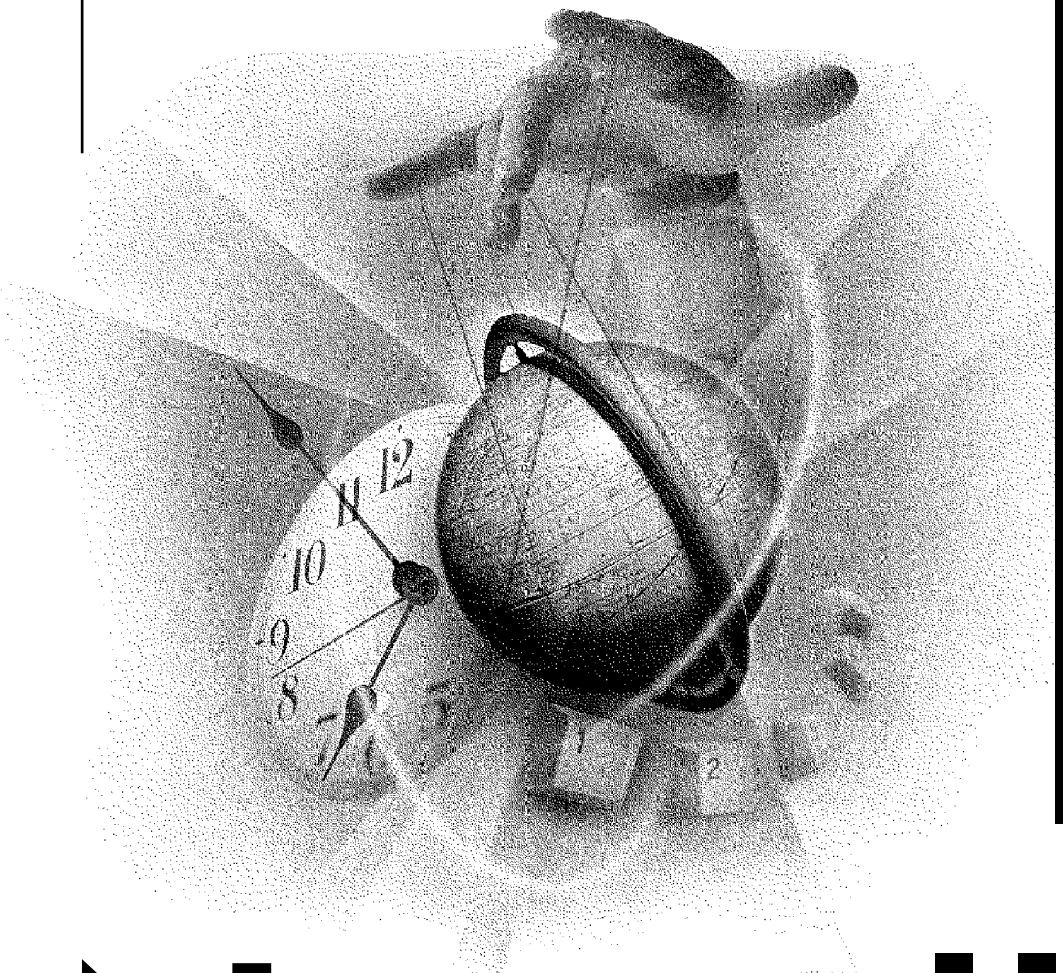
VERSION 1.0

Network Policy and Traffic 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.

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 Policy and Traffic 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

This guide describes how to create network traffic policies and how to monitor network traffic using the ZENworks™ for Networks software.

1 Understanding Traffic Management

With the network policy and traffic management components of ZENworks™ for Networks, you can set dynamic traffic control policies for devices such as routers and switches. You can specify control policies by application, sender and receiver addresses, time of day, day of week, and day of month.

The software also performs inbound and outbound monitoring, and generates alarms and appropriate actions in response to preconfigured events. ZENworks for Networks assists you in the entire spectrum of traffic monitoring and flow control, ranging from bandwidth and latency control to capacity planning.

This chapter defines concepts that are key to understanding traffic management and why traffic management policies enable you to optimize your network resources as part of a Quality of Service (QoS) solution. This chapter contains the following sections:

Traffic Management Concepts

To better explain the mechanics of traffic monitoring and management, the following definitions are provided:

- "Traffic Rules" on page 11
- "Traffic Entities" on page 11

Traffic Classes

Traffic management involves the identification (or classification) of different traffic flows to separate one kind of traffic from another. A traffic class can be distinguished by any of the following criteria:

- TCP/IP parameters—IP address or range of IP addresses, IP network, subnet, or group
- Type of service or groups of services—For example, HTTP or FTP
- Time—Month, week, day, or hour
- Direction of flow—Inbound or outbound
- Enforcement point—Where in a network the traffic is classified

When traffic classes are defined, they can be used for measurement (statistical purposes). However, the best use of traffic classes involves both measurement and subsequent control of network traffic based on those measurements. For example, you can configure a traffic class to differentiate between inbound and outbound traffic and measure the throughput of each class. However, it is far more effective to measure the throughput of each class and guarantee that a minimum bandwidth is reserved for outgoing traffic even when there is a lot of congestion in the inbound direction from large downloads. The differentiation of traffic into traffic classes enables traffic policies to control traffic, such as with a guaranteed bandwidth in one direction of traffic flow.

Traffic Policies

Traffic policies control the traffic flow of defined traffic classes. Properties of traffic policies can be used to set bandwidth guarantees, bandwidth limits, and priorities for different traffic classes. They can be defined to measure or control traffic at specific times, such as during peak network use.

While bandwidth guarantees grant a minimum bandwidth to critical traffic when there is congestion or competition between different traffic classes, bandwidth limits restrict the total bandwidth used by a specific traffic class. Traffic policies that use bandwidth guarantees and bandwidth limits are fairly straightforward.

Traffic policies that are based on set priorities for different traffic classes are more complex, and their design depends upon the routers in your network. To

handle more critical traffic first, routers typically separate traffic into three priority classifications: high, medium, and low. Some routers offer four classifications: high, medium, normal, and low. High-priority classes are serviced first and are affected the least during contention for bandwidth. Normal or low-priority classes are serviced after high-priority classes and are typically more affected by network congestion or bandwidth contention.

Packet Marking and Handling

Traffic policies that specify priority can modify the 8-bit Type of Service (TOS) field in an IP header. Four of the bits in the TOS byte are usually used to assign minimum delay, maximum throughput, maximum reliability, and cost to a packet. ZENworks for Networks policy rules allow you to classify packets by modifying the value of these four bits. The value assigned by the policy rule determines how the device that enforces the rule handles the packets.

Another three bits in the TOS byte are referred to as the precedence bits.The eighth must be zero (MBZ) bit is unused and always has a value of 0. The precedence bits are usually used to mark a packet for additional monitoring or as a drop priority downstream from the device that enforced the policy rule. ZENworks for Networks policy rules allow you to mark packets for monitoring by other devices. Acceptable values for the precedence bits are 1 through 6 (0 and 7 are typically not used by routers).

Traffic Rules

A traffic rule results when a traffic policy is associated with a specific traffic class. A class can have several policies that apply during different time intervals or at different enforcement points in a network.

Traffic Entities

Another important part of traffic management is real-time monitoring of traffic flows. When profiling traffic, there are two basic traffic entities: network entities and service entities.

A network entity refers to an IP address or range of IP addresses, host, subnet, or IP network.

A service entity refers to a single TCP/IP service or a group of services.

Traffic Management Goals

Traffic management involves the monitoring of network traffic and the application of policies to manage critical network resources. Goals of traffic management include the following:

- Improving overall performance and efficiency
- Ensuring fairness in resource allocation
- Protecting the performance of other applications when an application malfunctions or fails
- Providing predictability and a sense of order in the event of network congestion
- Isolating faults to make performance problems more visible
- Meeting the diverse user and application requirements specified by an organization's business goals
- Increasing the throughput of good traffic ("goodput") based on economic value to prevent the waste or abuse of network resources

To achieve these goals, you can apply traffic management policies to the following critical network resources:

- Internet access links
- Private WAN links to remote corporate sites
- Server farms (groups of servers located near access links for faster connectivity, such as servers hosting Web services)
- Mission-critical database and Web servers that service users who are either internal or external to your organization

Traffic Management Issues Addressed by Network Traffic Policies

Applying network traffic policies at critical enforcement points in your network can help you predict network performance and conform to your QoS specifications.

A comprehensive traffic management solution that incorporates the use of network traffic policies must address the following issues that are present in a complex network environment:

Variations in Bandwidth or Link Speeds

A traffic management solution must address the limited availability of bandwidth and the asymmetrical and heterogeneous speeds of various links.

Table 1 on page 13 summarizes the bandwidth requirements that various Internet users depend upon.

Table 1 User Bandwidth Requirements

Users	Bandwidth	Services Offered
Internet application developers, individual users, and international users whose bandwidth is expensive	28.8 Kbps to 56 Kbps	Dial-up services, Integrated Services Digital Network (ISDN), digital subscriber line (DSL)
Small- to medium-sized organizations with moderate Internet use	56 Kbps to 1.5 Mbps	Fractional T1, frame relay, cable modem
Medium-sized organizations with many users requiring moderate Internet use, or smaller organizations with a small number of users requiring large amounts of bandwidth	1.5 Mbps	Dedicated T1 circuit
Standard Ethernet-based LAN users	10 Mbps	Ethernet or Token Ring (4 Mbps or 16 Mbps)
Users in large corporations with Internet backbones	45 Mbps	Dedicated T3 circuit
Many users (hundreds or thousands) in a medium to large organization that has a huge bandwidth LAN backbone	100 Mbps to 1,000 Mbps	Fast Ethernet or Gigabit Ethernet

A request or a response to a request for an Internet service can traverse several different links. For example, the links used by a remote Web server to service a browser request can include the following:

- A client's 28.8-Kbps dial-in connection through a local Internet Service Provider (ISP)
- An ISP's T1 connection to the Internet
- A Web server's 10-Mbps Ethernet LAN connection
- A Web server's 56-Kbps frame relay connection to another ISP
- An Asynchronous Transfer Mode (ATM) backbone connecting the client's ISP carrier to the Web server's ISP carrier

When bandwidth is limited at a link in the access path, simply upgrading the capacity of the link may temporarily increase available bandwidth, but may not offer a long-term solution. Increasing bandwidth incurs significant expenses resulting from the purchase of new hardware, additional setup fees, and higher monthly fees. These costs do not necessarily translate into increased productivity because without proper limits, bandwidth utilization almost always rises to meet or exceed available bandwidth. You should evaluate productivity gains before upgrading bandwidth. Adding additional bandwidth is a reasonable solution only after you have implemented the management of existing bandwidth. Traffic management policies can help ensure efficient use of available bandwidth before you make that kind of investment.

Variations in Application Requirements

In today's networking environment, a large number of diverse applications and protocols are widely used. Many of these applications have their own performance and bandwidth requirements, depending on the nature of the data being accessed.

Table 2 on page 15 provides examples of applications with different performance and bandwidth requirements.

Table 2 Application Bandwidth Examples

Application Description	Examples
Low bandwidth, delay sensitive, and highly interactive	Domain Name System (DNS), ping, Telnet, Internet chat, and collaboration
High bandwidth and delay sensitive	Real-time audio and video
High bandwidth and nominally interactive	Web service requests, such as HTTP, and file downloads, such as FTP
Noninteractive	Mail and news services, such as Simple Mail Transfer Protocol (SMTP) and Network News Transfer Protocol (NNTP)

Because applications such as SMTP and NNTP are not interactive, they are not sensitive to transmission delays. However, applications such as real-time videoconferencing are extremely sensitive to transmission delays, but they are not sensitive to occasional packet loss. Telnet and DNS do not require significant bandwidth, but are sensitive to both transmission delays and packet loss, whereas FTP consumes a large amount of bandwidth, but is not sensitive to transmission delays.

In general, network applications can be categorized as follows:

- Interactive or noninteractive (delay sensitive or delay tolerant)
- Bandwidth intensive or nonbandwidth intensive (sending bulk data or a small amount of data)
- Bursty or nonbursty (prone to peak usage or steadily consuming the same amount of bandwidth)

A traffic management solution must respond to both performance and bandwidth requirements based on the type of application being used. Traffic management policies must be able to identify applications that are nominally interactive or nominally bandwidth intensive. Because these applications exhibit the nominal characteristics most of the time, but not all of the time, the bandwidth allocation can be adjusted accordingly.

Variations in User Requirements

An explosive number of network applications are now providing data to users who are internal and external to your network. As a result, network resources

are increasingly being used for a wide variety of purposes, ranging from business-critical to personal.

Table 3 on page 16 itemizes typical user priorities for a software company. The highest bandwidth priority is allocated to technical support staff, followed by sales and marketing personnel. Those sending e-mail have the lowest bandwidth priority.

Table 3 User Priorities for a Typical Company

Users (From Highest to Lowest Priority)	Application Class	Justification
Technical support staff	Mission-critical	Need the most bandwidth to work with customers who need assistance
Sales and marketing staff	Critical	Need larger than average amount of bandwidth to work with potential customers, answer inquiries, provide real-time quotes, and send multimedia presentations
Managers and administrators	Casual	Need bandwidth to perform tasks necessary to run the business
Development and manufacturing staff	Personal	Need bandwidth to send e-mail and subscribe to push technologies

Because Internet bandwidth is often a limited resource, a traffic management solution must implement policies to ensure that a business gets the maximum return on its bandwidth investment. The return on investment can result from direct revenue-generating activities, such as electronic commerce, or can result from greater user productivity. Like security policies, traffic management policies should be consistent with an organization's needs.

Variations in TCP/IP Flow Control

TCP/IP was designed as a "best-effort" protocol, and almost all network applications rely on TCP/IP. A best-effort service makes its best attempt to deliver all packets sent, but will indiscriminately drop packets when a network is congested. Because best effort is loosely defined, there is significant variation in how each application controls TCP connection parameters. TCP

flow algorithms tend to be either too aggressive or too conservative in the life of a connection. Often these algorithms attempt to ramp up point-to-point throughput without regard to the type of service, other connectivity activities that may be occurring simultaneously, or traffic policies. Simply stated, there exists a virtual “free for all” at critical bottlenecks, such as WAN access links.

A traffic management solution must take type of service, simultaneous connectivity, and traffic policies into consideration when attempting to control the flow and throughput for these applications.

Ports Used for Interapplication Communication

For the network configuration management functionality, the following ports are used by the Policy Server and Monitor Agent for interapplication communication:

- Policy Server

  Port 1205—The Policy Server listens on this port for configuration change events, user logon/logoff events, and Monitor Agent log events.

  - Configuration change events are sent by the user interface.
  - User logon/logoff events are sent by ZENEVENT.NLM.
  - Monitor log events are sent by the Monitor Agent.

  Port 1206—The Policy Server listens on this port to retrieve Policy Server/Monitor Agent log requests. These requests are sent by the user interface when user starts the event log.

- Monitor Agent

  Port 1201—The Monitor Agent listens on this port for profiles/real-time monitoring requests. These requests are sent by the user interface.

  Port 1207—The Monitor Agent listens on this port for configuration change events and user logon/logoff events.

  - Configuration change events are sent by the user interface.
  - Logon/logoff events are sent by ZENEVENT.NLM.

2 Setting Up Network Traffic Policies

This chapter describes how to start the ZENworks™ for Networks Console and how to configure policies for traffic control. It contains the following sections:

Accessing the ZENworks for Networks Console

The Policy Server must be running before you can access the ZENworks for Networks Console. This console allows you to configure your network policy rules.

To start the ZENworks for Networks Console, complete the following steps:

1. From your Windows* workstation or Windows NT* server that has the ConsoleOne™ 1.2c and the Management Console snap-ins installed, log in to NDS® with Admin (or Administrator) rights.
2. Run ConsoleOne.
3. Under the Policy Server container, highlight the QosService object.
4. Right-click and select Views > ZENworks for Networks.
5. (Optional) Click Auto Discovery to discover the devices in your network.

NOTE: Because you must specify where (on which device or Monitor Agent) a policy rule is enforced, monitors must be discovered, and Quality of Service (QoS) devices and groups must be discovered or created manually in NDS before configuring traffic policy rules. For more information on manually creating QoS devices in NDS, refer to "Managing Device Information in NDS" in *Network Configuration Management*.

Setting Up Traffic Policy Rules

When you first start the ZENworks for Networks Console, there are no default rules. To create a rule, select Rules > New Rule from the menu. A new row of rule properties is displayed in the interface. Each row represents a different rule.

ZENworks for Networks traffic policy rules consist of the following properties:

- Rule
- Sender
- Receiver
- Service
- Time
- Bandwidth
- Priority
- Actions

Because the rules are self validating, when you create a new rule, many of the properties are shown with a red X to indicate that they are invalid. This occurs because required properties have not yet been configured.

HINT: To speed things up, after you configure a property, just click on the next property to configure. Your configured property saves and closes, and the next property opens.

Refer to the following procedures for how to configure each policy rule property:

- "Configuring Rule Properties" on page 21
- "Configuring Sender and Receiver Properties" on page 21
- "Configuring Service Properties" on page 22
- "Configuring Time Properties" on page 23
- "Configuring Bandwidth Properties" on page 24
- "Configuring Priority Properties" on page 25
- "Configuring Action Properties" on page 25
- "Configuring Alarm Parameters" on page 27

Configuring Rule Properties

Rule properties specify the rule name, class name (if applicable), and where (on which device) the rule is enforced.

To configure rule properties, complete the following steps from the ZENworks for Networks Console:

NOTE: At any time before clicking Apply or OK, you can click Reset to revert to the original settings that were in effect when you opened the dialog box.

1. Double-click the rule icon in the row representing the policy rule.
2. Enter the rule name.
3. (Optional) Enter the class name.

   A default class name based on the service name is set when the service is configured.
4. Click the Enforcement tab.
5. Click Modify.
6. Add the devices from the Available list to the Selected list, then click Done.
7. Click Apply, or click OK to apply the changes and close the dialog box.

Configuring Sender and Receiver Properties

Sender and receiver properties specify the network entities or users to which the policy rule applies. A default object, ANY SOURCE, appears in the list of network entities for the sender property. It represents any server. Similarly, a default object, ANY DESTINATION, appears in the list of network entities for the receiver property. It represents any client. You cannot delete these objects.

To configure a specific sender or receiver for the policy rule, complete the following steps from the ZENworks for Networks Console:

NOTE: At any time before clicking Apply or OK, you can click Reset to revert to the original settings that were in effect when you opened the dialog box.

1. Double-click the sender or receiver icon in the row representing the policy rule.
2. If you want the rule to apply to any server or client, do the following:

   2a. Highlight ANY SOURCE or ANY DESTINATION.

2b Click Apply, or click OK to apply the changes and close the dialog box, then skip the rest of this procedure.

3 To configure a host, subnet, or network as the sender or receiver, click New and select a host, subnet, or network.

4 If you selected a host in Step 3, do the following:

4a Enter the name of the host.

4b Enter the IP address of the host.

4c Click Apply, or click OK to apply the changes and close the dialog box, then skip the rest of this procedure.

5 If you selected a subnet in Step 3, do the following:

5a Enter the name of the subnet.

5b Enter the subnet number.

5c Enter the subnet mask.

5d Click Apply, or click OK to apply the changes and close the dialog box, then skip the rest of this procedure.

6 If you selected a network in Step 3, do the following:

6a Enter the name of the network.

6b Enter the network number.

6c Click Apply, or click OK to apply the changes and close the dialog box.

7 To limit the rule to a specific NDS user, click the Users tab.

7a Locate and highlight the user object.

7b Click Apply, or click OK to apply the changes and close the dialog box.

Configuring Service Properties

The service property specifies the TCP/IP services to which the policy rule applies.

To configure a service property for the policy rule, complete the following steps from the ZENworks for Networks Console:

NOTE: At any time before clicking Apply or OK, you can click Reset to revert to the original settings that were in effect when you opened the dialog box.

1. Double-click the service icon in the row representing the policy rule.
2. If the specific service is in the list, do the following:
   - 2a Highlight the service.
   - 2b Click Apply, or click OK to apply the changes and close the dialog box.
3. If the specific service is not already in the list, click New and select Custom, then do the following:
   - 3a Enter a name for the service.
   - 3b Enter the start and stop ports for the service.

     If the service has only one port, enter it as the start port and do not enter a stop port.
   - 3c Select TCP or UDP for the service.
   - 3d Click Apply, or click OK to apply the changes and close the dialog box, then skip the rest of this procedure.
4. If you want to apply a group of services to the rule, click New, select Group, then do the following:
   - 4a Enter the name of the group.
   - 4b Click Modify, select the services for the group from the Available Services list, then click Done.
   - 4c Click Apply, or click OK to apply the changes and close the dialog box.

Configuring Time Properties

The time property specifies the times during which the rule is enforced. A default object, ANYTIME, appears in the list. It represents round-the-clock enforcement. You cannot delete this object.

To configure a specific time for the policy rule, complete the following steps from the ZENworks for Networks Console:

NOTE: At any time before clicking Apply or OK, you can click Reset to revert to the original settings that were in effect when you opened the dialog box.

1. Double-click the time icon in the row representing the policy rule.
2. If you want the rule to apply at all times, do the following:
   - 2a Highlight ANYTIME.

2b Click Apply, or click OK to apply the changes and close the dialog box.

3 If you want to specify a time slot for which the rule is valid, click New, then do the following:

3a Select the days of the month.

3b Select the days of the week.

3c Select the hours based on a 24-hour clock.

3d Click Apply, or click OK to apply the changes and close the dialog box.

NOTE: If the rule is to be applied to a single month or single day of the year only, specify the same month or day for the range. For example, for the rule to apply on Mondays only, specify Monday through Monday.

Configuring Bandwidth Properties

The bandwidth properties of a policy rule control traffic flow by using various weighted queueing and bandwidth shaping techniques.

To configure bandwidth properties for a policy rule, complete the following steps from the ZENworks for Networks Console:

1 Double-click the bandwidth icon in the row representing the policy rule.

2 At the bottom of the window, click Absolute or Weighted.

Absolute bandwidth properties do not adjust with differing levels of traffic. Weighted bandwidth properties come into play when there is competition for a limited amount of bandwidth. Priority is assigned based on the weight value or priority level in the rule.

3 If you selected Absolute, check the Allow To Drop Packets check box or the Limiting Rate (Class) check box, or both.

For Limiting Rate (Class), specify the percentage of bandwidth allowed (for maximum bandwidth limits).

4 If you selected Weighted, check the Weight (1-100) check box, the Fair Queue Sessions check box, or both.

You must enter a weight value (1-100), or for fair queue sessions, a priority level.

5 Click Apply, or click OK to apply the changes and close the dialog box.

Configuring Priority Properties

The priority properties of a policy rule specify priority queueing, packet handling, and packet marking parameters.

To configure bandwidth properties for a policy rule, complete the following steps from the ZENworks for Networks Console:

1. Double-click the priority icon in the row representing the policy rule.
2. For priority queueing, select Low, Medium, or High.
3. To enable packet handling, check the Classification TOS Byte check box and enter the hexadecimal value.

   The value can be 0 to 256 (0 to FF).
4. To enable packet marking, check the Mark IP Precedence check box and select a value between 0 and 7 for the precedence bits. Note that typically 0 and 7 are unused.
5. Click Apply, or click OK to apply the changes and close the dialog box.

Configuring Action Properties

If you plan to configure action properties, it is recommended that you configure the alarm parameters first. Refer to “Configuring Alarm Parameters” on page 27.

The action properties of a policy rule specify the actions taken by the Policy Server when a preconfigured event is triggered. An event is typically triggered when a statistic being monitored exceeds a set threshold value. Any of the following statistics can be configured to operate as events:

- Class bandwidth
- Round-trip time
- Connect time
- Request response time
- Sessions active
- Session bandwidth
- KB transferred
- Link load
- Class packet rate

- Connection retries
- Packet retransmits
- Session lifetime

NOTE: You must configure at least one event before you can configure action properties.

To configure events and action properties for a policy rule, complete the following steps from the ZENworks for Networks Console:

NOTE: At any time before clicking Apply or OK, you can click Reset to revert to the original settings that were in effect when you opened the dialog box.

1. Double-click the actions icon in the row representing the policy rule.
2. Select the Events tab.
3. Click Add and select Standard or Compound to create a standard or compound event.

   A standard event is a single instance in which a single measured statistic exceeds its set limits. A compound event is an instance of two events occurring at the same time or an instance in which one of two possible events occurs.
4. If you selected Standard in Step 3, do the following:

   4a Enter a name for the event.

   4b Use the drop-down list to select a value for the event.

   4c Select whether the event applies to a single traffic class or to all traffic classes.

   4d Check the appropriate check boxes (greater than or less than) and specify the threshold values for which the event is triggered.

   4e Specify the event trigger count. This is the number of times the threshold values are exceeded before an event is triggered.

   4f Specify the event polling interval, in seconds.

   4g Skip to Step 6.
5. If you selected Compound in Step 3, do the following:

   5a Enter a name for the event.

   5b For the first event list, select All if all the events need to occur, or Any if only one of the events in the list needs to occur.

5c If the Available Events list does not contain an event you need, click Add to create the event.

5d Click Modify to add events from the Available Events list to the event list.

5e For the second event list, select All if all the events need to occur, or Any if only one of the events in the list needs to occur.

5f Click Modify to add events from the Available Events list to the second event list.

5g Select And to specify that both event lists must occur, or select Or to specify that either of the event lists can occur to trigger the compound event.

6 Use the drop-down list to select a type of action for the response to the event.

NOTE: Before selecting SNMP to send traps to Simple Network Management Protocol (SNMP) management stations, you must have enabled SNMP Service in Windows NT and integrated the ZENworks for Networks PSERVER.MIB file into your SNMP management station. PSERVER.MIB is located in the /INSTALL directory.

7 Click Apply, or click OK to apply the changes and close the dialog box.

Configuring Alarm Parameters

NOTE: You do not have to configure alarm parameters to be able to send traps to SNMP management stations. Note, however that you must have enabled SNMP Service in Windows NT and integrated the ZENworks for Networks PSERVER.MIB file into your SNMP management station. PSERVER.MIB is located in the /INSTALL directory.

Alarm parameters are used to enable audit logs and to specify pager phone numbers and e-mail server IP addresses.

To configure alarm parameters, complete the following steps from the ZENworks for Networks Console:

1 Click the Alarms tab.

2 Do one or more of the following:

- Click the Audit Log tab, then check the Enable Logging check box and specify the maximum log file size in kilobytes.
- Click the Pager tab, then check the Enable Paging check box and specify the following:

- Maximum time allowed for pages
- COM port

- Click the E-Mail tab, then check the Enable Notification check box and specify the following:
  - Mail server IP address
  - Recipient e-mail address

3. If you checked the Enabled Notifications check box, specify the following:
   - Maximum time allowed for e-mail messages
   - Mail server IP address
4. Click Apply, or click OK to apply the changes and close the dialog box.

3 Monitoring Network Traffic

After you create network policies for different traffic classes, you should monitor your network traffic to further optimize your network.

This chapter describes how to use the Network Traffic Monitor Service to view network traffic in real time. It contains the following sections:

Running the ZENworks for Networks Real-Time Monitor

The ZENworks™ for Networks Real-Time Monitor enables you to monitor bandwidth consumption, response time, or connection failures in real time.

To launch the Real-Time Monitor from the ZENworks for Networks Console, complete the following steps:

1. Highlight a Monitor Agent.
2. Click the ZENworks for Networks Real-Time Monitor tab.
3. Select Bandwidth Consumption (Kbps), Response Time (ms), or Failures (%).
4. Select a list of classes to monitor from the list of available classes.

To launch the ZENworks for Networks Real-Time Monitor (Java* application) outside of the ConsoleOne™ application, click Launch.

Viewing Profiles

ZENworks for Networks provides the following four different profiles for viewing the statistics that the Monitor Agents monitor:

- Services
- Server
- Client
- User

To access these profiles, complete the following steps from the ZENworks for Networks Console:

1. Highlight a Monitor Agent.
2. Click the Profiles tab.
3. Select the Services, Server, Client, or User tab.

   NOTE: Click Refresh to get the latest statistics.

   - If you selected the Services tab, the following statistics are displayed:
     - Service—Name of service
     - Total Sessions—Total number of sessions established for this service
     - KB Transferred—Amount of data transferred in the inbound and outbound direction using this service
     - Connection Response Time (ms)—Average time taken to establish a session for this service
     - Request Response Time (ms)—Average response time for an application request
     - Retries—Percentage of connection requests that were retried
     - Server Aborts—Percentage of aborted sessions
     - Time—Last time the service was active
   - If you selected the Server tab, the following statistics are displayed:
     - Server—Server name, URL, or IP address
     - Total Sessions—Total number of sessions established with the server

- In KBytes—Amount of data transferred to the server in the inbound direction
- Out KBytes—Amount of data transferred from the server in the outbound direction
- Round Trip Time (ms)—Average round-trip delay for packets sent by the server
- Connection Response Time (ms)—Average time taken to establish a session with the server
- Retries—Percentage of connection requests that were retried
- Server Aborts—Percentage of sessions aborted by the server
- Access Speed—Bottleneck speed for the route between the traffic monitoring agent and the server
- Packet Retransmits—Percentage of packets retransmitted by the server
- Time—Last time that data was received by the server

- If you selected the Client tab, the following statistics are displayed:
  - Client—Name or IP address of client
  - Total Sessions—Total number of sessions established by the client
  - In KBytes—Amount of data transferred to the client in the inbound direction
  - Out KBytes—Amount of data transferred from the client in the outbound direction
  - Round Trip Time (ms)—Average round-trip delay for packets sent by the client
  - Connection Response Time (ms)—Average time taken to establish a session from the client
  - Retries—Percentage of connection requests that were retried
  - Server Aborts—Percentage of sessions aborted by the server
  - Time—Last time that data was received by the client
- If you selected the User tab, the following statistics are displayed:
  - User—Name of user
  - Total Sessions—Total number of sessions established by the user

- KB Transferred—Amount of data transferred for the user
- Round Trip Time (ms)—Average round-trip delay for packets sent to the user
- Connection Response Time (ms)—Average time taken to establish a session for the user
- Retries—Percentage of connection requests that were retried
- Server Aborts—Percentage of sessions aborted by the server
- Access Speed—Bottleneck speed for the route between the traffic monitoring agent and the server
- Packet Retransmits—Percentage of packets retransmitted by the server
- Time—Last time that data was received by the user

Using the Event Viewer

You can use the Event Viewer to view informational, error, and warning messages for all the devices configured for the Policy Server.

To use the Event Viewer, complete the following steps:

1. From the ConsoleOne menu bar, select Options > Start Event Viewer.

   The Event Viewer displays a chronological list of device-related events recorded by the Policy Server. Icons identify the messages as informational, error, or warning messages.

2. Do one of the following:

   - To save the list of messages to a text file, select Save As and supply the filename.
   - To clear the list of messages, select Clear.
   - To import a message list previously saved to a text file, select Import and supply the filename of the previously saved file.
   - To convert a previously saved message list into an Excel* file, open the text file in Excel and expand the column widths as necessary.