The Internet and e-business services have significantly increased the demands companies make on their networks. Companies are adding users, services, and applications to their networks nearly every day. If your company's network is expanding in this way, you are probably struggling to keep pace with the steadily growing demand for network bandwidth.

To help you address this issue, Novell recently released a new Net Services software product that adds to the ZEN works product line, ZEN works for Networks 1.0. With ZEN works for Networks 1.0, you can remotely manage network bandwidth and configure network switches and routers from a central location on the network.

A QUALITY-OF-SERVICE SOLUTION

Efficient use of bandwidth can significantly improve the performance of your company's network. Ideally, you want to provide network customers—such as users, applications, and devices—with the bandwidth they need to operate efficiently. The level of service the network delivers to a network customer is described as Quality of Service (QoS).

ZEN works for Networks is a QoS solution that leverages NDS eDirectory. With ZEN works for Networks, you can remotely control the QoS provided to network customers, and you can manage network devices, such as switches and routers. To control the bandwidth a specific user, application, or device uses, you establish policies that ZEN works for Networks stores in NDS eDirectory. Using these policies, you can ensure that network customers receive the throughput they require for optimal performance.

In addition, you no longer have to have several different proprietary programs to configure network routers and switches on a device-by-device basis. With ZEN works for Networks, you can remotely configure and manage all these devices through NDS.

Best of all, ZEN works for Networks is a vendor-neutral solution that supports devices from various vendors such as Cisco, Lucent, and 3Com. In contrast, many other QoS solutions on the market are hardware-specific and require you to manage each device individually.

WHO NEEDS ZENWORKS FOR NETWORKS?

ZEN works for Networks benefits any company that has multiple network segments connected through switches or routers. However, ZEN works for Networks provides the greatest benefit to companies that have multisite networks connected through WAN links. The following types of companies also benefit from using ZEN works for Networks:

- Companies that want to allocate bandwidth to mission-critical applications
- Web-hosting services that want to manage traffic between web sites
- Educational institutions that want to arbitrate bandwidth use between faculty and students
- Companies that want to allocate bandwidth between remote sites
- Companies that want to establish service-level agreements (SLAs) with internal or external customers

ZENWORKS FOR NETWORKS COMPONENTS

ZEN works for Networks includes the following components:

- Policy Servers to Support NetWare and Windows NT Platforms. Policy servers enforce the QoS and device configuration policies that you establish on the network. Policy servers access the policy information stored in NDS through Lightweight Directory Access Protocol (LDAP).

- Network-Traffic Monitor Agents to Support NetWare and Windows NT Platforms. Network-traffic monitor agents provide real-time monitoring and reporting of traffic on network segments that are assigned policies. These agents access policy information stored in NDS through LDAP. You should install network traffic monitor agents on each network segment.
NDS Schema Extensions. During installation, ZENworks for Networks extends the schema of the NDS tree to add the required object classes and associated attributes. The object classes added by ZENworks for Networks begin with the letters den, cim, or ps (policy server). Novell based the schema extensions for device management on the Distributed Management Task Force's (DMTF's) Directory-Enabled Network (DEN) and Common Information Model (CIM) specifications. (For more information about these specifications, see "What Are DEN and CIM?" on p. 40.) Because Novell based the schema extensions on the DEN and CIM specifications, ZENworks for Networks will interoperate with any device or application that is DEN compliant.

• ConsoleOne Snap-in Modules. The ConsoleOne snap-in modules for ZENworks for Networks let you configure and manage policies and ZENworks for Networks objects and properties.

BANDWIDTH MANAGEMENT THROUGH POLICIES
To ensure that network customers receive the bandwidth they need, many companies use overprovisioning. As the name implies, overprovisioning is the process of deploying significantly more bandwidth than required.

Unfortunately, just as people’s spending usually increases to meet or exceed their income, bandwidth usage usually increases to meet or exceed available bandwidth. Before you add bandwidth to your company’s network, you should implement a bandwidth-management solution (such as ZENworks for Networks) to help you use the existing bandwidth more efficiently.

With ZENworks for Networks, you can manage bandwidth by implementing traffic policies at critical points on the network. For example, critical Internet access points include WAN links to remote sites, mission-critical databases, and web servers.

Figure 1. ZEN works for Networks automatically adds network-policy and traffic-management objects to your company’s NDS tree.

• NDS Schema Extensions. During installation, ZENworks for Networks extends the schema of the NDS tree to add the required object classes and associated attributes. The object classes added by ZENworks for Networks begin with the letters den, cim, or ps (policy server). Novell based the schema extensions for device management on the Distributed Management Task Force’s (DMTF’s) Directory-Enabled Network (DEN) and Common Information Model (CIM) specifications. (For more information about these specifications, see “What Are DEN and CIM?” on p. 40.) Because Novell based the schema extensions on the DEN and CIM specifications, ZENworks for Networks will interoperate with any device or application that is DEN compliant.

• ConsoleOne Snap-in Modules. The ConsoleOne snap-in modules for ZENworks for Networks let you configure and manage policies and ZENworks for Networks objects and properties.

BANDWIDTH MANAGEMENT THROUGH POLICIES
To ensure that network customers receive the bandwidth they need, many companies use overprovisioning. As the name implies, overprovisioning is the process of deploying significantly more bandwidth than required.

Unfortunately, just as people’s spending usually increases to meet or exceed their income, bandwidth usage usually increases to meet or exceed available bandwidth. Before you add bandwidth to your company’s network, you should implement a bandwidth-management solution (such as ZENworks for Networks) to help you use the existing bandwidth more efficiently.

With ZENworks for Networks, you can manage bandwidth by implementing traffic policies at critical points on the network. For example, critical Internet access points include WAN links to remote sites, mission-critical databases, and web servers.

NETWORK-POLICY AND TRAFFIC-MANAGEMENT OBJECTS
When you install ZENworks for Networks, the installation program automatically adds the following network-policy and traffic-management objects to the NDS tree. (See Figure 1.)

• Policy Server Object. This container object defines the properties and policies for the policy server software that is hosted on a Netware server or a Windows NT server or workstation. This container object holds the QoS-Service object, the JCMA object, and the PolicySystem object. During the

Please visit our advertiser
Biscom
http://www.biscom.com/cd_offer

For more information, visit http://www.nwconnection.com/advertise.html.
installation of ZENworks for Networks, the installation program allows you to specify the location in the NDS tree where you want the object placed and names the object using the following naming convention: servername_POLICY.

- **QoSService Object.** This object allows you to manage ZENworks for Networks policies. The installation program automatically places the QoSService object in the Policy Server object.

- **JCMA Object.** The JCMA object communicates with the network device using native communications methods such as Telnet/Command Line Interface (CLI) and Trivial File Transfer Protocol (TFTP). This object handles the updates of policy configurations to the network device as well as the association between the policy server and the Java Configuration Management Agent (JCMA). The installation program automatically places the JCMA object in the Policy Server object.

- **PolicySystem Object.** This container object holds the Parameter, PolicyContainer, and QoSDevice container objects. You use these objects to store information about individual policies and network devices. The installation program automatically places the PolicySystem object in the Policy Server object.

**DEFINING POLICY RULES**

ZENworks for Networks includes the Policy Management Console, which allows you to establish policy rules for network monitors, QoS devices and interfaces, and smart groups. (Smart groups are groups of devices that share the same configuration or policy rules.) To access the Policy Management Console, you right-click the QoSService object in ConsoleOne, select Views, and then select ZENworks for Networks. (See Figure 2.)

ZENworks for Networks does not include default policy rules for a policy server. The first time you access the Policy Management Console, the Traffic Rules window shown in Figure 2 will be empty. You can create a policy rule by choosing Rules/New Rule from the ConsoleOne menu bar. When you create a policy rule, you define the following properties:

- **Rule.** You can assign each rule a unique name and define the traffic class to which the policy rule applies. You use traffic classes to differentiate types of network traffic. You also use the Rule property to specify the enforcement points to which the policy rule applies. A nonforcement point can be
any device, interface, or monitor agent on the network.

- **Sender.** You can specify the sender to which the policy rule applies. You can define the sender as any source server, specific network entities (such as hosts, subnets, or networks), or NDS users.

- **Receiver.** You can specify the receiver to which the policy rule applies. You can define the receiver as any destination client, specific network entities (such as hosts, subnets, or networks), or NDS users.

- **Service.** You can specify the TCP/IP services to which the policy rule applies. You can choose an existing service (such as FTP or HTTP) or define custom services or groups of services.

- **Time.** You can specify the times during which ZENworks for Networks enforces the policy rule. You can specify that the policy rule applies all the time or only on specific dates and times.

- **Bandwidth.** The bandwidth properties control traffic flow by using various weighted-queuing and bandwidth-shaping techniques. You can select Absolute properties that do not adjust to differing levels of traffic or Weighted properties that adjust to differing levels of traffic. For example, you can select Absolute properties such as allowing packets to be dropped and allocating a percentage of bandwidth. You can select Weighted properties such as the weight to be used for discarding packets and fair queue sessions that prevent a queue from monopolizing available bandwidth.

- **Priority.** You can configure priority queuing, packet handling, and packet marking parameters for the priority rule. Priority queuing allows you to specify a priority queuing level (such as low, medium, or high). Packet handling allows you to specify a classification for the Type of Service (TOS) field in an IP header. The device that enforces the policy rule will handle the packets it receives according to this classification. Packet marking allows you to specify a precedence level to be set. The device that enforces the policy rule will then mark the precedence bits for the packets it forwards to other routers.

- **Actions.** You can specify the actions a policy server should take when a pre-configured event (such as class bandwidth, kilobytes transferred, and link load) exceeds a threshold value. You can configure the policy server to take the following actions: execute a server command, send e-mail or pager notification to predefined users, generate a Simple Network Management Protocol (SNMP) message, or record the message in a log file.

Traffic policies improve overall network performance, ensuring that users, applications, and devices receive the QoS they require to operate efficiently.

### Monitoring the Network

ZENworks for Networks also includes real-time monitoring, which enables you to monitor bandwidth consumption, response time, or connection failures in real time. Monitoring your company's network is an important part of implementing policy rules for network traffic. By monitoring the network, you can determine if the policy rules you have implemented are effective, you can identify problem areas, and you can find ways to optimize the network.

When you install the real-time monitor component of ZENworks for Networks, the installation program creates a monitor object to represent each server that hosts a ZENworks for Networks monitor agent. The installation program automatically creates these objects, and you cannot create or delete them outside the installation program.

You launch the real-time monitor by highlighting a monitor agent in the ZENworks for Networks view in ConsoleOne and selecting the Real-Time monitor tab. You can then select and monitor the following:

- The connection time for connected traffic classes
- Bandwidth consumption
- Response times
- Failures

You can use four predefined profiles to view the statistics that the monitor agents track. (See Figure 3.)

**Services**
- **Server**
- **Client**
- **User**

ZENworks for Networks also provides an event view that allows you to view informational, error, and warning messages for all of the devices configured for a particular policy server. If you choose Options from the ConsoleOne menu bar and then choose Start Event Viewer, the Event Viewer will display a chronological list of device-related events that the policy server has recorded.

### Configuring and Managing Network Devices

ZENworks for Networks also enables you to remotely manage network routers and switches via NDS. Typically, you must manage these devices on a device-by-device basis.

In addition, most routers and switches have proprietary programs that you must use to configure the devices. If two iden-
tical devices have identical configuration information, you usually cannot share that information between the devices. What is more, there is no easy way to back up device configuration information, short of manually backing up each device individually.

To simplify the management of network devices, ZENworks for Networks stores device configurations in NDS. As a result, you can remotely view and configure devices, share configuration information between devices, and even remotely reboot devices. The distributed, replicated nature of NDS also provides fault tolerance ensuring that device configurations are always available.

DEVICE MANAGEMENT NDS OBJECTS
When you install ZENworks for Networks, the installation program automatically adds the following device management objects to the NDS tree:

- **QoSDeviceContainer**. This container object resides in the PolicySystem container object, which the installation program places in the Policy Server object. The QoSDeviceContainer object holds the following objects: the QoSDevice, QoSInterface, and QoSInterfaceGroup objects.

- **QoSDevice**. This container object stores objects that represent the network hardware devices and servers running software monitoring agents. You can use the properties of the QoSDevice object to import the current device configuration into NDS, to update the device with a new configuration defined in NDS, or to reboot the device.

- **QoSInterface**. This container object stores objects that represent each hardware interface on a device. Any protocols bound to an interface are nested under the QoSInterface object.

- **QoSInterfaceGroup**. This container object stores objects that represent smart groups. As mentioned earlier, smart groups are groups of devices that share the same configuration or policy rules. You create smart groups to simplify the management of these devices.

MANAGING DEVICE INFORMATION IN NDS
Before you can manage routers or switches through NDS, you need to create the devices in NDS. You can man-

Please visit our advertiser
Learn key
http://www.learnkey.com

For more information, visit http://www.nwconnection.com/advertise.html.
QoSDeviceContainer object with the devices it discovered. (See the left pane in Figure 4.)

After ZENworks for Networks discovers the devices, you can view and modify the device and interface properties, including changing the IP addresses. (See the Device Properties window in Figure 4.)

MANAGING ROUTERS
ZENworks for Networks also includes the following options, which allow you to perform additional router management tasks:

- **Import Router.** The Import Router option allows you to import a router’s existing configuration information so that you can view and modify it in NDS. This capability is available only for Cisco routers.
- **Update Router.** The Update Router option allows you to update a router remotely after you have changed a policy server in NDS.
- **Reboot Router.** The Reboot Router option allows you to remotely reboot a router through ConsoleOne.

CONCLUSION
With ZENworks for Networks, Novell has delivered a Net Services product that enables you to deliver end-to-end QoS to network customers. You can customize and control the bandwidth used by users, applications, and devices. You can also monitor network traffic in real time and use reports to validate your existing policies and identify problem areas on the network. Finally, you can configure and manage devices remotely through NDS.

ZENworks for Networks is a must-have for companies that want to reduce management costs and get the most out of their investment in their existing network infrastructure.

Sandy Stevens is a freelance writer based in San Diego, California. Stevens is co-author of Novell’s Guide to Integrating NetWare 5 and NT, Novell’s Guide to NetWare Printing, and Novell’s Guide to BorderManager.

**Figure 4.** You can configure ZEN works for Networks to automatically discover devices.

---

**What Are DEN and CIM?**

Directory-Enabled Networks (DEN) is a Desktop Management Task Force (DMTF) specification that defines an information model, a usage model, and a directory schema for integrating network components with a directory service. When network components are directory enabled, networks become easier to use, easier to manage, and more secure.

The DEN specification enables equipment vendors, directory service providers, software developers, common carriers, and users to develop interoperable, directory-enabled applications that address the following:

- The way the network functions
- The elements and services of the network
- The physical and logical topology of the network

If applications are integrated with the directory, they can leverage the network infrastructure on behalf of the user. As a network administrator, you can then provide and manage end-to-end network services on a per-user basis. For example, when a user logs into the network and launches a bandwidth-intensive application, network resources, such as the necessary bandwidth, can be allocated on demand for that application.

The DEN specification is actually part of the Common Information Model (CIM) standard. The CIM standard provides a framework for managing enterprise computing environments in a common way. The CIM standard allows you to see a consistent view of the managed environment, regardless of which protocols and data formats individual network devices and applications support.

The CIM standard addresses the management of the following elements in an enterprise network:

- Collections of general-purpose devices (non-network devices)
- Applications
- System components
- System data

The DEN specification expands the device schemas that CIM defines to include policy schemas and network models. In addition, the DEN specification expands CIM classes to address the specific requirements of network elements and services. For more information about DEN and CIM, visit http://www.dmtf.org.)

---

**39 NetWare Connection May 2000**