible beep function, check the Beep on Console check box.

   or

   To disable the audible beep function, uncheck the Beep on Console check box.
6. Click OK.

Archiving Alarm Statistics

The AMS system provides data to the reporting tools to generate detailed reports on alarms and network events. Enabling the Archive option stores the alarm in the alarm manager database on the management server. This option is enabled by default. You should disable this option only on the types of alarms that you do not want to track and analyze.

To enable or disable alarm archiving:

1. Right-click the ZENworks for Servers site object in the left frame of ConsoleOne > click Properties.
2. Click the Alarm Disposition tab.
3. Select the alarm that you want to edit from the Alarm Templates list > click Edit.

   The Edit Alarm Disposition dialog box is displayed.
4. Click the Other Configuration tab.
5. To disable alarm archiving, uncheck the Archive check box.

   or

   To enable alarm archiving, check the Archive check box.
6. Click OK.

Sorting Alarm Templates

The AMS system enables you to sort the alarm templates based on different conditions. This option is enabled by default. You can sort the templates based on Severity, Generator Type, Category or Type. By default, the sorting is done based on the Type. You can also sort the templates based on a single field by selecting the field from the drop-down list under the Sort Items By option, or you can sort the templates based on different combinations of fields by using the Then By options.

To sort the alarm templates:

1. Right-click the ZENworks for Servers site object in the left frame of ConsoleOne > click Properties.
2. Click the Alarm Disposition tab.
3. Click the Sort button.

   The Template Sorting dialog box is displayed.
4. Select fields from Sort Items By drop-down list.
5. Select fields from Then By drop-down list.
6. Select fields from Items by drop-down list.
7. Click OK.

   The templates are sorted based on the field selected in the Sort Items By option and the fields selected in these options.

For example, if you have chosen to sort the templates based on Severity in the Sort Items By list, and Category, Generator Type, in the three Then By lists, the templates will be sorted first based on severity, then on the category, followed by the generator type and the type of the template.

Maintaining the Alarm Management System

The alarm manager database on the ZfS management server increases in size each time AMS logs an alarm.

IMPORTANT: If you do not control the size of this database, it can increase until it fills the hard disk on the management server.

To control the size of the alarm manager database, regularly delete alarms that have been resolved or alarms that are not required for future reference or action. This deletes the instance of the alarm record from the alarm manager database and thus controls the size of the database.

You can delete alarms from the Alarm History view in ConsoleOne under the View menu. For more information, see "Deleting Alarms" on page 143.

Troubleshooting the Alarm Management System

When AMS receives an unsolicited SNMP trap from an agent, it locates the appropriate alarm template for the trap-type object that is defined in the MIB of the device. If the alarm template is not available, the AMS checks the IgnoreUnknownTrap flag in the <*install_volume*>\<*install_dir*>\ZENWorks\MMS\MWServer\Properties\Alarmmanager.properties file. If the flag value is set to True the alarm is ignored. If the flag value is set to False the alarm is archived in the database as an unknown trap.

To resolve this problem you need to add the MIB of the device to the MIB Pool on the management server. The MIB contains the trap definitions for traps sent from the device. If the trap-type object is undefined by AMS, it cannot resolve the type of alarm received from the trap object identifier (OID), and the alarm is unknown. See Chapter 6, "Using the MIB Tools," on page 211 for information on compiling MIBs and adding MIBs to the MIB Pool.

If you add a new device to your network, you must add the MIB to the MIB Pool. If the SNMP agent is a proxy agent hosted on a station and the software is updated, you need to update the MIB in the MIB Pool.

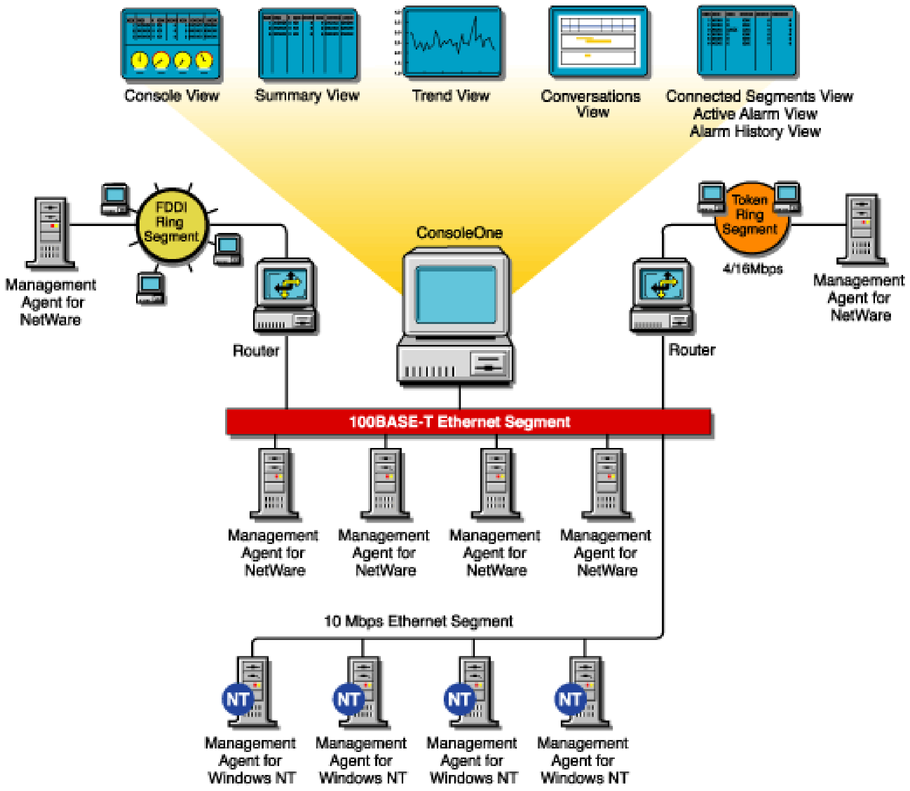
5 Understanding Server Management

The ZENworks® for Servers (ZfS) Server Management components allow you to monitor, configure, and control the managed servers and nodes on your network. The SNMP-based server Management Agents for NetWare® and Windows* NT* servers provide real-time server performance data and information about server alarms and events to the network management console. By selecting a server or node from atlas page maps or hierarchical lists in the left pane of ConsoleOne, you can access three main views of information:

- **Console View:** Provides details about the selected server or node. You can drill down into the server configuration to display information about the internal components of the machine, such as the devices, operating system, and services available on the machine.
- **Summary View:** Provides details about the server performance, such as alarms generated by the server, CPU utilization, and available disk space. By drilling down into the server configuration, you can also view summary information about other components, such as processors, threads, memory, and volumes.
- **Trend View:** Displays graphical representations of trend parameters, allowing you to monitor the state of a server over various periods of time. Using trend data, you can track the health status of servers, allowing you to predict potential problems and plan for future expansion of server configurations.

In addition to viewing information about the servers on your network, the server management components also enable you to configure your managed NetWare servers and execute frequently used commands from ConsoleOne.

The following figure displays a functional view of the ZfS Server Management components. It illustrates the Management Agent for NetWare and Management Agent for Windows NT distributed throughout a network.


Console View
Summary View
Trend View
Conversations View
Connected Segments View
Active Alarm View
Alarm History View
FDDI Ring Segment
Management Agent for NetWare
Router
ConsoleOne
Token Ring Segment
4/16Mbps
Management Agent for NetWare
Router
100BASE-T Ethernet Segment
Management Agent for NetWare
Management Agent for NetWare
Management Agent for NetWare
Management Agent for NetWare
10 Mbps Ethernet Segment
NT
Management Agent for Windows NT
Management Agent for Windows NT
Management Agent for Windows NT
Management Agent for Windows NT

This section contains the following topics to help you understand the server management components:

- "Understanding Server Management" on page 157
- "Planning for Server Management" on page 159
- "Optimizing Server Management" on page 162
- "Managing Servers" on page 171
- "Object Hierarchy and View Details" on page 181

Understanding Server Management

The Management Agent for NetWare and the Management Agent for Windows NT include features that offer benefits over server management functionality included with NetWare and Windows NT server software.

This section includes the following topics:

- "SNMP-Based Server Management" on page 157
- "SNMP Agent Functions" on page 158

SNMP-Based Server Management

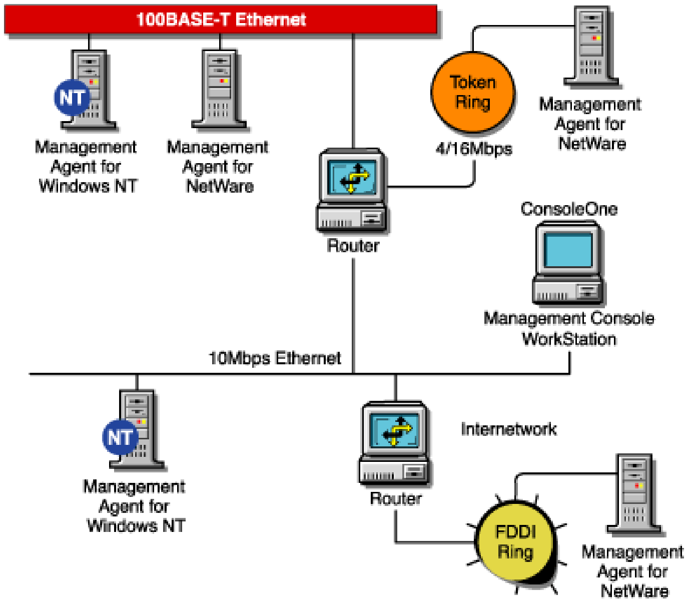
The main advantage of the Management Agent for NetWare and Management Agent for Windows NT is that they support the industry standard Simple Network Management Protocol (SNMP). SNMP is the protocol governing network management and the monitoring of network devices and their functions.

The ZfS SNMP agents support UDP/IP, IPX™, and NCP implementations for accepting and sending packets (datagrams). This standard mechanism allows any SNMP console or manager to request information from the ZfS Server Management SNMP agents. An SNMP console can be any console that supports SNMP; the ZfS ConsoleOne fully supports SNMP v.1 communication.

SNMP Agents

The ZfS server management SNMP agents run on NetWare and Windows NT servers in your network. The agents monitor servers, collecting historical data and dynamic data in response to requests from ConsoleOne. An administrator at the ZfS ConsoleOne can request data simply by clicking a representative icon for any device, operating system, or service discovered on a server.

The following figure illustrates an internetwork using the Management Agent for NetWare and Management Agent for Windows NT and the ZfS ConsoleOne.


100BASE-T Ethernet
NT
Management Agent for Windows NT
Management Agent for NetWare
Router
Token Ring
4/16Mbps
Management Agent for NetWare
ConsoleOne
Management Console WorkStation
10Mbps Ethernet
NT
Management Agent for Windows NT
Router
Internetwork
FDDI Ring
Management Agent for NetWare

SNMP Agent Functions

The functionality of the Management Agent for NetWare and Management Agent for Windows NT (the Novell SNMP-based agents for NetWare and Windows NT servers) can be divided into the following areas:

- Collecting Statistics
    - Monitoring: Server monitoring provides instant information about various monitored elements of the server, such as CPU utilization, memory size, cache buffers, connected users, volumes, disks, disk space usage per user, network adapters, print queues, print jobs, and loaded NetWare Loadable Module™ (NLM™) files on NetWare or Windows NT servers.
    - Trending: Trends provide historical data about various server objects and can be displayed in a diagram on the SNMP console. Trends are stored at the server side, which eliminates the need for continuous polling from an SNMP manager, and this data can be accessed via SNMP by any ZfS ConsoleOne or other SNMP-based console.
- Alarm Notification: More than 580 different types of alarms or events (SNMP traps) can be sent from any NetWare server to the ZfS management system or to any other SNMP-based console.

Any Windows NT system, security, or application event is converted to an SNMP trap and sent to the ZfS management system or to any other SNMP-based console.

The alarms inform the administrator about events that have occurred or thresholds which have been crossed.

- Configuration Management: The Management Agent for NetWare enables network administrators to remotely configure NetWare servers. There are 187 SET parameters on the NetWare server that can be used to tune the server's performance. Administrators can view settings and change all parameters from any ZfS ConsoleOne.

The SNMP agents must be installed on any server that you want to manage. For information on installing the SNMP agents, or if you have already installed the agent software to servers that you want to manage, see Installing and Setting Up Management and Monitoring Services in the *Installation* guide.

Planning for Server Management

A baseline defines the typical activity of your network servers. Keeping a baseline document of activity on a server lets you determine when the activity is atypical. To create a baseline activity, you should gather statistical information when the server is functioning typically.

This section contains the following information to help you plan your server management strategy:

- "Creating a Baseline of Typical Server Activity" on page 159
- "Using the Baseline Document" on page 160
- "Server Baseline Document Tips" on page 161

Creating a Baseline of Typical Server Activity

For server statistics such as CPU utilization, you should create a trend graph that plots information over a period of time. Statistics sampling that gathers data over a short period of time can be misleading. If you modify the server's configuration, it is useful to create another baseline against which you can compare future activity.

There are two ways to create baseline documents. The first is to create them manually by printing the various trend graphs for which you want to maintain baselines. The other way is to use the server management health reports as your baseline documents. For more information on creating and generating health reports, see "Managing the Server Management Health Reports" on page 402. In either case, the data gathered can be exported into programs, such as spreadsheets, for further analysis and to maintain records over time.

Using the Baseline Document

The following sections will help you plan and use the baseline document:

- "Using Baseline Documents to Set Alarm Thresholds Appropriately" on page 160
- "Using Baseline Documents to Track Server Utilization" on page 160
- "Use Baseline Documents in Troubleshooting" on page 160

Using Baseline Documents to Set Alarm Thresholds Appropriately

You should set alarm thresholds for statistics on servers monitored by the SNMP agent software, so that if the threshold is exceeded, you are notified at ConsoleOne. Setting alarm threshold values for statistics on a server eliminates the need for you to constantly monitor polled server statistics for problems.

Server Management components provide default values for thresholds set on server statistics; rising and falling statistics generate an alarm when a threshold is surpassed.

Using Baseline Documents to Track Server Utilization

By comparing current server performance statistics against the performance recorded in your baseline document, you can determine how performance is affected by server configuration changes. This comparison also helps you plan for growth and justify upgrades and expansion. You can view graphs of real-time trends and historical trends over hourly, daily, weekly, monthly, and yearly periods.

Use Baseline Documents in Troubleshooting

By knowing what the typical server activity is, you can recognize atypical activity, which might help you isolate the cause of a problem.

Server Baseline Document Tips

You should include the following key characteristics in each server baseline document:

- "CPU Utilization" on page 161
- "Cache Buffers" on page 161
- "File Reads and Writes" on page 161
- "Volume Utilization" on page 162
- "Running Software" on page 162

CPU Utilization

The CPU Utilization statistic indicates how busy the microprocessor is. High CPU utilization can cause slow network response time. Utilization is likely to be higher at some times during the day (for example, when users log in to the network in the morning, or access e-mail), week, or month. Tracking CPU utilization helps you track the load on the server processor at peak and low times. This information helps you determine the effect of current system and application processor demands and analyze the impact on performance.

Cache Buffers

Virtually all processes are handled through server cache, a block of server memory (RAM) in which files are temporarily stored. Cache buffers greatly increase server performance and enable workstations to access data quicker because reading from and writing to memory is much faster than reading from or writing to disk. The optimum cache buffer is 65% to 75% of total server memory (more does not hinder performance). Low cache buffers can cause slow server performance and abends. Service degrades noticeably at 45% of total server memory.

File Reads and Writes

By tracking data about file reads and writes in your baseline, you might be able to determine whether a bottleneck is caused by the disk I/O channel. For example, if an increasing number of "server busy" packets are sent to users and there is also an increase in the file read and write number, the cause of the bottleneck might be a slow disk I/O channel or bad disk adapter driver.

Volume Utilization

Tracking volume utilization is primarily for capacity planning. By tracking the volume space used over time, you can accurately predict when you must purchase additional storage. Tracking volume utilization can also help you prevent the server from running out of disk space.

Running Software

By including information about running software in your baseline, it is easier to spot a problem application when comparing software on different servers. It is useful to also include the memory each application uses. Then, if the server is running short of memory, you can quickly see which applications are using the most memory.

Optimizing Server Management

Examine each of the configuration options in the sections that follow to determine whether you require any of the functionality provided:

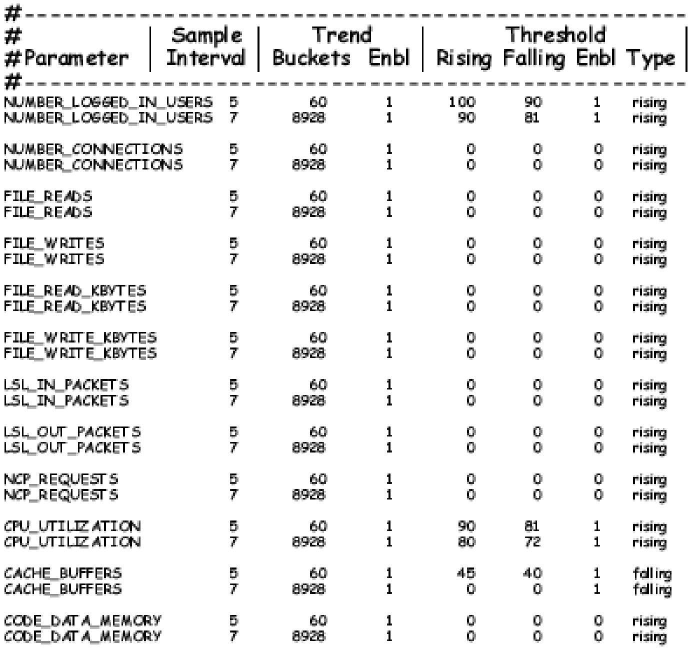
- "Setting Default Trends and Thresholds" on page 162
- "Controlling Alarm Generation" on page 168
- "Defining Recipients for SNMP Alarms" on page 171

Setting Default Trends and Thresholds

You can modify the default trends and threshold values from within ConsoleOne or manually modify files on servers that have the Management Agent for NetWare or Management Agent for Windows NT software installed.

When server agents are first loaded, the initial (default) values for trends and thresholds are read from the NTREND.INI file (NetWare) or the N_NTTREN.INI file (Windows NT). The initial values are also used whenever a new trend file is created. A new trend file is created when an instance of a monitored object (volume, disk, interface, and so on) is discovered on the server.

The following is a sample excerpt from an NTREND.INI file:



```
#---------------------------------------------------------------------
#                      | Sample  |     Trend     |          Threshold          |
#Parameter             | Interval| Buckets  Enbl | Rising Falling Enbl Type    |
#---------------------------------------------------------------------
NUMBER_LOGGED_IN_USERS  5          60      1      100     90     1    rising
NUMBER_LOGGED_IN_USERS  7        8928      1       90     81     1    rising

NUMBER_CONNECTIONS      5          60      1        0      0     0    rising
NUMBER_CONNECTIONS      7        8928      1        0      0     0    rising

FILE_READS              5          60      1        0      0     0    rising
FILE_READS              7        8928      1        0      0     0    rising

FILE_WRITES             5          60      1        0      0     0    rising
FILE_WRITES             7        8928      1        0      0     0    rising

FILE_READ_KBYTES        5          60      1        0      0     0    rising
FILE_READ_KBYTES        7        8928      1        0      0     0    rising

FILE_WRITE_KBYTES       5          60      1        0      0     0    rising
FILE_WRITE_KBYTES       7        8928      1        0      0     0    rising

LSL_IN_PACKETS          5          60      1        0      0     0    rising
LSL_IN_PACKETS          7        8928      1        0      0     0    rising

LSL_OUT_PACKETS         5          60      1        0      0     0    rising
LSL_OUT_PACKETS         7        8928      1        0      0     0    rising

NCP_REQUESTS            5          60      1        0      0     0    rising
NCP_REQUESTS            7        8928      1        0      0     0    rising

CPU_UTILIZATION         5          60      1       90     81     1    rising
CPU_UTILIZATION         7        8928      1       80     72     1    rising

CACHE_BUFFERS           5          60      1       45     40     1    falling
CACHE_BUFFERS           7        8928      1        0      0     1    falling

CODE_DATA_MEMORY        5          60      1        0      0     0    rising
CODE_DATA_MEMORY        7        8928      1        0      0     0    rising
```

After the Management Agent for NetWare and Management Agent for Windows NT software is running, trend and threshold values can be changed (using ConsoleOne) by making use of the threshold-setting features of ZfS. If the server is brought down, it retains the last trend and threshold settings that were set. Initial values are reset when any of the following situations occurs:

- Trend files have been deleted manually.
- If the server configuration is modified, for example, by adding a new volume, disk, or interface.

IMPORTANT: Trends are not maintained for CD volumes. Therefore, changing trend parameters for CD volumes has no effect.

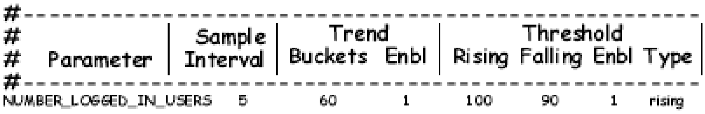
The following sections contain information to help you modify initial trend and threshold values:

- "Changing the Initial Trend Values" on page 163
- "Changing the Initial Threshold Values" on page 167

Changing the Initial Trend Values

The trend values in the NTREND.INI file (NetWare) and N_NTTREN.INI file (Windows NT) specify the time interval (Sample Interval) at which a particular trend parameter is sampled, the duration of time for which those samples are kept (Trend Buckets), and whether this sampling parameter is enabled (Enbl). For each value specified by a line in the NTREND.INI file or N_NTTREN.INI file, a trend record is stored in a separate file in the SYS:\NTREND directory on a NetWare server and the \TRENFILE directory on a Windows NT server.

The following illustration depicts a line in the NTREND.INI file for the NUMBER_LOGGED_IN_USERS trend parameter with a Sample Interval of 5, Trend Buckets specified at 60, and the enable parameter specified at 1 (enabled).



```
#---------------------------------------------------------------------------
#                        | Sample  |    Trend      |        Threshold         |
#   Parameter            | Interval| Buckets  Enbl | Rising Falling Enbl Type |
#---------------------------------------------------------------------------
NUMBER_LOGGED_IN_USERS    5          60       1      100     90      1   rising
```

The following sections describe how to set or alter each of the parameters required for a trend file:

- "Setting the Sample Interval" on page 164
- "Setting the Trend Buckets" on page 165
- "Enabling or Disabling a Trend File" on page 167
- "Backing Up Trend Data" on page 167

You can specify more than one sampling interval or duration for any trend parameter by creating another line in the NTREND.INI file or N_NTTREN.INI file.

Setting the Sample Interval

The trending software enables you to collect samples of a specified parameter at any of 12 possible time intervals (Sample Interval), from 5 seconds to 1 day.

Each of these sample intervals is specified by a code number in the NTREND.INI file and the N_NTTREN.INI file. The following table specifies the codes used in the NTREND.INI and N_NTREND.INI files for the permitted sample intervals. For example, if you want to sample a particular trend parameter once every hour, you would use the code 9.

Sample Interval	Code
5 seconds	1
10 seconds	2
15 seconds	3
30 seconds	4
1 minute	5
5 minutes	6
15 minutes	7
30 minutes	8
1 hour	9
4 hours	10
8 hours	11
1 day	12

Setting the Trend Buckets

After you have determined a sample interval for collecting samples, you must set a duration of time for which you want to collect samples. For example, if you selected a sample interval of one hour for a particular parameter, you might decide that you want to be able to review the state of that parameter for every hour over the duration of a day.

You determine the duration of time for which a parameter is collected by the number of trend buckets you specify. You must specify a trend bucket for each sample that is collected over a specific period of time. For example, to review the state every hour for 1 day, 24 trend buckets (1 per hour x 24 hours in a day) are required.

The number of trend buckets required for any particular time duration and sample interval is calculated easily. However, for your convenience, the following table shows the number of trend buckets required for each sample interval allowed, for each of seven possible time durations of from 1 hour to 1 year.

After you set the sample interval and the time duration for trend collection, you can compute the size of trend files. The number of trend buckets possible, and the approximate size in kilobytes (in parentheses), for a given sample interval and time duration are also given in the following table. The size of each trend bucket is 4 bytes plus 512 bytes for the header file. For example, if the sampling interval is 5 seconds for a period of 1 hour, the file size would be 720 trend buckets x 4 bytes long (rounded to the closest 4 KB boundary) plus 512 bytes for a total of 4.5 KB. There are always as many trend files as there are enabled trends.

Sample Interval	1 Hour Duration	1 Day Duration	1 Week Duration	1 Month Duration	3 Months Duration
0 seconds	720	17280	120960	535680	1607040
1.0 seconds	360	8640	60480	267840	803520
15 seconds	240	5760	40320	178560	535680
30 seconds	120	2880	20160	89280	267840
1 minute	60	1440	10080	44640	133920
5 minutes	12	288	2016	8929	26784
15 minutes	4	96	672	2975	8928
30 minutes	2	48	336	1488	4464
1 hour	1	24	168	744	2232
4 hours		6	42	186	558
8 hours		3	21	93	279
1 Day		1	7	31	93

After a particular time duration is exceeded for a file (all the trend buckets have been filled), the oldest samples are overwritten by the most recent samples. This means that the file contains the most recent duration recorded. For example, if you select a sample interval of 1 hour for a duration of 24 hours (using 24 trend buckets), the associated file contains the trend data for the last 24 hours.

Enabling or Disabling a Trend File

Each line in the NTREND.INI file and the N_NTTREN.INI file contains a parameter that either enables or disables the trending value to begin creating a trend file at startup. To enable the collection of data for a trend file, set this parameter to 1. To disable the collection of data for a trend file at startup, set this parameter to 0.

Backing Up Trend Data

Trend data is not automatically backed up. If you want to back up this data, you must do so manually.

Changing the Initial Threshold Values

The default threshold values in the NTREND.INI file and the N_NTTREN.INI file specify when a trap is generated. User-defined values are stored in the trend file header. If the parameter rises above or falls below the set threshold value, a rising or falling trap type is sent.

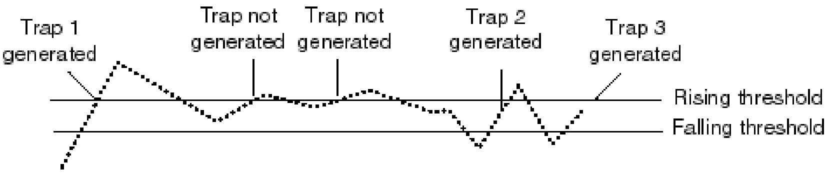
The following sections describe how to set or alter each of the parameters required for a threshold value:

- "Setting Rising and Falling Thresholds" on page 167
- "Enabling or Disabling a Threshold Trap" on page 168

Setting Rising and Falling Thresholds

Each line in the NTREND.INI file and the N_NTTREN.INI file contains a parameter for the rising threshold and the falling threshold. For each sample interval, a rising or falling trap can be generated as specified. After a trap is generated, another such trap is not generated until the sampled value falls below this threshold and reaches the falling threshold.

The following figure provides an example of this process for a rising threshold trap:



In this example, Trap 1 is generated because it is the first time that the parameter value rises above the Rising Threshold. The next two times the parameter value rises above the Rising Threshold, a trap is not generated because the parameter did not fall below the Falling Threshold. Trap 2 and Trap 3 are generated because the parameter value dropped below the Falling Threshold before exceeding the Rising Threshold.

Enabling or Disabling a Threshold Trap

Each line in the NTREND.INI file and N_NTTREN.INI file contains a parameter that enables or disables the NTREND.NLM software to send traps as determined by the rising and falling thresholds. This parameter is set to 1 to enable the software to send a trap for the values given, or to 0 to disable the software from sending a trap for this parameter.

Controlling Alarm Generation

Each managed server has files that specify which system events result in a trap. On NetWare, the NWTRAP.CFG and NDSTRAP.CFG files are stored in the SYS:\ETC directory. On Windows NT, this file is NTTRAP.INI, which is stored in the MW\INI directory.

On NetWare, the trap configuration file is read only when NWTRAP.NLM is loaded; therefore, any changes made to the file do not take effect until the next time you load NWTRAP.NLM or NDSTRAP.NLM.

IMPORTANT: On a NetWare 3.*x* server, EDIT.NLM does not have a large enough buffer to edit the NWTRAP.CFG file. To edit the NWTRAP.CFG file, map a drive to the server's SYS: volume and proceed from there.

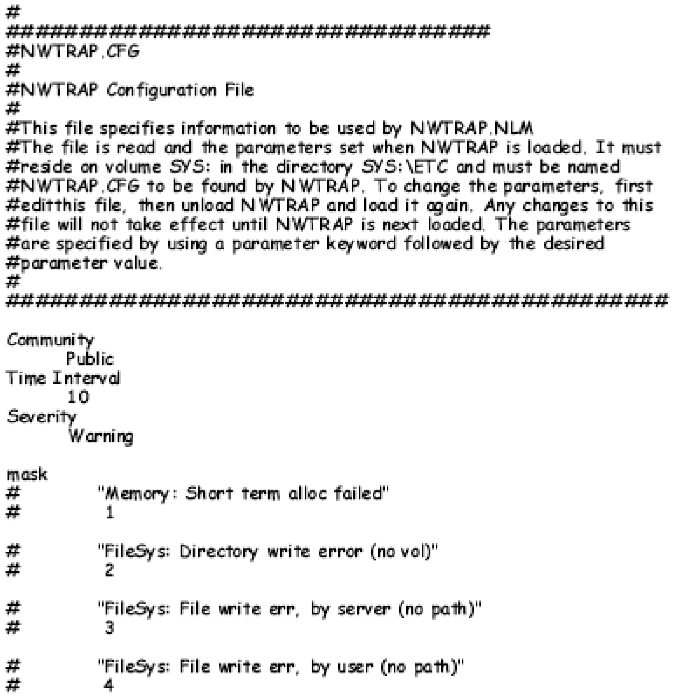
The .CFG files on NetWare contain the list of supported traps. You can modify the .CFG files or NTTRAP.INI file with the following:

- Types of alarms forwarded to ConsoleOne
- Community strings used for sending SNMP traps
- List of traps to be disabled, using the mask keyword
- Specific alarms that you want to prevent from forwarding

The configuration file consists of keywords and their associated data (case is ignored). Each keyword must be on a line by itself (except for mask values, where they might span several lines), and must be followed by one or more lines of associated data.

You can place comments anywhere in the file, even between a keyword and its associated information. A comment starts with a number sign (#), and continues to the end of the line.

The following is an example of an NWTRAP.CFG file:



```
#
#################################
#NWTRAP.CFG
#
#NWTRAP Configuration File
#
#This file specifies information to be used by NWTRAP.NLM
#The file is read and the parameters set when NWTRAP is loaded. It must
#reside on volume SYS: in the directory SYS:\ETC and must be named
#NWTRAP.CFG to be found by NWTRAP. To change the parameters, first
#editthis file, then unload NWTRAP and load it again. Any changes to this
#file will not take effect until NWTRAP is next loaded. The parameters
#are specified by using a parameter keyword followed by the desired
#parameter value.
#
##############################################

Community
        Public
Time Interval
        10
Severity
        Warning

mask
#            "Memory: Short term alloc failed"
#             1

#            "FileSys: Directory write error (no vol)"
#             2

#            "FileSys: File write err, by server (no path)"
#             3

#            "FileSys: File write err, by user (no path)"
#             4
```

The following sections contain information to help you control alarm generation:

- "Setting the Time Interval (Management Agent for NetWare Only)" on page 169
- "Configuring Alarm Severity Levels" on page 170

Setting the Time Interval (Management Agent for NetWare Only)

Sometimes an alarm repeats rapidly (several times per second or per minute) with identical or nearly identical parameters. When this occurs, the second and later alarms within a time interval are usually not as interesting as the first alarm.

To prevent the network and ConsoleOne from being inundated with identical alarms, you can specify a time interval to be applied to every alarm generated. During this interval, alarms that are identical to an initial alarm are discarded.

You can define the time interval in the configuration file as follows:

```
Time Interval
```

n

where *n* can take any value from 0 to 232 to indicate the number of seconds that must elapse before a later alarm is not discarded.

The default time interval is 10 seconds.

Configuring Alarm Severity Levels

Use the severity keyword to set a minimum alarm severity level so that traps for lesser severity alarms are not sent.

The severity levels you can set in the NWTRAP.CFG and NTTRAP.INI files are informational, warning, recoverable, critical, and fatal. The following table lists the NetWare severity level and corresponding SNMP and ZfS severity levels.

NetWare Severity Level	SNMP Severity Level	ZfS Severity Level
0 - Informational	Informational	Informational
1 - Warning	Minor	Minor
2 - Recoverable	Major	Major
3 - Critical	Critical	Severe
4 - Fatal	Fatal	Severe
5 - Operation Aborted	Fatal	Severe
Unrecoverable	Fatal	Severe

The default keyword is warning. Under the default, all alarms with a severity level of warning or greater are forwarded.

Defining Recipients for SNMP Alarms

You can configure the Management Agent for NetWare to send SNMP traps (alarms) to the ZfS management server or to other management nodes.

NOTE: For setting trap destinations on Windows NT servers, see the documentation on the SNMP Service provided with the Microsoft Windows NT operating system software.

Steps for designating trap target destinations are described in the following section.

Editing the TRAPTARG.CFG File Manually (Management Agent for NetWare Only)

You can configure trap recipients by manually adding them to the TRAPTARG.CFG file. This is useful for sending traps to third-party management consoles other than the ZfS management server.

You must add trap recipients manually by specifying their addresses in the TRAPTARG.CFG file, which is located in the SYS:\ETC directory of all NetWare servers.

The TRAPTARG.CFG file defines the recipients of SNMP traps. You can use this file to define recipients of SNMP traps over IPX and UDP/IP. The file is fully annotated to show you how to divide the file into IPX and UDP/IP sections and how to write the IPX and IP addresses of recipients.

The TRAPTARG.CFG file is read only when SNMP is loaded. In most cases, this means bringing the server down and restarting it because a variety of modules must be unloaded and reloaded as well. Thus, any changes made to the TRAPTARG.CFG file do not take effect until the next time you load NWTRAP.NLM.

IMPORTANT: The NWALARM.MIB file imports symbols from the Host Resources MIB (RFC1514.MIB), which can also be found in SYS:ZENWORKS\MMS\MWSERVER\MIBCSERVER\MIBSERVERPOOL\MIBPOOL.

Managing Servers

With the Management Agent for NetWare and Management Agent for Windows NT software installed on your NetWare and Windows NT servers, respectively, you can begin collecting data, receive alarm notifications, remotely manage configuration, and generate reports for managed servers.

Server Management tasks you can perform with ZfS include:

- "Displaying Server Configuration Information" on page 172

- “Displaying Summary Data” on page 173
- “Viewing Trend Data” on page 174
- “Managing Trend Samplings” on page 177
- “Configuring Server Parameters” on page 179
- “Executing Server Commands” on page 180

Displaying Server Configuration Information

Server configuration data is organized in a hierarchical listing expanding down from the server object. You can view information about the server's configuration, memory usage, adapters, network interfaces, disks and disk controllers, volumes, queues, users, connections, open files, NLM files (NetWare), and installed software.

To display server configuration information:

1. Locate the server object you want to expand.

   Servers are represented in atlas page maps and in the hierarchical list in the left pane of ConsoleOne by the following icons:

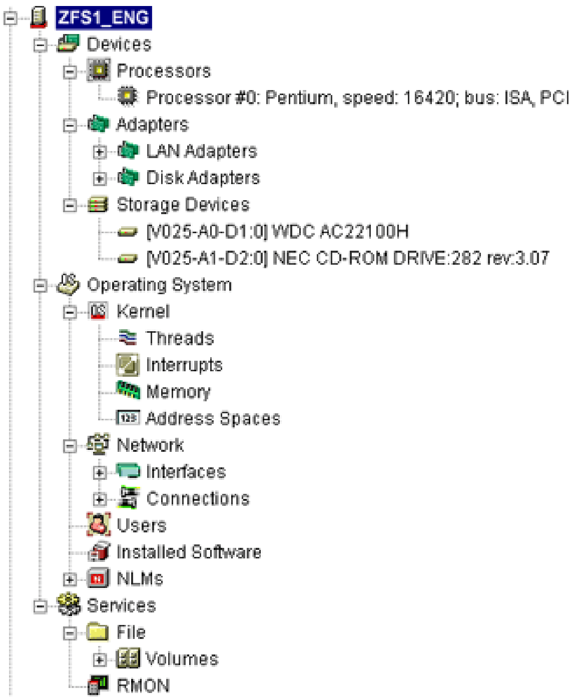
   - Server container
   - NetWare server with Management Agent
   - Windows NT server with Management Agent
   - Generic server

2. Click the plus sign (+) next to the server object.

   The server object opens in the left pane under its parent object and the server contents are displayed. Server data is grouped into the following three categories:

   - Devices
   - Operating System
   - Services

3. You can drill down into the server configuration farther by clicking the plus signs next to the Devices, Operating System, and Services objects as in the following example.



Displaying Summary Data

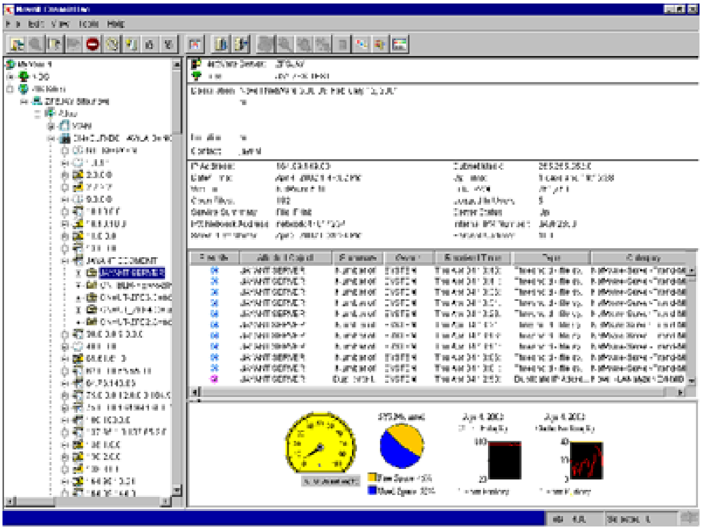
The Summary View contains tables of statistics obtained by SNMP GET requests to the Management Agent for NetWare and Management Agent for Windows NT software hosted on managed servers. Statistics are updated dynamically as the server is continually polled for data. Polling utilizes SNMP GET and GET NEXT requests to update the data. You can also control the polling of a selected object by using the stop and refresh functions.

You can view summary data for server, processors, LAN adapters, disk adapters, storage devices, threads, interrupts, memory, address spaces, interfaces, connections, users, installed software, NLM files (NetWare), and volumes. For detailed information about a specific Summary view, see "Object Hierarchy and View Details" on page 181.

To display summary information:

1 Right-click the object for which you want to view summary data > click Views > click Summary.

The Summary View is displayed. The following screen shows the Summary View for a server object. The server summary provides descriptive information including the server's eDirectory name and tree, IP address, RAM, operating system and version, IPX address, subnetwork mask, up time, logged-in users, open files, and status. In addition, the server summary lists all alarms, affected objects, summary, and owner and volume disk space, trend graphs for cache hits and cache buffers. The Summary view displays graphical indicators of the CPU utilization that depicts the average percentage of time that the CPU was not idle for the past minute.



Viewing Trend Data

On a server managed by Management Agent for NetWare or Management Agent for Windows NT, the agents automatically gather trend data on CPU usage, memory usage, and network interface traffic. You can then view current trend data, or historical trend data by hour, day, week, month, or year from ConsoleOne. In this view, the time interval that is being sampled is displayed on the x-axis. The parameter value over the sample period is plotted on the y-axis. Note that the values on the y-axis use the standard abbreviations K (for kilo), M (for mega), and G (for giga). Therefore, a value of 1K would equal 1000; similarly, a value of 1M would equal 1,000,000.

Monitoring trend data helps you with tasks such as setting trend alarm thresholds, determining who is using the server and when the server is used heavily, troubleshooting problems, balancing loads across multiple servers, and planning resources. You can also export trend view data to popular spreadsheet formats for sharing data with others.

You can view trend data for processors, LAN adapters, storage devices, memory, connections, users, and volumes. For information about a specific trend view, see "Object View Details" on page 183.

To view trend statistics:

1. Right-click the object for which you want to view trend data > click Views > click Trend.

   The Trend View is displayed. The following sections describe the tasks you can perform using the Trend View:

   - "Displaying the Legend" on page 175
   - "Modifying the Time Span" on page 175
   - "Customizing the Trend View Display" on page 176
   - "Modifying the Trend View Profile" on page 177

Displaying the Legend

The Trend View legend indicates what each color in the graph represents.

To display the legend:

1. Click the Legend button in the Trend View toolbar.

Modifying the Time Span

The Trend View time span specifies what time period the trend graphs represent. By default, a one-hour history is displayed.

To modify the time span:

1. Select a time span from the drop-down list in the Trend View toolbar. You can select from the following time spans:

   - 1 Hour
   - 1 Day
   - 1 Week
   - 1 Month
   - 1 Year

Customizing the Trend View Display

The Trend View provides several options for customizing the look of the screen. In customizing the view, you can choose from the following options:

- "Displaying Grid Lines" on page 176.
- "Stacking and Unstacking Graphs" on page 176.
- "Scaling the Y Axis" on page 176.

Displaying Grid Lines

By default, the trend charts do not include grid lines.

To display horizontal and/or vertical grid lines:

1. To display horizontal grid lines, select the Horizontal Grid button in the Trend View toolbar.
2. To display vertical grid lines, select the Vertical Grid button in the Trend View toolbar.

   Note that you remove the horizontal or vertical grid lines by clicking the same buttons.

Stacking and Unstacking Graphs

By default, all trends are displayed on a single graph with one vertical axis. However, you can customize the view so that each trend is displayed in its own separate graph.

To stack and unstack graphs:

1. To display the trends on separate graphs, click the Strip Chart button on the Trend View toolbar.
2. To display trends on the same graph, click the Stack Chart button on the Trend View toolbar.

Scaling the Y Axis

To display more useful information on your trend graphs, you may find that you need to modify the scale on the Y axis as follows:

1. To increase the scale on the Y axis, click the Increase Y Axis button, which is located to the left of the graph(s).
2. To decrease the scale on the Y axis, click the Decrease Y Axis button, which is located to the left of the graph(s).

3. To scale the Y axis to fit in the window, click the Scale to Fit button on the Trend View toolbar.

Modifying the Trend View Profile

The Trend View profile represents the set of parameters that are displayed graphically when the Trend View is invoked. You can modify which parameters are displayed in the Trend View by editing the profile.

To edit the profile:

1. Click the Profile button in the Trend View toolbar.

   The Profile dialog box is displayed. The parameters that are currently displayed in the Trend View for the object are selected.

2. Edit the profile by clicking a parameter name to select or deselect it.

   You can Shift+click multiple, consecutive parameters and Ctrl+click multiple, non-consecutive parameters.

3. Click OK.

Managing Trend Samplings

You can customize the parameters of the trend data displayed using the following options:

- "Modifying Trend Sampling and Intervals" on page 177.
- "Modifying Threshold Alarm Settings" on page 178.

Modifying Trend Sampling and Intervals

For each trend for which the server agents collect data, you can set sampling intervals and the number of samples stored on the server as follows:

1. Right-click the object > click Properties.
2. Click the Trend tab.
3. Select the trend parameter you want to modify > click Edit.

   The Edit Trend dialog box is displayed. The trend sampling and interval settings are displayed in the Sampling Parameters section of the screen.

4. To enable or disable the sampling parameter, select the appropriate value from the State drop-down list.

5. To modify the time interval (Sample Interval) at which the trend parameter is sampled, select a value from the Frequency drop-down list.

   You can select one of 12 possible time intervals from five seconds to one day.

6. Specify the duration of time for which to collect samples by entering a value in the Number of Samples field.

   You determine the duration of time for which a parameter is collected by the number of samples (trend buckets) you specify. You must specify a trend bucket for each sample that is collected over a specific period of time. For more information on setting the number of samples required, see "Setting the Trend Buckets" on page 165.

7. When you are done modifying the alarm threshold settings, click OK.

Modifying Threshold Alarm Settings

You can set an alarm threshold for each trend parameter for which the Management Agent for NetWare and Windows, collects data. After you set the alarm threshold, the Management Agent for NetWare sends an alarm to ConsoleOne if the trend crosses the threshold you set.

The Management Agent for NetWare tracks both rising and falling alarm thresholds. Each trend parameter has either a rising or a falling threshold associated with it; the type of threshold cannot be changed.

To change alarm thresholds through ConsoleOne:

1. Right-click the object > click Properties.

2. Click the Trend tab.

3. Select the trend parameter for which you want to modify threshold settings > click Edit.

   The Edit Trend dialog box is displayed. The threshold alarm settings are displayed in the Rising Alarm Parameters section of the screen.

4. To enable or disable the alarm parameter, select the appropriate value from the State drop-down list.

5. To set or modify the rising threshold, enter a value in the Rising Threshold field.

6. To set or modify the falling threshold, enter a value in the Falling Threshold field.

7. When you are done modifying the alarm threshold settings, click OK.

Configuring Server Parameters

In order to correct an alarm condition, fine-tune server performance, or fix other problems detected on a server, you need to modify the server configuration. Server configuration can be adjusted from ConsoleOne on any NetWare server hosting the Management Agent for NetWare. SET parameters, usually set at the server console or through a remote console, can be configured from ConsoleOne interface. From ConsoleOne, you can see the current settings, change one or more settings, and confirm your settings before adjustments are sent to the server.

For parameter values and descriptions, see the NetWare server documentation. This information is generally found in the Utilities Reference document.

To view or modify the NetWare SET parameters from ConsoleOne:

1. Drill down into the server you want to configure by clicking the plus sign (+) next to the server object.
2. Right-click the Operating System object > click Properties.

   The Set Parameters tab is displayed. This tab page lists the NetWare SET parameters and their current values.
3. Click the down-arrow icon on the Set Parameters tab > click the category of SET parameters you want to display.

   You can choose from the following categories: Communications, Directory Caching, Directory Services, Disk, Error Handling, File Caching, File System, Licensing Services, Locks, Memory, Miscellaneous, Multiprocessor, NCP, Service Location Protocol, Time, or Transaction Tracking.
4. Select the parameter you want to modify > click Edit.

   The Edit Parameters dialog box is displayed.
5. Enter the new parameter value in the appropriate field.
6. Indicate when you want the parameter change to take effect by selecting the appropriate radio button from the Apply Value box. You can choose to apply the change at the following times:

   - Now, until reboot
   - Only after reboot
   - Now, and after reboot
7. Click OK.

Executing Server Commands

You can execute the following frequently used NetWare server commands from ConsoleOne.

- "Loading and Unloading an NLM" on page 180
- "Mounting and Dismounting Volumes" on page 180
- "Clearing a Server Connection" on page 180
- "Restarting a Server" on page 181
- "Shutting Down a Server" on page 181

Loading and Unloading an NLM

To load or unload an NLM from ConsoleOne:

1. Right-click the NLM object > select a command from the menu as follows:
    - To load the NLM, select Load nlm
    - To unload the NLM, select Unload nlm

Mounting and Dismounting Volumes

To mount or dismount a volume:

1. Right-click the volume object > click Mount Volume.

    or
    Right-click the volume object > click Dismount Volume.

    The system displays a confirmation box.

2. Click OK.

Clearing a Server Connection

You can clear a server connection when the server has crashed and left open files on the server or before bringing down the server. This is equivalent to the CLEAR STATION command that you can execute from the server console.

To clear a server connection from ConsoleOne:

1. Locate the connection you want to close by expanding the following objects: Server > Operating System > Network > Connections.
2. Right-click the connection you want to close > click Clear Connection.

Restarting a Server

To restart a server from ConsoleOne:

1 Right-click the server object > click Restart Server.

Shutting Down a Server

To shut down a server from ConsoleOne:

1 Right-click the server object > click Down Server.

Object Hierarchy and View Details

When you expand a managed server object, you can view details about the contents of the server. The following sections detail the available objects on a managed server and provide information about the statistical information available in the views for each object. This topic contains the following sections:

- "Object Hierarchy" on page 181
- "Object View Details" on page 183

Object Hierarchy

The following table shows the hierarchy of available objects on a managed server along with their associated icons. For more information about the available views associated with an object, follow the corresponding link.

Category Container	Sub-category Containers	Object Containers	Objects
Devices	"Processors" on page 184		Processor
	"Printers" on page 208		Printers
	"Adapters" on page 188	LAN Adapters	Adapter
		Disk Adapters	Adapter

Category Container	Sub-category Containers	Object Containers	Objects
	“Storage Devices” on page 186		Storage Device
	“Other Devices” on page 208		Keyboard
			Mouse
	“Ports” on page 209		Parallel Port
			Serial Port
Operating System	Kernel	“Threads” on page 190	Thread
		“Interrupts” on page 190	Interrupt
		“Memory” on page 192	Memory
		“Address Spaces” on page 196	Address Space
	“Network” on page 197	“Interfaces” on page 197	Interface
		“Connections” on page 199	Connection
	“Users” on page 201		User
	“Installed Software” on page 202		Software
	“NLM” on page 203		NLM

Category Container	Sub-category Containers	Object Containers	Objects
Services	File	“Volumes” on page 204	Volume
	Print	“Queues” on page 206	Queue

Object View Details

The following sections provide details about the statistical information available in each object view:

- “Processors” on page 184
- “Storage Devices” on page 186
- “Adapters” on page 188
- “Threads” on page 190
- “Interrupts” on page 190
- “Memory” on page 192
- “Address Spaces” on page 196
- “Network” on page 197
- “Interfaces” on page 197
- “Connections” on page 199
- “Users” on page 201
- “Installed Software” on page 202
- “NLM” on page 203
- “Volumes” on page 204
- “Queues” on page 206
- “Printers” on page 208
- “Other Devices” on page 208
- “Ports” on page 209

Processors

Viewing processor speed helps you analyze and balance loads across servers. Viewing processor utilization data helps you detect problems with utilization and determine when server load is light enough to schedule tasks such as server backups. The server operating system (OS) automatically determines the CPU speed and is reported based on the OS data.

Processor speed is a major determinant of server performance. Therefore, it is important to know the processor speed of your servers when analyzing server load and balancing load across multiple servers. For example, one server might be handling twice as many users as another, but if the processor is twice as fast, the load might still be distributed correctly.

You should maintain a baseline of processor utilization for a server so that you can recognize when a server's processor utilization is higher than normal.

You can display the following views of information about the processors on your managed servers:

- "Processors Summary View" on page 184
- "Processor Summary View" on page 185
- "Processors Trend View" on page 185

Processors Summary View

You can access the Summary View for the Processors object container after expanding the following server objects: Devices > Processors. This view displays the following information for each processor object in the container:

- **Processor Number:** A unique number assigned to the processor.
- **Status:** The status of the processor is either online or offline.

The following statistics are displayed only if the processor is online:

- **Utilization %:** Processing load on this processor for the last second, expressed as a percentage.
- **Interrupts Processed:** Number of interrupts fired on this processor in the last second.
- **Time Spent in Interrupts Last Second, in Microseconds:** The amount of time in microseconds that the processor spent processing interrupts in the last second.

- **Number of Bound Threads:** The number of threads that have been bound to this processor. Threads that are bound to a processor run only on that processor. Unbound threads can be migrated from one processor to another when required.

Processor Summary View

You can select the Summary View for an individual processor after expanding the following server objects: Devices > Processors > *processor #x*. This view displays the following information:

- **Processor Number and Status:** A unique number assigned to the processor along with its current status. The status can be online or offline.

The following statistics are displayed only if the processor is online.

- **Utilization %:** The processing load on this processor for the last second, expressed as a percentage.
- **Interrupts Processed:** The number of interrupts fired on this processor in the last second.
- **Time Spent in Interrupts Last Second, in Microseconds:** The amount of time in microseconds that the processor spent processing interrupts in the last second.
- **Number of Bound Threads:** The number of threads that have been bound to this processor. Threads that are bound to a processor run only on that processor. Unbound threads can be migrated from one processor to another when required.

Processors Trend View

You can access the Trend View for the Processors object container after expanding the following server objects: Devices > Processors. This view displays the following graph for each processor:

- **CPU Utilization (avg. %):** The processing load on the processor for the last second, expressed as a percentage. This information is displayed only if the processor is online.

Storage Devices

You can get detailed information about the disk drives in a managed server, including disk size in megabytes, disk types, block size, and so on.

You can also view partition information for each disk drive. Partition information is especially informative because you can determine whether a partition is fault tolerant and whether the hard disk is losing data integrity.

Fault tolerance of a NetWare partition is part of the detailed information provided by ZfS server management. To determine whether a hard disk is losing data integrity, examine the redirected area. A number in the redirected area indicates the number of data blocks that have been redirected to the Hot Fix Redirection Area to maintain data integrity. The higher the redirected area number, the more faulty blocks there are on the hard disk. A redirected area growing over a period of time indicates a hard disk going bad.

On a NetWare server managed by the Management Agent for NetWare or a Windows NT server managed by the ZfS management agent, the Agent automatically gathers trend data on CPU usage, memory usage, and network interface traffic. In ZfS, you can view current trend data, or historical trend data by hour, day, month, or year. Monitoring trend data helps you with tasks such as setting alarm thresholds, determining who is using the server and when the server is used heavily, troubleshooting problems, balancing loads across multiple servers, and planning resources.

You can display the following views of information about the storage devices on your managed servers:

- "Storage Devices Summary View" on page 186
- "Storage Device Summary View" on page 187
- "Storage Devices Trend View" on page 188

Storage Devices Summary View

You can select the Summary View for the Storage Devices container object after expanding the following server objects: Devices > Storage Devices. This view provides the following information for each storage device on the server:

- **Disk Name:** The name of the disk drive.
- **Size (KB):** The total size of the disk drive in kilobytes.
- **Access:** Whether the disk drive is readable and writable or just readable.
- **Status:** Whether the disk drive is operational.

- **Type:** The type of media. Media types can include hard disk, floppy disk, tape, optical disk (read-only, write once read many, and read/write), or RAM disk. If unidentifiable, other or unknown is listed in this field.
- **Driver Description:** The name of the driver used by the disk drive.
- **Block Size:** The number of blocks used on the disk in kilobytes.
- **Heads:** the number of read/write heads on the disk drive.
- **Cylinders:** The number of cylinders on the disk drive.
- **Sectors/Track:** The number of sectors per track on the disk drive.
- **SCSI Target ID:** The target address for SCSI controllers or the unit number for other devices and the logical unit number for SCSI devices or the number zero for other devices.

Storage Device Summary View

You can display the Summary View for an individual storage device by expanding the following server objects: Devices > Storage Devices > *storage_device_x*. This view displays the following information:

- **Disk Name:** Name of the disk drive.
- **Logical ID:** The number assigned to a logical partition for identification.
- **Physical ID:** The number assigned to a physical partition for identification.
- **Type Partition:** The type of partition, including DOS, NetWare, and UNIX* partitions.
- **Size (KB):** The size of the partition, in kilobytes.
- **Redirection Area:** The size of the entire Hot Fix Redirection Area.
- **Redirected Area:** The number of bad blocks Hot Fix found.
- **Reserved Area:** The number of Hot Fix redirection blocks reserved for system use.
- **Fault Tolerance:** The type of fault tolerance used. The possible fault tolerance types are duplex and mirrored. If there is no fault tolerance, this field contains the value None.

Storage Devices Trend View

You can select the Storage Devices Trend View after expanding the following server objects: Devices > Storage Devices. This view provides the following information:

- **File System Reads (#/min):** Depicts the number of file system reads made per minute on multiple or single storage devices.
- **File System Writes (#/min):** Depicts the number of file system writes made per minute on multiple or single storage devices.
- **File System Reads (KB/min):** Depicts the number of file system reads per kilobyte volume made on multiple or single storage devices.
- **File System Writes (KB/min)** Depicts the number of file system writes per kilobyte volume made on multiple or single storage devices.
- **Free Redirection Area (%):** Depicts the percentage of total volume allocated to the disk redirection area.

Adapters

You can get detailed information about the network and disk adapters in a managed server, including I/O port, memory address, and interrupt configuration.

You can use this data to detect configuration problems such as the same address or interrupt is configured for two boards inside the server, or for a board and a component of the server's hardware. No two boards can use the same I/O port, memory address, and interrupt.

Problems with LAN adapters cause network problems, such as servers and workstations not being able to communicate. You can use the data collected on the LAN adapter to determine whether the frame type used by a network board is bound to a supported protocol. (A single network board might be bound to several protocols.) You can immediately tell whether a problem is due to something as simple as using the wrong frame type on the workstation (for example, an Ethernet_II frame type on the server and the Ethernet_802.2 frame type on the workstation).

You can display the following views of information about the adapters on your managed servers:

- "Adapters Summary View" on page 189
- "Adapters Trend View" on page 189

Adapters Summary View

You can select the Adapters Summary View after expanding the following server objects: Devices > Adapters > *adapter_x*. This view provides the following information:

- **Description:** The type of adapter hardware. This field can include the following types of information: manufacturer, model, and version. Or, for network boards, this field may contain a short board name and the board's burned-in MAC address.
- **Type:** The type of adapter (for example, network card or disk storage).
- **Devices Attached:** The number of devices associated with an adapter (for example, the number of drives attached to the disk controller).
- **Driver Description:** Description of the driver for this adapter.
- **Version:** The version number of the driver software.
- **Interrupt Number:** The unique interrupt number used by the adapter.
- **I/O Port:** The unique I/O port block used by the adapter.
- **Memory:** The unique memory address space used by the adapter.
- **DMA:** The Direct Memory Access (DMA) Channel used by the adapter.
- **Slot:** The slot in which the adapter is installed.

Adapters Trend View

You can select the Adapters Trend View after expanding the following server objects: Devices > Adapters > *adapter_ x*. This view provides the following graphs:

- **LSL Packets Received:** Depicts the number of LSL packets received by the adapter.
- **LSL Packets Transmitted:** Depicts the number of LSL packets transmitted by the adapter.
- **Packets Received:** Depicts the total number of packets received by the adapter.
- **Packets Transmitted:** Depicts the total number of packets transmitted by the adapter.

Threads

You can display information for all threads currently running on a managed server. A thread is recognized as an independent unit of execution.

You can display the following view of information about the threads on your managed servers:

- "Threads Summary View" on page 190

Threads Summary View

You can select the Threads Summary View after expanding the following server objects: Operating System > Kernel > Threads. This view provides the following information:

- **Name:** The application thread name.
- **Share Group:** The Application share groups and their associated threads and shares.
- **Parent Module:** Module (NLM) associated with this thread.
- **State:** The state of the thread, which can be one of the following: initializing, invalid, ready, running, suspended, terminated, or zombie.
- **Suspended Due To:** Reason the thread is suspended. If the thread is not in a suspended state, this field is blank.
- **Execution Time, Microseconds:** Amount of time in the last second that the processor spent executing the thread's code.
- **Stack Size, Bytes:** Size of the thread's stack.
- **Soft Affinity:** Processor on which the thread preferentially executes, but from which it can migrate when necessary.
- **Hard Affinity:** Indicates whether the thread is explicitly bound to a specified processor for the thread's lifetime. If the thread runs only on a specified processor, it is able to exploit the processor's cache state. If the thread is allowed to run on any available processor, the field value is zero.

Interrupts

You can display information for the registered interrupts on a managed server. On a multiprocessing system, interrupt information is displayed for all processors combined and individually for each online processor.

You can display the following views of information about the interrupts on your managed servers:

- "Interrupts Summary View" on page 191
- "Interrupts Service Routines View" on page 192

Interrupts Summary View

You can select the Interrupts Summary View after expanding the following server objects: Operating System > Kernel > Interrupts. This view provides the following information:

- **Name:** The name of the interrupt routine.
- **Interrupt Number:** Number for this service routine.
- **Processor:** Number of the processor.
- **Type:** The type of interrupt service routine. It can be one of the following:
    - **Bus:** A device I/O interrupt that is used (for example, by disk or LAN drivers).
    - **Local:** A hardware platform-specific interrupt local to an individual processor.
    - **System:** An interrupt category that is reserved for systems with unique interrupt requirements.
    - **Interprocessor:** An interrupt that is generated by one processor to affect another processor.
    - **Timer:** An interrupt that provides timer services for the OS as well as preemption support. (In multiprocessing systems, timer interrupts are local to a processor.)
- **Service Routines:** Number of service routines that are launched when this interrupt occurs.
- **Interrupt Occurrences:** Number of times in the last second that the interrupt occurred and was processed.
- **Execution Time:** Amount of time in the last second that the processor spent processing this interrupt.
- **Spurious Interrupts:** Number of times since the server started that an interrupt fired that should not have occurred.

Interrupts Service Routines View

The Interrupts Service Routines View provides information about the memory address spaces defined on the server.

NetWare runs in the OS address space (kernel), along with LAN drivers, storage device drivers, MONITOR, and network management agents (NMAs). OS address space is backed by physical memory.

All other address spaces are user space (ring 3) and are backed by virtual memory. Applications running in user space cannot cause the server to abend if the address space faults.

You can select the Service Routines View after expanding the following server objects: Operating System > Kernel > Interrupts. This view provides the following information:

- **Name:** The name of the interrupt service routine.
- **Service Routine Number:** Service Routine Number associated with this service routine.
- **Processor Number:** Processor number this routine is running on.
- **Interrupt Number:** Interrupt number associated with this service routine.
- **Interrupts Processed Last Second:** Number of interrupts that were processed by the ISR during the last second.

Memory

You can display the following views of information about the memory on your managed servers:

- "Memory Summary View" on page 192
- "Memory Trend View" on page 193
- "Disk Cache View" on page 193
- "Virtual Memory View" on page 195

Memory Summary View

You can select the Memory Summary View after expanding the following server objects: Operating System > Kernel > Memory. This view provides the following information:

- **Type:** The type of memory (for example, DOS, allocated memory, cache buffers, or code and data memory).
- **Unit Size (bytes):** The size of the memory allocation.
- **Total (KB):** The number of memory units × the unit size.
- **Units Used:** The number of memory units that have been allocated.
- **Used (KB):** The number of KB of memory that has been allocated.

The Memory Summary View also provides a pie chart depicting memory usage on the system.

Memory Trend View

You can select the Memory Trend View after expanding the following server objects: Operating System > Kernel > Memory. This view provides the following graphs:

- **Cache Buffers (%):** The percentage of memory allocated to cache buffers.
- **Code and Data Memory (%):** The percentage of memory allocated to code and data.
- **Allocated memory (%):** The amount of allocated memory.
- **Dirty Cache Buffers (%):** The amount of dirty cache buffer memory.

Disk Cache View

This view displays utilization for disk cache memory. Use cache utilization statistics to determine when you need to install more RAM for cache. You can select this view after expanding the following server objects: Operating System > Kernel > Memory. It provides the following information:

- **Short Term Cache Hits %:** Percentage of requests in the last second for disk blocks that were already in cache memory. When the requested data is already in memory, disk reads don’t need to be made. If this value falls below 98%, consider installing more RAM for cache. Also compare with Long Term Cache Hits.
- **Short Term Cache Dirty Hits %:** Percentage of requests in the last second for disk blocks that were already in cache memory but were dirty. Dirty cache must be written to disk before being used. Also check Long Term Dirty Cache Hits and LRU Sitting Time.

- **Long Term Cache Hits %:** Cumulative percentage of requests for disk blocks that were already in cache. When the requested data is already in memory, disk reads don't need to be made. Use this cumulative percentage to assess overall disk cache utilization. If this value falls below 90%, install more RAM for cache.
- **Long Term Cache Dirty Hits %:** Cumulative percentage of requests for disk blocks that were already in cache memory but were dirty. (Before dirty cache can be used, it must be written to disk.) Use this cumulative percentage to assess overall disk cache utilization. If this value is high or steadily incrementing, add more RAM for cache. Also check LRU Sitting Time.
- **Total Cache Blocks Allocated:** Cumulative number of requests for disk cache blocks that have been made since the server was started or rebooted. This value is the sum of the values of Allocated from Available List and Allocated from Least Recently Used (LRU). If the value of Allocated from Available is much higher, the server has sufficient RAM for cache. If the value of Allocated from LRU is high, install more RAM for cache.
- **Cache Blocks Allocated from Available List:** Number of requests for disk cache blocks that were filled by blocks in the available list (blocks that were not being used). When there are no free blocks available, requests are filled from the LRU list of cache blocks. If this value is much higher than the Allocated from LRU value, the server has sufficient RAM for cache.
- **Cache Blocks Allocated from LRU:** Number of requests for disk cache blocks that were filled by blocks from the Least Recently Used cache blocks. The system writes pending requests from the LRU cache block to disk then frees the block for the current request. Because LRU caches used only when no other cache is available, a steadily incrementing count indicates more RAM is needed.
- **Number of Times in Last 10 Minutes that the OS Had to Wait:** Number of times in the last 10 minutes that the OS waited for an LRU block in order to fulfill a request. If this value is greater than 7, install more RAM for cache.
- **Number of Times OS Had to Wait:** Number of times that the OS waited for an LRU block in order to fulfill a request.
- **Total Number of Times the Write Request Was Delayed:** Number of times a write request was delayed because there were too many writes to perform or because the disk channel was busy. A high value indicates

either that the disk channel has too much I/O traffic or that you need to install more RAM for cache.

- **Number of Times the Request Was Re-tried:** Number of times a disk cache request had to be retried because the target block was being used. If this value is high or steadily incrementing, install more RAM for cache.

Virtual Memory View

This view displays information about the virtual memory system. Use these statistics to monitor the efficiency of server memory usage. If these values are fairly stable over time and if server performance is satisfactory, the server has adequate memory for its load. For example, if the value of Page faults increases, this indicates that the server performance is degrading. Conversely, if the Free swap pages value increases, it is an indication of better server performance.

You can select this view after expanding the following server objects: Operating System > Kernel > Memory. It provides the following information:

- **Total Page-In Requests:** Number of requests that were made to move virtual memory from swap files since the server was started (server up time).
- **Page-In Requests in Last 5 Seconds:** Number of requests to move 4 KB virtual memory pages from swap files.
- **Total Page-Out Requests:** Number of requests that were made to move virtual memory to swap files since the server was started (server up time).
- **Page-Out Requests in Last 5 Seconds:** Number of requests to move 4 KB virtual memory pages to swap files.
- **Total Swap Pages:** Number of 4 KB pages in this server’s virtual memory system. (The size of the swap file in memory pages is the total number of bytes divided by 4 KB.) The size of the swap file grows or shrinks dynamically to match the memory requirements of the server’s load.
- **Free Swap Pages:** Number of 4 KB pages that are available for use by the virtual memory system.
- **Reserved Swap Pages:** Number of 4 KB pages that are reserved by the virtual memory system.
- **Total Page Faults:** Number of times the virtual memory system retrieved from the swap file since the server was started (server up time).

- **Page Faults in Last 5 Seconds:** Number of times in the last five seconds that the virtual memory system retrieved from the swap file. (This means that accessed memory wasn't backed by physical memory.)

Address Spaces

NetWare runs in the OS address space (kernel) along with LAN drivers, storage device drives, MONITOR, and network management agents (NMAs). OS address space is backed by physical memory.

All other address spaces are user space (ring 3) and are backed by virtual memory. Applications running in user space cannot cause the server to abend if the address space faults.

You can display the following view of information about address spaces on your managed servers:

- "Address Spaces Summary View" on page 196

Address Spaces Summary View

You can select the Address Spaces Summary View after expanding the following server objects: Operating System > Kernel > Address Spaces. This view provides the following information:

- **Name:** Name of the virtual memory address space where this module runs.
- **Number of NLMs Loaded:** Count of NLM programs loaded in this address space. NetWare, LAN drivers, storage device drivers, MONITOR, and Network Management Agents (NMAs) are loaded in OS address space (kernel). A server application, such as GroupWise®, Lotus Notes*, or an Oracle* database, can be loaded in its own address space (user space or ring 3).
- **Mapped Pages:** Total number of physical memory pages backing this address space. Note that the OS address space (kernel) is the only address space backed by physical memory.
- **Restarted:** Total number of times this address space faulted and restarted automatically. A value of zero (0) indicates that no fault has occurred. A non-zero value indicates that an address space has faulted and recovered. Follow online Troubleshooting documentation for core dump instructions for address spaces.
- **Memory in Use, Bytes:** Amount of allocated memory in use.

- **Memory Not in Use, Bytes:** Amount of unused allocated memory.
- **Memory As Overhead, Bytes:** Amount of memory used for managing the allocation pool plus the amount of memory fragmentation.
- **Total Blocks:** Number of memory blocks that are in use and that are available at the request of the NLM.
- **Blocks in Use:** Number of memory blocks that were allocated and used.
- **Block Not Used:** Number of memory blocks that were allocated but not used.

Network

You can display the following view of information about the network activity on your managed server:

- "Network Trend View" on page 197

Network Trend View

You can access the Trend View for the Network object container after expanding the following server objects: Operating System > Network. This view displays the following graph for each network adapter:

- **Packets Received (KB/min):** The number of kilobytes received by the adapter for the last minute.

Interfaces

You can display the following view of information about the network interfaces on your managed server:

- "Interfaces Summary View" on page 197
- "Interfaces Statistics View" on page 198

Interfaces Summary View

You can access the Summary View for the Network object container after expanding the following server objects: Operating System > Network > Interfaces.

This view displays the following information:

- **Frame Type:** The frame type that is bound to this logical board.
- **MAC Address:** The MAC address of the interface.

- **Description:** Text describing the interface board.
- **Line Speed:** The number of bits per second transmitted on this board.
- **Type:** The type of interface (for example, Ethernet CSMACD).
- **Logical Board #:** The number assigned to this logical board.
- **Logical Board Name:** The name assigned to this logical board.
- **Protocols:** The protocols to which the logical board is bound (for example, IP, ARP, or IPX).

Interfaces Statistics View

You can access the Statistics View for the Network object container after expanding the following server objects: Operating System > Network > Interfaces.

This view displays the following information:

- **Frame Type:** The frame type that is bound to this logical board.
- **MAC Address:** The MAC address of the interface.
- **MTU:** The size of the largest datagram which can be sent/received on the interface.
- **Admin Status:** The desired state of the interface.
- **Oper Status:** The current operational state of the interface.
- **Bytes In:** The total number of bytes received on the interface.
- **Bytes Out:** The total number of octets transmitted out of the interface.
- **Ucast Packets In:** The number of subnetwork-unicast packets delivered to a higher-layer protocol.
- **Ucast Packets Out:** The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address.
- **Nucast Packets In:** The number of non-unicast packets delivered to a higher-layer protocol.
- **Nucast Packets Out:** The total number of packets that higher-level protocols requested be transmitted to a non-unicast address.
- **Discards In:** The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.

- **Discards Out:** The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
- **Errors In:** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **Errors Out:** The number of outbound packets that could not be transmitted because of errors.
- **Unknown Protocols In:** The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.

The Clear Counters button in this view resets the values only on the Management Console and not on the Server. This is done to enable the user to get the current data from the server.

Connections

You can display the following views of information about the connections on your managed server:

- "Connections Summary View" on page 199
- "Connections Trend View" on page 201
- "Open Files View" on page 201

Connections Summary View

The Connections Summary View displays information and statistics for the connections on the selected server. For example, this view displays the number of files currently being accessed by the server and by other clients. Certain files, such as hidden files that support eDirectory, are always open. You can select this view after expanding the following server objects: Operating System > Network > Connections > *connection_x*.

This view provides the following information:

- **Connection# Login Name:** A string indicating the connection number and login name. Note that connection 0 (zero) is used by the system. The login name is the eDirectory full distinguished name where applicable.
- **Client Address:**

  IP: *xxx.xxx.xxx.xxx:port number*
  IPX: *network:node:socket*

- **Connection Time:** The date and time the connection was established.
- **Privileges:** A connection can have one or more of the following privileges:
  - Supervisor
  - Operator
  - Auditor
  - High_Privilege
  - Second_Authentication
  - Second_High_Privilege
- **Status:** The status can be one of the following:
  - Not logged in
  - Logged in
  - Need security change
  - MacStation
  - Connection abort
  - Audited
  - Authenticated temporary
  - Audit connection recorded
  - DS audit connection recorded
  - Logout in progress
- **Read (bytes):** Number of bytes the connection has read since it was established.
- **Written (bytes):** Number of bytes the connection has written since it was established.
- **NCP Requests:** Number of NCP requests the connection has made since it was established.
- **Open Files:** Number of files that are currently opened by the connection.
- **Locked Records:** Number of file records that are currently locked by the connection.

Connections Trend View

You can select the Connections Trend View after expanding the following server objects: Operating System > Network > Connections > *connection_x*. This view provides the following graphs:

- **Connections (avg. #):** The average number of connections over the last sample interval.

Open Files View

The Connection Open Files View displays information and statistics for the connection on the server. For example, this view displays the number of files currently being accessed by the server and by other clients. Certain files, such as hidden files that support eDirectory, are always open. You can select this view after expanding the following server objects: Operating System > Network > Connections > *connection_x*. This view provides the following information:

- **File Name:** The name of the open file, including the directory path.
- **Login Name:** The name of the user (if any) who opened the file. If the file was opened by the system or by an NLM, the Login Name will be a zero-length string.
- **Volume Name:** The physical name of the NetWare volume containing the open file.
- **Directory Number:** A number that uniquely identifies an open file within a NetWare volume.
- **Volume ID:** A number that uniquely identifies a NetWare volume. The value of this object for a particular volume has the same value as the nwVolID object for the same volume.

Users

You can display the following views of information about the users on a selected server:

- "Users Summary View" on page 201
- "Users Trend View" on page 202

Users Summary View

The Users Summary View provides information about the users who access the selected server. You can select this view after expanding the following server objects: Operating System > Users. This view provides the following information about each user:

- **Login Name:** The login name of the user.
- **Disk Usage:** The amount of disk space the user has used.
- **Last Login:** The date the user last logged in to the server.
- **Account Status:** Indicates whether the user account is valid.
- **Password:** Indicates whether the user's password is valid.
- **Real Name:** The user's eDirectory real name.
- **Bad Login:** The number of failed login attempts for the user.
- **Bad Login Address:** The network address of the location from which the user login failed, if any.

Users Trend View

The Users Trend View provides information about the users who access the selected server. You can select this view after expanding the following server objects: Operating System > Users. This view provides the following graph:

- **Logged-In Users (avg. #):** Depicts the average number of users logged in to the server.

Installed Software

You can display the following view of information about the software that is installed on a selected server:

- "Installed Software Summary View" on page 202

Installed Software Summary View

The Installed Software Summary View provides information about the software installed on the selected server. You can select this view after expanding the following server objects: Operating System > Installed Software. This view provides the following information:

- **Name:** The name of the installed software module.
- **Type:** The type of software (for example, device drivers, applications, or operating system).
- **Date Installed:** The date the software was installed.

NLM

You can display the following views of information about the NLM software on a managed server:

- "NLM Summary View" on page 203
- "Resource Tag View" on page 203

NLM Summary View

The NLM Summary View provides information about a selected NLM. You can select this view after expanding the following server objects: Operating System > NLMs > *nlm_x*. This view provides the following information:

- **Name:** The name of the NLM.
- **Version:** The version number of the NLM.
- **Released:** The date and time the NLM was released.
- **Memory (bytes):** The total memory in bytes used by this NLM. This is a composite total of short term memory, semi-permanent memory, and non-movable memory, cache memory allocated by the NLM plus the sizes of the code, and data sections of this instance of an NLM.
- **Description:** A text string that describes the NLM.
- **Copyright:** The copyright string for the NLM.

Resource Tag View

You can select the NLM Resource Tag View after expanding the following server objects: Operating System > NLMs > *nlm_x*. This view provides the following information:

- **Description:** The name that the owning module assigned to this resource tag.
- **Number in Use:** The number of instances of the resource tag.
- **Resource Type:** The type of resource tag that is being tracked (for example, semaphores or processors).
- **Address Space:** Name of the address space where the module that owns the resource tag is running.

Volumes

NetWare server disk storage space is divided into volumes. You can view various data about the volumes mounted on a server, such as size, free space, how the volumes are distributed across disks, and which users are using the space. For individual volumes you can view data on configuration, open files, segments, and usage. The available views of data include:

- "Volume Summary View" on page 204
- "Volume Trend View" on page 205
- "Open Files View" on page 205
- "Volume Segment View" on page 206
- "Volume Usage View" on page 206

Volume Summary View

The Volume Summary View provides details about a single volume. You can select this view after expanding the following server objects: Services > File > Volumes > *volume_x*. This view provides the following information:

- **Size (KB):** The size of the volume in kilobytes.
- **Free (KB):** The amount of free space on the volume in kilobytes. As files are added or expanded, this number approaches zero. A pie chart shows you how much of the total volume size is free.
- **Used (KB):** The amount of space, which is determined by subtracting the free disk space from the total volume size.
- **Status:** Whether the volume is mounted. If the volume is not mounted, only the volume name is listed.
- **Namespaces:** Namespaces that are supported on the volume. Namespaces supported are DOS, Macintosh*, NFS*, FTAM, OS/2*, and NT.
- **Attributes:** Attributes of the volume. Possible attributes are block sub-allocation, file compression, data migration, auditing, and read-only. A volume can have a combination of attributes, such as read-only volume with block sub-allocation.
- **# Logical Segment:** The number of segments comprising this volume.
- **DS Name:** The volume's full Directory Services distinguished name or a zero-length string if not applicable.

- **Non-Purgable:** The amount of space (in kilobytes) taken by the deleted files whose purge dates have not yet expired. Non-purgable space can be reclaimed as free space when the deleted files become eligible to be purged.
- **Block Size:** The block size on the volume in bytes.
- **Dir Slots:** The total number of directory table entries available on the volume.
- **Used Dir Slots:** The number of directory table entries that are currently in use.
- **File System Name:** The type of file system on the volume is either remote or local. The File System Name value is listed only if the volume is remote. In this case, the file system name is the remote mount point; for example, SITE1:/usr/x.

Volume Trend View

You can select the Volume Trend View after expanding the following server objects: Services > File > Volumes > *volume_x*. This view provides the following graph:

- **Volume % Free Space:** The percentage of space still available on the volume.

Open Files View

The Volume Open Files View displays a table of all open files on the volume. If it is opened by more than one connection, multiple entries for the same file will appear in the table. You can select the Open Files View after expanding the following server objects: Services > File > Volumes > *volume_x*. This view provides the following information:

- **File Name:** The name of the open file, including the directory path.
- **Connection #:** The number of the connection that opened the file.
- **Login Name:** The name of the user (if any) who opened the file. If the file was opened by the system or by an NLM, the Login Name will be a zero-length string.
- **Directory Number:** A number that uniquely identifies an open file within a NetWare volume.
- **Volume ID:** A number that uniquely identifies a NetWare volume.

Volume Segment View

The Volume Segment View provides information about the segments on a volume. You can select this view after expanding the following server objects: Services > File > Volume > *volume_x*. As long as the Volume Segment View is displayed, the server is polled for data and the view is constantly updated with real-time information. This view provides the following information about each segment on the selected volume:

- **ID:** The number assigned to the volume segment for identification.
- **Logical Partition ID:** The number assigned to a logical partition for identification.
- **Physical Partition ID:** The number assigned to a physical partition for identification.
- **Size:** The size of the segment.
- **Fault Tolerance:** The type of fault tolerance used on the segment. Possible types are duplex and mirrored. If there is no fault tolerance, the value is None.
- **Disk Drive:** The name of the disk drive on which the segment resides.

Volume Usage View

The Volume Usage View provides information about the amount of volume space in use per user. As long as the Volume Usage View is displayed, the server is polled for data and the view is constantly updated with real-time information.You can select this view after expanding the following server objects: Services > File > Volumes > *volume_x*. This view provides the following information per volume user:

- **Used KB:** Number of kilobytes currently in use.
- **Limit KB:** Number of kilobytes to which a user is limited.
- **User Name:** The user’s login name.

Queues

You can display the following views of information about the NLM software on a managed server:

- “Queues Summary View” on page 207
- “Queue Summary View” on page 207

- "Queue Trend View" on page 208

Queues Summary View

The Queues Summary View provides the following information about the print queues on the managed server:

- **Queue Name:** The name of the queue.
- **Type:** The type of queue (for example, archive queue, job queue, or print queue).
- **# Jobs:** The number of print jobs in the queue currently.
- **# Print Servers:** The number of print servers serviced by the queue.
- **Volume:** The volume where the queue resides.
- **Add Job State:** Indicates whether or not the queue can add jobs.
- **Attach State:** Indicates whether or not the queue can attach.

Queue Summary View

The Queue Summary View provides the following information about the print jobs in the selected queue:

- **Job #:** A unique number assigned to the print job.
- **Position:** The print job's order in the print queue.
- **Bytes:** The number of bytes to be printed.
- **Description:** A description of the print job.
- **User:** The username of the user who submitted the job.
- **Entry Time:** The time the job was added to the queue.
- **Control Flags:** A value representing the control flags for the job. For example, some possible control flags are service auto start, execute, user hold, or operator hold.
- **Target Time:** The date and time the job is to be printed.
- **Target Server:** The target server for the job.
- **Actual Server:** The name of the server currently processing the job.

Queue Trend View

The Queues Trend View provides the following graph for each queue on the managed server:

- **Wait Time of Next Ready Job (sec):** The average length of time the next job waits in the queue.

Printers

You can get the detailed information about the printers installed in a managed server, including printer name, port, driver and description, status, error conditions, etc. You can display the following views of information about the processors on your managed servers:

- "Printer Console View" on page 208
- "Printer Summary View" on page 208

Printer Console View

You can access the Console View for the Printers object container after expanding the following server objects: Devices > Printers. This view displays the following information for each printer object in the container:

- Printer Name: Name of the printer

Printer Summary View

You can display the Summary View for an individual printer by expanding the following server objects: Devices > Printer > printer_x. This view displays the following information:

- Printer Name: The name of the printer
- Printer Status: The current status of this printer device. The status can be idle, printing, warm-up, or unknown state.
- Error Condition: The error conditions include lowPaper, noPaper, lowToner, noToner, doorOpen, jammed, offline, or serviceRequested.

Other Devices

From this view, you can get other devices like the keyboard and the mouse installed on a managed server.

- "Other Devices on Console View" on page 209

Other Devices on Console View

This displays other devices like the keyboard and the mouse.

The information about the keyboard includes:

- Keyboard Name
- Keyboard Type
- Driver Name
- Class
- Bus Type

The information about the mouse includes:

- Mouse Name
- Mouse Type
- Driver Name
- Class
- Bus type

Ports

From this view, you can install serial ports and parallel ports on a managed server.

- "Ports Console View" on page 209

Ports Console View

This displays information about the serial ports such as COM ports and parallel ports such as LPT ports. The information about the ports includes:

- Port Name
- Controller
- Bus Type

6 Using the MIB Tools

ZENworks® for Servers (ZfS) provides the tools to manage Simple Network Management Protocol (SNMP)-manageable devices on your network. This section describes the Management Information Base (MIB) tools, the SNMP MIB Compiler and the SNMP MIB Browser. It also explains how to set up and use the tools. See the following sections for more information:

- "Understanding MIB Tools" on page 211
- "Configuring MIBs and Setting Up MIB Tools" on page 224
- "Using the MIB Browser" on page 227
- "Maintaining MIBs" on page 239

Understanding MIB Tools

The following sections provide information about the tasks required for managing SNMP devices using the MIB Compiler and the MIB Browser.

- "About MIBs" on page 211
- "Understanding the SNMP MIB Compiler" on page 212
- "Understanding the SNMP MIB Browser" on page 213
- "Managing Devices with MIB Tools" on page 216
- "Trap Definitions" on page 216

About MIBs

To manage a device, you must obtain a copy of the MIB or MIBs that the device supports. A MIB is an ASCII text file, written in a precise format that describes the management information available on a particular class of devices. If, for example, you have an XYZ router from company X and you want to use ZfS for managing the router, company X must provide you with the XYZ router MIB. ZENworks for Servers provides many standard and vendor-proprietary MIBs, which are found in the MIB Pool folder in the MIB Server Pool folder. By default, ZfS compiles the most generally applicable of these MIBs.

If you want to compile any new MIBs, you must store them in the MIB Pool folder in the MIB Server Pool folder. The console user can select or remove MIB files from the MIB Pool folder in the MIB Server Pool folder. The MIB Compiler compiles the files listed in the MIB Pool folder in the MIB Server Pool folder.

Understanding the SNMP MIB Compiler

The MIB Compiler does the following:

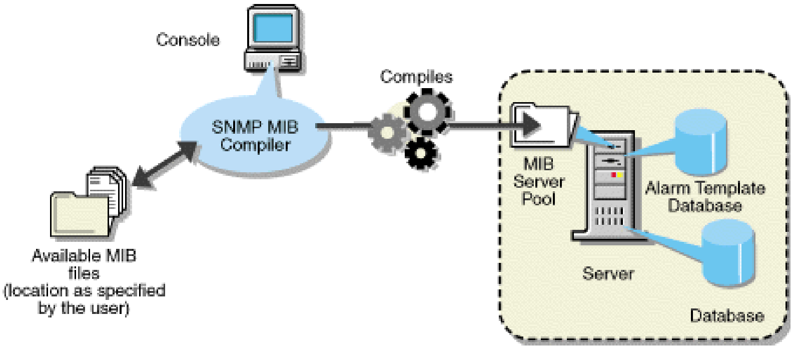
- Parses a set of predefined SNMP MIB files written in ASN.1 and SNMP V2 syntax and verifies their syntax.
- Stores the compiled files in the ZfS database, which lets all users access these compiled files from a central location.

  From the console, you can easily compile and maintain the MIB files located in the MIB Server Pool. You can add or remove MIB files from the MIB Pool.
- Updates trap definitions in the alarm template database.

  The MIB Compiler lets you introduce new SNMP alarm templates into ZfS so they can be recognized and interpreted as alarms when they arrive at the console.

  The Alarm Management System (AMS) interprets the annotations to trap definitions in a MIB to set the severity level and device status assigned to an alarm. The MIB files included with ZfS are already properly annotated.

The following figure demonstrates how the MIB Compiler incorporates information from the MIB files into the ZfS database:



During installation of ZfS, the MIB files that are precompiled using the MIB Compiler are also installed. The MIB for any SNMP node you want to manage must be compiled with ZfS. You can also integrate third-party MIBs. If you obtain a MIB file from a third-party vendor or any MIB file that was not installed with ZfS, you must compile the file using the MIB Compiler.

Using Role-Based Services with the MIB Compiler

ZfS role-based services let you assign various roles to users on your network. If your role is assigned the Enable MIB Compiler task, you can use the MIB Compiler.

See "Role-Based Administration" on page 34 for more information about the role-based administration provided by ZfS.

Understanding the SNMP MIB Browser

The MIB Browser lets you manage SNMP-instrumented devices on the network.

To use this tool, you must have knowledge of SNMP and a good understanding of the structure of MIBs. Using the MIB Browser, you can manage nodes on the network by setting values of the MIB objects at the target nodes.

If you are familiar with the structure of an SNMP MIB, you can use the MIB Browser to retrieve data from SNMP-manageable node.

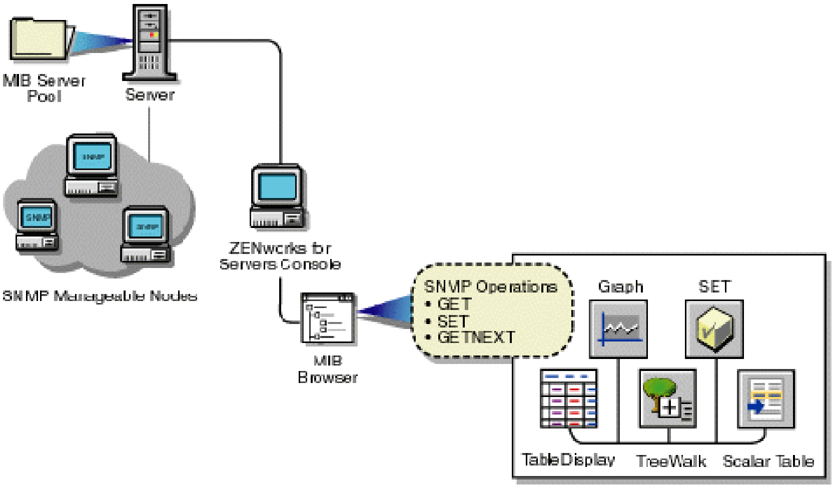
The MIB Browser lets you communicate with devices through an SNMP agent on the network over the User Datagram Protocol (UDP) or the Internet Protocol (IP). The results of SNMP commands are displayed in the MIB Browser window.

An SNMP agent is a program that provides access to management data about a particular network device and responds to SNMP Manager requests for the data. The NetWare® Management Agent software is an example of an SNMP agent that resides on a NetWare server. An SNMP agent resides in each manageable device on the network.

Although many ZfS windows display data retrieved from SNMP-manageable nodes, some administrators prefer the capability the MIB Browser provides for specifying the type of data they want to retrieve. Additionally, by using the MIB Browser, you can obtain some SNMP data that is not displayed in ZfS windows.

The MIB Browser takes the compiled MIB and displays the objects in a tree format. The MIB Browser also lets you walk the tree and look for the definitions of the selected MIB objects. You can set the community string to be used in the conversation between ConsoleOne® and the SNMP-manageable node to manage the device.

The following figure demonstrates the functionality of the MIB Browser:



The MIB Browser does the following:

- Represents the MIB information as a tree.

You can browse the objects in the MIB tree, which displays the composite OID (object identifier) for all compiled MIBs. The OID is the sequence of integers labeling each object on the path from the root of the tree to every object on the branches. The OID also describes the location of the object in the tree. For example, the novell(23) object in the tree is described as 1.3.6.1.4.1.23. For more information on the MIB tree, see "Browsing the MIB Tree" on page 227.

- Retrieves specific information about the node using the SNMP GET and GETNEXT commands.

  The MIB information is displayed as:

  - A table display for tabular objects

    You can add new rows to the table and issue SNMP SET commands to update the columnar values of the table. For more information, see "Modifying Instances of an SNMP Table" on page 232.

  - A graph display

    If you choose to plot the SNMP requests, the Graph window displays the polled data of one or more MIB objects. For more information, see "Graphing SNMP Request Results" on page 236.

  - A scalar table display

    You can form a scalar table by combining scalar objects. You can modify the scalar entries of the table. For more information, see "Forming Tables of Scalar Objects" on page 235.

  - A TreeWalk display

    You can browse the OID values of scalar and tabular objects. For more information, see "Viewing the Values of an Object and Its Child Nodes" on page 229.

- Changes the information at the target node using the SNMP SET command.

  You can retrieve or change the value of MIB objects if the community strings match at the target node. The node should also allow remote setting of its variables.

- Creates a profile by saving the properties of the table, scalar table, or graph.

  You open the profile to view a table, scalar table, or graph of different SNMP-manageable nodes on the segment with the properties specified in the profile. For more information, see "Using a Profile for Tables and Graphs" on page 238.

For more information on the MIB Browser, see "Using the MIB Browser" on page 227.

Using Role-Based Services with the MIB Browser

ZfS role-based services let you assign various roles to users on your network. If your role is assigned the Enable MIB Browser task, you can use the MIB Browser.

See "Role-Based Administration" on page 34 for more information about the role-based administration provided by ZfS.

Managing Devices with MIB Tools

ZfS lets you manage any SNMP-manageable devices on the network. In particular, you can do the following:

- Set alarm templates for receiving alarms, often referred to as SNMP traps, for these devices
- Use the MIB Browser to display and set values on these devices

Before using the MIB Browser to manage the devices, you need to perform the following tasks:

1. Acquire the necessary MIBs.
2. Add trap annotations, if required.
3. Add or remove MIBs using the MIB Compiler.
4. Run the MIB Compiler to compile the MIBs in ZfS.

ASN.1 and SNMP V2 Support

The MIB Compiler supports all MIB files written in ASN.1 and SNMP V2 syntax. The MIB Compiler allows relaxation of ASN.1 syntax.

Trap Definitions

Some SNMP MIBs define the traps that a device can send to ConsoleOne when an unusual event occurs on the network. When you compile a MIB containing traps, information about those traps is added to the ZfS alarm database. When ZfS receives a trap, the information in the alarm database is retrieved and used by ZfS to generate the alarm summary string and to determine the alarm type, alarm severity, state of the affected device, and other details.

You can improve the presentation of the alarm information in ZfS by adding annotations to the trap definitions in the MIB files. These annotations are added as comments to the trap definitions so that the MIB compiles with third-party MIB compilers.

All Novell® MIBs are annotated. If you choose not to annotate the traps in other MIBs, ZfS displays the alarms; however, they are less readable. SNMP MIBs use the TRAP-TYPE macro to define traps.

This section covers the following topics:

- "Keywords for Trap Definitions" on page 217
- "Template Database" on page 218
- "Keywords for Trap Annotations" on page 218
- "Example Trap Definitions" on page 220
- "Displaying Annotated Traps in ZENworks for Servers" on page 222
- "Formatting the SUMMARY String" on page 222

Keywords for Trap Definitions

The following table explains a trap definition.

Keyword	Example	Explanation
TRAP-TYPE	dupIpxNetAddr	Specifies the name of the trap. For example, dupIpxNetAddr represents a duplicated IPX network address.
ENTERPRISE	netware-GA-alert-mib	Contains the OBJECT identifier of a node in the vendor's tree, which, together with the trap number (the 8 following the ::= in DESCRIPTION) uniquely identifies the trap.

Keyword	Example	Explanation
VARIABLES	(osName, osLoc, tiTrapTime, tiEventValue, tiEventSeverity, tiServer)	Defines an ordered sequence of MIB objects that are passed as parameters of the trap to provide additional information about the event. For example, osName is a text string specifying the name of the server sending the trap; osLOC is a text string specifying the location of the server; tiTrapTime is an integer specifying the time the event occurred.
DESCRIPTION	"Two servers use the same IPX Internet address."	Provides a textual description of the semantics of the trap.
Trap_number	: :=8	Defines the trap.

Template Database

The MIB Compiler populates the alarm template database with the trap definitions in the MIB files. Any traps from the agents are stored in the database.

Keywords for Trap Annotations

The following table lists and explains the keywords you can use to annotate traps:

Keyword	Explanation
–#TYPE	Short name for the alarm. The name can contain a maximum of 40 characters. If this annotation is not present, the SNMP trap name is used. Every trap should have a unique type.

Keyword	Explanation
--#SUMMARY	Description of the alarm with placeholders and formatting information for the actual parameters passed with the alarm. See “Formatting the SUMMARY String” on page 222 for more information. Without this annotation, the alarm summary string lists each SNMP parameter name followed by its value.
--#ARGUMENTS	List of parameters to substitute in the SUMMARY string. Parameters are substituted in the order in which they appear in the list. Each element of the list is the index (zero-based) of the parameter in the VARIABLES clause.
--#SEVERITY	Default severity assigned to the trap. This can be one of the following: ◆ INFORMATIONAL ◆ MINOR ◆ MAJOR ◆ SEVERE ◆ UNKNOWN Alarms with a default severity set to SEVERE are displayed in the ticker tape. Without this annotation, the severity is displayed as UNKNOWN.
--#TIMEINDEX	Index of the variable in the VARIABLES clause. This index contains the time when the alarm was generated. The time is expected to be an integer representing the number of seconds since 1970 (UNIX* time). If such a variable does not exist in the VARIABLES clause, use an index greater than the total number of variables in the VARIABLE clause.
--#HELP	This index contains name of the help file.
--#HELPTAG	The index contains the reference to the Help ID of the help file that is specified in the HELP index.

Keyword	Explanation
--#STATE	Default state of the object when the alarm was generated. This can be one of the following: ◆ OPERATIONAL ◆ NONOPERATIONAL ◆ DEGRADED ◆ UNKNOWN Without this annotation, the state is UNKNOWN.

Note the following rules about adding trap annotations:

- Each annotation must be embedded in a comment. Everything from the double hyphen to the end of the line is treated as a comment.
- Each annotation must be on a separate line.
- Annotations must appear in the order in which they are discussed in "Trap Definitions" on page 216.
- All annotations must be inserted after the DESCRIPTION clause and before the ::= clause.
- STATE and SEVERITY values are written to the alarm database the first time the MIB is compiled, so any changes you make by clicking Fault > Alarm Disposition are not overwritten. If you want to overwrite the existing values, you must run the SNMP Compiler from ConsoleOne.
- The variable filename is the name of the MIB file that you want to overwrite. The optional -S switch (silent mode) causes the MIB Compiler to run in the background. We recommend that third-party developers use silent mode.

Example Trap Definitions

The following sections explain a trap description in an SNMP trap before and after annotation:

- "Example Trap Definition Before Annotation" on page 221
- "Example Trap Definition After Annotation" on page 221

Example Trap Definition Before Annotation

```
dupIPXNetAddr     TRAP-TYPE
ENTERPRISE netware-GA-alert-mib
VARIABLES{osName, osLoc, tiTrapTime, tiEventValue, tiEventSeverity, tiServer}
DESCRIPTION"Two servers use the same IPX internetwork address."
::=8
```

Example Trap Definition After Annotation

```
dupIPXNetAddr     TRAP-TYPE
ENTERPRISE netware-GA-alert-mib
VARIABLES{osName, osLoc, tiTrapTime, tiEventValue, tiEventSeverity, tiServer}
DESCRIPTION"Two servers use the same IPX internetwork address."
::=8
– Trap annotations are as follows:
--#TYPE "Duplicate IPX address"
--#SUMMARY "%s at %s and %s are using the same IPX address"
--#ARGUMENTS {0,1,5}
--#SEVERITY CRITICAL
--#TIMEINDEX 2
--#HELP "MYHELP.HLP"
--#HELPTAG 60004
--#STATE DEGRADED
::=8
```

Displaying Annotated Traps in ZENworks for Servers

Assume that the dupIpxNetAddr trap shown in "Keywords for Trap Definitions" on page 217 was received by ZfS with the following variables:

- osName = SJM-JACK
- osLoc = JACK's CORNER
- tiTrapTime = ~700000000
- tiServer = SJM-TIM

To display a trap, use the Alarm Monitor or Alarm Disposition table. The following example shows the result:

Receive Time:03/04/99 09:15:45

Alarm Type: Duplicate IPX address

Summary: SJM-JACK at JACK's Corner and SJM-TIM are using the same IPX address

Severity: Critical

State: Degraded

When you select the alarm on the Alarm Report table and click the NetWare Expert button, ZfS displays help information for this alarm.

Formatting the SUMMARY String

The SUMMARY keyword in the trap annotation lets you provide the actual wording of the alarm summary. This wording is used by ZENworks for Servers when the alarm occurs.

Placeholders within the string are replaced by actual parameters of the trap before the string is displayed by ZENworks for Servers. Each placeholder format string begins with a percentage sign (%) and tells ZENworks for Servers how to format the parameter that will be substituted for the placeholder in the final string. See "Trap Definitions" on page 216 for a list of all available format strings for each parameter type and the printed form for each value.

The placeholder format strings are substituted, in order, by the parameters specified in the ARGUMENTS keyword. The ARGUMENTS keyword lists the (zero-based) index of each trap parameter as specified in the VARIABLES clause. The indexes are listed in the order in which you want them to be substituted in the SUMMARY string.

ZENworks for Servers can display a maximum of 140 characters in the SUMMARY string. Use the characters to display the most relevant information about the alarm. If you have a long SUMMARY string and want to keep the line length of the MIB file reasonable, you can insert multiple, consecutive SUMMARY annotations and the strings will be concatenated. For example, the following annotations below yield the same string:

–#SUMMARY “%s at %s and %s are using the same”

–#SUMMARY “IPX address”

–#SUMMARY “%s at %s”

–#SUMMARY “and %s are”

–#SUMMARY “using the same IPX address”

The following table lists the format strings and parameter types.

Parameter Type	Format String	Printed Form
BOOLEAN	%s	True or False.
	%d	1 or 0.
INTEGER	%x	HEX.
	%d	DECIMAL.
	%t	Prints the integer or a date and time (Greenwich Mean Time). The integer represents seconds since 1970.
OCTET STRING	%s	Prints the text string with all control characters taken out.
	%m	Prints the first 6 bytes of data as a hyphen-separated MAC address. For example, 00-00-07-00-07.
	%x	Prints the octet string in hexadecimal. For example, 0000070007.

Parameter Type	Format String	Printed Form
NULL	%d	Prints the number 0.
	%s	Prints the string NULL.
OBJECT IDENTIFIER	%s	Prints dot-separated decimal values. For example, 1.3.6.5.4.
IP Address	%s	Prints dot-separated IP address. For example, 13.56.56.56.
	%x	Prints a long hexadecimal value.
BIT STRING	%s	Prints each byte as decimal.

Configuring MIBs and Setting Up MIB Tools

This section describes the procedural tasks for configuring MIBs and setting up the community strings for SNMP operations on an individual node. After you complete these tasks, you can perform SNMP operations using MIB Tools.

This section covers the following topics:

- "Annotating Third-Party MIBs for Integration with ZfS" on page 224
- "Compiling MIBs for SNMP-Manageable Nodes" on page 225

Annotating Third-Party MIBs for Integration with ZfS

When you compile a MIB containing SNMP traps (alarms), information about those traps is added to the ZfS alarm database. This information can then be displayed in ConsoleOne.

All Novell MIBs are annotated so that the alarm information displayed in ConsoleOne is easily readable. This alarm information includes a summary describing the alarm, the alarm severity, and the state of the affected node. Third-party MIB files do not necessarily contain this same information. Therefore, the information about the traps in third-party MIBs is not as meaningful when displayed in ConsoleOne.

You can add annotations to third-party MIB files for the trap definitions so that the alarm information displayed in ZfS for those traps is more readable than if you compile the MIB as is. Any annotations you add to a third-party MIB are added as comments to the trap definitions. This ensures that the MIB still compiles with third-party MIB compilers.

If you do not annotate the traps in third-party MIBs, ZfS will display the alarms. The MIB Compiler displays warnings in the status display about the missing annotations.

To add annotations to a third-party MIB:

1. Open the MIB in a text editor.
2. Add any of the annotations shown in "Keywords for Trap Annotations" on page 218, by following these rules:
   - Enter annotations only between the DESCRIPTION and the "::=" clause.
   - Each annotation must be on a separate line.
   - Annotations must be in the order shown in "Keywords for Trap Annotations" on page 218.
   - Embed each annotation as a comment. Precede each annotation with two hyphens and a pound sign (#).

     For example: --#Type "*type_description*"

     For a full example, see "Example Trap Definitions" on page 220.
3. When you finish annotating trap definitions, save your changes and exit the text file.

   Compile the MIB, as described in "Compiling MIBs for SNMP-Manageable Nodes" on page 225.

Use ConsoleOne Alarm Disposition table to view the values for the alarm severity level and alarm state from the default values in the SNMP MIBs. If you change the value for an alarm's severity or state after you compile the MIB, you must recompile the MIB for those changes to overwrite any changes made through the Alarm Disposition table.

Compiling MIBs for SNMP-Manageable Nodes

The MIB Compiler lets you manage the MIB Server Pool and also compile the .MIB files contained in the MIB Server Pool. The information in the compiled files is placed in the database on the ZfS server. The MIB Browser and the SNMP protocol decoder use this database.

The MIB Compiler also adds or updates any trap definitions to the alarm template database for use by the ZfS Alarm Management System (AMS).

The MIB Server Pool contains the list of MIB files. You can add or remove the MIB files from the MIB Server Pool.

To compile the MIBs:

1. From ConsoleOne, click the ZfS server node.
2. Right-click the node > click Properties > click the MIB Pool tab.

   The current MIB Pool lists the compiled MIB files present in the database.
3. Choose your options.
   - To add MIBs, click Add to locate the .MIB files and add them to the MIB Pool list.

     The added MIBs are displayed in the adjacent list box.

     When you add MIBs, you choose to integrate or exclude the trap information while compiling MIBs. If you do not integrate traps with the MIBs, only the MIB information is stored in the database on successful compilation of the MIBs. Click Advanced > select the Trap Integration check box to integrate the trap information with the MIBs.
   - To remove files from the MIB Pool list, select the MIB from the list > click Remove.
   - To compile the MIBs with less strict adherence to ASN.1 syntax, click Advanced > select the ASN.1 Syntax Relaxation option.
4. Click Compile.

   The MIB Compiler compiles all files in the MIB Pool list with the .MIB extension and updates the database. The compilation process is begun by launching a Results dialog box. This dialog box displays the status information of the MIBs including the MIBs that were successfully compiled, MIBs that were not compiled and the corresponding error message, and the status of updating the database with the MIB compile information, and the status of updating the Alarm database.

   IMPORTANT: You cannot closed the Results dialog box during compilation. The Close button in the Results dialog box is disabled during compilation. You can close this dialog box only after the compilation is successful or failed.
5. Click Close.

IMPORTANT: If the SNMP MIB is not set up correctly, or an imported Request for Comments (RFC) is not available during compilation of the MIB, or any other .MIB file is not available, an error message is generated in the MIB Compiler window. Add the required RFC or the dependent MIB and compile.

Using the MIB Browser

This section acquaints you with using the MIB Browser to manage SNMP-manageable nodes.

This section includes the following topics:

- "Browsing the MIB Tree" on page 227
- "Viewing the Values of an Object and Its Child Nodes" on page 229
- "Configuring a Node by Setting Object Values" on page 231
- "Modifying SNMP Preferences" on page 231
- "Modifying Instances of an SNMP Table" on page 232
- "Forming Tables of Scalar Objects" on page 235
- "Graphing SNMP Request Results" on page 236
- "Using a Profile for Tables and Graphs" on page 238

Browsing the MIB Tree

The MIB Browser lets you select the objects you want to display, and it sends SNMP queries to the node to obtain the data objects that you requested. It also allows SNMP operations such as GET, GETNEXT, and SET requests on a particular object in the MIB of an SNMP-managed node.

The MIB Browser periodically polls the node and continually updates the display. You can view and modify scalar and tabular data objects.

MIB Tree Browser

Within the MIB browser, the MIB Tree Browser is a graphical display of management data that consists of numerous objects.

The MIB Browser displays a composite OID tree for all compiled MIBs. Analogous to a file system, the MIB Browser shows leaf objects, which are the SNMP data objects.

The MIB Browser spans the selected node with its subtree and leaf objects and displays the name of the objects in the MIB Tree Browser. You browse from the highest level of the tree and view the leaf object values.

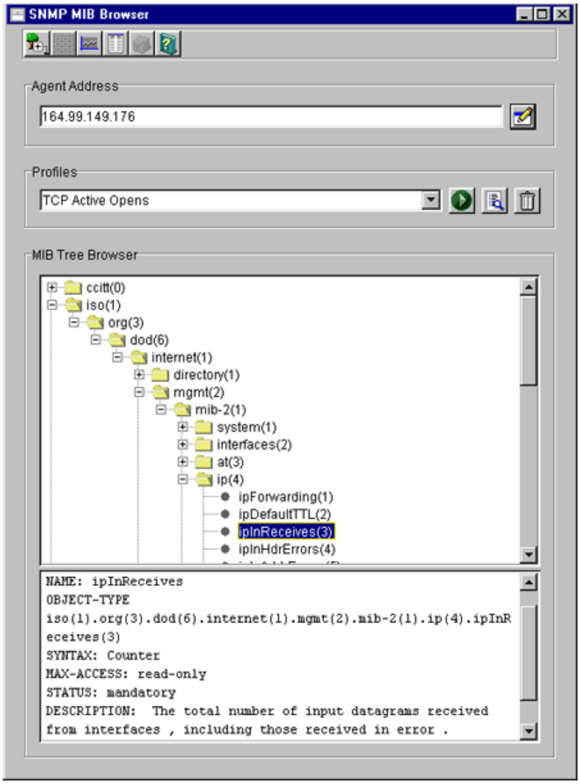
The top pane of the MIB Tree Browser displays the tree with the selected object. Each object is displayed as a file folder icon, followed by its SNMP name with the SubId appended in parentheses. If the object is a non-leaf node, the MIB Tree Browser also displays its children.

The bottom pane describes the selected object. The description is derived from the compiled MIB file. The format of the description is as follows: textual description of the object, full numeric OID and object name, ASN.1 type, size, textual convention, access, Index clause taken from the Entry object, status, and description.

For example, for an internal node SYSTEM with child nodes, the child nodes describe the properties of the SYSTEM. The OID of SYSTEM is iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1). Another equivalent representation of this OID is 1.3.6.1.2.1.1. Note that the parent node does not have information, and the child nodes contain the properties.

The child nodes of SYSTEM are sysDescr OID(1.3.6.1.2.1.1.1), sysObjectID OID(1.3.6.1.2.1.1.2), sysUpTime OID(1.3.6.1.2.1.1.3), sysContact OID(1.3.6.1.2.1.1.4), sysName OID(1.3.6.1.2.1.1.5), sysLocation OID(1.3.6.1.2.1.1.6), and sysServices OID(1.3.6.1.2.1.1.7).

The following figure shows the MIB Browser window.



Agent Address: 164.99.149.176

Profiles: TCP Active Opens

```
NAME: ipInReceives
OBJECT-TYPE
iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ip(4).ipInR
eceives(3)
SYNTAX: Counter
MAX-ACCESS: read-only
STATUS: mandatory
DESCRIPTION:  The total number of input datagrams received
from interfaces , including those received in error .
```

To browse the MIB objects:

1. From ConsoleOne, click the target SNMP-manageable node.
2. Click File > Action > MIB Browser.
3. Click the object whose values you want to view from the MIB Tree Browser.
   - To select an object, click the name text or the icon in the MIB Browser tree.
   - To expand or collapse the next level in the tree display, double-click the object.

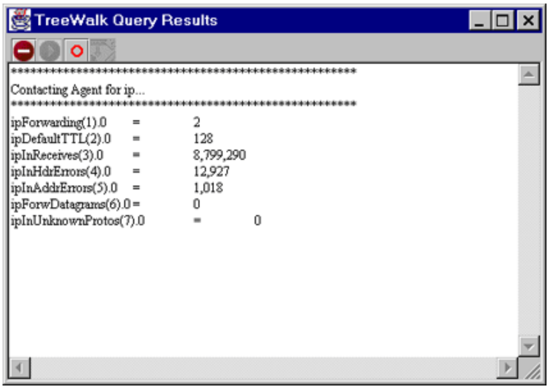
Viewing the Values of an Object and Its Child Nodes

The MIB Browser spans the selected node with its subtree and leaf objects and displays its values in the TreeWalk Query Results window. You can browse the OID values of scalar and tabular objects.

To view the values of the instances of a MIB object:

1. From ConsoleOne, click the target SNMP-manageable node.
2. Click File > Action > MIB Browser.
3. Click the object > Perform TreeWalk for the node button.

The following figure shows the TreeWalk Query Results window.



```
*****************************************************
Contacting Agent for ip...
*****************************************************
ipForwarding(1).0      =          2
ipDefaultTTL(2).0      =          128
ipInReceives(3).0      =          8,799,290
ipInHdrErrors(4).0     =          12,927
ipInAddrErrors(5).0    =          1,018
ipForwDatagrams(6).0=             0
ipInUnknownProtos(7).0            =        0
```

If you select a leaf object, you can view the values for each instance of this object. For non-leaf objects, this window will display all the values of the child node of this object. For example, if you want to view the values of the child nodes for the object *system*, click the parent object *system*.

The display process in the Treewalk Query Results window continues recursively for all the non-leaf objects of the selected object.You can pause and resume this display in the window.

Customizing the Display of TreeWalk Query Results Window

The TreeWalk Query Results window displays the number of lines based on the settings specified in the TREEWALK.PROPERTIES file.

This file, located in \CONSOLEONE*version*\BIN\SAVED-VIEWS\GENERIC directory, contains the following setting:
`MaximumNumberofLine=`***`number_of_lines_for_display`***

where *number_of_lines_for_display* is the number of lines that will be displayed at a time. The default setting is 10,000 lines.

You can modify this setting. The settings will apply only if you restart ConsoleOne and bring up the TreeWalk Query Results window.

To clear the display in the TreeWalk Query Results window when the text buffer is full, click the Clear button.

There may be some out of memory problems if you specify a large line setting in the TREEWALK.PROPERTIES file.

Configuring a Node by Setting Object Values

Using the MIB Browser, you can issue an SNMP SET command to change information at an SNMP-manageable node if you have the appropriate privileges. You select a scalar object from the MIB Browser and set its value.

You can modify the values for an integer, enumerated integer, object identifier, string, and IP address object types.

To issue an SNMP SET command for a scalar object:

1. From ConsoleOne, click the target SNMP-manageable node.
2. Click File > Action > MIB Browser.
3. Click a scalar object whose values you want to view > click Display Data As a Scalar Table.
4. Specify the object value for the scalar object.
5. Click OK.

To modify columnar values of an SNMP table, see "Modifying Instances of an SNMP Table" on page 232.

Modifying SNMP Preferences

SNMP parameters are used to communicate with the target device. The MIB Browser lets you change the SNMP community strings or specify the transport address of a new target device.

Any SNMP operation requires these values to be set. After starting an SNMP operation, such as polling a table, changing the SNMP preferences does not affect the operation.

You can modify the following parameters:

Agent Address: You can specify the IP or IPX address and the Domain Name System (DNS) name of the SNMP-manageable node to which you want to send an SNMP request. This node should have an SNMP agent.

SET and GET Community Strings: The community string that ZfS uses must match the one expected by the SNMP agent in the managed node or the SNMP operations will fail. If the SNMP agent on the node expects a community string for SET and GET operations that is different from public (the default), you can specify the expected community string to override the default community or those community strings you set previously. You can use Unicode* or International characters for the community string.

To modify the SNMP preferences:

1. From ConsoleOne, click the target SNMP-manageable node.
2. Click File > Action > SNMP MIB Browser.
3. Click Modify SNMP Preferences.
4. Specify the parameters > click Close.

Modifying Instances of an SNMP Table

A table in an SNMP MIB is an SNMP construct derived from the structure of the MIB. Each row in the table corresponds to a row in the SNMP table.

The MIB Browser provides the Table Display window to display tabular objects you select. This window displays one or more rows from an SNMP table in a two-dimensional grid and follows the SNMP index order to display rows.

The table shows each column in the SNMP table as columns. Each column heading is derived from the SNMP table columns. The Table Display window displays the columns with their values as single or multiple rows for the MIB you selected.

SNMP allows operations on individual table entries only. The OID identifies the column and row.

From the MIB Browser, you can perform the following operations:

- Add rows to an SNMP table

  For more information, see "Adding Rows to an SNMP Table" on page 234.

- Modify a row of an editable table

  For more information about adding or modifying rows, see "Adding Rows to an SNMP Table" on page 234.

- Save the table as a profile

  For more information about saving a table as a profile, see "Using a Profile for Tables and Graphs" on page 238.

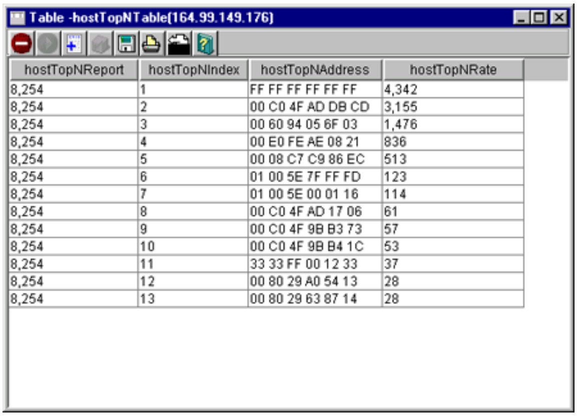
Viewing the SNMP Table

To view the SNMP table:

1. From ConsoleOne, click the target SNMP-manageable node.
2. Click File > Action > SNMP MIB Browser.
3. Click a tabular object whose values you want to view > Display Data As a Table.

From the Table Display window, you can add rows or modify the rows of the SNMP table and input values for each column. For more information about adding or modifying rows of an SNMP table, see "Adding Rows to an SNMP Table" on page 234.

The following figure shows the MIB Browser Table Display window.



hostTopNReport	hostTopNIndex	hostTopNAddress	hostTopNRate
8,254	1	FF FF FF FF FF FF	4,342
8,254	2	00 C0 4F AD DB CD	3,155
8,254	3	00 60 94 05 6F 03	1,476
8,254	4	00 E0 FE AE 08 21	836
8,254	5	00 08 C7 C9 86 EC	513
8,254	6	01 00 5E 7F FF FD	123
8,254	7	01 00 5E 00 01 16	114
8,254	8	00 C0 4F AD 17 06	61
8,254	9	00 C0 4F 9B B3 73	57
8,254	10	00 C0 4F 9B B4 1C	53
8,254	11	33 33 FF 00 12 33	37
8,254	12	00 80 29 A0 54 13	28
8,254	13	00 80 29 63 87 14	28

The MIB Browser periodically sends SNMP queries to the node to obtain the data objects you request. When you provide new values for writable objects, the MIB Browser writes these values to the node. The MIB Browser periodically polls the node and continually updates the display. You can change the polling interval by suspending the SNMP interaction or by canceling the SNMP interaction.

Adding Rows to an SNMP Table

When you add a new row to an SNMP Table, the MIB Browser generates the SNMP SET request.

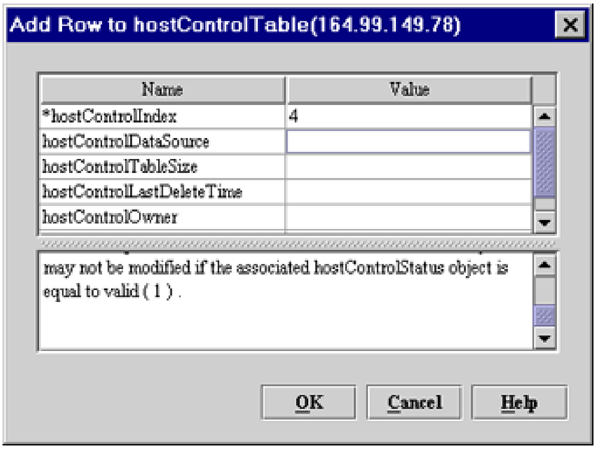
Before generating the SNMP Set request, the MIB Browser sends a GET command to the node that you selected in the MIB Browser table and retrieves the value of the object. On adding rows with the specified values for the objects, the MIB Browser issues multiple SNMP SET commands to update the SNMP table.

To add a row to an SNMP table:

1. Click the table object from the MIB Browser window > Add a New Row to the Table.

   For more information about selecting the table object, see “Modifying Instances of an SNMP Table” on page 232.

   The following figure shows the Add Row to Table window.



Name	Value
*hostControlIndex	4
hostControlDataSource	
hostControlTableSize	
hostControlLastDeleteTime	
hostControlOwner	

may not be modified if the associated hostControlStatus object is equal to valid (1) .

2. Double-click the row.
3. Modify the value > click OK > click OK.

To add rows in an SNMP table, you must input the values for all the index rows, which are denoted by asterisks.

To modify a row of an editable table:

1. Open the Table window.

2 Click the row whose values you want to modify > click Issue SNMP Set request for a column button.

3 Double-click the row.

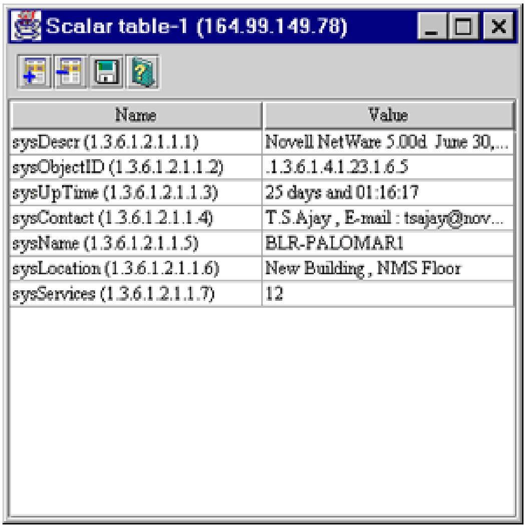
4 Modify the value of the object > click OK > click OK.

Forming Tables of Scalar Objects

You can make a scalar table by combining the scalar objects from the MIB Browser. A scalar table is a two-column table with the name and value of the scalar object entries. To create a scalar table, you select a group node with scalar child nodes or a group of scalar objects. For example, you add one or more scalar objects such as ipInDelivers and SysUpTime to make a new scalar table labeled ipInDeliversTable.

If you want to view the scalar tables that you create, save the scalar table as a profile. You can load the scalar table profiles when required.

The following figure shows the Scalar Table window.



Name	Value
sysDescr (1.3.6.1.2.1.1.1)	Novell NetWare 5.00d June 30,...
sysObjectID (1.3.6.1.2.1.1.2)	.1.3.6.1.4.1.23.1.6.5
sysUpTime (1.3.6.1.2.1.1.3)	25 days and 01:16:17
sysContact (1.3.6.1.2.1.1.4)	T.S.Ajay , E-mail : tsajay@nov...
sysName (1.3.6.1.2.1.1.5)	BLR-PALOMAR1
sysLocation (1.3.6.1.2.1.1.6)	New Building , NMS Floor
sysServices (1.3.6.1.2.1.1.7)	12

To combine scalar objects as a scalar table and view the table:

1 Create a new scalar table.

2 Add to or modify the existing table by adding scalar entries or by removing entries from the table.

3. Save the scalar table as a profile.
4. Launch the profile.

To create a new scalar table:

1. From ConsoleOne, click the target SNMP-manageable node.
2. Click File > Action > SNMP MIB Browser.
3. Right-click a scalar group or a scalar object > click New > click Scalar Table.

To add or remove scalar entries to an existing table:

1. Open an existing scalar table.
2. Toggle to the MIB Browser window > click Add to > click *Scalar_table_name*.

   Alternatively, click the scalar entry in the MIB Browser window, and from the Scalar Table window, click Add Node Selected from Browser Window.

To remove the scalar entry, click the scalar entry in the Scalar Table window, and click Remove the Node Selected in This Window.

Graphing SNMP Request Results

You can plot the SNMP request results in a graph that displays the polled data of the MIB objects. Only attributes of ASN.1 type Integer, Counter, Time Ticker, and Unsigned Integer are plotted as current absolute values.

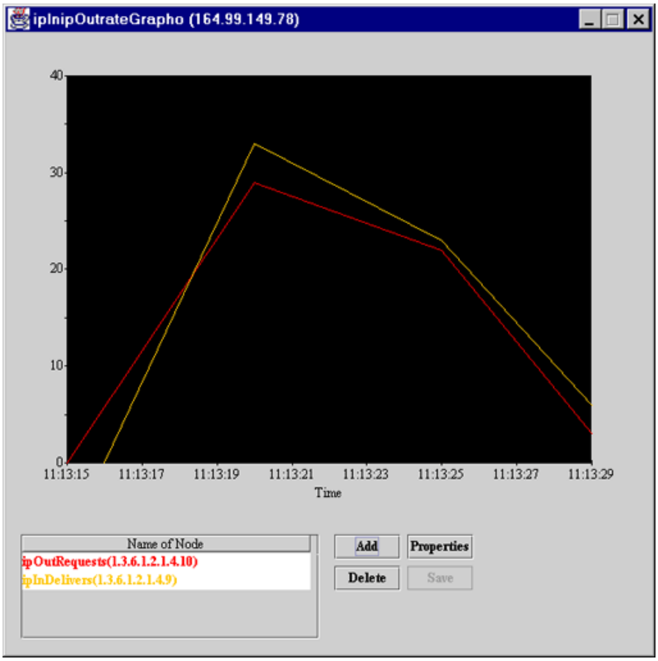
You can plot more than one object in the same graph, add more objects, or remove the MIB objects from the existing graph. If you want to view the graphs that you create, save the graph as a profile. You can then load the graph profiles when required.

To graph SNMP request results of one or more nodes:

1. Click the target SNMP-manageable node from the console.
2. Click File > Action > SNMP MIB Browser.
3. Click the MIB object whose values you want to plot.
4. Right-click the object > click New > click Graph.

The MIB Browser plots the graph with the values of the selected object and its leaf object values dynamically in the Graph pane of the window.

The following figure shows the Graph window.



iplnipOutrateGrapho (164.99.149.78)

Name of Node
ipOutRequests(1.3.6.1.2.1.4.10)
ipInDelivers(1.3.6.1.2.1.4.9)

To graphically plot the values of more than one object:

1. Toggle to the MIB Browser window.
2. Click the MIB object you want to plot > click Add To > click the Graph.

   You add these objects to any of the active graph windows you want.

Alternatively, you can click the MIB object from the MIB Browser window and then click the Add button in the MIB Browser Graph. Remove the objects from the list that you do not want by selecting the node from the list and clicking the Delete button.

From the Graph window, you can perform the following operations:

- Rescale the Y-axis of the graph
- Set the period to display
- Set the polling interval and refresh rate of the display

  By default, the values plotted in the graph are absolute. If you want to view the rate of change of values per second with respect to sysUpTime, you must click the Rate option. For example, if you click ipInPackets and choose the Rate option, you can view the values per second.

Using a Profile for Tables and Graphs

A profile contains information about the properties of the graph, table, or scalar table. You use a profile to specify the information, such as the method of display (table or graph) and polling interval.

You create a profile by saving the properties of the table, scalar table, or graph as a profile. You open the profile to view a table, scalar table, or graph of different SNMP-manageable nodes on the segment with the same properties specified in the profile. You can modify or delete the profile.

To form a profile:

1. Save the properties of the display window.
2. Open the profile.
3. Modify the properties of the profile as required.

To save a profile:

1. Click the Save button from the Scalar table window, Graph window, or Table window.
2. Type the details of the profile.

   Specify the name, description, and properties of the objects.
3. Click OK.

To open a profile:

1. From the MIB Browser window, click the profile you want from the drop-down list.
2. Click Launch This Profile.

To modify the selected profile:

1. Click View/Edit Profile Contents for the selected profile in the MIB Browser window.

To delete a selected profile:

1. Click Delete This Profile.

Maintaining MIBs

Depending on your need to add MIBs for managing nodes, you must compile the MIBs.

To delete a particular MIB from ZfS, remove the appropriate MIB text file from the MIB Server Pool and rerun the MIB Compiler. If the MIB you delete contains traps, you must remove the alarm definitions before you rerun the MIB Compiler.

When you add MIBs, you choose to integrate or exclude the trap information while compiling MIBs. If you disallow trap integration with the MIBs, only the MIB information is stored in the database on successful compilation of the MIBs.

For more information about how to add or remove MIBs, refer to "Compiling MIBs for SNMP-Manageable Nodes" on page 225.

7 Monitoring Services

ZENworks® for Servers (ZfS) lets you test the connectivity and availability of a service on a network device. This test checks and measures the response by sending diagnostic packets, and also notifies the console whenever the status of the service changes.

This section provides an overview of the testing facility, lists the services that can be monitored on the nodes, and discusses the test options. See the following sections for more information:

- "Understanding Monitoring Services" on page 241
- "Monitoring Services on Target Nodes" on page 244

Understanding Monitoring Services

Using the Monitoring Services facility, you test connectivity of services on one or more critical network devices, such as servers or routers. For example, you can monitor services because you want to be alerted immediately if the connectivity between the console and critical nodes is disrupted.

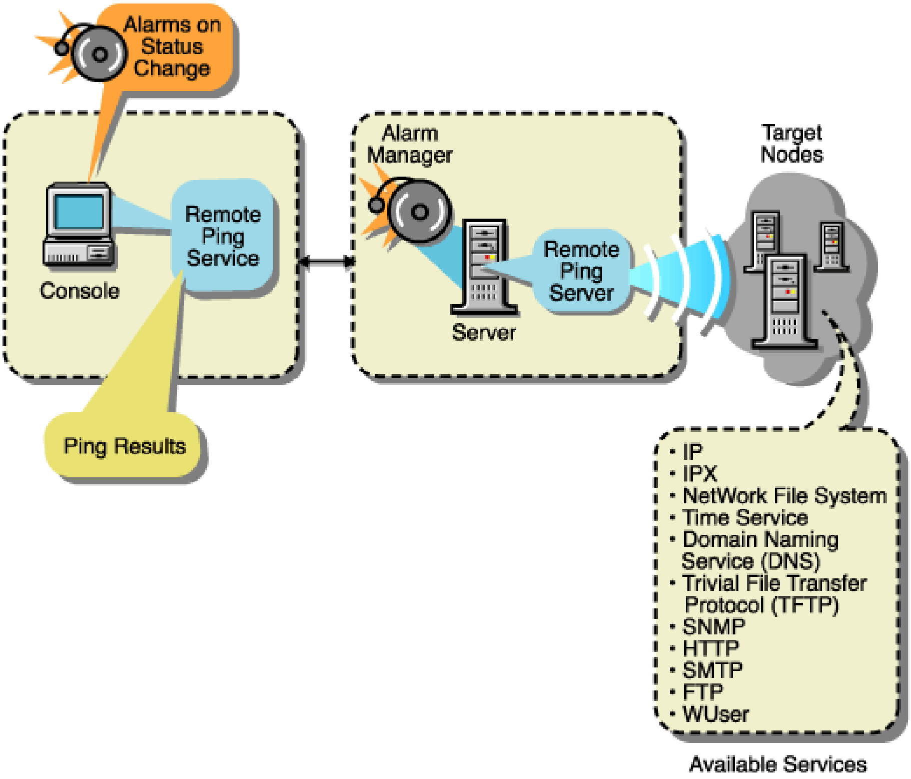
This test facility enables testing of the following services:

- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Echo
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol Secure (HTTPS)
- Internet Packet Exchange™ (IPX™)

- Internet Protocol (IP)
- Network File System (NFS)
- Network News Transfer Protocol (NNTP)
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
- Time Service
- Trivial File Transfer Protocol (TFTP)
- WUser

The test facility uses the ZfS server as the remote ping server. When you select the service on the node for testing, the console interacts with the remote ping server on the ZfS server and displays the results of the test on the console.

The following figure shows a graphical representation of Monitoring Services.



To monitor nodes, you choose the nodes and enable the monitoring session for the duration you require.

From the console, you monitor the services in the following ways:

- Test connectivity of the services on a node one time only when you suspect a problem with the connectivity.
- Continuously monitor connectivity of the services on a critical node until you close the test facility.
- Continuously poll the services of the nodes on the segment (for example, connectivity testing of the services on the target nodes runs uninterrupted until you disable monitoring). If you do not disable monitoring, this test facility continues even after you close the console.

For testing connectivity of services on the target nodes you select, you set the following options:

- Specify the services on the selected target nodes.

If you need to test any TCP-based services, add the service to the existing list of services.

- Define the test interval between two successive tests.
- Define the timeout value.

  The timeout value determines the time duration that the remote ping server waits to receive the response from the target node.

You can view the status of the connectivity and measure diagnostics, such as round trip delays or number of packets sent and received from the console.

Role-Based Services for Using the Monitoring Services

Role-based services (RBS) defines the task for Monitoring Services as Enable Remote Ping. If this task is assigned to your role, you can use the Monitoring Services facility.

For general information about role-based traffic analysis tasks, creating RBS role objects or specifying tasks that RBS roles can perform, see "Role-Based Administration" on page 34.

Monitoring Services on Target Nodes

This section guides you through the tasks involved in using the Monitoring Services facility.

From the console, you can monitor critical nodes on the network and manage potential connectivity problems before they affect the network. You define the services to test on the selected nodes, then view the test results and other data for each listed target. To perform the testing, complete the following general steps:

1. Define the targets to be monitored.

   See "Defining the Targets for Monitoring Services" on page 245 for information about specifying the services on the target nodes.

2. On a per-node basis or on multiple nodes, change the test interval or timeout value.

   These tests use default values for the test interval between two successive tests on the target and to determine the time duration that the remote ping server waits to receive the response from the target node. You can change these values for the test.

See "Changing the Test Options for a Node" on page 248 for information about editing the test options.

3. View the test results.

   The nodes are monitored continuously, at the defined test interval for the node. Depending on the Monitoring Services test that you choose, the corresponding test results are displayed.

   See "Displaying Test Results Data" on page 247 for information about test results data.

Defining the Targets for Monitoring Services

Monitoring Services requires that you specify the targets for the tests. You can choose from the following test options:

- "Test the Services on the Target Node One Time Only" on page 245
- "Continuously Monitor the Services on the Target Nodes" on page 246
- "Continuously Poll the Services of the Target Nodes on a Segment Until the Test Is Disabled" on page 246

NOTE: You can monitor approximately 50 critical services simultaneously on the servers. Monitoring more than 50 services may overload the server memory and result in performance degradation.

Test the Services on the Target Node One Time Only

If you suspect a problem with a node in the network, you can ping the node once for monitoring services. When you select the target node for testing the services and specify the IP or IPX address, this address will determine the service that will be tested at the node. For example, if you type the IPX address, the default IPX service is tested on the target node.

The results of the test will display the status of the target node and details of the round trip delay in the Ping window.

To test the services on a node once:

1. From ConsoleOne, right-click the selected node > click Ping.
2. Type the ping target details.
3. Click OK.

Continuously Monitor the Services on the Target Nodes

To specify the services for continuous monitoring, add the targets and choose the services on the node and other options. The target node will be added to the list of targets in the Connectivity Test Results window and the test results data will be displayed. Monitoring of services continues until you close this window.

To define the targets for testing services on the node:

1. From ConsoleOne, click Action > Connectivity Test.
2. Click Add.
3. Specify the details for the target nodes in the Add Ping Target dialog box.

   Refer to "Adding Services for Monitoring" on page 248 for more information about adding services.
4. Click OK.

The target node will be added to the list of targets in the Connectivity Test Results window.

Continuously Poll the Services of the Target Nodes on a Segment Until the Test Is Disabled

For polling the services on the nodes of a segment, select the nodes on a segment with the list of services you want to test. Enable the test in the Monitor Tab Services window and view the results of the test in the Polling view.

If you do not disable the test, polling of the services continues after you close the console.

To define the services on the nodes for polling:

1. From ConsoleOne, right-click the node of a segment > click Properties > click the Monitor Services tab.

   The List of Segment dialog box displays the different addresses of the same node on different segments if the node is connected to more than one segment. Click the node on the segment that you want to add.
2. Specify the details for the target nodes in the Monitor Services Tab window.

   Refer to "Adding Services for Monitoring" on page 248 for more information about adding services.
3. Click OK.

Displaying Test Results Data

After defining the services for testing on the target node, you can view the results from the console.

Depending on the test you choose, the test results are displayed in the corresponding window.

If you choose to test the services on the node one time only, the test results will be displayed in the Ping Status window of the Ping window. This target will not be tested in the Connectivity Test Results window.

If you choose to continuously monitor the services, the test continues until you close the window. You can view the results in the Connectivity Test window.

If you choose to continuously poll the services until you disable the test, you can view the test results in the Polling view.

The following test data is available when you monitor the services on the target nodes:

Ping Target: Name or address (IP or IPX) of the network device for which services are being tested.

Service: Monitored services that are being tested on the target.

Port: Port number that the service uses.

Status of the Target: Up Status means that the service is available on the node and can be reached from the remote ping server. Down Status means that the service is down and cannot be reached from the server.

RoundTrip Delay: Time interval (in milliseconds) between the instant the remote ping server sends the test packet to the target and the instant the response is received from the target.

Packets Sent: Number of packets sent from the remote ping server to the target node.

Packets Received: Number of packets received by the remote ping server from the target node.

Packets Lost: Number and percentage of packets lost during the testing of the target node.

Interval: Displays the test interval value, in seconds. This value determines the time duration between two successive tests on the target.

Timeout: Displays the timeout value, in milliseconds. This value determines the time duration that the remote ping server waits to receive the response from the target node.

To view the Connectivity Test Results window:

1. Click File > Action > Connectivity Test from the Console.

   If you select one or more target nodes from the right pane of the console, the list of nodes that you want to test for connectivity will be shown in the Connectivity Test Results window.

To view the results of the polling:

1. From the console, click a segment > View > Polling.

NOTE: To delete a target node from the list, from the Polling view, click the target node > click Delete.

Changing the Test Options for a Node

You can modify the test options, such as the test interval and timeout options, that you set earlier on an individual node or on multiple nodes. To modify multiple nodes, click more than one node from the Connectivity Test Results window; the test options apply to all selected target nodes.

To view the Connectivity Test Results window:

1. Click the target row from the Connectivity Test Results window > click the Edit button.
2. Type values for the Ping Interval and Timeout.
3. Click OK.

If you want to roll back to the default setting, click Apply Defaults.

Adding Services for Monitoring

Monitoring Services lets you test services on the nodes. If you need to test any TCP-based service that is not listed in the default services list, you add the details of the service when you are adding the targets.

You specify the name of the service in the Add Service dialog box. Ensure that the service name you add is a unique name. Also, you must specify the port number for the service.

You can add the details of the service under the following circumstances:

- "Continuously Monitor the Services on the Target Nodes" on page 246
- "Continuously Poll the Services of the Target Nodes on a Segment Until the Test Is Disabled" on page 246

The services that you add are stored in a file on the server.

8 Understanding Traffic Analysis

ZENworks® for Servers (ZfS) provides traffic analysis tools that monitor network traffic, capture data, and collect key statistics of monitored segments nodes, and devices, allowing you to obtain, review, and analyze vital information to effectively troubleshoot and manage your LAN and keep your network operating at peak performance.

This section contains the following topics:

Understanding Traffic Analysis

This section contains basic information to help you understand traffic analysis and describes the ZfS traffic analysis components.

Traffic Analysis Components

The ZfS traffic analysis components include:

- "Management Server" on page 252
- "Management Console" on page 252
- "Monitoring Agent Server" on page 252

Management Server

The management server comes with the robust and highly scalable Sybase* Adaptive Server Anywhere that stores static information, such as the names and addresses of the nodes and devices in your network. The management server components include the NetExplorer™, management database, Consolidator, and Atlas Manager. NetExplorer discovers the objects in your network and stores them in the management server. The Consolidator takes the information about network objects discovered by NetExplorer and builds the management database. For details about the functionality of NetExplorer, see "Understanding Network Discovery" on page 72.

The management database is comprised of the Common Information Model (CIM) schema that is used to establish the topology of the network. The CIM schema extension capabilities provide the ability to organize the information in the database and give this information the shape of a network map. The Atlas Manager obtains information from the management database and displays the network map on ConsoleOne.

Management Console

ConsoleOne®, the Novell® directory-enabled, Java*-based network management and administration tool, is the management console component. ZfS snaps in to ConsoleOne and expands ConsoleOne's capabilities by adding menu options, property pages for existing Novell™ objects, and ways to browse and organize network resources. ConsoleOne provides an intuitive, graphical user interface for ZfS traffic analysis. For details about the functionality of ConsoleOne, see "Managing the Atlas" on page 120.

Monitoring Agent Server

Before you start analyzing segments or devices on your network, you need to ensure that they are monitored. To enable monitoring, make sure you have installed the network monitoring agent software either on the management server or on an independent server in your network. For more information, see

Installing and Setting Up Management and Monitoring Services in the *Installation* guide. Network monitoring agents gather information or provide services that help you monitor your network.

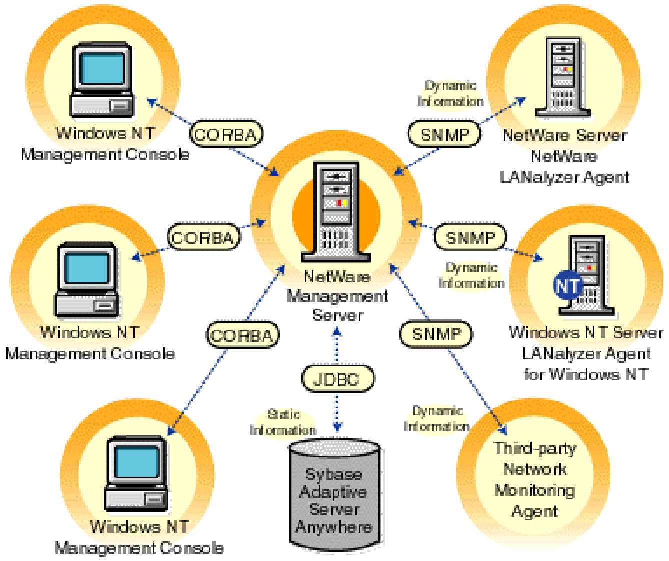
An agent program using parameters you have provided searches all or part of your network, gathers information you query, and presents it to you when you require it. You can use the information gathered by the agent to analyze the traffic on your network. The agent also warns you of problems, such as duplicate IP addresses, by sending an alert to ConsoleOne to help you solve problems before network performance is impacted. For details about managing alarms, see "Managing the Alarm Management System" on page 132.

Network monitoring agents observe traffic and capture frames to build a database of network objects and information to help you detect network aberrations. With the network monitoring agent software installed on a server on each of your segments, you can use the traffic analysis tools to help you monitor the traffic on your network, identify the source of network problems, and maintain optimum performance. For details, see "About Network Monitoring Agents" on page 256. The traffic analysis agents for NetWare® and Windows* NT*/2000 are part of ZfS that you can use to monitor Ethernet, FDDI, or token ring networks.

Communication Between Traffic Analysis Components

ConsoleOne communicates with the management server using common object request broker architecture (CORBA) to procure dynamic and static information about the nodes and devices in your network. When ConsoleOne requests static information from the management server, the management server communicates with the management database using Java Database Connectivity (JDBC), gathers the required static information from the database, and provides it to ConsoleOne. When ConsoleOne requests dynamic information from the management server, the management server communicates with the network monitoring agent using SNMP, gathers the required dynamic information, and provides it to ConsoleOne.

The following diagram illustrates this communication:


Windows NT Management Console
CORBA
Dynamic Information
SNMP
NetWare Server NetWare LANalyzer Agent
CORBA
NetWare Management Server
SNMP
Dynamic Information
NT
Windows NT Management Console
CORBA
SNMP
Windows NT Server LANalyzer Agent for Windows NT
JDBC
Static Information
Dynamic Information
Windows NT Management Console
Sybase Adaptive Server Anywhere
Third-party Network Monitoring Agent

Traffic Analysis Features

The ZfS traffic analysis components provide the following features:

- "Analyze Traffic Generated by Segments" on page 254
- "Analyze Traffic Generated by Nodes Connected to Segments" on page 254
- "Capture Packets, Decode Captured Packets, and Display Captured Information" on page 255
- "Analyze Traffic Generated by Protocols" on page 255
- "Analyze Traffic Generated by Switches" on page 255

Analyze Traffic Generated by Segments

You can use the traffic analysis tools to collect current and historical segment statistics that can be displayed in real time, stored for later display, or transferred to a database, spreadsheet, or management reporting system. For details, see "Analyzing Traffic on Segments" on page 274.

Analyze Traffic Generated by Nodes Connected to Segments

The traffic analysis tools allow you to obtain statistical information about nodes on monitored Ethernet, FDDI, or token ring segments, and determine the top nodes on a segment. You can monitor the status of nodes in your network so that you are alerted when a node becomes inactive. You can also view alarms that are generated when preset threshold parameters are exceeded. Alarms that require immediate attention can be forwarded via e-mail to remote users. For details, see "Analyzing Traffic on Nodes Connected to a Segment" on page 286.

Capture Packets, Decode Captured Packets, and Display Captured Information

You can use the traffic analysis tools to capture packets between nodes on a monitored segment, and you can quickly define a capture filter based on which you want the packets to be captured. After packets are captured, protocols are decoded and displayed in color-coded summary, decode, and hex panes. The information obtained from the captured packets can be used to examine the traffic on the segment and to analyze it. By providing analysis capabilities and advanced protocol decodes, the traffic analysis tools allow you to identify network aberrations and resolve network performance problems. For details, see "Capturing Packets" on page 295, "Protocol Decodes Suite Supported by ZfS" on page 266, and "Displaying Captured Packets" on page 299.

Analyze Traffic Generated by Protocols

You can use the traffic analysis tools to determine the distribution of protocols in the network, transport, and application layer of your network, and obtain statistical information of protocols discovered by the network monitoring agent. For details, see "Analyzing Traffic Generated by Protocols in Your Network" on page 308.

Analyze Traffic Generated by Switches

You can analyze switch traffic by using the traffic analysis tools to determine port statistics of monitored switches. For details, see "Analyzing Traffic on Switches" on page 313.

Traffic Analysis Fundamentals

ZfS provides tools to let you obtain statistical information about segments, nodes, and devices on your network. You can use this information to analyze and manage the performance of traffic on your network to help you keep the network operating smoothly. ZfS also provides tools to capture and decode packets between nodes. You can use the decoded information obtained from captured packets to analyze the traffic between nodes.

To be able to analyze the segments and nodes connected to a segment, you need to ensure that the segment is monitored by a network monitoring agent. You choose the agent based on the type of your network. The ZfS traffic analysis tools include the Traffic Analysis Agent for NetWare and Traffic Analysis Agent for Windows NT/2000, which you can use to monitor segments in your network. NetWare 5.*x*, the management server for ZfS, includes eDirectory, which is leveraged by ConsoleOne, to enable role-based administration.

The following sections provide information that will help you understand the ZfS traffic analysis functionality:

- "About Network Monitoring Agents" on page 256
- "Role-Based Traffic Analysis Tasks" on page 265
- "Protocol Decodes Suite Supported by ZfS" on page 266

About Network Monitoring Agents

Network monitoring agents provide the functionality to remotely monitor segments and devices on your network using SNMP. The agents collect and store statistical and trend information about nodes and devices on the network to provide real-time information about the status of your network. From your desktop, the agents let you troubleshoot and optimize Ethernet, FDDI, or token ring segments.

Based on the size and type of your network, you can use RMON, RMON Lite, RMON Plus, RMON2, or Bridge agents to monitor traffic. The following sections provide information to help you understand the functionality of agents:

- "Functionality of RMON Agents" on page 256
- "Functionality of RMON Lite Agents" on page 258
- "Functionality of RMON Plus Agents" on page 259
- "Functionality of RMON2 Agents" on page 261
- "Functionality of Bridge Agents" on page 262
- "Viewing the Summarized RMON Information" on page 263

Functionality of RMON Agents

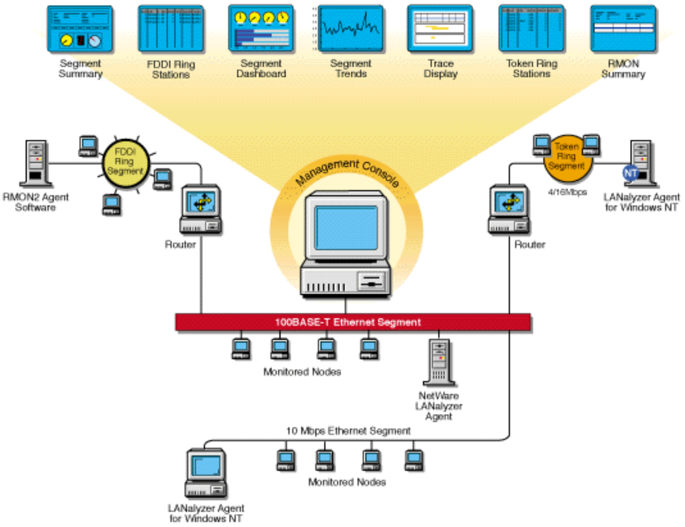
RMON agents use a standard monitoring specification that allows various nodes and console systems on your network to exchange network data. This data can be used by a network administrator to monitor, analyze, and troubleshoot a group of distributed LANs from a central site. RMON is specified as part of the MIB in RFC 1757 (http://www.isi.edu/in-notes/rfc1757.txt) as an extension of the SNMP.

RMON agents are ideally used for monitoring Ethernet, FDDI, or token ring segments.

RMON agents collect information in the following nine RMON groups of monitoring elements, each providing specific sets of data to meet network monitoring requirements. For details, see RFC 1757 (http://www.isi.edu/in-notes/rfc1757.txt).

RMON Group	Description
Statistics	Contains statistics measured by the agent for each monitored interface on the device.
History	Records periodic statistical samples from a network and stores them for later retrieval.
Alarm	Periodically takes statistical samples from variables in the agent and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.
Host	Contains statistics associated with each host discovered on the network.
HostTopN	Prepares tables that describe the hosts that top a list ordered by one of their statistics.
Matrix	Stores statistics for conversations between sets of two nodes. As the device detects a new conversation, it creates a new entry in its table.
Filters	Allows packets to be matched by a filter. These matched packets form a data stream that may be captured or generate events.
Packet Capture	Allows packets to be captured after they flow through a channel.
Events	Controls the generation and notification of events from the device.

The following figure illustrates the ZfS views that you can display when you use an RMON agent to monitor the nodes and devices on your network.



Functionality of RMON Lite Agents

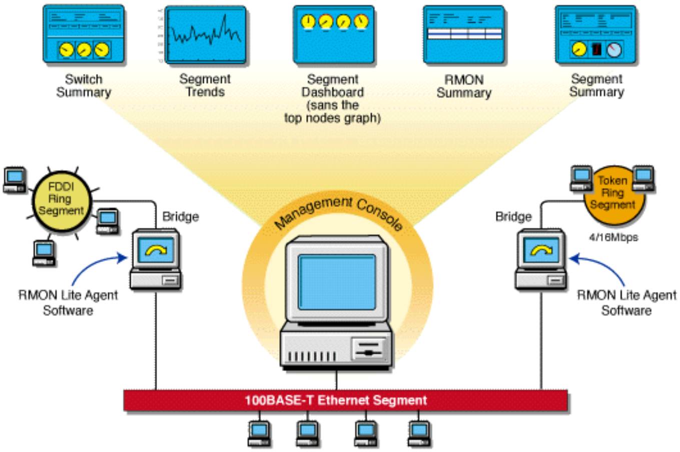
RMON Lite agents are ideally used for monitoring devices not dedicated for network management. For example, RMON Lite agents can be used to monitor a switch in your network.

RMON Lite agents support the following four RMON groups:

- Statistics
- History
- Alarm
- Event

Refer to the table in "Functionality of RMON Agents" on page 256 for a brief description of each group.

The following figure illustrates the ZfS views that you can display when you use an RMON Lite agent to monitor the nodes and devices on your network.



Functionality of RMON Plus Agents

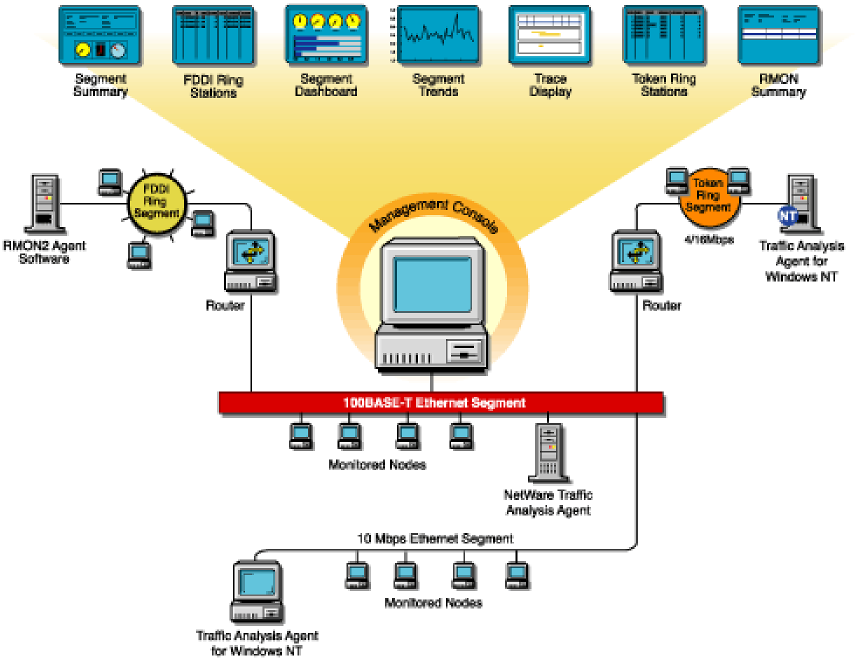
RMON Plus agents are proprietary agents that extend the functionality of the RMON agent by providing data collected from the RMON groups, explained in "Functionality of RMON Agents" on page 256, and the groups explained in the following table.

RMON Plus Group	Description
Buffer	Records the number of octets (excluding framing bits but including frame check sequence [FCS] octets and overhead) in packets which are captured in the buffer.
Admin	Collects information specific to the agent, such as the version number.
HostMonitor	Monitors a set of nodes for a particular host table and sets traps when a host becomes active or inactive.
DuplicateIP	Records and updates a list of packets arriving with duplicate IP addresses.
MacToIP	Stores records of the IP addresses associated with a host address for an individual host table.
BoardStatus	Records the status of each logical interface of the RMON agent.

RMON Plus agents are ideally used for monitoring Ethernet, FDDI, or token ring segments. Data from different media types can be collected based on the version of the RMON Plus agent that is used to monitor traffic on your network. Refer to the following table to determine the media type support based on the version of the RMON Plus agent.

RMON Plus Agent	Media Support
Traffic Analysis Agent for NetWare 1.1	Ethernet and token ring
Traffic Analysis Agent for NetWare 1.21 or later	Ethernet, FDDI, or token ring
Traffic Analysis Agent (version 1.30) for Windows NT/2000	Ethernet, FDDI, or token ring

The following figure illustrates the ZfS views that you can display when you use an RMON Plus agent to monitor the nodes and devices on your network.



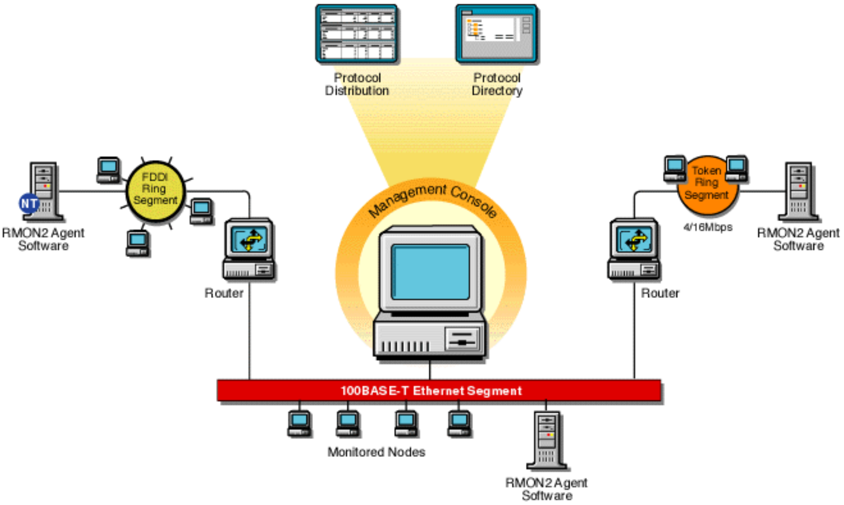
Functionality of RMON2 Agents

RMON agents can be used to collect data from nodes and devices in the physical and the data link layers and RMON2 agents can be used to collect data from nodes and devices in the network and application layers of your network. RMON2 agents can also determine network usage based on the protocol and application used by the nodes in your network. The following RMON2 groups make it possible to view traffic patterns above the data link layer. For details, see RFC 2021 (http://www.isi.edu/in-notes/rfc2021.txt).

RMON2 Group	Description
Protocol Directory	Provides a table of all identifiable protocols and their descriptions.
Protocol Distribution	Provides statistics for each protocol that the agent is configured to track.
Address Map	Maps a network layer address to the corresponding Media Access Control (MAC) address.
Network-Layer Host	Provides statistics for each host by network layer address.
Network-Layer Matrix	Provides statistics for each network conversation between pairs of network layer addresses.
Application-Layer Host	Provides statistics on traffic generated by each host for a specified application layer protocol. Traffic broken down by protocols can be recognized by the Protocol Directory group.
Application-Layer Matrix	Provides statistics on conversations between pairs of network layer addresses for a specified application layer protocol. Traffic broken down by protocols can be recognized by the Protocol Directory group.
User History	Enables the agent to save samples of RMON2 data for any MIB object at specified intervals.
Probe Configuration	Provides remote capability for configuring and querying agent parameters such as resets, software updates, IP address changes, and trap destinations.
RMON Conformance	Provides information to management software regarding the status of support for the groups.

IMPORTANT: The Console supports only the Protocol Directory and Protocol Distribution groups.

The following figure illustrates the ZfS views that you can display when you use an RMON2 agent to monitor the nodes and devices on your network.



Functionality of Bridge Agents

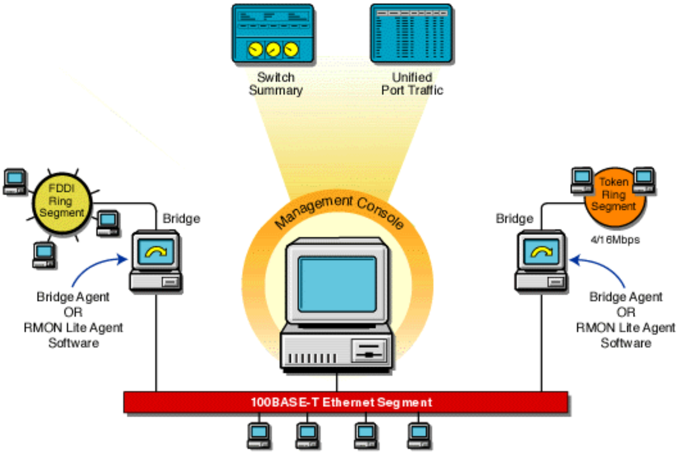
Bridges are used to connect LAN segments below the network layer. A bridge connects two or more physical networks, forwarding packets between networks based on the information in the data link header.

Bridge agents collect information in the following five Bridge groups. You can use this information to monitor switched networks. For details, see RFC 1493 (http://www.isi.edu/in-notes/rfc1493.txt).

Group	Description
Base	Stores information about objects that are applicable to all types of bridges.
Spanning Tree Protocol	Stores information regarding the status of the bridge with respect to the Spanning Tree Protocol.
Source Route Bridging	Provides information that describes the status of the device with respect to source route bridging.

Group	Description
Transparent Bridging	Provides information that describes the entity's state with respect to transparent bridging.
Static	Collects information that describes the entity's state with respect to destination address filtering.

The following figure illustrates the ZfS views that you can display when you use a Bridge agent to monitor the nodes and devices on your network.



Viewing the Summarized RMON Information

The RMON Summary view provides brief information about RMON service on a selected node. It displays static information about the RMON agent and details of the resources requested by the user from the agent. The resource requests that are displayed in the RMON Summary view are Packet Capture and Host TopN requests.

To view the summarized RMON information:

1. Click RMON under Services within a node.
2. Click View > RMON Summary.

The following table describes the static information displayed in the RMON Summary view.

Statistic	Explanation
Agent Name	Name of the RMON agent monitoring the selected segment
IP Address	IP address of the node on which the RMON agent is installed
IPX^{TM} Address	Internetwork Packet Exchange^{TM} (IPX) address of the node on which the RMON agent is installed
Number of Interfaces	Number of logical interfaces for the management server on which the RMON agent is installed
Version	Version number of the RMON Plus agent
Type of RMON Service	Type of the RMON agent: RMON, RMON Plus, or RMON2
Status of the Agent	Status of the RMON agent

The RMON Summary view displays the resource information described in the following table.

Statistic	Explanation
Resource Name	Type of resource requested: ◆ Packet Capture ◆ Host TopN
Owner	Owner string corresponding to the control entry of the row
Index	Channel, Filter, or Buffer control indexes for the Packet Capture resource and the Control index for the Host TopN resource

To delete a resource:

1. Select a row from the Resource table.
2. Click Delete.

   When you delete a resource, the entry on the agent corresponding to the selected row is deleted.

Role-Based Traffic Analysis Tasks

ZfS lets you perform the following traffic monitoring tasks based on your role:

- Add nodes to be monitored for inactivity.

  For details, see "Monitoring Nodes for Inactivity" on page 293.

- Add protocols to the protocol directory tree.

  For details, see "Displaying a List of Protocols Used in Your Network" on page 309.

- Capture packets.

  For details, see "Capturing Packets" on page 295.

- Disable nodes from being monitored for inactivity.

  For details, see "Monitoring Nodes for Inactivity" on page 293.

- Delete protocols from the protocol directory tree.

  For details, see "Displaying a List of Protocols Used in Your Network" on page 309.

- Free agent resources.

  For details, see "Viewing the Summarized RMON Information" on page 263.

- Set segment alarms.

  For details, see "Configuring Alarm Options from the Set Alarm Dialog Box" on page 326.

- View conversations.

  For details, see "Viewing Conversations (Traffic) Between Nodes" on page 292.

- View Traffic Analysis Agents.

  For details, see "Selecting the Preferred RMON Agent" on page 271.

- View the protocol directory.

  For details, see "Determining the Distribution of Protocols in a Segment" on page 312.

- View the RMON summary.

  For details, see "Viewing the Summarized RMON Information" on page 263.

- View segment alarms.

  For details, see "Viewing Alarm Statistics for a Segment" on page 283.

- View the segment dashboard.

  For details, see "Determining the Performance of Individual Segments" on page 277.

- View segments monitored for inactivity.

  For details, see "Monitoring Nodes for Inactivity" on page 293.

- View segment protocol distribution.

  For details, see "Determining the Distribution of Protocols in a Segment" on page 312.

- View segment stations.

  For details, see "Listing Statistics for Segments" on page 275.

- View the segment summary.

  For details, see "Viewing the Summarized Segment Information" on page 283.

- View segment trends.

  For details, see "Analyzing Traffic on Segments" on page 274.

- View switch or port traffic.

  For details, see "Viewing Statistics for Ports in a Switch" on page 314.

- View the switch summary.

  For details, see "Viewing the Summarized Switch Information" on page 314.

For more information about role-based services, see "Role-Based Administration" on page 34.

Protocol Decodes Suite Supported by ZfS

ZfS decodes several protocol suites. Using ZfS, you can analyze and troubleshoot problems in the following protocol suites:

- NetWare Protocol Suite
- NetWork File System Protocol Suite
- Systems Network Architecture Protocol Suite

- AppleTalk* Protocol Suite
- TCP/IP Protocol Suite

You need to understand these protocols in order to set up packet capture and interpret the results in the Trace Display window. For more information about these protocol suites and decoding support, see Appendix 10, "Protocol Decodes Suites Supported by ZfS," on page 377

ZfS also enables you to analyze and troubleshoot problems in the following media:

- Standard Ethernet
- IEEE 802.3
- Token Ring
- FDDI

Planning for Segment Monitoring

A baseline defines the typical activity of your network. Keeping a baseline document of activity on a segment lets you determine when the activity is atypical. Atypical activity might be caused by a problem or network growth. To create a baseline activity, you should gather statistical information when the network is functioning typically.

The following sections provide information about creating and using a baseline:

- "Creating a Baseline of Typical Segment Activity" on page 267
- "Using the Baseline Document" on page 268
- "Segment Baseline Document Tips" on page 269

Creating a Baseline of Typical Segment Activity

For segment statistics such as bandwidth utilization, you should create a trend graph that plots information over a period of time. Statistics sampling that gathers data over a short period of time can be misleading. If you have added one or more network components, it is useful to create another baseline against which you can compare future activity.

You can export the data you gather in ZfS into programs, such as spreadsheets, for further analysis and to maintain records over time.

Using the Baseline Document

You can use the baseline document for the following purposes:

- "Using Baseline Documents to Set Alarm Thresholds Appropriately" on page 268
- "Using Baseline Documents to Track Network Growth and Its Effect on Performance" on page 268
- "Using Baseline Documents to Troubleshoot Atypical Segment Activity" on page 269

Using Baseline Documents to Set Alarm Thresholds Appropriately

ZfS lets you set alarm thresholds for statistics on segments monitored by the network monitoring agent software, so that if the threshold is exceeded, you are notified at ConsoleOne. Setting alarm threshold values for statistics on a segment eliminates the need for you to constantly monitor segments for problems.

ZfS provides default values for thresholds of various alarms on Ethernet, FDDI, and token ring segments. Refer to the table in "Configuring Alarm Options from the Set Alarm Dialog Box" on page 326 for a list of alarm statistics tracked by ZfS. By creating a baseline of activity on the segment, you can determine whether the default values are appropriate for segments in your network. For example, after tracking segment utilization, you would set an alarm threshold for bandwidth utilization at about 5% to 10% higher than typical utilization. You are then alerted if utilization is greater than usual for that segment.

IMPORTANT: If you want to use this alarm notification feature, you must enable segment alarms.

Using Baseline Documents to Track Network Growth and Its Effect on Performance

By comparing current network performance against the performance recorded in your baseline document, you can determine how performance is affected by network changes. This comparison also helps you plan for network growth and justify network upgrades and expansion. You can view graphs of real-time trends for various Ethernet, FDDI, and token ring statistics. If an RMON2 agent is installed on a segment, you can also view historical trends for those statistics over hourly, daily, weekly, monthly, and yearly periods. Refer to "Analyzing Trend Data for a Segment" on page 279 for details about how to view a trend of segment performance. Refer to the table in "Choosing Options to Display Stations on a Segment" on page 316 for a list of statistics based on which you can display a trend of segment performance.

Using Baseline Documents to Troubleshoot Atypical Segment Activity

By knowing what the typical network activity is, you can recognize atypical activity, which might help you isolate the cause of a problem.

Segment Baseline Document Tips

You should include the following key characteristics in each network baseline document:

- "Bandwidth Utilization" on page 269
- "Packets Per Second" on page 269
- "Network Error Rates" on page 270
- "Kilobytes Per Second" on page 270
- "Most Active Servers on the Segment" on page 270

Bandwidth Utilization

The bandwidth utilization statistic indicates the percentage of network bandwidth used. Bandwidth utilization is likely to be higher at certain times during the day (for example, when users log in to the network in the morning), week, or month. Tracking bandwidth utilization helps you balance traffic loads among network segments, servers, and routers for a more efficient network. This information also helps you determine the effect of network growth on performance. As new workstations and applications are added to a network, bandwidth utilization typically increases.

Packets Per Second

Monitoring the number of packets on the wire provides information about the traffic on the segment. By looking at the change in the packets per second after a user launches a new application, you can calculate what the increase in packets per second will be when all the users you expect to use the application start using it. Packets per second differs from utilization. Utilization is based on the number of kilobytes on the segment per second, but packets can range in size. Therefore, utilization can increase as a result of an increase in the size or number of packets. If the number of packets increases but utilization does not, it is likely that the number of small packets increased but the increase did not affect utilization.

Network Error Rates

By including error rates in your baseline, you can determine when error rates on the network are atypical. This is important because network errors can bring down the network. A higher error rate can result from a hardware problem or network growth. If errors increase but utilization does not, there might be a problem with a component, for example a faulty network board or transceiver.

Kilobytes Per Second

Tracking kilobytes per second lets you determine the throughput of your network. From this information, you can determine the percentage of the total possible bandwidth that is in use. For Ethernet networks, the maximum possible utilization is 10 Mbps. For token ring networks, the maximum possible utilization is 4 or 16 Mbps (depending on the hardware).

Most Active Servers on the Segment

Keeping track of the top three servers on the network helps you distribute the load among them as you add new users and applications. See “Viewing Statistics of the Top 20 Nodes” on page 286 for details about how to display a list of top nodes on a monitored segment. You should also monitor the number of Request Being Processed packets. A constantly increasing number of these packets indicates a server overload condition. You can monitor these packets by doing a packet capture and decode. See “Capturing Packets” on page 295 and “Displaying Captured Packets” on page 299 for details about how to capture and display decoded packets.

With the Segment Trends view, you can view many segment statistics and export that data into another application (such as a spreadsheet) for later analysis. The data is saved as a text file that stores statistical values of the trend you display. To export the trend data to a file, click the Export button in the toolbar of the Segment Trends view. For details, see “Analyzing Trend Data for a Segment” on page 279.

You can view current utilization for a segment through the Segment Dashboard view. To access this view, select a segment, click View > click Segment Dashboard. For details, see “Determining the Performance of Individual Segments” on page 277.

Preparing to Analyze Network Traffic

The ZfS software components include the Traffic Analysis Agent for NetWare and Traffic Analysis Agent for Windows NT/2000. You can install the network monitoring agent on the management server or on an independent NetWare or Windows NT/2000 server. The agent monitors the traffic on the segment it is connected to, gathers information about the nodes and devices on that segment, and makes this information available to the management server, which provides it to ConsoleOne. The agent also sends traps to the management server that are forwarded to ConsoleOne. The management server and the monitoring agent communicate using SNMP. ZfS provides default values for SNMP parameters.

The following sections provide information about specifying a preferred agent for monitoring traffic on the segment and changing the default SNMP settings:

- "Selecting the Preferred RMON Agent" on page 271
- "Setting Up SNMP Parameters" on page 272

Selecting the Preferred RMON Agent

If more than one remote monitor (RMON) agent exists on a selected segment, you can choose which agent is to monitor the nodes on the segment from the RMON Agent property page. This page displays a list of servers on which the RMON Agent is installed. The agent installed on the server that you choose from this list becomes the preferred agent. The preferred agent is the primary agent that monitors the segment and sends information about segment activity to ConsoleOne.

To display the RMON Agent property page:

1. Select a segment from ConsoleOne.
2. Click File > Properties > the RMON Agent tab.

The following table describes the statistics displayed in the RMON Agent property page.

Statistic	Explanation
Preferred	Displays a check mark if the selected server is chosen to be the preferred RMON agent server.

Statistic	Explanation
Agent Name	Displays a list of all the servers on which the RMON agent is installed.
Version	Displays the version of the RMON agent installed on the server. The version is dynamically obtained. If ZfS cannot connect to the remote agent, or if a third-party agent is installed on the selected segment, this field is blank.
Status	Displays the status of the RMON agent on the segment.
MAC Address	Displays the physical Media Access Control (MAC) address of the node.
Interface Index	Displays the number of interface indexes in which each interface corresponds to a segment that the node can connect through the network board.
Available RMON Services	Displays the list of RMON services available from the selected agent: RMON, RMON Plus, or RMON2.

To choose an RMON agent as the preferred agent:

1. Choose a server or workstation name from the list of names displayed in the property page.

   The server and workstation names displayed are those on which the RMON agent is installed.

2. Click Apply.

Setting Up SNMP Parameters

When you request dynamic information to be displayed in ConsoleOne, it seeks the information from the management server. The management server communicates with the network monitoring agent using SNMP, obtains the required information from the agent, and provides it to ConsoleOne. SNMP communications between the server and the agent are based on default SNMP settings provided by ZfS. You can change the default SNMP settings using the

SNMP dialog box, which displays in ConsoleOne if an error occurs when the management server is communicating with the monitoring agent.

You can use the SNMP dialog box to specify the community strings and security settings for SNMP communication. You can change the default time-out value for the server to connect with the agent. If the default time-out value is exceeded before the server can communicate with the agent or if the community string of the server does not match that of the agent, the SNMP dialog box displays in ConsoleOne with the current settings. You can use the dialog box to change the current time-out value, the community string, and other SNMP parameters. The changed values are saved in the ZfS database and will be applied for all subsequent traffic management sessions.

To change the SNMP settings for all monitoring agents in your network:

1 Right-click the ZfS domain from ConsoleOne > click Global SNMP Parameters.

To change the SNMP settings for a specific agent:

1 Right-click the node on which the agent is installed from ConsoleOne > click Properties > click SNMP Settings.

The following table describes the SNMP parameters displayed in the SNMP Settings property page.

Parameter	Explanation
Community String	Community string of the node requesting dynamic data from the agent
Timeout	Maximum duration the server should wait for a response from the agent
Retry	Number of times the server should try to connect with the agent
Secure Set	Encrypts the packet sent by the management server to the monitoring agent
Secure Get	Encrypts the packet sent by the monitoring agent to the management server

HINT: If the network monitoring agent is running on NetWare 4.*x* and your network is IPX enabled, use the SNMP dialog box to communicate with the agent using IPX. This will significantly improve the performance of ZfS traffic analysis components.

Analyzing Network Traffic

You can use ZfS to monitor your network and collect information such as a summary of real-time statistics to determine the performance of your network, or detailed real-time statistics to determine the performance of segments in your network.

Information about the activity of nodes and segments in your network is presented in views containing tables, dials, and graphs. You can use the information to perform various traffic management tasks such as establishing a baseline on your network to help you identify typical traffic loads and control network problems, and analyze real-time performance to help you balance traffic loads among network segments, servers, and routers. You can also collect node information to help you focus on specific entities that might be the source of problems.

The following sections provide detailed information about how you can use ZfS to manage your network monitoring activities:

- "Analyzing Traffic on Segments" on page 274
- "Analyzing Traffic on Nodes Connected to a Segment" on page 286
- "Capturing Packets" on page 295
- "Displaying Captured Packets" on page 299
- "Analyzing Traffic Generated by Protocols in Your Network" on page 308
- "Analyzing Traffic on Switches" on page 313

Analyzing Traffic on Segments

Monitoring the segments on your network helps you keep the network operating cost effectively, consistently, and smoothly. Based on the kind of information you want to obtain, you can choose the agent that will monitor the segments on your network. For details, see "About Network Monitoring Agents" on page 256. The agent monitoring the segments will collect traffic data and provide real-time or historical information to you when you require it.

ZfS provides various views you can use to obtain statistical information about monitored segments. You can choose to view statistical information for all segments in your network or for individual segments. You can view a trend of segment performance and a list of alarms generated on a segment. The Segment Summary view provides a summary of segment performance.

The following sections provide information to help you analyze the performance of segments in your network:

- "Listing Statistics for Segments" on page 275
- "Determining the Performance of Individual Segments" on page 277
- "Analyzing Trend Data for a Segment" on page 279
- "Viewing Alarm Statistics for a Segment" on page 283
- "Viewing the Summarized Segment Information" on page 283

HINT: Servers running the remote monitor (RMON) agent can notify you when nodes you selected for monitoring become inactive. For details, see "Monitoring Nodes for Inactivity" on page 293. Sometimes the RMON agent server must be taken off the network for maintenance. To prevent the segment from going unmonitored, you can choose a different RMON agent on the segment. For details, see "Selecting the Preferred RMON Agent" on page 271.

Listing Statistics for Segments

The List Segments view displays a list of segments and statistical information for each segment on your network. Statistics are displayed in columns of the table in the view. The view displays a list of segments associated with the object or node you selected from ConsoleOne.

See "Analyzing Traffic on Nodes Connected to a Segment" on page 286 for details about how to use ZfS to get information about nodes on individual segments.

To view statistical information of all segments:

1. Select an Area or a node from ConsoleOne.
2. Click View > List Segments.

   If you select an Area, the List Segments view displays statistics for all segments found within that Area. If you select a node, statistics for all segments connected to that node will be displayed.

The following table describes the statistics displayed for each segment. The sampling interval for updating statistics on segments is 15 seconds.

HINT: Statistics of segments are displayed in the List Segments view only if the segments are monitored by a Traffic Analysis Agent for NetWare or Traffic Analysis Agent for Windows NT/2000.

Statistic	Explanation
Segment Name	Segment name or address.
Type	Physical segment type: Ethernet, FDDI, token ring, PPP, and unknown. Unknown indicates the segment whose physical segment type is other than the one listed.
Speed (Mbps)	The speed of the segment, as determined by the speed of the network board that attaches the RMON agent to the segment and factors such as the cable type of the segment. The value in this column appears only if you have at least one RMON agent connected to at least one server on your network.
Utilization%	Average percentage of the bandwidth currently used by all traffic on the segment.
Packets/s	Average number of packets per second currently transmitted on the segment.
KBytes/s	Average number of kilobytes per second currently transmitted on the segment.
Errors/s	Average number of errors per second currently appearing on the segment.
Message	Status of the RMON Agent on the segment. For details, see "Selecting the Preferred RMON Agent" on page 271.

As ZfS polls segments, messages in the Messages column vary. These messages display the status of the preferred RMON agent on the segment.

The preferred RMON agent is the node you selected to send information about the segment to ConsoleOne. You can make this selection from the RMON Agent property page. For details, see "Selecting the Preferred RMON Agent" on page 271.

You can modify the view to show fields; format columns; sort and group items; change the font of text fields; or display grid lines in the table view by selecting the required option from View > Settings. For details, see Chapter 3, "Understanding Network Discovery and Atlas Management," on page 71.

Determining the Performance of Individual Segments

ZfS provides real-time statistical information about the monitored segment on your network. This information is displayed in the Segment Dashboard view. The information displayed in this view is useful if you want to troubleshoot a segment.

The Segment Dashboard view displays four gauges that display the real-time statistics for a monitored segment. The lower portion of the view displays a bar graph of the top eight nodes, based on the value selected from the drop-down list. By default, it is based on packets out per second. See "Viewing Statistics of the Top 20 Nodes" on page 286 for details about how to display a list of the most active nodes on a monitored segment.

You can configure the Segment Dashboard view to display the top eight nodes based on a different statistic. You can also choose to display or disable the top nodes graph. For details, see "Choosing Options to Display Stations on a Segment" on page 316.

You can set alarm threshold values on segment alarms for packets per second, broadcasts per second, and utilization percentage statistics displayed in the Segment Dashboard view. For details, see "Defining Alarm Thresholds for Statistics Displayed in the Segment Dashboard View" on page 278.

To view statistical information of an individual segment:

1. Select a segment from ConsoleOne.
2. Click View > Segment Dashboard.

The Segment Dashboard view displays four gauges that display real-time statistics for a monitored segment. The peak value is indicated by a line on each bar in the graph. The following table describes the statistics displayed in the Segment Dashboard view.

Statistic	Explanation
Packets/s	Number of packets per second currently transmitted on the segment
Utilization%	Percentage of maximum network capacity currently consumed by packet traffic on the segment
Error/s	Number of error packets per second currently transmitted on the segment

Statistic	Explanation
Broadcasts/s	Number of broadcast packets per second currently transmitted on the segment (a broadcast packet is sent to all addresses on the segment)

Statistics are updated every five seconds. The numeric value of each statistic is displayed in the gauge.

Defining Alarm Thresholds for Statistics Displayed in the Segment Dashboard View

To set alarm threshold values for statistics displayed in the Segment Dashboard view:

1. Click the black ring outlining the gauge.
2. Drag the ring to increase or decrease the default values.

   As you drag the ring, the color of the ring changes to red.
3. Stop at the value you want to set as the threshold value for the statistic.

   The color of the ring is displayed in red up to the selected threshold value.

   If the statistic on the monitored segment exceeds the threshold value, the RMON agent sends a trap to the management server, which forwards it to ConsoleOne and an alarm is generated.

Viewing the Graph of the Top Nodes on a Monitored Segment

The lower portion of the Segment Dashboard view displays a bar graph of the top eight nodes on a monitored segment. The default statistic on which the graph is based is packets out per second. You can change the statistic on which the graph is based. For details, see "Choosing the Statistic Based on Which Top Nodes Graph Is Displayed" on page 323. You can also choose to display or disable the top nodes graph. For details, see "Choosing Options to Display the Top Nodes Graph" on page 323.

Statistics for the graph are updated every five seconds. Every 60 seconds, the graph is re-sorted and the new top nodes are displayed. At this point, new nodes might be added and existing nodes might be discarded from the list.

Analyzing Trend Data for a Segment

ZfS allows you to determine trends of traffic patterns on the monitored segment. You can view the trend of segment performance from the Segment Trends view. You can use trend information to create a baseline of typical activity on segments. Having a baseline helps you set appropriate thresholds for segment alarms and plan maintenance activities and backups. Additionally, if problems occur on the segment, you can compare the typical traffic level against the atypical traffic level to help you discover the cause of the problem. For details, see "Creating a Baseline of Typical Segment Activity" on page 267.

The following topics will help you analyze trend data:

- "Understanding the Trend Display" on page 279
- "Viewing Trend Statistics" on page 280

Understanding the Trend Display

Segment trend data is displayed depending on the type and settings of the RMON agent monitoring the selected segment.

- If RMON Plus is the segment's preferred RMON agent, you can view current trends gathered every 30 seconds over the last hour and historical trends displayed over hourly, daily, weekly, monthly, or yearly periods.

  IMPORTANT: If an RMON agent is installed on more than one node on a segment, the node you select in the RMON Agent property page as the node to send information about the segment to ConsoleOne is the preferred RMON agent server. For more details, see "Selecting the Preferred RMON Agent" on page 271.

- If RMON Plus is not selected as the preferred RMON agent for the segment, you can view only the current trends for the selected segment. Current trends are gathered every 30 seconds over the last hour. Select an RMON Plus agent as the preferred RMON agent for the segment to be able to view historical trends.
- If the preferred RMON agent is Traffic Analysis Agent for NetWare version earlier than 1.30, you can view current trends gathered over the past hour and trends for the past day.
- Real-time trends will not be displayed if memory usage is excessive or if configuration settings in the RMON agent are unacceptable.
- If the RMON agent is down or is experiencing problems, the trend for a monitored segment will be displayed as a broken graph.

- If the preferred RMON agent is a Novell Traffic Analysis Agent (version 1.30 or greater) or a third-party agent that implements the token ring Extensions to the Remote Network Monitoring MIB (RFC 1513), the segment bandwidth utilization graph displays slightly lower values than the actual utilization in the trend for the token ring segment view. This is because the MAC layer statistics are not taken into consideration for the utilization calculation.

Viewing Trend Statistics

To view the trend statistics for a segment:

1. Select a segment from ConsoleOne.
2. Click View > Segment Trends.

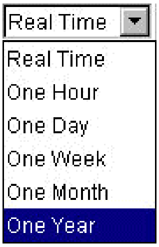
Trend graphs are displayed for Ethernet, FDDI, and token ring segments. The default statistics, based on which graphs are displayed for the three types of segments, are as follows:

Segment Type	Default Statistic
Ethernet	Total packets, good packets, and error packets
FDDI	Total packets
Token ring	Total packets

The toolbar options let you change the time span of the trend you view, select statistics based on which you want the graph to be displayed, and export data to a file.

The following table describes the toolbar options in detail.

Option	Explanation
Profile	Displays the Profile dialog box, from which you can select a default profile. The default profile displays a trend with statistical information for total packets, good packets, and error packets on the monitored segment. If you choose not to use the profiles listed in the Select Profile list, you can select the required statistics from the Select Statistics list. You can save the selected statistics if you want to display the trend of a different segment based on the statistics you selected. The default profile will be enabled the next time you launch the Segment Trends view.
Legend	Shows what each color in the graph represents. The Legend can be resized.
Stack	Stacks the trends in a single graph representing all selected statistics, on a single vertical axis.
Unstack	Un-stacks the trends and displays the graph as a separate strip for each statistic.
Horizontal Grid	Displays horizontal grid lines in the graph area of the Segment Trend view.
Vertical Grid	Displays vertical grid lines in the graph area of the Segment Trends view.
Scale To Fit	Maximizes or minimizes the graph to fit the trend entirely in the graph area of the view.
Export	Copies the information in the Segment Trends view to a file. The file stores the statistical values displayed by the trend. You can save the data for later analysis.

Option	Explanation
Time Scale drop-down list  Real Time Real Time One Hour One Day One Week One Month One Year	◆ Real Time: Displays a current trend graph. The default sampling time for this graph is once every minute. This graph updates in real time. ◆ One Hour: Displays a historical graph of the selected trend with a time span of one hour. ◆ One Day: Displays a historical graph of the selected trend with a time span of one day. ◆ One Week: Displays a historical graph of the selected trend with a time span of one week. ◆ One Month: Displays a historical graph of the selected trend with a time span of one month. ◆ One Year: Displays a historical graph of the selected trend with a time span of one year. Historical trends such as hourly, daily, weekly, monthly, and yearly trends are available only when Traffic Analysis Agent for NetWare version 1.1 or later is installed on the segment's preferred traffic analysis agent server.

The File menu of the Segment Trends view can be used to print the statistical information of the current trend or to export the statistical information of a trend to a file and store the data in text format. You can later import the file into a spreadsheet for analysis.

You can view earlier or ensuing trends and change the size of the graph by using the options available in the graph area of the Segment Trends view, as shown in the following table.

Option	Description
Scale Up	Increments the Y-axis of the graph by half the current size with each click.

Option		Description
Scale Down	↓	Decrements the Y-axis of the graph by half the current size with each click.
Previous	←	Displays the preceding graph based on the profile or statistics chosen. Enabled only when historical trends are displayed.
Next	→	Displays the subsequent graph. Enabled only when historical trends are displayed.

Viewing Alarm Statistics for a Segment

ZfS tracks alarm statistics for segments. Alarms are generated when threshold values for statistics on a segment are exceeded. You can view a list of all the alarms for the monitored segment in the Segment Alarms property page.

To view alarm statistics for a segment:

1. Select a segment from ConsoleOne.
2. Click File > Properties > the Segment Alarms tab.

ZfS provides default threshold values for various segment alarms. You can enable or disable the default values for a monitored segment. If you choose not to use the default values, you can set the threshold value using the Set Alarm dialog box. See "Configuring Alarm Options from the Set Alarm Dialog Box" on page 326 for details about how to set segment alarms.

If a segment does not have an RMON agent connected to it, an error message is displayed.

Viewing the Summarized Segment Information

The Segment Summary view provides brief information about a monitored segment in your network. It displays static information about the monitored segment, whether the segment is monitored or not, and information about the alarms generated on the segment. At a glance, you can determine the utilization of network capacity by nodes on the monitored segment, view a trend based on packets transmitted by nodes on the segment, and see the distribution of protocols on the segment.

To view the summarized segment information:

1. Select a segment from ConsoleOne.
2. Click View > Segment Summary.

The following table describes the static information displayed in the Segment Summary view.

Statistic	Explanation
Name	Name of the segment
Type	Media type of the segment: Ethernet, FDDI, or token ring
IP Address	IP addresses of the segment
IPX Address	IPX address of the segment
Primary Agent	Name of the preferred agent monitoring the nodes and traffic on the segment
Agent Status	Status of the preferred agent monitoring the nodes and traffic on the segment
Nodes	Number of nodes on the segment
IP Nodes	Number of nodes on the segment that have an IP address
IPX Nodes	Number of nodes on the segment that have an IPX address
Servers	Number of NetWare servers on the segments
Workstations/Others	Number of nodes on the selected segment that are not NetWare servers
Network Probes	Number of monitoring agents on the selected segment
Switches	Number of switches on the segment
Routers	Number of routers used to connect nodes and devices on the segment
Hubs	Number of hubs on the segment

The Segment Summary view displays information about alarms generated on a monitored segment, as described in the following table.

Statistic	Explanation
Severity	Severity level attributed to the trap.
From	Network address of the device that sent the alarm to the alarm management system.
Summary	Summary of the event, often including the name or address of the object affected by the alarm.
Owner	Segment or device affected by the alarm.
Received Time	Date and time when the alarm management system received the alarm.
Type	Generic description of the alarm, for example, Volume out of disk space.
Category	Displays the category of the alarm based on the MIB that defines the trap-type objects. The category is directly related to the MIBs included in the management server MIB pool. For example, the category for NetWare servers is based on the NetWare Server Alarm MIB.

The Segment Summary view displays dynamic information about a monitored segment, as described in the following table.

Statistic	Explanation
Utilization%	Displays a dial representing the real-time values of the network capacity consumed by packet traffic on the segment.
Packets	Displays the trend based on packets transmitted on the segment. Displays real-time trends for segments monitored by RMON agents and daily trends for segments monitored by RMON Plus agents.

Statistic	Explanation
Protocol Distribution	Displays a pie chart representing the distribution of application layer protocols for which the agent monitoring the segment can collect data. Each slice represents a protocol suite. Click a slice to view the names of protocols. Enabled if the agent monitoring the selected segment is an RMON2 agent.

Analyzing Traffic on Nodes Connected to a Segment

ZfS provides various views you can use to obtain information about nodes connected to the monitored segments in your network.

The following sections provide information that will help you monitor the performance of nodes connected to the segments in your network:

- "Viewing Statistics of the Top 20 Nodes" on page 286
- "Viewing Statistics of Nodes on an FDDI Segment" on page 288
- "Viewing Statistics of Nodes on a Token Ring Segment" on page 289
- "Viewing Conversations (Traffic) Between Nodes" on page 292
- "Monitoring Nodes for Inactivity" on page 293

Viewing Statistics of the Top 20 Nodes

You can use ZfS to determine the statistics of the most active nodes on a segment for a wide range of performance statistics. This is useful if you want to discover which node is generating the most traffic based on a particular statistic. For example, you can find the heaviest source of broadcast traffic.

The Stations view displays a list of all nodes on a monitored segment. You can use this view to determine the top 20 nodes on a monitored segment. The view lists the top 20 stations sorted by packets out per second. You can choose a different statistic based on which you want the top 20 nodes to display. For details, see "Choosing a Statistic Based on Which Top 20 Nodes Are Displayed" on page 317. If there are fewer than 20 top nodes, only the available number of top nodes are listed.

To view the statistics of the top 20 nodes on a segment:

1 Select a segment from ConsoleOne.

2 Click View > Stations.

3 From the Stations view, click View > Show Top N Stations.

The Stations view displays columns that provide statistical information for each station. The following table describes the statistics displayed in the Stations view.

Statistic	Explanation
MAC Address	Physical Media Access Control (MAC) address of a node
Node	Name of the node (or address, if the name is not in the database)
Util.%	Percentage of maximum network capacity consumed by packets sent by a node
Packets/s In	Packets per second received by a node
Packets/s Out	Packets per second transmitted by a node
Bytes/s In	Bytes per second received by a node
Bytes/s Out	Bytes per second transmitted by a node
Errors/s	Errors per second transmitted by a node
Broadcasts/s	Broadcast packets per second transmitted by a node
Multicasts/s	Multicast packets per second transmitted by a node (packets transmitted to a specific group of nodes)
Protocols	Types of protocols used by a node
First Transmit	Date and time a node first transmitted since the traffic analysis agent was started
Last Transmit	Date and time a node last transmitted since the traffic analysis agent was started

Stations statistics are updated periodically. Every 60 seconds, the table is resorted and new top nodes are displayed. At this point, new nodes might be added and existing nodes might be discarded from the list.

Viewing Statistics of Nodes on an FDDI Segment

ZfS lets you display data for nodes on monitored FDDI ring segments to help troubleshoot problems.

The FDDI Ring Stations view displays statistics for individual nodes on the monitored FDDI ring segment. The view lists the nodes on the segment and shows the order of each node on the ring and which node is the active monitor.

To view the statistics of nodes on an FDDI ring segment:

1. Select an FDDI ring segment from ConsoleOne.
2. Click View > FDDI Stations.

The statistics shown for each node are cumulative since the Traffic Analysis Agent for NetWare was last started and are updated every ten seconds as described in the following table:

Statistic	Explanation
Order	Relative position of the node on the FDDI ring from the traffic analysis agent.
Name	Name of the node or, if the name is not in the database, the physical (MAC) address of the node.
MAC Address	Physical (MAC) address of the node.
Status	Status of the node: ◆ On—The node is actively participating in a ring poll. ◆ Off—The node is not participating in a ring poll.
Duration	Time elapsed since the node was On or Off.
UpStream Neighbor	MAC address of the node upstream to this station on the logical ring.
DownStream Neighbor	MAC address of the node downstream to this station on the logical ring.
Last Entered Time	Date and time the node last entered the ring.
Last Exit Time	Date and time the node last exited the ring.

Statistic	Explanation
SMT Request Type	The SMT request to which the node is responding. Indicates if the node was able to successfully respond to the request. In case of a failure, the response code indicates the reason.
SMT Response Type	The SMT response generated by the node on receiving an SMT request. If the node was unable to respond, the response code indicates the reason.
Request Denied	The cumulative total of request denied responses generated by the node. A request denied frame is generated when the responding node does not support the SMT version number of the requesting node, when a set fails, or when a request for synchronous bandwidth allocation by a node cannot be honored.
In CRC Error	Total number of cyclic redundancy check (CRC) line errors reported by this node.
Out CRC Error	Total number of CRC errors reported by the nearest active downstream neighbor of this station and detected by the probe.
Lost Frames	Total number of lost frame errors received on the network. A lost frame error indicates that the end delimiter of a frame was lost in the network.
In Beacons	Total number of beacon frames detected by the probe that named this station as its upstream neighbor.
Out Beacons	Total number of beacon frames sent by this station and detected by the probe.
Insertions	Number of times the probe detected this station inserting onto the ring.

Viewing Statistics of Nodes on a Token Ring Segment

The Token Ring Stations view displays statistics for individual nodes on the monitored token ring segment. The view lists the nodes on the segment and shows the order of each node on the ring and which node is the active monitor.

To view the statistics of nodes on a token ring segment:

1. Select a token ring segment from ConsoleOne.

2 Click View > Token Ring Stations.

The view displays statistical information as described in the following table. Statistics are cumulative since the RMON agent was started and are updated every ten seconds.

Statistic	Explanation
Order	Relative position of the node on the token ring from the RMON agent.
Name	Name of the node or, if the name is not in the database, the physical (MAC) address of the node.
MAC Address	Physical (MAC) address of the node.
Status	Status of the node: ◆ On—The node is on the ring. ◆ Off—The node is off the ring. ◆ On (Monitor)—The node is on the ring and is the active monitor.
Duration	How long this node has been on or off.
Last Entered Time	Date and time the node last entered the ring.
Last Exit Time	Date and time the node last exited the ring.
Duplicate Address	Total number of duplicate address errors reported, generated when this node detects other nodes using its own address.
Soft Errors	Number of soft errors in packets transmitted by this node.
Inline Errors	The total number of line errors reported by this station in error reporting packets to the ring error monitor and detected by the probe.
Outline Errors	The total number of line errors reported in error reporting packets sent by the nearest active downstream neighbor of this station and detected by the probe.
Internal Errors	Number of internal errors this node has reported. Internal errors generally indicate a recoverable failure of a network adapter board.

Statistic	Explanation
In Burst Errors	The total number of burst errors reported to the Ring error monitor and detected by the probe.
Out Burst Errors	The total number of burst errors reported in error reporting packets sent by the nearest active downstream neighbor of this station and detected by the probe.
AC Errors	Number of times this node could not interpret the Address Recognized Indicator (ARI) and the Frame Copied Indicator (FCI) during the ring process.
Abort Errors	Number of times a node transmitted an abort sequence. Abort sequences are usually transmitted when a node detects an error in frames it is currently transmitting.
Lost Frame Errors	Number of times a node transmitted a frame but failed to receive it back in its entirety.
Congestion Errors	Number of times the node detected a frame addressed to its specific address but could not copy it (generally due to insufficient buffers).
Frame Copied Errors	Number of times a node detected a frame addressed to its specific address with either or both the ARI and FCI bits set to 1. (Indicates that another node is using its address.)
Frequency Errors	Number of times a node's internal clock differed from the ring clock.
Token Errors	Number of token errors. These occur when the token gets corrupted or when the Active Monitor does not see a new frame transmitted in the required amount of time. Only the Active Monitor can report this error.
In Beacon Errors	The total number of beacon frames sent by this station and detected by the probe.
Out Beacon Errors	Total number of beacon frames sent by this station and detected by the probe.
Insertions	Number of times the probe detected this station inserting onto the ring.
Last NAUN	The station that was last named by the probe as the next active upstream neighbor (NAUN).

Viewing Conversations (Traffic) Between Nodes

ZfS provides real-time data about all the network traffic between a selected node and one or more other nodes on a segment. This data can be viewed from the Conversations view. You can use the data displayed in this view to determine specific information about node communication. For example, it can show which nodes communicate with a router or server, determine the load on a server, or examine the traffic flowing to or from a node that is reporting difficulties.

To view conversations between nodes:

1 Select a node from ConsoleOne.

2 Click View > Conversations.

If the selected node is connected to more than one segment, the Select Segment dialog box displays.

2a Select the segment where the node you want to examine traffic is connected > click View > click Conversations.

The Conversations view lists the percentage of traffic that each destination node contributes to the load on the source node. However, due to sample skewing (samples not taking place at the same time) and rounding up of statistics, the numbers in the columns do not always add up to 100%.

The statistics displayed in the Conversations view are updated every 5 seconds. The following table describes the statistics displayed in the Conversations view.

Statistic	Explanation
Node	Name of the destination nodes with which the source node is communicating
% Pkt Load	Percentage of the packet load between a destination node and the source node
% Byte Load	Percentage of the byte load between a destination node and the source node
Pkts/s In	Packets per second received by a destination node from the source node
Pkts/s Out	Packets per second transmitted by a destination node to the source node

Statistic	Explanation
Bytes/s In	Bytes per second received by a destination node from the source node
Bytes/s Out	Bytes per second transmitted by a destination node to the source node
Pkts In	Number of packets received by a destination node from the source node since the view was opened
Pkts Out	Number of packets transmitted by a destination node to the source node since the view was opened
KBytes In	Total kilobytes received by a destination node from the source node since the view was opened
KBytes Out	Total kilobytes transmitted by a destination node to the source node since the view was opened
Protocols	Protocol packet types used by the destination node in this conversation
First Transmit	Date and time that the destination node first transmitted on the network since the traffic analysis agent was loaded
Last Transmit	Date and time that the destination node last transmitted since the traffic analysis agent was loaded
MAC Address	Physical (MAC) address of the destination node

Monitoring Nodes for Inactivity

For segments on which at least one Traffic Analysis Agent for NetWare version 1.0 or later is installed, you can specify the nodes on the segment you want to monitor so that you are alerted if they become inactive. You can do this using the Monitor Nodes for Inactivity view.

Monitoring nodes for inactivity has the following advantages:

- You can monitor any node on the segment, regardless of the protocol the node uses.
- This feature does not impact network traffic because the traffic analysis agent does not poll the nodes to obtain their status.

To view a list of nodes monitored for inactivity:

1. Select a segment from ConsoleOne.
2. Click View > Monitor Nodes for Inactivity.

Another way to monitor connectivity is to specify the target in the Ping window and test the status of the specified node. The Connectivity Test window displays statistics that enable you to determine the status of the specified target. For details, see Chapter 7, "Monitoring Services," on page 241.

By default, the poll interval for refreshing the Monitor Nodes for Inactivity view is zero seconds. You can configure the poll interval based on how often you want the view to be refreshed. For details, see "Specifying the Poll Interval for Refreshing the Monitor Nodes for Inactivity View" on page 331. You can also change the duration for the agent to verify the node before declaring it inactive. For details, see "Specifying the Duration for the Agent to Determine if a Node Is Inactive" on page 331.

IMPORTANT: You do not need to keep the Monitor Nodes for Inactivity view open or ConsoleOne for the nodes to be monitored because the RMON agent is doing the monitoring, not ConsoleOne. The Alarm Manager must be running to record an inactive node in the Alarm Report. If ConsoleOne is not running, check for alarms after you restart it.

To monitor a node for inactivity:

1. Right-click a node from ConsoleOne or from any view that displays a list of nodes > click Monitor Nodes for Inactivity > click Add.

To disable a node from being monitored for inactivity:

1. Right-click the node that is monitored for inactivity > click Monitor Nodes for Inactivity > click Delete.

IMPORTANT: After the addition of any inactive node, if the NIC card of the node is changed, you will be able to see the node in the Monitor Node for Inactivity view but will not be able to delete it because of the change of MAC address.

Statistics displayed in the Monitor Nodes for Inactivity view are described in the following table.

Statistic	Explanation
Name	Displays a list of nodes that are being monitored for inactivity
MAC Address	Displays the MAC address of the network interface
Status	Displays the status of a node as active or inactive

You can open the Monitor Nodes for Inactivity view to check the Status column any time ConsoleOne is running. To do this, complete the following steps:

1. Select a segment from ConsoleOne.
2. Click View > Monitor Nodes for Inactivity.

   The Status column displays if the selected node is active or inactive.

Capturing Packets

ZfS provides packet capture and decoding tools that help you analyze your network activity and identify the source of network problems. Capturing and decoding packets can help you troubleshoot network problems by giving you detailed information about what is actually happening on a segment.

ConsoleOne can request packet capture on any monitored segment. Each RMON agent captures packets on the segment it monitors and stores information in its local buffer.

The following sections contain detailed information about capturing packets:

- "Defining a Capture Filter" on page 295
- "Starting Packet Capture" on page 298
- "Creating Simultaneous Packet Capture" on page 298
- "Stopping Packet Capture" on page 299
- "Restarting a Stopped Packet Capture" on page 299
- "Saving and Viewing the Captured Packets" on page 299

Defining a Capture Filter

ZfS provides a capture filter with default values you can use to capture packets on any monitored segment. You can modify the values by defining a filter. For example, if you want to capture only NetWare packets sent by a certain node, you can define a filter to capture only those packets. As a result, the buffer has more space to store your selected packets.

When you specify a capture filter, you are specifying the packets to capture (include) in the buffer on the RMON agent, not the packets to exclude. When you specify both a node and a protocol, packets must meet both criteria to be captured. If you select more than one protocol family, packets can meet either protocol criterion to be captured.

To define a capture filter:

1. Select a node or a segment from ConsoleOne.
2. Click File > Actions > Capture Packets.
3. Type a name in the Buffer Name text box, if you do not want to use the default name.

   The buffer name helps you keep track of multiple captures on the same segment.
4. Type or select the source and destination nodes from the Stations box. You can also click the Find Node icon to select the node from the Find dialog box, an atlas component.

   The Stations box displays a list of nodes on the segment from which the user can capture packets. You can select from Hardware, IP, or IPX stations.

   If you choose ANY in both the source and destination node list, all packets sent by or received from any node are captured.
5. Select the direction of traffic flow between the nodes.

   Click an arrow option from the drop-down list to specify the direction of the traffic flow. The available node and traffic flow directions are shown in the following table.

Node	Arrow	Node	Effect
node1	<==>	node2	Capture packets that node1 sends to node2 and packets that node2 sends to node1.
node1	<==>	ANY	Capture packets that node1 sends to any node and packets that node1 receives from any node. This is equivalent to ANY <==> node1.
ANY	<==>	ANY	Capture all packets sent by or received from any node.
node1	==>	node2	Capture packets that node1 sends to node2. This is equivalent to node2 <== node1.
node1	==>	ANY	Capture packets that node1 sends to any other node. This is equivalent to ANY <== node1.
node1	<==	node2	Capture packets that node2 sends to node1. This is equivalent to node2 ==> node1.

Node	Arrow	Node	Effect
node1	<==	ANY	Capture packets that any node sends to node1. This is equivalent to ANY<== node1.

6 If you want to filter on protocols used, add the protocol suites you want to the Selected list box.

To add a protocol to the Selected list box, select it from the Available list box > click Add.

or

To delete a protocol from the Selected list box, select it > click Remove.

All protocols are selected by default when you first use ZfS. If no protocols are listed in the Selected list box, all protocols are captured.

See "Protocol Decodes Suite Supported by ZfS" on page 266 for details about the protocol decoding support that ZfS provides.

7 Specify what kind of packets to capture on Ethernet, FDDI, or token ring segments.

The default statistics for the segments are listed in the following table.

Segment Type	Available Statistics	Default Statistics
Ethernet	Only good packets, only error packets, or both good and error packets.	Good packets and error packets
FDDI ring	All packets, LLC packets, MAC packets, or SMT packets.	All packets
Token ring	All packets, non-MAC packets, or MAC packets. MAC packets are used to manage the operation of the token ring.	All packets

8 Specify whether to stop packet capture or to overwrite the oldest packets in the buffer with newer ones when the buffer is full.

Continuing packet capture means that a stop criteria does not exist and new packets will overwrite those already captured. You will need to manually stop packet capture if you select to overwrite the oldest packets.

9 Specify a buffer size.

Select a buffer size from the drop-down list or specify the size you want. The default buffer size is 32 KB.

The RMON agent will attempt to provide the buffer size requested. If not enough space is available in server memory for a large buffer, the RMON agent cannot create the requested size.

10 Select a slice size.

A slice specifies the maximum number of bytes of each packet, counting from the packet header, to keep in the buffer. This helps maximize the number of packets you can store in your buffer space, as well as reduce the load on the RMON agent to process captured packets. If you want to decode protocol header information, you need only 100 to 150 bytes. The rest is typically data that you need only if you suspect a data corruption problem. However, on certain very large packets, slicing can cause incorrect decodes by truncating information.

Your capture filter is now set up. If you decide not to capture packets, click the Cancel button.

Starting Packet Capture

To start packet capture:

1. Define a capture filter. See "Defining a Capture Filter" on page 295 for the procedure.
2. Click OK to apply the filter settings on the preferred RMON agent of the segment.
3. Click Start in the Capture Status dialog box.

When you start packet capture, the Start button in the Capture Status dialog box toggles to read Stop and the activity indicator reflects the capture buffer storage as it progresses. As packets that meet the filter criteria are captured, the capture buffer will begin to store the packet data, and a box below it will display the number of packets captured. The needle stops turning when the capture buffer is full.

Creating Simultaneous Packet Capture

You can create simultaneous packet captures by repeating the procedure you followed to start the first capture. This lets you set up and run captures with different capture criteria.

You can run a maximum of 20 packet captures with different capture criteria.

Stopping Packet Capture

When you set up a capture filter, you choose whether to stop packet capture when the capture buffer is full or to continue to capture packets but overwrite the oldest packets in the buffer.

By default, the packet capture will stop when the capture buffer is full. If you select to overwrite when the buffer is full, you must stop packet capture manually.

To stop packet capture manually, click the Close button in the Capture Status dialog box.

IMPORTANT: If you restart packet capture from the Packet Capture Setup window, the existing buffer is deleted and refreshed.

Restarting a Stopped Packet Capture

When the Packet Capture Setup window is open, you can start and stop capturing packets using the Start/Stop toggle button in the Capture Status dialog box. If ZfS is capturing packets, the button is labeled Stop; if it is not capturing packets, the button is labeled Restart. The RMON agent buffer is cleared when you restart.

Saving and Viewing the Captured Packets

You can save captured packets to a file and view as many files as you want, either while you are viewing a capture buffer or independently.

To view the saved packet capture files:

1. Click Tools > View Packet File.

   The File Open dialog box is displayed.

2. Browse and select the packet capture file.

   The .TR1 file extension will be appended automatically.

Displaying Captured Packets

You can display and view decoded packets stored in the capture buffer from the Trace Display window by clicking the View button in the Capture Status dialog box. If you display this window while packets are being captured, capture automatically stops.

ZfS retrieves packet data from the RMON agent only as necessary for ConsoleOne to decode and display the packets as you view them. This minimizes the amount of packet data transferred between the RMON agent and ZfS. If you prefer not to display all the packets you captured, you can create a display filter to display only a defined group of captured packets. For details, see "Defining the Display Filter" on page 304.

The following sections provide information on how you can view captured packets and perform trace display operations:

- "Viewing Captured Packets" on page 300
- "Filtering Packets for Display" on page 303
- "Defining the Display Filter" on page 304
- "Selecting and Decoding a Different Packet" on page 306
- "Highlighting Protocol Fields and Hexadecimal Bytes" on page 306
- "Saving Packet Files" on page 307
- "Opening Packet Files" on page 308
- "Printing Packets" on page 308

ZfS provides default settings based on which captured packets are displayed in the Trace Display window. To change the default values provided for displaying captured packet, see "Choosing Options to Display a Captured Packet" on page 325.

Viewing Captured Packets

You can use the Trace Display view to view the decoded packet capture information, the packet data in hexadecimal format, and a summary of the captured packets:

To view a captured packet:

1. Select a node or a segment from ConsoleOne.
2. Click File > Actions > Capture Packet.
3. Capture packets using the capture filter of your choice. See "Defining a Capture Filter" on page 295 for details.
4. Click the View button in the Capture Status dialog box.

The Trace Display window contains three panes that display captured and decoded packets, as described in the following sections:

- “Viewing the Packet Decode” on page 301
- “Viewing Packet Data in Hexadecimal Format” on page 301
- “Viewing a Summary of Captured Packets” on page 302

When you view packets initially, the first packet in the Summary pane is highlighted and selected. The contents of that packet are displayed in the Decode pane. If you select a different packet in the Summary pane, it is highlighted and the Decode pane displays its decoded contents.

You can change the size of the Trace Display panes by dragging the divider between windows.

Viewing the Packet Decode

The Decode pane displays detailed information about the contents of a selected packet. The packet contents are interpreted (decoded) and displayed by protocol fields.

By default, the Decode pane displays fully decoded packet data. You can configure the Trace Display window to display the decoded packets either as full protocol decodes or by one line per protocol layer. See “Choosing Options to Display a Captured Packet” on page 325 for details about how to change the default settings.

Viewing Packet Data in Hexadecimal Format

The Hexadecimal pane shows uninterpreted packet data in hexadecimal format. The ASCII or EBCDIC portion of the Hexadecimal pane (to the right) displays a dot for every hexadecimal byte that has no ASCII or EBCDIC equivalent.

The first column in the pane indicates the offset in hexadecimal bytes. The offset is the number of bytes counting from the beginning of the header. For example, the first three lines have the following offset:

- Hexadecimal 0—indicates zero offset
- Hexadecimal 10—indicates decimal 16 offset (16 bytes precede this)
- Hexadecimal 20—indicates decimal 32 offset (32 bytes precede this)

Regardless of whether you choose to display one-line decoded or fully decoded packets in the Decode pane, entire packets are displayed in the Hexadecimal pane. The Hexadecimal pane and the highlighting tool are especially helpful with the full-decode display when you are trying to associate protocol fields with specific bytes in a packet. For details, see "Highlighting Protocol Fields and Hexadecimal Bytes" on page 306.

Viewing a Summary of Captured Packets

The Summary pane gives you an overview of the conversation between the source and the destination nodes. You can select a packet in this pane for further decoding and display in the other panes. You can scroll the pane horizontally, and you can change the size and position of the columns in the pane.

Statistical information about the captured packets displayed by the Summary pane is described in the following table:

Statistic	Explanation
No.	Numbers the packets in order of arrival at the traffic analysis agent.
Source	IP address, IPX address, or the physical (MAC) address of the node that sent the packet. Names are stored in the database. If no name is found in the database, the MAC address is displayed.
Destination	Node to which the packet was sent. The node is displayed as the IP address, IPX address, or the physical (MAC) address of the node.
Layer	Abbreviation of the highest protocol layer in the packet. It might display NCP for NetWare Core Protocol™ (NCP™) software, ether for the Ethernet data link layer, RTMP for the AppleTalk Routing Table Maintenance Protocol layer, or 802.2 for the IEEE 802.2 Logical Link Control layer. If you choose the full decode option, the Decode pane displays the full name of the protocol layer and all its fields. The Hexadecimal pane shows the entire packet.
Summary	Brief description of the contents of the highest protocol layer.
Error	Type of errors, if any, in the packet. This column is displayed only for Ethernet media.
Size	Number of bytes in the packet. Packet size always excludes the packet preamble and the CRC.
Absolute Time	Clock time on your computer when the packet arrived.

Statistic	Explanation
Interpacket Time	Time elapsed from the end of the preceding packet to the end of the current packet.
Relative Time	Time that elapsed since the arrival of the first packet still in the buffer.

Filtering Packets for Display

After you have captured packets, you can apply a display filter to the capture buffer and view only the packets that interest you. You can filter on node names or addresses, protocol families or protocol layers, or contents of a selected field. This is useful in situations when, after you have captured packets, you realize there is a problem with a specific workstation and you want to display only the packets it has sent or received.

Display filtering requires the transfer of a portion of every captured packet from the RMON agent to ConsoleOne. For large captures, this consumes time and network bandwidth. We recommend that you define very specific capture filters rather than filtering during display. However, subsequent filtering of the same capture does not result in additional data transfer from the traffic analysis agent because the data is already transferred to ConsoleOne. Therefore, it is much quicker to filter the same packet capture a second time.

Display filters affect only the display; they do not change the capture buffer. All captured packets remain in the capture buffer and are available for viewing with a different display filter or without any display filter.

You can define a display filter in either of two ways:

- From the Trace Display window, click View > Filter.

  The Display Filter dialog box is displayed. For details, see "Defining the Display Filter" on page 304.

- Double-click a packet in the Summary pane or double-click a selected protocol layer or field in the Decode or Hexadecimal pane.

  A filter is set based on what you selected. You can also modify the filter information as needed. For details, see "Point-and-Click Filtering" on page 305.

Defining the Display Filter

Capture packets using the capture filter of your choice. See "Defining a Capture Filter" on page 295 for details. To define a display filter:

1 Select a segment from ConsoleOne.

2 Click File > Actions > Packet Capture.

3 Click the View button in the Capture Status dialog box.

4 With the Trace Display window displayed and active, click View > Filter.

5 Select the nodes from the drop-down lists. You can select from IP, IPX or MAC address.

Alternatively, you can enter a node name or address in place of ANY in either or both of the drop-down list boxes.

6 Select the direction of the traffic flow from the arrow options available in the drop-down list.

7 To display all the packets of a specific protocol layer:

7a Double-click a protocol suite name from the list of protocols to display a list of all the protocols in the suite.

7b Scroll through the list to find the protocol you want.

7c Select the protocol.

8 To display all the packets that have the same contents in a specific field:

8a Enter the offset in hexadecimal bytes.

You can count the offset in the Hexadecimal pane when the packet is decoded, using the offset column for guidance. See "Viewing Packet Data in Hexadecimal Format" on page 301 for details.

8b Specify whether the offset is counted from the beginning of the packet or from the beginning of a protocol layer.

If you choose the protocol layer option, you must select a specific protocol in the Protocol box.

8c Enter the data that you want to include in the filter.

8d Specify the format in which you want the data to be displayed. Select from hexadecimal, ASCII, or EBCDIC format options.

You can also fill in the values using point-and-click filtering. See "Point-and-Click Filtering" on page 305.

9 Click OK.

The dialog box closes and ZfS begins to select the required packets from the capture buffer.

If you have a large capture buffer, ZfS displays the initial packets that pass the filter. ZfS continues to filter in the background while you examine these packets.

The Summary pane shows the list of filtered packets that met the criteria in the display filter. You can view and decode them as described earlier in this section.

Point-and-Click Filtering

You can define a display filter using the point-and-click method by double-clicking a field in the Trace Display window.

To define a display filter using the point-and-click method:

1 To display only packets in one conversation (for example, between a node and a server), double-click a packet in that conversation in the Summary pane.

The Display Filter dialog box displays the source and destination of the selected packet. You can also modify the addresses, if needed. For example, you can change the destination address to ANY, the broadcast address, or a specific node address.

or

To display all the packets containing a specific protocol layer, double-click the protocol line in the Decode pane.

The Display Filter dialog box displays the protocol you selected.

or

To display all packets with the same contents as a specific field, double-click the field in the Decode pane.

The Display Filter dialog box displays the field, data, and type of data for the selected field.

or

To display all packets with the same content as a specific offset, click the field in the Hexadecimal pane.

The Display Filter dialog box displays the offset and the type of data for the selected field.

2. Click OK.

   The dialog box closes and ZfS begins to select the packets from the capture buffer.

   The Summary pane displays the list of packets that met the display filter criteria.

Selecting and Decoding a Different Packet

To select a different packet for decoding:

1. Select View > Go To.

   You can also use the arrow keys on your keyboard to highlight a different packet.

2. Enter the packet number.

   If the packet number specified is more than the total number of captured packets, an error message displays. If a display filter is set and the specified packet number has not passed the filter, then a packet closest to the specified packet is displayed.

Packets are retrieved from the RMON agent as you select their headers in the Summary pane using the mouse or the arrow keys. Using the Go To dialog box avoids transferring unwanted packet data from the RMON agent. Similarly, scrolling the Summary pane with the scroll button retrieves only the packet header data when creating the decode summary, whereas using the arrow keys retrieves all packet data.

Highlighting Protocol Fields and Hexadecimal Bytes

ZfS provides a highlighting tool that helps you associate protocol fields and hexadecimal bytes. Highlighting can be a useful training tool for new network managers who want to learn about protocol decoding.

You can use this tool in the following ways:

- Highlight a protocol layer in the Decode pane.

  All bytes are highlighted in the selected protocol layer of the Hexadecimal pane.

- Click a field in any of the protocol layers in the Decode pane.

Associated bytes are highlighted in the Hexadecimal pane.

- Click hexadecimal bytes in the Hexadecimal pane.

  All hexadecimal and ASCII or EBCDIC bytes of this field in the Hexadecimal pane are highlighted, and the associated field is highlighted in the Decode pane.

- Click ASCII or EBCDIC text in the Hexadecimal pane.

  All hexadecimal and ASCII or EBCDIC bytes that belong to the field are highlighted in the Hexadecimal pane, and the associated field is highlighted in the Decode pane.

Saving Packet Files

You can save captured packets to a file and open the file later to analyze or print. When you save packets to a file, ZfS creates a binary file with the name you specify. You might want to save packets to a file in the following situations:

- To transfer the packets to another system or to send them for analysis.
- To apply a display filter to decoded captured packets so you can view only the packets that interest you. After you apply the display filter, you can save the filtered packets to a file.
- To compare packets saved from your buffer with other packets. You can either save the other packets, or view them from the capture buffer. You can view only one active capture buffer at a time. However, after you have saved packets to a file, you can open as many files as you want, and simultaneously view a capture buffer, if desired.

Packet files are compatible with the Traffic Analysis Agent for Windows NT/2000 and earlier versions of ManageWise®. Hence, packets captured and saved using Traffic Analysis Agent for Windows NT/2000 can be viewed using ZfS.

To save captured packets to a file while viewing the capture buffer:

1. Click File > Save As.

   The Save Filtered Packets or Save Unfiltered Packets dialog box is displayed, depending on whether you filtered your packets.

2. Enter the name in the File Name text box.

   The .TR1 file extension is appended automatically.

3. Click OK.

   IMPORTANT: Filter out the captured packets you want to save. (See "Filtering Packets for Display" on page 303.) When you save packets, you save only those that pass the display filter. If you did not filter the display, all packets are saved.

Opening Packet Files

To open a packet file:

1. From the main menu of ConsoleOne, click Tools > View Packet File.
2. Double-click the file you want to open.

Printing Packets

To print packets:

1. Open a Trace Display window, either by capturing packets or by opening a packet file.
2. Click File > Print.
3. Select the print options you want.

   You can select the destination, format, and the packets you want to print.

   - Choose whether to print to your default printer or to a file. If you choose a file, enter its name and specify whether the current packet data should overwrite the file or be appended to it.
   - Choose whether you want a summary of the packet information, only the hexadecimal information, a full decode, or a brief decode. These formats correspond to the three panes described in "Viewing Captured Packets" on page 300.
   - Choose whether to print all packets, a range of packets, or only the filtered packets.
4. Click OK.

Analyzing Traffic Generated by Protocols in Your Network

ZfS lets you determine the distribution of protocols in your network and provides statistical information of the protocols discovered by the RMON2 agent in the network, as well as transport and application layers. You can also add supported and custom protocols to your network. Supported protocols are those that the RMON2 agent is able to decode and count the number of packets transmitted in your network using the protocol. Custom protocols are not supported by the RMON2 agent but are used by nodes in your network.

The following sections explain how you can use ZfS to manage protocols in your network:

- "Displaying a List of Protocols Used in Your Network" on page 309
- "Determining the Distribution of Protocols in a Segment" on page 312

Displaying a List of Protocols Used in Your Network

You can use the Protocol Directory property page to view a hierarchical representation of supported and custom protocols used in the network, transport, and application layers in your network. By default, the page displays the Protocol Directory Tree that displays a collapsed list of protocols. The protocols used in the data link layer are displayed at the top level. You can expand each protocol to display the list of supported and custom protocols under the selected protocol.

You can also use the Protocol Directory property page to add or delete the protocols supported by the RMON2 agent. For details, see "Adding Supported Protocols to the Protocol Directory Tree" on page 310. The custom protocols that are used by the nodes in your network but are not supported by the RMON2 agent can also be added using the limited extensibility feature of RMON2. For details, see "Adding Custom Protocols to a Supported Protocol Tree" on page 311. For details about the limited extensibility feature, see RFC 2021 (http://www.isi.edu/in-notes/rfc2021.txt).

For a selected protocol, you can specify the RMON2 groups you want the RMON2 agent to support. This will let you obtain the RMON2 details of the groups that you specify the agent to support. While adding the protocol, you can enable the agent support for the Host group, Matrix group, and Address Map group. The Groups Supported box in the lower portion of the property page indicates whether the agent support for the Host and Matrix groups in the network layer and application layer, and support for the Address Map group are enabled, disabled, or not supported for the selected protocol. You can configure the values displayed in the Groups Supported box.

The Add and Remove buttons are enabled only when you select a protocol in the Protocol Directory tree.

IMPORTANT: The Traffic Analysis Agent for NetWare and Traffic Analysis Agent for Windows NT/2000 do not support enabling of the Address Map, Host, and Matrix groups for protocols in the Protocol Directory.

To open the Protocol Directory property page:

1. Click RMON2 under Service within a node from ConsoleOne.
2. Click File > Properties > the Protocol Directory tab.

Refer to the following sections:

- "Adding Supported Protocols to the Protocol Directory Tree" on page 310
- "Adding Custom Protocols to a Supported Protocol Tree" on page 311

Adding Supported Protocols to the Protocol Directory Tree

Supported protocols are those that the RMON2 agent is able to decode and count the number of packets transmitted in your network using the protocol.

Default values are provided for the parameters of protocols supported by the RMON2 agent. When you enter the name of a protocol, the default values are displayed if the protocol is supported.

To add a protocol to the Protocol Directory tree:

1. Open the Protocol Directory property page.
2. Select a protocol from the Protocol Directory tree.
3. Click Add.

   The following table describes the parameters for a selected protocol.

   IMPORTANT: The Protocol Name parameter cannot be configured. If you configure the port number or protocol code of a selected protocol, all child protocols of the selected protocol will be deleted.

Parameter	Description
Protocol Name	Displays the name of the protocol.
Protocol ID	Displays the identifier for the protocol. Displays the port number for an application layer protocol or the protocol code for protocols in other layers. The protocol identifier is always a decimal value.
Description	Displays a short description of the selected protocol.
Groups Supported	Displays whether the agent support of the Address Map group, Host group, or Matrix group is enabled for the selected protocol.

If the protocol name you enter or select from the Protocol Name list is supported by the RMON2 agent, the default parameters for the protocol are displayed in the appropriate fields of the Add Protocol dialog box. You cannot edit the parameters once you have added, if you do not want to use the default values.

4 Click OK.

The new protocol is added as a child protocol of the selected protocol. You cannot edit the parameters of the protocol you have added. You would need to delete the protocol and add the protocol again with different parameters.

Adding Custom Protocols to a Supported Protocol Tree

Custom protocols are those that are not supported by the RMON2 agent but are used by nodes in your network. If the RMON2 agent supports the limited extensibility feature of RMON2 for a selected protocol, you can add custom protocols under the selected protocol. See RFC 2021 (http://www.isi.edu/in-notes/rfc2021.txt) for more information. If the RMON2 agent does not support the limited extensibility feature for a protocol, you cannot add custom protocols under that protocol. A custom protocol cannot have child protocols.

Because default values are not provided for custom protocols, you must enter the appropriate values if you are adding a protocol that is not supported by the RMON2 agent.

To add a custom protocol to the Protocol Directory tree:

1 Select a supported protocol from the Protocol Directory tree.

2 Click Add.

3 In the Protocol Name field, enter the name of the protocol.

4 In the Protocol ID field, enter the port number for an application layer protocol or a protocol code for protocols in other layers.

IMPORTANT: The port number or protocol code should be a decimal value.

5 From the Groups Supported box, select the groups you want the RMON2 agent to support for the protocol.

The custom protocol is added as a child protocol of the supported protocol.

To remove a protocol from the Protocol Directory tree:

1 Select a protocol from the Protocol Directory tree.

2 Click Remove.

IMPORTANT: If you remove a protocol that has child protocols, all the child protocols are also removed from the Protocol Directory tree.

Determining the Distribution of Protocols in a Segment

ZfS lets you determine the distribution of protocols discovered by the RMON2 agent. You can use the information displayed in this view to analyze the traffic in your network and to troubleshoot network problems. Use the Protocol Directory property page to add, delete, or edit a protocol. See "Adding Supported Protocols to the Protocol Directory Tree" on page 310 and "Adding Custom Protocols to a Supported Protocol Tree" on page 311 for details.

The distribution of protocols discovered by the RMON2 agent is displayed in the Protocol Distribution view, based on the layer in which the protocols are discovered.

To view the distribution of protocols in the selected segment:

1. Select a segment from ConsoleOne.
2. Click View > Protocol Distribution.

The view displays the following three tables that list the protocols discovered in the network:

- Network layer table
- Transport layer table
- Application layer table

The protocols discovered by the RMON2 agent are placed in the appropriate table in the Protocol Distribution view depending on the layer in which they were discovered. Each table displays protocol statistics that are updated every 15 seconds.

The following table describes the protocol statistics displayed in the Protocol Distribution view.

Statistic	Description
Protocol Name	The name of the protocol

Statistic	Description
Packets/s	The average number of packets transmitted per second using the protocol discovered by the agent on the monitored segment
Bytes/s	The average number of bytes transmitted per second using the protocol discovered by the agent discovered on the monitored segment
Packet Rate %	The percentage of packets transmitted using the protocol; this is relative to the total percentage of packets transmitted using all protocols discovered by the agent
Byte Rate %	The percentage of bytes transmitted using the protocol; this is relative to the total percentage of bytes transmitted using all protocols discovered by the agent

IMPORTANT: Only one entry of each protocol is displayed in the Protocol Distribution view. Consolidated statistics are displayed for a supported protocol in more than one protocol suite.

Analyzing Traffic on Switches

ZfS provides statistical information about ports in a monitored switch and a list of nodes connected to each port in your switched network. This information is displayed in the Unified Port Traffic view. You can use the view to determine the load on the desktop and workgroup switches in your switched network. When only one node can be connected to each port in a switch, the switch is known as a desktop switch. When one port of a switch is connected to a connecting device to which more than one node is connected, the switch is called a Workgroup switch.

Ports and nodes connected to ports of a switch can be monitored using an embedded RMON agent or external RMON agent. An embedded RMON agent is installed on the port of a switch. An external RMON agent is installed on a node connected to a switch.

The following sections explain how you can obtain information about switch ports and nodes connected to ports in your switched network:

- "Viewing Statistics for Ports in a Switch" on page 314
- "Viewing the Summarized Switch Information" on page 314

Viewing Statistics for Ports in a Switch

You can use the Unified Port Traffic view to obtain statistical information about every switch port in your network. The view also displays a drop-down list of nodes connected to each port. The information displayed in this view is useful if you want to troubleshoot a port.

The Unified Port Traffic view displays a list of nodes connected to ports on the switch and statistics for each port. You can view Ethernet specific statistics for Ethernet ports on a switch. Statistics specific to FDDI and token ring ports are not displayed with this version of ZfS, although general port statistics are displayed for all ports on a switch regardless of the media type. You can choose to display all statistics or configure the Unified Port Traffic view to display selected statistics. For details, see "Choosing Statistics to Display in the Unified Port Traffic View" on page 324.

To display the statistics of ports in a switch:

1. Select Switch/Bridge under Services within a switch from ConsoleOne.
2. Click View > Port Traffic.

Viewing the Summarized Switch Information

The Switch Summary view provides brief information about a selected switch. You can view static information about a selected switch and information about alarms generated on the switch. You can also determine the packets and broadcasts received by the switch per second.

To view the summarized switch information:

1. Select Switch/Bridge under Services within a switch from ConsoleOne.
2. Click View > Switch Summary.

The Switch Summary view displays static information about a selected switch, as described in the following table.

Statistic	Explanation
Vendor	Name of the switch vendor
Switch Type	Type of switch: Transparent or Source Route
Number of Ports Active	Number of active ports on the switch

Statistic	Explanation
Forwarding Table Overflow Count	Number of times the forwarding table has exceeded its capacity
Up Time	Time since the switch was last rebooted
Number of Ports Present	Number of ports present on the selected switch
Number of MAC Addresses Learned	Number of MAC addresses dynamically discovered by the switch

The Switch Summary view displays information about alarms generated on a selected switch, as described in the following table.

Statistic	Explanation
Severity	Severity level attributed to the trap.
From	Network address of the device that sent the alarm to the alarm management system.
Owner	Segment or device affected by the alarm.
Summary	Summary of the event, often including the name or address of the object affected by the alarm.
Received Time	Date and time when the alarm management system received the alarm.
Type	Generic description of the alarm. For example, Volume out of disk space.
Category	Displays the category of the alarm based on the MIB that defines the trap-type objects. The category is directly related to the MIBs included in the management server MIB pool. For example, the category for NetWare servers is based on the NetWare Server Alarm MIB.

The Switch Summary view displays dynamic information about a selected switch, as described in the following table.

Statistics	Explanation
Switch Load (pkts/sec)	The load on the switch based on packets received by the switch per second
Frames Dropped/sec	The number of received packets discarded per minute
Broadcasts/sec	The number of broadcasts received by the switch from the nodes connected to ports of the switch

Optimizing Traffic Analysis

The tools provided by ZfS to analyze your network performance have default settings. You can change the default settings of various views to display only the information you require.

The following sections provide information about how you can configure the ZfS tools to suit your networking environment:

- "Choosing Options to Display Stations on a Segment" on page 316
- "Choosing Options to Display Trend Statistics" on page 318
- "Choosing Options to Display the Top Nodes Graph" on page 323
- "Choosing Statistics to Display in the Unified Port Traffic View" on page 324
- "Choosing Options to Display a Captured Packet" on page 325
- "Configuring Alarm Options from the Set Alarm Dialog Box" on page 326
- "Configuring the Monitor Nodes for Inactivity View" on page 330

Choosing Options to Display Stations on a Segment

You can configure the Stations view to display only the top 20 nodes or all nodes on the monitored segment. You can also choose the statistic based on which you want to display the top 20 nodes.

The following configuring options are available:

- "Displaying Statistics for All Nodes on a Segment" on page 317

- "Displaying Statistics for the Top 20 Nodes on a Segment" on page 317
- "Choosing a Statistic Based on Which Top 20 Nodes Are Displayed" on page 317

Displaying Statistics for All Nodes on a Segment

To display statistics for all nodes on a segment:

1. Select a segment from ConsoleOne.
2. Click View > Stations.

   To display all nodes on a segment, more time is required and more network traffic is generated.
3. From the Stations view, click View > Show All Stations.

Displaying Statistics for the Top 20 Nodes on a Segment

To display statistics for the top 20 nodes on a segment:

1. Select a segment from ConsoleOne.
2. Click View > Stations.
3. From the Stations view, click View > Show Top N Stations.

Choosing a Statistic Based on Which Top 20 Nodes Are Displayed

Packets out per second is the default statistic based on which top 20 nodes are displayed in the Stations view. To choose a different statistic based on which you want the top 20 nodes to be displayed, do either of the following:

- From the Stations view, click View > Show Top N Stations > choose a statistic from the list of statistics displayed.
- Click the Top Nodes Statistics drop-down box in the toolbar of the Stations view > choose a statistic from those displayed.

  The available statistics are described in the following table.

Statistic	Explanation
Packets/s In	Packets per second received by a node
Packets/s Out	Packets per second transmitted by a node
Bytes/s In	Bytes per second received by a node

Statistic	Explanation
Bytes/s Out	Bytes per second transmitted by a node
Errors/s	Errors per second transmitted by a node
Broadcasts/s	Broadcast packets per second transmitted by a node
Multicasts/s	Multicast packets per second transmitted by a node (packets transmitted to a specific group of nodes)

If you close the Stations view after changing the default settings, you will be prompted to save the changes made to the default settings. If you want the Stations view to be displayed based on the statistic you chose, you can save the setting. The next time you open ConsoleOne and launch the Stations view, you will be able to view the nodes on the monitored segment based on the statistic you specified.

Choosing Options to Display Trend Statistics

You can change the default settings based on which the segment performance trends are displayed in the Segment Trends view.

The following configuration options are available:

- "Choosing Statistics Based on Which Trend is Displayed" on page 318
- "Setting the Time-Scale Options" on page 322

Choosing Statistics Based on Which Trend is Displayed

To change the statistics based on which segment performance trend is displayed:

1. Click the Profile button in the Segment Trends view.
2. Select a profile from the Select Profile list.

   The default profile will display a trend with statistical information of total packets, good packets, and error packets on the monitored segment.

   If you choose not to use the profiles listed in the Select Profile list, you can select the required statistics from the Select Statistics list.

   The statistics list lets you examine the Ethernet, FDDI, and token ring statistics described in the following table.

Statistic	Media Support	Explanation
Abort Delimiter Errors/s	Token ring	Average number of abort delimiter errors observed per second. This error indicates that a node aborts a transmission.
AC Errors/s	Token ring	Average number of AC errors observed per second. This error is reported when an intended recipient of a packet fails to mark it as received or flags an error on it.
Beacons	FDDI and token ring	Average number of beacons per second observed in the sampling interval. A station transmits these packets when it detects a hard failure upstream.
Broadcast Packets/s	Ethernet, FDDI, token ring	Number of broadcast packets per second.
Burst Errors/s	Token ring	Average number of burst errors observed per second. This error indicates that a node detects the absence of transitions for the required time.
Claim Tokens/s	FDDI ring	Average number of times that the ring enters the claim token state from the normal ring state or ring purge state per second.
CRC/Alignment Errors/s	Ethernet and FDDI ring	Number of cyclic redundancy check (CRC)/alignment errors per second.
Echo Pkts/s	FDDI ring	Average number of echo frames received on the network per second.

Statistic	Media Support	Explanation
Elasticity Buffer Errors/s	FDDI ring	Average number of elasticity buffer overflow errors reported by this station per second. This is due to the difference in the clock frequency between the transmitting and receiving stations.
Error Packets/s	Ethernet	Number of error packets per second.
Fragments/s	Ethernet	Number of fragments per second.
Frame Copied Errors/s	FDDI ring	Average number of frame copied error frames reported per second by the station.
Frequency Errors/s	Token ring	Average number of frequency errors observed per second. This error indicates that a token ring clock on a node differs too much from the clock on the active monitor.
Good Packets/s	Ethernet	Number of good packets per second.
Internal Errors/s	Token ring	Average number of internal errors observed per second. These errors generally indicate a network board failure.
Jabbers/s	Ethernet	Number of jabbers per second.
Line Errors/s	Token ring	Average number of line errors observed per second. These packets are of valid size but have a faulty Frame Check Sequence (FCS) and do not end on an 8-bit boundary.
Lost Frames/s	FDDI and token ring	Average number of lost frame errors on the network observed per second.

Statistic	Media Support	Explanation
Monitor Contentions/s	Token ring	Average number of monitor contentions observed per second; these packets are transmitted by all active nodes when no active monitor is detected on the ring.
Multicast Packets/s	Ethernet, FDDI, and token ring	Number of multicast packets per second.
Oversize Packets/s	Ethernet	Number of oversize packets per second.
Packets	FDDI and token ring	Average number of packets observed per second in the sampling interval.
Receive Congestion Errors/s	Token ring	Average number of receive congestion errors observed per second. This error indicates that a node recognizes a frame addressed to its address, but has no available buffer space.
Ring Wraps/s	FDDI ring	Average number of times a wraparound condition has been detected at this interface per second. This entry does not indicate the number of times the ring has actually wrapped around. It only indicates the number of times the ring has wrapped around this physical path.
Token Errors/s	Token ring	Average number of token errors observed per second. This error indicates that a token is corrupted or the active monitor did not see a new frame in the required amount of time.
Total Bytes/s	Ethernet	Average number of total bytes per second.

Statistic	Media Support	Explanation
Total Packets/s	Ethernet	Average number of total packets per second.
Undersize Packets/s	Ethernet	Number of undersize packets per second.
Unicast Packets/s	Ethernet	Number of unicast packets per second.
Utilization%	Ethernet, FDDI, and token ring	Percentage of maximum network capacity used by all packets in the sampling interval.

If you close the Segment Trends view after changing the default statistics based on which trend is displayed, you will be prompted to save the changes made to the default settings. If you want the segment performance trend to be displayed based on the profile or statistics you chose, you can save the settings that you define. The next time you open ConsoleOne and launch the Segment Trends view, you will be able to view the trend based on the profile or statistics you defined.

Setting the Time-Scale Options

The segment performance trend is updated once every minute. You can set a different time scale based on which you want to update a graph. Select from the following time-scale options:

- Real Time
- One Hour
- One Day
- One Week
- One Month
- One Year

HINT: If you close the Segment Trends view after changing the default time-scale option based on which trend is displayed, you will be prompted to save the changes made to the default settings. If you do not want the trend to be updated in real time, you can save the time-scale setting you choose. The next time you open ConsoleOne and launch the Segment Trends view, the trend will be updated based on the time-scale option you selected.

Choosing Options to Display the Top Nodes Graph

You can configure the Segment Dashboard view to display or disable the top nodes graph. For details, see “Viewing the Graph of the Top Nodes on a Monitored Segment” on page 278. The top nodes graph is displayed in the lower portion of the Segment Dashboard view. Packets out per second is the default statistic based on which the graph is displayed. You can choose a different statistic based on which you want the graph to be displayed.

The following configuring options are available:

- “Displaying the Top Nodes Graph in the Segment Dashboard View” on page 323
- “Choosing the Statistic Based on Which Top Nodes Graph Is Displayed” on page 323
- “Disabling the Top Nodes Graph in the Segment Dashboard View” on page 324

Displaying the Top Nodes Graph in the Segment Dashboard View

To display the top nodes graph in the Segment Dashboard view:

1. From the Segment Dashboard view, click View > Show Top N Graph.

Choosing the Statistic Based on Which Top Nodes Graph Is Displayed

To display the top nodes graph based on a different statistic, do either of the following from the Segment Dashboard view:

- Click View > Show Top N Graph > choose a statistic.
- Click the Top Nodes Statistics drop-down box in the toolbar of the Segment Dashboard view > select a statistic.

  The statistics are described in the following table.

Statistic	Explanation
Broadcasts/min	Broadcast packets per minute transmitted by a node
Bytes/s in	Bytes per second received by a node
Bytes/s out	Bytes per second transmitted by a node
Errors/min	Errors per minute transmitted by a node

Statistic	Explanation
Packets/s in	Packets per second received by a node
Packets/s out	Packets per second transmitted by a node
Multicasts/min	Multicast packets per minute transmitted by a node

IMPORTANT: Errors per minute, broadcasts per minute, and multicasts per minute are updated every 60 seconds rather than every 5 seconds.

Disabling the Top Nodes Graph in the Segment Dashboard View

To disable the top nodes graph in the Segment Dashboard view:

1. From the Segment Dashboard view, click View > Disable Top N Graph.

Choosing Statistics to Display in the Unified Port Traffic View

ZfS provides statistics for each port on the switch. You can view port statistics and a list of nodes connected to each port using the Unified Port Traffic view. You can view Ethernet-specific statistics for Ethernet ports on a switch. Although statistics specific to FDDI and token ring ports will not be displayed with this version of ZfS, general port statistics are displayed for all ports on a switch regardless of the media type. For details, see "Viewing Statistics for Ports in a Switch" on page 314. You can choose to display only the selected statistics in the Unified Port Traffic view.

To select statistics to be displayed in the Unified Port Traffic view:

1. From the Unified Port Traffic view, click View > Settings.
2. Click the statistics from the Available Columns list > click Add.

The following table describes the general port statistics displayed for a port, regardless of the media type of the port.

Statistic	Explanation
Frames In/sec	Number of frames received by the port per second.
Frames Out/sec	Number of frames sent by port per second.
Port Link Status	Displays if the port is active or inactive. If the port is active, it can transmit and receive packets.

Statistic	Explanation
Speed	The speed at which packets are transmitted or received by the port.
Media Type	Media type of the selected port.
Local Traffic	Rate of traffic going towards nodes on the same port.

The following table describes the Ethernet-specific statistics displayed for an Ethernet port in addition to the general port statistics listed above.

Statistic	Explanation
Collisions/sec	Number of collisions per second
Utilization	Percentage of maximum network capacity currently consumed by packet traffic on the port
Broadcasts/sec	Number of broadcast packets per second currently received and sent by the port
Multicasts/sec	Multicast packets per second received and sent by the port
Packets/sec	Number of packets per second received and sent by the port
CRC Align Error	Total number of line errors reported by the port
Oversize Pkts	Number of oversize packets received and sent by the port

Choosing Options to Display a Captured Packet

ZfS provides default settings to display a captured packet in the Trace Display window.

To change the default settings and display the trace differently:

1. Open the Trace Display window.
2. From the Trace Display menu, click View > Options.
3. Select how you want to display the decoded packet.
    - Full Protocol Decode: Provides information about each field in each protocol layer in a selected packet. This is the default decoding.

- One Line Per Protocol Layer: Provides a line of information for each protocol layer of a selected packet.

4. Select the level at which you want to display the initial highlight position.

   - At Highest Protocol Layer: Places the initial highlighting at the highest protocol layer in a packet. This is the default.
   - At Packet Header: Places the initial highlighting at the packet header.

5. Select the format in which you want to display the decoded packet.

   - ASCII: Displays the hex data in ASCII format. This is the default.
   - EBCDIC: Displays the hex data in EBCDIC format.

Configuring Alarm Options from the Set Alarm Dialog Box

ZfS provides default alarm threshold values for a segment. You can set threshold values for various error conditions on Ethernet, FDDI, and token ring segments to eliminate the need to constantly monitor the segments.

When a segment alarm is enabled, the RMON agent monitors the segment based on the alarm threshold settings. If the configured threshold value is exceeded, the RMON agent sends a trap to the management server, which forwards it to ConsoleOne.

You should change the default values for alarm thresholds as appropriate for your organization. You can determine the appropriate value by observing average and peak traffic levels on your network using the Segment Trends view. For details, see "Analyzing Trend Data for a Segment" on page 279. You can do this as a part of creating a baseline of typical segment activity on your network.

To set an alarm threshold for a segment:

1. Select a segment from ConsoleOne.
2. Click File > Properties > the Segment Alarms tab.
3. Select a segment statistic > click Edit.
4. Click Enable to enable the alarms set for the monitored segment.

   When you click Enable, the text fields and the Default button will be enabled. However, if the default threshold values are not found, the Default button will not be enabled.

5. Enter the threshold value.

6 Specify the sampling time interval.

The RMON agent uses the sampling time interval to average the statistic to determine whether the alarm threshold was exceeded.

HINT: You can also use the Segment Dashboard view to define alarm threshold values for segment statistics. For details, see "Defining Alarm Thresholds for Statistics Displayed in the Segment Dashboard View" on page 278.

The following table describes the alarm statistics that ZfS tracks for Ethernet, FDDI, and token ring segments.

Statistic	Media Support	Explanation
Abort Errors	Token ring	Average number of abort errors observed per second in the sampling interval. These errors resemble line errors, but occur in the middle of a transmission.
AC Errors	Token ring	Average number of Address Recognition (and Frame Copied) errors observed per second in the sampling interval. This error is reported when an intended recipient of a packet fails to mark it as received or flags an error on it.
Beacons	FDDI and token ring	Average number of beacons per second observed in the sampling interval. A station transmits these packets when it detects a hard failure upstream.
Broadcasts	Ethernet, FDDI, and token ring	Average number of packets per second sent to the broadcast address FF-FF-FF-FF-FF-FF. Broadcast messages typically consist of general requests for information or transmission of status information to all stations.
Burst Errors	Token ring	Average number of burst errors observed per second in the sampling interval. A burst error is caused by a lack of signal transitions between stations for a short period of time.
Claim Tokens	FDDI ring	Average number of times that the ring enters the claim token state from the normal ring state or ring purge state per second.

Statistic	Media Support	Explanation
Congestion Errors	Token ring	Average number of congestion errors observed per second in the sampling interval. The receiving station runs out of buffer space to store the packet.
CRC Errors	Ethernet and FDDI ring	Average number of CRC errors observed per second in the sampling interval. These packets are of valid size but have a faulty FCS.
Echo Pkts	FDDI ring	Average number of echo frames received on the network per second.
Elasticity Buffer Errors/s	FDDI ring	Average number of elasticity buffer overflow errors reported per second by this station. This is due to the difference in the clock frequency of the transmitting and receiving stations.
Fragments	Ethernet	Average number of fragments observed per second in the sampling interval. Fragments are packets that contain fewer than 64 bytes and have a faulty FCS. They are typically a result of collisions.
Frame Copied Errors	FDDI and Token ring	Average number of frame copied errors observed per second in the sampling interval. This error indicates that a station has detected that another station accepted a packet addressed to the first station.
Frequency Errors	Token ring	Average number of frequency errors observed per second in the sampling interval. This error indicates that a token ring clock on a station differs from the clock on the active monitor.
Internal Errors	Token ring	Average number of internal errors observed per second in the sampling interval. These errors generally indicate a network adapter board failure.

Statistic	Media Support	Explanation
Jabbers	Ethernet	Average number of jabber packets observed per second in the sampling interval. A jabber consists of packets that contain more than 1518 bytes and have a faulty FCS.
Line Errors	Token ring	Average number of line errors observed per second in the sampling interval. These packets are of legal size but have a faulty FCS and do not end on an 8-bit boundary.
Lost Frames	FDDI and token ring	Total number of lost frame errors received on the network. A lost frame error indicates that the end delimiter of a frame is lost in the network.
Monitor Contentions	Token ring	Average number of monitor contentions observed per second in the sampling interval. These packets are transmitted when no active monitor is detected on the ring.
Multicasts	Ethernet, FDDI, and token ring	Average number of packets per second sent to multicast addresses.
Oversize	Ethernet	Average number of oversized packets observed per second in the sampling interval. Oversized packets contain more than 1518 bytes, including the FCS.
Packets	Ethernet, FDDI, and token ring	Total number of packets observed per second in the sampling interval.
Ring Wraps/s	FDDI ring	Average number of times a wraparound condition has been detected at this interface per second. This entry does not indicate the number of times that the ring has actually wrapped around. It only indicates the number of times the ring has wrapped around this physical path.

Statistic	Media Support	Explanation
Token Errors	Token ring	Average number of token errors observed per second in the sampling interval. This error indicates that a token is corrupted or the active monitor did not detect a new frame transmitted during the current sampling interval.
Undersize	Ethernet	Average number of undersized packets observed per second in the sampling interval. Undersized errors are shorter than 64 bytes.
Utilization(%)	Ethernet, FDDI, and token ring	Percentage of maximum network capacity used by all packets in the sampling interval.

When you have set the appropriate threshold values for the segments in your network, you can use the Save As Default button on the Segment Alarms property page to save the values you defined as the default values. However, the default threshold values provided by ZfS will not be available once you apply the new values.

Configuring the Monitor Nodes for Inactivity View

By default, the poll interval for refreshing the Monitor Nodes for Inactivity view is zero seconds. You can configure the poll interval based on which you want the view to be refreshed. The agent monitoring nodes on a monitored segment declares a node as inactive after verifying it for a specified period of time. You can change the time duration for the agent to verify the node before declaring it inactive.

The following configuring options are available:

- "Specifying the Poll Interval for Refreshing the Monitor Nodes for Inactivity View" on page 331
- "Specifying the Duration for the Agent to Determine if a Node Is Inactive" on page 331

Specifying the Poll Interval for Refreshing the Monitor Nodes for Inactivity View

You can modify the PollInterval parameter in the LSMPARAMETERS.PROPERTIES file to specify the poll interval for refreshing the Monitor Nodes for Inactivity view.

To specify a poll interval for refreshing the Monitor Nodes for Inactivity view:

1. Open the LSMPARAMETERS.PROPERTIES file located in the *operating_system_drive*\INSTALL\CONSOLEONE\BIN directory.
2. Specify a value for the PollInterval parameter.

   The PollInterval value should be a positive value, in seconds. The default value is zero (0) seconds.

Specifying the Duration for the Agent to Determine if a Node Is Inactive

When a selected node becomes inactive, the agent monitoring the node verifies the state of the node for one minute before declaring it inactive. You can modify the HostTimeOut parameter in the LSMPARAMETERS.PROPERTIES file to change the duration for the agent to verify the selected node before declaring it inactive. The agent verifies the inactive node for the specified period of time before declaring it inactive.

To change the duration for the agent to verify a node before declaring it inactive:

1. Open the LSMPARAMETERS.PROPERTIES file located in the *operating_system_drive*\INSTALL\CONSOLEONE\BIN directory.
2. Specify a value for the HostTimeOut parameter.

   The HostTimeOut value should be a positive value, in minutes. The default value is one (1) minute.

Understanding the Traffic Analysis Agents

Traffic Analysis agents enable you to monitor a heterogeneous LAN environment comprised of Ethernet, FDDI, and token ring segments from the easy-to-use ZfS interface.

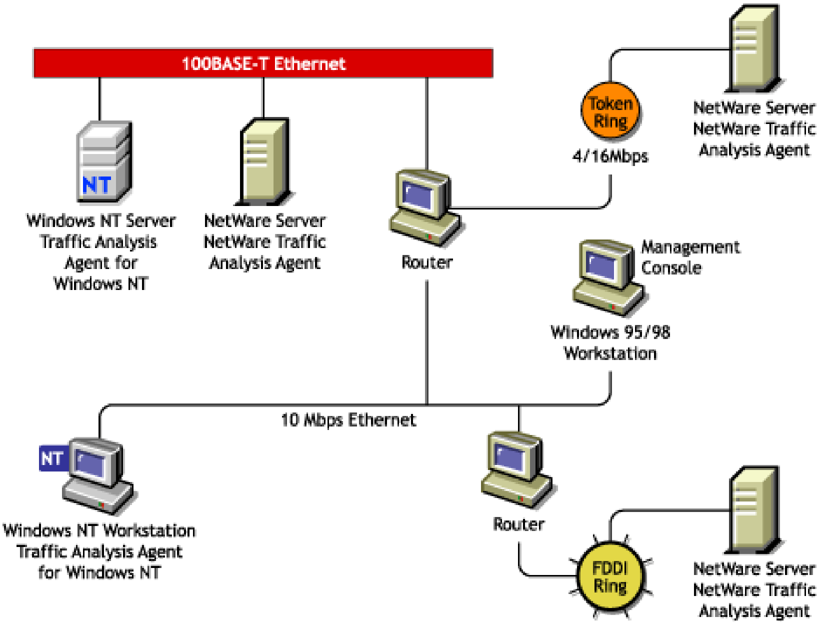
Traffic Analysis agents are RMON agents that can run on a NetWare server, Windows NT/2000 server, or a Windows NT workstation. They implement a set of functionality defined by the RMON MIB (RFC 1757 (http://

www.isi.edu/in-notes/rfc1757.txt)). These agents collect information about activity on your network and make it available to ConsoleOne via SNMP.

The following functionality is provided by the Traffic Analysis Agents:

- Monitor the performance of segments and provide vital network statistical information to ConsoleOne
- Make it easy to set alarm thresholds for proactive network management
- Capture all packets or selected packets to help you diagnose and resolve problems on the monitored networks
- Monitor multiple network segments including the Symmetric Multi-Processing (SMP) architecture
- Monitor network segments for problems, such as high network utilization and communication errors
- Track dynamic IP address assignments from the DHCP server to the nodes on the network
- Store data to display real-time trends (hourly) and historical trends (daily, weekly, monthly, and yearly) for statistics such as Total Bytes, Total Packets, Good Packets, Error Packets, and so forth
- Monitor nodes for inactivity, so that you are alerted if the monitored nodes becomes inactive

The following figure illustrates the functionality of traffic analysis agents.


100BASE-T Ethernet
NT
Windows NT Server Traffic Analysis Agent for Windows NT
NetWare Server NetWare Traffic Analysis Agent
Router
Token Ring
4/16Mbps
NetWare Server NetWare Traffic Analysis Agent
Management Console
Windows 95/98 Workstation
10 Mbps Ethernet
NT
Windows NT Workstation Traffic Analysis Agent for Windows NT
Router
FDDI Ring
NetWare Server NetWare Traffic Analysis Agent

ZfS includes the following traffic analysis agents:

- Traffic Analysis Agent for NetWare.

  For details, see "Using the Traffic Analysis Agent for NetWare" on page 334.

- Traffic Analysis Agent for Windows NT/2000.

  For details, see "Using the Traffic Analysis Agent for Windows NT/ 2000" on page 353.

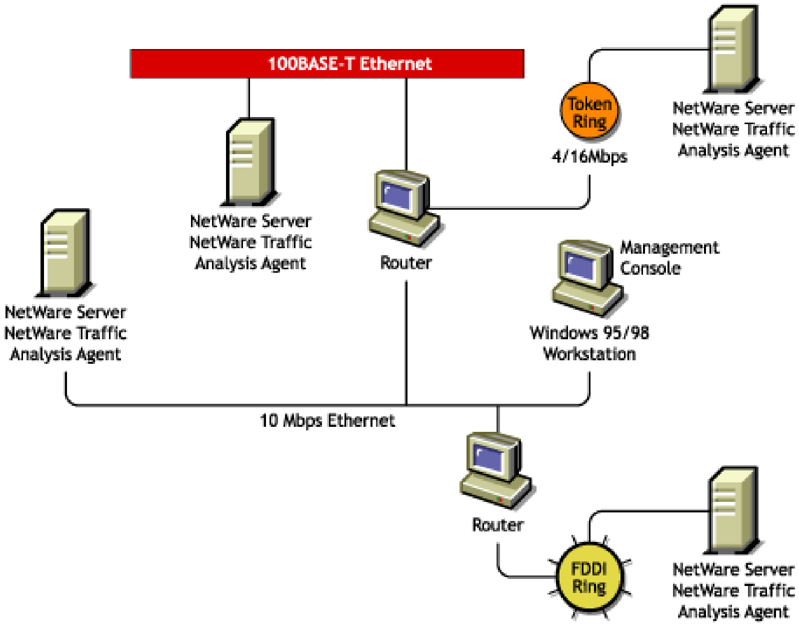
The ZfS traffic analysis agents are RMON Plus agents. For details, see "Functionality of RMON Plus Agents" on page 259. These agents also implement the first two RMON2 groups. The first RMON2 group is the Protocol Directory group, which provides a table of protocols for which the agent will monitor and maintain statistics. The second RMON2 group is the Protocol Distribution group, which provides a table of statistics for each protocol in the directory. For details, see "Functionality of RMON2 Agents" on page 261.

Using the Traffic Analysis Agent for NetWare

The Traffic Analysis Agent for NetWare (NLA 1.30) runs on a NetWare server. It is a set of NLM programs that enable NetWare 4.*x* and 5.*x* to monitor traffic on Ethernet, FDDI, or token ring segments.

The Traffic Analysis Agent for NetWare implements token ring extensions for the RMON MIB (RFC 1513 (http://www.isi.edu/in-notes/rfc1513.txt)) for token ring media, and a Novell proprietary MIB for FDDI media, in addition to implementing an RMON (RFC 1757 (http://www.isi.edu/in-notes/rfc1757.txt)) for Ethernet media. The Traffic Analysis Agent for NetWare also implements the first two groups for RMON2 (RFC 2021 (http://www.isi.edu/in-notes/rfc2021.txt)).

The following figure illustrates a functional view of the Traffic Analysis Agent for NetWare:


100BASE-T Ethernet
Token Ring
4/16Mbps
NetWare Server NetWare Traffic Analysis Agent
NetWare Server NetWare Traffic Analysis Agent
Router
Management Console
NetWare Server NetWare Traffic Analysis Agent
Windows 95/98 Workstation
10 Mbps Ethernet
Router
FDDI Ring
NetWare Server NetWare Traffic Analysis Agent

The following sections provide information about optimizing and using the Traffic Analysis Agent for NetWare:

- "Planning to Install the Traffic Analysis Agent for NetWare" on page 335

- “Optimizing the Traffic Analysis Agent for NetWare Performance” on page 335
- “Using the Console Utility of the Traffic Analysis Agent for NetWare” on page 345

Planning to Install the Traffic Analysis Agent for NetWare

To successfully install the Traffic Analysis Agent for NetWare on a NetWare server, the server must meet the system requirements specified in Installing and Setting Up Management and Monitoring Services in the *Installation* guide.

You should configure NetWare SNMP parameters as explained in Chapter 13, “Using SNMP Community Strings,” on page 411. This will ensure a smooth installation of the Traffic Analysis Agent for NetWare on the server.

NOTE: Although it is not required, it is recommended that you uninstall previous versions of the LANalyzer Agent (referred to as the Traffic Analysis Agent in ZfS). If you do not uninstall the previous version of the agent, you must verify that the upgraded NetWare servers run the new Traffic Analysis Agent.

Optimizing the Traffic Analysis Agent for NetWare Performance

The measures described in the following sections can improve the performance of your Traffic Analysis Agent for NetWare servers.

You can configure the Traffic Analysis Agent for NetWare functions described in the following sections by setting the parameters in the LANZ.NCF file.

- “Contents of the LANZ.NCF File” on page 335
- “Modifying the LANZ.NCF File” on page 340

Contents of the LANZ.NCF File

The LANZ.NCF file loads all the NLM software required for the Traffic Analysis Agent for NetWare operation. The LANZ.NCF file resides in the SYS:\Zfs_agnt\lanz directory.

The following example displays the complete text of the default LANZ.NCF file.

```
#

# NetWare LANalyzer Agent
# Version 1.3

#

# - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

# LANZ.NCF: NetWare LANalyzer Agent Load File

#

# This NCF file is created by the NetWare LANalyzer Agent
install program.

# It is used to load the NetWare Loadable Module files that
make up NetWare

# LANalyzer Agent.

# WARNING:   You should not modify this file unless you need
to change one of

# the configuration parameters documented below. Other
changes to this

# file are not recommended. Should you damage this file, you
must reinstall

# NetWare LANalyzer Agent.

#

# NOTE:      To enable or disable the monitoring of network
adapters by

# NetWare LANalyzer Agent, use the LANZCON utility as
described in the

# NetWare LANalyzer Agent Installation and Administration
guide.

#

# - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

# Load Parameter Descriptions

#

# load LANZSU debug=1

#

# debug=1    Turns on the LANZ Control screen to see the
transactional
```

```
# messages from the NetWare LANalyzer Agent.

#

# load LANZMEM bound=KB age=HHH

#

# bound=KB   This is the upper limit on memory that can be
allocated

# dynamically by the NetWare LANalyzer Agent.

#

# Increasing this number allows you to create larger packet

# capture buffers and maintain data for inactive stations

# for a longer period of time.

#

# Decreasing this value reduces the amount of memory that

# can be used by NetWare LANalyzer Agent. This leaves more

# memory for the other server tasks.

#

# NetWare LANalyzer Agent automatically purges data for

# inactive stations as the memory boundary is approached.

# This allows NetWare LANalyzer Agent to adjust to

#

# the memory that is available to it dynamically.

#

# If the boundary is low, purging occurs frequently, saving

# only data for stations that have been recently active on

# the network. If this happens, a message appears on the

# system console indicating that not enough memory has been

# allocated to NetWare LANalyzer Agent.

#
```

```
# KB is the memory boundary in kilobytes.
#
# Initial value: Set by the installation program
# based on memory usage
#
# Minimum recommended value:      512
#
# Maximum recommended value:      75% of free server memory
# when NLM files are loaded
#
# Default value:                If bound=KB is not specified,
# it defaults to 3072.
#
# age=HHH   NetWare LANalyzer Agent purges data for stations
that have
# not been active on the network recently. This parameter
# controls how long data for inactive stations is maintained.
#
# Memory that is used by the station table is not available
# for other uses, such as capturing packets. Reducing the
# AGE value tends to increase the amount of memory
# available for capturing packets.
#
# If you cannot allocate capture buffers that are large,
# you may need to reduce the AGE value.
#
# HHH is the inactivity period, in hours, before station data
# is purged.
```

```
#
# Minimum recommended value:      1
#
# Default value:                 If age=HHH is not specified,
# it defaults to 168 (1 week)
#
# load LANZDI level=1
#
# level=1   It indicates that the LANZDI will stop receiving
packets
# when CPU utilization gets high.
#
# Default is OFF. LANZDI will continue to receive packets even
# when CPU utilization gets high.
#
# load LANZSM topn=N
#
# topn=N    The number of concurrent sorts of top N nodes that
#
# NetWare LANalyzer Agent supports for each network adapter.
#
# Recommended value: 4
# Minimum value:     2
# Maximum value:     10
#
# load LANZTR poll = 1
#
# poll=1     Polls token ring source-routed bridges.
```

```
#

# load LANZCTL trapreg=1

#

# trapreg=1 Causes SNMP traps to be sent to management
consoles

# advertising themselves on the network, as well as stations

# listed in SYS:\ETC\TRAPTARG.CFG. Omitting this parameter

# or setting it to 0 causes traps to be sent only to those

# stations listed in the SYS:\ETC\TRAPTARG.CFG file.

#

# - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

load gtrend.nlm

load lanzsu.nlm

load lanzmem.nlm bound = 3072 AGE = 168

load lanzlib.nlm

load lanzdi.nlm

load lanzael.nlm

load lanzhis.nlm

load lanzfcb.nlm

load lanzsm.nlm topn = 4

load lanztr.nlm

load lanzfddi.nlm

load lanzctl.nlm trapreg = 1
```

Modifying the LANZ.NCF File

The following sections describe how to modify the parameters of the commands in the LANZ.NCF file to configure the Traffic Analysis Agent for NetWare functions:

- "Turning On the LANZ Control Screen" on page 341
- "Disabling Packet Capture" on page 341

- “Disabling Generation of Duplicate IP Address Alarms” on page 342
- “Setting Packet Flow Control” on page 342
- “Setting the Upper Limit of Available Memory” on page 342
- “Purging Data from Server Memory” on page 343
- “Sorting Concurrent Top Stations” on page 343
- “Automatically Sending Alarms to the ZfS Site Server” on page 344
- “Polling Source Route Bridges” on page 344
- “Activating Changes in the LANZ.NCF File” on page 345

To make changes in the LANZ.NCF file and modify the configuration of the Traffic Analysis Agent for NetWare:

1. Open the LANZ.NCF file with a text editor.
2. Insert or modify the appropriate parameter as shown and save the file.
3. Unload and reload the Traffic Analysis Agent for NetWare, as described in “Activating Changes in the LANZ.NCF File” on page 345.

Turning On the LANZ Control Screen

The LANZ control screen reports significant events for the Traffic Analysis Agent for NetWare.

To turn on the LANZ control screen, insert the DEBUG parameter in the LOAD LANZSU.NLM statement, as shown below:

```
LOAD LANZSU.NLM DEBUG=1
```

The default is Off.

Disabling Packet Capture

You might want to disable packet capture to prevent others from observing sensitive data captured in the packets sent on the network segment.

To disable the packet capture, insert a comment mark (#) in the LOAD LANZFCB statement, as shown below:

```
LOAD LANZFCB.NLM
```

You can also control packet capture during high levels of traffic instead of disabling packet capture entirely. For details, see “Setting Packet Flow Control” on page 342.

Disabling Generation of Duplicate IP Address Alarms

In the DHCP environment, the IP address is released to the DHCP server when a DHCP client is shut down. During the process of releasing the IP address to the DHCP server, the client sends a DHCPRELEASE packet. If this packet does not reach the agent, false duplicate IP address alarms will be generated.

To disable the generation of duplicate IP address alarms, specify zero (0) as the value for the DUPIP parameter, as shown below:

```
LOAD LANZSM DUPIP=0
```

If the DUPIP parameter contains a non-zero value or if the parameter is not specified, duplicate IP address alarms are generated.

Setting Packet Flow Control

The Traffic Analysis Agent for NetWare typically operates in promiscuous mode, receiving all packets on the network. However, if server utilization is high and performance becomes degraded, you can set the LEVEL parameter to 1, which configures the agent to pause when server traffic is high, and then automatically resume operation in promiscuous mode when the traffic level returns to normal.

The default is not to specify the LEVEL parameter at all, which allows continuous operation in promiscuous mode.

To set packet flow control, use the LEVEL parameter setting, as shown below:

```
LOAD LANZDI LEVEL=1
```

Setting the Upper Limit of Available Memory

The BOUND parameter sets the upper limit of available memory that can be allocated dynamically to the Traffic Analysis Agent for NetWare.

The value of the BOUND parameter is measured in kilobytes (KB). The default value is 3072 KB. The minimum recommended value is 512 KB. The maximum recommended value is 75% of the memory that is available after all NLM files are loaded.

You might receive the message "Insufficient memory available for the Traffic Analysis Agent for NetWare" in the following situations:

- The server has too little memory

- The server has sufficient memory, but the memory is not available to the Traffic Analysis Agent for NetWare
- You requested a packet capture buffer that is too large, and the agent granted you less memory than requested

In each case, you should increase the value of the BOUND parameter and add more RAM to your NetWare server.

To change the upper limit of available memory, edit the BOUND parameter, with the appropriate value, as shown below:

```
LOAD LANZMEM BOUND=3072 AGE=168
```

Purging Data from Server Memory

The Traffic Analysis Agent for NetWare holds its data in server memory. You can control the amount of data held in memory by setting the value of the AGE parameter. When data reaches the age specified in the parameter, the data is purged from memory. The AGE parameter is particularly useful on large, bridged networks.

The value of the AGE parameter is measured in hours. The default value is 168, or one week. The minimum recommended value is one hour.

You should lower the AGE parameter if you receive the message "Insufficient memory available for the Traffic Analysis Agent for NetWare" and you have allocated sufficient memory for the agent.

Having insufficient memory is not harmful to the agent or the server. The Traffic Analysis Agent for NetWare can run indefinitely, even when the memory allocated to it is not sufficient.

To modify the amount of data held in server memory, change the value of the AGE parameter, as shown below:

```
LOAD LANZMEM BOUND=3072 AGE=168
```

Sorting Concurrent Top Stations

The Traffic Analysis Agent for NetWare sorts stations whenever the top eight graphs on the Segment Dashboard view, the Stations view, or both are displayed by ConsoleOne. The sorts are independent of each other and can be computed on the basis of different statistics.

Because each of the sort computations uses server CPU cycles, you should limit the number of concurrent computations.

To set the number of concurrent sort computations per network adapter, set the TOPN parameter, as shown below:

```
LOAD LANZSM TOPN=n
```

The default value is 4. The minimum value is 2. The maximum value is 10.

Automatically Sending Alarms to the ZfS Site Server

The Traffic Analysis Agent for NetWare can automatically send SNMP alarms (sometimes referred to as SNMP traps) to the ZfS site server or other nodes on the network in the following configurations:

- The Traffic Analysis Agent for NetWare receives the SAP packets sent by the ZfS site server
- The ZfS site server or other node is listed in the server's TRAPTARG.CFG file. This file can be edited to add other trap targets.

The TRAPTARG.CFG file is stored in the SYS:\ETC directory. The file provides instructions for its use. You can edit the file with any ASCII text editor.

To enable alarms to be sent automatically, add the TRAPREG parameter setting, as shown below:

```
LOAD LANZCTL TRAPREG=1
```

The default is 1. If you omit the TRAPREG parameter or set its value to zero (0), the agent sends alarms only to management consoles listed in the TRAPTARG.CFG file.

Polling Source Route Bridges

To control source route bridge polling on token ring networks, use the POLL parameter, as shown below:

```
LOAD LANZTR POLL=1
```

1 = On and 0 = Off.

Setting the POLL parameter to 1 polls source routed bridges once every second. You cannot change the polling rate. The default is On.

To turn off this function, set the POLL parameter to zero (0), as shown below:

```
LOAD LANZTR POLL=0
```

The default is to omit the POLL parameter. Also, the LOAD LANZTR statement is commented out on systems that do not have a token ring adapter installed.

Activating Changes in the LANZ.NCF File

To activate the changes you make in the LANZ.NCF file:

1. Save the LANZNCF file.
2. Enter **ULANZ** at the server prompt to unload the agent.
3. Enter **LANZ** to reload the agent.

Using the Console Utility of the Traffic Analysis Agent for NetWare

The Traffic Analysis Agent for NetWare 1.3 provides a console utility (LANZCON.NLM) that performs the following three tasks:

- Enables or disables network monitoring by the selected network adapters
- Provides a source of detailed troubleshooting information
- Resolves a residual entry (for example, a Host TopN entry created by a management console that terminated unexpectedly)

When you install the Traffic Analysis Agent for NetWare, LANZCON.NLM is installed automatically in the SYS:\ZFS_AGNT\LANZ directory.

The following topics are discussed in greater detail in this section:

- "Loading the Console Utility of the Traffic Analysis Agent for NetWare" on page 345
- "Enabling or Disabling Network Adapter Monitoring" on page 346
- "Viewing Network Adapter Information" on page 347
- "Viewing the Agent Item Status" on page 348
- "Accessing Detailed Information About Each Item" on page 349
- "Migrating Trend Files" on page 352

Loading the Console Utility of the Traffic Analysis Agent for NetWare

To use LANZCON.NLM, enter the following command at the NetWare console prompt:

```
LOAD LANZCON CONTROLCOMMUNITY = <control community string>
```

IMPORTANT: If LANZCON is launched without any command line argument, then the default control community string is PUBLIC.

LANZCON.NLM is loaded and displays a list of network adapters, along with summary information about the network adapters currently installed on the server.

The following information is displayed for each network adapter:

- **Number (#):** The network adapter entry number in the network interface table.
- **Description:** A brief description of the network adapter.
- **Media Type:** The type of network connected to the network adapter: Ethernet, FDDI, or token ring.
- **Adapter Address:** The physical address of the network adapter.

Enabling or Disabling Network Adapter Monitoring

To enable or disable monitoring of a selected network adapter:

1. From the Network Adapters screen, select the appropriate adapter > press F3.
   - If the selected adapter is currently monitoring an Ethernet or token ring network, the console displays the Adapter Is Monitoring screen.
   - If the selected adapter is not monitoring an Ethernet or token ring network, the console displays the Adapter Is Not Monitoring screen.
2. Select Yes or No to enable or disable monitoring.

   If you disable monitoring, all LAN analysis data for the selected adapter is deleted.

Using LANZCON, an FDDI adapter cannot be disabled. To disable an FDDI adapter:

1. Unload LANZCON, if loaded.
2. Unload LANZ, if loaded.
3. Open LANZ.NCF from SYS:\ZFS_AGNT\LANZ directory for editing.
4. Comment the statement LOAD LANZFDDI.NLM by entering the # symbol at the beginning of this statement.
5. Save LANZ.NCF and exit.

6. Reload LANZ.

Viewing Network Adapter Information

To bring up detailed information for network adapter items:

1. From the Network Adapters screen, select an adapter > press Enter.
2. From the Select Information to View screen, select Show Adapter Items.

   The LANZCON utility displays the Network Adapter Items screen that lists all the items related to the selected network adapter.

The screen for a token ring adapter includes the information from the Novell Token Ring RMON MIB. For details, see "Viewing the Agent Item Status" on page 348.

To return to the Select Information to View menu, press Esc.

The following information is provided for the selected adapter:

- **Item:** The types of items that are currently being monitored by the selected adapter. The Network Adapter Items screen shows a set of typical items consisting of token ring, Statistics, History, Host, Matrix, and Host TopN. The Traffic Analysis Agent for NetWare monitors these items by default. In the Network Adapter Items screen, the Host TopN item, indicating the list of the busiest nodes, has been added by a user. You can add other items to this display from ConsoleOne, depending on your configuration.

  You can select any item to view more information about each topic. To view the values for the selected item, select the desired item > press Enter. Refer to the following sections for more examples of the screens.

- **Index:** The entry number of the displayed item in the list of all the items of the same type. The related tables are identified by this index.

- **Description:** A textual description of the entry. This column indicates the software entity or user that created the item. The items automatically monitored by the Traffic Analysis Agent for NetWare are indicated by the monitor.

  For a token ring network entry, this column shows the media speed and the local ring number.

Viewing the Agent Item Status

When you click the Select Information to View menu > Show Agent Items, LANZCON displays all the items for each network adapter being monitored by the Traffic Analysis Agent for NetWare.

To view the agent item status for the selected agent:

1. From the Network Adapters screen, select an adapter > press Enter.
2. From the Select Information to View screen, select Show Agent Items.

The All NetWare LANalyzer Agent Items screen shows all the items related to the agent monitoring the segment. For example, if you are using multiple adapters to monitor multiple network segments, the screen lists all the items being monitored by the agent.

To delete any entry (except the token ring network entry), select the entry > click Delete > click Yes.

To return to the Network Adapter Items screen, press Esc.

The following information is provided for the agent:

- **Item:** The types of items available. The All NetWare LANalyzer Agent Items screen shows a set of typical items consisting of Statistics, History, Host, Matrix, and Host TopN. Additional items can be displayed, depending on your configuration.

  You can select any item for more information about each topic. To view the values for an item, select the desired item > press Enter. See the following sections for more examples of the screens.
- **Index:** The entry number of the displayed item in the list of all items of the same type. The related tables are identified by this index.
- **Description:** A textual description of the entry. This column indicates the software entity or user that created the item table. The items automatically monitored by the Traffic Analysis Agent for NetWare are indicated by the monitor.

  For a token ring network entry, this column shows the media speed and the local ring number.

Accessing Detailed Information About Each Item

This section describes the major categories of information available for both the selected network adapter and the Traffic Analysis Agent for NetWare. The following topics are covered:

- "Viewing the Token Ring RMON MIB Information" on page 349
- "Viewing the FDDI Ring RMON MIB Information" on page 349
- "Viewing Statistics Information" on page 349
- "Viewing History Information" on page 350
- "Viewing Host Information" on page 351
- "Viewing Matrix Information" on page 351

Viewing the Token Ring RMON MIB Information

To view the Token Ring RMON MIB information:

1. From the Network Adapter Items screen, select the token ring item > press Enter.
2. From the Select Information to View screen, select Show Adapter Items > press Enter.
3. Press Esc to exit this screen.

Viewing the FDDI Ring RMON MIB Information

To view the FDDI ring RMON MIB information:

1. From the Network Adapter Items screen, select the FDDI Ring item > press Enter.
2. From the Select Information to View screen, select Show Adapter Items > press Enter.

Viewing Statistics Information

The statistics information presents the basic statistics for each monitored adapter per segment.

To view the statistics information:

1. From the Network Adapter Items screen, select Statistics.
2. Press Enter.

For an Ethernet network entry, the LANZCON utility displays the Statistics Information screen.

This screen displays the statistical values of the selected network adapter. The display is updated periodically with the latest values for each field.

3 To exit this screen, press Esc.

Viewing History Information

The history information defines sampling functions for the networks that are being monitored. The History Control table defines a set of samples at a particular sampling interval for a particular network adapter.

To view the history information:

1 From the Network Adapter Items screen, select History.

2 Press Enter.

3 To exit this screen, press Esc.

The field descriptions are as follows:

- **Index:** An integer that uniquely identifies a row in the History Control table.
- **Data Source:** Identifies the network adapter and the Ethernet, FDDI, or token ring segment that is the source of the data for entries defined by this object.
- **Buckets Requested:** The requested number of discrete sampling intervals over which data will be saved in the portion of the media-specific table associated with this entry.
- **Buckets Granted:** The actual number of discrete sampling intervals over which data will be saved.
- **Interval:** The interval, in seconds, over which data is sampled for each bucket. The interval can be set to any number between 1 and 3,600 (one hour). The default interval for past hour is 30 seconds per sample, and the default interval for past day is 30 minutes (or 1,800 seconds) per sample.

  The sampling scheme is determined by the buckets granted and the control interval.
- **Owner:** The entity that created the item. "Monitor" indicates that the item was created by the Traffic Analysis Agent for NetWare.

- **Status:** A status of Valid indicates that the agent is operating normally under the instructions given by the table.

Viewing Host Information

The host group gathers statistics about specific hosts or nodes on the LAN. The Traffic Analysis Agent for NetWare learns of new nodes on the LAN by observing the source and destination MAC addresses in good packets. For each node known to the agent, a set of statistics is maintained.

To view the host (node) information:

1. From the Network Adapter Items screen, select Host.
2. Press Enter.

The host group consists of three tables: two data tables and one control table. The two data tables are hostTable and hostTimeTable. The control table, hostControlTable, includes the following objects, which correspond to the fields displayed in the Host Information screen:

- **Index:** An integer that uniquely identifies a row in the hostControlTable. Each row in the control table refers to a unique network adapter, and thus, a unique segment.
- **Data Source:** Identifies the network adapter and the Ethernet, FDDI, or token ring segment that is the source of the data for the entries defined by this object.
- **Table Size:** The number of rows in the hostTable associated with this row.
- **Last Delete Time:** The value of the sysUpTime MIB object that corresponds to the last time an entry was deleted from the portion of the hostTable associated with this row. The value is zero (0) if no deletions occurred.
- **Owner:** Indicates the entity or user that created the item. "Monitor" indicates that the item was created by the Traffic Analysis Agent for NetWare.
- **Status:** A status of Valid indicates that the agent is operating normally under the instructions given by the table.

Viewing Matrix Information

The matrix group records information about the conversations between pairs of nodes on a network segment. The information is stored in the form of a matrix. This method of organization is useful to retrieve specific pairings of traffic information, such as finding out which nodes are making the most use of a server.

To view the matrix information:

1. From the Network Adapter Items screen, select Matrix.
2. Press Enter.

The matrix group consists of three tables: two data tables and one control table. The data tables are matrixSDTable and matrixDSTable. The control table, matrixControlTable, includes the following objects, which correspond to the fields displayed in the Matrix Information screen:

- **Index:** An integer that uniquely identifies a row in the matrixControlTable. Each row in the control table defines a function that discovers conversations on a particular network and places statistics about them in the two data tables.
- **Data Source:** Identifies the network adapter, and the Ethernet, FDDI, or token ring segment that are the source of the data for the entries defined by this object.
- **Table Size:** The number of rows in the matrixTable associated with this row.
- **Last Delete Time:** The value of the sysUpTime object that corresponds to the last time an entry was deleted from the portion of the matrixTable associated with this row. The value is zero (0) if no deletions occurred.
- **Owner:** Indicates the entity or user that created the item. "Monitor" indicates that the item was created by the Traffic Analysis Agent for NetWare.
- **Status:** A status of Valid indicates that the agent is operating normally under the instructions given by the table.

Migrating Trend Files

From ConsoleOne, you can view trends of traffic patterns on the monitored Ethernet, FDDI, and token ring segments. You can use the trend data to analyze traffic on the segment. For details, see “Analyzing Trend Data for a Segment” on page 279.

Earlier versions of the Traffic Analysis Agent for NetWare (1.20 and 1.21) collected trend data that was sampled every one minute. The Traffic Analysis Agent for NetWare 1.30 that ships with ZfS collects trend data that are sampled every one minute, one hour, and one day. This functionality of version 1.30 of the Traffic Analysis Agent for NetWare ensures minimal communication between the agent and ConsoleOne, to reduce network traffic.

You can use the migrating tool (GTREND.EXE) to convert the trend data collected by earlier versions of the Traffic Analysis Agent for NetWare to trend data that can be used by version 1.30 of Traffic Analysis Agent for NetWare and ConsoleOne.

To migrate trend files collected by versions 1.20 or 1.21 of the Traffic Analysis Agent for NetWare:

1. Copy GTREND.EXE from the Installation CD to a TEMP folder on a 32-bit Windows NT, Windows 2000, Windows 95, or Windows 98 machine.
2. Copy the trend data files collected by earlier versions of the Traffic Analysis Agent for NetWare to the TEMP folder.
3. Run GTREND.EXE.

   This will migrate the existing one-minute trend files to the corresponding one-hour and one-day trend files that can be used by version 1.30 of the Traffic Analysis Agent for NetWare.
4. Copy the migrated trend files to the SYS:\GTREND\ folder on the NetWare server and run the version 1.30 of the Traffic Analysis Agent for NetWare on the same server.

   NOTE: The migration tool will not migrate older token ring trend data collected by version 1.20 or 1.21 of the Traffic Analysis Agent for NetWare because the older agents implemented a proprietary Token Ring MIB that enabled the agent to collect trend data sampled every one minute. Version 1.3 of the Traffic Analysis Agent for NetWare implements the standard Token Ring MIB that supports historical trends (one minute, one hour and one day).

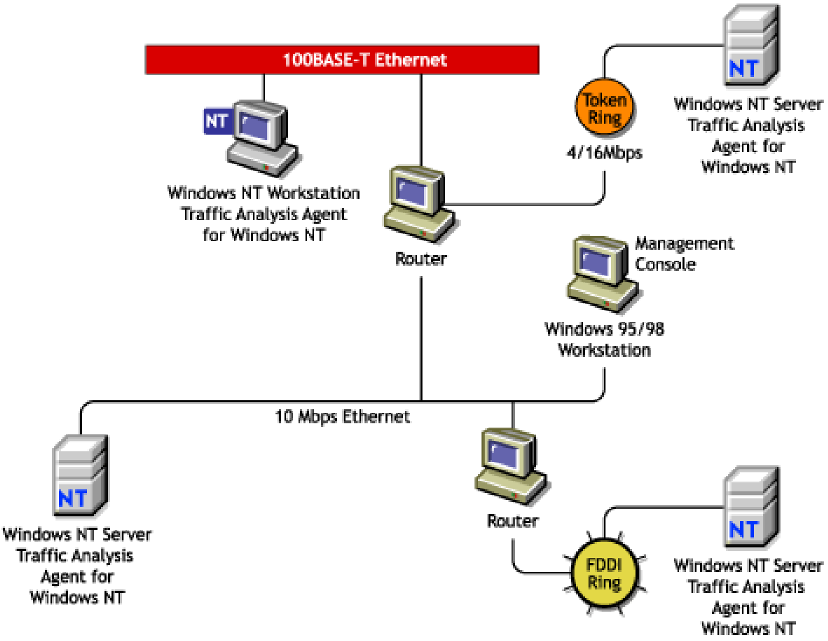
Using the Traffic Analysis Agent for Windows NT/2000

The Traffic Analysis Agent (version 1.30) for Windows NT/2000 runs on a Windows NT/2000 server or on a Windows NT workstation. The Traffic Analysis Agent for Windows NT/2000 monitors traffic on Ethernet, FDDI, or token ring segments.

The Traffic Analysis Agent for Windows NT/2000 is an RMON agent that implements functionality defined by the RMON MIB. It implements token ring extensions for RMON (RFC 1513 (http://www.isi.edu/in-notes/rfc1513.txt)) for token ring media, and a Novell proprietary MIB for FDDI media, in addition to implementing an RMON (RFC 1757 (http://www.isi.edu/in-notes/rfc1757.txt)) for Ethernet media.

The agent collects information about activity on your network and makes it available to ConsoleOne via SNMP. The Traffic Analysis Agent for Windows NT/2000 also implements the first two groups of RMON2 (RFC 2021 (http://www.isi.edu/in-notes/rfc2021.txt)).

The following figure illustrates a functional view of the Traffic Analysis Agent for Windows NT/2000:


100BASE-T Ethernet
NT
Windows NT Workstation Traffic Analysis Agent for Windows NT
Router
Token Ring
4/16Mbps
NT
Windows NT Server Traffic Analysis Agent for Windows NT
Management Console
Windows 95/98 Workstation
10 Mbps Ethernet
NT
Windows NT Server Traffic Analysis Agent for Windows NT
Router
FDDI Ring
NT
Windows NT Server Traffic Analysis Agent for Windows NT

Changes Made During Installation

When you install the Traffic Analysis Agent for Windows NT/2000, the following files are copied to Windows NT/2000:

File Name	Location	Description
LANZNDIS.SYS	\WINNT\SYSTEM32\DRIVERS	Kernel mode driver interface
LANZCTL.DLL	\WINNT\SYSTEM32	Control module

File Name	Location	Description
LANZMEM.DLL	\WINNT\SYSTEM32	Memory manager module
LANZLIB.DLL	\WINNT\SYSTEM32	Library module
LANZDI.DLL	\WINNT\SYSTEM32	User mode driver interface
LANZSM.DLL	\WINNT\SYSTEM32	Monitor module
LANZHIS.DLL	\WINNT\SYSTEM32	History module
LANZAEL.DLL	\WINNT\SYSTEM32	Alarm, event, and log module
LANZFCB.DLL	\WINNT\SYSTEM32	Filter capture, buffer module
LANZTR.DLL	\WINNT\SYSTEM32	Token ring manager module
LANZFDDI.DLL	\WINNT\SYSTEM32	FDDI manager module
GTREND.DLL	\WINNT\SYSTEM32	Trend module
LANZCON.EXE	\LANZNT	Agent console application
LANZCON.HLP	\LANZNT	Agent console help
LANZCON.CNT	\ZFS_AGNT\LANZCON	Required for online help from the application
GTREND.EXE	\ZFS_AGNT\LANZCON	Tool for migration of trend data from the older agent.
MGMTAPI.DLL	\ZFS_AGNT\LANZCON	SNMP application file
MSVCP50.DLL	\ZFS_AGNT\LANZCON	MFC APIs required for LANZCON
LANZCTL.DLL	\ZFS_AGNT\LANZCON	Required for LANZCON
MSFLXGRD.OCX	%SystemRoot%\System32	Enables ActiveX* Controls in LANZCON

IMPORTANT: The default directory location for the LANZCON application is ZFS_AGNT\LANZCON. You can change the location of LANZCON during installation.

The following sections provide information about optimizing and using the Traffic Analysis Agent for Windows NT/2000:

- "Planning to Install the Traffic Analysis Agent for Windows NT/2000" on page 356
- "Optimizing the Traffic Analysis Agent for Windows NT/2000" on page 359
- "Using LANZCON" on page 363

Planning to Install the Traffic Analysis Agent for Windows NT/2000

The Traffic Analysis Agent for Windows NT/2000 requires configuration of the Windows NT/2000 SNMP service before installing the agent. This section contains: Perform the following tasks to allow communication with the management server:

- WinNT
- Win2K

Installing and Configuring the Windows NT SNMP Service

Before installing the ZfS agent, you must install and configure the Windows NT SNMP service. This is required to enable communication with the management server.

To install and configure SNMP on Windows NT:

1 Install the SNMP service.

1a In the Control Panel, select Network > select Services > click Add.

1b Select SNMP Service from the Select Network Service dialog box.

1c Click OK.

1d Enter the full path to the Windows NT distribution files.

1e Click Continue.

2 Configure SNMP to start automatically.

2a In the Control Panel, double-click Services.

2b Click SNMP > Startup.

2c In the Startup Type options, select Automatic.

3 Configure the SNMP Trap service to start automatically.

3a In the Control Panel, double-click Services.

3b Click SNMP Trap Service > Startup.

3c In the Startup Type options, select Automatic.

4 Specify the trap community name and trap destination address so that the agent sends traps to the management server.

4a In the Control Panel, double-click Network.

4b Click the Services tab > select SNMP Service.

4c Click Properties.

4d Click the Traps tab.

4e Select a name from the Community Names box > click Add.

The Add button is disabled if there are no Community Names available.

4f If the public community name is not present, type **`public`**.

4g Click Add.

4h Use the Trap Destinations box to add other DNS names and IP addresses in addition to the loopback IP address for the workstations or servers that should receive traps.

4i Click OK.

5 Set the SNMP security options trap community name so that SNMP packets from any host are accepted by the agent.

5a In the Control Panel, double-click Network.

5b Click the Services tab > select SNMP Service.

5c Click Properties.

5d Click the Security tab.

5e In the Accepted Community Names box, click Add.

5f In the Community Name box, type **`public`**.

The Accepted Community Names list displays the community names from which Windows NT will accept requests.

5g Click Add.

5h Select Accept SNMP Packets from Any Host > click OK.

Installing and Configuring the Windows 2000 SNMP Service

Before installing the ZfS agent, you must install and configure the Windows 2000 SNMP service. This is required to enable communication with the management server.

To install and configure SNMP on Windows 2000:

1 Install the SNMP service.

1a In the Control Panel, select Administrative Tools > Configure Your Server.

1b In the Application Server option, select Terminal Services.

1c Click Start.

1d In the Windows Components Wizard, double-click Management and Monitoring Tools.

1e Select Simple Network Management Protocol.

1f Click OK.

1g Click Next.

SNMP is started automatically after installation.

2 Configure the SNMP Trap service to start automatically.

2a In the Control Panel, select Administrative Tools > Services.

2b Click SNMP Trap Service > Startup.

2c In the Startup Type options, select Automatic.

3 Specify the trap community name and trap destination address so that the agent sends traps to the management server.

3a In the Control Panel, select Administrative Tools > Services

3b Double-click SNMP Service.

3c Click Properties.

3d Click the Traps tab.

3e Select a name from the Community Names box > click Add.

The Add button is disabled if there are no Community Names available.

3f If the public community name is not present, type **`public`**.

3g Click Add.

3h Use the Trap Destinations box to add other DNS names and IP addresses in addition to the loopback IP address for the workstations or servers that should receive traps.

3i Click OK.

4 Set the SNMP security options trap community name so that SNMP packets from any host are accepted by the agent.

4a In the Control Panel, select Administrative Tools > Services.

4b Double-click SNMP Service.

4c Click Properties.

4d Click the Security tab.

4e In the Accepted Community Names box, click Add.

4f Select a name from the Community Name box.

The Accepted Community Names list displays the community names from which Windows 2000 will accept requests.

4g Click Add.

4h Select Accept SNMP Packets from Any Host > click OK.

IMPORTANT: After installing the SNMP services, you should re-install the service packs again.

Optimizing the Traffic Analysis Agent for Windows NT/2000

The Traffic Analysis Agent for Windows NT/2000 parameters are configured for optimal performance on Windows NT/2000. You can optimize the performance of the agent to suit your networking environment.

This section explains how to optimize the agent and monitor the functionality Traffic Analysis Agent for Windows NT/2000 using the agent console (LANZCON) for Windows NT/2000. For details, see "Using LANZCON" on page 363.

The following sections explain the Traffic Analysis Agent for Windows NT/2000 configuration options:

- "Configuring the Traffic Analysis Agent for Windows NT/2000" on page 360

- “Configuring the Modules of the Traffic Analysis Agent for Windows NT/2000” on page 360
- “Configuring the Parameters of the Traffic Analysis Agent for Windows NT/2000” on page 361
- “Automatically Loading the Agent with the SNMP Service” on page 363

Configuring the Traffic Analysis Agent for Windows NT/2000

The Traffic Analysis Agent for Windows NT/2000 provides default values for modules and parameters. You can change the default values to optimize the performance of the Traffic Analysis Agent for Windows NT/2000.

You can configure the following modules of the Traffic Analysis Agent for Windows NT/2000:

- Packet Capture
- Station Monitor
- Token Ring Manager
- FDDI Manager

  For details, see “Configuring the Modules of the Traffic Analysis Agent for Windows NT/2000” on page 360.

You can configure the following parameters of the Traffic Analysis Agent for Windows NT/2000:

- Memory Bound
- Memory Age
- Top N Station
- Generate Duplicate IP Address Alarms
- Trend Files Location

  For details, see “Configuring the Parameters of the Traffic Analysis Agent for Windows NT/2000” on page 361.

Configuring the Modules of the Traffic Analysis Agent for Windows NT/2000

By default, all agent modules are enabled to load. You can choose to disable the modules.

To disable the modules of the Traffic Analysis Agent for Windows NT/2000:

1. From the LANZCON main menu, click Configure > LANalyzer Agent Modules > Disable.
2. Deselect the module you want the agent to monitor.
3. Click OK.

Configuring the Parameters of the Traffic Analysis Agent for Windows NT/2000

The Traffic Analysis Agent for Windows NT/2000 modules are loaded with default parameters. You can modify the parameters to optimize the performance of the agent.

The following table describes the parameters of the Memory Manager module:

Parameter	Default Value	Range	Description
Memory Bound	4 MB	1 MB - 10 MB	Sets the upper limit of available memory that can be allocated dynamically to the Traffic Analysis Agent for Windows NT/2000.
Memory Age	168 hours	1 hour - 720 hours	Controls the duration for which the Traffic Analysis Agent for Windows NT/2000 stores data in memory. When the duration setting is reached, existing data is purged from memory.

To modify the Memory Bound parameter:

1. From the LANZCON main menu, click Configure > LANalyzer Agent Parameters.
2. Click the Memory Manager tab.
3. Move the Memory Bound slider to the point you want to set as the memory bound value.

To modify the Memory Age parameter:

1. From the LANZCON main menu, click Configure > LANalyzer Agent Parameters.
2. Click the Memory Manager tab.
3. Move the Memory Age slider to the point you want to set as the memory age value.

IMPORTANT: Restart the Traffic Analysis Agent for Windows NT/2000 to ensure that the agent utilizes the changed parameter values. For details, see Installing and Setting Up Management and Monitoring Services in the *Installation* guide.

The following table describes the parameters of the Station Monitor module:

Parameter	Default Value	Range	Description
TopN Station	4 reports	2 - 10 reports	Controls the number of TopN reports the agent can generate.
Generate Duplicate IP Address Alarms	On	-	Controls the generation of duplicate IP address alarms.

To specify the number of TopN reports you want the agent to generate:

1. From the LANZCON main menu, click Configure > LANalyzer Agent Parameters.
2. Click the Station Monitor tab.
3. Select the number of TopN reports.

To stop generation of duplicate IP address alarms:

1. From the LANZCON main menu, click Configure > LANalyzer Agent Parameters.
2. Click the Station Monitor tab.
3. Deselect the Generate Duplicate IP Address Alarms check box.

The following table describes the Network Trend parameter:

Parameter	Default Path	Description
Trend Files Location	*system root*\GTREND	Specifies the directory path and location where trend files (*.GT) are created and updated.

IMPORTANT: If you delete the *.GT file. all the previous trend information will be lost.

To specify a path to a location for storing trend data:

1. From the LANZCON main menu, click Configure > LANalyzer Agent Parameters.
2. Click the Network Trends tab.
3. Enter or browse to select the directory path to the location where you want the Traffic Analysis Agent for Windows NT/2000 to store trend data.

Automatically Loading the Agent with the SNMP Service

The Traffic Analysis Agent depends on the Microsoft* SNMP service on Windows NT/2000. When SNMP starts, it loads agent DLLs in its address space. Once the agent is installed, it will be always loaded by the SNMP service, by default, whenever the service starts.

You can enable or disable loading of the agent DLLs with SNMP by checking the desired options in the Novell Traffic Analysis Agent Loading with SNMP dialog box. If you disable the agent, the SNMP service will start normally but the Traffic Analysis Agent will not work. The Traffic Analysis Agent will neither capture packets by placing the NIC cards into the promiscuous mode nor will respond to SNMP requests.

Using LANZCON

This section explains how you can use the LANZCON utility to configure and diagnose the Traffic Analysis Agent for Windows NT/2000.

LANZCON for Windows NT/2000 is a graphical user interface provided by the Traffic Analysis Agent for Windows NT/2000 to configure the agent modules and parameters and to diagnose the agent. You can use LANZCON to obtain information about network segments monitored by the agent to help you troubleshoot problems.

To open the LANZCON utility, do one of the following:

- From the Windows NT/2000 Programs menu, click LANalyzer Agent for Windows NT > LANZCON.
- Double-click the LANZCON icon on your desktop.

You can perform the following tasks with LANZCON:

- "Viewing Network Adapters" on page 364

Viewing Network Adapters

On loading LANZCON, you will see the Network Adapters window. The Network Adapters window displays information about monitored adapters in two panes.

The following table describes the two panes in the Network Adapters window:

Pane	Displays	Description
Left pane	Adapter Tree view	Displays a list of network adapters discovered by the Traffic Analysis Agent for Windows NT/2000. The default view displays a collapsed tree. You can expand each network adapter in the tree to view the list of RMON tables for the selected adapter.
Right pane	Table view	Displays details about the object you select in the left pane. If you select an adapter in the left pane, interface table (RFC 1213 (http://www.isi.edu/in-notes/rfc1213.txt)) details such as media type, MAC address, and description of the selected adapter are displayed in the right pane. If you select an RMON table in the left pane, table data is displayed in the right pane.

Enabling or Disabling Network Adapter Monitoring

The Traffic Analysis Agent for Windows NT/2000 collects information about monitored adapters and displays it in the right pane of the Network Adapters window.

By default, adapter monitoring is enabled. LANZCON lets you disable adapter monitoring. If you disable adapter monitoring, the Traffic Analysis Agent for Windows NT/2000 will stop collecting data for the adapter and the RMON tables for the adapter will be deleted.

IMPORTANT: You cannot disable monitoring FDDI adapters through LANZCON.

To enable adapter monitoring:

1. Select an adapter in the left pane of the Network Adapters window.
2. Click View > NetWork Adapters > Enable.

To disable adapter monitoring:

1. Select an adapter in the left pane of the Network Adapters window.
2. Click View > NetWork Adapters > Disable.

Viewing the Agent Log

The Traffic Analysis Agent for Windows NT/2000 logs significant events and error messages that occurred during a session.

To view the agent log:

1. From the LANZCON main menu, click View > Agent Log.

Viewing the Agent Status

You can view the status of the agent from the LANalyzer Agent Status window. The agent status window indicates whether the agent modules are loaded or not loaded.

To view the agent status:

1. From the LANZCON main menu, click View > Agent Status.

Viewing RMON Tables

RMON tables are listed under each network adapter. You can view the RMON tables by selecting a table in the left pane of the Network Adapters window. RMON table data is displayed in the right pane.

The Network Adapter tree displays the following RMON tables:

- Statistics
- History Control

- History Data
- Host Control
- Host Entry
- Host TopN Control
- Host TopN Entry
- Matrix Control
- Matrix SD Entry
- Filter, Channel, and Buffer

The Alarm Information tree displays the following RMON tables:

- Alarm
- Event
- Log

Viewing SNMP Traps

The Traffic Analysis Agent for Windows NT/2000 monitors network segments and sends traps to the management server. ConsoleOne displays the alarm when it receives the trap from the management server.

Trap information is displayed in the SNMP Traps window. For each trap, the table shows trap data that can be obtained.

Statistic	Explanation
Receive Time	Displays the time when the trap occurred
Trap Summary	Displays a description of the trap

IMPORTANT: LANZCON will receive trap notifications if you have ensured that Windows NT/2000 SNMP has been configured to send traps to a loopback trap destination address. For details, see "Planning to Install the Traffic Analysis Agent for Windows NT/2000" on page 356.

To view SNMP traps from LANZCON main menu, click > View > SNMP Traps.

9 Customizing Agent Configuration

The ZENworks® for Servers (ZfS) server management SNMP agents run on NetWare® and Windows* NT* servers in your network. The agents monitor servers, collecting historical data and dynamic data in response to requests from ConsoleOne®. An administrator at the ZfS ConsoleOne can request data simply by clicking a representative icon for any device, operating system, or service discovered on a server.

After the Management Agent for NetWare and the Management Agent for Windows NT have been installed on your network NetWare and Windows NT servers, they are ready to operate with the default settings. In most cases, this configuration is sufficient; however, you can customize the agent settings to enhance management functionality.

This appendix contains the following sections:

- "Agent Files" on page 367
- "Customizing the Management Agent for NetWare" on page 371
- "Customizing the Management Agent for Windows NT Server" on page 374

Agent Files

The following sections describe the agent files that are installed on each managed server:

- "Management Agent for NetWare Files" on page 368
- "Management Agent for Windows NT Server Files" on page 370

Management Agent for NetWare Files

The following table describes the Management Agent for NetWare NLM™ files installed on a NetWare server:

Management Agent for NetWare NLM Files	**Description**
SERVINST.NLM	Implements the NetWare server MIB (NWSERVER.MIB).
HOSTMIB.NLM	Implements the standard Host Resources MIB [RFC 1514] and Novell® extensions to that MIB (NWHOSTX.MIB).
NTREND.NLM	Implements the Threshold and Trend MIB (NWTREND.MIB). When loaded, NTREND.NLM sets trends and thresholds for each monitored attribute according to the server's configuration. The NTREND.INI file contains configuration parameters for NTREND.NLM.
NWTRAP.NLM	Implements the NetWare Server Trap MIB (NWALARM.MIB). The NWTRAP.CFG file contains configuration parameters for NWTRAP.NLM.
FINDNMS.NLM	Used by NetWare servers running the Management Agent for NetWare. Employ FINDNMS.NLM to listen for SNMP Management console advertising themselves using the Service Advertising Protocol (SAP) number 0x026a. FINDNMS.NLM then adds the Internetwork Packet Exchange™ (IPX™) address of each ConsoleOne discovered to the list of stations that receive traps.
NDSTRAP.NLM	Implements the NDSTRAP.MIB to capture and forward Novell eDirectory events to SNMP Management console.
MONDATA.NLM	Allows you to monitor NetWare servers.

The following table provides a brief description of the enterprise MIBs associated with the Management Agent for NetWare:

MIB Name	Description
NDSTRAP.MIB	A Novell proprietary MIB designed to capture eDirectory events and forward them to SNMP Management console as SNMP traps. There are more than 130 traps currently in the MIB and new ones are being added as they are identified.
NWALARM.MIB	A Novell proprietary MIB that handles all the NetWare Core OS alerts and forwards them as SNMP traps. It currently supports more than 375 traps and new ones are being added as they are identified.
NWHOSTX.MIB	A Novell extension to RFC1514 (the Host Resources MIB). It adds devices and components that are specific to NetWare that were not directly included in RFC1514.
NWSERVER.MIB	A Novell proprietary MIB that is the basis for NetWare Core OS management. More than 300 objects are identified in this MIB. Access to the parameters that can be set from the console for both GET and SET is defined. The MIB has several groups and tables for users, file systems, volumes, queues, Open Data-Link Interface^{TM} (ODI^{TM}), set parameters, and so forth.
NWTMSYNC.MIB	A Novell proprietary MIB that allows for SNMP management of TIMESYNC.NLM. It provides access to the list of time sources as well as time clients. You may also access the clock structure through this MIB.
NWTREND.MIB	A Novell proprietary MIB that keeps track of objects that are most useful when tracked over a period of time. For example, CPU utilization and packets received have limited value as static numbers, but when monitored at regular intervals for a period of time, they tell a great deal about what is happening on a server. This MIB also lets you set user-definable thresholds for the managed objects and will send SNMP traps when a threshold is exceeded.
RFC1514.MIB	The Internet Standard Host Resources MIB. It defines general categories about a host machine, including physical components of the system such as disks, memory, CPU, printers, adapter cards, and so forth.

Management Agent for Windows NT Server Files

Following is a list of files that can be manually configured with a text editor to modify default results of the Management Agent for Windows NT:

Management Agent for Windows NT Server .INI Files	Description
N_NTTREN.INI	Specifies the initial values for the trends and thresholds supported by the Management Agent for Windows NT.
NTTRAP.INI	Specifies settings to troubleshoot your Windows NT server that runs the Management Agent for Windows NT and settings to enable you to send Windows NT events to the management system as SNMP traps.
NTHOST.INI	Specifies the SNMP settings supported by the Management Agent for Windows NT.
N_NTFMW.INI	Allows you to specify IPX addresses that will be ignored and will not receive SNMP traps.

The following table provides a brief description of the enterprise MIBs associated with the Management Agent for Windows NT. In addition, the Management Agent for Windows NT converts all Windows NT system, security, and application events to SNMP traps.

MIB Name	Description
NTSERVER.MIB	Gives minimal Windows NT system information like Server Name, OS, major and minor versions, time zone, remote and local volumes count, etc.
RFC1514.MIB	The Internet Standard Host Resources MIB. It defines general categories about a host machine, including physical components of the system such as disks, memory, CPU, printers, adapter cards, and so forth.

MIB Name	Description
NTTRAP.MIB	A generic MIB based on RFC1514. Windows NT events that are converted into traps are forwarded to the ZfS network management system.
NTTREND.MIB	A Novell proprietary MIB that keeps track of objects that are most useful when tracked over a period of time. For example, CPU utilization and packets received have limited value as static numbers, but when monitored at regular intervals for a period of time, they tell a great deal about what is happening on a server. This MIB also lets you set user-definable thresholds for the managed objects and will send SNMP traps when a threshold is exceeded.

Customizing the Management Agent for NetWare

The Management Agent for NetWare installation process creates the NMA2.NCF file (NetWare 3.*x* and 4.*x* servers) or the NMA5.NCF file (NetWare 5.*x* servers) in the SYS:\ZFS_AGNT\NMA directory. When the NetWare server is started, this file automatically loads all the NLM files required for the Management Agent for NetWare in a default configuration state. There are, however, several LOAD parameters that you can configure for each of the NLM files used with the agent.

You can configure your server to use these options by editing the NMA2.NCF or NMA5.NCF file on your server. Also, if your server is already running, you can unload any of these NLM files and then load them at the NetWare server console using any of the configuration parameters. You can configure these parameters at the NetWare server console or by using the NetWare remote console utility, RCONSOLEJ.

The sections that follow describe each of the command-line parameters that you can configure for the Management Agent for NetWare.

- "SERVINST.NLM Load Parameters" on page 372
- "HOSTMIB.NLM Load Parameters" on page 372
- "NTREND.NLM Load Parameters" on page 373

SERVINST.NLM Load Parameters

SERVINST.NLM implements the NWSERVER.MIB NetWare Server MIB. You can load SERVINST.NLM at the command line with any or all of the following parameters:

```
LOAD SERVINST D, U=n, V, B=n H
```

Parameter	Description
D	DisableSets: If this parameter is present, SERVINST.NLM does not allow SNMP SET commands for objects in NWSERVER.MIB. Default: SETS enabled (subject to SNMP security).
U=*n*	UpdateInterval=*n*: Sets the list update interval to *n* (*n* is a value in seconds). This determines how often certain internal lists kept by SERVINST.NLM (such as volumes and queues) are updated. Set this parameter higher to minimize the number of CPU cycles used by SERVINST.NLM, or lower to guarantee immediate reporting of server status changes that affect the lists. Default: 300 seconds.
V	Verbose: Displays informational messages. Default: Off.
B=*n*	BuildUserListHour=*n*: The local time each day on a 24-hour clock (0 to 23) at which the SERVINST.NLM software builds a list of users that have access to the server. Default: 2 (2:00 AM).
H	Help: Displays help on command line parameters. If you use the H parameter, SERVINST.NLM displays the help messages and then exits. It does not remain loaded even if other parameters are entered on the command line. Default: Off.

HOSTMIB.NLM Load Parameters

HOSTMIB.NLM implements both the standard Host Resources MIB (RFC 1514) and the Novell extensions to the Host Resources MIB

(NWHOSTX.MIB). You can load HOSTMIB.NLM at the command line with any or all of the following parameters:

```
LOAD HOSTMIB.NLM D, U=n, V, H
```

Parameter	Description
D	DisableSets: If this parameter is present, HOSTMIB.NLM does not allow SNMP SET commands for objects in RFC1514.MIB or NWHOSTX.MIB. Default: SETS enabled (subject to SNMP security).
U=*n*	UpdateInterval=*n*: Sets the list update interval to *n* (*n* is a value in seconds). This determines how often certain internal lists kept by HOSTMIB.NLM are updated. Set this parameter higher to minimize the number of CPU cycles used by HOSTMIB.NLM, or lower to guarantee immediate reporting of server status changes that affect the lists. Default: 60 seconds.
V	Verbose: Displays informational messages. Default: Off.
H	Help: Displays help on command-line parameters. If you use the H parameter, HOSTMIB.NLM displays the help messages and then exits. It does not remain loaded even if other parameters are entered on the command line. Default: Off.

NTREND.NLM Load Parameters

NTREND.NLM implements the Threshold and Trend MIB (NWTREND.MIB).

When first loaded, NTREND.NLM automatically sets trends and thresholds for each monitored attribute according to the server's configuration from values stored in the NTREND.INI file (located in the SYS:\ETC directory). You can edit this file as described in "Setting Default Trends and Thresholds" on page 162.

Thereafter, as configuration changes occur over time, NTREND.NLM adjusts to changes in the number and type of physical network interfaces, queues, volumes, and disks. Default thresholds are set only for important parameters.

You can later use SNMP SET commands to set thresholds for parameters such as files read and packets in.

A trend file is created for each monitored attribute instance, even if trending is disabled for that object. The file header contains all the information from nwtControlTableEntry, and the rest of the file stores the sample history (if any). Once a trend file is created, it exists until explicitly deleted by the operator, even if the monitored object (a queue, for example) no longer exists. When a monitored object no longer exists, the associated nwtControlStatus is recorded as invalid.

You can load NTREND.NLM at the command line with any or all of the following parameters:

```
LOAD NTREND D=dir, R, V, H
```

Parameter	Description
D=*dir*	Directory=*dir*: Enables you to specify the volume and directory where NTREND.NLM stores the history data files. Example: To use VOL1:\TEST as the directory for trending files, enter the following command: **load ntrend D=vol1:\test** Default: SYS:\NTREND.
R	Reset: Causes NTREND.NLM to discard all the old trending history data and restart the sampling.
V	Verbose: Displays informational messages. Default: Off.
H	Help: Displays help on command-line parameters. Default: Off.

Customizing the Management Agent for Windows NT Server

You can manually edit the following files to modify the default Management Agent for Windows NT configuration on a managed Windows NT server.

Management Agent for Windows NT Server .INI Files	Description
N_NTFMW.INI	Allows you to specify IPX addresses that will be ignored and will not receive SNMP traps.
NTTRAP.INI	Specifies settings to troubleshoot your managed Windows NT servers and set trap filters to specify which Windows NT events are sent to the management system as SNMP traps. See "Controlling Alarm Generation" on page 168 for detailed information on configuring trap filters and trap generation.
N_NTTREN.INI	Specifies the initial values for the trends and thresholds supported by the Management Agent for Windows NT. See "Setting Default Trends and Thresholds" on page 162 for detailed information on modifying default trends and thresholds.

Configuring the Management Agent for Windows NT Server

By default, the Management Agent for Windows NT sends traps to SNMP Management console on IPX networks broadcasting the 0x026 Service Advertising Protocol (SAP) ID. You can edit the N_NTFMW.INI file to include the IPX addresses of SNMP Management console that you do not want to include as trap targets.

To add the IPX address of a SNMP Management console to omit as an automatic trap recipient:

1. Open the N_NTFMW.INI file in a text editor.
2. Add the IPX address for omitted SNMP Management console using the following syntax:

   xxxxxxxx.yyyyyyyyyyyy

   where *xxxxxxxx* is the net address and *yyyyyyyyyyyy* is the node address, such as 01014044.00001B4DDAFD.
3. Save the file and restart the Management Agent for Windows NT.

Third-Party Agent Configuration

Third-party SNMP agents require the following tasks to be completed before traps are received:

- "Ensuring that Traps Are Received" on page 376
- "Integrating Vendor-Specific SNMP Traps" on page 376

Ensuring that Traps Are Received

When configuring the SNMP agent or SNMP Remote Network Monitoring (RMON) agent on a network device, configure the agent's trap destination list (trap-target list) to include the ZfS management server station IP address or server name. Refer to the agent's documentation for information on configuring this. ConsoleOne displays alarms for all devices that forward alarms to the management server.

If your network device is using the Management Agent for NetWare, Management Agent for Windows NT Server, NetWare LANalyzer® Agent™, or the LANalyzer Agent for Windows NT, the agent's trap destination list is automatically configured for you. For information on configuring the trap destination list, see "Setting Up Discovery" on page 106 for configuration information and Chapter 8, "Understanding Traffic Analysis," on page 251 for information on configuring the RMON agents.

Integrating Vendor-Specific SNMP Traps

Before AMS can process the alarm, you must include vendor-specific MIBs for the third-party SNMP agents in the management server MIB pool. You can further integrate third-party SNMP agents by annotating the trap definitions in the vendor MIB.

AMS interprets ASN.1 annotations to trap definitions in a MIB to set the severity level and device status assigned to an alarm. The MIBs included with ZfS already include the proper annotations. The annotations provide detail on severity levels and device status to the AMS.

See Chapter 6, "Using the MIB Tools," on page 211 for information on adding a MIB to the management server's MIB pool and annotating third-party MIBs.

10 Protocol Decodes Suites Supported by ZfS

ZENworks® for Servers (ZfS) provides packet capture and decoding tools that help you analyze the network activity and identify the source of network problems. Capturing and decoding packets can help you troubleshoot network problems by giving you detailed information about segment activity. For details, see "Capturing Packets" on page 295 and "Displaying Captured Packets" on page 299.

This section provides information about decoding support provided by ZfS for the following protocol suites:

- "NetWare Protocol Suite" on page 377
- "Network File System Protocol Suite" on page 380
- "Systems Network Architecture Protocol Suite" on page 381
- "AppleTalk Protocol Suite" on page 382
- "TCP/IP Protocol Suite" on page 384

NetWare Protocol Suite

NetWare® contains a group of protocols that perform various functions in a NetWare network. Each protocol in the NetWare protocol suite works with the IPX™ protocol. ZfS supports the following protocols in the NetWare suite of protocols:

NetWare Protocol	Description
BCAST	NetWare Broadcast Message Notification. The protocol a NetWare server uses to inform an idle workstation that a message is pending. This message appears on the top or bottom line of the monitor on DOS stations.
DIAG	Diagnostic Responder. A protocol used for connectivity testing and information gathering. By default, NetWare clients use the Diagnostic Responder to reply to diagnostic requests.
IPX	Internetwork Packet Exchange™. A protocol that routes outgoing data packets across a network. Every NetWare network has a unique address assigned when its servers are configured. IPX routers use this address to route packets through an internetwork. IPX makes routing decisions based on information compiled by the Routing Information Protocol (RIP).
LSP	NetWare Lite™ Sideband Protocol. A connectionless (datagram) oriented protocol that operates as a sideband for NetWare Lite Transport Protocol (NLTP) connections.
NBIOS	NetBIOS. An emulator that allows workstations to run applications that support IBM* NetBIOS calls. NetBIOS is the IBM standard protocol for applications developed to run peer-to-peer communications on token ring networks.
NCP™	NetWare Core Protocol™. A set of procedures that a file server operating system follows to accept and respond to workstation requests. An NCP exist for every service a workstation might request from a file server. Common requests handled by the NCP protocols include creating or deleting a file, manipulating directories and files, performing a directory listing, altering the bindery (drive mappings and security), and printing.
NDS®	The NDS protocol, called the Novell Directory Access Protocol (NDAP), is a wire protocol that allows Novell eDirectory to service client requests and to send client requests to other Novell eDirectory servers. NDAP is built based on NCP.

NetWare Protocol	Description
NLP	NetWare Lite Protocol. A protocol that is an integral part of NetWare Lite, which operates on top of the Novell IPX protocol. NLP is an application-layer and service-layer protocol that performs file system and print functions. NLP also uses NLTP, which is similar in function to the transport protocol used in NCP.
NLSP™	NetWare Link Services Protocol™. A link-state routing protocol designed for IPX internetworks.
RIP	Routing Information Protocol. A protocol that automates the process of updating routing tables. Routing is the process of moving network packets between separate networks. With RIP, when one router learns about changes in its routes, it broadcasts this information to neighboring routers so they can update their routing tables. As a result, if a network component fails (such as a router or a phone line), the other network components can inform each other of alternate routes. When the faulty component is repaired, the network changes back to the previous condition.
SAP	Service Advertising Protocol. A protocol that lets NetWare servers advertise their services by name and type. A workstation can broadcast a request to find all services available or a specific service closest to the client.
SER	Novell Serialization (Copy Protection) Packets. Packets that NetWare servers send to other NetWare servers to ensure that each server has a unique serial number.
SNMP	Simple Network Management Protocol. An application-layer protocol designed to facilitate the exchange of management information between network devices. By using SNMP to access management information data (such as packets per second and network error rates), network administrators can easily manage network performance and find and solve network problems.

NetWare Protocol	Description
SPX™	Sequenced Packet Exchange™. A connection-oriented transport protocol that monitors network transmissions to ensure successful delivery of packets. SPX enhances the IPX protocol by supervising data sent across the network. SPX can track data transmissions consisting of a series of separate packets. SPX also requests acknowledgments from and returns acknowledgments to a communications partner, ensuring successful data delivery. If an acknowledgment request brings no response within a specified time, SPX retransmits the request. After a reasonable number of retransmissions fail to return a positive acknowledgment, SPX assumes the connection has failed and reports the error. The NetWare print server uses SPX.
WDOG	Watchdog. A maintenance protocol provided with NetWare. Watchdog monitors stations that are logged in to a NetWare server. Watchdog determines whether the NetWare shells are still operating and, if not, releases the connection.

Network File System Protocol Suite

The Network File System (NFS) suite of protocols is described in the following table.

Network File System Protocol	Description
MOUNT	The MOUNT protocol, used in conjunction with NFS, performs operating system-specific functions that allow NFS clients to attach remote directory trees to a point within the local file system.
NFS	Network File System. This protocol provides transparent remote access to shared file systems across networks. NFS uses Remote Procedure Call (RPC) and is machine, operating system, network architecture, and transport protocol independent.

Network File System Protocol	Description
PORTMAP	The PORTMAP protocol converts RPC program numbers into Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port numbers. When a client wants to make an RPC call to a given program number, it will first contact PORTMAP on the remote machine to determine the port number where RPC packets should be sent.
RPC	Remote Procedure Call. This protocol allows a program on one computer to make a subroutine call on a remote computer. Every subroutine or remote procedure is identified by a unique program number.

Systems Network Architecture Protocol Suite

The Systems Network Architecture (SNA) suite of protocols is described in the following table.

Systems Network Architecture Protocol	Description
RH	Request/Response Header. This protocol carries the SNA Request/Response Units as its payload.
RU	Request/Response Unit. An SNA client uses this protocol to communicate with an SNA server.
TH	Transmission Header. This protocol runs on a data link layer and serves as the transmission layer for an SNA Path Information Unit.
XID	Exchange Station Identification. An SNA node uses this protocol to check whether its peer SNA node is ready for communication and to exchange its station details with it.

AppleTalk Protocol Suite

The AppleTalk* and AppleTalk-related suite of protocols is described in the following table.

AppleTalk Protocol	Description
AARP	AppleTalk Address Resolution Protocol. An AppleTalk protocol that reconciles addressing differences between a data link protocol and the rest of a protocol family. For example, by resolving the differences between an Ethernet addressing scheme and the AppleTalk addressing scheme, AARP facilitates the transport of datagram delivery protocol (DDP) packets over a high-speed EtherTalk* connection.
ADSP	AppleTalk Data Stream Protocol. A connection-oriented protocol that provides a reliable, full-duplex, byte stream service between any two sockets in an AppleTalk internetwork. ADSP ensures sequential, duplicate-free delivery of data over its connections.
AEP	AppleTalk Echo Protocol. A simple protocol that allows a node to send a packet to any other node in an AppleTalk internetwork and receive an echoed copy of that packet in return.
AFP	AppleTalk Filing Protocol. A presentation layer protocol that allows users to share data files and applications that reside in an AppleTalk shared resource, such as a file server.
ASP	AppleTalk Session Protocol. A general, all-purpose protocol that uses the services of the AppleTalk Transaction Protocol (ATP) to provide session establishment, maintenance, and tear-down, along with request sequencing.
ATP	AppleTalk Transaction Protocol. A transport protocol that provides a loss-free transaction service between sockets. This service allows exchanges between two socket clients in which one client requests the other to perform a particular task and report the results. ATP binds the request and response together to ensure the reliable exchange of request-response pairs.

AppleTalk Protocol	Description
E-DDP	Extended Datagram Delivery Protocol. A datagram delivery protocol that uses an extended header. An extended header is required for packets that are transmitted from one network to another network within an AppleTalk Internet.
ELAP	EtherTalk Link Access Protocol. The link-access protocol used in an EtherTalk network. It is built on the top of the standard Ethernet data link layer.
NBP	Name Binding Protocol. A transport layer protocol that translates a character string name into the internetwork address of the corresponding socket client. NBP enables AppleTalk protocols to understand user-defined zones and device names by providing and maintaining translation tables that map these names to corresponding socket addresses.
PAP	Printer Access Protocol. This protocol manages interaction between workstations and print servers. It handles connection setup, maintenance, and termination. It can also handle data transfer.
RTMP	Routing Table Maintenance Protocol. This AppleTalk protocol establishes and maintains the routing information that is required by internetwork routers to route datagrams from any source socket to any destination socket in the internetwork. Using RTMP, internetwork routers dynamically maintain routing tables to reflect changes in internetwork topology.
S-DDP	Short Datagram Delivery Protocol. A DDP that uses a short header. A short header is often used for packets whose source and destination sockets are within the boundaries of a single AppleTalk network.
ZIP	Zone Information Protocol. A protocol that maintains up-to-date routing information across the internetwork.

TCP/IP Protocol Suite

The TCP/IP suite of protocols is described in the following table.

TCP/IP Protocol	Description
ARP	Address Resolution Protocol. A protocol used by a host to determine the hardware address of another host. A TCP/IP system contains a table that maps IP addresses to the hardware addresses of the different hosts and routers on the internetwork. This table works in much the same way as a host table, translating an IP address to an Ethernet address. Unlike the host table, however, the ARP table is not usually maintained by you or your network administrator. The ARP protocol creates entries in this table as needed. If the hardware address of the destination is not found in your station's ARP table, a broadcast is sent to every host on the network requesting the address. If that host is up and supports the ARP protocol, it receives the broadcast from your station and responds by sending its hardware address back to your station. This address is then added to your station's ARP table.
IMAP	IMAP stands for Internet Message Access Protocol. It is a method of accessing electronic mail or bulletin board messages that are placed on a (possibly shared) mail server. It permits a "client" e-mail program to access remote message stores as if they were local.
BOOTP	BootStrap Protocol. This protocol allows a diskless workstation to determine its IP address and other information without using the Reverse Address Resolution Protocol (RARP).
DHCP	Dynamic Host Configuration Protocol. This protocol supplies hosts with configuration parameters, leases dynamically allocated IP addresses, and acts as an enhancement to BOOTP.
DNS	Domain Name System. The distributed naming service used on the Internet. DNS provides a computer's IP address if domain names exist for the computer.
FTP	File Transfer Protocol. TCP/IP application-layer protocol that supports file transfers.

TCP/IP Protocol	Description
HTTP	Hypertext Transfer Protocol. An application-layer protocol that Web browsers and Web servers use to communicate with each other.
ICMP	Internet Control Message Protocol. A protocol that works with IP to provide routing efficiency and error information. ICMP is part of the TCP/IP protocol suite. Because IP is connectionless, it cannot detect anomalous internetwork conditions. ICMP works with IP to provide TCP or other upper-layer protocols with this information.
IGMP	Internet Group Management Protocol. A protocol used by IP hosts to report their multicast group memberships to routers. The protocol is also used to query routers on memberships and to generate reports on group membership. Termination of group membership can be quickly reported using this protocol.
IP	Internet Protocol. A protocol that provides connectionless, nonguaranteed delivery of transport layer packets (also called transport protocol data units or TPDUs) across an internetwork. IP is part of the TCP/IP protocol suite. IP can fragment TPDUs into smaller parts, if necessary, and then reassemble them at an intermediate station (usually a router) or at their destination host. Each TPDU or fragment is fitted with an IP header and transmitted as a packet by lower-layer protocols. IP moves datagrams through the internetwork, one hop at a time. If a TPDU fragment arrives at its destination out of order, IP reassembles the fragments, in sequence, at the destination.
LDAP	Lightweight Directory Access Protocol. This protocol provides access to the x.500 Directory while not incurring the resource requirements of the Directory Access Protocol (DAP). LDAP is specifically targeted at simple management applications and browser applications that provide read/write interactive access to the x.500 Directory, and is intended to be a complement to the DAP itself.

TCP/IP Protocol	Description
NFS	The Network File System (NFS) protocol provides transparent remote access to shared files across networks. The NFS protocol is designed to be portable across different machines, operating systems, network architectures, and transport protocols. This portability is achieved through the use of Remote Procedure Call (RPC) primitives built on top of an eXternal Data Representation (XDR).
NTP	Network Time Protocol. A protocol used to synchronize timekeeping among a set of distributed time servers and clients. It is used to convey timekeeping information in a hierarchical method from servers to clients. It is also used to cross-check clocks and control errors due to equipment or propagation failures.
NWIP	NetWare/IP. Allows total or partial replacement of the IPX transport subsystem with the industry-standard TCP/IP subsystem, in a NetWare network. The following constitute the core components of the technology: ◆ Communication between the NetWare/IP server and the Domain SAP/RIP Service (DSS) for - Retrieval of configuration parameters - Registration of SAP and RIP information - SAP/RIP database synchronization ◆ Synchronization of the NetWare/IP server with the DSS database with respect to SAP/RIP information ◆ Communication between secondary DSS and primary DSS to synchronize the SAP/RIP database on the two servers
OSPF	Open Shortest Path First. A protocol in the TCP/IP protocol suite is an interior gateway protocol algorithm and is proposed as a standard for the Internet. OSPF incorporates least-cost routing, multipath routing, load balancing, and efficient bandwidth utilization.
POP3	Post Office Protocol 3. A protocol used for interacting with a central mailbox server. It is a client/server protocol used to receive e-mail. The protocol holds the e-mail messages in the Internet server. Periodically, you can download the messages from the server.

TCP/IP Protocol	Description
RARP	Reverse Address Resolution Protocol. A protocol in the TCP/IP protocol suite that is used to determine a software address based on a hardware address. This protocol is often used by diskless workstations during startup.
RIP	Routing Information Protocol. A protocol in the NetWare protocol suite that automates the process of updating routing tables. Routing is the process of moving network packets between separate networks. With RIP, when one router learns about changes in its routes, it broadcasts this information to neighboring routers so they can update their routing tables. As a result of RIP, if a network component fails (such as a router or a phone line), the other network components can inform each other of alternate routes. When the faulty component is repaired, the network changes back to the previous condition.
SSL	SSL is an open, nonproprietary protocol. It has been submitted to the W3 Consortium (W3C) working group on security for consideration as a standard security approach for World Wide Web browsers and servers on the Internet.
SLP	Service Location Protocol. This protocol provides a scalable framework for the discovery and selection of network services. Using this protocol, computers using the Internet no longer need as many static configurations of network services for network-based applications.
SMTP	Simple Mail Transfer Protocol. The application layer protocol that e-mail clients and servers use to exchange e-mail messages with each other.

TCP/IP Protocol	Description
SNMP	Simple Network Management Protocol. A protocol in the TCP/IP protocol suite that enables you to monitor a network from a single network management station called an SNMP Manager. From an SNMP Manager, you can make inquiries to another network device called the SNMP Agent. The SNMP Agent can be a TCP/IP host, router, terminal server, or another SNMP Manager. The information you can request from an SNMP Agent is contained in the MIB of that TCP/IP host. RFC 1066 (http://www.isi.edu/in-notes/rfc1066.txt) (Internet standard MIB) defines the types of objects that can be in an SNMP Agent MIB. These objects include network and hardware addresses, counters, and statistics, as well as routing and Address Resolution Protocol tables. Different vendors might not support all data types within their MIB or might include other information not defined within the RFC.
TCP	Transmission Control Protocol. This primary Internet transport protocol accepts messages of any length from an upper-layer protocol and provides full-duplex, acknowledged, connection-oriented, flow-controlled transport.
TELNET	Protocol in the TCP/IP suite that governs character-oriented terminal traffic.
TFTP	Trivial File Transfer Protocol. TCP/IP protocol commonly used for software downloads.
UDP	User Datagram Protocol. A protocol similar to TCP that provides connectionless, nonguaranteed transport services. UDP accepts and transports datagrams from an upper-layer protocol. Unburdened by the overhead of establishing and removing connections, controlling data flow, and performing other TCP functions, UDP usually provides a faster data conduit than TCP. For these reasons, and because it is easier to implement, UDP is the transport method of choice for many upper-layer protocols.

11 ZENWorks Management and Monitoring Services Database

ZENworks® for Servers (ZfS) provides a centralized Common Information Model (CIM)-compliant Sybase* database on the Management and Monitoring Services management server. The database serves as a repository for server and network data that can be displayed or formatted in various ways to provide you with exactly the information you need to manage your network.

The following sections provide information on understanding and using the ZENworks database:

- "Understanding the ZfS Database" on page 389
- "Backing Up the Database" on page 390
- "Changing Database Passwords" on page 391

Understanding the ZfS Database

The ZfS database consists of files located in the \ZENWORKS\MMS\DB directory on the management server. The ZfS data is stored in the following logical database:

- Topology/alarm database containing topology, alarms, and map information associated with the following files:
    - MW.DB
    - MW1.DB
    - MW2.DB
    - MW3.DB

  The MW.LOG file in the \ZENWORKS\MMS\DB subdirectory saves your transaction information with the database files.

Running the Database

The database is run using the MGMTDBS.NCF file (located in the \SYSTEM directory on a server volume), which is executed from AUTOEXEC.NCF.

IMPORTANT: Ensure that the database is running as long as the ZfS services are running.

Database Caching

Increasing the database cache improves the database performance. The default database cache size is 48 MB. You can increase the cache size to an optimum level depending on the server memory. To increase the cache size, modify the **-c** option in SYS:\SYSTEM\MGMTDBS.NCF. For example, **-c 64M** sets the cache size to 64 MB. Reload the database after modifying the cache size.

Backing Up the Database

You should plan to regularly back up the ZfS database:

- "Backing Up the Topology/Alarm Database" on page 390

Backing Up the Topology/Alarm Database

From ConsoleOne, follow this procedure to back up the topology/alarm database:

1. Right-click the Site Server object > select Properties.
2. Select the Database Administration tab.
3. Enter the path of the directory to back up.

   You can back up the database files to any volume on the management server only.
4. Click Apply.

   ZfS sends a remote SQL command to store the file. The four MW*.DB and MW.LOG files are copied to the backup directory.

Changing Database Passwords

ZfS allows you to access the topology/alarm database at three different levels: Administrator account, Updater account, and Reader account. You can set passwords for any of the three different user accounts.

From ConsoleOne, follow this procedure to modify the database passwords:

1. Right-click the Site Server object > select Properties.
2. Select the Change Database Passwords tab.
3. Enter the new passwords and confirm.
4. Click Apply.

   ZfS sends a remote SQL command to change the passwords of appropriate user objects in the database. The passwords are also stored in the Novell eDirectory

12 Using Reports in Management and Monitoring Services

The ZENworks® for Servers (ZfS) Management and Monitoring Services provide the following predefined reports:

- Topology Reports
- Alarm Reports
- Health Reports

The following sections describe the available reports and provide procedures for customizing and generating the reports:

- "Understanding Management and Monitoring Services Reports" on page 393
- "Managing Reporting" on page 401

Understanding Management and Monitoring Services Reports

The following sections describe each predefined report available in Management and Monitoring Services:

- "About the Topology Reports" on page 394
- "About the Alarm Reports" on page 397
- "About the Health Reports" on page 399

About the Topology Reports

The topology reports provide information about the topology of a selected ZfS site or segment. There are two types of topology reports you can generate: site-level reports and segment-level reports. The site-level reports provide details about the discovered devices on each segment in the ZfS site. The segment-level reports provide information about the discovered devices on the selected network segment.

Prior to generating the reports, you will need to perform a few operations. For more information see "Prerequisites for Generating the Reports" on page 394.

There are five predefined topology reports:

- "Computer Systems by Segment Report" on page 395
- "NCP Servers Report" on page 395
- "Router Report" on page 396
- "Segment Report" on page 396
- "Segment Topology Report" on page 396

The NCP Servers report is available only at the site level.

Prerequisites for Generating the Reports

Because Crystal Reports is invoked by DLLs on the system, you need to install the Sybase ODBC driver. To check if the driver is installed:

1 From the desktop Start menu, click Settings > Control Panel > ODBC Data Source.

1a In the System Data Source Name (DSN) pane click Add.

1b Select the Adaptive Server Anywhere driver. You must install Adaptive Server Anywhere if you do not have it on your system. You can install it from the SYBASE.ZIP file at COMPANIONCD\ODBC\SYBASE\*.*

2 If you have an older version of ZfS, you will need to uninstall it and install the latest version of ZfS before you can run the reports.

To uninstall the previous version:

2a From the desktop Start menu, click Settings > Control Panel > Add/Remove Programs.

2b Select ConsoleOne from the list and remove it.

If you have already installed the latest version, then delete the zenSnapins.jar file from CONSOLEONE\LIB\ZEN.

3 You will need at least MDAC 2.6 SP1 (Microsoft Data Access Component) for running Crystal Reports, particularly on a Windows NT machine. Check the version of MDAC on your box: select Control panel > ODBC Data sources > the About tab pane. The minimum version required is 3.520.7326.0. If the version you have does not match the minimum requirement, you need to upgrade the ODBC core components by downloading from Microsoft site (http://microsoft.com/data/download.htm).

Computer Systems by Segment Report

This report lists the number of computer systems on the selected segment. If the report is generated at the site level, the report lists the number of systems on each segment. For each segment, the report provides the following information about each connected computer system:

- Segment Name
- Segment Type
- Total nodes on a segment
- Node Name
- Node Address
- Services
- MIBs

NCP Servers Report

This report lists the following information for each server on the selected ZfS site:

- Server Name
- Total NCP servers on the site
- Server Label
- Server Address
- Labels (other names by which the server is known)
- MIBs

Router Report

This report provides the following information for each router on the selected ZfS segment or site:

- Total number of routers on the segment or site
- IPX Address
- Bound Segments
- Services
- MIBs
- IP Address
- MAC Address

Segment Report

This report lists the number of computer systems on the selected segment (segment level) or on all segments in the ZfS site (site level). For each segment, the report provides the following information about the systems connected to the segment:

- Segment Name
- Segment Type
- Total segments on the site
- IP configuration
- IPX configuration
- Total nodes on the segment

Segment Topology Report

This report provides information about the routers and bridges on a selected ZfS segment or site.

For each router, the report provides the following information:

- Router Name
- IP Address
- IPX Address
- MAC Address
- Bound Segment

For each bridge, the report provides the following information:

- Bridge Name
- Bridge Type
- Number of Ports
- Port: MAC Address and Bound Segment

About the Alarm Reports

The alarm reports provide information about the alarms received by the ZfS server. There are two types of alarm reports you can generate: Alarm details report and Alarm summary report.

Prerequisites for Generating the Reports

Because Crystal Reports is invoked by DLLs on the system, you need to install the Sybase ODBC driver. To check if the driver is installed:

1 From the desktop Start menu, click Settings > Control Panel > ODBC Data Source.

1a In the System Data Source Name (DSN) pane click Add.

1b Select the Adaptive Server Anywhere driver. You must install Adaptive Server Anywhere if you do not have it on your system. You can install it from the SYBASE.ZIP file at COMPANIONCD\ODBC\SYBASE\*.*

2 If you have an older version of ZfS, you will need to uninstall it and install the latest version of ZfS before you can run the reports.

To uninstall the previous version:

2a From the desktop Start menu, click Settings > Control Panel > Add/Remove Programs.

2b Select ConsoleOne from the list and remove it.

If you have already installed the latest version, then delete the zenSnapins.jar file from CONSOLEONE\LIB\ZEN.

3 You will need at least MDAC 2.6 SP1 (Microsoft Data Access Component) for running Crystal Reports, particularly on a Windows NT machine. Check the version of MDAC on your box: select Control panel > ODBC Data sources > the About tab. The minimum version required is 3.520.7326.0. If the version you have does not match the minimum requirement, you need to upgrade the ODBC core components by downloading from the Microsoft site (http://microsoft.com/data/download.htm).

Alarms Details Report

This report lists Information of the alarms on the site. The report is generated based on the customized settings. The report provides the following information about each connected computer system:

- Alarm Severity
- Affected object name
- Source address
- Alarm state
- Alarm category
- Alarm generator
- Alarm time
- Alarm owner
- Alarm type
- Alarm summary

Alarms Summary Report

This report generates a brief summary of the alarms on the site. It provides a graphical representation of the distribution of alarms, for the selected number of days. The report provides the following information about each connected computer system:

- Alarm Severity
- Alarm Category
- Alarm Owner
- Alarm state
- Top alarm types
- Top affected objects
- Top source address

About the Health Reports

The Health Reports provide information about the overall health of a specified ZfS site or network segment. Each health report is based on a predefined health profile. The health profiles define the trend parameters that are used to calculate the overall health of the segment or site. There are five predefined health profiles:

- "NetWare Server Profile" on page 399
- "Microsoft Windows Profile" on page 399
- "Ethernet Network Profile" on page 400
- "Token Ring Network Profile" on page 400
- "FDDI Network Profile" on page 400

In addition, you can modify any of the existing profiles or create your own health report profiles. See "Customizing a Health Profile" on page 402 or "Adding a New Health Profile" on page 403.

NetWare Server Profile

Reports generated using this profile provide graphs of the following trend parameters and use these parameters to calculate the overall health of the NetWare servers in the selected atlas, segment, or page:

- Cache Buffers
- Cache Hits
- CPU Utilization
- Volume Free Space

Microsoft Windows Profile

Reports generated using this profile use the following trend parameters to calculate health:

- Cache Hits
- CPU Utilization
- Disk Free Space
- Available Memory

In addition, reports generated using this profile contain trend graphs for the following parameter:

- Logged in Users

Ethernet Network Profile

Reports generated using this profile use the following trend parameters to calculate overall health:

- Total Errors
- Network Utilization

In addition, reports generated using this profile contain trend graphs for the following parameters:

- CRC error packets
- Undersized packets
- Oversized packets
- Fragmented packets
- Jabbers

Token Ring Network Profile

Reports generated using this profile use the following trend parameters to calculate overall health. In addition, reports generated using this profile contain also contain trend graphs for the following parameters:

- Network Utilization
- Total Errors

FDDI Network Profile

Reports generated using this profile use the following trend parameters to calculate overall health:

- Total Errors
- Network Utilization

In addition, reports generated using this profile contain trend graphs for the following parameters:

- CRC error packets

- Undersized packets
- Oversized packets
- Lost frame errors

Managing Reporting

The following sections provide procedures for customizing, generating, printing, and exporting the ZfS reports:

- "Managing the Topology Reports" on page 401
- "Managing the Server Management Health Reports" on page 402

Managing the Topology Reports

You can generate two types of topology reports: site-level reports and segment-level reports. The site-level reports provide details about the discovered devices on each segment in the ZfS site. The segment-level reports provide information about the managed devices on the selected network segment. Note that the NCP Servers report is available only at the site level.

The following section describes how to generate, print, and export a topology report.

Generating a Topology Report

To generate a topology report:

1. Select the ZfS site object (to generate a site-level report) or a network segment object (to generate a segment-level report) > click Reports.
2. Select the report you want to generate > click Run Selected Report.
3. To print the report, click File > Print.

   or

   To export the report, click File > Export.

Managing the Server Management Health Reports

The server management component provides five standard profiles that you can use to generate health reports. You can set up reports based on these standard profiles or you can customize these profiles or create your own profiles on which to base your reports. For information about the standard health profiles, see "About the Health Reports" on page 399.

This section contains the following tasks:

- "Customizing a Health Profile" on page 402
- "Adding a New Health Profile" on page 403
- "Creating and Scheduling Health Reports" on page 404
- "Viewing and Printing a Health Report" on page 405
- "Running a Health Report" on page 406
- "Calculating the Overall Health" on page 407

Customizing a Health Profile

To customize a health profile:

1. Right-click the ZfS site object > click Properties.
2. Select the Health Profiles tab.
3. Select the health profile you want to customize > click Edit.

   The Edit Profile dialog box is displayed. This dialog box contains a list of the parameters that can be used to calculate the overall health of the device or segment to which the profile is applied.
4. Specify the directory location to which reports generated using this profile should be published by entering a value in the Publish Directory field.

   To browse for a directory, click the Browse button (...).
5. Modify the parameters that are used to calculate health by checking or unchecking the In Health Calculation check box next to each parameter. For more information on the parameters that are used in health calculation see, "About the Health Reports" on page 399.
6. Rank the importance of each trend parameter in calculating health by entering a number in the Weight field for each parameter you checked to include in the health calculation.

You can enter any whole number in the Weight field. The system will use the weights to determine how important the parameter is in calculating overall health. The larger the number, the more weight the parameter is given in calculating health.

7. Modify which parameters to render graphically in the health report by checking or unchecking the Show Trend on Report check box next to each parameter.

8. To save your changes, click OK.

Adding a New Health Profile

To add a new health profile:

1. Right-click the ZfS site object > click Properties.

2. Select the Health Profiles tab.

3. Click New.

   The New Profile dialog box is displayed.

4. Enter a name for the new profile in the Name field.

5. Select the type of device or segment to which the profile applies from the Type drop-down list > click OK.

   The Edit Profile dialog box is displayed.

6. Specify the directory location to which reports generated using this profile should be published by entering a value in the Publish Directory field.

   To browse for a directory, click the Browse button (...).

7. Select the parameters you want to use to calculate health for reports generated using this profile by clicking the In Health Calculation check box next to the appropriate parameters. For more information on the parameters that are used in health calculation see, “About the Health Reports” on page 399.

8. For each parameter you selected to include in the health calculation, indicate how important the parameter is in calculating overall health by entering a value in the Weight column.

   You can enter any whole number in the Weight field. The system will use the weights to determine how important the parameter is in calculating overall health. The larger the number, the more weight the parameter is given in calculating health.

9 For each parameter that you want to be represented graphically in associated health reports, click the Show Trend on Report check box.

10 Click OK.

Creating and Scheduling Health Reports

To create and schedule a health report:

1 Right-click the ZfS site object or a container object > click Properties.

2 Select the Health Reports tab.

3 Click New.

The Edit Report dialog box is displayed.

4 Enter a name for the report in the Name field.

5 Select the profile to use when generating the report by selecting a value from the Profile drop-down list.

6 Indicate how often you want to generate the reports by selecting a value from the Period drop-down list.

You can choose to generate reports daily, weekly, or monthly.

7 Set the time and date you want the reports generated by selecting or entering the appropriate values in the Start Time, Day of the Week, and/or Day of the Month fields.

The available fields will depend on the period you selected.

8 Click OK.

The report will be generated at the date and time you entered and stored in the directory specified in the associated report profile. For information on viewing the reports, see "Viewing and Printing a Health Report" on page 405.

Editing, Scheduling, and Deleting Health Reports

To edit and schedule a health report:

1 Right-click the atlas, page, or segment > click Properties.

2 Select the Health Reports tab.

3 Click Edit.

The Edit Report dialog box is displayed. Edit the required information

4 Click OK.

IMPORTANT: If you want to edit the schedule time of the report, it is recommended that you create a new report with the changed schedule time or delete the report.

To delete a health report:

1 Right-click the atlas, segment, or page > click Properties.

2 Select the Health Reports tab.

3 Click Delete.

4 Click OK.

Viewing and Printing a Health Report

After you create a health report, the report will be automatically generated on the day and time you specified. You can view the reports using a Web browser to open the INDEX.HTM file in the directory that is designated as the publish directory in the associated report profile.

IMPORTANT: Before you can view the health reports you must install Java* plug-in 1.3.1_01. You can get this plug-in from Sun Microsystems, Inc.

To view a health report:

1 Browse to the directory where the health reports for the associated profile are stored.

2 Use your browser to open the INDEX.HTM file.

The INDEX.HTM file is a Java file containing all reports that are stored in the directory. The left column of the INDEX.HTM file lists report hierarchy.

3 Click the plus sign next to the profile that is associated with the reports you want to view.

The profile object expands to display a list of container objects.

4 Click the plus sign next to the container object associated with the reports you want to view.

The object expands to display a list of report names associated with the object.

5 Click the plus sign next to the report you want to view.

The object expands to display a list of individual report instances. For example, a report that is scheduled to run daily will have a report instance for each day. The reports are named by date and time. For example, 2000.09.09_11.15.10_PDT is the name assigned to a report generated on September 9, 2000 at 11:15:10 Pacific daylight time.

6 Click the plus sign next to the report name to display a list of individual report pages.

The number of individual report pages depends on what report profile you selected and the object where you generated the report. For example, if you generated a report at the segment level using the Ethernet Network profile, there will only be one report page for the segment. If you generated a report at the site level using the Ethernet Network profile, there will be a report page for each Ethernet segment within the site. If you generated a report at the segment level using the NetWare Server profile, there will be a separate report page for each NetWare server on the segment.

7 Click an individual report page to display the health report in the right frame.

The top of the report displays statistical information about the segment or server and provides a calculation of overall health. The parameters used to determine overall health are defined in the associated health report profile. The bottom of the profile displays trend graphs depicting the overall performance of the server or segment. See "About the Health Reports" on page 399 for a list of the parameters tracked and graphed in each of the standard profiles.

8 To print the report, click the Print Report button at the bottom of the left frame.

Running a Health Report

Although Health Reports are usually scheduled to run at a specified time of the day, week, or month, you may occasionally want to generate a Health Report on demand. To generate a Health Report on demand:

1 Right-click the atlas, segment, or page > click Properties.

2 Select the Health Reports tab.

3 Select the report you want to generate > click Now.

The report is saved to the directory specified in the report profile. See "Viewing and Printing a Health Report" on page 405.

Calculating the Overall Health

Overall health is calculated using the following parameters:

- Attributes selected for health calculation.
- Associated weights assigned to each attribute.

  You can only associate weights, which are used for health calculations.
- Values for each attribute

  Yellow threshold (YT), Red threshold (RT), and maximum value (maxValue).
- Global threshold values

  Global Green threshold (GG) is 100, Global Yellow threshold (GY) is 66, and Global Red threshold (GR) is 33.

Health Calculation

For each of the attribute used in overall health calculation, sample values based on the schedule specified while generating the reports are collected. These sample values are normalized using global thresholds and attribute thresholds, where Global Green is 100, Global Yellow is 66, and Global Red is 33. The global Green range = global Green - global Yellow; the global Yellow range = global Yellow - global Red; and the global Red range = global Red.

Normalization Formula

Normalized Value = Global Threshold - ((value - attribute Threshold))/(attribute Threshold Range) * (Global Range)

```
if (value > attribute's RED threshold)
    global Threshold = global Red
    attribute threshold = attribute Red threshold
    attribute threshold range = attribute maxValue - attribute Red threshold
    global Range = global Red range
if (value > attribute's Yellow threshold)
    global threshold = global Yellow
    attribute threshold = attribute Yellow threshold
    attribute threshold range = attribute Red - attribute Yellow
    global range = global Yellow range
if (value > 0)
    global threshold - ((value)) / (attribute threshold range) * (global range)
    global threshold = global Green
attribute threshold Range = attribute Yellow threshold
     global range = global Green range
```

Each of these may have an associated weight attached to it, which is configured in the respective profiles. Each of these attribute samples is then multiplied by the corresponding weights using the formula:

value = value * attributeWeight / TotalWeight;

where — value is the particular sample after normalization, attributeWeight is the weight associated with the attribute and the TotalWeight is the total weight of all the attributes used in health calculation.

The other values displayed in Health Reports are based on the following calculations:

- Minimum Value = minimum of all the values in a given sample
- Maximum Value = Maximum value of all the values in a given sample
- Average Value = Sum of all the Values / no of Samples
- Trend is calculated based on the Slope:

  $\text{Slope} = (n * \Sigma\, x * y - \Sigma\, x * \Sigma\, y) / (n * \Sigma\, x * x - \Sigma\, x * \Sigma\, x)$

  where   n = number of samples

  x = time at which these samples were captured

  y = trend values

  if Slope > 0, then the trend is increasing

  if Slope < 0, then the trend is decreasing

  if Slope = 0, then the trend is steady

- $\text{Intercept} = (\Sigma\, y - \text{Slope} * \Sigma\, x) / n$

- Next Week Projection or Next Month Projection Value = Slope * time + Intercept Where time = Report Schedule Time (time when the report was scheduled) + 7 * 24 * 60 * 60 * 1000 for weekly Projection
- Report Schedule Time (time when the report was scheduled) + 30 * 24 * 60 * 60 * 1000 for Monthly Projection.

WARNING: Exporting data in CSV (Comma Separated Value), Character Separated Value, and Tab SeparatedValue(TSV), does not export the complete data. As a workaround the you need to first export data in MS Excel format and then save it in the desired format.

If you export the generated reports in formats other than HTML or DHTML, the correct page numbers are not displayed. The page number is displayed incorrectly as Page -1 of 1, for all pages.

13 Using SNMP Community Strings

This chapter is referenced from the other sections. This section provides you information on SNMP, the SNMP community strings and how to configure SNMP community strings.

This section contains the following information:

- "About SNMP Community Strings" on page 411
- "Setting the SNMP Community Strings" on page 412

About SNMP Community Strings

SNMP is a protocol that offers network management services within the Internet suite of protocols.

SNMP uses a lightweight security mechanism whereby each protocol data unit (PDU) contains a community string. The SET community string is used in an SNMP Control operation and the GET community string is used in an SNMP Monitor operation.

SNMP community strings provide only a rudimentary form of security because they are transmitted in clear text in each SNMP request. Therefore, the community strings are exposed to any stations capable of monitoring an IP or Internetwork Packet Exchange™ (IPX™) network

Because Management Agent for NetWare and Management Agent for Windows are based on SNMP, all actions that are directed from network ConsoleOne to a server involve SNMP SET and GET requests from the manager to the agent. ConsoleOne® requests data from a managed server by issuing an SNMP GET request. An SNMP SET command is required to set server alarm thresholds or configuration parameters. In most cases, you are unaware of the underlying SNMP commands required to carry out requests you make from ConsoleOne, unless you are issuing requests on an SNMP-enabled device through the MIB Browser.

SNMP Security

Conducting management operations from ConsoleOne raises the issue of ensuring security. In particular, if unauthorized users configuration parameters on a server, severe performance problems or even sabotage network operations are encountered.

For these reasons, you should establish a scheme for changing the default community string PUBLIC to a proprietary community string used for communication between the management system and your SNMP agents.

Use the community keyword to define the community string to be used in the generated traps. The length of the community string is restricted to 32 bytes and cannot contain a space (except between quotes), tab, square bracket, equals sign, colon, semicolon, or number sign (#) characters. You can use Unicode* or International characters for the community string.

The default community string for Monitor operations is PUBLIC and for Control operations is null.

Setting the SNMP Community Strings

This section provides the following information:

- "Setting the SNMP Community String: NetWare Server" on page 412
- "Setting the SNMP Community String: ConsoleOne" on page 415
- "Setting Community Strings for an Individual Node" on page 416
- "Setting the SNMP Community String: Windows NT" on page 416

Setting the SNMP Community String: NetWare Server

You configure security access for SNMP communications using either SNMP LOAD command line parameters (NetWare 3*.x*/4*.x*/5*.x/6* servers) or through INETCFG (NetWare 4*.x*/5*.x/6* servers, or servers with NetWare MultiProtocol Router™ software installed).

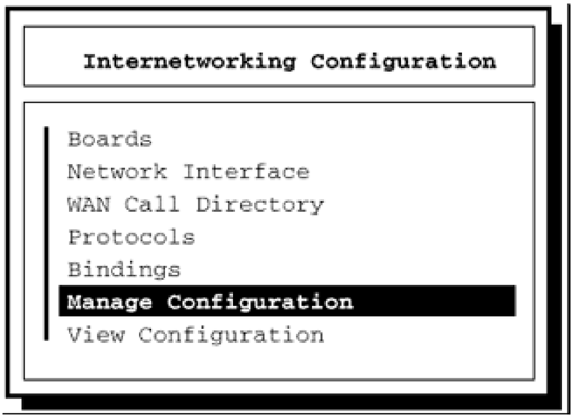
The following sections contain additional information to help you configure your NetWare servers:

- "Configuring Community String Options Using INETCFG" on page 413
- "Configuring Community String Options Using SNMP LOAD Commands" on page 414

Configuring Community String Options Using INETCFG

To configure the community string options using INETCFG:

1. At the server prompt, enter **`LOAD INETCFG`**.



2. From the Internetworking Configuration menu, click Manage Configuration > Configure SNMP Parameters > Monitor State.
3. Select one of the following options:

   These options let you indicate how SNMP handles SNMP read operations coming from outside this server.

Option	Description
Any Community May Read	Allows all GET (read) commands no matter what community string is provided in the incoming read request.
Leave as Default Setting	Avoids changing the Monitor community string from its default (which is usually PUBLIC). The default Monitor Community can still be changed manually through SNMP command line options, as described in "Configuring Community String Options Using SNMP LOAD Commands" on page 414.

Option	Description
No Community May Read	Allows GET (read) commands only for requests that are made by ConsoleOne that have logged in to the server with SUPERVISOR or OPERATOR privileges. Any community string provided in an incoming read request is ignored.
Specified Community May Read	Allows only GET (read) commands for requests that contain the name specified in the Monitor Community field. If you selected this option, type a name in the Monitor Community field, then press Enter. Enter the name of the community that is allowed to read management information. SNMP management stations that belong to this community can read the network management database.

4 Press Enter.

To change the Control community options, repeat Step 1 to Step 4 and choose the appropriate options for the community strings.

5 When you are finished, press Esc. If prompted, click Yes to save changes to the SNMP parameters > press Enter.

6 To return to the Internetworking Configuration menu, press Esc.

7 To exit INETCFG, press Esc.

8 Re-initialize the system.

To re-initialize, at the server prompt, enter **`reinitialize system`**.

Configuring Community String Options Using SNMP LOAD Commands

The LOAD command accepts the following SNMP option parameters:

- **MonitorCommunity:** Sets the community string for read-only (GET) access. The default value is PUBLIC. The syntax is as follows:

```
LOAD SNMP MonitorCommunity=community_name
```

- **ControlCommunity:** Sets the community string for read and write (GET and SET) access. By default, this community string is disabled.

The syntax is as follows:

```
LOAD SNMP ControlCommunity=community_name
```

These options set the community string for the indicated community. The following table shows examples of available settings:

IMPORTANT: Community strings are case-sensitive.

Access Available to Requester	Read Only	Read/Write
Community name: "secret"	Load SNMP MonitorCommunity= *secret* or LOAD SNMP ControlCommunity= *secret*	LOAD SNMP ControlCommunity= *secret*
Community name: "str1" or "str2"	Load SNMP MonitorCommunity= *str1* and LOAD SNMP ControlCommunity= *str2*	
Any community name	Load SNMP MonitorCommunity= “” or LOAD SNMP ControlCommunity=””"	LOAD SNMP ControlCommunity=""

Setting the SNMP Community String: ConsoleOne

You set global community and trap target information using the SNMP property page associated with the site-level object. You can also customize the setting for a specific device using the SNMP property page of the device itself.

Setting Community Strings for an Individual Node

This section describes the procedure to set up the community strings for SNMP SET and GET operations on an individual node.

Typically, community strings are configured to be identical over all nodes in a network, or at least over a portion of the network. The default value for both SET and GET is public. The community strings are case-sensitive.

By default, ZfS uses the public community string for SNMP GET and SET operations. You can configure a community string other than public on a node-by-node basis, or you can configure a community string globally on all SNMP-managed nodes. The community string that ZfS uses must match the string expected by the SNMP agent in the managed node; otherwise, the operation will fail.

To set up the community strings for SET and GET operations for an individual node:

1. From ConsoleOne, click the target SNMP-manageable node.
2. Right click the node > SNMP Settings.
3. Type the community string.

   ZfS uses this community string for SET and GET operations when communicating with the device.
4. Click OK.

Setting the SNMP Community String: Windows NT

You configure security access for SNMP communications on Windows NT servers using the Network applet in the Windows NT Control Panel. For detailed information, refer to your Windows NT documentation or online help.

You must load the Microsoft* SNMP Service on your Windows NT servers. The SNMP community string setting must be the same as the SNMP community string setting on your ConsoleOne.

14 Documentation Content Changes

This section contains information on documentation content changes that have been made for Management and Monitoring Services since the initial release of ZENworks® for Servers 3 (ZfS). The information will help you to keep current on changes to the documentation and, in some cases, the ZfS software (such as with a Service Pack release).

The information is grouped according to the date the documentation changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for Management and Monitoring.

The documentation is provided on the Web in two formats: HTML (standard Web help) and PDF. The Web help and PDF help are both kept up to date with the documentation changes listed in this section.

The documentation was updated on the following dates:

- "May 17, 2002" on page 417
- "September 27, 2002" on page 420
- "December 19, 2002" on page 420

May 17, 2002

Changes were made to the following sections:

- Using SNMP Community Strings
- Understanding Server Management
- Using the MIB Tools
- Understanding Traffic Analysis
- Protocol Decodes Suites Supported by ZfS

Using SNMP Community Strings

The following changes were made in this section:

Location	Change
Chapter 13, “Using SNMP Community Strings,” on page 411	This chapter was added. This chapter provides information about SNMP community strings, and how to configure the SNMP community strings on servers.

Understanding Server Management

The following changes were made in this section:

Location	Change
Chapter 5, “Understanding Server Management,” on page 155	Information on community strings, securing SNMP transaction, and defining community string for NetWare Management Agent have been removed and re-written in Chapter 13, “Using SNMP Community Strings,” on page 411.

Using the MIB Tools

The following changes were made in this section:

Location	Change
Chapter 6, “Using the MIB Tools,” on page 211	Information on setting community strings on an individual node, and the SNMP related information for working with MIB tools have been removed and re-written in Chapter 13, “Using SNMP Community Strings,” on page 411.
Chapter 6, “Using the MIB Tools,” on page 211	Two keywords HELP and HELPTAG have been added for the trap annotations.
Chapter 6, “Using the MIB Tools,” on page 211	Information on updating vendor MIBs and updating ZfS MIBs are removed.

Understanding Traffic Analysis

The following changes were made in this section:

Location	Change
Chapter 8, “Understanding Traffic Analysis,” on page 251	Information on configuring the SNMP parameters has been removed and re-written in Chapter 13, “Using SNMP Community Strings,” on page 411.

Protocol Decodes Suites Supported by ZfS

The following changes were made in this section:

Location	Change
Chapter 10, “Protocol Decodes Suites Supported by ZfS,” on page 377	The information for the NDS protocol under the NetWare Protocol Suite is changed.
Chapter 10, “Protocol Decodes Suites Supported by ZfS,” on page 377	In the AppleTalk Protocol Suite, the following protocols are deleted: ARI, RPC, SLP, SMTP, SNMP, TCP, TELNET, TFTP, UDP.
Chapter 10, “Protocol Decodes Suites Supported by ZfS,” on page 377	In the TCP/IP Protocol Suite, the following protocols are deleted: DIAG, NCP, RPC. These protocols are replaced with the following: IMAP, NFS, SSL.

September 27, 2002

The following changes were made in this section:

Location	Change
"Setting Up Discovery" on page 106	Added the following information about configuring the Consolidator to discover multiple IP addresses and a single MAC address connected to a more than one segment.
"Sending SMTP Mail Notification" on page 146	Following changes were made in this section: ◆ Changed the description of the `n` parameter. ◆ Added the following variable parameters: `p, h,` and *nnn*X.
"Launching an External Program" on page 148	Following changes were made in this section: ◆ Changed the description of the `n` parameter. ◆ Added the following variable parameters: `p, h,` and *nnn*X.

December 19, 2002

The following changes were made in this section:

Location	Change
"Configuring the Java Processes" on page 117	Added this new section on configuring Java processes in setting up Discovery.