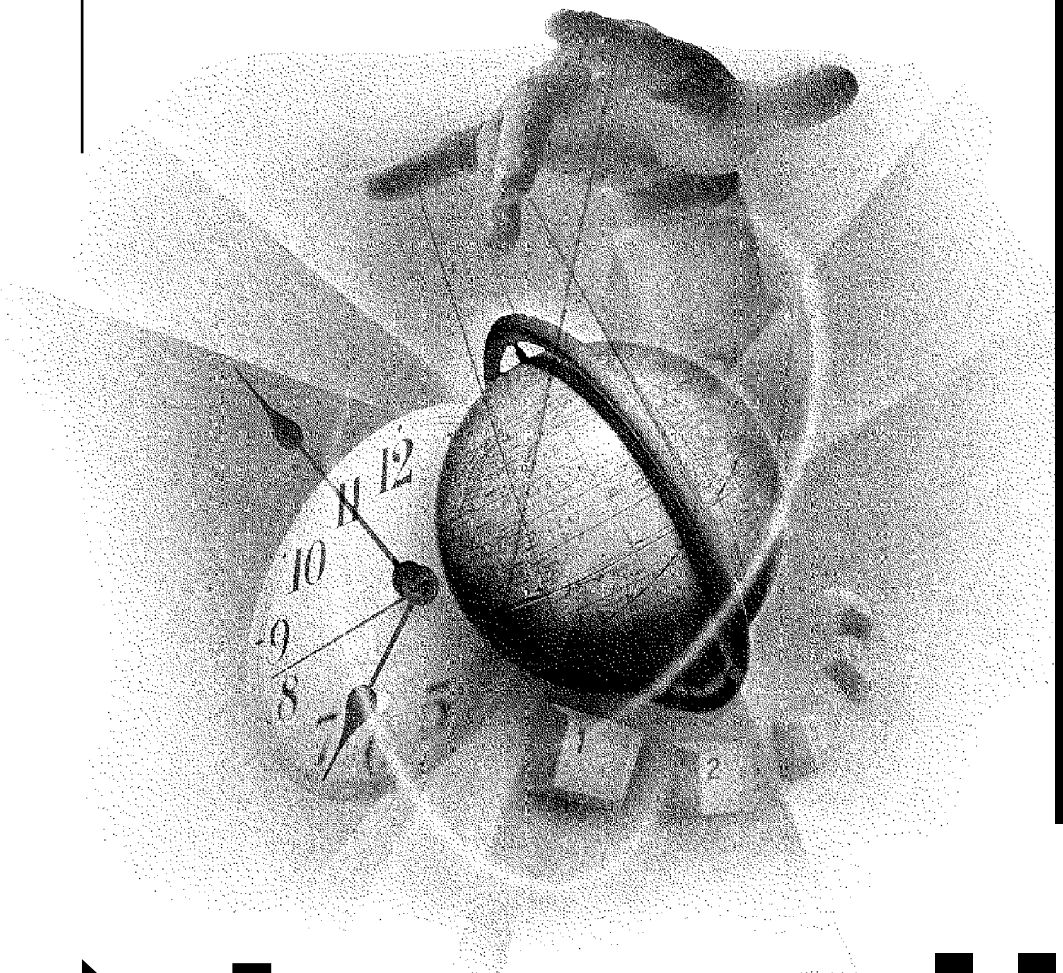
VERSION 1.0

ZENworks™ for Networks

Installation



Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

U.S. Patent No. 5,864,865; 5,910,803; 5,933,602; 5,963,938; 5,964,872; 5,983,234. Patents Pending.

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

www.novell.com

Installation
January 2000

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

ConsoleOne is a trademark of Novell, Inc.
Novell Client is a trademark of Novell, Inc.
ZENworks is a trademark of Novell, Inc.
NDS is a registered trademark of Novell, Inc.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide provides an overview of the components of ZENworks™ for Networks and instructions for installing each component.

1 Understanding ZENworks for Networks

This chapter describes ZENworks™ for Networks, its software components, and the Quality of Service (QoS) and configuration management solutions it offers. This chapter covers the following topics:

Quality of Service

Quality of Service (QoS) began as a cell-switching technology used with Asynchronous Transfer Mode (ATM). QoS has now broadened to include all performance specifications that an application requires from its underlying infrastructure, but its primary focus is still traffic management. The efficient use of bandwidth can significantly improve the performance of network devices and applications.

Some applications are better designed as best-effort services so that they can adapt to available bandwidth and network conditions. Other applications that have not been optimized can be extremely sensitive to delays or can produce large traffic bursts that affect other applications while providing users with little to no performance improvement. When viewed as a process, QoS consists of monitoring resources, controlling resources, and revising the

network infrastructure to better accommodate applications that are in high demand.

QoS enables diverse applications to request and receive predictable levels of service based on performance specifications for the following:

- Bandwidth
- Latency
- Latency variations
- Packet loss and failure

Bandwidth

Bandwidth, also known as throughput capacity, is defined as the available bit rate for a network device or transmission medium. Synchronous, interactive, or real-time applications that are bandwidth-sensitive can require a minimum guaranteed bandwidth at sustained or burst-scale bit rates. However, even though a certain bandwidth may be allocated for specific applications, the entire bandwidth may not necessarily be consumed at all times. Therefore, a good traffic management policy should enforce strict bandwidth allocations only when there is competition or demand for a limited shared resource.

For example, because push technologies usually require a lot of bandwidth, network administrators may want to use a traffic management policy to limit the allocation of bandwidth to these nonessential technologies when a mission-critical application needs additional bandwidth.

Latency

Latency is defined as the delay experienced by a packet being transmitted from a sender to a receiver. Applications that are considered delay-sensitive are real-time audio and video applications, Domain Name System (DNS), HTTP, and Telnet.

Latency is caused by a propagation of timing delays due to limitations of physical media and queueing at intermediate nodes such as routers, gateways, and servers. A certain percentage of the delay can be controlled by how the queues are serviced at the intermediate nodes and the control of congestion at known bottlenecks.

To control how intermediate nodes handle traffic, a traffic management policy can consider the following:

- Mean delay time

- Worst-case delay
- Packet round-trip delay
- Connection response time

Latency Variations

Latency variations, also known as jitter, measure an application's tolerance to delay that is not constant for all packets of a given flow. Real-time applications require a worst-case jitter. They often overcome latency variations by performing advanced packet buffering. A traffic management policy can control the amount of buffering for an application based on the expected latency variation or jitter associated with the application.

Packet Loss and Failure

Packet loss occurs when a router or server fails to forward or deliver packets and usually occurs during severe network congestion, when a router or server overloads, or when a router or server is down. Even if a packet has not been dropped, but has been simply delayed longer than expected, protocols and applications typically assume it was lost. Lost packets can cause application timeouts, loss of quality, and the retransmission of redundant packets.

To minimize packet loss and failure, a traffic management policy can consider the following:

- Rate of packet loss (packets per second) tolerated by an application
- Number of connection retries allowed
- Number of data retransmits allowed

Developing Quality of Service Performance Specifications

To develop meaningful and effective QoS performance specifications, consider the following:

- Type of business on the Internet—Are you running a business, such as an Internet Service Provider (ISP), that needs to develop a pricing model for the bandwidth allocated? Have you identified the business-critical services in your organization?
- Priority of clients, servers, or URLs accessed—Have you classified these as business-critical, casual, or personal?

- Properties of applications used—Have you classified your applications as high-bandwidth or low-bandwidth? Have you accounted for the types of files commonly downloaded by users?
- Traffic measurements—Have you monitored and analyzed your network traffic and the types of services being accessed?

After you have determined how applications use your network resources, you can use the following guidelines to develop your QoS performance specifications:

- Delay-sensitive, low-bandwidth applications, such as Telnet and DNS, are best controlled by assigning them a high priority.
- Delay-sensitive, high-bandwidth streaming multimedia applications, such as Vxtreme, are best controlled by assigning them a high priority with a limit on the number of sessions allowed to cap bandwidth use while still maintaining a reasonable quality per session.
- Delay-tolerant, bandwidth-tolerant applications, such as push technologies that download large files, are best controlled by assigning them a low priority and limiting the bandwidth they consume.
- Mission-critical applications, such as Lotus Notes*, Oracle* SQL*Net*, and the Lightweight Directory Access Protocol (LDAP), are best controlled by assigning them a high priority with a guaranteed bandwidth.
- Bulk-data, noninteractive applications, such as the Simple Mail Transfer Protocol (SMTP) and Network News Transfer Protocol (NNTP), should be guaranteed a small amount of bandwidth so they are not totally squeezed out by congestion or other control policies.
- Bulk-download, nominally interactive applications, such as FTP or some HTTP downloads, that have varying uses from critical to casual based on the file type accessed or the sender or receiver addresses, can be assigned a small minimum guaranteed bandwidth.
- Bulk-download applications with significant download traffic larger than 20 KB and burstiness are best controlled by only slightly limiting this traffic so the overall performance of the downloads is not impacted.

Adaptive Management of Bandwidth with Quality of Service

In general, QoS solutions can be classified as those that reserve bandwidth and those that prioritize bandwidth. Bandwidth reservation techniques allocate bandwidth based on flow parameters such as transport protocol, source address, source port, destination address, and destination port. Bandwidth prioritizing techniques rely on definitions of service class to allocate bandwidth.

QoS solutions adaptively manage bandwidth by implementing technologies or protocols to queue or discard packets, and to shape, prioritize, and reserve the bandwidth that is available. The following definitions are provided as a glossary and brief introduction to the technologies used in QoS solutions.

- *First-in, first-out (FIFO) queuing*—A technique used by network devices to buffer and handle packets in the order they are received so as to reduce network congestion.
- *Weighted fair queuing (WFQ)*—A technique that adds functionality to FIFO queuing by allowing network devices to monitor traffic and ensure that a single application does not monopolize the available bandwidth.
- *Random early discard (RED)*—A technique used by network devices in conjunction with queuing to randomly drop packets to reduce the rate at which packets are sent before buffers become full.
- *Class-based queuing (CBQ)*—A technique used by network devices to classify and queue packets based on the class criteria (prioritization) specified by an administrator.
- *Class-based fair queuing (CFQ)*—A technique that adds functionality to CBQ by allowing network devices to monitor traffic and ensure that a single application does not monopolize the available bandwidth.
- *Weighted random early discard (WRED)*—A technique that implements RED with classification criteria.
- *Bandwidth shaping*—A technique used to require network devices to reduce the rate at which they send packets by adjusting the TCP window size or delaying TCP acknowledgments.

Using Existing Quality of Service Methods

A number of QoS technologies have been implemented to address bandwidth management. Many of these solutions are suitable for LANs, and theoretically

apply to WAN and Internet links as well. Table 1 on page 14 summarizes some of the QoS technologies that have been designed to solve bandwidth allocation.

Table 1 Technologies to Solve QoS Challenges

Technology	Description	Advantages	Disadvantages
Asynchronous Transfer Mode (ATM)	Cell-switching technology designed for audio, video, and data	Small cells for excellent handling of audio and video Low latency Fine level of control	Requires custom applications Expensive to implement Can degrade performance of existing applications because of IP emulation Requires new hardware and software Slow acceptance in industry
Differentiated Services (DiffServ)	Proposed standard that uses IP header fields to specify how different traffic types are to be handled	Good solution for data traffic Most currently deployed network hardware enabled to handle DiffServ (or to approximate it using queuing and discarding techniques) Inexpensive	Rudimentary form of QoS based on business priorities Does not guarantee level of service, but instead gives preference to high-priority traffic

Technology	Description	Advantages	Disadvantages
Resource Reservation Protocol (RSVP)	Reservation and flow control standard	Handles bidirectional applications like audio and video	Requires custom applications Expensive to implement Can degrade performance of existing applications because of IP emulation Requires new hardware and software Slow acceptance in industry
Routers (and other link-level products)	Software and router upgrades offered to improve bandwidth guarantees and packet flow efficiencies	Positioned at Internet links to offer network-layer control	Does not handle inbound flow control well Does not offer application-level control Requires expensive software and proprietary hardware
Transport protocols (TCP/IP)	Pervasive technology in every Internet device	Included with every IP stack	TCP/IP flow is the source of problems at Internet access points Individual TCP/IP protocol stacks are largely unaware of other host processes

These QoS solutions, however, frequently involve end-to-end, “rip-and-replace” network modifications that are extremely difficult and expensive to implement on a universal scale. Additionally, interoperability between vendors cannot be guaranteed for these technologies. The greatest limitation of implementing these end-to-end QoS solutions in today’s networks is that they focus on very fine control of a small minority of applications, such as network-based telephony or videoconferencing. The majority of applications are not well served by these end-to-end solutions.

Using a Software-Based Quality of Service Method

Another QoS approach involves using a software-based gateway service to adaptively manage how bandwidth is allocated based on the type of business, service, user, time, congestion, and other meaningful criteria. Only a software-based gateway solution offers effective end-to-end control of Internet bandwidth with minimal cost and disruption to your network. A software-based QoS solution can provide this kind of control in a highly granular and flexible manner without the need for expensive hardware exchanges.

Granular control is expressed as a meaningful differentiation between various traffic flows to maximize the net benefit to an organization. Traffic flows can be differentiated as follows:

- Guaranteed—Guaranteed shares of a resource, such as a minimum bandwidth or a maximum latency.
- Best-effort—Allocation of a resource without regard to guarantees.
- Limited—Resource utilization or admission that is limited under certain conditions.
- Prioritized—Contention is resolved or a service is provided based on a priority scheme agreed upon by different entities.

The flexibility of a software-based approach results in the following benefits:

- The most valued (mission-critical) applications and users get faster and more reliable service.
- Less critical applications and users get an appropriate level of service.
- Available bandwidth is fairly shared between equally prioritized applications and users.
- Link efficiency improves because overall congestion is avoided.

Novell's ZENworks for Networks Quality of Service Solution

ZENworks for Networks is a Novell® QoS solution. It leverages NDS® to configure and manage switches, routers, and network traffic within a policy domain, a single administrative organization for creating, storing, and enforcing policies. It is an important part of Novell's Directory-Enabled Network (DEN) initiative as part of standardization efforts by the Distributed

Management Task Force (DMTF) and the Internet Engineering Task Force (IETF) to automate configuration management of devices.

With ZENworks for Networks, you can use business criteria to provide end-to-end QoS by allocating and prioritizing bandwidth on your network. For example, you can set a maximum bandwidth allocation for low-priority traffic, or you can set a minimum bandwidth allocation for traffic associated with mission-critical applications. Maximum and minimum allocations can also be assigned to users. You can also perform configuration management tasks on edge devices, such as routers that control traffic flow between networks.

ZENworks for Networks consists of policy servers and traffic management agents hosted on NetWare® servers or Windows NT* servers or workstations throughout management domains in your network. In addition, QoS policies are stored in NDS to enable enforcement of service levels. You configure and manage ZENworks for Networks from a Novell ConsoleOne™ network management console.

Components of ZENworks for Networks

The key software components of ZENworks for Networks include:

- Policy Server for NetWare and Policy Server for Windows NT server or workstation to enforce QoS policies.

  The Policy Server updates switch and router configuration parameters based on policy settings and schedules within a policy domain in NDS. Dynamic QoS policies are assigned to all or a selected number of switches and routers in a policy domain to provide an end-to-end solution. The Policy Server uses LDAP to read the policies stored in NDS.

- NDS schema extensions to configure properties for Policy Servers, QoS objects, Network Traffic Monitor Agents, and LDAP services.

  Bandwidth management schemas are stored as properties of policy objects in NDS to support directory-enabled management of switches and routers in your network. These policies define the way a specific traffic flow is managed throughout a policy domain.

- Network Traffic Monitor Agents for NetWare servers or Windows NT servers or workstations to monitor and report segment traffic.

  Network Traffic Monitor Agents provide real-time monitoring and report statistics for all traffic flows that have QoS policies assigned to them. They use LDAP to read the policies stored in NDS and measure and send QoS metrics back to the Policy Server to control traffic flow. A Network

Traffic Monitor Agent should be installed on each network segment in your network.

- ConsoleOne snap-ins for the configuration of devices managed by the ZENworks for Networks software.

  These provide an intuitive, easy-to-use administrative interface for setting up and managing policy domains and ZENworks for Networks object properties created in NDS.

NDS Schema Extensions for ZENworks for Networks

The open DMTF DEN standard is based on an object-oriented data model called the Common Information Model (CIM) which defines how managed devices are to be described in a directory structure. The DEN standard expands the device schemas defined by CIM to include policy schemas, network models, and CIM-to-LDAP mappings to use existing X.500 directories.

The NDS schema extensions for ZENworks for Networks define the classes of objects that can be created in your NDS tree and the object information that is required or optional when the objects are created. Each object associated with ZENworks for Networks in an NDS tree has a class and associated attributes defined for it in the tree's schema.

Classes of NDS objects include:

- Network Traffic Monitor Agents
- Policy Servers (domains)
- QoS policies

All NDS attribute names added by the ZENworks for Networks schema extension begin with den, cim, or ps (for Policy Server).

The following table summarizes the primary NDS objects that are added to NDS after the schema has been extended to support ZENworks for Networks.

NDS Object	Description
*servername*_POLICY	The Policy Server container object is named by appending _POLICY to the server's name. It defines the properties and policies for the Policy Server hosted on a NetWare server or a Windows NT server or workstation. This required container is automatically created during the software installation.
Nested Objects:	
QoSService	The QoSService object is used to administer ZENworks for Networks policies and is always created in a Policy Server container. This required object is automatically created during the software installation and is used to start the Network Policy Management Console.
JCMA	The Java Configuration Management Agent (JCMA) object represents a service required by the Policy Server. This required object resides in the Policy Server container and is automatically created during the software installation.
PolicySystem	The PolicySystem container holds Policy Server parameter settings and the policy and QoS device containers that store information about individual policies. This required container is automatically created during the software installation.

For instructions on how to perform specific tasks using these objects, refer to Setting Up Network Traffic Policies in the *Network Policy and Traffic Management Guide* and Managing Device Information in NDS in the *Network Management Configuration Guide*. For basic information about the types of objects in an NDS tree, access (http://www.novell.com/documentation/lg/nw/docui/index.html) and select Contents > Directory Services > NDS Concepts and Planning.

Using ZENworks for Networks

Some reasons to deploy ZENworks for Networks might be as follows:

- For an ISP—To manage inbound and outbound traffic on Internet links
- For a company providing Web hosting services—To manage inbound and outbound traffic between Web sites primarily containing multimedia and the Internet

- For a university or college that supports different LAN and WAN configurations that compete for bandwidth—To arbitrate bandwidth use among faculty and students
- For a large corporation with a private WAN connecting multiple LANs to its headquarters site—To allocate bandwidth between the competing remote sites
- For multiple types of networking companies—To enter into service level agreements (SLAs) with internal or external customers.

Using ZENworks for Networks for Traffic Management

In a typical network, network infrastructure management involves a cycle of continually monitoring the system, reporting on the system, and modifying the system to match network growth or changing needs. This cycle exists at various levels and time scales. A few examples of changes resulting from this process involve:

- Enforcing a QoS policy for a critical service
- Adding WAN bandwidth
- Segmenting the network
- Upgrading a router
- Choosing a guaranteed service level for your Web site
- Notifying a user to schedule large personal downloads at more prudent times

ZENworks for Networks has been designed to recognize and facilitate this entire process through monitoring, reporting, and actively controlling traffic.

The following are examples of some monitoring and control activities at various time scales:

- Second-to-second monitoring and control—Examples include ensuring that critical traffic gets the right-of-way during traffic bursts and enforcing bandwidth allocations. The affected entities are particular sessions in progress at a particular point. The changes are affected by a controlling device that is monitoring traffic.
- Day-to-day monitoring and control—Examples include managing time-of-day congestion and responding to intermittent problems or perceived problems. You may be dealing with problems that are very specific and

isolated to particular users or particular services at specific times that need to be tracked down quickly.

- Week-to-week monitoring and control—Examples include analyzing traffic usage and performance patterns, monitoring which services or hosts are active on your network, and troubleshooting chronic problems. You are looking at aggregates, such as a particular segment of your network, comparing Web sites, or comparing groups of users.
- Longer-term monitoring and control—Examples include implementing or changing organizational priorities, billing, providing adequate service for new applications as they are introduced, and capacity planning for network resources. You can also use network stress testing tools in conjunction with the Monitoring Agents to obtain a detailed analysis of flows and traffic behavior (with and without policy enforcement) before you deploy a change in your network infrastructure.

Using ZENworks for Networks for Traffic Control

ZENworks for Networks includes the Network Traffic Policy Management Console, a comprehensive, flexible, rule-based paradigm for implementing traffic control. Rules can be created for very specific groups of flows or for more general groups of flows. (Groups of flows are also referred to as traffic classes.) You can define classes by sender, receiver, application, file type, and URL.

Policies can be specified to control traffic flows in terms of overall bandwidth guarantees, bandwidth limits, priority of service, and how individual sessions within a class are serviced or admitted. The Network Policy Management Console has intelligent policy validation to prevent users from defining any contradictory or ambiguous rules.

Using ZENworks for Networks for Monitoring and Reporting

ZENworks for Networks offers an intuitive user interface for performance monitoring and profiling (accounting). Profiling is based upon active services, servers, clients, and users, and is started as soon as the infrastructure management software is installed. This provides accounting and service measurement on a variety of QoS measures.

ZENworks for Networks also provides congestion, utilization, and performance degradation reports. These reports make day-to-day troubleshooting much simpler and serve to justify or validate policy setting decisions. For example, a chronic problem affecting a particular service through the day can be monitored by a combination of real-time monitoring

and congestion reports. In this case, the finding may be that during link congestion, the affected service is not getting its due share, or it may be that the problem lies at the server or in the Internet backbone.

ZENworks for Networks also supports a comprehensive rule-based measurement and real-time monitoring capability for highly granular, time-critical monitoring. For example, problems may be diagnosed by setting up a rule for measuring the affected entities and tracking key measures using the ZENworks for Networks Real-Time Monitoring module. When deployed at a key access point, ZENworks for Networks can quickly monitor a problem area in the context of overall traffic.

2 Prerequisites for Installing ZENworks for Networks

This chapter specifies the prerequisites for installing ZENworks™ for Networks on a NetWare® 5 server or a Windows NT* 4.0 server or workstation, the system requirements for the Java*-based Novell Management Console, and the administrative requirements to configure and manage network devices after installation.

This chapter covers the following topics:

NetWare Server Prerequisites

The complete ZENworks for Networks installation extends the NDS® schema, installs the Policy Server, and installs the Network Traffic Monitor Agents on a single NetWare server. You can also select to install the Policy Server and Network Traffic Monitor Agents on different NetWare servers by performing a remote installation. Because you are not required to install all of the components on a single NetWare server, the requirements for each component are listed separately in this section.

Required Software and Services

ZENworks for Networks requires that some supporting NetWare services are running. Before you extend the NDS schema and install the Policy Server and

traffic monitoring agents, verify that your NetWare server meets the following requirements:

- ❑ A Pentium* or compatible 200-MHz or faster processor
- ❑ 128 MB of RAM
- ❑ 500-MB hard drive (with 100 MB of free disk space)
- ❑ NetWare 5 installed
- ❑ NetWare 5 Support Pack 3a or later installed
- ❑ Latest TCPIP.NLM installed
- ❑ Dedicated IP address assigned to server
- ❑ Lightweight Directory Access Protocol (LDAP) services installed

  For best performance, the LDAP server should reside in the same context as the Policy Server.

  For more information on configuring LDAP services on a NetWare 5 server, access the following URLs:

  - (http://www.novell.com/coolsolutions/nds/features/a_ldap.html)
  - (http://developer.novell.com/research/appnotes/1998/December/02/index.htm)

Policy Server Requirements

In addition to the requirements described in "Required Software and Services" on page 23, the NetWare server hosting the Policy Server must be running a Simple Network Management Protocol (SNMP) agent. If the SNMP agent is not running, the Policy Server will be unable to generate SNMP trap alerts.

Additionally, depending on your network configuration, one or more Ethernet or Token Ring network interface cards (NICs) should be installed.

Traffic Monitor Requirements

In addition to the requirements described in "Required Software and Services" on page 23, depending on your network configuration, one or more Ethernet or Token Ring NICs should be installed.

Windows NT Server or Workstation Prerequisites

ZENworks for Networks cannot be deployed in a pure Windows NT environment. At least one NetWare 5 server must be running to handle event monitoring and policy enforcement. You must have administrative access to the NetWare server to extend the NDS schema. Refer to "Required Software and Services" on page 23 for the NetWare 5 software requirements.

Because a remote installation allows you to install the Policy Server and Network Traffic Monitor Agents on different Windows NT servers or workstations, the requirements for each component are listed separately in this section.

Policy Server Requirements

Before you install the Policy Server, verify that your Windows NT server or workstation meets the following hardware and software requirements:

- A Pentium or compatible 200-MHz or faster processor
- 128 MB of RAM
- 500-MB hard drive (with 100 MB of free disk space)
- 128-MB page file size
- One or more Ethernet or Token Ring NICs installed

  SMC network interface cards are not supported. Refer to "Tested Network Interface Cards" on page 27 for a list of compatible network interface cards.
- Windows NT 4.0 server or workstation software installed
- Windows NT 4.0 Service Pack 5 or later installed
- TCP/IP installed
- Dedicated IP address assigned to Windows NT machine
- SNMP installed and running

  SNMP is required to support ZENworks for Networks SNMP alert notifications. You can install the SNMP agent from your Windows NT Server CD-ROM. If the SNMP agent is not installed, you will not be able to send SNMP trap alerts.
- Novell Client™ for Windows NT version 4.6 or later with Support Pack 2 installed

IMPORTANT: If you will also run the Java-based Novell Management Console on your Windows NT server instead of from a Windows 95*, Windows 98*, or Windows NT workstation, you will also need the ConsoleOne™ 1.2c software. The ConsoleOne 1.2c software is provided on the ZENworks for Networks Support CD-ROM.

Traffic Monitor Requirements

Before you install the traffic monitoring agents, verify that your Windows NT server or workstation meets the following hardware and software requirements:

- ❑ For a sustained traffic load of up to 40 Mbps at the LAN interface:
  - A Pentium or compatible 200-MHz or faster processor
  - 128 MB of RAM
  - 500-MB hard drive with 100 MB of free disk space (for extensive logging activity, increase the amount of free disk space)
  - 256-MB page file size (or twice the available RAM)
- ❑ For a sustained traffic load of more than 40 Mbps at the LAN interface:
  - A Pentium or compatible 400-MHz or faster processor
  - 128 MB of RAM
  - 500-MB hard drive with 100 MB of free disk space (for extensive logging activity, increase the amount of free disk space)
  - 256-MB page file size (or twice the available RAM)
- ❑ One or more Ethernet or Token Ring NICs installed

  SMC network interface cards are not supported. Refer to "Tested Network Interface Cards" on page 27 for a list of compatible network interface cards.
- ❑ Windows NT 4.0 installed
- ❑ Windows NT 4.0 Service Pack 5 or later installed
- ❑ TCP/IP installed
- ❑ Dedicated IP address assigned to server
- ❑ Novell Client for Windows NT version 4.6 or later with Support Pack 2 installed

IMPORTANT: If you will also run the Java-based Novell Management Console on your Windows NT server instead of from a Windows 95, Windows 98, or Windows NT

workstation, you will also need the ConsoleOne 1.2c software. The ConsoleOne 1.2c software is provided on the ZENworks for Networks Support CD-ROM.

Tested Network Interface Cards

The following network interface cards have been tested with the traffic monitoring agents running on a Windows NT server:

- 3Com* Fast EtherLink* XL PCI 10/100-MB adapter (3C905-TX)
- 3Com EtherLink III Parallel Tasking 16-bit 3C509B-COMBO
- Intel* EtherExpress* PRO/100 LAN adapter, Model B
- LINKSYS Ether 16 LAN Card, ISA, Model No. LNE2000
- EFA Corp. NE2000 Combo, InfoExpress PnP
- Vision Net RealTek RTL8029 PCI adapter
- LONG SHINE Shine Net, Model No. LCS-8634PTB
- DLink DFE 500 Tx
- Hewlett-Packard* HPJ2585B Desk Direct
- DEC* PCI Fast Ethernet DECchip 21140
- IBM* Combo 16/4 Token Ring adapter for ISA
- NX-32PCI adapter
- Compaq* NetFlex*–3/P PCI adapter
- NDC ND 4300 PCI Ethernet adapter
- PN102TX PCI Ethernet adapter

Network Policy Management and Network Configuration Requirements

You can run the Java snap-ins for network policy management and network configuration directly on a Windows NT server or workstation. However, if you installed the ZENworks for Networks components on NetWare 5 servers, or want a separate administrative workstation to administer the components installed on Windows NT machines, your administrative workstation must meet the following requirements:

- A Pentium or compatible 200-MHz or faster processor
- 128 MB of RAM

- 500-MB hard disk
- Windows 95, Windows 98, or Windows NT 4.0 with Service Pack 5 or later
- ConsoleOne 1.2c installed
- Novell Client version 4.6 or later for Windows 95, Windows 98, or Windows NT with Support Pack 2 installed

Administrative Requirements

Before installing the ZENworks for Networks software, ensure that the following administrative criteria are met:

- The NetWare 5 server from which you extend the NDS schema (to add the ZENworks for Networks extensions) has a local replica of the NDS Root partition.
- You have administrative (Admin) rights to the root of your NDS tree (to extend the schema).
- You have administrative (Admin) rights to the NetWare 5 servers providing LDAP services.
- If you plan to install components of ZENworks for Networks on NetWare 5 servers, you have administrative (Admin) rights to those servers.
- If you plan to install components of ZENworks for Networks on Windows NT 4.0 servers or workstations, you have administrative (Administrator) rights to those servers.
- If you plan to install components of ZENworks for Networks on a remote Windows NT 4.0 server or workstation, the Windows* machine from which you are performing the remote installation must be running the NETBEUI service.
- If you plan to install components of ZENworks for Networks on a remote Windows NT 4.0 server or workstation, you must create a shared folder on the remote server or workstation.

  For instructions on sharing a folder within a Windows workgroup, refer to the Microsoft* Windows NT Help.

3 Installing ZENworks for Networks

This chapter describes the tasks to install and start the ZENworks™ for Networks software. It covers the following topics:

IMPORTANT: Before you begin your installation, click Readme from the Installation Wizard menu for additional information.

Installing a Complete Policy Domain

A complete policy domain comprises the following components:

- Schema extension
- Policy Server
- Monitor Agent
- Management Console

The ZENworks for Networks Installation Wizard allows you to install a complete policy domain by installing these software components at one time. The advantage of installing a complete policy domain is that the installation program automatically extends the NDS® tree to support the administration of Quality of Service (QoS) policies and network device configurations, and installs the policy domain components in the correct sequence.

When you install a complete policy domain, you can also install the ZENworks for Networks Management Console. If you install the Management Console as part of a complete policy domain on a Windows NT* server or workstation, the Management Console is installed on the local Windows NT server or workstation by default. However, if you install a complete policy domain on a remote Windows NT server or workstation or on a NetWare® server, the Management Console is installed on the Windows* client from which you are running the Installation Wizard.

As an alternative to installing a complete policy domain, you can perform unbundled installations to install the individual software components one at a time. However, the unbundled installations are typically used to install software components on additional machines after the initial policy domain has been installed. For example, you can install additional Monitor Agents on NetWare servers or Windows NT servers or workstations and the Management Console on multiple Windows 95*, Windows 98*, or Windows NT workstations.

NOTE: It is possible to select to install only one component during a complete policy installation. Selecting one option from the list of four options available is simply equivalent to installing the software component using the unbundled installation procedure.

For the unbundled installation instructions, refer to "Installing Individual Policy Domain Components" on page 36.

IMPORTANT: If you choose to bypass a complete policy domain installation to install the components of ZENworks for Networks individually, you should perform the installations in the order that the unbundled procedures are presented.

For instructions on installing a complete policy domain, refer to:

- "Installing a Complete Policy Domain on a NetWare Server" on page 30
- "Installing a Complete Policy Domain on a Windows NT Server or Workstation" on page 33

Installing a Complete Policy Domain on a NetWare Server

NOTE: During a complete policy domain installation, Monitor Agent cannot be selected unless Monitor Agent is selected.

To extend the NDS schema, install the Policy Server and the Monitor Agent on a NetWare 5 server, and install the Management Console on your local Windows client, complete the following steps:

1. From a workstation running the Novell Client™ software, log in to NDS as Admin or a user with rights to [Root] to extend the NDS schema.

The primary NDS tree you are attached to must be the one for which you are extending the schema. To verify your primary tree, right-click Network Neighborhood and select NetWare Connections. An asterisk appears next to the primary tree. If you want to change the setting, select the target tree in the list, click Set Primary, and log in to NDS again.

To successfully extend the NDS schema, the server you are attached to must have a local replica of the Root partition.

You also need administrative rights to the Lightweight Directory Access Protocol (LDAP) Group object to install a Policy Server. With administrative rights to [Root], you should automatically have these rights when you log in.

2. Insert the ZENworks for Networks CD-ROM in your workstation's CD-ROM drive to display the installation menu.
3. From the available options, click Install Complete Policy Domain.
4. Click Next.
5. Read the license agreement and click Yes to proceed.
6. Select Monitor Agent and Management Console. (Schema Extension and Policy Server are already selected by default.)

   IMPORTANT: Monitor Agent is not an available option unless Policy Server has been selected. Select Management Console only if your Windows client already has ConsoleOne™ 1.2c installed. If it doesn't, exit the installation and install it from the ZENworks for Networks Support CD-ROM, or deselect Management Console before continuing to the next step.
7. Click Next.
8. Enter or browse for and select the path to the ZENworks for Networks license, or select Install License Later if you want the Policy Server to use an evaluation (trial) license.

   To install the license from a license diskette, accept the default path of A:\. If you select Install License Later, the evaluation license is activated. To install a valid license later using a separate license installation procedure, refer to "Installing a ZENworks for Networks License" on page 47.
9. Click Next.
10. Select the NDS tree whose schema is to be extended.
11. Browse for and select the LDAP Group object.

    A distinguished LDAP Group object name has the syntax LDAP Group - *server name.context*.

12 Browse for and select the Organization or Organizational Unit under which the Policy Server container will be created.

A distinguished Organizational Unit name has the syntax *Organizational Unit.context*.

13 Browse for and select a NetWare server on the same network segment as the Policy Server that will handle NDS events such as login and logout processes. This can be a different server than the one hosting the Policy Server.

A distinguished NetWare server name has the syntax *server name.context*.

14 Browse for and select a User object, such as Admin, and enter the password to log in to the NetWare server.

A distinguished User name has the syntax *username.context*.

15 Click Next.

16 Select NetWare for the Policy Server platform.

17 Browse for and select the NetWare server that will host the Policy Server.

A distinguished NetWare server name has the syntax *server name.context*.

18 Select NetWare for the Monitor Agent platform.

19 Browse for and select the NetWare server that will host the Monitor Agent.

A distinguished NetWare server name has the syntax *server name.context*.

20 Click Next.

21 If necessary, use the drop-down list to change the IP address of the NetWare server to host the Policy Server.

NOTE: The drop-down list contains all IP addresses bound to the server that were detected by the installation program. The address displayed may not be the server's primary IP address; it is merely the first address that was detected.

22 If necessary, use the drop-down list to change the IP address of the NetWare server to host the Monitor Agent.

NOTE: The drop-down list contains all IP addresses bound to the server that were detected by the installation program. The address displayed may not be the server's primary IP address; it is merely the first address that was detected.

23 Click Next.

24 When you see the message “Schema Extension Done,” click OK.

The Policy Server and Monitor Agent files will be copied to the NetWare server. The Management Console snap-ins will be copied to your local Windows client.The entire process may take several minutes.

25 Click Next to return to the installation menu.

26 Click Exit.

27 Restart the NetWare server.

During installation, commands are automatically added to AUTOEXEC.NCF to load the Policy Server and Monitor Agent modules.

Installing a Complete Policy Domain on a Windows NT Server or Workstation

NOTE: During a complete policy domain installation, Monitor Agent cannot be selected unless Monitor Agent is selected.

IMPORTANT: You can perform a local or remote installation when you install a complete policy domain on a Windows NT server or workstation. If you want to perform a remote installation from a Windows 95 or Windows 98 client, you must install the Microsoft Remote Registry Service on the client machine first. For instructions on how to install this service, access (http://support.microsoft.com/search/default.asp) and perform a keyword search on “How to Install Remote Administration Services.”

To extend the NDS schema, and install the Policy Server, Monitor Agent, and Management Console on a Windows NT 4.0 server, complete the following steps:

1 From a Windows NT server running the Novell Client software or a Windows client, log in to NDS as Admin or a user with rights to [Root] to extend the NDS schema.

The primary NDS tree you are attached to must be the one for which you are extending the schema. To verify your primary tree, right-click Network Neighborhood and select NetWare Connections. An asterisk appears next to the primary tree. If you want to change the setting, select the target tree in the list, click Set Primary, and log in to NDS again.

To successfully extend the NDS schema, the server you are attached to must have a local replica of the Root partition.

You also need administrative rights to the LDAP Group object to install a Policy Server. With administrative rights to [Root], you should automatically have these rights when you log in.

2. Insert the ZENworks for Networks CD-ROM in the CD-ROM drive to display the installation menu.
3. From the available options, click Install Complete Policy Domain.
4. Click Next.
5. Read the license agreement and click Yes to proceed.
6. Select Monitor Agent and Management Console. (Schema Extension and Policy Server are selected by default.)

   IMPORTANT: Monitor Agent is not an available option unless Policy Server has been selected. Select Management Console only if the Windows NT server or client already has ConsoleOne 1.2c installed. If it doesn't, exit the installation and install it from the ZENworks for Networks Support CD-ROM, or deselect Management Console before continuing to the next step.
7. Click Next.
8. Enter or browse for and select the path to the ZENworks for Networks license, or select Install License Later if you want the Policy Server to use an evaluation (trial) license.

   To install the license from a license diskette, accept the default path of A:\. If you select Install License Later, the evaluation license is activated. To install a valid license later using a separate license installation procedure, refer to "Installing a ZENworks for Networks License" on page 47.
9. Click Next.
10. Select the NDS tree whose schema is to be extended.
11. Browse for and select the LDAP Group object.

    A distinguished LDAP Group object name has the syntax LDAP Group - *server name.context*.
12. Browse for and select the Organization or Organizational Unit under which the Policy Server container will be created.

    A distinguished Organizational Unit name has the syntax *Organizational Unit.context*.
13. Browse for and select a NetWare server on the same network segment as the Policy Server that will handle NDS events such as login and logout processes. This can be a different server than the one hosting the Policy Server.

NOTE: Although you are installing a complete policy domain on a Windows NT server, a NetWare server is still required for NDS event handling.

A distinguished NetWare server name has the syntax *server name.context*.

14 Browse for and select a User object, such as Admin, and enter the password to log in to the NetWare server.

A distinguished User name has the syntax *username.context*.

15 Click Next.

16 Select NT for the Policy Server platform.

17 Select Local (for installation on the local server or workstation) or Remote (for installation on a remote server or workstation).

18 If you selected Remote in Step 17, browse for and select the Windows NT server or workstation shared folder to install the Policy Server.

19 Select NT for the Monitor Agent platform.

20 Select Local (for installation on the local server or workstation) or Remote (for installation on a remote server or workstation).

21 If you selected Remote in Step 20, browse for and select the Windows NT server or workstation shared folder to install the Monitor Agent.

22 Click Next.

23 If necessary, use the drop-down list to change the IP address of the Windows NT server to host the Policy Server.

NOTE: The drop-down list contains all IP addresses bound to the server that were detected by the installation program. The address displayed may not be the server's primary IP address; it is merely the first address that was detected.

24 If necessary, modify the default destination directory.

If you selected a local installation, the default destination directory is Zen_Policy, and the default drive is the Windows NT installed drive. If you selected a remote installation, the default destination directory is Zen_Policy in the Windows NT server or workstation shared folder.

25 If necessary, use the drop-down list to change the IP address of the Windows NT server to host the Monitor Agent.

NOTE: The drop-down list contains all IP addresses bound to the server that were detected by the installation program. The address displayed may not be the server's primary IP address; it is merely the first address that was detected.

26 If necessary, modify the default destination directory.

If you selected a local installation, the default destination directory is MON_AGENT, and the default drive is the Windows NT installed drive. If you selected a remote installation, the default destination directory is MON_AGENT in the Windows NT server or workstation shared folder.

27 Click Next.

28 When you see the message “Schema Extension Done,” click OK.

The Policy Server and Monitor Agent files will be copied to the Windows NT server or workstation you specified. The Management Console snap-ins will be copied to the local Windows NT machine from which you are performing the installation. The entire process may take several minutes.

29 If you selected to install the Monitor Agent on a local Windows NT server or workstation in Step 20, click Finish and click Yes when prompted to reboot the server.

30 If you selected to install the Monitor Agent on a remote Windows NT server or workstation in Step 20, click Next. You must reboot the remote Windows NT server or workstation manually in Step 33.

31 Click Exit.

32 Start the Novell Policy Server by selecting Programs > ZENworks for Networks > Novell Policy Server from the Start menu of the Windows NT server or workstation hosting the Policy Server.

IMPORTANT: Do not change the Policy Server startup setting from Manual to Automatic because this does not start the Java*-based NDS Configuration Management Agent which is required to start before the Policy Server starts.

33 Reboot the Windows NT server or workstation hosting the Monitor Agent.

Because the Monitor Agent startup setting is Automatic, the Monitor Agent service automatically starts each time the server is rebooted.

Installing Individual Policy Domain Components

The primary convenience of using the complete policy domain installation option is that the installation program installs the components in the correct sequence. Typically, the unbundled installations are used to install software components on additional machines after an initial policy domain has already been installed.

However, if you choose to bypass the complete policy domain installation to install each policy domain component separately, adhere to these guidelines:

- The NDS schema must be extended before a Policy Server or Monitor Agent can be installed.
- Do not install a Monitor Agent unless a Policy Server has already been installed. Always install the Policy Server first.

This section describes the following unbundled installation procedures you can use to install the components of ZENworks for Networks individually, rather than as part of a complete policy domain installation:

- "Extending the NDS Schema" on page 37
- "Installing a Policy Server" on page 38
- "Installing a Monitor Agent" on page 42
- "Installing the Management Console" on page 46

Extending the NDS Schema

NDS schema extensions are required to support the administration of QoS policies and network device configurations. An NDS tree needs to be extended only once.

NOTE: If you already extended the schema as part of the installation of a complete policy domain, you may skip this procedure.

If you want to extend the NDS schema without installing a Policy Server or a Monitor Agent, do not select to install a complete policy domain. Instead, select the unbundled installation option by completing the following steps:

1. From a workstation running the Novell Client software, log in to NDS as Admin or a user with rights to [Root].

   The primary NDS tree you are attached to must be the one for which you are extending the schema. To verify your primary tree, right-click Network Neighborhood and select NetWare Connections. An asterisk appears next to the primary tree. If you want to change the setting, select the target tree in the list, click Set Primary, and log in to NDS again.

   To successfully extend the NDS schema, the server you are attached to must also have a local replica of the Root partition.

2. Insert the ZENworks for Networks CD-ROM in your workstation's CD-ROM drive to display the installation menu.
3. From the available options, click Extend Schema.

4. Click Next.
5. Select the NDS tree whose schema is to be extended.
6. Browse for and select the LDAP Group object.

   A distinguished LDAP Group object name has the syntax LDAP Group - *server name.context*.
7. Click Next to add the schema extensions and create the LDAP-to-NDS mappings.
8. When you see the message “Schema Extension Done,” click OK.
9. Click Finish to return to the installation menu.
10. Click Exit.

Installing a Policy Server

A Policy Server updates switch and router configuration parameters based on policy settings and schedules within a policy domain. Only one Policy Server is required per policy domain.

IMPORTANT: Before you install a Policy Server, make sure that the NDS schema has already been extended to include the extensions for ZENworks for Networks. Additionally, the Simple Network Management Protocol (SNMP) is required to support ZENworks for Networks SNMP alert notifications. If an SNMP agent is not installed, you will receive a warning message. If you choose to continue the Policy Server installation without SNMP support, the Policy Server’s ability to send SNMP alerts will be disabled until an SNMP agent is installed on the server. If you configure an SNMP agent on a Windows NT server after a Policy Server has been installed, refer to “Changing a Windows NT Registry for SNMP” on page 51 for additional instructions.

Refer to the procedure corresponding to the platform on which you are installing the Policy Server:

- “Installing a Policy Server on a NetWare Server” on page 39
- “Installing a Policy Server on a Windows NT Server or Workstation” on page 40

Installing a Policy Server on a NetWare Server

If you want to install a Policy Server on a NetWare 5 server, but do not want to install any other components, do not select to install a complete policy domain. Instead, complete the following steps:

1. Log in to NDS as Admin or a user with administrative rights to the LDAP Group object. You must also have administrative rights to the NetWare server on which you will install the Policy Server.
2. Insert the ZENworks for Networks CD-ROM in your workstation's CD-ROM drive to display the installation menu.
3. From the available options, click Install Policy Server.
4. Click Next.
5. Read the license agreement and click Yes to proceed.
6. Enter or browse for and select the path to the ZENworks for Networks license, or select Install License Later if you want the Policy Server to use an evaluation (trial) license.

   To install the license from a license diskette, accept the default path of A:\. If you select Install License Later, the evaluation license is activated. To install a valid license later using a separate license installation procedure, refer to "Installing a ZENworks for Networks License" on page 47.
7. Click Next.
8. Select the tree name containing the LDAP Group object.
9. Browse for and select the LDAP Group object.

   A distinguished LDAP Group object name has the syntax LDAP Group - *server name.context*.

   IMPORTANT: The same LDAP Group object has to be specified during Monitor Agent installation.
10. Browse for and select the Organization or Organizational Unit under which the Policy Server will be created.

    A distinguished Organizational Unit name has the syntax *Organizational Unit.context*.
11. Browse for and select a NetWare server on the same network segment as the Policy Server that will handle NDS events such as login and logout processes. This can be a different server than the one hosting the Policy Server.

A distinguished NetWare server name has the syntax *server name.context*.

12 Browse for and select a User object, such as Admin, and enter the password to log in to the NetWare server.

A distinguished User name has the syntax *username.context*.

13 Click Next.

14 Select NetWare for the Policy Server platform.

15 Browse for and select the NetWare server that will host the Policy Server.

A distinguished NetWare server name has the syntax *server name.context*.

16 Click Next.

17 If necessary, use the drop-down list to change the IP address of the NetWare server to host the Policy Server.

NOTE: The drop-down list contains all IP addresses bound to the server that were detected by the installation program. The address displayed may not be the server's primary IP address; it is merely the first address that was detected.

18 Click Next to install the Policy Server object in NDS and copy files to the server.

19 Click Finish to return to the installation menu.

20 Click Exit.

21 Restart the NetWare server. (During installation, a command is automatically added to AUTOEXEC.NCF to load the Policy Server each time the server is started.)

Installing a Policy Server on a Windows NT Server or Workstation

If you want to install a Policy Server on a Windows NT 4.0 server or workstation, but do not want to install any other components, do not select to install a complete policy domain. Instead, complete the following steps:

1 Log in to NDS as Admin or a user with administrative rights to the LDAP Group object.

2 To display the installation menu, insert the ZENworks for Networks CD-ROM in the Windows CD-ROM drive.

3 From the available options, click Install Policy Server.

4 Click Next.

5. Read the license agreement and click Yes to proceed.

6. Enter or browse for and select the path to the ZENworks for Networks license, or select Install License Later if you want the Policy Server to use an evaluation (trial) license.

   To install the license from a license diskette, accept the default path of A:\. If you select Install License Later, the evaluation license is activated. To install a valid license later using a separate license installation procedure, refer to "Installing a ZENworks for Networks License" on page 47.

7. Click Next.

8. Select the tree name containing the LDAP Group object.

9. Browse for and select the LDAP Group object.

   A distinguished LDAP Group object name has the syntax LDAP Group - *server name.context*.

   IMPORTANT: The same LDAP Group object has to be specified during Monitor Agent installation.

10. Browse for and select the Organization or Organizational Unit under which the Policy Server container will be created.

    A distinguished Organizational Unit name has the syntax *Organizational Unit.context*.

11. Browse for and select a NetWare server on the same network segment as the Policy Server that will handle NDS events such as login and logout processes.

    A distinguished NetWare server name has the syntax *server name.context*.

    NOTE: Although you are installing a Policy Server on a Windows NT server or workstation, the NetWare server is still required for NDS event handling.

12. Browse for and select a User object, such as Admin, and enter the password to log in to the NetWare server.

    A distinguished User name has the syntax *username.context*.

13. Click Next.

14. Select NT for the Policy Server platform.

15. Select Local (for installation on the local Windows NT server or workstation) or Remote (for installation on another Windows NT server or workstation).

16 If you selected Remote in Step 15, browse for and select the Windows NT server or workstation shared folder to install the Policy Server.

17 If necessary, modify the default destination directory.

If you selected a local installation, the default destination directory is Zen_Policy, and the default drive is the Windows NT installed drive. If you selected a remote installation, the default destination directory is Zen_Policy in the Windows NT server or workstation shared folder.

18 Click Next.

19 If necessary, use the drop-down list to change the IP address of the Windows NT server to host the Policy Server.

NOTE: The drop-down list contains all IP addresses bound to the server that were detected by the installation program. The address displayed may not be the server's primary IP address; it is merely the first address that was detected.

20 Click Next to install the Policy Server object in NDS and copy files to the server.

21 Click Finish to return to the installation menu.

22 Click Exit.

23 From the Windows NT server or workstation hosting the Policy Server, start the Novell Policy Server by selecting Programs > ZENworks for Networks > Novell Policy Server from the Windows Start menu.

This starts the Java-based NDS Configuration Management Agent and the Policy Server.

24 Verify that the startup setting for the Novell Policy Server is Manual by selecting Settings > Control Panel > Services from the Windows Start menu.

IMPORTANT: Do not change the Policy Server startup setting from Manual to Automatic because this does not start the Java-based NDS Configuration Management Agent which is required to start before the Policy Server starts.

Installing a Monitor Agent

Traffic Monitoring Agents report traffic statistics for all traffic flows that have policies assigned to them. An agent should be installed on each network segment on your network.

IMPORTANT: Before you install the traffic monitoring software, make sure that the NDS schema has already been extended to include the extensions for ZENworks for Networks. Further, because it requires the use of an NDS object created when a Policy

Server is installed, the traffic monitoring software should be installed only if a Policy Server already exists.

Refer to the procedure corresponding to the platform on which you are installing the traffic monitoring software:

- "Installing a Monitor Agent on a NetWare Server" on page 43
- "Installing a Monitor Agent on a Windows NT Server or Workstation" on page 44

Installing a Monitor Agent on a NetWare Server

If you want to install a Monitor Agent on a NetWare 5 server, but do not want to install any other components, do not select to install a complete policy domain. Instead, complete the following steps:

1. Log in to NDS as Admin or a user with administrative rights to the LDAP Group object. You must also have administrative rights to the NetWare server on which you will install the traffic monitoring software.
2. Insert the ZENworks for Networks CD-ROM in your workstation's CD-ROM drive to display the installation menu.
3. From the available options, click Install Monitor Agent.
4. Click Next.
5. Read the license agreement and Click Yes to proceed.
6. Select the tree name containing the LDAP Group object.
7. Browse for and select the LDAP Group object.

   A distinguished LDAP Group object name has the syntax LDAP Group - *server name*.*context*.

   IMPORTANT: The same LDAP Group object has to be specified during Policy Server installation.
8. Browse for and select the QosService object name.

   The QosService object is created when the Policy Server component is installed and is located in the Policy Server container. A distinguished QosService object name has the syntax QosService.*server name*_POLICY.*context*.
9. Browse for and select a NetWare server on the same network segment as the Policy Server that will handle NDS events such as login and logout

processes. This can be a different server than the one hosting the Monitor Agent.

A distinguished NetWare server name has the syntax *server name.context*.

10 Browse for and select a User object, such as Admin, and enter the password to log in to the NetWare server.

A distinguished User name has the syntax *username.context*.

11 Click Next.

12 Select NetWare for the Monitor Agent platform.

13 Browse for and select the NetWare server that will host the Monitor Agent.

A distinguished NetWare server name has the syntax *server name.context*.

14 Click Next.

15 If necessary, use the drop-down list to change the IP address of the NetWare server to host the Monitor Agent.

NOTE: The drop-down list contains all IP addresses bound to the server that were detected by the installation program. The address displayed may not be the server's primary IP address; it is merely the first address that was detected.

16 Click Next to create the Monitor object in NDS and copy the necessary files to the server.

17 Click Finish to return to the installation menu.

18 Click Exit.

19 Restart the NetWare server. (During installation, a command is automatically added to AUTOEXEC.NCF to load the Monitor Agent each time the server is started.)

Installing a Monitor Agent on a Windows NT Server or Workstation

If you want to install a Monitor Agent on a Windows NT 4.0 server or workstation, but do not want to install any other components, do not select to install a complete policy domain. Instead, complete the following steps:

1 Log in to NDS as Admin or a user with administrative rights to the LDAP Group object.

2. To display the installation menu, insert the ZENworks for Networks CD-ROM in the Windows CD-ROM drive.
3. From the available options, click Install Monitor Agent.
4. Click Next.
5. Read the license agreement and Click Yes to proceed.
6. Select the tree name containing the LDAP Group object.
7. Browse for and select the LDAP Group object.

   A distinguished LDAP Group object name has the syntax LDAP Group - *server name.context*.

   IMPORTANT: The same LDAP Group object has to be specified during Policy Server installation.
8. Browse for and select the QosService object name.

   The QosService object is created when the Policy Server component is installed and is located in the Policy Server container. A distinguished QosService object name has the syntax QosService.*server name*_POLICY.*context*.
9. Browse for and select a NetWare server on the same network segment as the Monitor Agent that will handle NDS events such as login and logout processes.

   A distinguished NetWare server name has the syntax *server name.context*.

   NOTE: Although you are installing a Monitor Agent on a Windows NT server or workstation, the NetWare server is still required for NDS event handling.
10. Browse for and select a User object, such as Admin, and enter the password to log in to the NetWare server.

    A distinguished User name has the syntax *username.context*.
11. Click Next.
12. Select NT for the Monitor Agent platform.
13. Select Local (for installation on the local Windows NT server or workstation) or Remote (for installation on another Windows NT server or workstation).
14. If you selected Remote in Step 13, browse for and select the Windows NT server or workstation shared folder to install the Monitor Agent.

15 If necessary, modify the default destination directory.

If you selected a local installation, the default destination directory is MON_AGENT, and the default drive is the Windows NT installed drive. If you selected a remote installation, the default destination directory is MON_AGENT in the Windows NT server or workstation shared folder

16 Click Next.

17 If necessary, use the drop-down list to change the IP address of the Windows NT server or workstation to host the Monitor Agent.

NOTE: The drop-down list contains all IP addresses bound to the server that were detected by the installation program. The address displayed may not be the server's primary IP address; it is merely the first address that was detected.

18 Click Next to create the Monitor object in NDS and copy the necessary files to the server.

19 If you selected to install the Monitor Agent on a local Windows NT server or workstation in Step 13, click Finish and click Yes when prompted to reboot the server.

20 If you selected to install the Monitor Agent on a remote Windows NT server or workstation in Step 13, click Next. You must reboot the remote Windows NT server or workstation manually in Step 22.

21 Click Exit.

22 Reboot the Windows NT server or workstation.

The Monitor Agent startup setting is Automatic so the Monitor Agent service will automatically start each time the server is rebooted.

Installing the Management Console

The Management Console for ZENworks for Networks allows you to administer policies and router configurations from your Windows 95, Windows 98, or Windows NT 4.0 desktop. This procedure installs the Java snap-ins required to administer ZENworks for Networks using ConsoleOne.

IMPORTANT: Proceed with the Management Console installation only if your Windows machine already has ConsoleOne 1.2c installed. If it doesn't, you should install it from the ZENworks for Networks Support CD-ROM before continuing.

You can install the Management Console on a Windows NT server or on a Windows workstation. To install the Management Console, complete the following steps:

1. Insert the ZENworks for Networks CD-ROM in the CD-ROM drive to display the installation menu.
2. From the available options, click Install Management Console.
3. Click Next to copy the files.
4. Click Finish to return to the installation menu.
5. Click Exit.

NOTE: You do not need to reboot your workstation or Windows NT server after copying the files. You can run ConsoleOne immediately after the installation of the ZENworks for Networks snap-ins.

Installing a ZENworks for Networks License

To effectively use ZENworks for Networks software, you must install a valid Policy Server license. The ZENworks for Networks software includes an evaluation (trial) Policy Server license that expires 90 days after you install it. To activate the evaluation license when you install a Policy Server, select the Install License Later option. Refer to Step 8 on page 31, Step 8 on page 34, Step 6 on page 39, or Step 6 on page 41 in the procedure you are using.

If you are unsure whether the license you are using is an evaluation license or a valid license with no expiration, do the following:

1. Log in as Admin or a user with administrative rights to the Policy Server container.
2. Insert the ZENworks for Networks CD-ROM in the CD-ROM drive to display the installation menu.
3. From the available options, click License.
4. Click View.
5. Select the NDS tree where the Policy Server is installed.

   NOTE: Only the NDS trees you are authenticated to are displayed in the drop-down list.
6. Browse for and select the QosService object.

   The QosService object is created when the Policy Server component is installed and is located in the Policy Server container. A distinguished

QosService object name has the syntax QosService.*server name*_POLICY.*context*.

7. Click View License Information to display information about the license the Policy Server is currently using.

   The license information will display the number of licensed users. For example, for a 25-user license, it displays:

   License = 25 users

   For an MLA license, it displays:

   License = unlimited users

8. Click Finish to return to the installation menu.

9. Click Exit.

If your evaluation license has expired, you can install a valid license by completing the following steps:

1. Log in as Admin or a user with administrative rights to the Policy Server container.

2. Insert the ZENworks for Networks CD-ROM in the CD-ROM drive to display the installation menu.

3. From the available options, click License.

4. Click Install.

5. Select the NDS tree where the Policy Server is installed.

   NOTE: Only the NDS trees you are authenticated to are displayed in the drop-down list.

6. Browse for and select the QosService object.

   The QosService object is created when the Policy Server component is installed and is located in the Policy Server container. A distinguished QosService object name has the syntax QosService.*server name*_POLICY.*context*.

7. Enter or browse for and select the path to the license, or accept the default path of A:\ to install the license from a license diskette.

8. Click Next > Finish > Exit.

Using the ZENworks for Networks Administrative Utilities

The ZENworks for Networks installation menu includes a Utilities option. Utilities are provided to make the administration of ZENworks for Networks easier under the following conditions:

- The password for the user specified during a policy domain installation was changed in NDS.

  For more information about this condition, refer to "Changing an Administrator Password for a Policy Server" on page 49.

- A Policy Server was installed on a Windows NT server or workstation that did not have an SNMP agent installed and running.

  For more information about this condition, refer to "Changing a Windows NT Registry for SNMP" on page 51.

Changing an Administrator Password for a Policy Server

When you install a policy domain, you specify a username and password to log in to NDS and create the Policy Server container. If you subsequently change this user's password in NDS, you must update the Policy Server with the new password by completing the following steps:

1. Log in as the user whose password has been updated in NDS.
2. Insert the ZENworks for Networks CD-ROM in the CD-ROM drive to display the installation menu.
3. From the available options, click Utilities.
4. Click Change Administrator Password.
5. Click Policy Server.
6. Select the NDS tree containing the Policy Server.

   NOTE: Only the NDS trees you are authenticated to are displayed in the drop-down list.

7. Browse for and select the user whose password has been updated in NDS.
8. Enter the new password for the user.
9. Click Next.
10. Select NT or NetWare for the Policy Server platform. If you select NetWare, skip to Step 12.

11 Select Local (for installation on the local Windows NT server or workstation) or Remote (for installation on another Windows NT server or workstation). If you select Local, skip to Step 13.

12 Browse for and select the NetWare server or Windows NT server or workstation that hosts the Policy Server.

13 Browse for and select the NetWare server the Policy Server uses to handle NDS events.

14 Click Next > Back > Back > Exit.

Changing an Administrator Password for a Monitor Agent

When you install a Monitor Agent, you specify a username and password to log in to NDS and create the Monitor Agent container. If you subsequently change this user's password in NDS, you must update the Monitor Agent with the new password by completing the following steps:

1 Log in as the user whose password has been updated in NDS.

2 Insert the ZENworks for Networks CD-ROM in the CD-ROM drive to display the installation menu.

3 From the available options, click Utilities.

4 Click Change Administrator Password.

5 Click Monitor Agent.

6 Select the NDStree containing the Monitor Agent object.

NOTE: Only the NDS trees you are authenticated to are displayed in the drop-down list.

7 Browse for and select the user whose password has been updated in NDS.

8 Enter the new password for the user.

9 Click Next.

10 Select NT or NetWare for the Monitor Agent platform. If you select NetWare, skip to Step 12.

11 Select Local (for installation on the local Windows NT server or workstation) or Remote (for installation on another Windows NT server or workstation). If you select Local, skip to Step 13.

12 Browse for and select the NetWare server or Windows NT server or workstation that hosts the Monitor Agent.

13 Click Next > Back > Exit.

Changing a Windows NT Registry for SNMP

It is recommended that you install a Policy Server on a Windows NT server or workstation only if SNMP is already installed and running. A warning message is displayed when you install a Policy Server on a Windows NT server or workstation that is not running an SNMP agent. If you choose to continue the Policy Server installation without SNMP support, the Policy Server's ability to send SNMP alerts is disabled until an SNMP agent is installed on the server or workstation.

If you configure an SNMP agent on a Windows NT server or workstation *after* installing a Policy Server, you must add entries to the Windows NT registry to support SNMP by completing the following steps:

1. Log in as Admin or a user with administrative rights to the Windows NT server.
2. Insert the ZENworks for Networks CD-ROM in the CD-ROM drive to display the installation menu.
3. From the available options, click Utilities.
4. Click NT Registry Changes for SNMP.
5. Select Local (if the Policy Server is hosted on the local Windows NT server or workstation) or Remote (if the Policy Server is hosted on another Windows NT server or workstation).
6. If you selected Remote in Step 5, browse for and select the Windows NT server or workstation hosting the Policy Server.
7. Click Next > Back > Exit.

Uninstalling ZENworks for Networks

The ZENworks for Networks installation menu includes options for uninstalling the software. Because of NDS object dependencies, the uninstall procedures should be performed in the following order:

- "Uninstalling a Monitor Agent" on page 52
- "Uninstalling a Policy Server" on page 52
- "Removing NDS Schema Extensions" on page 53

Uninstalling a Monitor Agent

Uninstalling a Monitor Agent from a server:

- Uninstalls the Novell Monitor Agent
- Deletes Monitor Agent registry entries (Windows NT servers or workstations only)
- Deletes Monitor Agent files
- Deletes the Monitor Agent object from NDS

To uninstall a Monitor Agent, complete the following steps:

1. Insert the ZENworks for Networks CD-ROM in the CD-ROM drive to display the installation menu.
2. From the available options, click Uninstallation.
3. Click Uninstall Monitor Agent.
4. Select NT or NetWare for the Monitor Agent platform. If you select NetWare, skip to Step 6.
5. Select Local (for installation on the local server or workstation) or Remote (for installation on another server). If you select Step 7.
6. Browse for and select the NetWare server that hosts the Monitor Agent or a shared folder on the Windows NT server or workstation that hosts the Monitor Agent. (The shared folder need not be the same folder used to install the Monitor Agent.)
7. Click Next > Finish > Back > Exit.

Uninstalling a Policy Server

WARNING: Uninstall Monitor Agents linked to a particular Policy Server object before uninstalling that Policy Server.

Uninstalling a Policy Server from a server:

- Uninstalls the Novell Policy Server
- Deletes Policy Server registry entries (Windows NT servers or workstations only)
- Deletes Policy Server files
- Deletes the Policy Server object from NDS

To uninstall a Policy Server, complete the following steps:

1. Insert the ZENworks for Networks CD-ROM in the CD-ROM drive to display the installation menu.
2. From the available options, click Uninstallation.
3. Click Uninstall Policy Server.
4. Select NT or NetWare for the Policy Server platform. If you select NetWare, skip to Step 6.
5. Select Local (for installation on the local server or workstation) or Remote (for installation on another server). If you select Local, skip to Step 7.
6. Browse for and select the NetWare server that hosts the Policy Server or a shared folder on the Windows NT server or workstation that hosts the Policy Server. (The shared folder need not be the same folder used to install the Policy Server.)
7. Click Next > Finish > Back > Exit.

Removing NDS Schema Extensions

WARNING: Uninstall Monitor Agents and the Policy Server before removing the NDS schema extensions.

NOTE: Removing NDS schema extensions also deletes the LDAP-to-NDS mappings used by the Policy Server and Monitor Agent software.

To remove the schema extensions, complete the following steps:

1. Insert the ZENworks for Networks CD-ROM in the workstation's CD-ROM drive to display the installation menu.
2. From the available options, click Uninstallation.
3. Click Remove Schema.
4. Select the NDS tree whose schema is to be removed.
5. Enter the distinguished name of the LDAP Group, or browse for and select the LDAP Group object.

   A distinguished LDAP Group object name has the syntax LDAP Group - *server name.context*.
6. Click Next to remove the LDAP-to-NDS mappings and the schema extensions.
7. When you see the message "Remove Schema Ended," click OK.
8. Click Finish > Back > Exit.

Documentation for Management Tasks

After you install the necessary components of ZENworks for Networks, you can create and manage network policies, monitor network traffic, and configure and manage routers and other edge devices on your network. In addition to this installation guide, two additional ZENworks for Networks guides are provided:

- *Network Policy and Traffic Management*

  For information on creating traffic policies, refer to "Setting Up Network Traffic Policies."

  For information on monitoring network traffic, refer to "Monitoring Network Traffic."

- *Network Configuration Management*

  For information on router configuration management, refer to "Managing Device Information in NDS."