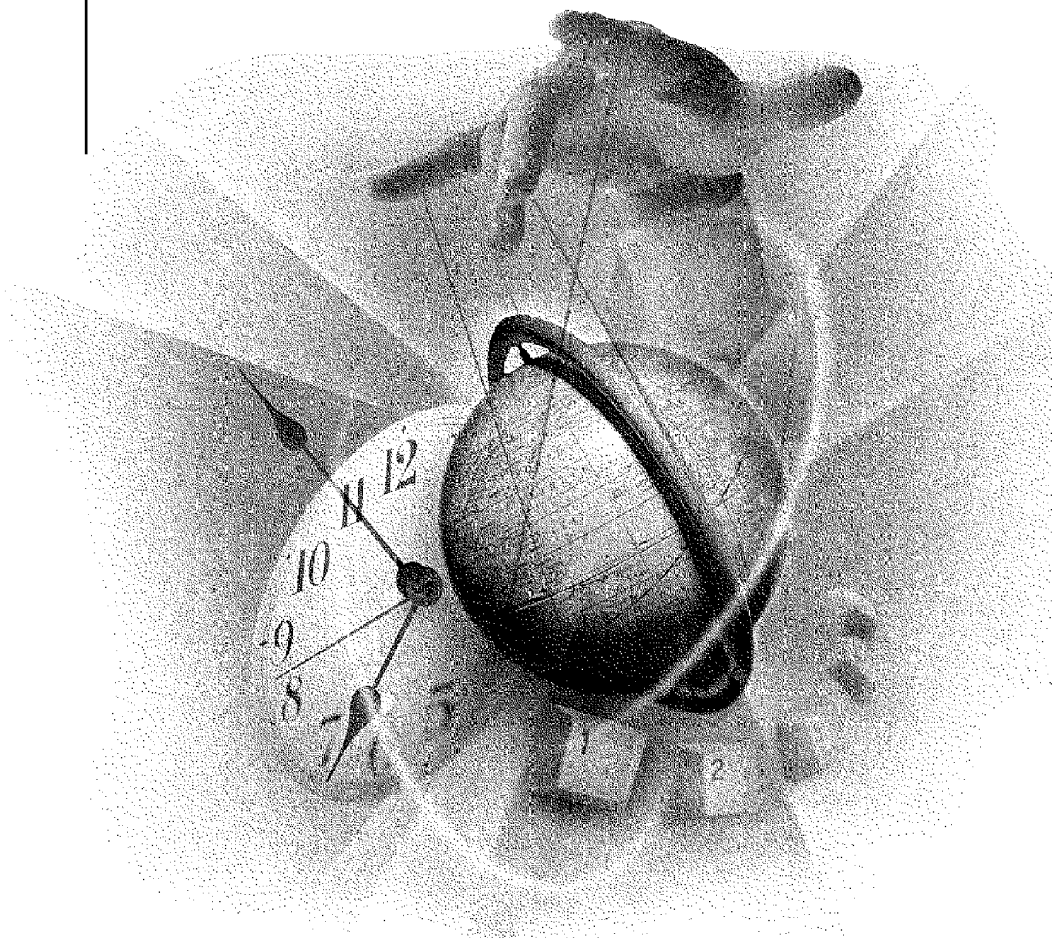


VERSION 1.0

Network Configuration Management



ZENworks™ for Networks

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.

Copyright © 1993-2000 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

Network Configuration Management
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.

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

1 Understanding Device Management

Benefits of Directory-Enabled Management of Devices	9
Device Objects for ZENworks for Networks	10
QoSDeviceContainer	10
QoSDevice	11
QoSInterface	11
QoSInterfaceGroup	11
Port Used for Interapplication Communication	11

2 Managing Device Information in NDS

Running Auto Discovery	13
Creating Device Objects in NDS	14
Creating New Devices	14
Creating New Interfaces	15
Creating New Groups	16
Viewing and Modifying Device Objects in NDS	17
Viewing and Modifying Device Properties	17
Viewing and Modifying Interface Properties	18
Viewing and Modifying Group Properties	19
Viewing Monitor Properties	20
Changing IP Addresses Assigned to Interfaces	21
Managing Routers	21
Importing Router Configurations	21
Updating Router Configurations	22
Rebooting Routers	22

About This Guide

This guide describes how to import router configurations into NDS[®], download router configurations to devices, and restart devices using the Configuration Management Agent (CMA).

1

Understanding Device Management

This chapter describes the built-in capability of ZENworks™ for Networks to remotely manage routers and other edge devices on your network using NDS®. This chapter contains the following sections:

- ♦ “Benefits of Directory-Enabled Management of Devices” on page 9
- ♦ “Device Objects for ZENworks for Networks” on page 10
- ♦ “Port Used for Interapplication Communication” on page 11

Benefits of Directory-Enabled Management of Devices

Configuration and management of network hardware devices, such as routers and switches, is typically performed manually by network administrators on a device-by-device basis.

The complexities of configuring and managing these devices in an enterprise environment include the following:

- ♦ The use of multiple proprietary hardware interface programs or Telnet to configure devices
- ♦ The inability of individual devices to share configuration information
- ♦ The use of different administrator accounts and passwords per managed device
- ♦ The use of decentralized backup systems for the configuration of each device

ZENworks for Networks provides a scheme for managing network hardware devices based on the Distributed Management Task Force (DMTF) Common Information Model (CIM) and Directory-Enabled Network (DEN) specifications.

ZENworks for Networks makes the management of network devices easier by providing the following benefits to administrators:

- ◆ NDS—A secure, centralized, and fault-tolerant directory in which to store all device configurations.
- ◆ A Java*-based Configuration Management Agent (CMA) to communicate with NDS through the Lightweight Directory Access Protocol (LDAP) to retrieve configurations for network devices.
- ◆ The ability to separate and delegate specific responsibilities for device management based on NDS group and user rights and logins.
- ◆ The ability to share configuration information between network devices.
- ◆ The ability to remotely configure devices and download these configurations to other devices.
- ◆ The ability to view the status of devices remotely and reboot them, if necessary.

Device Objects for ZENworks for Networks

During the installation of ZENworks for Networks, several NDS objects are automatically created to support device management. This section provides a brief overview of the following objects:

- ◆ [“QoSDeviceContainer” on page 10](#)
- ◆ [“QoSDevice” on page 11](#)
- ◆ [“QoSInterface” on page 11](#)
- ◆ [“QoSInterfaceGroup” on page 11](#)

For information about creating devices and using these objects to manage devices, refer to [Chapter 2, “Managing Device Information in NDS,” on page 13](#).

QoSDeviceContainer

The QoSDeviceContainer object resides in the PolicySystem container which is nested under the Policy Server object (*servername_POLICY*). The QoSDeviceContainer object holds the following additional containers:

- ◆ QoSDevice
- ◆ QoSInterface
- ◆ QoSInterfaceGroup

QoSDevice

The QoSDevice container stores objects representing individual network hardware devices and servers running software monitoring agents. Each device or monitoring agent must have a unique name. The properties of these objects enable you to do the following:

- ◆ Import the current configuration of a device into NDS
- ◆ Update the device with a new configuration configured in NDS
- ◆ Reboot the device

QoSInterface

The QoSInterface container stores objects representing individual interfaces. For example, a single network hardware device, such as a router, can have several interfaces.

Protocols bound to these interfaces are shown as objects nested under the interface object. For example, if TCP/IP is bound to the interface, a TCPIP object appears.

QoSInterfaceGroup

The QoSInterfaceGroup container stores objects representing smart groups. Smart groups are groups of devices that you can create to facilitate administration when multiple devices share the same configuration or network policy rules.

Port Used for Interapplication Communication

For the network configuration management functionality, the Configuration Management Engine uses port 8000 for interapplication communication. The Java Configuration Management Engine listens on this port for import/update/reboot router events. These events are sent by the Configuration Management device snap-in.

2

Managing Device Information in NDS

This chapter describes how to use the Quality of Service (QoS) objects in NDS[®] to configure and manage your network hardware devices that are QoS-enabled. If you run Auto Discovery from the ZENworks[™] for Networks Console, the software automatically populates the QoSDevice container with device objects representing the devices it discovered.

This chapter contains the following sections:

- ◆ [“Running Auto Discovery” on page 13](#)
- ◆ [“Creating Device Objects in NDS” on page 14](#)
- ◆ [“Viewing and Modifying Device Objects in NDS” on page 17](#)
- ◆ [“Changing IP Addresses Assigned to Interfaces” on page 21](#)
- ◆ [“Managing Routers” on page 21](#)

Running Auto Discovery

The Auto Discovery module launched from the ZENworks for Networks Console automatically discovers the network devices in your network and populates NDS with the appropriate objects representing these devices.

IMPORTANT: For Auto Discovery, devices on each network segment must be running a Simple Network Management Protocol (SNMP) service to be discovered.

To run Auto Discovery, complete the following steps:

- 1** Run ConsoleOne[™].
- 2** Under the Policy Server container, highlight the QoSService object.
- 3** Right-click and select Views > ZENworks for Networks.
- 4** Click Auto Discovery.

Creating Device Objects in NDS

If you add a new device to your network, you can immediately create an object for it in NDS instead of running Auto Discovery. This section describes how to perform the following tasks in NDS:

- ◆ “Creating New Devices” on page 14
- ◆ “Creating New Interfaces” on page 15
- ◆ “Creating New Groups” on page 16

Creating New Devices

You can create a device object for a router or a switch. You cannot create a device object for a monitor.

To manually create a device object, complete the following steps from the ZENworks for Networks Console:

- 1** Right-click the Devices folder and select Device.
The options in the Device tab are displayed.
- 2** Enter a unique name for the device.
- 3** Enter the device model number.
- 4** Enter the software version the device runs.
- 5** From the drop-down list, select the vendor name, or select Other Vendor and enter the name of the vendor.
- 6** Enter the primary IP address of the device.
- 7** Click the Capabilities tab.
- 8** Select the QoS capabilities that the device supports.
 - ◆ Weighted Fair Queueing—A technique used to monitor traffic and ensure that a device does not monopolize the available bandwidth.
 - ◆ Priority Queueing—A technique used to assign priority to traffic classes so that the most critical traffic is routed first.
 - ◆ Rate Limit—A technique used to reduce the rate at which packets are sent from a device.
- 9** Select the classification capabilities that apply to the device.
 - ◆ Layer 2—The device can filter packets at network Layer 2.
 - ◆ Static IP Filter—The device can filter IP packets.
 - ◆ Static Filter—The device can filter packets other than IP.

- 10** Enter a Login password and an Enable password.

The Login password enables you to log in to (establish a connection to) the device. The Enable password enables you to update the configuration of the device.

- 11** Click Apply, or click OK to apply the changes and close the dialog box.

Creating New Interfaces

An interface object represents one of a possible number of interfaces in a network device. For example, a router can have multiple interfaces that route traffic to different network segments.

To manually create an interface object for a device, complete the following steps from the ZENworks for Networks Console:

- 1** Right-click the device object and select Interface.
The options in the Interface tab are displayed.
- 2** Enter a unique name for the interface.
- 3** Enter the IP address for the interface.
- 4** Enter the subnet mask for the interface.
- 5** Enter the interface number (if the device has multiple interfaces).
- 6** Enter the interface speed in Kbps.
- 7** Check the Primary IP Address check box if this interface is to be the primary IP address.
- 8** From the drop-down list, select the media type, such as Ethernet, or select Other and enter the media type.
- 9** Click the Capabilities tab.
- 10** Select the QoS capabilities that the interface supports.
 - ◆ Weighted Fair Queueing—A technique used to monitor traffic and ensure that a device does not monopolize the available bandwidth.
 - ◆ Priority Queueing—A technique used to assign priority to traffic classes so that the most critical traffic is routed first.
 - ◆ Rate Limit—A technique used to reduce the rate at which packets are sent from a device.

- 11** Select the classification capabilities that apply to the interface.
 - ◆ Layer 2—The device can filter packets at network Layer 2.
 - ◆ Static IP Filter—The device can filter IP packets.
 - ◆ Static Filter—The device can filter packets other than IP.
- 12** Click Apply, or click OK to apply the changes and close the dialog box.

Creating New Groups

Smart groups are groups of existing devices that share common configuration parameters or common policy rules. Similar to how User Group objects in NDS simplify the management of access rules, the creation of smart groups significantly decreases the number of configurations and policy rules you are required to manage.

To create a new smart group from the ZENworks for Networks Console, complete the following steps:

- 1** Right-click the Groups folder and select Smart Group.

The options in the Smart Group tab are displayed.
- 2** Enter a unique name for the smart group.
- 3** Enter the start and stop IP addresses representing the address range for the devices in the smart group.
- 4** Check the Enable check box to enable the smart group.
- 5** Click the Vendors tab.
- 6** Select the vendors corresponding to the devices in the smart group. If a check box for a vendor is not provided, select Other and enter the name of the vendor.
- 7** Click the Interface Types tab.
- 8** Select the types of interfaces in the smart group.
- 9** Click the Capabilities tab.
- 10** Select the QoS capabilities the smart group supports.
 - ◆ Weighted Fair Queueing—A technique used to monitor traffic and ensure that a device does not monopolize the available bandwidth.
 - ◆ Priority Queueing—A technique used to assign priority to traffic classes so that the most critical traffic is routed first.
 - ◆ Rate Limit—A technique used to reduce the rate at which packets are sent from a device.

- 11** Select the classification capabilities that apply to the smart group.
 - ◆ Layer 2—The device can filter packets at network Layer 2.
 - ◆ Static IP Filter—The device can filter IP packets.
 - ◆ Static Filter—The device can filter packets other than IP.
- 12** To add a list of interfaces to a smart group, do the following:
 - 12a** Right-click the smart group object and select Modify.

A dialog displays the list of available interfaces and the list of selected interfaces.
 - 12b** Select the interfaces to be added to the smart group object.
- 13** Click Apply, or click OK to apply the changes and close the dialog box.

Viewing and Modifying Device Objects in NDS

This section describes how to perform the following tasks in NDS:

- ◆ [“Viewing and Modifying Device Properties” on page 17](#)
- ◆ [“Viewing and Modifying Interface Properties” on page 18](#)
- ◆ [“Viewing and Modifying Group Properties” on page 19](#)
- ◆ [“Viewing Monitor Properties” on page 20](#)

For information related to managing device objects that are routers, refer instead to [“Managing Routers” on page 21](#).

Viewing and Modifying Device Properties

A device object can represent a router, a switch, or a Monitor Agent. To view or configure the properties of a device in NDS, complete the following steps from the ZENworks for Networks Console:

- 1** Right-click a device object in the Devices folder and select Properties.

The following is displayed in the Device tab:

 - ◆ Name of the device
 - ◆ Device model number
 - ◆ Software version the device is running
 - ◆ Vendor name
 - ◆ Primary IP address of the device

- 2** To configure QoS and the classification methods the device will use, click the Capabilities tab.
- 3** Select the QoS capabilities that the device supports.
 - ◆ Weighted Fair Queueing—A technique used to monitor traffic and ensure that a device does not monopolize the available bandwidth.
 - ◆ Priority Queueing—A technique used to assign priority to traffic classes so that the most critical traffic is routed first.
 - ◆ Rate Limit—A technique used to reduce the rate at which packets are sent from a device.
- 4** Select the classification capabilities that apply to the device.
 - ◆ Layer 2—The device can filter packets at network Layer 2.
 - ◆ Static IP Filter—The device can filter IP packets.
 - ◆ Static Filter—The device can filter packets other than IP.
- 5** To configure passwords to enable remote configuration of the device from the ZENworks for Networks Console, click the Passwords tab.
- 6** Enter a Login password and an Enable password. These passwords need not be the same.

The Login password enables you to log in to (establish a connection to) the device. The Enable password enables you to update the configuration of the device.
- 7** Click Apply, or click OK to apply the changes and close the dialog box.

Viewing and Modifying Interface Properties

An interface object represents one of a possible number of interfaces in a network device. For example, a router can have multiple interfaces that route traffic to different network segments.

To view or configure the properties of an interface object for a device, complete the following steps from the ZENworks for Networks Console:

- 1** Right-click an interface object and select Properties.

The following is displayed in the Interface tab.

- ◆ Name of the interface
- ◆ IP address of the interface
- ◆ Subnet mask for the interface

- ◆ Interface number (if the device has multiple interfaces)
 - ◆ Primary IP address check box
 - ◆ Interface speed (Kbps)
 - ◆ Media type
- 2** To configure QoS and the classification methods the interface will use, click the Capabilities tab.
 - 3** Select the QoS capabilities that the interface supports.
 - ◆ Weighted Fair Queueing—A technique used to monitor traffic and ensure that a device does not monopolize the available bandwidth.
 - ◆ Priority Queueing—A technique used to assign priority to traffic classes so that the most critical traffic is routed first.
 - ◆ Rate Limit—A technique used to reduce the rate at which packets are sent from a device.
 - 4** Select the classification capabilities that apply to the interface.
 - ◆ Layer 2—The device can filter packets at network Layer 2.
 - ◆ Static IP Filter—The device can filter IP packets.
 - ◆ Static Filter—The device can filter packets other than IP.
 - 5** Click Apply, or click OK to apply the changes and close the dialog box.

Viewing and Modifying Group Properties

Smart groups are groups of existing devices that share common configuration parameters or common policy rules. Similar to how User Group objects in NDS simplify the management of access rules, the creation of smart groups significantly decreases the number of configurations and policy rules you are required to manage.

To view or configure the properties of a smart group from the ZENworks for Networks Console, complete the following steps:

- 1** Right-click a group object and select Properties.

The following is displayed in the Smart Group tab.

- ◆ Smart group name
- ◆ Start and start IP addresses representing the address range for the devices in the smart group

- 2** To view the vendors of devices in the smart group, click the Vendors tab.
- 3** To view the types of interfaces in the smart group, click the Interface Types tab.
- 4** To configure QoS and the classification methods the smart group will use, click the Capabilities tab.
- 5** Select the QoS capabilities the smart group supports.
 - ◆ Weighted Fair Queueing—A technique used to monitor traffic and ensure that a device does not monopolize the available bandwidth.
 - ◆ Priority Queueing—A technique used to assign priority to traffic classes so that the most critical traffic is routed first.
 - ◆ Rate Limit—A technique used to reduce the rate at which packets are sent from a device.
- 6** Select the classification capabilities that apply to the smart group.
 - ◆ Layer 2—The device can filter packets at network Layer 2.
 - ◆ Static IP Filter—The device can filter IP packets.
 - ◆ Static Filter—The device can filter packets other than IP.
- 7** Click Apply, or click OK to apply the changes and close the dialog box.

Viewing Monitor Properties

A monitor object represents each server that hosts a ZENworks for Networks Monitor Agent. Monitor Agents are installed during installation. You cannot add or delete Monitor Agents. To view the properties of a monitor object from the ZENworks for Networks Console, complete the following steps:

- 1** Right-click a monitor object and select Properties.

The following is displayed in the General tab.

 - ◆ Name of the Monitor Agent
 - ◆ IP address of the server hosting the Monitor Agent
 - ◆ Software version the Monitor Agent runs
- 2** Click OK.

Changing IP Addresses Assigned to Interfaces

After Auto Discovery has populated NDS with the discovered devices, ZENworks for Networks allows you to easily change the IP addresses assigned to devices.

To change the IP address assigned to an interface, complete the following steps from the ZENworks for Networks Console:

- 1 Right-click an interface object for a device and select Properties.
- 2 Change the IP address in the Interface tab.
- 3 (Optional) To make this the primary IP address, check the Primary IP Address check box.

Enabling this check box automatically updates the primary IP address shown in the properties page for the device.

- 4 Click Apply, then click OK.

Managing Routers

As explained in the previous sections, the properties of QoS devices created in NDS enable you to do the following from the ZENworks for Networks Console:

- ◆ Log in to a device such as a router
- ◆ View the status of a device such as a router

You can also manage routers as explained in the following sections:

- ◆ [“Importing Router Configurations” on page 21](#)
- ◆ [“Updating Router Configurations” on page 22](#)
- ◆ [“Rebooting Routers” on page 22](#)

IMPORTANT: To do router configuration, Policy Server must be started, and the Java Configuration Management Agent (JCMA) must be running.

Importing Router Configurations

IMPORTANT: You can import router configurations for only Cisco routers.

Before you configure a router using its NDS properties, it is essential to import its existing configuration to ensure that the configuration in NDS is in sync with that maintained on the device.

To import a router's existing configuration into NDS, complete the following steps from the ZENworks for Networks Console:

- 1** Right-click the device in the QoSDevice container and select Properties.
- 2** If you haven't already set passwords, do the following:

- 2a** Click the Passwords tab

- 2b** Enter a Login password and an Enable password. These passwords need not be the same.

The Login password enables you to log in to (establish a connection to) the router. The Enable password enables you to update the configuration of the router.

- 3** Click the Router Control tab, then click Import Router and OK.

- 4** (Optional) To view an existing or new router configuration, click the Configuration tab.

The Configuration tab displays command line-based configuration information for the router.

Updating Router Configurations

After you have made Policy Server changes in NDS, you can update the router directly from the ZENworks for Networks Console. To update the router, complete the following steps:

- 1** Right-click the device in the QoSDevice container and select Properties.

- 2** If you haven't already set passwords, enter a Login password and an Enable password.

The Login password enables you to log in to (establish a connection to) the router. The Enable password enables you to update the configuration of the router.

- 3** Click the Router Control tab, then click Update Router and OK.

Rebooting Routers

To reboot a router directly from the ZENworks for Networks Console, complete the following steps:

- 1** Right-click the device in the QoSDevice container and select Properties.

- 2** If you haven't already set passwords, enter a Login password and an Enable password.

The Login password enables you to log in to (establish a connection to) the router. The Enable password enables you to update the configuration of the router.

- 3** Click the Router Control tab, then click Reboot Router and OK.

